

# User Guide

24 NOV 2022

VMware Cloud Director Availability 4.5

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](http://www.vmware.com)

Copyright © 2018-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>1</b>	<b>User Guide</b>	<b>5</b>
<b>2</b>	<b>Accessing VMware Cloud Director Availability</b>	<b>6</b>
	Access the VMware Cloud Director Availability vSphere Client Plug-In	6
	Accessing the VMware Cloud Director Availability Tenant Portal	7
	Log In to the VMware Cloud Director Availability Tenant Portal	8
	Log In by Using the VMware Cloud Director™ Tenant Portal	8
	Accessing the VMware Cloud Director Availability Provider Portal	9
	Log In to VMware Cloud Director Availability as a Provider	9
	Log In by Using the VMware Cloud Director™ Provider Admin Portal	10
<b>3</b>	<b>Authenticating to Remote Sites</b>	<b>12</b>
	Authenticate to Remote Sites as a Tenant	16
	Authenticate to Remote Sites as a Provider	17
	Multisite Authentication	18
<b>4</b>	<b>Replicating Workloads</b>	<b>20</b>
	Create a Protection	28
	Create a Migration	31
	Create a Replication for Encrypted Virtual Machines	34
	Migrating, Failing Over, Testing, and Reversing Replications	37
	Migrate a Replication	37
	Failover of a Replication	40
	Test Failover a Replication	43
	Reverse a Replication	46
	Edit Replication Settings	48
	Configure Recovery Settings for vSphere DR and Migration	49
	Replicating with Cloud Director Site	50
	Configuring Replication Policies	51
	Configuring SLA Profiles	60
	Grouping Virtual Machine Replications in a vApp Replication to the Cloud	65
	Using Replication Seeds	68
	Select a Storage Policy	73
	Configure Recovery Settings and Guest Customization	74
	Recovery Plans	84
	Migrating vApp Templates between Cloud Sites	92
	VDC Compute Policies	95
	Using Instances	97

Store an Instance	101
Delete an Instance	102
Selecting Replicated Disks	102
Select Replicated Disks	104
Replication States	104

## 5 Monitoring 106

Advisories Notifications	106
RPO Compliance Reports	108
Monitoring the Traffic Usage	110
Monitor the Traffic Usage as a Tenant	111
Monitor and Export Organization Traffic Usage as a Service Provider	112
Monitor the Traffic Usage of a Virtual Machine Replication	113
Monitoring the Disk Usage	114
Monitor the Disk Usage as a Tenant	114
Monitor and Export Organization Disk Usage as a Service Provider	115
Monitor the Disk Usage of a Virtual Machine Replication	116
Monitoring the Required Resources	117
Monitor the Required Resources as a Tenant	118
Monitor the Required Resources as a Provider	119
Forward Tenant Event Notifications	120

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:

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

## Access the VMware Cloud Director Availability vSphere Client Plug-In

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 registers in vCenter Server during the initial configuration of the VMware Cloud Director Availability appliance.

Access the VMware Cloud Director Availability vSphere Client Plug-In for monitoring and operating with incoming and outgoing replications and performing appliance management tasks.

### Prerequisites

- Verify that your user profile is a member of the **ADMINISTRATORS** group in vSphere and ensure that the user has sufficient privileges to see and interact with vSphere workloads.
- Verify that the version of vCenter Server is 6.5 Update 3 or later. For vCenter Server 6.5 Update 2 or earlier, see [Accessing the VMware Cloud Director Availability Tenant Portal](#).

### Procedure

- 1 Log in to the vSphere Client.

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 On-Premises to Cloud Director Replication 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.
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.

## 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.

- Alternatively, tenants can directly log in by using vSphere. For more information, see [Access the VMware Cloud Director Availability vSphere Client Plug-In](#).
- **VMware Cloud Director-backed sites:**  
VMware Cloud Director Availability allows logins by using the VMware Cloud Director credentials.
- **vSphere DR and Migration:**  
VMware Cloud Director Availability 4.4 or later allows logins to vCenter Server sites, not backed by VMware Cloud Director by using the vSphere single-sign-on credentials.

### Prerequisites

- **For VMware Cloud Director-backed sites:**  
Verify that your VMware Cloud Director tenant user profile has **Organization Administrator** privileges.
- **Alternatively, for vSphere DR and migration:**  
Verify that your vSphere tenant user profile has **VRUSERS** privileges and ensure that the user has sufficient privileges to see and interact with vSphere workloads.

### Procedure

- 1 In a Web Browser, go to the VMware Cloud Director Availability Tenant Portal at **https://Service Endpoint/ui/login**.
- 2 Authenticate to VMware Cloud Director Availability as a tenant.
  - **For VMware Cloud Director-backed sites:**  
Enter your **Organization Administrator** user credentials as **username@Org-Name**.
  - **For vSphere DR and migration:**  
Enter your vSphere single-sign-on user credentials.
- 3 To login as a tenant, 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.

---

**Note** Attempting to log in by using a user with insufficient rights assigned to their role in VMware Cloud Director results in:

The original error message is:

Permission denied.

For information about the required user roles privileges, see [Users Roles Rights and Sessions](#) in the Security Guide.

---

## 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.

- **VMware Cloud Director-backed sites:**

VMware Cloud Director Availability allows logins by using VMware Cloud Director credentials.

- **vSphere DR and Migration:**

VMware Cloud Director Availability 4.4 or later allows logins to vCenter Server sites, not backed by VMware Cloud Director by using vSphere single-sign-on credentials.

### Prerequisites

- **For VMware Cloud Director-backed sites:**

Verify that your VMware Cloud Director provider user profile has **System Administrator** privileges.

■ **For vSphere DR and Migration:**

Verify that your vSphere provider user profile has **ADMINISTRATORS** or **VRADMINISTRATORS** privileges and ensure that the user has sufficient privileges to see and interact with vSphere workloads.

For example, the **Administrator@vsphere.local** single sign-on user is a member of the **ADMINISTRATORS** group.

#### 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 Authenticate to VMware Cloud Director Availability as a provider.
  - Select **Appliance login** and enter the **root** user password.
  - Alternatively, select **SSO login** and enter the user name as:
    - **For VMware Cloud Director-backed sites:**

Enter your **System Administrator** user credentials as **`providerusername@system`**.

- **For vSphere DR and migration:**

Enter your vSphere single-sign-on user credentials, for example **`Administrator@vsphere.local`**.

- 3 To login as a provider, click **Login**.

## 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.

---

**Note** As a **System Administrator** user, for impersonation on behalf of the tenant organization:

- 1 As a **provider**, create a new user with **Organization Administrator** role for the tenant organization.
  - 2 Authenticate with the new user account for managing replications on behalf of the tenant organization.
- 

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 Director Replication Management Appliance by clicking **Accept**.

You must trust the SSL certificate of the Cloud Director 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.

# 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

By replicating the workload from the source site to the destination site, VMware Cloud Director Availability protects or migrates vApps and virtual machines. These replications are either incoming from a source site or outgoing to a destination site. One vApp or one virtual machine replicates only to one destination site.

Replicate a single workload by protecting or migrating its vApps and virtual machines from one source site to a single destination site.

## Replication Types

The replications are two 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.

The providers allow 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 the protections to or from the site, the provider must modify the default policy. Alternatively, to keep disaster recovery only for subscribers, the provider assigns 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 replications to and from sites backed by VMware Cloud Director with **Classic** data engine selected, when starting a replication with a virtual machine that is already configured for replication by another replication solution, VMware Cloud Director Availability reconfigures it for replicating.

## Replications Use Cases

VMware Cloud Director Availability supports cross-site replications between the following source and destination sites, as shown in the table, depending on both the source and the destination of the replication and the selected data engine:

- **Classic** data engine supports both replication types - protections and migrations: 
- **VMC** data engine supports migrations only: 
- Not available: 

**Table 4-1. VMware Cloud Director Availability cross-site support**

Source site*	Destination site						
	VMware Cloud Director site	On-premises vCenter Server	CDS-managed VMC SDDC	CDS-managed AVS SDDC	CDS-managed GCVE SDDC	CDS-managed OCVS SDDC	CDS-managed on-premises pVDC
VMware Cloud Director site							
On-premises vCenter Server		 **					
CDS-managed VMC SDDC							
CDS-managed AVS SDDC							
CDS-managed GCVE SDDC							
CDS-managed OCVS SDDC							
CDS-managed on-premises pVDC							

\* Source and destination sites architecture and deployment information can be found in the following documentation:

- For VMware Cloud Director-backed cloud sites, see [Deployment Architecture in the Cloud Director Site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

- For on-premises vCenter Server sites, in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site* see:
  - On-premises vCenter Server site paired with VMware Cloud Director-backed cloud site - [Deployment Architecture On-Premises](#).
  - \*\* vSphere DR and migration between two vCenter Server instances - [Deployment Architecture and Requirements for vSphere DR and Migration](#).
- CDS-managed VMC SDDC - for a software-defined data center (SDDC) in VMware Cloud on AWS (VMC) that is managed by VMware Cloud Director service (CDS), see [Migration to VMware Cloud Director service](#) in the *Migration to VMware Cloud Director service Guide*.
- CDS-managed AVS SDDC - for an SDDC in Azure VMware Services (AVS) that is managed by VMware Cloud Director service, see [Migration to VMware Cloud Director service](#).
- CDS-managed GCVE SDDC - for an SDDC in Google Cloud VMware Solution (GCVE) that is managed by VMware Cloud Director service, see [Deployment Architecture in the Cloud Director Site](#).
- CDS-managed OCVS SDDC - for an SDDC in Oracle Cloud VMware Solution (OCVS) that is managed by VMware Cloud Director service, see [Deployment Architecture in the Cloud Director Site](#).
- CDS-managed on-premises pVDC - for an on-premises provider VDC managed by VMware Cloud Director service, see [Deployment Architecture in the Cloud Director Site](#).

For information about selecting the **VMC** and the **Classic** data engines, see [Activate Data Engine for Replications](#).

## 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, a 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, 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

---

**Note** For vSphere DR and migration between vCenter Server instances not backed by VMware Cloud Director, the principal always is **System**. This user is the **SSO Admin Username** that registers the appliance with the vCenter Server Lookup service. This same user owns all replications, meaning all users that see a replication have full control over it.

---

For replications with cloud sites backed by VMware Cloud Director, the user that starts a new replication becomes its owner, depending on the selected default replication 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.

### Change Default Replication Owner

In VMware Cloud Director Availability 4.4 and later, as a **system administrator**, to change the default replication owner for new replications, in the left pane under **Configuration**, click **Settings**, then under **Site settings** next to **Default Replication owner**, click **Edit**. In the **Change Default Replication Owner** window, select an owner as default for new replications and click **Apply**.

- **System organization** - assigns the system administrator as a default replication owner for new replications. Tenants do not see replications owned by the system organization.
- **Tenant organization** - assigns the organization in the destination\* site as a default replication owner for new replications, allowing the tenants from the destination organization both to see and interact with the new replications.

### Change Existing Replications Owner

As a **system administrator**, to change the owner of one or more already started replications, in the left pane choose a replication direction and click **Incoming Replications** or **Outgoing Replications**, then select the replications 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 the replications owner.
- **Tenant organization** - assigns the organization in the destination\* site as replications owner.

\* Destination organization ownership applies both for replications from cloud sites to cloud sites and from on-premises sites to cloud sites. When the destination of the replication is an on-premises site, assigns the organization in the source site as a replication owner, allowing the tenants from the source organization seeing and interacting 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.



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

**Note** The hardware version of the virtual machines in the source site must not be higher than the destination site. This limitation applies both for vSphere DR and migration between vCenter Server instances and for replications with cloud sites backed by VMware Cloud Director.

For information about the hardware versions, see [Virtual Machine Compatibility](#) in the *vSphere* documentation.

- 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

After starting a replication or changing its storage profile, VMware Cloud Director Availability creates the independent disk with thick provision VMDK, which, on its first resize, becomes a thin provision VMDK.

As a result, from the replication start or change of storage profile until the first resize, the consumed storage equals double the source virtual machine size.

**Table 4-2. Replication alignment with the destination storage profile**

Replications		Replica Disk Provisioning Type
Replications using seed	Thin provision seed disk	Thin provision
	Thick provision lazy zeroed seed disk	Thick provision lazy zeroed
	Thick provision eager zeroed seed disk	Thick provision eager zeroed
New replications with no seed in VMware Cloud Director Availability 4.4 and later	Allowed organization VDC thin provisioning.	Thin provision
	Disallowed organization VDC thin provisioning.	Thick provision lazy zeroed

Table 4-2. Replication alignment with the destination storage profile (continued)

Replications	Replica Disk Provisioning Type
Existing started replications: <ul style="list-style-type: none"> <li>■ in earlier VMware Cloud Director Availability versions.</li> <li>■ after upgrading to VMware Cloud Director Availability 4.4.</li> </ul>	Retain the existing disks types, depending on the seed disk types
vSphere DR and migration between vCenter Server sites	When creating each replication, select one of the following provisioning formats for the destination disk: <ul style="list-style-type: none"> <li>■ Thin provision</li> <li>■ Thick provision lazy zeroed</li> <li>■ Thick provision eager zeroed</li> </ul>

By default, VMware Cloud Director Availability 4.4 and later for new replications:

- To and from cloud sites backed by VMware Cloud Director provision the disk type, depending on whether the destination storage allows thin provisioning in the VMware Cloud Director organization VDC. For more information, see [Modify the VM Provisioning Settings of an Organization Virtual Data Center](#) in the *VMware Cloud Director* documentation.
- For vSphere DR and migration between vCenter Server sites, select the destination disk provisioning format when creating each replication.

The disk provisioning type never changes after creating the replication: starting a replication permanently provisions its replicated disks as thin or thick. The disk provisioning type does not change during the replication lifespan, neither when performing a failover nor when performing a migration.

Existing replications started in an earlier VMware Cloud Director Availability version, after upgrading to version 4.4 retain their disk provisioning type, and for the organization VDC storage policy to take precedence, delete the replications then create and start them again, without using existing replication seeds.

## Seed

The replicated disk provisioning type always depends on whether a replication uses a seed. For information about the seeds, see [Using Replication Seeds](#).

- When using seed in the replication, the provisioning of each replica disk retains the provisioning of each replication seed virtual machine disk:
  - Thick-provisioned replication seed disks always provision thick lazy zeroed replica disks.
  - Thin-provisioned replication seed disks always provision thin replica disks.

For example, a replication seed virtual machine that contains one thin-provisioned and one thick-provisioned disk always replicates as one thin and one thick disk in the destination site, regardless of the storage policy of the organization VDC.

- When not using seed in the replication, the provisioning of the replicated disks follows the preceding logic.

## Replicating Other Storage

### Non-volatile memory express (NVMe)

To replicate virtual machines with an NVMe disk controller, VMware Cloud Director Availability requires that both the source and the destination sites run vCenter Server 7.0 U2 or later.

### 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 replicated.
- RDM in **physical** compatibility mode is skipped from replication.

### Multi-writer Disks

VMware Cloud Director Availability does not replicate disks in multi-writer mode.

### Independent Disks

VMware Cloud Director Availability does not replicate independent disks.

### Change Block Tracking (CBT)

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

## Storage Space Consumption in the Destination

**Note** Replica files keep expanding until there is space on the datastore, disregarding any restrictions in VMware Cloud Director:

VMware Cloud Director Availability resizes the independent disks associated with the replicated virtual machines to represent the actual used space by the replica data. That causes VMware Cloud Director to display the actual allocation size, which might be greater than the configured allocation size limit of the organization VDC.

Some replication settings and operations require double space in the destination storage, compared with the size of the source virtual machine.

- For both test failover and for reverse operations, the destination storage must accommodate double the space for the disk size of the source virtual machine. For information about the prerequisites for each operation, see [Test Failover a Replication](#) and [Reverse a Replication](#). In VMware Cloud Director Availability 4.2 and later, failover tasks require destination storage space equal to the source workload size. For information about the test failover storage consumption with examples for a datastore and for VMware vSAN storage, see [VMware Cloud Director Availability Storage Requirements](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- When using seed, the destination storage must accommodate double the space for the disk size of the source virtual machine. For information about the space requirements when using seed, see [Destination datastore space consumption](#).

This chapter includes the following topics:

- [Create a Protection](#)
- [Create a Migration](#)
- [Create a Replication for Encrypted Virtual Machines](#)
- [Migrating, Failing Over, Testing, and Reversing Replications](#)
- [Edit Replication Settings](#)
- [Configure Recovery Settings for vSphere DR and Migration](#)
- [Replicating with Cloud Director Site](#)
- [Using Instances](#)
- [Selecting Replicated Disks](#)
- [Replication States](#)

## Create a Protection

Configure new protection to replicate the workload from one site to another while keeping it running in the source site. After a successful replication, if the source site becomes unavailable, you can fail over and power on the protected workload in the destination site.

### Prerequisites

- Verify that VMware Cloud Director Availability 4.5 or later is deployed for selecting a sizing 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**.

- Alternatively, from the on-premises vSphere Client either under the **Hosts and Clusters** or under the **VMs and Templates** inventories, right-click the virtual machine or from the **Actions** menu select:

- **Configure Protection**
- **Configure Migration**
- **Fast Migration**

- 2 Click **All Actions > New Protection**.

- 3 To create the protection, depending on the source and destination sites complete the **New Replication** wizard.

- **For on-premises site as source:**

- On the **Source VMs** page, select the source virtual machines, then click **Next**.

For cloud site backed by VMware Cloud Director as destination, optionally activate the **Group VMs to a single vApp** toggle.

- (Optional) On the **vApp Settings** page that shows after activating the **Group VMs to a single vApp** toggle from the **Source VMs** page, if you enter the vApp name of an already existing vApp replication the selected virtual machines become part of that replication. Optionally, when protecting multiple virtual machines change their order of boot by dragging each row and set optional boot delay between each replicated virtual machine in the resulting vApp, then click **Next**.

- **For cloud site backed by VMware Cloud Director as source:**

- On the **Source VMs and vApps** page, select the source workloads, then click **Next**.

- **For vSphere DR and migration from vCenter Server site to vCenter Server site as destination:**

- On the **Datastore** page, select the destination datastore for placing the recovered workloads, then click **Next**.

- **For cloud site backed by VMware Cloud Director as destination:**

- On the **Destination VDC and Storage policy** page, select the destination virtual data center and the storage policy for placing the recovered workloads, then 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 refreshes once every 10 minutes.

- On the **Settings** page, configure the following protection settings depending on the source and destination sites, then click **Next**.

Option	Description
Use SLA profile	<ul style="list-style-type: none"> <li>■ To set the SLA settings of the replication, select any of the preconfigured SLA profiles.</li> <li>■ Alternatively, select <b>Configure settings manually</b> then select the following SLA settings.</li> </ul>
Target recovery point objective (RPO)	<p>If you selected <b>Configure settings manually</b>, 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.</p> <p><b>Note</b> 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 <a href="#">Chapter 4 Replicating Workloads</a>.</p> <p>With one minute RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.</p>
Retention policy for point in time instances	<p>If you selected <b>Configure settings manually</b>, 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.</p> <p>The retention distance unit must be greater than RPO.</p>
Compress replication traffic	<p>If you selected <b>Configure settings manually</b>, to apply compression on the replication data traffic for reducing the network data traffic at the expense of CPU, select this option.</p>
Disk Provisioning	<p>For vSphere DR and migration between vCenter Server sites, select one of the following provisioning formats for the destination disk:</p> <ul style="list-style-type: none"> <li>■ <b>Thin Provision</b></li> <li>■ <b>Thick Provision Lazy Zeroed</b></li> <li>■ <b>Thick Provision Eager Zeroed</b></li> </ul> <p>For information about the disk provisioning, see <a href="#">Replicating Thin or Thick Provisioning Virtual Disks</a>.</p>
Delay start synchronization	<p>If you selected <b>Configure settings manually</b>, choose the following option.</p> <ul style="list-style-type: none"> <li>■ To schedule the start of the replication, select this option and enter the local date and time to start the replication.</li> <li>■ To start the replication when the wizard finishes, leave this option deselected.</li> </ul>

Option	Description
VDC policy settings	<ul style="list-style-type: none"> <li>■ VDC VM placement policy</li> <li>■ VDC VM sizing policy</li> </ul> <p>For a protection to a cloud site backed by VMware Cloud Director, optionally from the drop-down menus, select the organization VDC compute policies to apply on the recovered workloads. For more information, see <a href="#">VDC Compute Policies</a>.</p> <p>If you do not select a sizing policy for the replication, then VMware Cloud Director automatically applies the system default sizing policy on the destination virtual machine.</p>
Exclude disks	Optionally, to select specific hard disks of the virtual machines for replicating to the destination site and reduce the replication data network traffic, activate this toggle.
Configure Seed VMs	For protection to or from a cloud site backed by VMware Cloud Director, optionally, to select a previous copy of the virtual machines in the destination site and reduce the replication data network traffic, activate this toggle.

- (Optional) On the **Replicated Disks** page that shows after activating the **Exclude disks** toggle from the **Settings** page, deselect the disks of the selected workload to exclude from replicating, then click **Next**.
- (Optional) On the **Seed VM** page, that shows after activating the **Configure Seed VMs** toggle from the **Settings** page, select a vApp or a virtual machine as a replication seed, then click **Next**.
- On the **Ready to complete** page, verify that the protection settings are correct, then click **Finish**.

## Results

After completing the wizard, in the Replication type column for this replication, you see a `Protection` state.

## What to do next

You can fail over, or test, or migrate the protected workload to the destination site. To fail over, the source workload does not need be operational. For more information, see [Failover of a Replication](#), or [Test Failover a Replication](#), or [Migrate a Replication](#).

# Create a Migration

Configure a new migration to replicate the workload from one site to another. After a successful replication, you can migrate the workload to a remote site for running it in the destination site.

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

## Prerequisites

- Verify that VMware Cloud Director Availability 4.5 or later is deployed for selecting a sizing 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**.
  - Alternatively, from the on-premises vSphere Client either under the **Hosts and Clusters** or under the **VMs and Templates** inventories, right-click the virtual machine or from the **Actions** menu select:
    - **Configure Protection**
    - **Configure Migration**
    - **Fast Migration**
- 2 After selecting the replication direction, initiate creating a new migration.
  - To configure the migration with all migration settings, click **All Actions > New migration**.
  - Alternatively, for one-click migration while skipping the settings, click **All Actions > Fast migration**. vSphere DR and migration between vCenter Server sites do not allow one-click migration.

One-click migration requires only selecting the source workloads for migration, skipping the migration settings configuration and allowing finishing the replication wizard or navigating back for configuring the settings.

- 3 To create the migration, depending on the source and destination sites complete the **New Migration** wizard.
  - **For on-premises site as source:**
  - On the **Source VMs** page, select the source virtual machines, then click **Next**.  
 For cloud site backed by VMware Cloud Director as destination, optionally activate the **Group VMs to a single vApp** toggle.
  - (Optional) On the **vApp Settings** page that shows after activating the **Group VMs to a single vApp** toggle from the **Source VMs** page, if you enter the vApp name of an already existing vApp replication the selected virtual machines become part of that replication. Optionally, when migrating multiple virtual machines change their order of boot by dragging each row and set optional boot delay between each replicated virtual machine in the resulting vApp, then click **Next**.



- **For cloud site backed by VMware Cloud Director as source:**
- On the **Source VMs and vApps** page, select the source workloads, then click **Next**.
- **For vSphere DR and migration from vCenter Server site to vCenter Server site as destination:**
- On the **Datastore** page, select the destination datastore for placing the recovered workloads, then click **Next**.
- **For cloud site backed by VMware Cloud Director as destination:**
- On the **Destination VDC and Storage policy** page, select the destination virtual data center and the storage policy for placing the recovered workloads, then 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 refreshes once every 10 minutes.

- On the **Settings** page, configure the following migration settings depending on the source and destination sites, then click **Next**.

One-click **Fast migration** skips the **Settings** page directly to the **Ready to complete** page. To configure the migration settings, click the **Settings** page, or alternatively, click **Back**.

Option	Description
<b>Compress replication traffic</b>	For an incoming migration to an on-premises site, to apply compression on the replication data traffic and reduce the network data traffic at the expense of CPU, leave this toggle activated.
<b>Disk Provisioning</b>	<p>For vSphere DR and migration between vCenter Server sites, select one of the following provisioning formats for the destination disk:</p> <ul style="list-style-type: none"> <li>■ <b>Thin Provision</b></li> <li>■ <b>Thick Provision Lazy Zeroed</b></li> <li>■ <b>Thick Provision Eager Zeroed</b></li> </ul> <p>For information about the disk provisioning, see <a href="#">Replicating Thin or Thick Provisioning Virtual Disks</a>.</p>
<b>Delay start synchronization</b>	<ul style="list-style-type: none"> <li>■ To start the initial synchronization when the wizard finishes, leave this toggle deactivated.</li> <li>■ Alternatively, to schedule the start of the first synchronization, activate this toggle, then enter the local date and time.</li> </ul>
<b>VDC policy settings</b>	<ul style="list-style-type: none"> <li>■ <b>VDC VM placement policy</b></li> <li>■ <b>VDC VM sizing policy</b></li> </ul> <p>For a migration to a cloud site backed by VMware Cloud Director, optionally from the drop-down menus, select the organization VDC compute policies to apply on the recovered workloads. For more information, see <a href="#">VDC Compute Policies</a>.</p> <p>If you do not select a sizing policy for the replication, then VMware Cloud Director automatically applies the system default sizing policy on the destination virtual machine.</p>

Option	Description
<b>Exclude disks</b>	Optionally, to select specific hard disks of the virtual machines for replicating to the destination site and reduce the replication data network traffic, activate this toggle.
<b>Configure Seed VMs</b>	For migration to or from a cloud site backed by VMware Cloud Director, optionally, to select a previous copy of the virtual machines in the destination site and reduce the replication data network traffic, activate this toggle.

- (Optional) On the **Replicated Disks** page that shows after activating the **Exclude disks** toggle from the **Settings** page, deselect the disks of the selected workload to exclude from replicating, then click **Next**.
- (Optional) On the **Seed VM** page, that shows after activating the **Configure Seed VMs** toggle from the **Settings** page, select a vApp or a virtual machine as a replication seed, then click **Next**.
- On the **Ready to complete** page, verify that the migration settings are correct, then click **Finish**.

One-click migration, once used, skips the migration settings configuration. You can still configure the migration settings, by clicking the **Settings** page, or alternatively, by clicking **Back**.

## Results

After completing the wizard, in the Replication type column for this replication, you see a *Migration state*.

## What to do next

You can migrate, or test, or fail over the workload to the destination site. For more information, see [Migrate a Replication](#) or [Test Failover a Replication](#) or [Failover of a Replication](#).

# Create a Replication for Encrypted Virtual Machines

The storage policy drives the encryption for virtual machines. Enable the encryption in the storage policy then 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.

---

**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 it then starting it.

## Prerequisites

### Prerequisites for the versions in the source and in the destination sites:

- For vSphere DR and migration, use vCenter Server 7.0 U2 or later and VMware Cloud Director Availability 4.5 in both the source and the destination site.
- Alternatively, for cloud sites backed by VMware Cloud Director, use vCenter Server 6.7 U3 or later, any supported version of VMware Cloud Director Availability, and VMware Cloud Director 10.1 or later.

### Prerequisites for the ESXi hosts in both the source and in the destination sites:

Install the HBR agent VIB in all the ESXi hosts. To download the HBR agent VIB file directly from the appliance:

- Depending on the appliance type and deployment, from the following URL on the appliance download the:
  - `https://vCenter_Replication_Management_Appliance_Address:8043/hbr-agent.vib` file.
  - `https://Replicator_Appliance_Address/hbr-agent.vib` file.
- Alternatively, from the appliance filesystem, download the `/opt/vmware/hbr/vib/vmware-hbr-agent-build_number.i386.vib` file.

After installing the HBR agent, it encrypts the traffic originating from the source ESXi host, providing end-to-end encryption. Installing the HBR agent in the destination ESXi host allows reversing the replications and the reverse replications traffic is also encrypted end-to-end.

For more information about VIBs and how to install them, see [VIBs, Image Profiles, and Software Depots](#) in the *VMware ESXi Upgrade Guide*.

### Prerequisites for the vCenter Server instances in both the source and in the destination sites:

- Configure a key provider in vSphere. For more information, see [Virtual Machine Encryption](#) in the *vSphere Security Guide*.
  - For vSphere 7.0 and later, configure a VMware vSphere® Native Key Provider™ which does not require an external key server. For more information, see [Configuring and Managing vSphere Native Key Provider](#) in the *vSphere Security Guide*.
  - Alternatively, for vSphere 6.x or 7.x and cloud sites backed by VMware Cloud Director, configure an external key server, previously known as Key Management Server cluster and ensure that the cluster names match. For information about configuring a standard key provider, see [Set up the Key Management Server Cluster](#) in the *vSphere Security Guide*.
- Use the same key provider for both the source and the destination vCenter Server instances. For more information, see [vSphere Native Key Provider Overview](#) in the *vSphere Security Guide*.

To ensure that both sites use the same vSphere key provider, for example, backup the key provider from site A then restore it and set it as default in site B.

- In vSphere, the encrypted virtual machines require an encryption storage policy. For more information, see [Create an Encryption Storage Policy](#) and [Create an Encrypted Virtual Machine](#) or [Encrypt an Existing Virtual Machine or Virtual Disk](#) in the *vSphere Security Guide*.

#### Prerequisites for cloud sites backed by VMware Cloud Director:

- Verify that the same key provider is used in both the source and the destination vCenter Server instances. For more information, see [vSphere Native Key Provider Overview](#) or [Set up the Key Management Server Cluster](#) in the *vSphere Security Guide*.
- 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 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 between cloud sites backed by VMware Cloud Director, choose either an incoming replication from a cloud site, or an outgoing replication to a cloud site.
  - For vSphere DR and migration, encrypted replications support all replication directions and you can choose any replication direction.
- 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**.

---

**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 that contains only encrypted virtual machines uses encryption for the replication data communication.

## Migrating, Failing Over, Testing, and Reversing Replications

From either the source or the destination sites, migrate, failover, test, and reverse already replicated workloads in VMware Cloud Director Availability.

### Migrate a Replication

Migrating an already created replication to a remote site runs the workload in the destination site, powering off the source workload.

#### Prerequisites

- Verify that the workload is already protected in the destination site, before performing a migrate. For more information, see [Create a Migration](#).
- Verify that VMware Cloud Director Availability 4.5 or later is deployed for selecting VDC compute policies when migrating to and from cloud sites backed by VMware Cloud Director.
- 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 an exiting replication to migrate over and click **All actions > Migrate**.
- 3 Complete the **Migrate** wizard and depending on the source and destination sites configure the different migration settings for the selected workloads.
  - Start from step **e** when migrating to or from cloud sites backed by VMware Cloud Director, skipping steps **a**, **b**, **c**, and **d**.
  - Start from step **a** for vSphere DR and migration between vCenter Server sites.
  - a The **Default Settings** page shows when the selected replication is already configured with recovery settings and to use them and skip to step **e**, select **Use preset Recovery Settings**.

For information about configuring the recovery settings for vSphere DR and migration between vCenter Server sites, see [Configure Recovery Settings for vSphere DR and Migration](#).
  - b On the **VM Folder** page, select a destination location for storing the recovered virtual machines, then click **Next**.
  - c On the **Compute Resource** page, select a destination compute resource for the recovered virtual machines, then click **Next**.
  - d On the **Network Mappings** page, select a network mapping for each adapter connected to each virtual machine, then click **Next**.

- e On the **Migrate Settings** page, select the configuration for the recovered workloads depending on the destination site, then click **Next**.

Option	Description
Instances handling after recovery	<ul style="list-style-type: none"> <li>■ <b>Default:</b> selecting this option provides the lowest Recovery Time Objective (RTO). To optimize performance, perform instances consolidation after the recover task completes.</li> <li>■ <b>Expose PITs:</b> only available for migrating already protected virtual machines to an on-premises site as a destination, selecting this option allows instances older than the selected instance to be exported as snapshots to the recovered virtual machine.</li> <li>■ <b>Consolidate:</b> selecting this option consolidates all instances into the recovered disk. This can improve the runtime performance of the recovered virtual machine in the destination site but might significantly increase the RTO.</li> </ul>
Power settings	<p>Powers on the recovered workloads in the destination site after the migrate task completes.</p> <hr/> <p><b>Note</b> In the source site, all source workloads in the replication power off after a successful recovery.</p>
Network Settings	<p>For migrations to and from cloud sites backed by VMware Cloud Director:</p> <ul style="list-style-type: none"> <li>■ Select <b>Apply preconfigured network settings on failover</b>, to assign the network configured during the virtual machine replication.</li> <li>■ Select <b>Connect all VMs to network</b> and from the drop-down menu select a network to connect the replicated virtual machines to.</li> </ul>
VDC policy settings	<ul style="list-style-type: none"> <li>■ <b>VDC VM placement policy</b></li> <li>■ <b>VDC VM sizing policy</b></li> </ul> <p>For a migration to or from a cloud site backed by VMware Cloud Director, optionally from the drop-down menus, select the organization VDC compute policies to apply on the recovered workloads. For more information, see <a href="#">VDC Compute Policies</a>.</p> <p>If you do not select a sizing policy for the replication, then VMware Cloud Director automatically applies the system default sizing policy on the destination virtual machine.</p>

- f On the **Ready To Complete** page, verify that the migration settings are correct, then click **Finish**.

After completing the **Migrate** wizard, the migration workflow now executes the following steps:

- 1 Powered on source virtual machines first synchronize.
- 2 Power off the source virtual machines.
- 3 After the source virtual machines power off then synchronize.
- 4 Finally, import the recovered virtual machines in the destination site.

The Last changed column shows the migration progress in percentages. When the migration completes, the Recovery state column of this replication shows a `Failed-Over` state.

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

## Results

After the migrate task completes, the failed over workload runs in the destination site and the source workload powers off and is no longer protected.

## 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 traffic of this replication, remove the replication and remove all retained replication instances, by clicking **All actions > Delete replication**.

## Failover of a Replication

If the protected source site is unavailable, in the destination site for an already created replication perform a disaster recovery operation and recover the workload.

## Prerequisites

### Important

- 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 workload is already protected in the destination site. For more information, see [Create a Protection](#).
- Verify that VMware Cloud Director Availability 4.5 or later is deployed for selecting VDC compute policies when failing over to and from cloud sites backed by VMware Cloud Director.
- 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 an exiting replication to fail over and click **All actions > Failover**.



- 3 Complete the **Failover** wizard and depending on the source and destination sites configure the different failover settings for the selected workloads.

- Start from step **e** when migrating to or from cloud sites backed by VMware Cloud Director, skipping steps **a**, **b**, **c**, and **d**.
- Start from step **a** for vSphere DR and migration between vCenter Server sites.
- a The **Default Settings** page shows when the selected replication is already configured with recovery settings and to use them and skip to step **e**, select **Use preset Recovery Settings**.

For information about configuring the recovery settings for vSphere DR and migration between vCenter Server sites, see [Configure Recovery Settings for vSphere DR and Migration](#).

- b On the **VM Folder** page, select a destination location for storing the failed over virtual machines, then click **Next**.
- c On the **Compute Resource** page, select a destination compute resource for the failed over virtual machines, then click **Next**.
- d On the **Network Mappings** page, select a network mapping for each adapter connected to each virtual machine, then click **Next**.

- e On the **Recovery Settings** page, select the configuration for the recovered workload depending on the destination site, then click **Next**.

Option	Description
<b>Instances handling after recovery</b>	<ul style="list-style-type: none"> <li>■ <b>Default:</b> selecting this option provides the lowest Recovery Time Objective (RTO). To optimize performance, perform instances consolidation after the recover task completes.</li> <li>■ <b>Expose PITs:</b> only available for failing over already protected virtual machines to an on-premises site as a destination, selecting this option allows instances older than the selected instance to be exported as snapshots to the recovered virtual machine.</li> <li>■ <b>Consolidate:</b> selecting this option consolidates all instances into the recovered disk. This can improve the runtime performance of the recovered virtual machine in the destination site but might significantly increase the RTO.</li> </ul>
<b>Power settings</b>	Powers on the recovered workload in the destination site after the failover task completes.
<b>Network Settings</b>	<p>For migrations to and from cloud sites backed by VMware Cloud Director:</p> <ul style="list-style-type: none"> <li>■ Select <b>Apply preconfigured network settings on failover</b>, to assign the network configured during the virtual machine replication.</li> <li>■ Select <b>Connect all VMs to network</b> and from the drop-down menu select a network to connect the replicated virtual machines to.</li> </ul>
<b>VDC policy settings</b>	<ul style="list-style-type: none"> <li>■ <b>VDC VM placement policy</b></li> <li>■ <b>VDC VM sizing policy</b></li> </ul> <p>For a failover to or from a cloud site backed by VMware Cloud Director, optionally from the drop-down menus, select the organization VDC compute policies to apply on the recovered workloads. For more information, see <a href="#">VDC Compute Policies</a>.</p> <p>If you do not select a sizing policy for the replication, then VMware Cloud Director automatically applies the system default sizing policy on the destination virtual machine.</p>

- f On the **Recovery Instance** page, if instances are preserved configure the recovery point in time, then click **Next**.

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

- g On the **Ready To Complete** page, verify that the failover settings are correct, then click **Finish**.

The Last changed column shows the failover progress in percentages. When the failover of the workload completes, the Recovery state column of this replication shows a green **Failed-Over** state.

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

### Results

After the failover task completes, the failed over workload runs in the destination site and the source workload is no longer protected.

### 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 traffic of this replication, remove the replication and remove all retained replication instances, by clicking **All actions > Delete replication**.

## Test Failover a Replication

Performing a test failover for an already created replication validates that the workload from the source site replicates correctly in the destination site.

Perform a test failover for an existing replication, then cleanup 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 a successful test failover. For information about the storage requirements, see [Storage Space Consumption in the Destination](#).
- 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 workload is already protected in the destination site. For more information, see [Create a Protection](#).
- Verify that VMware Cloud Director Availability 4.5 or later is deployed for selecting VDC compute policies when testing failover to and from cloud sites backed by VMware Cloud Director.
- 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 an exiting replication to test the failover, then click **All actions > Test**.
- 3 Complete the **Test** wizard and depending on the source and destination sites configure the different test failover settings for the selected workloads.
  - Start from step **e** when migrating to or from cloud sites backed by VMware Cloud Director, skipping steps **a**, **b**, **c**, and **d**.
  - Start from step **a** for vSphere DR and migration between vCenter Server sites.
  - a The **Default Settings** page shows when the selected replication is already configured with recovery settings and to use them and skip to step **e**, select **Use preset Recovery Settings**.

For information about configuring the recovery settings for vSphere DR and migration between vCenter Server sites, see [Configure Recovery Settings for vSphere DR and Migration](#).
  - b On the **VM Folder** page, select a destination location for storing the test failover virtual machines, then click **Next**.
  - c On the **Compute Resource** page, select a destination compute resource for the test failover virtual machines, then click **Next**.
  - d On the **Network Mappings** page, select a network mapping for each adapter connected to each virtual machine, then click **Next**.

- e On the **Recovery Settings** page, select the configuration for the recovered test workload depending on the destination site, then click **Next**.

Option	Description
<b>Instances handling after recovery</b>	<ul style="list-style-type: none"> <li>■ <b>Default:</b> selecting this option provides the lowest Recovery Time Objective (RTO). To optimize performance, perform instances consolidation after the recover task completes.</li> <li>■ <b>Expose PITs:</b> only available for test failing over already protected virtual machines to an on-premises site as a destination, selecting this option allows instances older than the selected instance to be exported as snapshots to the recovered virtual machine.</li> </ul>
<b>Power settings</b>	Powers on the recovered workload in the destination site after the test task completes.
<b>Network Settings</b>	<p>For migrations to and from cloud sites backed by VMware Cloud Director:</p> <ul style="list-style-type: none"> <li>■ Select <b>Apply preconfigured network settings on failover</b>, to assign the network configured during the virtual machine replication.</li> <li>■ Select <b>Connect all VMs to network</b> and from the drop-down menu select a network to connect the replicated virtual machines to.</li> </ul>
<b>VDC policy settings</b>	<ul style="list-style-type: none"> <li>■ <b>VDC VM placement policy</b></li> <li>■ <b>VDC VM sizing policy</b></li> </ul> <p>For a test to or from a cloud site backed by VMware Cloud Director, optionally from the drop-down menus, select the organization VDC compute policies to apply on the recovered workloads. For more information, see <a href="#">VDC Compute Policies</a>.</p> <p>If you do not select a sizing policy for the replication, then VMware Cloud Director automatically applies the system default sizing policy on the destination virtual machine.</p>

- f On the **Recovery Instance** page, if instances are preserved configure the recovery point in time, then click **Next**.

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

- g On the **Ready To Complete** page, verify that the test settings are correct, then click **Finish**.

The Last changed column shows the test progress in percentages. When the test of the workload completes, the Recovery state column of this replication shows a green **Test image ready state**.

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

- 5 To delete the test failover results, select the replication to clean.

Performing test failover without cleaning the previous test results, executes an automatic clean up first.

- 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 [Failover of a Replication](#).
- You can perform a failover or edit the replication settings. To no longer protect the workload, you can permanently stop the traffic of this replication, remove the replication and remove all retained replication instances and cleanup any test data, by clicking **All actions > Delete replication**.

## 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

- Optimized reverse works only with replications using the **Classic** data engine. For more information, see [Activate the data engines for replicating workloads](#).
  - For vSphere DR and migration, the reversed replications always starts with a seed. As a result, the original virtual machine is deleted at the new destination. Also, **All Actions > Recovery settings** of the reversed replication pre-populate with **Recovery settings** from the original virtual machine with the test networks being the same as the failover networks.
  - 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. For information about the storage requirements, see [Storage Space Consumption in the Destination](#).
- 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 [Failover of a Replication](#) or [Migrate a Replication](#).
- 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 a Replication](#), [Failover of a Replication](#), or [Migrate a Replication](#).

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**.

# Edit Replication Settings

Modify the settings of any existing incoming or outgoing replications. The protections allow modifying RPO, instances retention rules, quiescing, and compressing the replication traffic. The migrations only allow compressing the traffic. The replications with a site backed by VMware Cloud Director also allow selecting an SLA profile and VDC compute policies.

## 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 Select a replication with a **Green** overall health.



3 Click **All Actions > Replication Settings**.

4 In the **Edit Replication Settings** window, modify the available replication settings, according to the type of the selected replications then click **Apply**.

Option	Description
Protection	<ul style="list-style-type: none"> <li>■ Select the target recovery point objective (RPO), or for protections to and from cloud sites backed by VMware Cloud Director, you can also select an SLA profile</li> <li>■ Retention rules for instances</li> <li>■ Quiesce</li> <li>■ Compress replication traffic</li> <li>■ For protections to and from cloud sites backed by VMware Cloud Director you can also select the VDC policy settings:               <ul style="list-style-type: none"> <li>■ VDC VM placement policy</li> <li>■ VDC VM sizing policy</li> </ul> </li> </ul>
Migration	<ul style="list-style-type: none"> <li>■ Compress replication traffic</li> <li>■ For migrations to and from cloud sites backed by VMware Cloud Director you can also select the VDC policy settings:               <ul style="list-style-type: none"> <li>■ VDC VM placement policy</li> <li>■ VDC VM sizing policy</li> </ul> </li> </ul>

## Results

In the **Tasks** pane, a **Reconfigure replication settings** task runs.

## Configure Recovery Settings for vSphere DR and Migration

For vSphere DR and migration between vCenter Server sites, specify the location, the compute resource, and the networks that apply when recovering the workload in the destination site.

When replicating between vCenter Server sites, before recovering the workload in the destination site, you can reconfigure the destination location and compute resource for placing the recovered workloads, and the networks for each network interface card (NIC) that connect to after recovery.

**Note** This procedure applies only for replications between vCenter Server sites, without VMware Cloud Director.

For replications to and from cloud sites backed by VMware Cloud Director, see [Configure Recovery Settings and Guest Customization](#) under [Replicating with Cloud Director Site](#).

### Prerequisites

- Verify that VMware Cloud Director Availability 4.5 is or later 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 one or more replications.
- 3 Click **All Actions > Recovery Settings**.
- 4 Complete the **Recovery settings** wizard.

- a On the **VM Folder** page, select a location for the recovered virtual machines then click **Next**.
- b On the **Compute Resource** page, select the destination compute resource for the recovered virtual machines then click **Next**.

The compute resources settings are filtered by the replica datastore placement.

- c On the **Network Mappings** page, select the networks to be applied after performing migrate or failover of each virtual machine then click **Next**.

You can select different networks to be applied for DR and for test failover:

- Under the Network column, select the destination network to apply after performing migrate or failover.
- Under the Test Network column, select the destination network that applies after a test failover.

If you do not select a network for a NIC for the specific scenario, the NIC is not connected after performing migrate, failover, or test failover.

- d On the **Ready to Complete** page, verify the selected settings before proceeding then click **Finish**.

On the **Recovery settings** tab under the replications list, you can see the configured recovery settings that apply when performing migrate, failover, or test failover.

## Results

You configured the recovery settings for the selected replications. To update the location, the compute resource, or the networks you can reconfigure the recovery settings at any time before performing migrate, failover, or test failover.

## What to do next

When performing migrate, failover, or test failover for the selected replications, on the **Default Settings** page, to use these configured recovery settings, select **Use preset Recovery Settings**. For more information, see [Migrating, Failing Over, Testing, and Reversing Replications](#).

# Replicating with Cloud Director Site

When replicating vApps and virtual machines to and from cloud sites backed by VMware Cloud Director, group the virtual machines in a vApp, organizations control replication policies, SLA

profiles, RPO, automate recovery by using plans, and advanced destination site settings like replication seed, configuring the network settings of the workload, and migrating templates.

This current chapter lists the specific replication procedures that you can only perform when replicating workloads with cloud sites backed by VMware Cloud Director.

For vSphere DR and migration, when replicating virtual machines between vCenter Server sites, only see the replication procedures under the [Chapter 4 Replicating Workloads](#) chapter which are common for replicating with any site.

## 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 to a cloud site.
- Whether an organization can be used as a replication source for outgoing migrations to an on-premises site.

#### 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 On-Premises to Cloud Director Replication Appliance. For information about the throttle, see [Bandwidth 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	Activated, by default. In both directions, the migrations are allowed, to both cloud sites and to on-premises sites.
Outgoing migrations to cloud	
Outgoing migrations to On-Premises	
Incoming protections	Deactivated, by default. In both directions, the protections are disallowed.
Outgoing protections	
Custom SLA settings	Unavailable with <b>Incoming protections</b> deactivated, as 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 activate the <b>Incoming protections</b> toggle.
Allow advanced retention rules	
Max rotated instances per protection	
Max stored instances per protection	

Table 4-3. Default Policy Attributes (continued)

Setting	Default Value
Minimum allowed RPO	
Settings changes	Activated, allowing modifying the settings of the replications.
Limit the number of configured replications	Deactivated (unlimited). To activate and configure the limit for the number of configured replications, activate the <b>Incoming migrations</b> , or <b>Incoming protections</b> toggles.
Bandwidth throttling	Deactivated (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 and whether the destination is on-premises or cloud site.
- 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 On-Premises to Cloud Director Replication 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 4.5 or later is deployed in the cloud site for finer control over the allowed destination of the migration, restraining tenants from migrating to on-premises or to other cloud sites.
- 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
<b>Policy name</b>	Enter a unique, case-sensitive name for the new policy.
<b>Incoming migrations</b>	To allow incoming migrations, activate the toggle.
<b>Outgoing migrations to cloud</b>	To allow outgoing migrations, where the destination is a cloud site, activate the toggle.
<b>Outgoing migrations to On-Premises</b>	To allow outgoing migrations, where the destination site is on-premises, activate the toggle.
<b>Incoming protections</b>	To allow incoming protections, activate the toggle.
<b>Outgoing protections</b>	To allow outgoing protections, activate the toggle.
<b>Custom SLA settings</b>	To allow custom SLA settings per replication, activate the toggle. Alternatively, to allow only the SLA profiles to set the SLA settings, deactivate the toggle.
<b>Allow advanced retention rules</b>	If incoming protections are activated, to allow advanced retention rules for protections for configuring the number of rotated instances and their time distance spread apart, activate the toggle.
<b>Max rotated instances per protection</b>	If incoming protections are activated, enter the maximum number of rotated instances per protection, up to 24.
<b>Max stored instances per protection</b>	If incoming protections are activated, enter the maximum number of stored instances per protection, up to 24.
<b>Minimum allowed RPO</b>	<p>If incoming protections are activated, set the minimum allowed RPO by using the <b>Recovery Point Objective (RPO)</b> slider or by clicking the time ranges.</p> <p><b>Note</b> For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see <a href="#">Chapter 4 Replicating Workloads</a>.</p> <p>With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.</p>

Option	Description
Events and Notifications	To allow tenants control of the event notification, activate the toggle.
Limit the number of configured replications	If incoming migrations or incoming protections or both are activated, enter the maximum number of replications.
Bandwidth throttling	To allow bandwidth throttling, activate the toggle then enter the maximum throughput per each On-Premises to Cloud Director Replication Appliance. After you modify the value, the new value takes effect after 30 minutes.

## 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](#).

## Clone a Replication Policy

To duplicate the replication settings of the replication policies and assign it to VMware Cloud Director organizations, as a **service provider** you can clone any existing replication policy.

## Prerequisites

- Verify that VMware Cloud Director Availability 4.5 or later is deployed.
- 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 for duplicating and click **Clone**.
- 3 In the **Clone Policy** window, enter the new replication policy name and click **Clone**.

## Results

You cloned the replication policy and its already assigned organizations remain in the original policy.

## What to do next

You can assign the cloned policy to VMware Cloud Director organizations. 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 4.5 or later is deployed in the cloud site for finer control over the allowed destination of the migration, restraining tenants from migrating to on-premises or to other cloud sites.
- 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
<b>Policy name</b>	Edit the policy name, entering a unique, case-sensitive name.
<b>Incoming migrations</b>	To allow incoming migrations, activate the toggle.
<b>Outgoing migrations to cloud</b>	To allow outgoing migrations, where the destination is a cloud site, activate the toggle.
<b>Outgoing migrations to On-Premises</b>	To allow outgoing migrations, where the destination site is on-premises, activate the toggle.
<b>Incoming protections</b>	To allow incoming protections, activate the toggle.
<b>Outgoing protections</b>	To allow outgoing protections, activate the toggle.
<b>Custom SLA settings</b>	To allow custom SLA settings per replication, activate the toggle. Alternatively, to allow only the SLA profiles to set the SLA settings, deactivate the toggle.
<b>Allow advanced retention rules</b>	If incoming protections are activated, to allow advanced retention rules for protections for configuring the number of rotated instances and their time distance spread apart, activate the toggle.
<b>Max rotated instances per protection</b>	If incoming protections are activated, enter the maximum number of rotated instances per protection, up to 24.
<b>Max stored instances per protection</b>	If incoming protections are activated, enter the maximum number of stored instances per protection, up to 24.
<b>Minimum allowed RPO</b>	If incoming protections are activated, set the minimum allowed RPO by using the <b>Recovery Point Objective (RPO)</b> slider or by clicking the time ranges.  <b>Note</b> For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see <a href="#">Chapter 4 Replicating Workloads</a> .  With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.
<b>Events and Notifications</b>	To allow tenants control of the event notification, activate the toggle.



Option	Description
<b>Limit the number of configured replications</b>	If incoming migrations or incoming protections or both are activated, enter the maximum number of replications.
<b>Bandwidth throttling</b>	To allow bandwidth throttling, activate the toggle then enter the maximum throughput per each On-Premises to Cloud Director Replication 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 **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

### Procedure

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

### Results

You assigned the selected SLA profile to the selected organizations.

### What to do next

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



## 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@VCLLOUD_DIRECTOR_IP:443?
org=ORG_NAME&vdc=VDC_NAME&vapp=VAPP_NAME' VAPP_NAME.ova
```

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

## Importing a Virtual Machine from a Removable Media

You can import a virtual machine from a removable media directly in VMware Cloud Director™. Alternatively, you can import a virtual machine in vCenter Server and then import the virtual machine in VMware Cloud Director™ by using the vSphere Client.

### Import a Virtual Machine Directly in VMware Cloud Director™

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

### Prerequisites

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

### Procedure

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

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

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

---

**Note** Do not power on the imported virtual machine.

---

#### What to do next

You can now configure a replication by using the created seed vApp in VMware Cloud Director Availability.

#### Import a Virtual Machine in VMware Cloud Director Through vCenter Server

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

#### Prerequisites

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

#### Procedure

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

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

---

**Note** Do not power on the imported VM.

---

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

#### What to do next

You can now configure a replication by using the created seed vApp in VMware Cloud Director Availability.

### Configure a Replication by Using a Replication Seed

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

#### Prerequisites

- Verify that the free space in the destination datastore is at least double that of the source vApp or virtual machine. For information about the double space requirement, see [Destination datastore space consumption](#).
- Verify that the seed vApps or virtual machines exist in the target site.
- Before starting a replication using a seed, in the target site you must power off the seed virtual machines, because they are unregistered from the target VMware Cloud Director

and vCenter Server inventories. If the new replication fails, the virtual machine files and disks remain on the datastore. For the virtual machine to appear in the inventories, locate the `.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 <b>Storage policy</b> 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	<p>Select to preserve multiple distinct replication instances (snapshots) to which virtual machines can be recovered. Also select the number of replication instances to keep, and select the preservation period.</p> <p>The number of preserved replication instances depends on the configured retention policy and requires that the RPO period is short enough for the replication instances to be created. For example, if you select to preserve four replication instances per day, the RPO period must not exceed six hours, to allow for the retention of four replication instances in 24 hours.</p>

---



Option	Description
Enable quiesce	Select the quiescing method for the guest OS of the source virtual machine.  <b>Note</b> Quiescing is available only for virtual machines that support quiescing. For more information, see <a href="#">Guest OS Quiescing Support</a> .
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.

## 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.

## Configure Recovery Settings and Guest Customization

For replications to cloud sites backed by VMware Cloud Director, specify the destination network settings, the guest customization, and the script that apply when recovering the workload in the destination site.

When replicating to a cloud site backed by VMware Cloud Director, before recovering the workload in the destination site, you can configure the destination network, the operating system guest customizations, and a shell script that executes after recovery.

---

**Note** This procedure applies only for replications to cloud sites backed by VMware Cloud Director.

For vSphere DR and migration between vCenter Server sites, see [Configure Recovery Settings for vSphere DR and Migration](#).

---

### Prerequisites

- Prerequisites for guest customization:
  - Guest customization requires the virtual machine to be running VMware Tools.
  - To customize a Windows guest operating system, the **system administrator** must install the appropriate Microsoft Sysprep files on the VMware Cloud Director server group. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.
  - To customize a Linux guest operating system, Perl must be installed in the guest.
- Verify that VMware Cloud Director Availability 4.5 or later 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 To modify virtual machine replications, in the top right of the page click the **VM** button, or to modify vApp replications, click the **vApp** button.
- 3 Select one or more replications.
- 4 Click **All Actions > Recovery Settings**.
- 5 In the **Recovery settings** window, to modify the settings for the guest OS in the destination site, click **Guest customization**.
  - For migration and failover settings, click the **Migrate/failover** tab.
  - Alternatively, for test failover settings, click the **Test** tab.

For information about configuring the networks, see [Configuring Network Settings of Replications to the Cloud](#).

- a Expand the virtual machine name and to allow guest customization, keep the **Use source settings** toggle deactivated.

By default, the **Use source settings** toggle is activated and the source virtual machine settings apply when the source is a cloud site and after the settings from the source replicate. The **Use source settings** toggle is deactivated when no settings come from the source.

- b Configure the **General** section.

The default settings in the following three tables apply for source workloads that do not already use guest customization. If the source workload already uses guest customization, by enabling the **Use source settings** toggle, the settings reflect the already customized source workload.

Option	Description
<b>Guest customization</b>	Deactivated by default. To apply any customizations, activate this toggle. When the virtual machine uses Guest Properties for customization do not activate the <b>Guest customization</b> toggle.
<b>Computer name</b>	<p>Change the computer name of the destination virtual machine.</p> <p><b>Note</b> With active <b>Guest customization</b> toggle, if you skip entering the computer name, VMware Cloud Director automatically generates one, for example <i>vmname-001</i> then virtual machines running a Windows guest operating system may disjoin from the domain.</p> <p>The computer name and network settings apply to the guest operating system when the virtual machine is powered on.</p>
<b>Change SID</b>	<p>To change the Security ID (SID) for uniquely identifying systems and users, activate this toggle.</p> <p>The SID applies only for virtual machines running a Windows guest operating system. VMware Cloud Director runs <code>sysprep</code> to change the Windows SID. On Windows NT, VMware Cloud Director uses <code>sidgen</code>. Running <code>sysprep</code> is a prerequisite for completing domain join.</p> <p>By not activating this toggle, the destination virtual machine has the same SID as the source virtual machine.</p> <p>Change SID only applies the first time the virtual machine powers on, or if in VMware Cloud Director you perform <b>Power on and Force Recustomization</b>.</p>

- c Expand the **Password Reset** section.

Password reset only applies the first time the virtual machine powers on, or if in VMware Cloud Director you perform **Power on and Force Recustomization**.

Option	Description
<b>Allow local administrator password</b>	Activate this toggle to allow setting an administrator password on the guest operating system.
<b>Require Administrators to change password on first login</b>	Activate this toggle to require administrators to change the password of the guest operating system on the first login.
<b>Auto generate password</b>	Activate this toggle to allow password auto generation.
<b>Specify password</b>	To enter a password, activate the <b>Allow local administrator password</b> toggle and deactivate the <b>Auto generate password</b> toggle.
<b>Number of times to log on automatically</b>	Required for automatically generated passwords, or else the user is not able to log in. Enter 0 to disable the automatic log on as an <b>Administrator</b> user.

- d Expand the **Join Domain** section.

This section only applies for virtual machines running a Windows guest operating system. Join domain only applies the first time the virtual machine powers on, or if in VMware Cloud Director you perform **Power on and Force Recustomization**.

Option	Description
Join domain	Activate this toggle to join the virtual machine to a Windows domain, then enter the following domain properties.
Use organization's domain	Activate this toggle to use the domain of the organization. Alternatively, override the organization's domain by entering the domain properties.
Domain name	Enter the Windows domain name.
Domain username	Enter the name of the domain user account.
Domain password	Enter the password of the domain user account.
Account organizational unit	Enter the account organizational unit.

- e Expand the **Script** section then in the **Script content** text box, enter the contents of the script that executes in the recovered virtual machine.

The script only applies the first time the virtual machine powers on, or if in VMware Cloud Director you perform **Power on and Force Recustomization**.

When entering a customization script in a virtual machine, the script:

- Cannot contain more than 1500 characters.
- Needs to be a batch file for Windows virtual machines and a shell script for Unix virtual machines.
- The `precustomization` command line parameter calls the script before guest customization begins.
- The `postcustomization` command line parameter calls the script after guest customization finishes.

Example scripts:

Virtual Machine Guest Operating System	Example script
Windows sample batch file	<pre>@echo off if "%1" == "precustomization" ( echo Do precustomization tasks ) else if "%1" == "postcustomization" ( echo Do postcustomization tasks )</pre>
A Linux sample shell script	<pre>#!/bin/sh if [ \$1 == "precustomization" ]; then echo Do Precustomization tasks elif [ \$1 == "postcustomization" ]; then echo Do Postcustomization tasks fi</pre>

- The following script contents output a text string, followed by the date in a text file placed in the root of the filesystem of the virtual machine in the destination site:

```
echo 'Test string' "$(date)" > /file.txt
```

- The following example deliberately fails the script execution. The replication task succeeds with a green check, but shows a warning: Unable to apply Guest Customization for recovery virtual machine '*vm-name*'.

```
exit 1
```

## 6 Click **Apply**.

### Results

In the **Tasks** pane, a replication task runs. In case the prerequisites for guest customization are not met, the workload is recovered without customizations and the replication task succeeds with a green check but shows a warning: Unable to apply Guest Customization for recovery virtual machine '*vm-name*'. Guest Customization couldn't complete in 300000 ms for recovery virtual machine '*vm-name*'.

## 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 for On-Premises to Cloud Replications

For the on-premises to cloud replications, you can specify the destination network settings of the vApp or virtual machine. After performing a migration, failover, or a test failover, VMware Cloud Director Availability attaches the selected network settings in the destination 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 4.5 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 To configure their destination network settings, select one or more on-premises to cloud replications and click **All actions > Recovery settings**.
- 2 In the **Recovery settings** window, to configure the destination network settings of the selected replications click the **Nics** tab.

---

**Note** **Networks** is inactive for on-premises to cloud replications and is active only for cloud to cloud replications. For more information, see [Configure the Network Settings for Cloud to Cloud Replications](#).

---

Option	Description
<ul style="list-style-type: none"> <li>■ <b>vApp</b></li> <li>■ <b>#VMs</b></li> </ul>	To see the number of the virtual machines and their network interface cards (NIC), expand the name of the parent vApp then expand each NIC. For each NIC, the network resolution, by default selected as <b>Automatic</b> means the source network gateway matches the destination gateway. Alternatively, select an organization VDC network to connect to.
<b>Status</b>	To activate the connection for that NIC to the destination organization VDC network, select the <b>Connect at Power On</b> check box.
<b>State</b>	Select the <b>Primary NIC</b> for each virtual machine.



Option	Description
MAC Address	To reset the MAC address of the expanded NIC in the destination site, from the drop-down menu select <b>Reset</b> .
IP Address	<ul style="list-style-type: none"> <li>■ <b>None</b> selected by default, no IP addressing mode is specified.</li> <li>■ <b>Static - IP POOL</b> select to obtain an IP address for the expanded NIC from an IP pool in the destination network. To commit the IP address changes to the virtual machine guest OS, click <b>Guest customization</b>.</li> <li>■ <b>DHCP</b> select to obtain an IP address for the expanded NIC when the connected destination network is configured with a DHCP server.</li> <li>■ <b>Static - Manual</b> select to enter a static IP address to the expanded NIC. To commit the IP address changes to the virtual machine guest OS, click <b>Guest customization</b>.</li> </ul> <p>For more information about <b>Guest customization</b>, see <a href="#">Edit Replication Settings</a>.</p>

### 3 Click **Apply**.

#### Results

For the selected replications, after a successful on-premises to cloud migration, failover, or a test failover, VMware Cloud Director Availability replicates the workload to the destination cloud site. Then VMware Cloud Director Availability attaches the selected network settings to the destination vApp or virtual machine.

#### Configure the Network Settings for Cloud to Cloud Replications

For the cloud to cloud replications, you can specify the automatically discovered network settings of the vApp or virtual machine. After performing a migration, failover, or a test failover, VMware Cloud Director Availability attaches the selected network settings in the destination 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.

Since VMware Cloud Director Availability 4.4, a reversed replication now creates the following auto-resolved and original mappings for the vApp networks:

**Table 4-5. Reversed Replication vApp Network Mappings**

Original Network Mapping	Reverse Replication Network Mapping
If no destination network match for the reversed replication network is found.	No change. Keep the auto-resolved mapping of the source networks.
Alternatively, if multiple source networks connect to one destination network.	
If a matching destination network for the reversed replication network is found.	Reverse the original network mapping, preserving the protected vApp configuration for connection to destination networks.

## Prerequisites

- Verify that VMware Cloud Director Availability 4.4 or later is deployed in both cloud sites for preserving the original network settings of the protected vApps after reversing the replication.
- 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 To configure their destination network settings, select one or more cloud to cloud replications and click **All Actions > Recovery Settings**.
- 2 In the **Recovery settings** window, configure the destination network settings of the selected replications.
  - For migration and failover network settings, click the **Migrate/failover** tab.

- Alternatively, for test failover network settings, click the **Test** tab.
- a In the left pane, click **Networks**.

Option	Description
Source networks	See the name of the networks, and the virtual machine network interface cards (NIC).
Type	Shows the type of the network in the source site: <ul style="list-style-type: none"> <li>■ Direct: network that directly connects to the organization VDC network.</li> <li>■ Isolated: network only within the vApp, not connected externally.</li> <li>■ Routed: you can specify a CIDR and connect to an external network.</li> </ul>
Target networks	Select the destination network to connect to in the destination site after a migration, failover, or test failover: <ul style="list-style-type: none"> <li>■ <b>Network name</b> select to replicate the source vApp network in the destination site and connect the destination vApp to the selected orgVDC <i>Network name</i> in the destination site.</li> <li>■ <b>Isolated</b> replicates the source networks without connecting them to any network in the destination site.</li> <li>■ <b>Network name (Not Available)</b> when the destination network is no longer available it is listed as grayed-out.</li> </ul>

- b In the left pane, click **Nics**.

Option	Description
<ul style="list-style-type: none"> <li>■ vApp</li> <li>■ #VMs</li> </ul>	To see the number of the virtual machines and their NICs, expand the name of the parent vApp then expand each NIC. For each NIC, the network resolution, by default selected as <b>Automatic</b> means the source network gateway matches the destination gateway. Alternatively, select an organization VDC network to connect to.
Status	To activate the connection for that NIC to the destination organization VDC network, select the <b>Connect at Power On</b> check box.
State	Select the primary NIC for each virtual machine.
MAC Address	To reset the MAC address of the expanded NIC in the destination site, from the drop-down menu select <b>Reset</b> .
IP Address	<ul style="list-style-type: none"> <li>■ <b>None</b> selected by default, no IP addressing mode is specified.</li> <li>■ <b>Static - IP POOL</b> select to obtain an IP address for the expanded NIC from an IP pool in the destination network. To commit the IP address changes to the virtual machine guest OS, click <b>Guest customization</b>.</li> <li>■ <b>DHCP</b> select to obtain an IP address for the expanded NIC when the connected destination network is configured with a DHCP server.</li> <li>■ <b>Static - Manual</b> select to enter a static IP address to the expanded NIC. To commit the IP address changes to the virtual machine guest OS, click <b>Guest customization</b>.</li> </ul> <p>For more information about <b>Guest customization</b>, see <a href="#">Configure Recovery Settings and Guest Customization</a>.</p>

- 3 Click **Apply**.

## Results

For the selected replications, after performing a migration, failover, or a test failover, VMware Cloud Director Availability replicates the workload to the destination cloud site. Then VMware Cloud Director Availability attaches the selected network settings to the destination vApp or virtual machine.

## Recovery Plans

From cloud sites backed by VMware Cloud Director, orchestrate complex failover or migration to and from paired cloud and on-premises sites by using recovery plans. These 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 recovery plans. These plans orchestrate step-by-step the failover or migrations of already created vApp and virtual machine incoming replications to the disaster recovery site. Sequence and organize disaster recovery or migration of each workload by priority, with available delays and prompts.

### Recovery Plans

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

- Recovery plans contain steps that perform only test failover or failover of the protected workloads.
- Migration plans allow scheduling of the synchronization and contain steps that perform only migrations.

### Steps

Each step in the recovery 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 the initial synchronization of a migration

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

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

### Scheduling the migrations auto synchronization of a plan

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

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

### Delayed synchronization

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

### Synchronize before migrate

At the migration plan scheduled time, if a migration is already synchronized, meaning the virtual machine is running and no initial synchronization time of the migration 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** Scheduling the auto synchronization in a migration plan overwrites the initial synchronization schedule of all its migrations.

---

## Step and Recovery Plan Execution

In VMware Cloud Director Availability 4.4 and later, selecting a step shows its detailed execution sequence, highlighting the currently performed activity when the step executes. Also, while executing a recovery plan, the active **Follow plan** toggle selects the currently executed step showing its detailed execution sequence with the currently performed activity. Then, after the currently executed step completes automatically follows the next executed step and keeps showing the currently active step details as the plan proceeds. Selecting another step deactivates the **Follow plan** toggle and keeps showing the selected step details without advancing while the recovery plan completes its steps. For example, a recovery plan that consists of the following steps, with their detailed execution sequence:

- **Not Started > Delay (wait *X* seconds) > Completed**
- **Not Started > Failover & Delay (Failover *X* vApps and *Y* VMs, then wait *Z* seconds) > Completed**
- **Not Started > Delay (Wait *X* seconds) > Prompt (*Message*) > Completed**
- **Not Started > Failover (Failover *X* vApps and *Y* VMs) > Completed**

The execution of a recovery 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 recovery plan completes with a `Completed Failover` or a `Completed Migrate` state, regardless of whether certain replication operations completed with a warning.
  - Alternatively, the recovery 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, any recovery plan suspends at a migration step that requires authentication with the remote site.

## Recovery Plan States

The allowed operations on a recovery plan depend on its current state and on the last operation in the plan.

### Not started recovery plans

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

### Running recovery plans

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

### Suspended recovery plans

- Suspended on prompt recovery plans resume after clicking **Approve Prompt**. Alternatively, they resume by using failover or migrate.
- Suspended recovery plans after test or cleanup step allow resuming by using test failover or test cleanup, failover or migrate.
- Suspended recovery plans after a failover or a migrate step, allow resuming by using failover or migrate.
- All suspended recovery plans allow editing and modifying the steps and attaching and detaching replications. For example, detaching replications that suspend the recovery 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 recovery 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 recovery 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 recovery 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 recovery plans but not in multiple steps in the same plan.

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

For example, running two recovery 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 recovery plan executing the test failover task fails, at the step containing the already failed over replication.

- Deleting a replication while used in a recovery plan, detaches the replication from the step where attached, without causing 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.

## Recovery Plans Operations

After logging in the cloud site, in the left pane, under the **Replications** section click **Recovery Plans**.

---

**Note** The recovery plans are only available only from the cloud site and 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 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`, `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.

Deleting a recovery plan also removes all of its reports.

## 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 in a `Completed`, `Test`, or in a `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 recovery plan creates a 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.
- **Reports** - new for VMware Cloud Director Availability 4.4, shows the **Recovery Plan Reports** window for the selected recovery plan. This page contains entries for the performed operation of each completed plan execution, the start and end timestamps and the result of each execution. For example, the following recovery plan executed four times, with the latest performed operation on top:

**Table 4-6. Recovery Plan Reports**

Operation	Start Date	End Date	Result
Failover	<i>d/m/yyyy, h:mm:ss</i>	<i>d/m/yyyy, h:mm:ss</i>	Success
Test	<i>d/m/yyyy, h:mm:ss</i>	<i>d/m/yyyy, h:mm:ss</i>	Error
Cleanup	<i>d/m/yyyy, h:mm:ss</i>	<i>d/m/yyyy, h:mm:ss</i>	Success
Test	<i>d/m/yyyy, h:mm:ss</i>	<i>d/m/yyyy, h:mm:ss</i>	Error

Selecting any of these performed and completed operations activates **View Report File** for the selected operation. Clicking **View Report File** opens its **Recovery Plan Execution Report**.

### Recovery Plan Execution Report

VMware Cloud Director Availability 4.4 and later show reports for each execution of a recovery plan by selecting the plan and clicking **Other Actions > Reports**.

In the **Recovery Plan Reports** window, selecting an operation and clicking **View Report File** opens a new **Recovery Plan Execution Report** page that contains the following information:

- Plan: *name*.
- Type: RECOVERY or MIGRATION.
- Site: *name*.

- Owner: *org@site*.
- Steps: *X* executed of *Y* total.
- Duration: *start date - end date*.
- Operation: Test, or Cleanup, or Failover, or Migrate, with operation state Completed or Failed.  
     Operation suspended by user. operations show as Failed.
- Step information: *Step name, Delay if exists, Duration, Outcome, Prompt if exists*.
  - Recovery information: *VM/vApp Name, Source site, State, Duration if executed, Outcome*.
 The *Outcome* can be Completed, Failed, or when the recovery plan failed or suspended before that step - Not Started.

Recovery executions are nested into steps, similar to how replications associate to the steps in the plan. The report can contain multiple steps and multiple recovery executions within each of those steps.

## Steps Operations

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

### New step

- For 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 recovery 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 recovery 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 recovery 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.

Dragging and dropping each step in a recovery plan re-arranges the plan steps order.

## Migrating vApp Templates between Cloud Sites

Templates are primary copies of virtual machines, ready for instantiating. Migrating vApp templates to a site allows the tenants to deploy consistently configured virtual machines across multiple VMware Cloud Director instances.

A vApp template represents a collection of always powered off or suspended virtual machine images loaded with an operating system, configured applications, networks, and data.

VMware Cloud Director Availability 4.3.1 introduced vApp templates migration across VMware Cloud Director instances. Version 4.4 replicates the following additional settings:

- vApp networks with their connectivity.
- Activated **General > "Gold\_Master."**
- Activated **Customize VM settings.**

### View vApp Templates Migrations

First, choose a direction for the migration:

- Click **Incoming Replications.**
- Alternatively, click **Outgoing Replications.**

Then, on the right side, under **Grouping** to see the templates migrations, click **Templates.**

## Create a New vApp Templates Migration

After under **Grouping** you click **Templates**,

- Click the **New Migration** button.
- Alternatively, click **All Actions > New Migration**.

The **New *Direction* Migration** wizard opens.

- 1 On the **Catalogs** page, configure the source migration settings.

- a Select a source catalog.

The table shows only catalogs owned by the selected **Source organization** from the drop-down menu.

The tenants also see shared catalogs between organizations. To show a shared catalog, the providers must select the source organization sharing it.

Catalogs that are subscribed to other catalogs are excluded from the available destination catalogs only for tenants. For providers, they still appear, but attempting a migrate throws an error.

- b Select one or more source vApp templates for migrating.
  - c Click **Next**.

- 2 On the **Destination VDC and Storage policy** page, configure the destination settings.

- a Select a virtual data center from the destination site as a replication target.
  - b Select the new destination storage policy for placing the recovered virtual machines.

If the destination catalog has differing storage policies assigned, the selected storage policy only applies to the replica files and might differ from the storage policy of the migration catalog. Similar to vApp or virtual machine migrations, template migrations allow changing the storage policy before the recovery.

The resulting vApp template matches the datastore catalog.

- c Click **Next**.

- 3 On the "**Settings**" page, configure the migration settings.

- a Optionally, to compress the replication traffic, leave the toggle active. The traffic compression lowers the network requirements at the expense of higher CPU consumption for the Replicator Appliance instances.
  - b Optionally, delay the synchronization start and set a convenient time for the first synchronization of the templates migration.

---

**Note** By not scheduling a time for the initial synchronization, it must be performed later either manually or during **Migrate**.

---

- c Click **Next**.

- 4 On the **Ready to complete** page, verify the selected migration settings and click **Finish**.

## Templates Migrations Settings

After under **Grouping** you click **Templates**, select one or more existing templates migrations, then click:

- **All Actions > Replication Settings** and in the **Edit Replication Settings** window, configure the **Compress replication traffic** toggle, then click **Apply**.
- **All Actions > Network settings** and in the **Network Settings** window, expand the vApps and virtual machines and configure the source vApp template networks connectivity with the destination networks after migrate, then click **Apply**.
- **All Actions > Change owner** and in the **Change Replication Owner** window, choose a new owner organization, then click **Apply**:
  - **System organization**
  - **Tenant organization**
- **All Actions > Change storage policy** in the **Edit storage policy** window, select the new storage policy placement, then click **Apply**.

## Migrate vApp Templates

After under **Grouping** you click **Templates**, select one or more existing templates migrations, then:

- Click **Migrate**.
- Alternatively, click **All Actions > Migrate**.

The **Migrate vApp Templates** wizard opens.

- 1 On the **Destination Catalog** page, select a destination catalog owned by the destination organization.
- 2 On the **Network Settings** page, choose the destination network settings.
  - **Apply preconfigured network settings on migrate** keeps the source vApp networks with their connectivity.
  - **Connect all VMs to network**, then select the *destination-network*.
- 3 On the **Ready to Complete** page, verify the selected migration settings and click **Finish**.

In the destination site, during the migration process, VMware Cloud Director Availability creates a temporary vApp that is an instantiated source template. After completing the migration, VMware Cloud Director Availability captures this temporary vApp in a template in the destination catalog. After a successful capture, it deletes the temporary vApp, leaving only the template.

There is a point in time during the template migration when VMware Cloud Director contains both the temporary vApp and the vApp template and vSphere shows both the virtual machines and their temp copies.

## Synchronize the vApp Templates Migrations

After under **Grouping** you click **Templates**, select one or more existing templates migrations, then click:

- **All Actions > Sync** performs an offline synchronization after clicking **Sync**. The disks of the virtual machines are locked and the source template is not unusable until the synchronization operation completes.
- **All Actions > Pause** pauses the selected migrations and does not send data to the destination site after clicking **Pause**.
- **All Actions > Resume** resumes the selected paused migrations and starts sending data again at the configured time after clicking **Resume**.

Migrating the templates, performing synchronization, or scheduling a delayed initial synchronization, each performs an offline synchronization that cannot be interrupted. This synchronization locks the source virtual machines disks. As a result, until this synchronization completes:

- Cannot use the source virtual machines included in the template.
- Cannot instantiate the source template.

---

**Note** VMware Cloud Director Availability does not support replications for templates with one or more encrypted virtual machines. Tenants without the **vApp: View VM and VM's Disks Encryption Status** right see the template tagged with encryption set to N/A as all the virtual machines in the template have an encrypted value 'null'. For more information, see [Create a Replication for Encrypted Virtual Machines](#).

---

## VDC Compute Policies

For the recovered virtual machine (VM), to configure VM-host affinity rules that control the placement of the workload, when creating or modifying a replication, select a VM placement policy for a specific cluster or host. By using a VM sizing policy, the provider sets the compute resources consumption for the recovered workload within an organization VDC to several predefined sizes.

VMware Cloud Director Availability allows the providers and their tenants to select two types of VDC compute policies for the recovered virtual machine:

- **VDC VM placement policy**
- **VDC VM sizing policy**

Select the VDC VM compute policy when configuring a new replication or in the replication settings of an existing replication. For more information:

- See [Create a Protection](#).
- See [Create a Migration](#).

For information about the compute policies in VMware Cloud Director, see [Understanding VM Sizing and VM Placement Policies](#) in the *VMware Cloud Director Service Provider Admin Portal Guide*.

## Placement Policy

VMware Cloud Director Availability 4.3 and later allow selecting a placement compute policy for a specific cluster or host for the recovered virtual machine.

### VDC VM placement policy

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 a 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](#).

## Sizing Policy

VMware Cloud Director Availability 4.5 and later allow selecting a sizing compute policy for a specific set of predefined compute resource allocation for the recovered virtual machine.

### VDC VM sizing policy

Sizing policies define the compute resource allocation for virtual machines within the organization VDC. With these policies, VMware Cloud Director **system administrators** control the following compute resources consumption at the virtual machine level:

- vCPUs number and clock speed.
- Memory amount.
- CPU and memory reservation, limit, and shares.
- Extra configurations.

For information about these attributes, see [Attributes of VM Sizing Policies](#) in the *VMware Cloud Director Service Provider Admin Portal Guide*.

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

- See [Create a VM Sizing Policy](#).
- See [Add a VM Sizing Policy to an Organization VDC](#).



## 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.

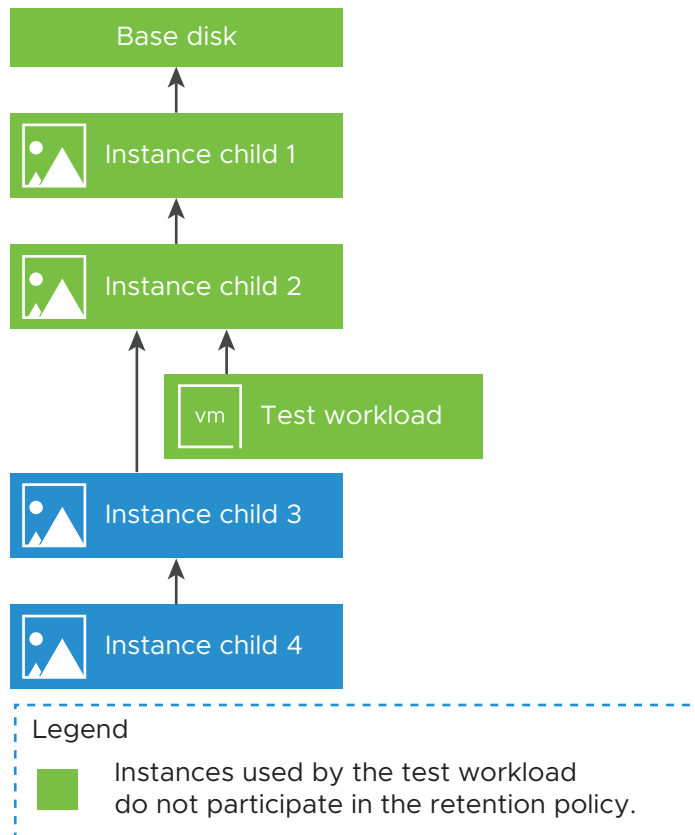
---

**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](#).

## 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.

## 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

As a **provider**, generate RPO compliance reports with the RPO violations of the existing replications for a specific period. As a **tenant** or as a **provider**, see notification advisories, monitor the traffic data usage and the disk usage of each organization or each replication, and the required compute resources like CPU, memory, and storage. Also, as a **tenant**, forward event notifications.

This chapter includes the following topics:

- [Advisories Notifications](#)
- [RPO Compliance Reports](#)
- [Monitoring the Traffic Usage](#)
- [Monitoring the Disk Usage](#)
- [Monitoring the Required Resources](#)
- [Forward Tenant Event Notifications](#)

## Advisories Notifications

In cloud sites backed by VMware Cloud Director, create simple notifications that show on top of all pages. Select a priority and duration for displaying the messages and their audience: the administrator users, users within a specific organization, or users in all organizations.

### Note:

- Advisories do not support editing, once created.
- Snoozing displays the notification message later.
- **Dismissing advisories:**
  - When the **root** user dismisses an advisory message, all system administrators get it dismissed.
  - Dismissing an advisory message permanently dismisses the notification without logging the dismissal action.
  - All tenant advisories are per user. For example, when **admin1@org** dismisses an advisory, it does not dismiss it for **admin2@org**.

- When dismissing the advisory message from VMware Cloud Director, the advisory message also dismisses from VMware Cloud Director Availability and conversely.

## VMware Cloud Director advisories

For more information, see [Create an Advisories Dashboard](#) in the *VMware Cloud Director documentation*.

### Create an advisory in VMware Cloud Director:

- 1 As a **system administrator**, create the advisories from the context of VMware Cloud Director.
- 2 In VMware Cloud Director, in the top navigation bar, click the **Administration** tab.
- 3 In the left pane, under the **Settings** section, click **Advisories**.
- 4 On the **Advisories** page, click **New**.
- 5 In the **Create New Advisory** window, configure the notification settings and click **OK**.
  - a In the **Description** text-box, enter the notification message.
  - b From the **Priority** drop-down menu, select the notification importance.
  - c From both **Active From** and **Active Until**, select the visibility duration.
  - d Select users or organization for the notification visibility:
    - **Publish to all users in all organizations.**
    - **Publish to all system administrators** in the system organization.
    - **Publish to specific tenant** organization.

### Delete an advisory in VMware Cloud Director:

In VMware Cloud Director, on the **Advisories** page, the advisories appear even after they expire.

To remove an advisory from the list, select the radio button next to it then click **Delete**.

## Visibility of the advisories

- The notification messages are visible from the context of:
  - VMware Cloud Director Availability standalone portal both in cloud and in on-premises sites.
  - VMware Cloud Director Availability vSphere Client Plug-In both in cloud and in on-premises sites.
  - VMware Cloud Director plug-in and in standalone portal.

- Once created, only the specific user group (all users in all organizations / all system administrators / specific tenant organization) selected during the creation of the advisory sees the notification message. Upon a tenant user first log in, only mandatory notifications display.

Only after the session is extended from the on-premises appliance or from the vSphere plug-in to the cloud by providing the cloud credentials the tenant sees all applicable notifications with options to **Snooze** or **Dismiss** them.

- Only the local cloud site advisories display. No cross-site advisories are visible, for example, when org1@siteA replicates to org2@siteB, only advisories targeted at org1@siteA are visible from the context of site A.
- On-premises users receive and see only notifications targeted to their organization.
  - Only mandatory notifications display until the on-premises user provides their organization credentials. For example, when prompted when creating a new replication.
  - After the user authenticates with their organization credentials, they see all their advisory messages, including critical, important, and notice.
- System notifications sent to all system administrators or to an organization that is different than the organization that the user belongs to do not appear for the on-premises users.
- The duration of the visibility is for a specific interval, active from a set time and active until a set time, as configured during the notification creation.

### Advisory priorities

The notifications have priorities and when multiple advisories with different priority display, they show in the following order:

- 1 **Mandatory:** Red, mandatory messages that always display these advisories do not allow snoozing nor dismissing.
- 2 **Critical:** Red, high priority, potentially actionable messages that can be either snoozed or dismissed.
- 3 **Important:** Orange, potentially actionable messages that can be either snoozed or dismissed.
- 4 **Notice:** Blue, informational messages that do not allow snoozing but allow dismissing.

## RPO Compliance Reports

As a **service provider**, you can generate and export Recovery Point Objective (RPO) compliance reports, grouped on an organization level, listing any RPO violations of the existing protections for a specified period. These reports show whether, in the given period, any protection to the site and from it to on-premises sites meets its RPO.

For all organizations or for a selected organization, the RPO compliance reports include all existing protections for a specified period. View the currently generated report and optionally, export it in a couple of file formats. Optionally, on the reports page select showing only protections with RPO violations and only non-deleted protections.

For more information about RPO, see [Recovery Point Objective - RPO](#).

## Generating and Exporting RPO Compliance Reports

### Generate an RPO Compliance Report

To generate an RPO compliance report, in the left pane click **Reports**.

The **RPO Compliance Reports** page generates the RPO compliance report data for all organizations. When generating a report, specify the following report options that affect both the generated and the exported reports.

- In the top, enter the beginning and the end of the reporting period.
- Optionally, filter the organizations in the generated report by selecting it from the **Organization** drop-down menu:
  - To include every organization in the report, select **All**.
  - Alternatively, to filter the report by an organization, select one.
- Optionally, to filter out the protections owned by the system and not visible for the tenants from the generated report, with any specific organizations selected from the **Organization** drop-down menu, deselect **Include system owned replications**.

### Export an RPO Compliance Report

After generating the report with all the specified options above, you can export the generated report to a file in your browser that you can save. The exported report contains the same information, filtered as selected above.

- To export the report in an HTML file, click **View HTML Report File**.
- To export the report in a tab-delimited file, click **View TSV Report File**.

## RPO Compliance Report Structure

- Paused protections report RPO violations and are present in the report.
- If no protections exist for the specified period, the report is empty.

For each organization, under its own section, the report orders the data in the following two sections:

### Cloud Destination Report

Ordered by: **source site > vApp name > vApp ID > VM name > VM ID > start time** in descending order, that is newest first.

This destination report section includes protections from both on-premises sites and from cloud sites to cloud sites.

### On-premises Destination Report

Ordered by: **destination site > vApp name > vApp ID > VM name > VM ID > start time** in descending order, that is newest first.

This destination report section includes protections from this cloud site to on-premises sites.

## Viewing a Generated RPO Compliance Report

After generating the report, you can further filter the displayed data on the **RPO Compliance Reports** page. The following options do not affect exported reports and only affect the page view.

- **Expand** and **Collapse** toggle expansion and contraction for all the sections.
- To hide any protections without existing RPO violations, select **Show violations only**. Each protection can show multiple violations.
- To hide any non-active protections, deleted by the time the report runs, select **Hide deleted replications**. The Is alive column shows **No** for protections that existed at the specified period and are no longer active at the runtime of the report.
- For any still existing protection, clicking the replication id link under the Replication id column navigates you to the replications page, filtered for displaying only the specified protection.

---

**Important** The RPO compliance reports include only data for replications configured as protections. Migrations are not part of these reports.

### Disclaimer:

The content of this article is provided "as-is" and to the maximum extent permitted by applicable law, VMware disclaims all other representation and warranties, expressed or implied, regarding this content, including their fitness for a particular purpose, their merchantability, or their noninfringement. VMware shall not be liable for any damages arising out of or in connection with the use of this content, including direct, indirect, consequential damages, loss of business profits or special damages, even if VMware has been advised of the possibility of such damages.

---

## 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 From the **Organization** drop-down menu select an organization for which you want to filter the displayed traffic information.
- 3 In the top, enter the beginning and the end of the traffic reporting period, then in the organization traffic chart 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.

In the bottom of the traffic 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 in your browser, enter the beginning and the end of the reporting period and click **Export daily usage** or **Export daily traffic**.

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

#### What to do next

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

## Monitor the Traffic Usage of a Virtual Machine Replication

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

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

#### Prerequisites

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

#### Procedure

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

In the bottom pane, the **Traffic** data chart shows the amount of traffic transferred by the selected replication in the past three minutes.

- 5 To switch the data chart from a live traffic view to historical data, click **Recorded**.
- 6 To change the data chart reporting interval, enter the beginning and the end of the traffic reporting period and select an interval of reporting.
  - To see the last five hours of traffic, select the **5 minutes** interval.
  - To see the last two weeks of traffic, select the **1 hour** interval.
  - To see the last two months of traffic, select the **1 day** interval.

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

## Results

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

## What to do next

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

# Monitoring the Disk Usage

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

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

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

## Disk Usage Monitoring Retention

- When querying the historical disk usage information, you can set the beginning and the end of the information period.
- VMware Cloud Director Availability stores the historical disk usage information for the following intervals:
  - 5 minutes intervals, available for the last 5 hours.
  - Hourly intervals, available for the last 14 days.
  - Daily intervals, available for the last 60 days.

## Monitor the Disk Usage as a Tenant

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

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

## Prerequisites

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

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

#### Procedure

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

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

#### Results

You see the disk usage information for your organization.

#### What to do next

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

## Monitor and Export Organization Disk Usage as a Service Provider

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

#### Prerequisites

- Verify that VMware Cloud Director Availability 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 From the **Organization** drop-down menu select an organization for which you want to filter the displayed disk usage information.
- 3 In the top, enter the beginning and the end of the disk usage period, then in the organization disk usage chart 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.

In the bottom of the disk usage 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 in your browser, enter the beginning and the end of the reporting period and click **Export daily disk usage**.

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 Required Resources

VMware Cloud Director Availability shows the destination required resources of the replications provisioned on a failover. Select a destination organization, or organization VDC, a replication, or one or more source replication sites for the required destination resources to calculate the required destination capacity and compute resources for successfully failing over the protected source workloads to the destination site.

**Required resources** aggregates the following information:

## CPU

The sum of the number of vCPUs of the source virtual machines.

## Memory

The sum of the source virtual machine memory sizes.

## Disk capacity

The sum of the capacity of the replicated disks.

---

**Note** In VMware Cloud Director Availability 4.3.1 and later, vApp template replications include only the storage calculation.

---

The required resources are available for each replication that does not have a test failover and is not failed over. Replicated templates are not part of the required resources calculation.

Aggregated information about the required resources is available on a vApp replication level as a sum of the required resources for each virtual machine replication in the vApp.

The required resources can help both the **tenants** and the **providers** with estimates about their organization VDCs:

- The **tenants** can see the required resources to fail over and power on the protected workloads from any or all source sites in the destination cloud site. Also, the required resources per VDC help the tenants estimate their organization VDCs capacity and help with provisioning planning.

- The **providers** can see the required resources to fail over and power on the protected virtual machines:
  - On a destination organization level as a sum of the required resources for each organization VDC in the organization.
  - On a destination organization VDC level as a sum of the required resources for each virtual machine replication to the organization VDC to provide extra capacity in the organizations VDCs.
  - Required resources per provider VDC and as a sum of the required resources for each organization VDC in the provider VDC to calculate the level of over-provisioning for the disaster recovery environment.

## Monitor the Required Resources as a Tenant

As a **tenant**, in VMware Cloud Director Availability, you can see the required compute resources per source site, per organization VDC, or per replication for failing over the protected workloads in the destination site. With this information, you can estimate your organization VDC capacity and it helps you with provisioning planning.

VMware Cloud Director Availability presents the destination site required resources as the sum of the CPU, memory, and disk capacity provisioned on a failover for all incoming replications.

### Prerequisites

- Verify that VMware Cloud Director Availability 4.4 or later is deployed in the cloud site for selecting the **Source sites** filter.
- 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

- ◆ To see the aggregated required resources for failing over to this destination site, at the bottom of the **Dashboard** page, under **Required resources** select one or more **Source sites** or select **All**.

### Required resources

For all incoming replications from the selected source sites, the **Required resources** aggregates the CPU, the Memory, and the Disk capacity required resources from all the organization VDCs in your organization for failing over all source workloads to this destination site.

---

**Note** For outgoing replications, to see their required resources, for example, outgoing from site *A* to site *B*, log in to site *B* and from the **Source sites** filter, select site *A*. This selection shows the required resources for failing over all the incoming replications to site *B* from site *A*.

---

- ◆ To see the resources required by an organization VDC, in the left pane, click **Required Resources**.

#### Organization VDC resources

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

- ◆ To see the resources required by a replicated workload, in the left pane, click **Incoming Replications** or **Outgoing Replications**. Then, to see the resources required by the replications, under `Show details` click **Resources**.

#### Replication resources

The replications view table shows columns for CPU, for Memory, and for Disk capacity resources required for failing over of each replication.

## Monitor the Required Resources as a Provider

As a **provider**, in VMware Cloud Director Availability, you can see the required destination site resources per source site, per organization or an organization VDC, per provider VDC, or per replication for failing over the protected workloads in the destination site. With this information, you can calculate the level of over-provisioning in the disaster recovery infrastructure and provide extra capacity for the tenants.

VMware Cloud Director Availability presents the destination site required resources as the sum of the CPU, memory, and disk capacity resources provisioned on failover for all incoming replications.

#### Prerequisites

- Verify that VMware Cloud Director Availability 4.4 or later is deployed in the cloud site for selecting the **Source sites** filter.
- Verify that you can access VMware Cloud Director Availability as a **provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

#### Procedure

- ◆ To see the aggregated required resources for failing over to this destination site, at the bottom of the **Dashboard** page, under **Required resources** select one or more **Source sites** or select **All**.

#### Required resources

For all incoming replications from the selected source sites, **Required resources** aggregates the following information:

- For the selected source sites, `Top 5 organizations` displays each of the organizations, up to five. With more than five organizations, displays the top five organizations and an `Other` category, that aggregates the remaining organizations.

- CPU, Memory, and Disk capacity required resources for each displayed organization.
- Three piecharts aggregating the proportional required resources for CPU, for memory, and for disk capacity among the displayed organizations.

---

**Note** For outgoing replications, to see their required resources, for example, outgoing from site *A* to site *B*, log in to site *B* and from the **Source sites** filter, select site *A*. This selection shows the required resources for failing over all the incoming replications to site *B* from site *A*.

---

- ◆ To see the resources required by an organization, in the left pane click **Reports** and in the top right corner click **Organization resources**.

### Organization resources

The table shows the resources required for failing over to this site for each organization. By expanding an organization, you can also see the required resources for each organization VDC in it.

- ◆ To see the resources required by a provider VDC, in the left pane click **Reports** and in the top right corner click **Provider VDC resources**.

### Provider VDC resources

The table shows the resources required for failing over to this site for each provider VDC. At the top of the page, you can see the sum of the combined required resources from all provider VDCs.

- ◆ To see the resources required by a replicated workload, in the left pane, click **Incoming Replications** or **Outgoing Replications**. Then, to see the resources required by the replications, under *Show details* click **Resources**.

### Replication resources

The replications view table shows columns for CPU, for Memory, and for Disk capacity resources required for failing over of each replication.

## 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 Director Replication Management Appliance.
  - a In a Web browser, go to **`https://Appliance-IP-Address`**.
  - b Enter **tenant** user credentials.
  - c Click **Login**.
- 2 In the left pane, click **Event and Notifications**.
- 3 To configure email notifications in the VMware Cloud Director Tenant Portal, next to **Cloud Director Email** click **Configure in VCD**.

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

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

- 5 To configure the notification delivery channels and settings for replication monitoring, next to **Replication Monitoring Events** click **Edit**.

Option	Description
Replication Monitoring Channels	<ul style="list-style-type: none"> <li>■ To receive the events in VMware Cloud Director, select <b>Cloud Director events</b> as the notifications delivery channel.</li> <li>■ If configured in VMware Cloud Director, to receive the events over email by using the VMware Cloud Director email configuration, select <b>Cloud Director email</b> as the notifications delivery channel.</li> </ul>
RPO violation threshold time	Only forward events for replications with RPO violation time above this threshold. Use <i>0</i> 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 <i>0</i> 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.