

## **VMware Cloud Director Availability 4.7**

---

---

---

# Table of Contents

<b>Release Notes</b> .....	<b>9</b>
VMware Cloud Director Availability 4.7.3.1 Release Notes.....	9
VMware Cloud Director Availability 4.7.3 Release Notes.....	10
VMware Cloud Director Availability 4.7.2 Release Notes.....	12
VMware Cloud Director Availability 4.7.1 Release Notes.....	13
VMware Cloud Director Availability 4.7 Release Notes.....	15
VMware Aria Operations Management Pack for Cloud Director Availability 1.4 Release Notes.....	20
<b>What is VMware Cloud Director Availability</b> .....	<b>22</b>
<b>Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site</b> .....	<b>25</b>
Interoperability and vSphere product edition.....	26
Installing and configuring both appliances for vSphere DR and migration.....	27
Deployment architecture and requirements for vSphere DR and migration.....	27
Deploy both appliances for vSphere DR and migration.....	32
Configure and pair both appliances for vSphere DR and migration.....	34
Add an additional Replicator Appliance instance for vSphere DR and migration.....	37
<b>Installing and configuring the On-Premises to Cloud Director Replication Appliance</b> .....	<b>38</b>
Deployment architecture for the On-Premises to Cloud Director Replication Appliance.....	38
Deployment requirements for the On-Premises to Cloud Director Replication Appliance.....	40
Deploying the On-Premises to Cloud Director Replication Appliance.....	43
Deploy the On-Premises to Cloud Director Replication Appliance by using the vSphere Client.....	44
Deploying by using the VMware OVF tool.....	45
Configuring the On-Premises to Cloud Director Replication Appliance.....	47
Configure the On-Premises to Cloud Director Replication Appliance.....	47
Configure local placement for the On-Premises to Cloud Director Replication Appliance.....	49
<b>Upgrading on-premises and provider site</b> .....	<b>50</b>
Management interface upgrading.....	52
Upgrade by using the default repository.....	52
Upgrade by using a specified repository.....	53
Upgrade by using an ISO image file.....	55
Command-line upgrading.....	56
Command-line upgrade by using an ISO image file.....	57
Post-upgrade configuration.....	58
<b>Installation, Configuration, and Upgrade Guide in the Cloud Director Site</b> .....	<b>59</b>
Deployment architecture in the Cloud Director site.....	59
Services.....	66
Installing and configuring the appliances in the Cloud Director site.....	67

Installation requirements and deployment prerequisites in the Cloud Director site.....	67
Interoperability and vSphere product edition.....	67
Deployment requirements in the Cloud Director site.....	68
Network requirements and prerequisites in the Cloud Director site.....	71
Deploying the appliances in the Cloud Director site.....	74
Deploy the appliances by using the vSphere Client.....	75
Deploying by using the VMware OVF tool.....	76
Configuring the appliances in the Cloud Director site.....	78
Configure the Cloud Service in the Cloud Director site.....	78
Add an additional Replicator Service instance in the Cloud Director site.....	82
Add a second Tunnel Appliance for HA in the Cloud Director site.....	84
Configuring Customer Experience Improvement Program.....	86
Categories of information that VMware receives.....	87
Join or leave the Customer Experience Improvement Program.....	87
<b>Upgrading in the Cloud Director site.....</b>	<b>87</b>
Appliances upgrade sequence and prerequisites.....	88
Management interface upgrading.....	90
Upgrade by using the default repository.....	90
Upgrade by using a specified repository.....	92
Upgrade by using an ISO image file.....	94
Command-line upgrading.....	96
Command-line upgrade by using an ISO image file.....	96
Post-upgrade configuration in the Cloud Director site.....	97
<b>Administration Guide.....</b>	<b>98</b>
<b>Administration in the Cloud Director site.....</b>	<b>99</b>
Activate the data engines for replicating workloads.....	100
Managing pairing with Cloud Director sites.....	101
Pair two Cloud Director sites.....	105
Re-pair Cloud Director sites.....	106
Unpair paired sites from the Cloud Director site.....	106
Control the paired sites organization access.....	107
Restricting the administrative sessions access by source IP.....	108
Allow admin access from anywhere.....	108
Do not allow admin sessions from the Internet.....	109
Control the accessible provider virtual data centers.....	109
Certificates management in the Cloud Director site.....	110
Replacing the services certificates in the Cloud Director site.....	110
Replacing external infrastructure certificates in the Cloud Director site.....	116
Network settings configuration.....	119
Configure the network settings of the appliance.....	121

Configure a network adapter.....	122
Configure static routes.....	123
Add an additional network adapter.....	124
Select the endpoint address for each network adapter.....	125
Command-line network configuration.....	127
Stretching layer 2 networks in the Cloud Director site.....	130
Create a server L2 VPN session with NSX in the Cloud Director site.....	132
Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site.....	133
Bandwidth throttling.....	135
Configure bandwidth throttling to the cloud site.....	136
Configure on-premises bandwidth throttling to the Cloud Director site.....	137
Backing up and restoring in the Cloud Director site.....	137
Back up all the appliances in the cloud.....	139
Restore the appliances in the cloud.....	141
Maintenance in the Cloud Director site.....	144
Evacuate the replications data from a datastore.....	144
Replicator Service maintenance mode.....	145
Rebalance the replications across the Replicator Service instances.....	146
Replace a Tunnel Appliance instance.....	147
Uninstall VMware Cloud Director Availability from the Cloud Director site.....	148
<b>Administration in the on-premises and in the provider sites.....</b>	<b>150</b>
On-premises stretching layer 2 networks to the Cloud Director site.....	150
Deploy an NSX Autonomous Edge appliance on-premises.....	152
Register the NSX Autonomous Edge on-premises.....	154
Configure the networks of the NSX Autonomous Edge on-premises.....	155
Create a client L2 VPN session on-premises.....	156
Back up the appliance.....	157
Restore the appliance.....	159
Managing pairing with on-premises sites and between provider sites.....	160
Generate an API access token for pairing from VMware Cloud Director.....	161
Repair with a remote site.....	162
Unpair a remote site.....	166
Replace the SSL certificate of the appliance.....	167
Change the IP address of the appliance.....	168
Unregister the VMware Cloud Director Availability vSphere Client Plug-In from vCenter Server.....	172
<b>Monitoring and troubleshooting.....</b>	<b>173</b>
Events and notifications.....	173
Configure provider event notifications in the Cloud Director site.....	175
Configure tenant event notifications in the Cloud Director site.....	178
Configure event notifications for vSphere DR and migration.....	181

Subscribe for weekly summary email.....	183
Update the principal user of a Replicator instance.....	184
Schedule backup archives.....	185
Verify uptime and local and remote connectivity in the Cloud site.....	188
Restart the services.....	191
Collect support bundles.....	191
Record your screen and browser logs.....	193
Allow SSH access to the appliance.....	194
Configure the logging levels.....	195
Change the password of the appliance <b>root</b> user.....	196
Configure after changing the vCenter SSO credentials.....	197
Free up VMware Cloud Director Availability appliance disk space.....	198
Cannot access the VMware Cloud Director Availability Tenant Portal through VMware Cloud Director.....	198
Unregister the VMware Cloud Director Availability plug-ins from VMware Cloud Director.....	199
<b>User Guide.....</b>	<b>201</b>
<b>Accessing VMware Cloud Director Availability.....</b>	<b>201</b>
Access the VMware Cloud Director Availability vSphere Client Plug-In.....	201
Accessing the VMware Cloud Director Availability Tenant Portal.....	202
Log in to the VMware Cloud Director Availability Tenant Portal.....	203
Log in by using the VMware Cloud Director™ Tenant Portal.....	203
Accessing the VMware Cloud Director Availability Provider Portal.....	204
Log in to VMware Cloud Director Availability as a provider.....	204
Log in by using the VMware Cloud Director™ Provider Admin Portal.....	205
Authenticating to paired remote cloud sites.....	205
Authenticate to remote sites as a tenant.....	208
Authenticate to remote sites as a provider.....	209
Multisite authentication.....	209
Configure my preferences.....	210
<b>Replicating workloads.....</b>	<b>212</b>
Creating a new replication.....	218
Create a protection.....	218
Create a migration.....	221
Create a replication for encrypted virtual machines.....	223
Migrating, failing over, testing failover, and reversing replications.....	224
Migrate a replication.....	225
Failover of a replication.....	226
Test failover a replication.....	228
Reverse a Replication.....	232
Replicating with Cloud Director sites.....	233
Replication tracking placement solution.....	233

Configuring replication policies.....	235
Configuring SLA profiles.....	241
Grouping virtual machines in a vApp replication to the Cloud Director site.....	245
Configure recovery settings and guest customization.....	248
Replicating vApp templates between Cloud Director sites.....	257
VDC compute policies.....	261
Configuring settings.....	262
Using instances.....	262
Using replication seeds.....	267
Edit replication settings.....	270
Select a storage policy.....	271
Configure recovery settings for vSphere DR and migration.....	271
Selecting disks for replication.....	272
Recovery Plans.....	274
Replication states.....	279
<b>Monitoring.....</b>	<b>281</b>
View the activity summary report in the Cloud Director site as a provider.....	281
Advisories notifications.....	281
RPO compliance reports.....	283
Monitoring the traffic usage.....	284
Monitor the traffic usage as a tenant.....	285
Monitor and export organization traffic usage as a provider.....	286
Monitor the traffic usage of a virtual machine replication.....	286
Monitoring the disk usage.....	287
Monitor the disk usage as a tenant.....	287
Monitor and export organization disk usage as a provider.....	288
Monitor the disk usage of a virtual machine replication.....	288
Monitoring the required resources.....	289
Monitor the required resources as a tenant.....	290
Monitor the required resources as a provider.....	290
<b>Modify the VMware Cloud Director Availability License Key.....</b>	<b>291</b>
<b>Security Guide.....</b>	<b>292</b>
<b>Services and network ports.....</b>	<b>292</b>
<b>Services network connectivity.....</b>	<b>295</b>
<b>Services configuration files.....</b>	<b>296</b>
<b>Services security configuration properties.....</b>	<b>297</b>
<b>Services logs locations.....</b>	<b>299</b>
<b>Users roles rights and sessions.....</b>	<b>303</b>
<b>VMware General Terms and open-source license.....</b>	<b>310</b>
<b>Upgrade for the latest updates.....</b>	<b>311</b>

---

<b>Migration to VMware Cloud Director service Guide.....</b>	<b>312</b>
Prepare the SDDC in VMware Cloud on AWS for deployment.....	317
Deploy VMware Cloud Director Availability in the SDDC.....	321
Configure the network of the SDDC in VMware Cloud on AWS.....	323
Configure VMware Cloud Director Availability in VMware Cloud on AWS.....	329
Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS.....	332
SDDC network configuration summary.....	334
Pairing with remote sites.....	335
Configure and Pair the On-Premises to Cloud Director Replication Appliance.....	335
Pair VMware Cloud Director Cloud Sites.....	338
Post-configure the SDDC networking in VMware Cloud on AWS.....	339
<b>VMware Cloud Director Availability Cold Migration.....</b>	<b>344</b>
Activate the cold migrations.....	345
Cold migrate.....	346
Post cold migrate.....	348
Post cold migrate for Windows-based machines.....	348
Post cold migrate for Linux-based machines.....	348
Cold migrate support matrix.....	349
<b>VMware Cloud Director Availability in Azure VMware Solution.....</b>	<b>351</b>
Run command in Azure VMware Solution.....	356
VMware Cloud Director Availability Run command glossary.....	357
<b>API Guides.....</b>	<b>367</b>
<b>Terminology.....</b>	<b>368</b>
<b>Changelog.....</b>	<b>371</b>
<b>Documentation Legal Notice.....</b>	<b>374</b>

---

# Release Notes

---

Includes product enhancements and notices, bug fixes, and resolved issues.

## VMware Cloud Director Availability 4.7.3.1 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Upgrade](#)
- [Interoperability](#)
- [Configuration maximums](#)
- [APIs](#)
- [Caveats and limitations](#)
- [Resolved Issue](#)

### **Introduction**

VMware Cloud Director Availability 4.7.3.1   13 FEB 2025   Build 24563708 (Product version: 4.7.3.1.10992338-4bf87a35d5) Check for additions and updates to these release notes.
---

### **What's New**

VMware Cloud Director Availability 4.7.3.1 includes important resolved issues and enhancements.

### **Upgrade**

VMware Cloud Director Availability 4.7.3.1 supports an in-place upgrade directly from versions 4.5.x, 4.6.x, and 4.7.x.

For information about the upgrade process, see [Upgrading in the Cloud Director site](#) and [Upgrading on-premises and provider site](#).

### **Interoperability**

For information about the products and versions that are compatible with VMware Cloud Director Availability, see the [Product Interoperability Matrix](#).

#### **NOTE**

The VMware Cloud Director Availability 4.7.3.1 interoperability is the same as VMware Cloud Director Availability 4.7.3.

### **Configuration maximums**

For information about the tested and verified uptime, concurrency, and scale limits, see [VMware Configuration Maximums](#).

## APIs

The step-by-step guides to configure a deployed appliance by using APIs are available at [VMware Cloud Director Availability Cloud Director DR and Migration API Reference](#) and [VMware Cloud Director Availability vSphere DR and Migration API Reference](#).

## Caveats and limitations

- When replicating a VM with enabled vTPM, the VM must follow an encrypted storage policy.
- Encryption of an attached storage disk during the replication process is supported only when the configuration files of the VM are encrypted and the VM follows an encrypted storage policy at the destination site.
- Replication of an encrypted VM, originally protected or migrated as a non-encrypted VM, is not supported.
- For replications using the **Classic** data engine, VMware Cloud Director Availability 4.7.3.x uses vSphere Replication module called Host-based Replication (HBR) version 9.0.1. For information about its inherited caveats and limitations, see the [vSphere Replication 9.0.1 Release Notes](#).
- With deactivated telemetry in VMware Cloud Director 10.5 and later, when opening VMware Cloud Director Availability from the plug-in in VMware Cloud Director, providing **Feedback** is not possible.
- The three-tier tenancy capability in VMware Cloud Director is not supported.

## Resolved Issue

### After extending a session to a peer site by using authentication challenge and pVDC filtering, VMs are not listed in the new replication wizard

When initiating an authentication challenge, the VMware Cloud Director login API is case-insensitive and accepts the organization name with the casing that is provided during the initiation of the challenge. The query API is case-sensitive and requires the organization name to entirely match the VMware Cloud Director name. As a result, the query call for listing the VMs does not provide the expected results. This issue is fixed in this release.

## VMware Cloud Director Availability 4.7.3 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New in 4.7.3](#)
- [Upgrade](#)
- [Interoperability](#)
- [Configuration maximums](#)
- [APIs](#)
- [Caveats and limitations](#)
- [Known Issue](#)

## Introduction

VMware Cloud Director Availability 4.7.3 | 18 SEP 2024 | Build 24280288 (Product version: 4.7.3.10534495-154c9f5866)  
Check for additions and updates to these release notes.

---

### **What's New in 4.7.3**

VMware Cloud Director Availability 4.7.3 includes important resolved issues and updates of third-party libraries that provide security fixes.

- Added support for VMware Cloud Director 10.6.0.1.
- Added support for VMware vCenter 8.0 Update 3b.
- Added support for product activation by using a VMware Live Recovery license key.
  - For more information see [Get Software and License Key for VMware Cloud Director Availability](#).

### **Upgrade**

VMware Cloud Director Availability 4.7.3 supports an in-place upgrade directly from versions 4.5.x, 4.6.x, and 4.7.x.

For information about the upgrade process, see [Upgrading in the Cloud Director site](#) and [Upgrading on-premises and provider site](#).

### **Interoperability**

For information about the products and versions that are compatible with VMware Cloud Director Availability, see the [Product Interoperability Matrix](#).

### **Configuration maximums**

For information about the tested and verified uptime, concurrency, and scale limits, see [VMware Configuration Maximums](#).

### **APIs**

The step-by-step guides to configure a deployed appliance by using APIs are available at [VMware Cloud Director Availability Cloud Director DR and Migration API Reference](#) and [VMware Cloud Director Availability vSphere DR and Migration API Reference](#).

### **Caveats and limitations**

- When replicating a VM with enabled vTPM, the VM must follow an encrypted storage policy.
- Encryption of an attached storage disk during the replication process is supported only when the configuration files of the VM are encrypted and the VM follows an encrypted storage policy at the destination site.
- Replication of an encrypted VM, originally protected or migrated as a non-encrypted VM, is not supported.
- For replications using the **Classic** data engine, VMware Cloud Director Availability 4.7.3 uses vSphere Replication module called Host-based Replication (HBR) version 9.0.1. For information about its inherited caveats and limitations, see the [vSphere Replication 9.0.1 Release Notes](#).
- With deactivated telemetry in VMware Cloud Director 10.5 and later, when opening VMware Cloud Director Availability from the plug-in in VMware Cloud Director, providing **Feedback** is not possible.
- The three-tier tenancy capability in VMware Cloud Director is not supported.

### **Known Issue**

#### **After extending a session to a peer site by using authentication challenge and pVDC filtering, VMs are not listed in the new replication wizard**

When initiating an authentication challenge, the VMware Cloud Director login API is case-insensitive and accepts the organization name with the casing that is provided during the initiation of the challenge. The query API is case-sensitive and requires the organization name to entirely match the VMware Cloud Director name. As a result, the query call for listing the VMs does not provide the expected results.

**Workaround:** Upgrade to VMware Cloud Director 4.7.3.1. Alternatively, when initiating an authentication challenge, use the case sensitivity and name of the organization that you saved in your VCD.

## VMware Cloud Director Availability 4.7.2 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's new](#)
- [Upgrade](#)
- [APIs](#)
- [Configuration maximums](#)
- [Caveats and limitations](#)
- [Resolved issues](#)
- [Known issues](#)

### **Introduction**

VMware Cloud Director Availability 4.7.2 | 04 JUL 2024 | Build 24058656 (Product version: 4.7.2.10056114-4ada44c9c3)  
Check for additions and updates to these release notes.

### **What's new**

VMware Cloud Director Availability 4.7.2 includes important resolved issues and updates of third-party libraries that provide security fixes.

- Added support for protection and migration of virtual machines with enabled vTPM, and with full, partial, or no encryption of the attached storage disks.
- Added support for encryption of non-encrypted VM as a part of the protection or migration process.
- Added support for protection or migration processes with storage policies that use mixed encryption capabilities.

### **Upgrade**

VMware Cloud Director Availability 4.7.2 supports an in-place upgrade directly from versions 4.5.x, 4.6.x, 4.7, and 4.7.1.

For information about the upgrade process, see [Upgrading in the Cloud Director site](#) and [Upgrading on-premises and provider site](#).

### **APIs**

The step-by-step guides to configure a deployed appliance by using APIs are available at [VMware Cloud Director Availability Cloud Director DR and Migration API Reference](#) and [VMware Cloud Director Availability vSphere DR and Migration API Reference](#).

### **Configuration maximums**

For information about the tested and verified uptime, concurrency, and scale limits, see [VMware Configuration Maximums](#).

### **Caveats and limitations**

- When replicating a VM with enabled vTPM, the VM must follow an encrypted storage policy.
- Encryption of an attached storage disk during the replication process is supported only when the configuration files of the VM are encrypted and the VM follows an encrypted storage policy at the destination site.
- Changing the encryption storage policy of a replicated VM is not supported.

- For replications using the **Classic** data engine, VMware Cloud Director Availability 4.7.2 uses vSphere Replication module called Host-based Replication (HBR) version 9.0.1. For information about its inherited caveats and limitations, see the [vSphere Replication 9.0.1 Release Notes](#).
- With deactivated telemetry in VMware Cloud Director 10.5 and later, when opening VMware Cloud Director Availability from the plug-in in VMware Cloud Director, providing **Feedback** is not possible.

### **Resolved issues**

The following issues have been resolved in this release.

#### **When using seed disks, you cannot create a virtual machine replication from a Cloud Director site to an on-premises site**

This issue is fixed in this release.

#### **When using the default online repository, upgrading VMware Cloud Director Availability might fail**

The default online repository of VMware Cloud Director Availability changed to `https://packages-prod.broadcom.com/vcav/`. When VMware Cloud Director Availability tries to access the legacy repository, the upgrade process might fail. This issue is fixed in this release.

#### **After a migration from an on-premises site to a Cloud Director site, the network settings of the new VM are missing**

When using VMware Cloud Director Availability 4.7 and later to migrate a VM from an on-premises site to a Cloud Director site with version 10.5.1 and later, and with enabled Replication tracking placement solution, the NIC adapter type of the new VM changes from VMXNET3 to E1000, which results in losing all network settings from the source VM. This issue is fixed in this release.

#### **Replicating workloads to a Cloud Director site might fail**

When performing a protection or migration to a Cloud Director site and a source VM has attached storage disks with the same name on different datastores, VMware Cloud Director Availability attempts to recreate the disks with the same name on the destination, which results in the replication process failing with an error message: Unable to create replica placeholder disk. This issue is fixed in this release.

#### **This release resolves CVE-2024-22277**

For more information on this vulnerability and its impact on VMware by Broadcom products, see [VMSA-2024-0016](#).

### **Known issues**

There are no known issues identified in this release.

## **VMware Cloud Director Availability 4.7.1 Release Notes**

This document contains the following sections

- [Introduction](#)
- [What's new](#)
- [Upgrade](#)
- [APIs](#)
- [Configuration maximums](#)
- [Caveats and limitations](#)
- [Resolved issues](#)
- [Known issue](#)

## Introduction

VMware Cloud Director Availability 4.7.1 | 15 FEB 2024 | Build 23265673 (Product version: 4.7.1.8968498-0422b55a9e)  
Check for additions and updates to these release notes.

## What's new

VMware Cloud Director Availability 4.7.1 includes important resolved issues and updates of third-party libraries that provide security fixes.

## Upgrade

VMware Cloud Director Availability 4.7.1 supports an in-place upgrade directly from versions 4.5.x, 4.6.x and 4.7. To upgrade to version 4.7.1 from an earlier version, first upgrade to either version 4.5.x, or to version 4.6.x.

For information about the upgrade process, see [Upgrading in the Cloud Director site](#) and [Upgrading on-premises and provider site](#).

## APIs

The step-by-step guides to configure a deployed appliance by using APIs are available at [VMware Cloud Director Availability Cloud Director DR and Migration API Reference](#) and [VMware Cloud Director Availability vSphere DR and Migration API Reference](#).

## Configuration maximums

For information about the tested and verified uptime, concurrency, and scale limits, see [VMware Configuration Maximums](#).

## Caveats and limitations

- For replications using the **Classic** data engine, VMware Cloud Director Availability 4.7 uses vSphere Replication module called Host-based Replication (HBR) version 8.8. For information about its inherited caveats and limitations, see the [vSphere Replication 8.8 Release Notes](#).
- With deactivated telemetry in VMware Cloud Director 10.5 and later, when opening VMware Cloud Director Availability from the plug-in in VMware Cloud Director, providing **Feedback** is not possible.

## Resolved issues

The following issues have been resolved in this release.

### **A recovered VM might have a different amount of NICs than the source VM**

After a failover or a test failover, the operation of adding or removing network adapters from a protected VM that is backed up by a replication tracking VM, might not be reflected on the resulting VM. Only the network adapters present at the start of the replication operation might be available to the recovered VM. The issue might occur only when using VCDA 4.7.0 with VCD 10.5.1 and later, and does not affect replications that are backed up by independent disks. This issue is fixed in this release.

### **For replications to Cloud Director sites, when using a flexible storage profile in a recovery plan, the health validation does not check the availability of the disk storage profiles**

If a disk in a replication is assigned with a storage profile that is no longer available, while the VM configuration is assigned with an available storage profile, once this replication is added in a recovery plan, the health validation reports no issues. This issue affects only replications to a Cloud Director site as destination. This issue is fixed in this release.

### **For vSphere DR and migration, using per-disk Placement Datastore on test failover produces a VM which seemingly has all its disks on the VM Placement Datastore**

When you perform test failover, the disks of the test failover VM appear on the **VM Placement Datastore** despite another storage policy assigned to its disks. Technically, the disks reside both on the **Placement Datastore**, where you select the disks to replicate, and on the **VM Placement Datastore**, where you select the VM configuration files to replicate.

Most of the replica data is still on the disks storage where you selected. Only a child disk resides on the configuration files datastore, which you can safely ignore. This issue only affects vSphere DR and migration between vCenter Server sites.

This issue is fixed in this release.

### **The context menu in VMware Cloud Director does not allow to edit the replication settings page**

For existing replications, in VMware Cloud Director, selecting **Actions > Availability (site) > Replication settings** opens the **Replication settings** window, where all settings are inactive and cannot be modified. This issue is fixed in this release.

### **Replications using the Classic data engine fail to synchronize or show a red state**

Due to specific networking requirements, replications that use the **Classic** data engine are affected:

- Attempting to configure a new replication results in a task that is stuck. After about 10 minutes, the task might finish successfully, but the replication remains in red state.
- Attempting to synchronize an existing replication fails with *sync timeout*.

This issue is fixed in this release.

### **Known issue**

The following known issue is currently identified in this release.

### **When using the default online repository, upgrading VMware Cloud Director Availability might fail**

The default online repository of VMware Cloud Director Availability changed to `https://packages-prod.broadcom.com/vcav/`. When VMware Cloud Director Availability tries to access the legacy repository, the upgrade process might fail.

**Workaround:** Perform one of the following tasks.

- When upgrading in an on-premises and provider site, [upgrade by using a specified repository](#).
- When upgrading in a Cloud Director site, [upgrade by using a specified repository](#).

## **VMware Cloud Director Availability 4.7 Release Notes**

This document contains the following sections

- [Introduction](#)
- [What's new](#)
- [Upgrade](#)
- [APIs](#)
- [Interoperability](#)
- [Legacy migrations](#)
- [Configuration maximums](#)
- [Caveats and limitations](#)
- [Supported browsers](#)
- [Resolved issues](#)
- [Known issues](#)

## Introduction

VMware Cloud Director Availability 4.7 | 23 NOV 2023 | Build 22817906 (Product version: 4.7.0.8400987-96215f032c)  
Check for additions and updates to these release notes.

## What's new

VMware Cloud Director Availability 4.7 supports the following new functionality:

- Storage policy reassignment during workload recovery - now you can activate Change storage placement, then select a different datastore than the selected one in the existing replication, resulting in move of the data after the performed failover or migrate operation completes. All the disks and the vmdk files move to the newly selected storage. For example, the tenants can initially send the replica files to a cheaper and slower storage, where the vmdk gets constructed, then once failed over, the workload moves to expensive and fast storage. For information about changing the storage placement during recovery, see [Migrate](#) and [Failover](#).
- Security tags - now, the NSX security tags can be replicated between cloud sites, both running VMware Cloud Director 10.3 and later and VMware Cloud Director Availability 4.7. The security tags apply during the recovery of virtual machine, vApp, and vApp template replications. For information about copying the security tags to the destination, see [Migrate](#), [Failover](#), and [Test Failover](#).
- VDC VM policies pre-selected - now, when creating a replication to a Cloud Director site as a destination, when a VM placement or a VM sizing policy with the same name already applies on the source workload, the matching VDC policy becomes pre-selected, allowing to finish the new replication wizard quicker. For information about using the selected VDC policies in the new replication wizard, see [Create a protection](#) and [Create a migration](#).
- Recovery plans health validation - now, after creating a recovery plan, on the Health tab you see a validation of the infrastructure and the data for the replications in the plan to check whether the plan execution might fail on some steps. The validation can show a warning when the observed issues cannot prevent the recovery process, or an error when the issues prevent the recovery process, for example, when the destination storage policy is disabled. For information about the health validations, see [Recovery plans](#).
- Flexible storage profile assignment - now allows replicating one virtual machine to multiple datastores. For example, place one of its disks on a separate datastore, or split some disks from the .vmx file. For information about activating Advanced Datastore Settings and how to use flexible storage profile assignment in the New Replication wizard, see [Create a protection](#) and [Create a migration](#).
- Pairing sites filtering - now the providers can hide some peer sites for certain organizations to prevent every tenant from seeing all paired sites for convenience. The restricted tenants can continue to manage existing incoming replications, but not start new ones as the source site is not visible and cannot see the outgoing replications as they are filtered by site. For information about filtering the peer sites, see [Control the paired sites organization access](#).
- Cloud Director authentication model compliance - now prepares VMware Cloud Director Availability for the future deprecation of local users in VMware Cloud Director. For information about this deprecation, see VMware Cloud Director 10.4.1 Release Notes. API token pairing - now also supports pairing an on-premises site to a Cloud Director site by using a one-time access token, see [Generate an API access token from VMware Cloud Director](#). Next, for information about using such API token for the initial pairing, see [Configure the On-Premises to Cloud Director Appliance](#). VMware Cloud Director Availability 4.7 continues to fully-support local users while they are under deprecation.
- Replication tracking virtual machine (RT VM) placement solution for Cloud Director replications - now replaces the independent disk and represents a shadow VM for replication placement to allow per-disk placement. The providers can also configure replication tracking for the existing vApp and VM replications. With a supported version of VMware Cloud Director in the destination site, RT VM replaces the independent disk as placement and reporting solution and allows per-disk storage profiles. For more information about RT VM, see [Replication tracking placement solution](#).
- Seed for vSphere DR and migration - now using a seed virtual machine is also available for replications between vCenter sites. For information about using a seed, see [Configure a replication with a seed](#).
- Deactivate protections to on-premises - protections now allow for finer control on the allowed destination site, separating on-premises from cloud sites, similarly to controlling migrations separately for on-premises and cloud

destinations. For information about the policies to control this, see [Configuring replication policies](#), [Create a replication policy](#), and [Edit a replication policy](#).

- **My Preferences** now allows each user to select the language of their interface, dark, light, or high contrast theme, and select number of rows and whether the selected row follows the clicked row.

## **Upgrade**

VMware Cloud Director Availability 4.7 supports an in-place upgrade directly from versions 4.5.x or 4.6.x. To upgrade to version 4.7 from earlier versions, first upgrade to either version 4.5.x, or to version 4.6.x.

For information about the upgrade process, see [Upgrading in the Cloud Director site](#) and [Upgrading on-premises and provider site](#).

## **APIs**

The step-by-step guides to configure a deployed appliance by using APIs are available at [VMware Cloud Director Availability Cloud Director DR and Migration API Reference](#) and [VMware Cloud Director Availability vSphere DR and Migration API Reference](#).

## **Interoperability**

- For the interoperability between paired sites that run mismatching VMware Cloud Director Availability versions, see *Managing pairing with Cloud Director sites* in the *Administration Guide*.
- For the interoperability between VMware Cloud Director Availability and other VMware products and versions, see the [Product Interoperability Matrix](#).

## **Legacy migrations**

VMware Cloud Director Availability 4.7 continues to support migrations from legacy vCenter Server versions 5.5, 6.0, 6.5, and 6.7. Note: vCenter Server 6.5 and 6.7 are legacy versions since VMware Cloud Director Availability 4.6.

For information about the legacy migrations, see KB [89181](#).

## **Configuration maximums**

For information about the tested and verified uptime, concurrency, and scale limits, see [VMware Configuration Maximums](#).

## **Caveats and limitations**

- For replications using the **Classic** data engine, VMware Cloud Director Availability 4.7 uses vSphere Replication module called Host-based Replication (HBR) version 8.8. For information about its inherited caveats and limitations, see the [vSphere Replication 8.8 Release Notes](#).
- With deactivated telemetry in VMware Cloud Director 10.5 and later, when opening VMware Cloud Director Availability from the plug-in in VMware Cloud Director, providing **Feedback** is not possible.

## **Supported browsers**

VMware Cloud Director Availability 4.7 supports the following versions of the browsers:

- Google Chrome 117 and later
- Microsoft Edge 117 and later
- Mozilla Firefox 117 and later
- Apple Safari 16 and later

## **Resolved issues**

The following issues have been resolved in this release.

### **With over 25 organizations in VMware Cloud Director, vApp templates migrations result in an error when logged in as a provider in VMware Cloud Director Availability**

When the VMware Cloud Director environment has more than 25 organizations and you log in as a **provider** in VMware Cloud Director Availability, then if the vApp template you are trying to replicate is listed on a position over 25, you see an error message: *Cannot read properties of undefined (reading 'id')*

### **For replications with Cloud Director sites, you cannot finish the New Recovery Step wizard if you filter the Recover replications list after you select workloads**

In the **New Recovery Step** wizard, on page **2 Recover replications**, once you select the workloads, then if you filter the list by the name of the **vApp/VM** entering 3 characters or more, the selection invalidates. When you click **Next**, then **Finish**, the **Ready to complete** page remains opened with an error message: *Cannot read properties of undefined (reading 'vmReplications')*

This issue only affects replications with Cloud Director sites.

### **For vSphere DR and migration, attempting to repair the Replicator instances fails after upgrading to 4.6.1**

In vSphere DR and migration sites only, once upgraded to 4.6.1, you cannot repair the Replicator Service, for example, after changing an SSL certificate, or after changing the SSO credentials of the vCenter Server Lookup Service.

## **Known issues**

The following known issues are currently identified in this release.

### **When using seed disks, you cannot create a virtual machine replication from a Cloud Director site to an on-premises site**

**Workaround:** Upgrade to VMware Cloud Director Availability 4.7.2.

### **After a migration from an on-premises site to a Cloud Director site, the network settings of the new VM are missing**

When using VMware Cloud Director Availability 4.7 and later to migrate a VM from an on-premises site to a Cloud Director site with version 10.5.1 and later, and with Replication tracking placement solution, the NIC adapter type of the new VM changes from VMXNET3 to E1000, which results in losing all network settings from the source VM.

**Workaround:** Upgrade to VMware Cloud Director Availability 4.7.2.

### **Replicating workloads to a Cloud Director site might fail**

When performing a protection or migration to a Cloud Director site and a source VM has attached storage disks with the same name on different datastores, VMware Cloud Director Availability attempts to recreate the disks with the same name on the destination, which results in the replication process failing with an error message: Unable to create replica placeholder disk.

**Workaround:** In the source site, before the replication process, perform one of the following tasks.

- Move one of the disks with duplicate names to the same datastore.
- Rename one of the disks with duplicate names.

### **When using the default online repository, upgrading VMware Cloud Director Availability might fail**

The default online repository of VMware Cloud Director Availability changed to `https://packages-prod.broadcom.com/vcav/`. When VMware Cloud Director Availability tries to access the legacy repository, the upgrade process might fail.

**Workaround:** Perform one of the following tasks.

- When upgrading in an on-premises and provider site, [upgrade by using a specified repository](#).
- When upgrading in a Cloud Director site, [upgrade by using a specified repository](#).

### **A recovered VM might have a different amount of NICs than the source VM**

After a failover or a test failover, the operation of adding or removing network adapters from a protected VM that is backed up by a replication tracking VM, might not be reflected on the resulting VM. Only the network adapters present at the start of the replication operation might be available to the recovered VM. The issue might occur only when using VCDA 4.7.0 with VCD 10.5.1 and later, and does not affect replications that are backed up by independent disks.

**Workaround:** Perform one of the following tasks.

- In the configuration of the recovered VM, add or remove network adapters manually.
- Upgrade to VMware Cloud Director Availability 4.7.1.

### **Replications using the Classic data engine fail to synchronize or show a red state**

Due to specific networking requirements, replications that use the **Classic** data engine are affected:

- Attempting to configure a new replication results in a task that is stuck. After about 10 minutes, the task might finish successfully, but the replication remains in red state.
- Attempting to synchronize an existing replication fails with *sync timeout*.

The issue might occur only when using VCDA 4.7.0

**Workaround:** Perform one of the following tasks.

- Open an SSH session to each Replicator Appliance and execute the following commands:
  - a. 

```
/usr/bin/sed -i '/useDatastoreTickets/a\ \ \ \ \ \  
<hostConnectionUseHbrTunnelEndpoint>>false</hostConnectionUseHbrTunnelEndpoint>' /etc/  
vmware/hbrsrv.xml
```
  - b. 

```
/usr/bin/sed -i '/useDatastoreTickets/a\ \ \ \ \ \  
<hostConnectionUseSdkEndpoint>>false</hostConnectionUseSdkEndpoint>' /etc/vmware/  
hbrsrv.xml
```
  - c. 

```
systemctl restart hbrsrv
```
- Upgrade to VMware Cloud Director Availability 4.7.1.

### **For replications to Cloud Director sites, when using a flexible storage profile in a recovery plan, the health validation does not check the availability of the disk storage profiles**

If a disk in a replication is assigned with a storage profile that is no longer available, while the VM configuration is assigned with an available storage profile, once this replication is added in a recovery plan, the health validation reports no issues. This issue affects only replications to a Cloud Director site as destination.

**Workaround:** Upgrade to VMware Cloud Director Availability 4.7.1.

### **For vSphere DR and migration, using per-disk Placement Datastore on test failover produces a VM which seemingly has all its disks on the VM Placement Datastore**

When you perform test failover, the disks of the test failover VM appear on the **VM Placement Datastore** despite another storage policy assigned to its disks. Technically, the disks reside both on the **Placement Datastore**, where you select the disks to replicate, and on the **VM Placement Datastore**, where you select the VM configuration files to replicate.

Most of the replica data is still on the disks storage where you selected. Only a child disk resides on the configuration files datastore, which you can safely ignore. This issue only affects vSphere DR and migration between vCenter Server sites.

**Workaround:** Upgrade to VMware Cloud Director Availability 4.7.1.

### **The context menu in VMware Cloud Director does not allow to edit the replication settings page**

For existing replications, in VMware Cloud Director clicking **Actions > Availability (site) > Replication settings** opens the **Replication settings** window where all settings are inactive and cannot be modified.

Workaround:

To modify the replication settings:

- Use the plug-in for VMware Cloud Director Availability by clicking **More > Availability (site)**
- Alternatively, log in to the VMware Cloud Director Availability interface.

Then navigate to the replication, select it and click **All Actions > Replication settings**.

### **For vSphere DR and migration, duplicate virtual machine names show under Advanced Datastore Settings when using the vSphere plug-in**

From the vSphere plug-in, after initially activating the **Advanced Datastore Settings** toggle, the virtual machine names show duplicates. This issue only affects vSphere DR and migration between vCenter Server sites.

Workaround:

- Deactivate the **Advanced Datastore Settings** toggle, then activate it again.
- Alternatively, log in directly to VMware Cloud Director Availability then repeat the replication operation.

## **VMware Aria Operations Management Pack for Cloud Director Availability 1.4 Release Notes**

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Upgrade](#)

### **Introduction**

VMware Aria Operations Management Pack for Cloud Director Availability 1.4 | 13 APR 2023 | Build 21371223  
VMware Aria Operations Management Pack for Cloud Director Availability 1.4.1 | 19 DEC 2024 | Build 24443579  
Check for additions and updates to these release notes.

### **What's New**

#### **VMware Aria Operations Management Pack for Cloud Director Availability 1.4.1**

- When registering the VMware Aria Operations Management Pack for Cloud Director Availability 1.4, if you select a Cloud Director site and the Cloud Director Address leads to a VMware Cloud Director instance version 10.6.0.1 and later, the registration operation fails. This issue is fixed in VMware Aria Operations Management Pack for Cloud Director Availability 1.4.1.

#### **VMware Aria Operations Management Pack for Cloud Director Availability 1.4**

- Now allows registering cloud vCenter sites to see their metrics, dashboards, views, alerts, and reports, similarly to Cloud Director sites.
- Now tracks replications from a Cloud Director site to an on-premises site, similarly to cloud site to cloud site replications.
- Adds new metrics for cloud site to cloud site replications.
- Now provides recommendations for each alert to help remedy the issue.

- Now separates the Views into Cloud Director sites and cloud vCenter sites.
- Now allows for improved resiliency if VMware Cloud Director Availability is offline. For example, when the Manager Service or the Cloud Service is not available or with changed credentials, VMware Aria Operations handles the situation correctly with alerts and recommendations.

For more information about installing, configuring this management pack and using the:

- Dashboards
- Views
- Metrics
- Alert definitions
- Reports

see each respective chapter in the *VMware Aria Operations Management Pack for Cloud Director Availability Install, Upgrade, and Use Guide*, available on the VMware Marketplace website, along with the installation *vmware-VcdaAdapter-1.4.0-build\_no.pak* file.

### **VMware Sovereign Cloud**

VMware Aria Operations Management Pack for Cloud Director Availability 1.4 supports VMware Aria Operations Compliance Pack for VMware Sovereign Cloud 1.1 and later.

For VMware Sovereign Cloud, a new property under System Health, called CEIP Enabled tracks whether telemetry is allowed in VMware Cloud Director Availability.

### **Upgrade**

To upgrade from versions 1.2.x or 1.3 to VMware Aria Operations Management Pack for Cloud Director Availability 1.4.x, in VMware Aria Operations, install the .pak file with version 1.4.x. Verify that the version of VMware Aria Operations is 8.10 or later.

In the **Add Solution** wizard, on the **Select Solution** page, select the **Reset the Default Content** check box.

For information about the upgrade, see the **Upgrade** page in the *VMware Aria Operations Management Pack for Cloud Director Availability Install, Upgrade, and Use Guide*.

## What is VMware Cloud Director Availability

VMware Cloud Director Availability™ is a Disaster Recovery-as-a-Service (DRaaS) solution. Between providers' clouds or on-premises, with asynchronous replications, VMware Cloud Director Availability protects, migrates, fails over, and reverses failovers of vApps and virtual machines. VMware Cloud Director Availability is available through the Partner Connect Program.

VMware Cloud Director Availability introduces a unified architecture for the disaster recovery protection and migration of VMware vSphere® workloads. In both sites with VMware Cloud Director Availability, formerly known as vCloud Availability, the providers and their tenants can protect and migrate vApps and virtual machines:

- Between an on-premises vCenter Server site and a multi-tenant provider cloud site with VMware Cloud Director™.
- Between multi-tenant provider cloud sites with VMware Cloud Director.

vSphere DR and migration is another deployment topology for both sites, and the providers and their tenants can protect and migrate vSphere workloads:

- Between an on-premises vCenter Server site, and a provider cloud vCenter Server site.
- Between providers' cloud vCenter Server sites.

### Cloud site

- In a multi-tenant provider cloud site backed by VMware Cloud Director, one VMware Cloud Director Availability instance consists of the following number of appliances:
  - one Cloud Director Replication Management Appliance,
  - one or more Replicator Appliance instances, and
  - one or, optionally, two Tunnel Appliance instances operating in an active-active mode for high availability (HA).
 Multiple Availability cloud sites can coexist in one VMware Cloud Director instance. In a cloud site, all the appliances operate together, supporting the management of replications, secure SSL communication, and storage of the replicated data. The provider can support recovery for multiple tenants environments that can scale, allowing handling the increasing workloads.
- In a provider cloud vCenter Server site, one VMware Cloud Director Availability instance consists of one vCenter Replication Management Appliance and, optionally, one or more Replicator Appliance instances. VMware Cloud Director is not required.

### On-premises site

In an on-premises disaster recovery environment, tenants manage their replications using the VMware Cloud Director Availability vSphere Client Plug-In, supported by a VMware Cloud Director Availability On-Premises Appliance. In the on-premises vCenter Server instance, depending on the provider cloud site, deploy the on-premises appliance:

- as either an On-Premises to Cloud Director Replication Appliance, or
- as an On-Premises to Cloud vCenter Replication Appliance.

### Documentation phases map

#### **Day 0 operations**

Represents the design phase, when requirements and security are specified and the architecture is completed. For the latest VMware Cloud Director Availability version, in the following table see the *Release Notes* and the *Security Guide*.

#### **Day 1 operations**

Contains the prerequisites for deploying the virtual appliances and their installation and configuration as designed in the Day 0 phase. Also in this phase, the infrastructure, network, and external services are initially configured. The initial design is deployed and the infrastructure is configured, based on the designed specifications.

For each VMware Cloud Director Availability version, in the following table see the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*, the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*, and the *Migration with VMware Cloud Director service Guide*.

## Day 2 operations

Focuses on the daily routine operations like authentication, using replications, and maintenance, monitoring, and troubleshooting. Configuring the settings of the network interface cards (NIC), replacing the SSL certificates of the appliances, configuring provider and tenants events, and others.

For each VMware Cloud Director Availability version, in the following table see the *User Guide* and the *Administration Guide*.

## vCloud Usage Meter integration

VMware vCloud® Usage Meter must meter the configured for protection or migration virtual machines using VMware Cloud Director Availability.

### Metering instances

As a provider, you must meter the consumption data of VMware Cloud Director Availability and generate monthly usage reports for protections and for migrations, by adding each cloud VMware Cloud Director Availability instance in vCloud Usage Meter, depending on the network access:

When vCloud Usage Meter is internal to the network of VMware Cloud Director Availability, you must meter each VMware Cloud Director Availability cloud site in vCloud Usage Meter by adding:

- Each instance of Cloud Director Replication Management Appliance, or
- Each instance of vCenter Replication Management Appliance.

Enter each appliance-IP-address-or-hostname, port 443, then select one of the following authentication providers:

- Cloud Director Availability - authentication method for metering either a vCenter Replication Management Appliance or a Cloud Director Replication Management Appliance. This authentication provider requires the root user credentials of the Replication Management Appliance. Only this authentication method is supported in earlier versions than vCloud Usage Meter 4.7.
- vSphere SSO - authentication method for metering a vCenter Replication Management Appliance. This authentication provider requires a valid vSphere SSO account, member of the VrMonitoringAdministrators SSO group. For information about this account, see the *Security Guide*.
- Cloud Director - authentication method for metering a Cloud Director Replication Management Appliance. This authentication provider requires a valid VMware Cloud Director provider account with the VCDA\_VIEW\_RIGHT assigned. For information about this account, see the *Security Guide*.
- Alternatively, when vCloud Usage Meter is external to the network of VMware Cloud Director Availability, you must meter the entire VMware Cloud Director Availability cloud site in vCloud Usage Meter by adding the Public Service Endpoint:443, and the root user credentials of all Replication Management Appliances. For cloud sites backed by VMware Cloud Director, also activate Allow admin access from anywhere on the Settings page in the Cloud Director Replication Management Appliance.

## Supported versions

Use only VMware Cloud Director Availability 4.7.x or 4.6.x.

## **vSphere DR and migration between vCenter Server sites:**

Pairing vCenter Server sites requires the following versions between source and destination:

- Versions 4.4.x interoperate only with sites running versions 4.4.x.
- Versions 4.5.x interoperate with sites running either versions 4.5.x, or 4.6.x, or 4.7.x.
- Versions 4.6.x interoperate with sites running either versions 4.5.x, or 4.6.x, or 4.7.x.
- Version 4.7.x interoperates with sites running either versions 4.5.x, or 4.6.x., or 4.7.x.

**Cloud Director sites**

Pairing sites backed by VMware Cloud Director requires using the latest maintenance patch release for VMware Cloud Director Availability.

# Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site

VMware Cloud Director Availability™ is a Disaster Recovery-as-a-Service (DRaaS) solution. VMware Cloud Director Availability On-Premises Appliance protects and migrates vSphere workloads between the on-premises vCenter Server instance and either a provider vCenter Server site or a multi-tenant cloud site backed by VMware Cloud Director™.

VMware Cloud Director Availability is available through the Partner Connect Program. This solution provides multi-tenant workload protection and recovery between various cloud sites and with on-premises vCenter Server sites. Choose one of the two VMware Cloud Director Availability deployment types, depending on whether the destination cloud site is backed by VMware Cloud Director:

- **On-premises site and Cloud Director site:**  
Replication management and monitoring between on-premises sites and multi-tenant cloud sites backed by VMware Cloud Director, by using a VMware Cloud Director Availability On-Premises Appliance at each on-premises vCenter Server site. For information about this architecture, see [Deployment architecture for the On-Premises to Cloud Director Replication Appliance](#).
- **vSphere DR and migration between vCenter Server sites:**  
The VMware Cloud Director Availability On-Premises Appliance deployment file contains an additional appliance role that can replicate between an on-premises vCenter Server site and a cloud vCenter Server site. For this, during the initial on-premises appliance deployment, select its role as On-Premises to Cloud vCenter Replication Appliance. Then pair the new on-premises appliance with a vCenter Replication Management Appliance, deployed, licensed, and metered in the cloud vCenter Server instance. For information about this architecture, see [Deployment architecture and requirements for vSphere DR and migration](#).

During the on-premises appliance deployment in the on-premises vCenter Server instance, depending on the cloud site type, select the appliance role as either:

- **On-Premises to Cloud Director Replication Appliance:**  
Pairs with a cloud site backed by VMware Cloud Director. For more information, see [Installing and configuring the On-Premises to Cloud Director Replication Appliance](#).
- **On-Premises to Cloud vCenter Replication Appliance:**  
Pairs to a cloud vCenter Server site, running vCenter Replication Management Appliance. For more information, see [Installing and configuring both appliances for vSphere DR and migration](#).

As **provider**, in the cloud vCenter Server site deploy:

## vCenter Replication Management Appliance

Pairs to another cloud vCenter Server site, running vCenter Replication Management Appliance. Allows pairing from On-Premises to Cloud vCenter Replication Appliance. For more information, see [Installing and configuring both appliances for vSphere DR and migration](#).

VMware Cloud Director Availability provides:

- Test failover or failover on-premises workloads to the cloud site and fallback of recovered in the cloud workloads back to the on-premises site.
- Migration of protected virtual machines in the cloud site back to the on-premises site and vice versa.
- Self-service protection and failover workflows per virtual machine.
- One vApp or virtual machine replicates to a one destination site. That is, the same source workload can replicate only on a single destination.
- Each deployment can serve as both a source and a recovery site. There are no dedicated source and destination sites.
- Symmetrical replication flow that can be started from either the source or the recovery site.
- Built-in secure tunneling that requires no incoming allowed ports in the firewall in the on-premises site.

- Built-in end-to-end TLS encryption of the replication traffic that is terminated at each VMware Cloud Director Availability appliance.
- Optional compression of the replication traffic.
- VMware Cloud Director Availability vSphere Client Plug-In integration with the existing vSphere environment.
- Support for multiple vCenter Server and ESXi versions.
- Single installation package, distributed as a Photon-based virtual appliance.

## Interoperability and vSphere product edition

Before deploying and pairing VMware Cloud Director Availability, first verify the interoperability between VMware Cloud Director Availability and ESXi, the vSphere product edition, and the other VMware products in the disaster recovery infrastructure, the interoperability and the supported versions between the source site and the destination site.

### **VMware Cloud Director Availability interoperability matrices**

Before installing VMware Cloud Director Availability, verify the supported versions of ESXi and vSphere. For interoperability information between VMware Cloud Director Availability and other VMware products, see the [Product Interoperability Matrix](#).

### **vSphere product edition**

All sites participating in a replication must run vSphere product editions that include the vSphere Replication feature in their licenses. The ESXi hosts in all paired on-premises sites and in all paired cloud sites must run one of the following vSphere product editions that include the vSphere Replication feature:

- vSphere Essentials Plus
- vSphere Standard
- vSphere Enterprise
- vSphere Enterprise Plus
- vSphere Desktop

#### **NOTE**

Cannot replicate virtual machines to or from ESXi hosts that do not include the vSphere Replication feature in their licenses. Attempting to configure a replication for virtual machines to or from such a host causes failure for the replication with the following error message.

```
Operation aborted due to an unexpected error.
```

This issue occurs when in the source or in the destination site the underlying vSphere environment uses, for example, a vSphere Essentials license. To successfully replicate, configure the underlying environments with licenses that support the vSphere Replication feature in all participating sites.

For information about the license requirements for vSphere Replication, see *vSphere Replication Licensing* in the *vSphere Replication* documentation.

### **Paired sites versions interoperability**

You can pair Cloud Director sites that have mismatching VMware Cloud Director Availability versions deployed. For information about the source site VMware Cloud Director Availability interoperability with the disaster recovery infrastructure in the destination site, select your version and see *Managing pairing with Cloud Director sites* in the *Administration Guide*.

## **Metering cloud sites**

As **provider**, you must meter the consumption data of each cloud site instance of VMware Cloud Director Availability by adding the Public Service Endpoint of the appliances in VMware vCloud® Usage Meter. For more information, see the *Usage Meter integration* section in the *VMware Cloud Director Availability documentation*.

## **Supported versions**

For information about the currently supported VMware Cloud Director Availability versions, see the *VMware Cloud Director Availability supported versions* section in the *VMware Cloud Director Availability documentation*.

# **Installing and configuring both appliances for vSphere DR and migration**

To replicate vSphere workloads between vCenter Server instances, in the provider vCenter Server instance deploy and license a vCenter Replication Management Appliance, optionally deploy one or more Replicator Appliance instances, and in the tenant vCenter Server instance deploy a On-Premises to Cloud vCenter Replication Appliance.

- For vSphere DR and migration between vCenter Server sites, install and configure VMware Cloud Director Availability as a new deployment in both the provider and the tenant vCenter Server instances by following this current chapter.
- Alternatively, for on-premises replication with cloud sites backed by VMware Cloud Director, to install and configure VMware Cloud Director Availability, see the [Installing and configuring the On-Premises to Cloud Director Replication Appliance](#) chapter.

## **Deployment architecture and requirements for vSphere DR and migration**

To protect or migrate vSphere workloads between two vCenter Server sites, deploy two VMware Cloud Director Availability appliances, in each respective vCenter Server instance. Before installing each appliance, verify that each site meets the deployment requirements. Also, allow the network communication within the site and between the sites.

### **vSphere DR and migration**

Between two vCenter Server instances, any user that is a member of **ADMINISTRATORS**, or **VRADMINISTRATORS**, or **VRUSERS** can protect or migrate vSphere workloads after pairing the following VMware Cloud Director Availability appliances in each site, deployed and configured by a user member of **ADMINISTRATORS**. Configuring the appliances with the local vCenter Server Lookup service creates the groups **VRADMINISTRATORS** and **VRUSERS** in the local vCenter Server instance.

## **Appliances Deployment**

- To replicate workloads between provider vCenter Server and tenant vCenter Server, deploy and configure the following appliances, then pair them.

### **vCenter Replication Management Appliance**

In the provider vCenter Server instance, as a vSphere **administrator** user deploy, license, and configure a vCenter Replication Management Appliance, then add it for metering in VMware vCloud® Usage Meter.

Optionally, after configuring the vCenter Replication Management Appliance, the provider can add one or more Replicator Appliance instances for scaling the replication performance.

### **On-Premises to Cloud vCenter Replication Appliance**

---

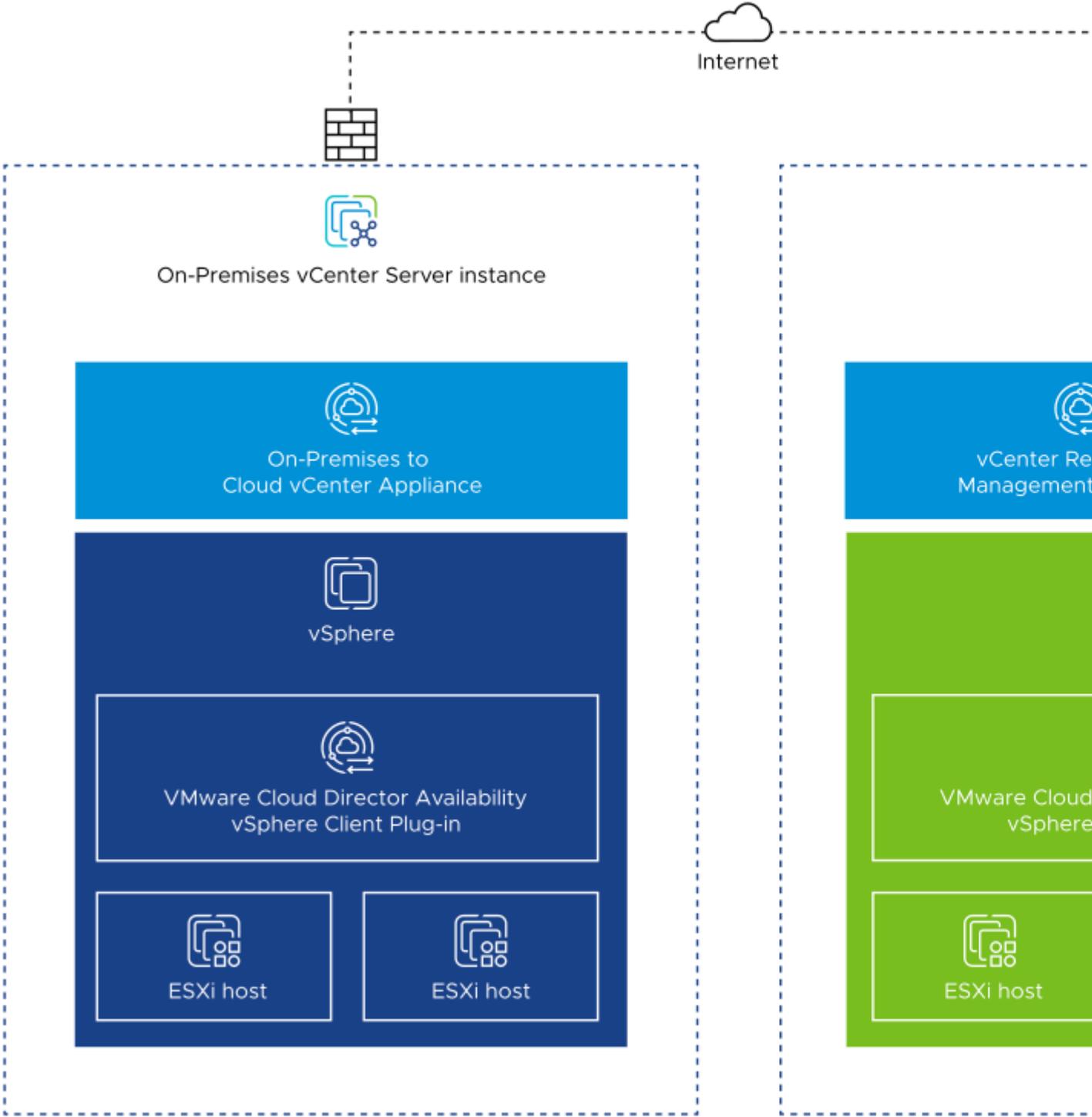
In the tenant vCenter Server instance, as a vSphere **administrator** user, only deploy and configure an On-Premises to Cloud vCenter Replication Appliance.

- For information about deploying both appliances in each vCenter Server instance, see [Deploy both appliances for vSphere DR and migration](#).
- For information about licensing, configuring, metering, and pairing the appliances, see [Configure and pair both appliances for vSphere DR and migration](#).
- Alternatively, to replicate workloads between provider vCenter Server instances, deploy, license, and configure a vCenter Replication Management Appliance in each provider vCenter Server instance. Then add the appliances for metering in vCloud Usage Meter. Finally, pair both appliances, similarly to the example for pairing a tenant and a provider instance.

Optionally, after configuring the appliances, the provider can add one or more Replicator Appliance instances in each provider site for scaling the replication performance.

The following architecture diagram shows an On-Premises to Cloud vCenter Replication Appliance, a vCenter Replication Management Appliance, and optionally, one or

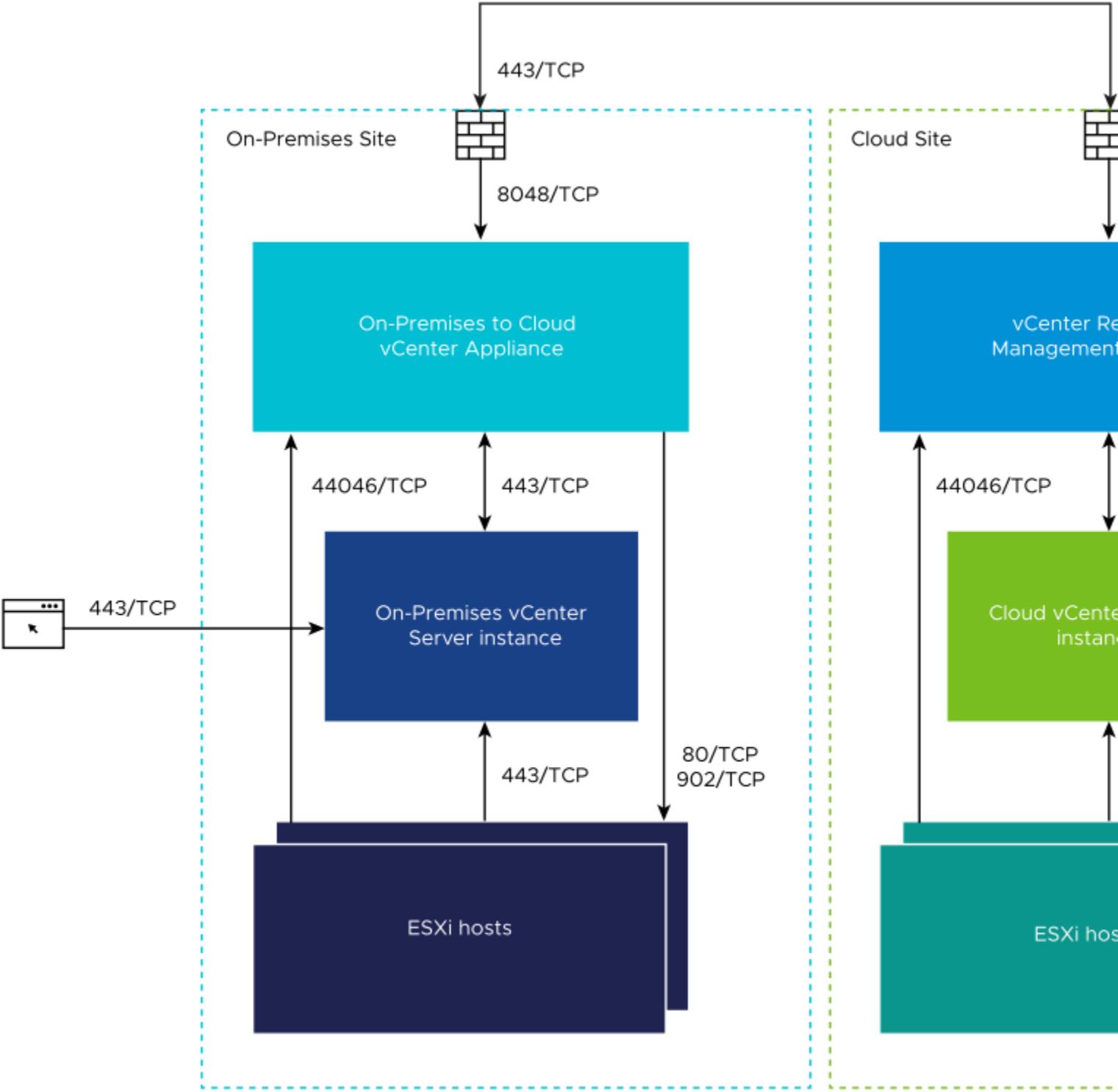
more Replicator Appliance instances, deployed in each respective vCenter Server



instance.

**Network Requirements**

The following diagram shows the network connections and the required network ports for the communication between the vCenter Replication Management Appliance, the On-Premises to Cloud vCenter Replication Appliance, and the disaster recovery infrastructure.



Both appliances expect to receive pairing requests on port 8048/TCP and depending on whether pairing them over a public network or whether pairing them directly over a private network:

**Table 1: Pairing Network Requirements**

Pairing Prerequisites	Private Network Pairing	Public Network Pairing
Destination Network Address Translation (DNAT)	Do not configure DNAT rules.	First, configure a DNAT rule for translating the public <i>Service-Endpoint-IP-address:443</i> to the private <i>Appliance-IP-address:8048</i>
In the <b>New Pairing</b> window enter:	For <b>Service Endpoint</b> , enter <i>Appliance-IP-adress:8048</i> .	For <b>Service Endpoint</b> , enter the public <i>Service-Endpoint-IP-address:443</i> .

For a full list of the required firewall ports to be opened, see [VMware Cloud Director Availability Network Ports](#).

### **Connectivity Requirements**

The two appliances in each site must be able to communicate with each other and with the disaster recovery infrastructure in the sites. The appliances must have TCP access to the ESXi hosts, to the vCenter Server instance, where the vCenter Server Lookup service is hosted, and to the remote VMware Cloud Director Availability appliance in the remote site.

#### **NOTE**

VMware Cloud Director Availability uses end-to-end encryption for the communication across sites. For example, when the On-Premises to Cloud vCenter Replication Appliance is communicating to the vCenter Replication Management Appliance, VMware Cloud Director Availability expects that the TLS session is terminated at both appliances.

VMware Cloud Director Availability does not support any TLS terminating products or solutions placed between the appliances, for example, HAProxy, Nginx, Fortinet, and others. If such tools are in place, they must be configured in pass-thru mode, also known as TCP mode, to prevent from interfering with the TLS traffic of VMware Cloud Director Availability.

### **Hardware Requirements**

From a hosting perspective, the appliances are virtual machines with the following hardware requirements:

- 8 vCPUs
- 8 GB RAM
- 10 GB Storage

These same hardware requirements apply for:

- vCenter Replication Management Appliance and for Replicator Appliance
- On-Premises to Cloud vCenter Replication Appliance

### **Deployment Requirements**

#### **Dedicated ESXi replication VMkernel interfaces**

For production sites, to isolate the replication data traffic in the ESXi hosts, dedicate a VMkernel interface for that. By default, ESXi handles the replication data traffic through its management VMkernel interface. Since one VMkernel adapter must handle one traffic type, separate the management traffic from the replication traffic by creating a dedicated replication VMkernel interface.

In every ESXi host that is used as a replication source or as a replication destination, when creating a VMkernel interface dedicated for the replication traffic, use the following tags:

- For replication sources, to configure each ESXi host for the outgoing replication traffic, select `vSphere Replication`. For more information, see *Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host* in the *vSphere Replication* documentation.
- For replication destinations, to configure each ESXi host for the incoming replication traffic, select `vSphere Replication NFC`.

To keep the replication traffic between the ESXi hosts and the appliance instances in the same broadcast domain, configure the dedicated replication VMkernel interface in its own IP subnet and connect each appliance instance to the same virtual port group. As a result, the uncompressed replication traffic avoids crossing a router and saves network bandwidth.

## Deploy both appliances for vSphere DR and migration

By using the vSphere Client, in providers vCenter Server instances, deploy vCenter Replication Management Appliance and optionally, deploy one or more Replicator Appliance instances. Similarly, in tenants vCenter Server instances, deploy On-Premises to Cloud vCenter Replication Appliance by using the OVA files for each appliance.

- Verify that the disaster recovery environment in each site meets the deployment requirements. For information about each appliance prerequisites, see [Deployment architecture and requirements for vSphere DR and migration](#).
- Download the installation files, containing the binaries for the two appliances.
  - To deploy the provider appliances, download the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build-sha_OVF10.ova` file.
  - To deploy the tenant On-Premises to Cloud vCenter Replication Appliance, download the `VMware-Cloud-Director-Availability-On-Premises-release.number.xxxxxxx-build-sha_OVF10.ova` file.

Deploy two VMware Cloud Director Availability appliances, depending on the desired topology and on the available licensing:

- For replicating workloads between a provider vCenter Server instance and a tenant vCenter Server instance:
  - In the provider vCenter Server, deploy and license one vCenter Replication Management Appliance, and optionally, one or more Replicator Appliance instances.
  - In the tenant vCenter Server, deploy one On-Premises to Cloud vCenter Replication Appliance.
- Alternatively, for replicating workloads between provider vCenter Server instances, deploy and license one vCenter Replication Management Appliance in each provider vCenter Server instance, and optionally, one or more Replicator Appliance instances in each provider site.
- In a provider vCenter Server instance, deploy a vCenter Replication Management Appliance, and optionally, repeat this step and deploy one or more Replicator Appliance instances.
  - a) Log in to the provider vCenter Server instance by using the vSphere Client and authenticate as a `vSphereadministrator` user.
  - b) Navigate to a target object where you want to deploy the provider appliances.  
As a target object you can use: a data center, a folder, a cluster, a resource pool, or a host.
  - c) Right-click the target object and from the drop-down menu select **Deploy OVF Template**.  
The **Deploy OVF Template** wizard opens. The following steps depend on the vSphere version that you use.

- d) On the **Select an OVF template** page, browse to the downloaded file location and click **Next**.
- e) On the **Select a name and folder** page, enter a name for the cloud on-premises appliance, select its deployment location, and click **Next**.
- f) On the **Select a compute resource** page, select a host, or cluster as a destination compute resource for running the appliance on, and click **Next**.
- g) On the **Review details** page, verify that the selected template details are correct and click **Next**.
- h) On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.
- i) On the **Configuration** page, select the deployment configuration for the appliance type and click **Next**.
  - To deploy the all-in-one provider appliance, select **vCenter Replication Management Appliance**. This appliance contains all services required for replication, including one Replicator Service instance.
  - Optionally, to deploy an additional Replicator Service instance, select **Replicator Appliance**. To scale the replication performance, deploy multiple Replicator Service instances. For more information, see [Add an additional Replicator Appliance instance for vSphere DR and migration](#).

Once selected, the appliance role changes only by redeploying the appliance.

- j) On the **Select storage** page, select the virtual disk format and the storage policy for the appliance and click **Next**.
- k) On the **Select networks** page, optionally configure the network settings and click **Next**.

For information about configuring the network settings after the deployment is complete, see the *Administration Guide*.

- l) On the **Customize template** page, customize the deployment properties of the appliance and click **Next**.

Root Password	Enter and confirm the initial password for the appliance <b>root</b> user. Later, when logging in for the first time as the <b>root</b> user, the appliance requires changing this initial password.
NTP Server	Enter an NTP server hostname or IP address.  <b>IMPORTANT</b> In the disaster recovery environment, ensure that both vCenter Server instances in the source and in the destination, the ESXi hosts, and the VMware Cloud Director Availability appliances all use the same NTP server.
Hostname	Enter the appliance hostname. Leave blank if DHCP is desired.
Address	Enter the IP address of the appliance. Leave blank if DHCP is desired. Ensure that the IP is in the CIDR notation, for example, enter <code>192.168.0.222/24</code> . Otherwise, the boot-up sequence shows an error and <code>127.0.0.1</code> as the IP address.
Gateway	Enter the gateway of the appliance network. Leave blank if DHCP is desired.
MTU	Enter the maximum transmission unit of the network. Leave blank if DHCP is desired.
DNS servers	Enter DNS servers for the appliance network. Leave blank if DHCP is desired.
Search domains	Enter the search domains for the appliance network. Leave blank if DHCP is desired.

m) On the **Ready to complete** page, review the settings and begin the installation process by clicking **Finish**.

The **Recent Tasks** pane shows a new task for initializing the provider appliance deployment. After the task is complete, the new appliance is created in the selected vCenter Server resource.

- In a tenant vCenter Server instance, deploy an On-Premises to Cloud vCenter Replication Appliance.
  - a) Log in to the tenant vCenter Server instance by using the vSphere Client and authenticate as a **vSphereadministrator** user.
  - b) Repeat the previous steps for deploying the On-Premises to Cloud vCenter Replication Appliance.
  - c) On the **Configuration** page, select the **On-Premise to Cloud vCenter Replication Appliance** deployment configuration as the appliance type, then complete the remaining wizard steps.

Once selected, the appliance role changes only by redeploying the appliance. For information about the alternative On-Premises to Cloud Director Replication Appliance role, see [Installing and configuring the On-Premises to Cloud Director Replication Appliance](#).

The **Recent Tasks** pane shows a new task for initializing the tenant appliance deployment. After the task is complete, the new appliance is created in the selected vCenter Server resource.

The appliances are deployed in each vCenter Server site and are ready for their initial configuration.

## Configure and pair both appliances for vSphere DR and migration

In their management interfaces, configure both appliances by first changing their initial root user password set during each appliance deployment. Then register each appliance with the local vCenter Server Lookup service in each site. Finally, pair the on-premises appliance with the provider site.

Verify that in both vCenter Server instances, each appliance is deployed and powered on. For information about the appliance requirements and deployment, see [Deploy both appliances for vSphere DR and migration](#).

1. Repeat the following steps for each appliance and configure both appliances.
2. In a Web browser, go to `https://Appliance-IP-address`.
3. Log in by using the **root** user password that you set during the OVA deployment.
4. If you log in to the appliance for the first time, you must change the initial **root** user password.
  - a) Enter the initial **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password.

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

- At least one lowercase letter.
- At least one uppercase letter.
- At least one number.
- At least one special character, such as & # %.

- c) Click **Apply**.

The **Getting Started** tab opens.

5. To configure this appliance for the first time, click **Run the initial setup wizard**.
6. In the **Initial Setup** window, configure the site name, the local vCenter Server Lookup service, and its credentials.

Option	Description
<b>Site name</b>	Enter a name for this site.  <b>IMPORTANT</b> This site name is used as an identifier and cannot be changed later without impacting the active replications.

Option	Description
<b>Lookup Service Address</b>	<p>Enter the IP address or the FQDN of the local vCenter Server Lookup service in this site and press Tab, auto-completing the address as <code>https://Lookup-Service-IP-or-FQDN:443/lookupservice/sdk</code>.</p> <p><b>NOTE</b> To use the VMware Cloud Director Availability vSphere Client Plug-In, go to the URL of the vSphere Client by using the same method - an IP address or an FQDN. Match the configuration in the <b>Lookup Service Address</b> text box.</p>
<b>SSO Admin Username</b>	<p>Enter the vSphere <b>administrator</b> single sign-on (SSO) user name for the vCenter Server Lookup service. This user must belong to the <b>ADMINISTRATORS</b> group.</p> <p><b>IMPORTANT</b> For all vSphere DR and migration workflows the principal is this user. That is, this user owns all replications, meaning all users that see the replication have full control over it.</p> <p>For information about the required vSphere privileges, see <a href="#">Users Roles Rights and Sessions</a> in the <i>Security Guide</i>.</p>
<b>Password</b>	Enter the vSphere <b>administrator</b> user password for the vCenter Server Lookup service.

- a) As **provider**, for the vCenter Replication Management Appliance, in the **License Key** text box, enter the VMware Cloud Director Availability license.  
When deploying On-Premises to Cloud vCenter Replication Appliance, skip this step as this appliance requires no licensing for operations.
  - b) To complete the initial setup, click **Apply**.
  - c) Verify the thumbprint and accept the SSL certificate of the local vCenter Server Lookup service in this site.  
This appliance is configured. Before pairing, repeat the above steps and similarly configure the remaining appliance until both appliances are configured and ready for pairing.
7. As **provider**, before allowing pairing, you must add each vCenter Replication Management Appliance instance for metering in vCloud Usage Meter.  
For information about adding the appliance instances in vCloud Usage Meter, see [vCloud Usage Meter Integration](#).  
On-Premises to Cloud vCenter Replication Appliance is not metered.
  8. After configuring both appliances, pair the On-Premises to Cloud vCenter Replication Appliance to the vCenter Replication Management Appliance.  
On-premises to provider pairing is managed only from the on-premises site. The On-Premises to Cloud vCenter Replication Appliance does not require a publicly available address for pairing to the provider.

**NOTE**

When pairing, depending on the appliance type you can pair:

- On-Premises to Cloud vCenter Replication Appliance instances to vCenter Replication Management Appliance in a single pairing step, initiated and completed from the on-premises site.
- vCenter Replication Management Appliance with another vCenter Replication Management Appliance instance. Then complete the pairing from the remote vCenter Replication Management Appliance.

Attempting to pair On-Premises to Cloud vCenter Replication Appliance with another On-Premises to Cloud vCenter Replication Appliance shows the following error message in the **New Pairing** window: Sites are not allowed to pair or start replication. Check site(s) licensing. However, the pairing remains visible and must be manually deleted from both sides. Attempting to create a replication between such paired on-premises sites gets prevented by an error checking the licensing of the sites.

- a) In the left pane, click **Peer Sites**.
- b) To complete the pairing with the provider, on the **Peer Sites** page, click **New pairing**.
- c) In the **New Pairing** window, enter the pairing details of the provider site then click **Pair**.

Public Service Endpoint	<ul style="list-style-type: none"> <li>Enter the address of the Public Public Service Endpoint: 443 of the vCenter Replication Management Appliance.</li> <li>Alternatively, enter port 8048 when both appliances reside in the same network.</li> </ul>
SSO Username	<p>Enter the user name of the single-sign-on user from the provider site for the pairing. For example, enter Administrator@vsphere.local.</p> <p>To pair the on-premises appliance with the provider site it is recommended to use a less-privileged user that belongs to the <b>VRUSERS</b> group in the provider site. Alternatively, you can still use a user member of the <b>VRADMINISTRATORS</b> or the <b>ADMINISTRATORS</b> groups in the provider site. For information about these groups, see <a href="#">Users Roles Rights and Sessions</a> in the <i>Security Guide</i>.</p>
SSO Password	Enter the password of the remote single-sign-on user in the provider site.
Description	Optionally, enter a description for this pair.

- d) Verify the thumbprint and accept the SSL certificate of the vCenter Replication Management Appliance.
- Both appliances paired with each other and are ready for replications.

After the vCenter Replication Management Appliance integrated with VMware vCloud® Usage Meter for metering, both vCenter Server sites are ready for replications between each other.

After adding the vCenter Replication Management Appliance in vCloud Usage Meter, you can now create and manage replications between both vCenter Server sites by accessing either of the following two interfaces:

- Log in to any of the two vCenter Server sites by using the vSphere Client and authenticating in one of the following ways, then access the VMware Cloud Director Availability vSphere Client Plug-In.

#### NOTE

Ensure that the user has sufficient privileges granted to see and interact with vSphere workloads.

- To authenticate as **tenant**, for pairing or replicating workloads, log in by using single sign-on user credentials that belong to the **VRUSERS** group that VMware Cloud Director Availability created by registering with the vCenter Server Lookup service.
- To authenticate a session with **administrator** privileges, log in by using single sign-on user credentials that belong to the **ADMINISTRATORS** or **VRADMINISTRATORS** groups.  
For example, the Administrator@vsphere.local single sign-on user is a member of the **ADMINISTRATORS** group.
- Any single sign-on users that do not belong to any of these three groups cannot authenticate.
- Alternatively, go to <https://Appliance-IP-address/ui/admin> of either of the newly paired VMware Cloud Director Availability appliances management interfaces and log in by using single sign-on user credentials that belong to the **ADMINISTRATORS** or **VRADMINISTRATORS** groups, or alternatively by using the password for the built-in **root** user of the appliances.

For information about accessing the appliances, creating and managing replications, and monitoring, see the *User Guide*.

## Add an additional Replicator Appliance instance for vSphere DR and migration

As **provider**, depending on the deployment requirements, you can add more Replicator Appliance instances to the vSphere DR and migration environment after configuring the vCenter Replication Management Appliance.

- Deploy one or more Replicator Appliance instances by using the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build-sha_OVF10.ova` file. For more information, see [Deploy both appliances for vSphere DR and migration](#).
- Verify that the vCenter Replication Management Appliance in the disaster recovery environment is already configured. For information about configuring the appliance, see [Configure and pair both appliances for vSphere DR and migration](#).

After configuring the vCenter Replication Management Appliance it provides all necessary services for vSphere DR and migration with a remote vCenter Server site. To further scale the replication performance, in addition to the Replicator Service instance that operates in the vCenter Replication Management Appliance, you can deploy one or more Replicator Appliance instances, each running one Replicator Service.

1. Log in to the service management interface of the vCenter Replication Management Appliance.
  - a) In a Web browser, go to `https://Replication-Management-Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the `root` or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Replicator Services**.
3. On the **Replicator Services administration** page, click **New**.
4. In the **New Local Replicator Service** window, enter the details for the new Replicator Service instance then click **Add**.
  - a) Enter the address and the `root` user password of the new Replicator Appliance then click **Test Connection**.
  - b) Verify and accept the SSL certificate of the new Replicator Service instance.
  - c) Enter the single-sign-on user credentials for the single sign-on domain in the local site.
  - d) Optionally, if you deployed multiple Replicator Appliance instances, to register the additional ones click **Add a Replicator Service instance** then repeat entering the configuration details for each one.

Option	Description
<b>Replicator API Service Endpoint</b>	Enter the IP address and port 8043 of the newly deployed Replicator Appliance instance.  For example, enter <code>https://Replicator-Appliance-IP-address:8043</code> .
<b>Replicator Service Root Password</b>	Enter the <code>root</code> user password for the new Replicator Appliance as set during the OVA deployment of the new appliance then click <b>Test Connection</b> .
<b>New Password</b>	If you did not log in to the new Replicator Appliance, you must now change the initial <code>root</code> user password:  Enter a new password for the <code>root</code> user of the new appliance.  The password that you enter must be a secured password with a minimum of eight characters and it must consist of: <ul style="list-style-type: none"> <li>• At least one lowercase letter.</li> <li>• At least one uppercase letter.</li> <li>• At least one number.</li> <li>• At least one special character, such as <code>&amp;</code> <code>#</code> <code>%</code>.</li> </ul>

Option	Description
<b>Confirm Password</b>	Confirm the new password for the <b>root</b> user of the new appliance, matching the above entry.
<b>SSO Username</b>	Enter a user with administrative privileges in the local site single sign-on domain. For example, enter <i>Administrator@VSPHERE.LOCAL</i> .  <b>NOTE</b> If you do not enter SSO credentials, the appliance uses the administrative credentials, provided during the local site configuration.
<b>SSO Password</b>	Enter the password for the single sign-on administrative user.
<b>Description</b>	Optionally, enter a description for the new Replicator Service instance you are registering.

On the **Replicator Services administration** page, you now see a green check status for the newly added Replicator Service instances.

5. Verify that the connectivity to the new Replicator Service instances is operational.
  - a) In the left pane under **System**, click **System Health**.
  - b) Under **Local Replicator Services**, verify that for the new Replicator Service instances **Service connectivity** shows a green check status.

The Replicator Service instances are added to the provider VMware Cloud Director Availability site. The paired sites automatically detect the new Replicator Appliance instances and automatically reconfigure to start using the new Replicator Service instances.

## Installing and configuring the On-Premises to Cloud Director Replication Appliance

To replicate vSphere workloads between an on-premises vCenter Server instance and a provider cloud site backed by VMware Cloud Director, in the tenant vCenter Server deploy a VMware Cloud Director Availability On-Premises Appliance instance and during deployment select the On-Premises to Cloud Director Replication Appliance role then pair it with the provider site.

- For on-premises replication with cloud sites backed by VMware Cloud Director, install and configure VMware Cloud Director Availability in the on-premises vCenter Server instance by following this current chapter.
- Alternatively, for vSphere DR and migration between vCenter Server sites, to install and configure VMware Cloud Director Availability as a new deployment see the [Installing and configuring the On-Premises to Cloud Director Replication Appliance](#) chapter.

## Deployment architecture for the On-Premises to Cloud Director Replication Appliance

To protect or migrate vSphere workloads between cloud sites and on-premises vCenter Server deploy one or multiple On-Premises to Cloud Director Replication Appliance instances. The following architecture diagram of the VMware Cloud Director Availability solution shows the protection direction to and from an on-premises site and a cloud site.

In an on-premises vCenter Server environment, every organization **Administrator** can protect or migrate on-premises workloads to and from a paired cloud site.

## **On-premises Appliance Deployment**

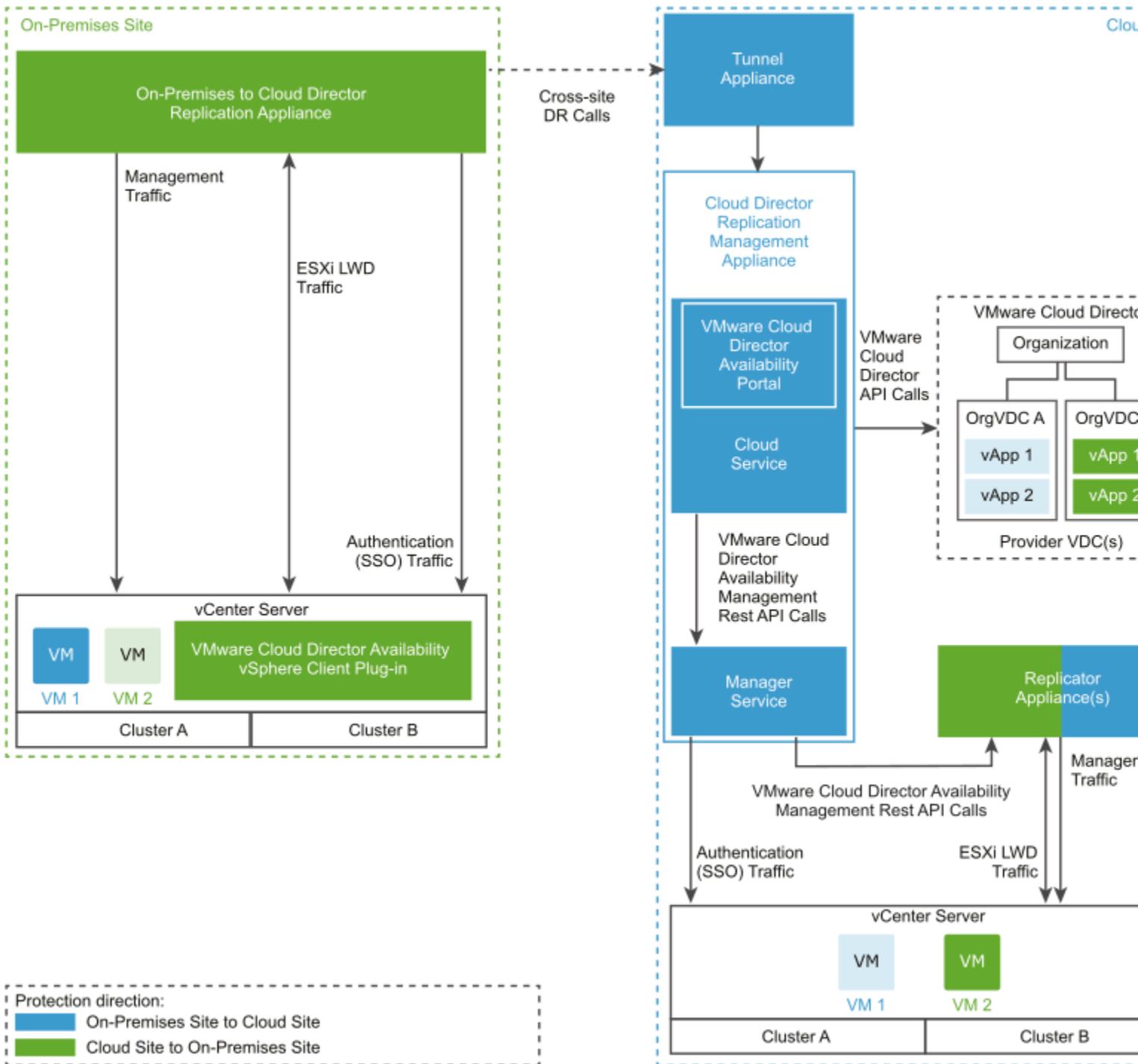
In the on-premises site, deploy and configure one or more On-Premises to Cloud Director Replication Appliance instances as a vSphere **Administrator** user. Internally, each on-premises appliance instance contains a Replicator Service and a Tunnel Service.

### **NOTE**

With more than one On-Premises to Cloud Director Replication Appliance instance paired with the same organization in the same cloud site, you see the number of replications, recent tasks, traffic, and disk usage of all the on-premises appliance instances paired with the cloud organization, similar to VMware Cloud Director.

In the diagram, the cells without color show the existing components in the on-premises environment. The colored cells show the VMware Cloud Director Availability services that deploy during the On-Premises to Cloud Director Replication Appliance installation and configuration procedures.

VMware Cloud Director Availability always initiates the network connection from the on-premises site to the cloud site.



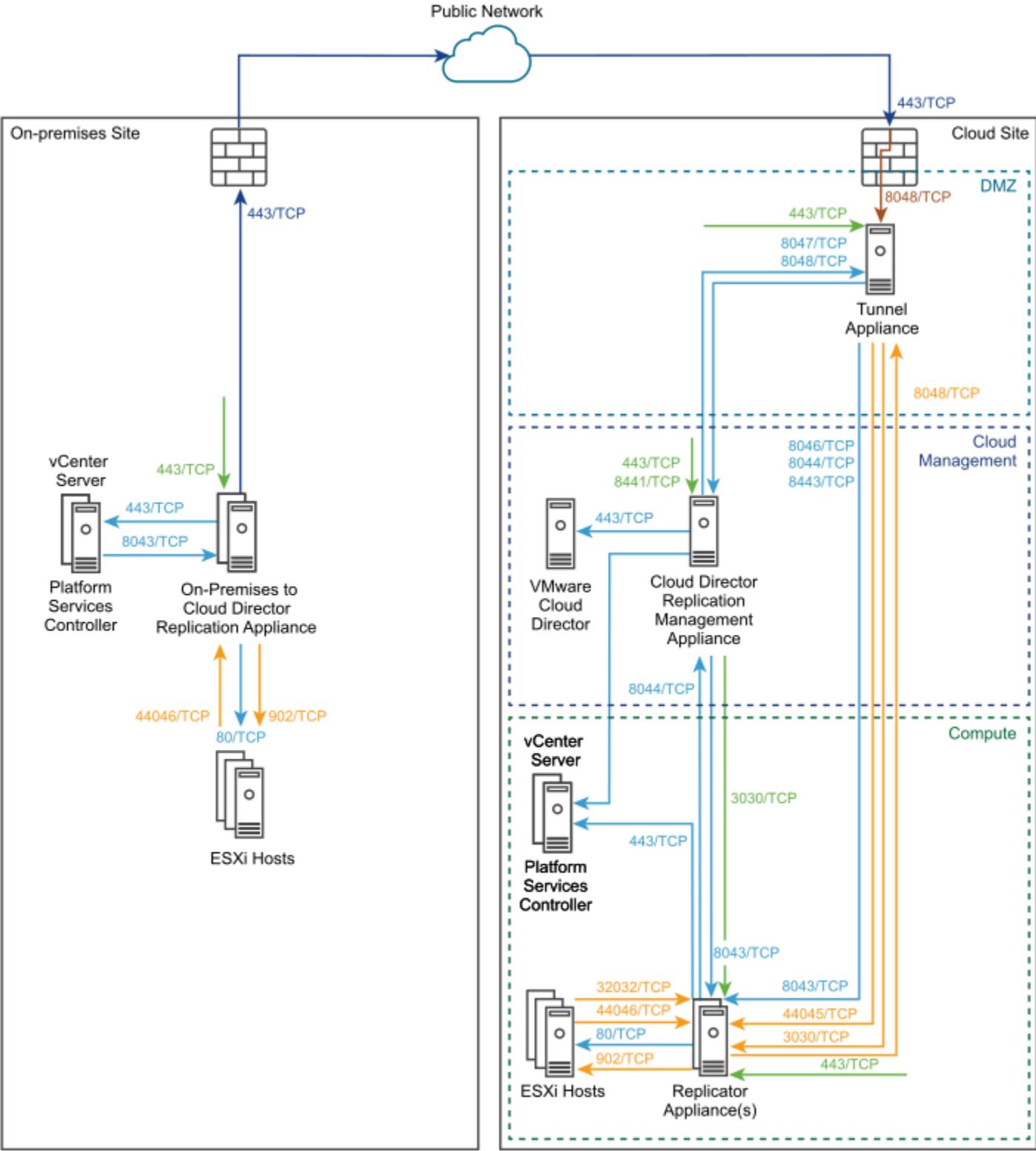
## Deployment requirements for the On-Premises to Cloud Director Replication Appliance

Before installing the On-Premises to Cloud Director Replication Appliance, verify that the on-premises site meets the deployment requirements. Also, allow the network communication within the on-premises site and to the cloud site.

## **Network Requirements**

To get a list of the required firewall ports to be opened, see [VMware Cloud Director Availability Network Ports](#).

The following diagram shows the direction of the data flow and the type of data traffic. The diagram also shows the required network ports for the communication between the On-Premises to Cloud Director Replication Appliance and the disaster recovery infrastructure.



- Traffic type:
- Replication data traffic
  - Administration traffic
  - VMware Cloud Director Availability service management traffic
  - ~~DNAT VMware Cloud Director Availability Service endpoint: 443 to Cloud Tunnel Appliance: 8048~~
  - Replication data traffic and VMware Cloud Director Availability service management traffic

## **Connectivity Requirements**

The VMware Cloud Director Availability appliances must be able to communicate with each other and with the disaster recovery infrastructure. The On-Premises to Cloud Director Replication Appliance must have a TCP access to the resource vCenter Server, where the resource vCenter Server Lookup service is hosted and to all the Replicator Appliance(s) in the cloud site.

### **NOTE**

VMware Cloud Director Availability uses end-to-end encryption for the communication across sites. For example, when the On-Premises to Cloud Director Replication Appliance is communicating to the Replicator Service in the cloud site, VMware Cloud Director Availability expects that the TLS session is terminated at both the On-Premises to Cloud Director Replication Appliance and the cloud site Replicator Service.

VMware Cloud Director Availability does not support any TLS terminating products or solutions placed between the appliances, for example, HAProxy, Nginx, Fortinet, and others. If such tools are in place, they must be configured in pass-thru mode, also known as TCP mode, to prevent from interfering with the TLS traffic of VMware Cloud Director Availability.

## **Hardware Requirements**

From a hosting perspective, the On-Premises to Cloud Director Replication Appliance is a virtual machine with the following hardware requirements since VMware Cloud Director Availability 4.5:

- 8 vCPUs
- 8 GB RAM
- 10 GB Storage

## **Deployment Requirements**

- In the ESXi hosts, a VMkernel interface can be dedicated for the replication traffic. By default, ESXi handles the replication traffic through its management VMkernel interface. As a good practice, you can separate the management traffic from the replication traffic by creating a dedicated replication VMkernel interface. Use the following tags when creating a VMkernel interface for the replication traffic:
  - Use the `vSphere Replication` tag to configure the ESXi host for the outgoing replication traffic.
  - Use the `vSphere Replication NFC` tag to configure the ESXi host for the incoming replication traffic.

Configure the replication VMkernel interface in its own IP subnet and connect the On-Premises to Cloud Director Replication Appliance to the same virtual port group. Using this configuration, the replication traffic between the ESXi hosts and the On-Premises to Cloud Director Replication Appliance stays in the same broadcast domain. As a result, uncompressed replication traffic avoids crossing a router and saves the network bandwidth. For information about configuring a dedicated replication VMkernel interface, see *Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host* in the vSphere Replication documentation.

- If more than one vCenter Server instances exist in the on-premises site:
  - vCenter Server instances dedicated for management operations
  - vCenter Server instances dedicated for resources

VMware Cloud Director Availability uses the resource vCenter Server instances to locate and authenticate to resources and create or edit inventory objects. Register the On-Premises to Cloud Director Replication Appliance with the vCenter Server Lookup service, provided by the Platform Services Controller used by the resource vCenter Server instances.

## **Deploying the On-Premises to Cloud Director Replication Appliance**

In an on-premises environment, use VMware Cloud Director Availability™ after deploying a On-Premises to Cloud Director Replication Appliance from a single OVA file, either by using the vSphere Client, or by using VMware OVF Tool.

The On-Premises to Cloud Director Replication Appliance comes as a preconfigured virtual machine that is optimized for running the VMware Cloud Director Availability services.

The appliance has a name in the form `VMware-Cloud-Director-Availability-On-Premises-x.x.x.xxxx-yyyyyyyy_OVF10.ova`, where `x.x.x` represents the product version and `yyyyyyyy` the build number.

#### NOTE

After deploying the appliance, for the first time only power it on from vSphere. Attempting to power it on for the first time from the ESXi user interface results in errors and that require redeploying the appliance from the scratch and powering it on from vSphere.

## Deploy the On-Premises to Cloud Director Replication Appliance by using the vSphere Client

In the vSphere Client, you can deploy the On-Premises to Cloud Director Replication Appliance by using a single `.ova` file.

- Download the `VMware-Cloud-Director-Availability-On-Premises-release.number.xxxxxx-build_sha_OVF10.ova` file, containing the binaries for the On-Premises to Cloud Director Replication Appliance.
  - If using vSphere Client earlier than version 6.5, install the Client Integration Plug-in to use **Deploy OVF Template** in the vSphere Web Client.
1. Log in to the vCenter Server by using the vSphere Client.
  2. Navigate to a target object where you want to deploy the On-Premises to Cloud Director Replication Appliance. As a target object you can use: a data center, a folder, a cluster, a resource pool, or a host.
  3. Right-click the target object and from the drop-down menu select **Deploy OVF Template**. The **Deploy OVF Template** wizard opens. The following steps depend on the vSphere version that you use.
  4. On the **Select an OVF template** page, browse to the `.ova` file location and click **Next**.
  5. On the **Select a name and folder** page, enter a name for the on-premises appliance, select a deployment location, and click **Next**.
  6. On the **Select a compute resource** page, select a host, or cluster as a compute resource to run the appliance on, and click **Next**.
  7. On the **Review details** page, verify the OVF template details and click **Next**.
  8. On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.
  9. On the **Configuration** page, select the **On-Premises to Cloud Director Replication Appliance** deployment configuration for the appliance type and click **Next**.  
Once selected, the appliance role changes only by redeploying the appliance. For information about the alternative On-Premises to Cloud vCenter Replication Appliance role, see [Installing and configuring both appliances for vSphere DR and migration](#).
  10. On the **Select storage** page, select the virtual disk format and the storage policy for the appliance and click **Next**.
  11. On the **Select networks** page, optionally configure the network settings and click **Next**.  
For more information about configuring the network settings after the deployment is complete, see *Network Settings Configuration* in the *Administration Guide* document.
  12. On the **Customize template** page, customize the deployment properties of the on-premises appliance and click **Next**.

Option	Description
Root Password	Enter and confirm the initial password for the <code>appliance:root</code> user.

Option	Description
	Later, when logging in for the first time as the <b>root</b> user, the appliance requires changing this initial password.
<b>NTP Server</b>	Enter an NTP server hostname or IP address.  <b>IMPORTANT</b> In the disaster recovery environment, ensure that both vCenter Server instances in the source and in the destination, the ESXi hosts, and the VMware Cloud Director Availability appliances all use the same NTP server.
<b>Hostname</b>	Enter the appliance hostname. Leave blank if DHCP is desired.
<b>Address</b>	Enter the IP address of the appliance. Leave blank if DHCP is desired.  Ensure that the IP is in the CIDR notation, for example, enter <i>192.168.0.222/24</i> . Otherwise, the boot-up sequence shows an error and <i>127.0.0.1</i> as the IP address.
<b>Gateway</b>	Enter the gateway of the appliance network. Leave blank if DHCP is desired.
<b>MTU</b>	Enter the maximum transmission unit of the network. Leave blank if DHCP is desired.
<b>DNS servers</b>	Enter DNS servers for the appliance network. Leave blank if DHCP is desired.
<b>Search domains</b>	Enter the search domains for the appliance network. Leave blank if DHCP is desired.

13. On the **Ready to complete** page, review the settings, and to begin the `.ova` installation process, click **Finish**.

The **Recent Tasks** pane shows a new task for initializing the `.ova` deployment. After the task is complete, the new appliance is created on the selected resource.

## Deploying by using the VMware OVF tool

To deploy VMware Cloud Director Availability by using the VMware OVF Tool, define deployment parameters and run a deployment script.

### Define the OVF tool parameters for appliance deployment

Before you deploy the VMware Cloud Director Availability appliances, you must define the specific VMware OVF Tool parameters for deployment.

The following table describes the parameters you must define when deploying the VMware Cloud Director Availability appliances by using the VMware OVF Tool scripts.

Parameter	Description
OVA	The local client path to the installation OVA package. For example, use <code>OVA="local_client_path/VMware-Cloud-Director-Availability-Deployment-release.number-xxxx-build_number_OVF10.ova"</code> , where <i>Deployment</i> is <code>Provider</code> or <code>On-Premises</code> .
VMNAME	Virtual machine name.
VSPHERE_DATASTORE	The <code>VSPHERE_DATASTORE</code> value is the datastore name as it is displayed in the .

Parameter	Description
VSPHERE_NETWORK	The name of the network on which the appliance to run.
VSPHERE_ADDRESS	The IP address of the vCenter Server instance on which you deploy the appliance.
VSPHERE_USER	User name for a vCenter Server administrator.
VSPHERE_USER_PASSWORD	Password for a vCenter Server administrator.
VSPHERE_LOCATOR	<p>The VSPHERE_LOCATOR value contains the target data center name, the tag <i>host</i>, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The VSPHERE_LOCATOR value depends on the topology of your vSphere environment. Following are examples for valid VSPHERE_LOCATOR values.</p> <ul style="list-style-type: none"> <li><code>/data-center-name/host/cluster-1-name/ESXi-host-fully-qualified-domain-name</code></li> <li><code>/data-center-name/host/cluster-2-name/ESXi-host-IP-address</code></li> </ul> <p>If the target ESXi host is not part of a cluster, skip the <i>cluster-name</i> element, as shown in the following examples.</p> <ul style="list-style-type: none"> <li><code>/data-center-name/host/ESXi-host-fully-qualified-domain-name</code></li> <li><code>/data-center-name/host/ESXi-host-IP-address</code></li> </ul> <p>For more information about the VSPHERE_LOCATOR value, run the <code>./ovftool --help locators</code> command.</p>

## Deploy the On-Premises to Cloud Director Replication Appliance by using the OVF tool

In the VMware OVF Tool console, you can deploy a On-Premises to Cloud Director Replication Appliance by using a single `.OVA` installation file. You define deployment parameters in the OVF Tool console and run the deployment script.

- Download the `VMware-Cloud-Director-Availability-On-Premises-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the On-Premises to Cloud Director Replication Appliance.
- Verify that the VMware OVF Tool is installed and configured. For more information, see <https://code.vmware.com/tool/ovf>.
- Before running the deployment command, see [Deployment requirements for the On-Premises to Cloud Director Replication Appliance](#).

- Log in to a server where the OVF Tool is running, by using a Secure Shell (SSH) client.
- Define deployment parameters in the OVF Tool console by running the following commands.

```
# VMNAME="Name-to-be-Assigned-to-the-VM"

# VSPHERE_DATASTORE="vSphere-datastore"

# VSPHERE_NETWORK="VM-Network"

# ova="local_client_path/VMware-Cloud-Director-Availability-On-Premises-release_number-xxx-build_number_OVF10.ova"

# VSPHERE_USER="vCenter-Server-admin-user"

# VSPHERE_USER_PASSWORD="vCenter-Server-admin-user-password"

# VSPHERE_ADDRESS="vCenter-Server-IP-address"

# VSPHERE_LOCATOR="vSphere-locator"
```

### 3. Deploy the On-Premises to Cloud Director Replication Appliance.

The following example script deploys a On-Premises to Cloud Director Replication Appliance and sets a static IP address.

```
# echo $VMNAME

#./ovftool/ovftool --name="${VMNAME}" --datastore="${VSPHERE_DATASTORE}" --acceptAllEulas
--powerOn --X:enableHiddenProperties --X:injectOvfEnv --X:waitForIp
--ipAllocationPolicy=fixedPolicy --machineOutput --noSSLVerify
--overwrite --powerOffTarget "--net:VM Network=${VSPHERE_NETWORK}" --diskMode=thin
--prop:guestinfo.cis.appliance.root.password='Your-Root-Password'
--prop:guestinfo.cis.appliance.ssh.enabled=True
--prop:guestinfo.cis.appliance.net.ntp='Your-NTP-Servers-IP-Addresses (comma-separated) '
--prop:net.hostname='Appliance-Hostname'
--prop:net.address='IP-In-CIDR-Notation'
--prop:net.gateway='Your-Gateway-IP'
--prop:net.mtu='Your-MTU'
--prop:net.dnsServers='Your-DNS-Servers-IP-Addresses (comma-separated) '
--prop:net.searchDomains='Your-DNS-Search-Domains (comma-separated) '
"${OVA}" "vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"
```

The console outputs the IP address of the On-Premises to Cloud Director Replication Appliance.

## Configuring the On-Premises to Cloud Director Replication Appliance

After deploying the On-Premises to Cloud Director Replication Appliance, to enable pairing, you must first configure the appliance. To perform the initial configuration, navigate to the management interface of the on-premises appliance.

### Configure the On-Premises to Cloud Director Replication Appliance

To configure the On-Premises to Cloud Director Replication Appliance by using the appliance management interface, you must first change the initial **root** user password that you set during the OVA deployment. Then you register the on-premises appliance with the vCenter Server Lookup service.

- Verify that the On-Premises to Cloud Director Replication Appliance is installed and powered on. For more information, see [Deploying the On-Premises to Cloud Director Replication Appliance](#).
- Verify that the cloud provider enabled the replication policy for your organization.
- Verify that the Public Service Endpoint address from the cloud provider is obtained.

1. In a Web browser, go to `https://On-Prem-Appliance-IP-address`.
2. Log in by using the **root** user password that you set during the OVA deployment.
3. If you log in to the appliance for the first time, you must change the initial **root** user password.
  - a) Enter the initial **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password.

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

- At least one lowercase letter.
  - At least one uppercase letter.
  - At least one number.
  - At least one special character, such as `&` `#` `%`.
- c) Click **Apply**.  
The **Getting Started** tab opens.

4. Click **Pair now**.  
The **New Cloud Pairing** wizard opens.
5. On the **Site Details** page, enter a name that identifies this on-premises site to the cloud provider and click **Next**.

Option	Description
<b>Site name</b>	Enter a name for the on-premises site.  <b>IMPORTANT</b> This site name is used as an identifier and cannot be changed later without impacting the active replications.
<b>Description</b>	Optionally, enter a description for this on-premises site that identifies it to the cloud provider.

6. On the **Lookup Service** page, enter the connection details for the vCenter Server Lookup service.

Option	Description
<b>Lookup Service Address</b>	Enter the IP address or the FQDN of the vCenter Server Lookup service and press Tab, auto-completing the address as <code>https://Lookup-Service-IP-or-FQDN:443/lookupservice/sdk</code> .  <b>NOTE</b> To use the VMware Cloud Director Availability vSphere Client Plug-In without errors, when going to the URL of the on-premises vSphere Client, use the same method - an IP address or an FQDN. Match the configuration in the <b>Lookup Service Address</b> text box.
<b>SSO Admin Username</b>	Enter the <i>single sign-on</i> user name for the vCenter Server Lookup service.
<b>Password</b>	Enter the <i>single sign-on</i> user password for the vCenter Server Lookup service.

- a) To establish a connection with the vCenter Server Lookup service, click **Next**.
- b) Verify the thumbprint and accept the SSL certificate of the vCenter Server Lookup service.
7. On the **Cloud Service Details** page, pair the On-Premises to Cloud Director Replication Appliance with the cloud provider and click **Next**.

Option	Description
<b>Public Service Endpoint address</b>	Enter the address of the cloud site Public Service Endpoint: 443 as given by the provider and press Tab, auto-completing the address as <code>https://Public Service Endpoint-IP-or-FQDN</code>
<b>Authorization type</b>	When using token authentication for VMware Cloud Director, select <b>VCD API Token</b> .  Alternatively, when using local users in VMware Cloud Director, select <b>VCD Local User (DEPRECATED)</b>
	In the <b>Organization</b> text box, enter the name of the organization.  In the <b>Organization Admin</b> text box, enter the user name of a VMware Cloud Director <b>organization administrator</b> user. For example, enter <code>admin1@org</code> .

Option	Description	
	In the <b>VCD API Token</b> text box, paste the token from VMware Cloud Director. Once used for pairing, the token is not stored and can be revoked at any time. For more information, see <a href="#">Generate an API access token for pairing from VMware Cloud Director</a> .	In the <b>Organization Password</b> text box, enter the <i>password</i> of the VMware Cloud Director <b>organization administrator</b> user.
Allow access from Cloud	<p><b>Activated access from the cloud site:</b></p> <p>Allows privileged VMware Cloud Director users like the cloud provider and the organization administrators without authenticating to the on-premises site to perform operations from the VMware Cloud Director Availability Tenant Portal.</p> <ul style="list-style-type: none"> <li>• Browse and discover on-premises workloads to replicate them to the cloud site.</li> <li>• Reverse existing replications from the cloud site to the on-premises site.</li> <li>• Replicate cloud site workloads to the on-premises site.</li> </ul> <p><b>Deactivated cloud site access:</b></p> <ul style="list-style-type: none"> <li>• Configuring a new replication requires users to explicitly authenticate to the on-premises VMware Cloud Director Availability Tenant Portal.</li> <li>• Cannot reverse existing replications to the on-premises site.</li> <li>• Allows privileged VMware Cloud Director users to modify existing replications and perform migrate or failover.</li> </ul>	
Allow log collection from Cloud	<ul style="list-style-type: none"> <li>• To simplify troubleshooting, activate log collection from the cloud site. This allows the cloud provider and the organization administrators without authenticating to each paired on-premises appliance to obtain its logs.</li> <li>• Leave cloud site log collection deactivated to require authenticating to the on-premises appliance management interface for downloading the on-premises appliance logs.</li> </ul>	

If the cloud site does not use a valid CA-signed certificate, verify the thumbprint and accept the SSL certificate of the Public Service Endpoint.

- On the **Ready To Complete** page, optionally, configure the on-premises local placement, and to complete the wizard click **Finish**.
  - You can now configure on-premises to cloud replications and you can leave the **Configure local placement now** toggle deactivated.
  - To enable the cloud to on-premises replications now by configuring the local placement, activate the **Configure local placement now** toggle.

If you skipped configuring local placement in the last step of the wizard, you can proceed with [Configure local placement for the On-Premises to Cloud Director Replication Appliance](#).

## Configure local placement for the On-Premises to Cloud Director Replication Appliance

To enable replications from the cloud to the on-premises site, in the on-premises appliance you must configure the local placement settings.

Follow this procedure only if you skipped **Configure local placement now** during the initial setup wizard of the On-Premises to Cloud Director Replication Appliance. If configuring On-Premises to Cloud vCenter Replication Appliance skip this chapter and see [Installing and configuring both appliances for vSphere DR and migration](#).

**NOTE**

When using replication seed, the datastores of the seed disks are reused and the network connections of the original virtual machine are reapplied.

1. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
  - a) In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
  - b) Log in as the **root** user.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Site settings**, next to **Placement to newly recovered VMs on this site** click **Edit**.
4. Complete the **Configure Placement** wizard.
  - a) On the **VM Folder** page, select the destination location for storing the recovered virtual machines and click **Next**.
  - b) On the **Compute Resource** page, select the destination compute resource for the recovered virtual machines and click **Next**.
  - c) On the **Default Network** page, optionally select the default network that the virtual machines automatically connect to after their failover and click **Next**.  
 If you skip selecting a default network, the incoming virtual machine replications are recovered with their NIC adapters disconnected. The supported networks types are: standard networks, distributed port groups, and NSX networks (opaque networks).
  - d) On the **Datastore** page, select the datastore in which to store the replicated virtual machines and their disk files and click **Next**.  
 Datastore clusters are not supported for the on-premises local placement and the clusters do not show for selection.
  - e) On the **Ready To Complete** page, verify that the selected placement configuration is correct and click **Finish**.

The **Placement to newly recovered VMs on this site** section expands, showing the placement configuration. You can start creating and managing replications from the on-premises site by accessing one of the interfaces:

- Log in to the on-premises vCenter Server instance by using vSphere Client, authenticate with the single sign-on **administrator** credentials then access the VMware Cloud Director Availability vSphere Client Plug-In. For more information, see the *User Guide* document.
- Navigate to the Public Service Endpoint of the cloud site and log in by using VMware Cloud Director **organization administrator** credentials.

## Upgrading on-premises and provider site

Follow the upgrade path and choose an upgrade method for the currently installed VMware Cloud Director Availability version. Follow the **prerequisites** and take both a back up and a snapshot, then choose a source repository for the upgrade files and perform the upgrade.

## Upgrade Paths

For on-premises site upgrade to the latest version, use the following upgrade methods, according to the currently installed version.

Current Version	Next Version	Upgrade Method
4.5.x or 4.6.x	4.7.x	<p><b>IMPORTANT</b> Before starting the upgrade:</p> <ul style="list-style-type: none"> <li>• Verify that you take <b>snapshots</b> of all appliances while powered off.</li> <li>• <b>Back up</b> each appliance in the site. For more information, see <a href="#">Back up the appliance</a>.</li> </ul> <ul style="list-style-type: none"> <li>• You can upgrade by using the appliance management interface, see the updated <a href="#">Management interface upgrading</a> procedures.</li> <li>• Alternatively, you can upgrade by using the command-line interface, see the updated <a href="#">Command-line upgrading</a> procedures.</li> </ul>
4.4.x or 4.5.x	4.6.x	
4.3.x or 4.4.x	4.5.x	
4.2.x or 4.3.x	4.4.x	
4.0.x or 4.1.x	4.2.1	
3.0.x or 3.5.x	4.0	<ul style="list-style-type: none"> <li>• You can upgrade by using the appliance management interface, see the legacy <a href="#">Management Interface Upgrading</a> procedures.</li> <li>• Alternatively, you can upgrade by using the command-line interface, see the legacy <a href="#">Command-Line Upgrading</a> procedures.</li> </ul>
3.0	4.0	You must upgrade only by using the command-line interface, see the legacy <a href="#">Command-Line Upgrading On-Premises</a> procedures.

## NOTE

### Interoperability with paired peer sites running earlier VMware Cloud Director Availability versions:

For information about interoperability between paired sites that run mismatching versions of VMware Cloud Director Availability, see [Paired sites versions interoperability](#).

- For the On-Premises to Cloud Director Replication Appliance, once you back it up and take a snapshot, before starting the upgrade:
  - Ensure that you have not manually enabled the Photon repository of the appliance.  
To verify for enabled repositories, open an SSH connection to the appliance, log in by using the **root** user credentials and run the following command:
 

```
yum -v repolist all | grep enabled
```

 When no repository is active, the command returns no result and you can proceed with the upgrade.
  - Ensure that you have not installed any packages or third-party software or made any manual modifications of `yum` configuration files.
- To complete the upgrade sequence, see [Post-upgrade configuration](#).

## Upgrade Repository

To upgrade VMware Cloud Director Availability, you can configure the appliance to download the upgrade files from one of the following source repositories.

Repository	Description
<b>An ISO image</b>	Use an upgrade ISO file mounted in the virtual appliance CD-ROM drive for environments without an external Internet access.
<b>A specified repository</b>	<p>To upgrade multiple appliances or after deploying the appliances in different datastores, specify a repository as a content source:</p> <ul style="list-style-type: none"> <li>You can specify a local repository where you can upload the upgrade files, for environments where the network restricts the online Internet access to the appliances.</li> <li>Alternatively, with available Internet access, specify <code>https://packages-prod.broadcom.com/vca/v/4.7/</code> as an online upgrade repository.</li> </ul>

## Management interface upgrading

To upgrade VMware Cloud Director Availability, you can use the management interface of the appliance, select an upgrade repository, and follow the updated management interface upgrade procedures for the selected repository.

### Upgrade by using the default repository

In the appliance management interface, you can upgrade to the latest version by using the default VMware repository.

Verify that the appliance has an external Internet access to the VMware repository.

- Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
  - In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
  - Log in as the **root** user.
- In the left pane, click **Settings**.
- Under **Version**, next to **Product version** click **Check for updates**.
- To upgrade, complete the **Update** wizard.
  - On the **Repository** page, select **Use Official Online Repository** then click **Next**.
  - On the **Available updates** page, select the update then click **Next**.
  - On the **Release notes** page, read the notes for this version then click **Next**.
  - On the **EULA Review** page, to accept the end-user license agreement click **Next**.
  - On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.

The upgrade process starts. Wait for the installation process to finish.

#### NOTE

If you see either of the following messages, wait a few minutes before attempting to log back in:

`Timeout has occurred` or `Operation aborted due to an unexpected error`.

5. After the appliance restarts, verify that the upgrade is successful.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Open the upgrade log file.

```
less /var/log/upgrade.log
```

- c) When upgrading to version 4.6.x, verify that the upgrade log contains the following log entry near the end.

```
'Postupgrade to 4.6.x complete.'
```

Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: `[date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]"), $0 }' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit: run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as unit: run-re595c8a07fe845bbb87e6c36f866caf2.service`

The upgrade was successful! Scheduling reboot in 15 seconds.

After you upgrade the On-Premises to Cloud Director Replication Appliance, complete the upgrade with a post-upgrade configuration. For more information, see [Post-upgrade configuration](#).

## Upgrade by using a specified repository

In the appliance management interface, you can upgrade VMware Cloud Director Availability to the latest version by specifying an online or a local repository that contains the upgrade binaries.

Verify that the appliance has a network access to the specified repository.

1. If the network restricts the appliances online Internet access, prepare a local repository with the upgrade files.
  - a) To host the upgrade files inside the internal network, install and configure a local Web server.
  - b) Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.
  - c) To access the image file contents, mount the downloaded `.iso` file to a local computer.
  - d) Copy the `update` directory to the local Web server.

The `update` directory contains the manifest files and the `dnf` subdirectory.

2. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
  - a) In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
  - b) Log in as the **root** user.
3. In the left pane, click **Settings**.
4. Under **Version**, next to **Product version** click **Check for updates**.
5. Upgrade the appliance by completing the **Update** wizard.
  - a) On the **Repository** page, select **Use Specified Repository**.
  - b) On the **Repository URL** text box, specify the repository URL address then click **Next**.
    - If the appliance has Internet access, enter the following URL and specify the target version `https://packages-prod.broadcom.com/vcav/4.7/`.
    - Alternatively, enter the URL address of the local repository pointing to the `update/dnf` directory of the local Web server. For example, enter `http://local-Web-server-address/update/dnf`.
  - c) On the **Available updates** page, select an update then click **Next**.
  - d) On the **Release notes** page, read the notes for this version then click **Next**.
  - e) On the **EULA Review** page, to accept the end-user license agreement click **Next**.
  - f) On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.

The appliance automatically restarts.

6. After the appliance restarts, verify that the upgrade is successful.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Open the upgrade log file.
  - c) When upgrading to version 4.6.x, verify that the upgrade log contains the following log entry near the end.

```
'Postupgrade to 4.6.x complete.'
```

```
Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: [date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]"), $0 }' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit: run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as unit: run-re595c8a07fe845bbb87e6c36f866caf2.service
```

After you upgrade the On-Premises to Cloud Director Replication Appliance, complete the upgrade with a post-upgrade configuration. For more information, see [Post-upgrade configuration](#).

## Upgrade by using an ISO image file

In the appliance management interface, you can upgrade VMware Cloud Director Availability to the latest version by using an `.iso` file containing the upgrade binaries that you mount to the CD-ROM drive of the virtual appliance.

- Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.
1. Copy the `.iso` file to a datastore that is accessible from the vCenter Server instance that you use with VMware Cloud Director Availability.
  2. Mount the `.iso` file to the appliance.
    - a) Log in to the on-premises vCenter Server by using the vSphere Client.
    - b) Navigate to the virtual machine that hosts the VMware Cloud Director Availability appliance.
    - c) Right-click the virtual machine and select **Edit Settings**.
    - d) On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
    - e) Follow the prompts to add the CD/DVD drive to the VMware Cloud Director Availability virtual machine then select the **Connected** checkbox.
  3. By using the virtual appliance console, mount the `.iso` file inside the guest operating system of the appliance.
    - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
    - b) Mount the `.iso` file inside the guest operating system of the appliance.

```
mount /mnt/cdrom
```

4. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
  - a) In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
  - b) Log in as the **root** user.
5. In the left pane, click **Settings**.
6. Under **Version**, next to **Product version** click **Check for updates**.
7. Upgrade the appliance by completing the **Update** wizard.
  - a) On the **Repository** page, select **Use CDRM Updates** then click **Next**.  
If you skipped mounting the image, you see an error message: `Could not download the release manifest from file:///mnt/cdrom/update/rel-manifest.json`. To continue, perform step 3.
  - b) On the **Available updates** page, select an update then click **Next**.
  - c) On the **Release notes** page, read the notes for this version then click **Next**.
  - d) On the **EULA Review** page, to accept the end-user license agreement click **Next**.
  - e) On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.
8. After the upgrade finishes, verify that the upgrade is successful.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Open the upgrade log file.

```
less /var/log/upgrade.log
```

```
'Postupgrade to 4.6.x complete.'
```

Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: `[date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]"),`

```
$0 }' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit:  
run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as  
unit: run-re595c8a07fe845bbb87e6c36f866caf2.service
```

9. Unmount the `.iso` file.
  - a) In the vSphere Client, shut down the virtual machine that hosts the appliance.
  - b) Right-click the virtual machine and select **Edit Settings**.
  - c) In the **Virtual Hardware** tab, select **CD/DVD Drive** and uncheck the **Connected** and the **Connect At Power On** checkboxes.
  - d) Power on the virtual machine that hosts the appliance.

After you upgrade the On-Premises to Cloud Director Replication Appliance, complete the upgrade with a post-upgrade configuration. For more information, see [Post-upgrade configuration](#).

## Command-line upgrading

To upgrade VMware Cloud Director Availability by using the command-line interface of the appliance, select an upgrade repository, and follow the command-line procedures for the selected repository.

## Command-line upgrade by using an ISO image file

From the appliance command-line interface, you can upgrade VMware Cloud Director Availability to the latest version by using an `.iso` file containing the upgrade binaries that you mount to the CD-ROM drive of the virtual appliance.

- Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.
1. Copy the `.iso` file to a datastore that is accessible from the vCenter Server instance that you use with VMware Cloud Director Availability.
  2. Mount the `.iso` file to the appliance.
    - a) Log in to the vSphere Client in the site where you want to upgrade VMware Cloud Director Availability.
    - b) On the **Home** page, click **Hosts and Clusters**.
    - c) Right-click the virtual machine that hosts the appliance and select **Edit Settings**.
    - d) On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
    - e) Follow the prompts to add the CD/DVD drive to the VMware Cloud Director Availability virtual machine then select the **Connected** checkbox.
  3. Connect to the VMware Cloud Director Availability appliance by using a Secure Shell (SSH) client.
    - a) Open an SSH connection to `Appliance-IP-Address`.
    - b) Authenticate as the **root** user.
  4. Upgrade the appliance.

### NOTE

Proceed with the upgrade only after taking a snapshot of the appliance.

- a) Mount the `.iso` file inside the guest operating system.

```
mount /mnt/cdrom
```

- b) Review the end-user license agreement (EULA) and if you accept the EULA, press `q`.

```
python3 /mnt/cdrom/update/iso-upgrade.py eula | less
```

- c) Install the upgrade.

```
python3 /mnt/cdrom/update/iso-upgrade.py
```

After successfully completing, the upgrade outputs both in the console and in the `/var/log/upgrade.log` file:

```
[date-timestamp] Postupgrade to 4.6.x complete.
Nothing to do.
Loaded plugin: tdnfrepogpgcheck
```

- d) After the upgrade completes, restart the appliance.

```
reboot
```

After you upgrade the On-Premises to Cloud Director Replication Appliance, complete the upgrade with a post-upgrade configuration. For more information, see [Post-upgrade configuration](#).

## Post-upgrade configuration

After upgrading the appliance, complete the upgrade by reconfiguring the on-premises appliance with the vCenter Server Lookup service.

1. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.

- a) In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
- b) Log in as the **root** user.

2. Reconfigure the appliance with the vCenter Server Lookup service.

- a) In the left pane, click **Settings**.

To ensure that you load the upgraded management interface and to avoid the `The requested resource was not found` error message, clear the browser cache. You can press Ctrl+F5 or Ctrl+Shift+R (Cmd+Shift+R for Mac) or clear the cache in the browser settings.

- b) Under **Service endpoints** next to **Lookup Service Address**, click **Edit**.
- c) In the **Lookup Service Details** window, enter the single sign-on user name and password, and click **Apply**.

The appliance is successfully upgraded and you can configure new replications. For more information, see the *User Guide*.

# Installation, Configuration, and Upgrade Guide in the Cloud Director Site

---

The VMware Cloud Director Availability™ solution provides replication and failover capabilities for VMware Cloud Director™ and for vCenter Server workloads at both the virtual machine and at the vApp level.

VMware Cloud Director Availability is available through the Partner Connect Program. The solution provides multi-tenant workload recovery to cloud sites and to on-premises environments. VMware Cloud Director Availability provides:

- One cloud site supports multiple tenants. Each deployment can serve as both a replication source and as a recovery site. There are no dedicated source and destination sites.
- Replication management and monitoring from an on-premises site to a cloud site and reverse.
- Replication and recovery of vApps and virtual machines between VMware Cloud Director sites.
- Failback of recovered in the cloud workloads to the on-premises site.
- Migration of protected virtual machines in the cloud site back to the on-premises site.
- Self-service protection and failover workflows per virtual machine.
- Symmetrical replication flow that can be started from either the source or the recovery site.
- One single-site VMware Cloud Director Availability instance can migrate virtual machines and vApps between Virtual Data Centers belonging to one VMware Cloud Director organization.
- Multiple VMware Cloud Director Availability instances can coexist in one VMware Cloud Director.
- Built-in secure tunneling that requires no incoming allowed ports in the firewall in the on-premises site.
- The cloud site TCP tunneling allows for optional high availability of the incoming/outgoing traffic entry point.
- Built-in end-to-end TLS encryption of the replication traffic that is terminated at each Replicator Appliance instance.
- Optional compression of the replication traffic for reducing the network load on the disaster recovery infrastructure.
- VMware Cloud Director Availability vSphere Client Plug-In integration with the existing vSphere environment.
- Support for multiple vCenter Server and ESXi versions, including support for migrations from legacy versions.
- A single installation package, distributed as a Photon-based virtual appliance deploys each of the appliances of VMware Cloud Director Availability.

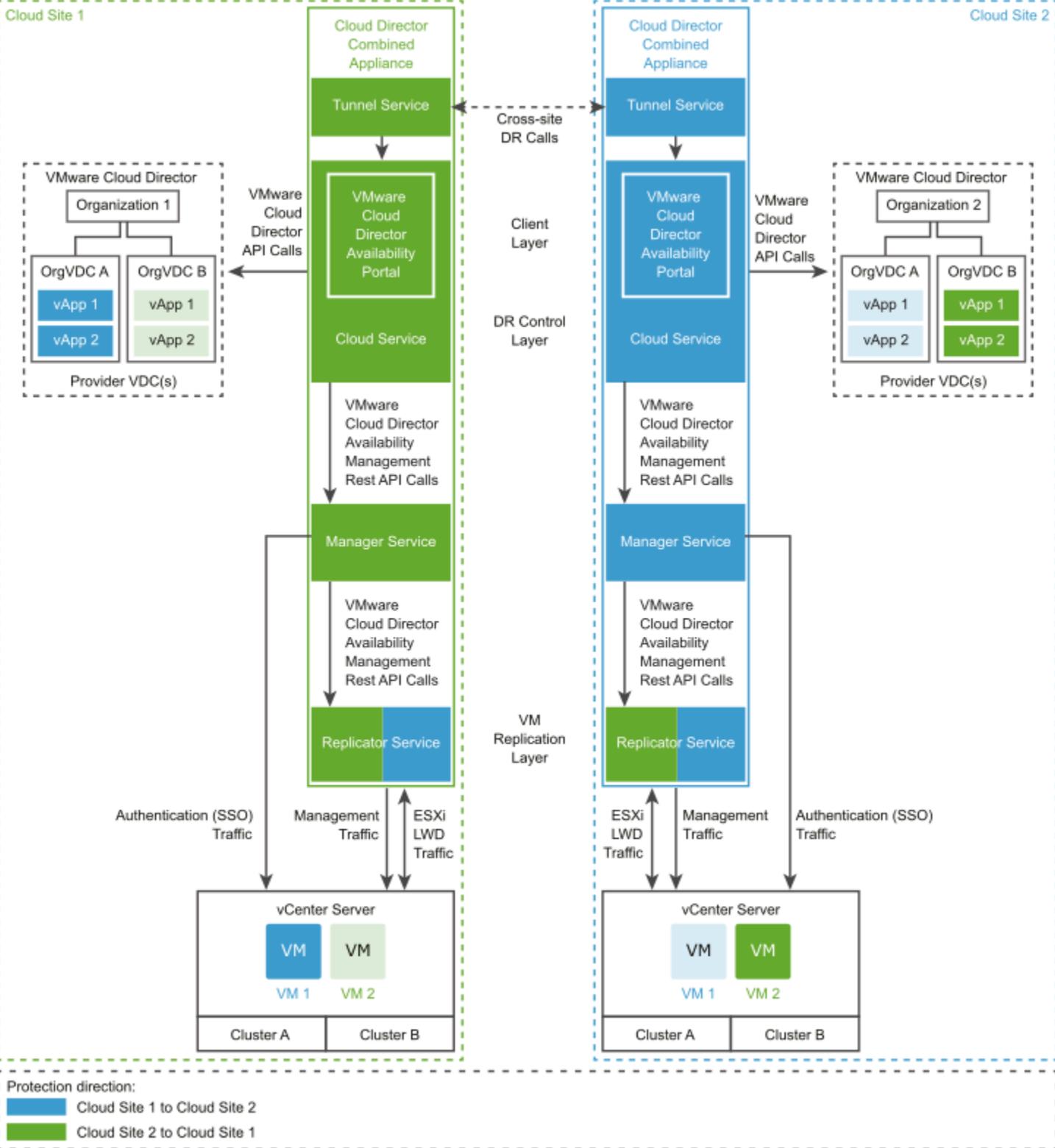
## Deployment architecture in the Cloud Director site

The cloud deployment architecture of VMware Cloud Director Availability relies on symmetrical replication operations between the two sites. Deploying multiple VMware Cloud Director Availability instances under one VMware Cloud Director™ site allows for granular access to multiple provider virtual data centers (VDCs), each representing a separate site.

### Test and Development Deployment

In a test or in a development VMware Cloud Director site, perform minimal deployment. In the test cloud site, one Cloud Director Combined Appliance runs all the four main services of VMware Cloud Director Availability:

- The Tunnel Service,
- The Manager Service,
- The Cloud Service,
- And the Replicator Service.



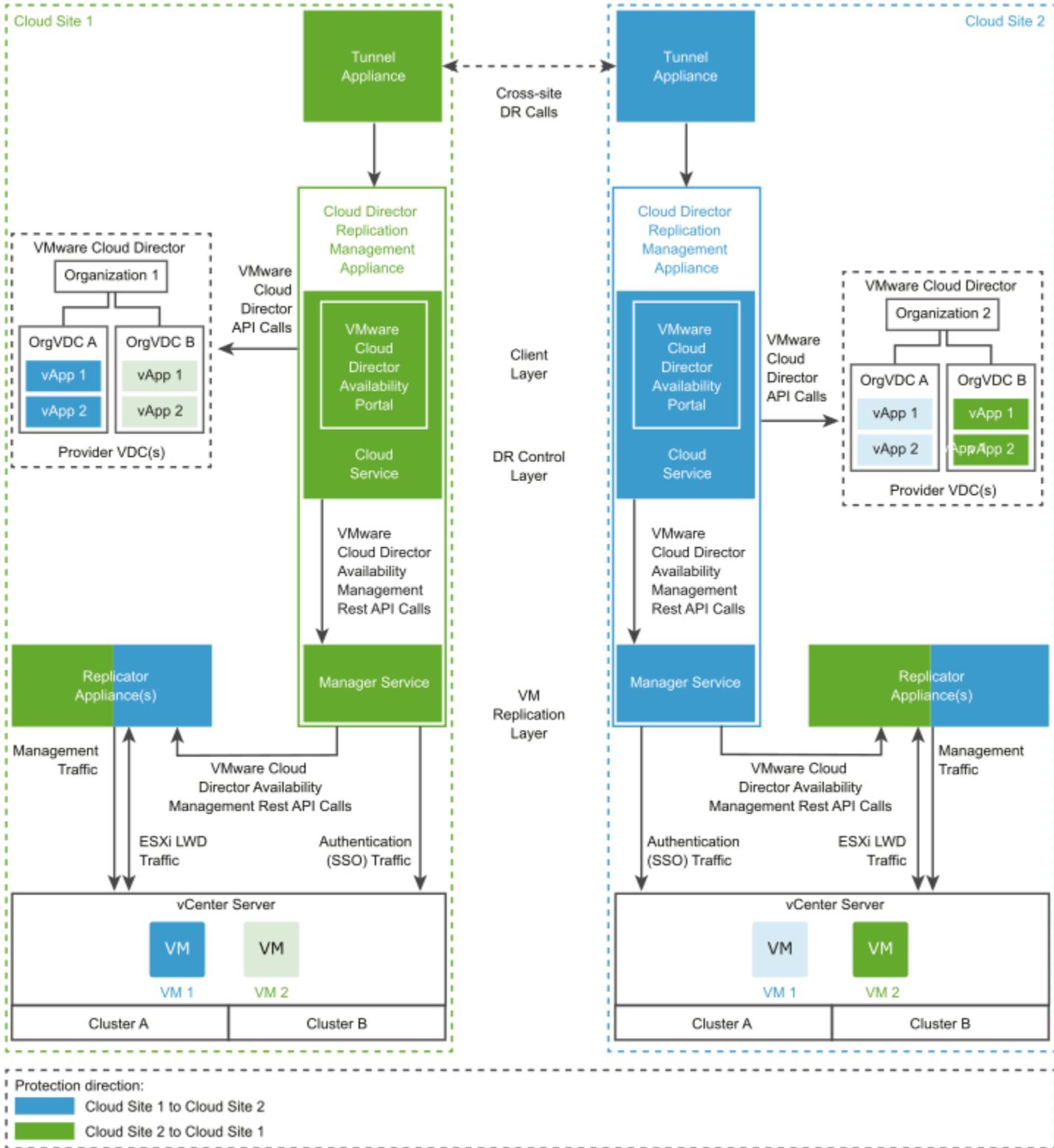
In the diagram:

- The colored components inside the two Cloud Director Combined Appliance instances represent the VMware Cloud Director Availability services, deployed during the installation and the initial configuration of the two appliances.
- Each component has the color of the replication direction it manages. For example, the protected Organization VDC B vApps and VM 2 from Cloud Site 1 to Cloud Site 2 use the Replicator Service from Cloud Site 2.
- Each replication resides in its destination site. For example, the protections from Cloud Site 1 to Cloud Site 2 reside in Cloud Site 2.
- The components with no color represent existing components in the two VMware Cloud Director sites.

### **Production Deployment**

In a production VMware Cloud Director site, deploy and configure one or more VMware Cloud Director Availability instances. A single VMware Cloud Director Availability instance consists of the following services, running on three or more dedicated appliances.

- One, or optionally for active-active high availability - two Tunnel Appliance instances, each running the Tunnel Service. For information about configuring Tunnel Appliance high availability (HA), see [Add a second Tunnel Appliance for HA in the Cloud Director site](#).
- One Cloud Director Replication Management Appliance, running the Cloud Service and the Manager Service. For information about the initial VMware Cloud Director Availability configuration, see [Configure the Cloud Service in the Cloud Director site](#).
- One, or optionally for performance scalability and capacity - multiple Replicator Appliance instances, each running a Replicator Service instance. For information about configuring multiple Replicator Service instances, see [Add an additional Replicator Service instance in the Cloud Director site](#).



---

For information about the network connectivity between the services and between the sites, see [Network requirements and prerequisites in the Cloud Director site](#). For information about each service of VMware Cloud Director Availability, see [Services](#).

### **Deploying Multiple VMware Cloud Director Availability Instances in VMware Cloud Director**

In a production cloud site, you can deploy one or multiple VMware Cloud Director Availability instances, distributed in provider VDCs under one VMware Cloud Director instance.

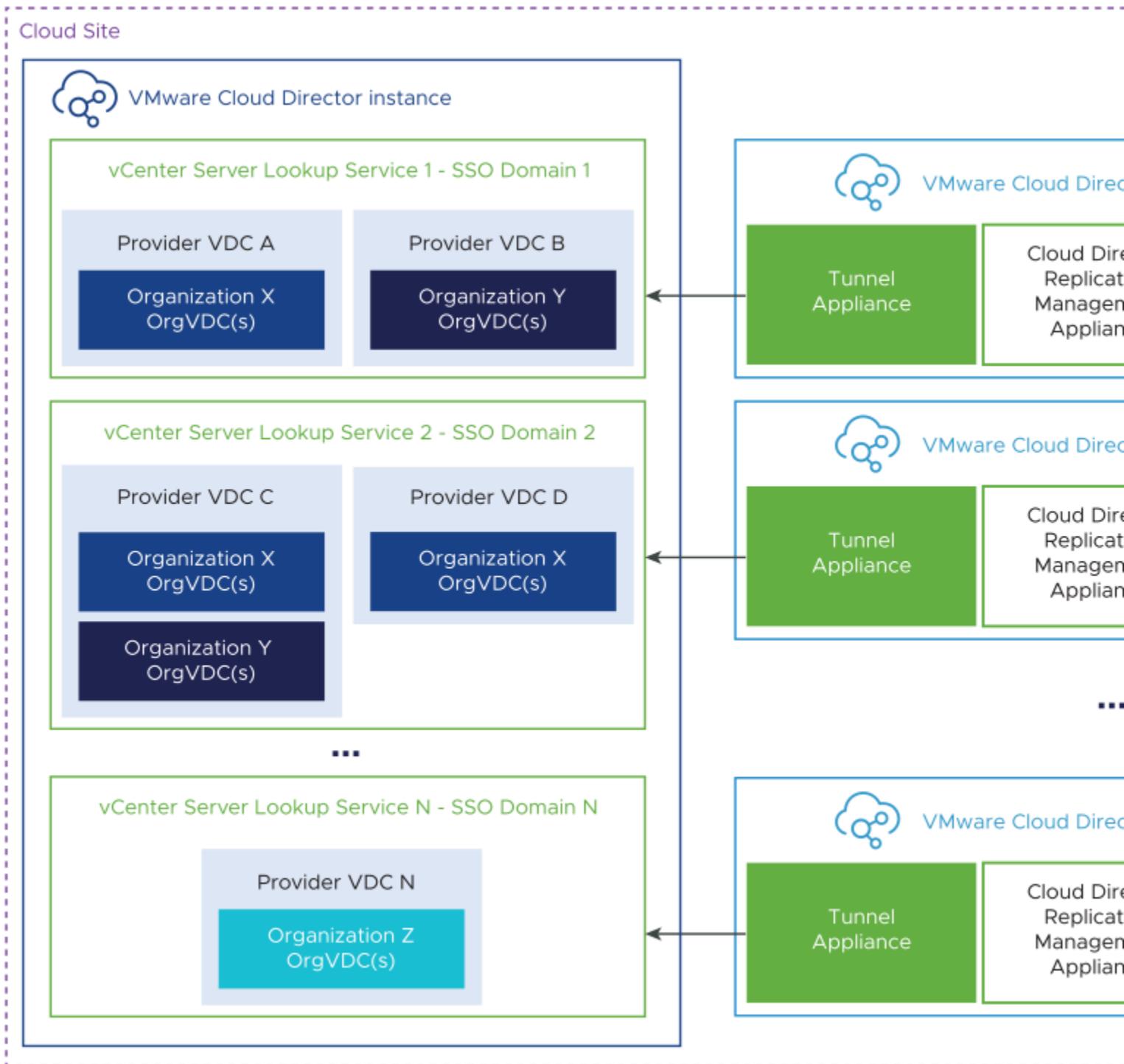
- In VMware Cloud Director Availability, each provider VDC represents a cloud site. In each VMware Cloud Director Availability instance, the service provider controls the accessible provider VDCs for that instance.

**NOTE**

A single VMware Cloud Director Availability instance must manage each provider VDC.

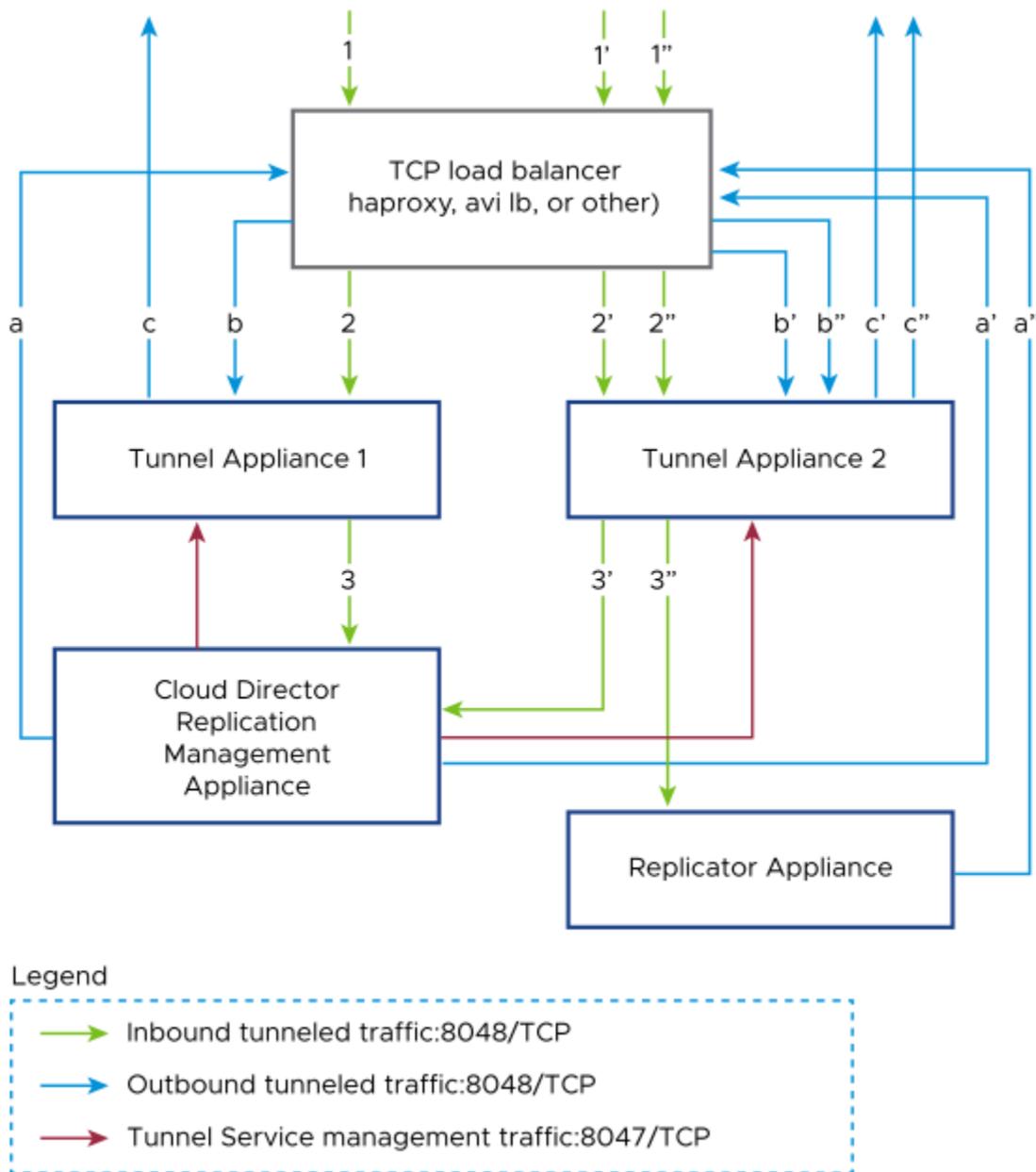
There must be no overlapping provider VDCs managed by multiple VMware Cloud Director Availability instances.

- One VMware Cloud Director instance manages all VMware Cloud Director Availability instances, for both a replication source or a replication destination. Each VMware Cloud Director Availability instance registers as a plug-in with its local site name in VMware Cloud Director.
- Each VMware Cloud Director Availability instance connects to one vCenter Server Lookup service for one single sign-on (SSO) domain and can access all the organization VDCs of the organizations, part of the provider VDC.



- In SSO domain 1, VMware Cloud Director Availability instance 1 connects to vCenter Server Lookup service 1 and can access the organization VDCs of Organizations X and Y, part of Provider VDC A and B, respectively.
- In SSO domain 2, VMware Cloud Director Availability instance 2 connects to vCenter Server Lookup service 2 and can access the organization VDCs of Organizations X and Y, part of Provider VDC C and the organization VDCs of Organization X, part of Provider VDC D.
- In SSO domain N, VMware Cloud Director Availability instance N connects to vCenter Server Lookup service N and can access the organization VDCs of Organization Z, part of Provider VDC N.

## Deploying Two Active-Active Tunnel Appliance Instances



In the above diagram, the three example network traffic flows, depending on their direction are marked as:

- **Incoming direction (green):**  
1, 1', 1''; 2, 2', 2''; 3, 3', 3''.
- **Outgoing direction (blue):**  
a, a', a''; b, b', b''; c, c', c''.

For high availability, the Tunnel Service supports active-active mode behind a provider-configured load balancer with no TLS termination nor TLS inspection, meaning two independent Tunnel Service instances running on two separate Tunnel Appliance instances, where both handle the network traffic to and from VMware Cloud Director Availability. The load

balancer distributes the traffic among them, ensuring one Tunnel Service is always accessible and responsive, even if the other one fails or becomes unavailable.

With the round robin algorithm, the load balancer without terminating the SSL traffic and without inspecting it distributes it among both active-active Tunnel Appliance instances, improving the Tunnel Service availability and performance by avoiding the impacts of one failing or its overload. Each Tunnel Service acts as both an ingress and an egress point of the VMware Cloud Director Availability network traffic. When configured behind a load balancer, both Tunnel Service instances run simultaneously and receive incoming requests from the load balancer then forward them to the remaining services of VMware Cloud Director Availability, and send outgoing responses from the remaining services back to the load balancer. For information about the connectivity between the services and TLS termination, see [VMware Cloud Director Availability Services Connectivity](#).

With this configuration, if one Tunnel Appliance fails, the other can continue serving the network requests. By using two Tunnel Appliance instances also increases the network scalability and capacity of the disaster recovery environment by using two independent points for all the network traffic that comes to and leaves VMware Cloud Director Availability.

After configuring VMware Cloud Director Availability in the Cloud Director site, you can configure the second Tunnel Service. For both existing installations and for upgraded ones, you can also follow the same procedure. For information about configuring the active-active mode for the Tunnel Appliance, see [Add a second Tunnel Appliance for HA in the Cloud Director site](#).

## Services

When deploying VMware Cloud Director Availability, by selecting the virtual appliance deployment type places the services of VMware Cloud Director Availability on dedicated cloud appliances, or on a combined appliance for testing purposes.

**Table 2: VMware Cloud Director Availability services**

Service Name	Service Description
Replicator Service	Exposes the low-level Host Based Replication (HBR) primitives as REST API calls.
Manager Service	A management service operating with vCenter Server-level concepts for managing the replication workflow.
Cloud Service with an embedded VMware Cloud Director Availability Tenant Portal	Provides the main interface for replication operations and operates with VMware Cloud Director-level concepts and works with vApps and virtual machines. The embedded VMware Cloud Director Availability Tenant Portal provides the tenants and the service providers of the VMware Cloud Director Availability Provider Portal with a graphic user interface to operate with VMware Cloud Director Availability.
Tunnel Service	The single point that channels all the site traffic: both management and replication data (LWD) traffic. Since VMware Cloud Director Availability 4.6, a second instance can be configured for Tunnel Service high availability. For more information, see <a href="#">Add a second Tunnel Appliance for HA in the Cloud Director site</a> .

For information about the VMware Cloud Director Availability appliances, see [Deployment requirements in the Cloud Director site](#).

Each service provides a dedicated service management interface for configuration and administration.

You perform an initial configuration by using the Manager Service, the Replicator Service, and the Cloud Service service management interfaces. After VMware Cloud Director Availability is deployed and configured, tenants can access the VMware Cloud Director Availability Tenant Portal. For information about the network connectivity between the services, see [Network requirements and prerequisites in the Cloud Director site](#) and for diagrams showing all services in the cloud

site and a diagram showing multiple VMware Cloud Director Availability instances, see [Deployment architecture in the Cloud Director site](#).

**Table 3: Replication services**

Service Name	Service Description
vSphere® Replication™ Service with vSphere Replication filter	The vSphere Replication Service, also called the HBR Service receives and records the delta information for each replicated workload. During a replication, only the delta information is sent from one ESXi host to another ESXi host.
Lightweight Delta Protocol Service (LWD Proxy)	A proprietary replication protocol service. Verifies that each incoming replication data stream comes only from the authorized source LWD Proxy instance. Also verifies that each outgoing replication data stream goes only to an authorized destination LWD Proxy instance.

**Table 4: External components**

Component Name	Component Description
VMware Cloud Director	Service providers can build secure, multi-tenant private clouds. Pools infrastructure resources into virtual data centers. Exposes them to tenant users through Web portals and programmatic interfaces as fully automated, catalog-based services.
Platform Services Controller	Provides common infrastructure services to the vSphere environment. Services include licensing, certificate management, and authentication with vCenter Server Single Sign-On.

For information on which VMware Cloud Director Availability appliance each service operates, see [Services and network ports](#) in the *Security Guide*.

## Installing and configuring the appliances in the Cloud Director site

As a **provider**, first deploy each of the VMware Cloud Director Availability appliances. Then perform an initial configuration of the Cloud Director Replication Management Appliance and register it with all the components in the disaster recovery infrastructure.

## Installation requirements and deployment prerequisites in the Cloud Director site

Before you start deploying and configuring the VMware Cloud Director Availability appliances, verify that your cloud site environment meets the specific requirements.

For information about the users and their permissions, see the [Users roles rights and sessions](#) in the *Security Guide*.

## Interoperability and vSphere product edition

Before deploying and pairing VMware Cloud Director Availability, first verify the interoperability between VMware Cloud Director Availability and ESXi, the vSphere product edition, and the other VMware products in the disaster recovery infrastructure, the interoperability and the supported versions between the source site and the destination site.

### VMware Cloud Director Availability interoperability matrices

Before installing VMware Cloud Director Availability, verify the supported versions of ESXi and vSphere. For interoperability information between VMware Cloud Director Availability and other VMware products, see the [Product Interoperability Matrix](#).

## **vSphere product edition**

All sites participating in a replication must run vSphere product editions that include the vSphere Replication feature in their licenses. The ESXi hosts in all paired on-premises sites and in all paired cloud sites must run one of the following vSphere product editions that include the vSphere Replication feature:

- vSphere Essentials Plus
- vSphere Standard
- vSphere Enterprise
- vSphere Enterprise Plus
- vSphere Desktop

### **NOTE**

Cannot replicate virtual machines to or from ESXi hosts that do not include the vSphere Replication feature in their licenses. Attempting to configure a replication for virtual machines to or from such a host causes failure for the replication with the following error message.

```
Operation aborted due to an unexpected error.
```

This issue occurs when in the source or in the destination site the underlying vSphere environment uses, for example, a vSphere Essentials license. To successfully replicate, configure the underlying environments with licenses that support the vSphere Replication feature in all participating sites.

For information about the license requirements for vSphere Replication, see *vSphere Replication Licensing* in the *vSphere Replication* documentation.

## **Paired sites versions interoperability**

You can pair Cloud Director sites that have mismatching VMware Cloud Director Availability versions deployed. For information about the source site VMware Cloud Director Availability interoperability with the disaster recovery infrastructure in the destination site, select your version and see *Managing pairing with Cloud Director sites* in the *Administration Guide*.

## **Metering cloud sites**

As **provider**, you must meter the consumption data of each cloud site instance of VMware Cloud Director Availability by adding the Public Service Endpoint of the appliances in VMware vCloud® Usage Meter. For more information, see the *Usage Meter integration* section in the *VMware Cloud Director Availability documentation*.

## **Supported versions**

For information about the currently supported VMware Cloud Director Availability versions, see the *VMware Cloud Director Availability supported versions* section in the *VMware Cloud Director Availability documentation*.

## **Deployment requirements in the Cloud Director site**

Before deploying VMware Cloud Director Availability, verify that the disaster recovery environment in the cloud site backed by VMware Cloud Director™ satisfies the following requirements for the appliances.

### **Deployment Types and Hardware Requirements**

In all cloud sites backed by VMware Cloud Director, deploy all the appliances of VMware Cloud Director Availability by using a single installation OVA file. For information about the appliances location in the disaster recovery infrastructure, see [Deployment architecture in the Cloud Director site](#).

Depending on scale and deployment goals, you can select various deployment roles. The following table describes the virtual appliances of VMware Cloud Director Availability in a cloud site and their hardware requirements from a hosting perspective.

Appliance deployment role	Description and services	Hardware requirements
Cloud Director Replication Management Appliance	<p><b>IMPORTANT</b> As <b>provider</b>, before configuring any replications you must add each instance of Cloud Director Replication Management Appliance for metering in VMware vCloud® Usage Meter. For information about adding the appliances in vCloud Usage Meter, see <a href="#">vCloud Usage Meter Integration</a>.</p> <p>A dedicated appliance role, that runs the following VMware Cloud Director Availability services:</p> <ul style="list-style-type: none"> <li>• Manager Service</li> <li>• Cloud Service with embedded VMware Cloud Director Availability Tenant Portal</li> </ul> <p>Deploy one Cloud Director Replication Management Appliance for configuring replications from and to cloud sites backed by VMware Cloud Director.</p>	<ul style="list-style-type: none"> <li>• 2 vCPUs</li> <li>• 4 GB RAM</li> <li>• 10 GB Storage</li> </ul>
Replicator Appliance	<p>A dedicated appliance role for the Replicator Service that handles the replication traffic in a cloud site.</p> <p>For large-scale environments, you can deploy more than one Replicator Appliance instance per cloud site. Depending on the cloud site type, to add more instances:</p> <ul style="list-style-type: none"> <li>• For cloud sites backed by VMware Cloud Director, see <a href="#">Add an additional Replicator Service instance in the Cloud Director site</a>.</li> <li>• Since VMware Cloud Director Availability 4.5, in cloud sites for vSphere DR and migration you can also deploy one or more Replicator Appliance instances alongside the Replicator Service in the vCenter Replication Management Appliance. For more information, see <i>Add an additional Replicator Appliance instance in the Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site</i>.</li> </ul>	<ul style="list-style-type: none"> <li>• 8 vCPUs</li> <li>• 8 GB RAM</li> <li>• 10 GB Storage</li> </ul>
Tunnel Appliance	<p>A dedicated appliance role for the Tunnel Service.</p> <p>Since VMware Cloud Director Availability 4.6, in cloud sites backed by VMware Cloud Director a second Tunnel Appliance can be configured for high availability. For more information, see <a href="#">Add a second Tunnel Appliance for HA in the Cloud Director site</a>.</p>	<ul style="list-style-type: none"> <li>• 4 vCPUs</li> <li>• 4 GB RAM</li> <li>• 10 GB Storage</li> </ul>
<i>Only for testing:</i> Cloud Director Combined Appliance	<p>An all-in-one appliance role, only suitable for testing and evaluation environments. This Cloud Director Combined Appliance includes all VMware Cloud Director Availability services:</p> <ul style="list-style-type: none"> <li>• Manager Service</li> <li>• Replicator Service</li> <li>• Cloud Service with embedded VMware Cloud Director Availability Tenant Portal</li> <li>• Tunnel Service</li> </ul>	<ul style="list-style-type: none"> <li>• 4 vCPUs</li> <li>• 6 GB RAM</li> <li>• 10 GB Storage</li> </ul>
<i>Only for vSphere DR and migration:</i> vCenter Replication Management Appliance	<p><b>NOTE</b> For information about this appliance role and about deploying and configuring vSphere DR and migration, see <i>Installing and configuring the appliances for vSphere DR and migration</i> in the <i>Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site</i>.</p> <p>VMware Cloud Director Availability 4.4 introduces this appliance role, only suitable for vSphere DR and migration, with no backing VMware Cloud Director. This vCenter Replication Management Appliance includes the following active VMware Cloud Director Availability services:</p> <ul style="list-style-type: none"> <li>• Manager Service</li> <li>• Replicator Service</li> <li>• Tunnel Service</li> </ul> <p><b>IMPORTANT</b> As <b>provider</b>, before configuring any replications you must add each instance of vCenter Replication Management Appliance for metering in VMware vCloud® Usage Meter. For information about adding the appliances in vCloud Usage Meter, see <a href="#">vCloud Usage Meter Integration</a>.</p>	<ul style="list-style-type: none"> <li>• 8 vCPUs</li> <li>• 8 GB RAM</li> <li>• 10 GB Storage</li> </ul>
		69

For information about each service and on which appliance it runs, see [Services](#) and for the network connectivity between the services, see [Network requirements and prerequisites in the Cloud Director site](#).

## **Deployment Requirements**

In a cloud site backed by VMware Cloud Director, deploying VMware Cloud Director Availability requires:

- **Resource vCenter Server Lookup service**

Use the resource vCenter Server Lookup service instance, when in a single site several vCenter Server instances are dedicated for different tasks:

- vCenter Server instances dedicated for management operations.
- vCenter Server instances dedicated as VMware Cloud Director resources.

VMware Cloud Director Availability uses the resource vCenter Server instances for locating and authenticating to resources and create or edit inventory objects. Register the Replicator Service instances and the Cloud Service, and optionally, the Tunnel Service and the Manager Service, with the vCenter Server Lookup service, provided by the Platform Services Controller used by the resource vCenter Server instances.

- **Availability instances per VMware Cloud Director server group**

In each cloud site backed by VMware Cloud Director, deploy one or more instances of Cloud Director Replication Management Appliance per a VMware Cloud Director server group. The server group in VMware Cloud Director consists of a VMware Cloud Director cell and a resource vCenter Server with at least one ESXi host.

For information about deploying multiple instances, see [Deploying Multiple VMware Cloud Director Availability Instances in VMware Cloud Director](#).

- **Certificate of VMware Cloud Director**

VMware Cloud Director Availability verifies the VMware Cloud Director host name in its certificate. The `CommonName` or at least one of the entries in the `Subject Alternative Name` must match the VMware Cloud Director FQDN or IP used when registering it in VMware Cloud Director Availability.

- **Deactivate vApps discovery and adoption in VMware Cloud Director**

VMware Cloud Director vApps discovery and adoption must not be active. For more information, see [Discovering and Adopting vApps](#) in the *VMware Cloud Director* documentation.

- **Dedicated ESXi replication VMkernel interfaces**

To isolate the replication data traffic in the ESXi hosts, dedicate a VMkernel interface for that. By default, ESXi handles the replication data traffic through its management VMkernel interface. Since one VMkernel adapter must handle one traffic type, separate the management traffic from the replication traffic by creating a dedicated replication VMkernel interface.

In every ESXi host that is used as a replication source or as a replication destination, when creating a VMkernel interface dedicated for the replication traffic, use the following tags:

- For replication sources, to configure each ESXi host for the outgoing replication traffic, select `vSphere Replication`. For more information, see *Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host* in the *vSphere Replication* documentation.
- For replication destinations, to configure each ESXi host for the incoming replication traffic, select `vSphere Replication NFC`.

To keep the replication traffic between the ESXi hosts and the Replicator Service instances in the same broadcast domain, configure the dedicated replication VMkernel interface in its own IP subnet and connect each Replicator Service instance to the same virtual port group. As a result, the uncompressed replication traffic avoids crossing a router and saves network bandwidth.

## **VMware Cloud Director Availability Storage Requirements**

### **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.

For both test failover and for reverse operations, and when using seed, the destination storage must accommodate double the space for the disk size of the source virtual machine during the test failover, as in the following two examples.

Since VMware Cloud Director Availability 4.2, for a failover this does not apply and the storage space equals the source workload size during the failover.

- Example required space in the datastore, for a test failover of a source virtual machine with a 2 TB virtual disk:
  1. When creating the replication, VMware Cloud Director Availability allocates 2 TB of space in the destination storage.
  2. When starting a test failover, VMware Cloud Director Availability allocates additional 2 TB, for a total of 4 TB allocated space in the destination storage during the test failover.
  3. After finishing the test failover cleanup task, the additional 2 TB space is unallocated, remaining with 2 TB allocated space in the destination storage when the test failover completes.
- Example required space by a test failover, for VMware vSAN storage, with the same virtual machine:

The same storage space implication applies - the vSAN must accommodate double the disk size of the virtual machine for a test failover. When creating the replication in this example, VMware Cloud Director Availability allocates 2 TB multiplied by the vSAN\_Protection\_Level\_Disk\_Space\_Penalty. When starting a test failover, additional 2 TB are allocated multiplied by the vSAN\_Protection\_Level\_Disk\_Space\_Penalty. For more information, see *About vSAN Policies* and *Planning Capacity in vSAN* in the vSphere documentation.

## **Supported Topologies**

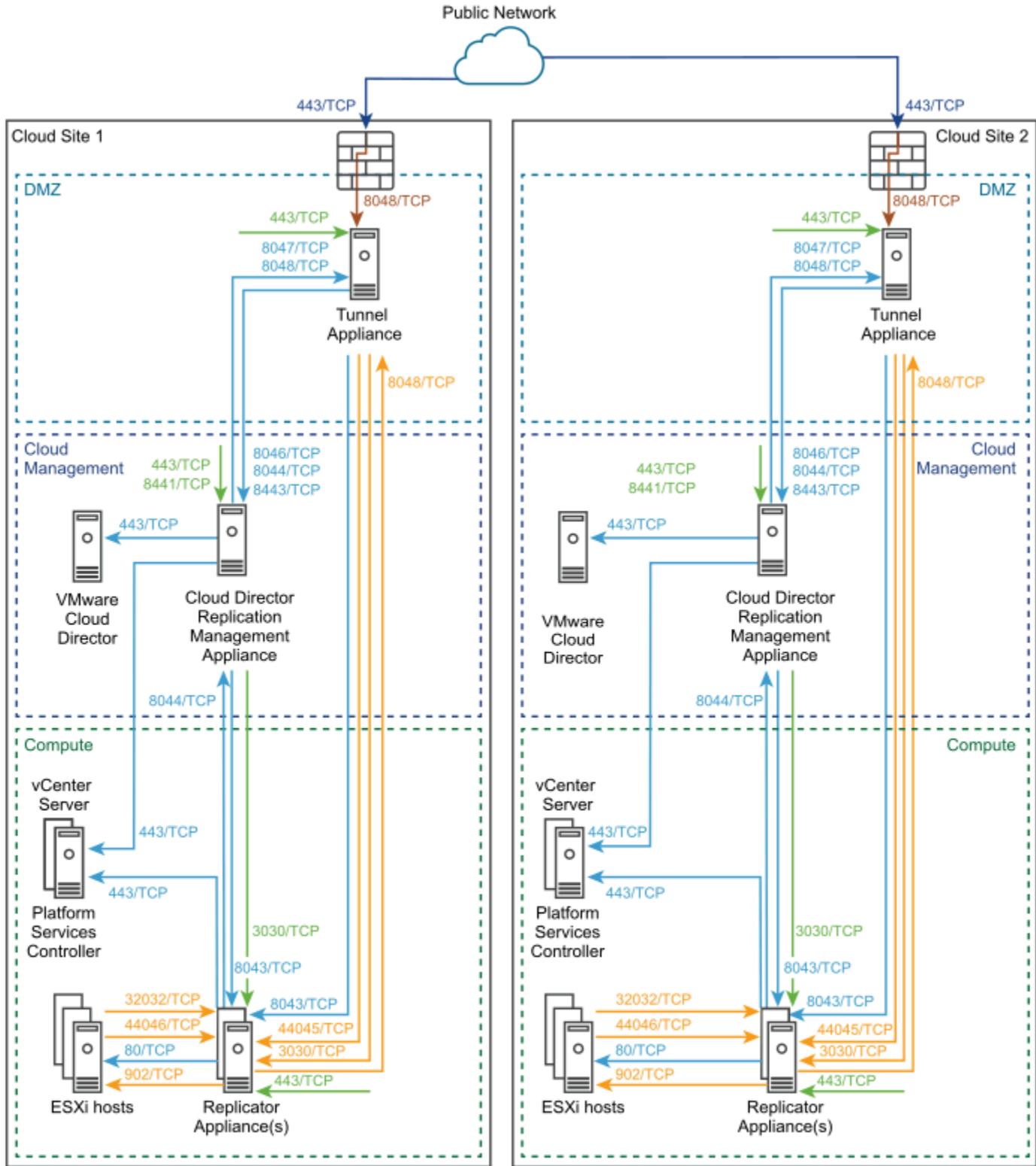
The resource vCenter Server instances within a cloud site backed by VMware Cloud Director must be within the same single sign-on (SSO) domain. All Replicator Service, Manager Service, Cloud Service, and Tunnel Service instances within the respective site must be configured with that same SSO domain. For diagrams showing all services in the cloud site and a diagram showing multiple VMware Cloud Director Availability instances, see [Deployment architecture in the Cloud Director site](#).

## **Network requirements and prerequisites in the Cloud Director site**

Before you start deploying and configuring VMware Cloud Director Availability, ensure that the required network ports are opened and allow the VMware Cloud Director Availability services communication within a site and between sites.

For information about the required firewall ports to be opened, see [VMware Cloud Director Availability Network Ports](#).

The following network diagram shows the data flow direction and the data traffic type. The diagram also shows the required network ports for communication between the VMware Cloud Director Availability appliances and the disaster recovery infrastructure for a deployment with two cloud sites.



Traffic type:

- Replication data traffic
- Administration traffic
- Service management traffic
- DNAT
- Replication data traffic and VMware Cloud Director Availability service management traffic

• Production deployment architecture:

For an architecture diagram showing all services operating in a VMware Cloud Director Availability instance in a production Cloud Director site, see [Production Deployment](#).

- **Multiple instances of VMware Cloud Director Availability:**

For a diagram showing multiple VMware Cloud Director Availability instances per one VMware Cloud Director instance, see [Deploying Multiple VMware Cloud Director Availability Instances in VMware Cloud Director](#).

- **Active-active mode Tunnel Appliance instances:**

For a diagram showing two Tunnel Appliance instances in active-active mode behind a TCP load balancer, see [Deploying Two Active-Active Tunnel Appliance Instances](#).

All the components of VMware Cloud Director Availability must be able to communicate with each other and with the disaster recovery infrastructure:

### **VMware Cloud Director Availability Appliances Connectivity**

On appliances-level, the VMware Cloud Director Availability appliances must be able to communicate with each other and with the disaster recovery infrastructure:

- The Cloud Director Replication Management Appliance must have TCP access to all the Replicator Appliance instances in both local, and in remote sites, to the local VMware Cloud Director, and to the resource vCenter Server, where the resource vCenter Server Lookup service is hosted.
- The Replicator Appliance instances must have TCP access to the Cloud Director Replication Management Appliance, to the same resource vCenter Server, and to the same resource vCenter Server Lookup service.

### **VMware Cloud Director Availability Services Connectivity**

For information about each service, see [Services](#).

On services-level, the VMware Cloud Director Availability services must be able to communicate with each other and with the local disaster recovery infrastructure in the site backed by VMware Cloud Director:

- The Cloud Service must have TCP access to the Manager Service, to the local VMware Cloud Director in the site, to the local vCenter Server and its Platform Services Controller, depending on where the vCenter Server Lookup service is hosted.
- The Manager Service must have TCP access to all the Replicator Service instances in both local, and in remote sites and to the local vCenter Server Lookup service in the site.
- All the Replicator Service instances must have TCP access to the Manager Service, to the local vCenter Server and to its vCenter Server Lookup service.

#### **IMPORTANT**

##### **TLS termination proxy is not supported and SSL termination must not be used:**

The VMware Cloud Director Availability services use end-to-end encryption for the communication across sites. For example when a Replicator Service on site 1 is communicating to a Replicator Service on site 2, VMware Cloud Director Availability expects that the TLS session is terminated at each Replicator Service.

VMware Cloud Director Availability does not support any TLS terminating products or solutions placed between the appliances, for example, VMware NSX® Edge™ instances, HAProxy, Nginx, Fortinet, and others. If such solutions are in place, they must be configured in pass-thru mode, also known as TCP mode, to prevent from interfering with the TLS traffic of VMware Cloud Director Availability. For information about the load balancer configuration, see [Add a second Tunnel Appliance for HA in the Cloud Director site](#).

## Firewall Rules for External Communication

Ensure that the firewall rules are correctly configured to allow site-to-site communication and pairing between the local and remote sites:

Original destination	Original destination port	Translated destination	DNAT translated port	Protocol	Description
Public network / Uplink interface	443	Tunnel Appliance	8048	TCP	Used for incoming replication management and replication data traffic from public networks to the Tunnel Service. This service then routes the traffic to the local services.

For information about the load balancer configuration for two Tunnel Appliance instances in active-active mode, see [Add a second Tunnel Appliance for HA in the Cloud Director site](#).

For information about pairing remote Cloud Director sites in VMware Cloud Director Availability, see [Managing pairing with Cloud Director sites](#) in the *Administration Guide*.

## Deploying the appliances in the Cloud Director site

In a cloud environment with VMware Cloud Director™, deploy VMware Cloud Director Availability from a single OVA file for deploying all of the appliances roles, either by using the vSphere Client, or the VMware OVF Tool.

The VMware Cloud Director Availability appliances come as preconfigured virtual machines that are optimized for running the VMware Cloud Director Availability services.

The provider appliances have a name in the form `VMware-Cloud-Director-Availability-Provider-release.number.xxxx-build_number_OVF10.ova`.

### NOTE

After deploying an appliance, for the first time only power it on from vSphere. Attempting to power it on for the first time from the ESXi user interface results in errors and that require redeploying the appliance from the scratch and then powering it on from vSphere.

Follow this chapter and in a production cloud site backed by VMware Cloud Director, repeat the procedures to deploy all of the following VMware Cloud Director Availability appliances:

- One Cloud Director Replication Management Appliance.
- One or more Replicator Appliance instances.
- One, or optionally, two Tunnel Appliance instances.

For information about the architecture and each appliance role, see [Deployment architecture in the Cloud Director site](#).

## Deploy the appliances by using the vSphere Client

In the vSphere Client, you can deploy each VMware Cloud Director Availability appliance role from a single .ova file.

- Download the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
  - If using a version of vSphere earlier than 6.5, install the Client Integration Plug-in to use the **Deploy OVF Template** option in the vSphere Web Client.
1. Log in to vCenter Server by using the vSphere Client.
  2. Navigate to a target object where you want to deploy the VMware Cloud Director Availability services. As a target object you can use a data center, a folder, a cluster, a resource pool, or a host.
  3. Right-click the target object and from the drop-down menu select **Deploy OVF Template**. The **Deploy OVF Template** wizard opens.
  4. On the **Select an OVF template** page, browse to the .ova file location and click **Next**.
  5. On the **Select a name and folder** page, enter a name for the appliance, select a deployment location, and click **Next**.
  6. On the **Select a compute resource** page, select a host, or cluster as a compute resource to run the appliance on, and click **Next**.
  7. On the **Review details** page, verify the OVF template details and click **Next**.
  8. On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.
  9. On the **Configuration** page, select the appliance deployment type configuration and click **Next**.
    - For information about the **vCenter Replication Management Appliance**, see [Deploy the appliances for vSphere DR and migration](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
    - For information about the deployment roles of each appliance, see [Deployment requirements in the Cloud Director site](#).
  10. On the **Select storage** page, select the virtual disk format and the storage policy for the appliance and click **Next**.
  11. On the **Select networks** page, optionally configure the network settings of the appliance and click **Next**.  
For more information about configuring the network settings after the deployment is complete, see the *Network settings configuration* chapter in the *Administration Guide* document.
  12. On the **Customize template** page, customize the deployment properties of the appliance and click **Next**.

Option	Description
<b>Root Password</b>	Enter and confirm the initial password for the appliance <b>root</b> user.  Later, when logging in for the first time as the <b>root</b> user, the appliance requires changing this initial password.
<b>NTP Server</b>	Enter an NTP server hostname or IP address.  <b>IMPORTANT</b> In the disaster recovery environment, ensure that both vCenter Server instances in the source and in the destination, the ESXi hosts, and the VMware Cloud Director Availability appliances all use the same NTP server.
<b>Hostname</b>	Enter the appliance hostname. Leave blank if DHCP is desired.
<b>Address</b>	Enter the IP address of the appliance. Leave blank if DHCP is desired.

Option	Description
	Ensure that the IP is in the CIDR notation, for example, enter <i>192.168.0.222/24</i> . Otherwise, the boot-up sequence shows an error and <i>127.0.0.1</i> as the IP address.
<b>Gateway</b>	Enter the gateway of the appliance network. Leave blank if DHCP is desired.
<b>MTU</b>	Enter the maximum transmission unit of the network. Leave blank if DHCP is desired.
<b>DNS servers</b>	Enter DNS servers for the appliance network. Leave blank if DHCP is desired.
<b>Search domains</b>	Enter the search domains for the appliance network. Leave blank if DHCP is desired.

13. On the **Ready to complete** page, review the settings, optionally select **Power on after deployment** and to begin the `.ova` installation process, click **Finish**.

The **Recent Tasks** pane shows a new task for initializing the `.ova` deployment. After the task is complete, the new appliance is created on the selected resource.

Repeat this procedure as needed for deploying the remaining appliances.

## Deploying by using the VMware OVF tool

To deploy VMware Cloud Director Availability by using the VMware OVF Tool, define deployment parameters and run a deployment script.

### Define the OVF tool parameters for appliance deployment

Before you deploy the VMware Cloud Director Availability appliances, you must define the specific VMware OVF Tool parameters for deployment.

The following table describes the parameters you must define when deploying the VMware Cloud Director Availability appliances by using the VMware OVF Tool scripts.

Parameter	Description
OVA	The local client path to the installation OVA package. For example, use <code>OVA="local_client_path/VMware-Cloud-Director-Availability-Deployment-release.number-xxxx-build_number_OVF10.ova"</code> , where <i>Deployment</i> is <i>Provider</i> or <i>On-Premises</i> .
VMNAME	Virtual machine name.
VSPHERE_DATASTORE	The <code>VSPHERE_DATASTORE</code> value is the datastore name as it is displayed in the .
VSPHERE_NETWORK	The name of the network on which the appliance to run.
VSPHERE_ADDRESS	The IP address of the vCenter Server instance on which you deploy the appliance.
VSPHERE_USER	User name for a vCenter Server administrator.
VSPHERE_USER_PASSWORD	Password for a vCenter Server administrator.

Parameter	Description
VSPHERE_LOCATOR	<p>The VSPHERE_LOCATOR value contains the target data center name, the tag <i>host</i>, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The VSPHERE_LOCATOR value depends on the topology of your vSphere environment. Following are examples for valid VSPHERE_LOCATOR values.</p> <ul style="list-style-type: none"> <li><i>/data-center-name/host/cluster-1-name/ESXi-host-fully-qualified-domain-name</i></li> <li><i>/data-center-name/host/cluster-2-name/ESXi-host-IP-address</i></li> </ul> <p>If the target ESXi host is not part of a cluster, skip the <i>cluster-name</i> element, as shown in the following examples.</p> <ul style="list-style-type: none"> <li><i>/data-center-name/host/ESXi-host-fully-qualified-domain-name</i></li> <li><i>/data-center-name/host/ESXi-host-IP-address</i></li> </ul> <p>For more information about the VSPHERE_LOCATOR value, run the <code>./ovftool --help locators</code> command.</p>

## Deploy the appliances by using the OVF tool

In the VMware OVF tool console, you can use a single `.OVA` installation file to deploy the VMware Cloud Director Availability appliances. You define deployment parameters in the OVF Tool console and run the deployment script.

- Download the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
- Verify that the VMware OVF Tool is installed and configured. For more information, see <https://code.vmware.com/tool/ovf>.

- Log in to a server where the OVF Tool is running, by using a Secure Shell (SSH) client.
- Define deployment parameters in the OVF Tool console by running the following commands.

```
# VMNAME="Name-to-be-Assigned-to-the-VM"

# VSPHERE_DATASTORE="vSphere-datastore"

# VSPHERE_NETWORK="VM-Network"

# ova="local_client_path/VMware-Cloud-Director-Availability-Provider-release_number-xxx-build_number_OVF10.ova"

# VSPHERE_USER="vCenter-Server-admin-user"

# VSPHERE_USER_PASSWORD="vCenter-Server-admin-user-password"

# VSPHERE_ADDRESS="vCenter-Server-IP-address"

# VSPHERE_LOCATOR="vSphere-locator"
```

- Deploy a VMware Cloud Director Availability appliance.

To select the deployment type for the appliance that you are deploying, set the `--deploymentOption` argument to `cloud`, `tunnel`, `replicator`, or `combined`.

The following example command deploys a combined VMware Cloud Director Availability appliance and sets a static IP address.

```
#!/ovftool/ovftool --name="{VMNAME}" --datastore="{VSPHERE_DATASTORE}" --acceptAllEulas
```

```

--powerOn --X:enableHiddenProperties --X:injectOvfEnv --X:waitForIp
--ipAllocationPolicy=fixedPolicy --deploymentOption=combined --machineOutput --noSSLVerify
--overwrite --powerOffTarget "--net:VM Network=${VSPHERE_NETWORK}" --diskMode=thin
--prop:guestinfo.cis.appliance.root.password='Your-Root-Password'
--prop:guestinfo.cis.appliance.ssh.enabled=True
--prop:guestinfo.cis.appliance.net.ntp='Your-NTP-Servers-IP-Addresses (comma-separated) '
--prop:net.hostname='Appliance-Hostname'
--prop:net.address='IP-In-CIDR-Notation'
--prop:net.gateway='Your-Gateway-IP'
--prop:net.mtu='Your-MTU'
--prop:net.dnsServers='Your-DNS-Servers-IP-Addresses (comma-separated) '
--prop:net.searchDomains='Your-DNS-Search-Domains (comma-separated) '
"${OVA}" "vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"

```

The console outputs the IP address of the VMware Cloud Director Availability appliance.

## Configuring the appliances in the Cloud Director site

To configure VMware Cloud Director Availability in the cloud site, first you perform an initial configuration of the Cloud Service that registers with VMware Cloud Director, with the vCenter Server Lookup service, with the Replicator Service instances, and with the single, or optionally, the dual Tunnel Service instances. Then you can proceed to pair cloud sites.

### NOTE

In the previous chapter you deployed in a production cloud site backed by VMware Cloud Director, all of the following VMware Cloud Director Availability appliances:

- One Cloud Director Replication Management Appliance, where the appliance runs the Cloud Service.
- One or more Replicator Appliance instances, where each appliance runs one Replicator Service instance.
- One, or optionally, two Tunnel Appliance instances, where each appliance runs one Tunnel Service instance.

For information about the architecture and each appliance role, see [Deployment architecture in the Cloud Director site](#).

As a best practice, first configure all services in a single cloud site: register the Cloud Service with VMware Cloud Director, with the vCenter Server Lookup service, with the Replicator Service instances in the same site, and with the single or, optionally, dual Tunnel Service instances in active-active mode for high availability (HA).

Then, to allow for pairing, perform the initial configuration and the registration in the remote VMware Cloud Director Availability site.

After configuring the VMware Cloud Director Availability services, you can validate that the setup is complete by opening the service management interface. On the **System health** page, the entries show green to indicate the successfully configured services.

## Configure the Cloud Service in the Cloud Director site

Enter a site name as an identifier of this Cloud Service instance and register this Cloud Service with VMware Cloud Director™ and with the local vCenter Server Lookup service. By following the wizard, register this Cloud Service with one or more Replicator Service instances and with the primary\* Tunnel Service.

- Verify that the installation requirements in the cloud site are met. For information about the requirements, see [Installation requirements and deployment prerequisites in the Cloud Director site](#).
- Verify that all the appliances of VMware Cloud Director Availability are successfully deployed. For information about deploying the appliances, see [Deploying the appliances in the Cloud Director site](#).

1. In a Web browser, go to `https://Cloud-Replication-Management-Appliance-IP-Address/`.

As this Cloud Director Replication Management Appliance is not yet configured, you are redirected to `https://Cloud-Replication-Management-Appliance-IP-Address/ui/provider`.

2. Log in by using the **root** user password that you set during the OVA deployment.
3. If you log in to the appliance for the first time, you must change the initial **root** user password.
  - a) Enter the initial **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password.  
The password that you enter must be a secured password with a minimum of eight characters and it must consist of:
    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as & # %.
  - c) Click **Apply**.  
The **Getting Started** tab opens.
4. Under **Steps for fresh installation** click **Run the initial setup wizard**.  
Under **Deploy the Cloud Replication Management Appliance**, you see the IP address of this newly deployed Cloud Director Replication Management Appliance.
5. To set up this Cloud Service instance, complete the **Initial Setup** wizard.
  - a) On the **Licensing** page, enter a license key for VMware Cloud Director Availability™ and click **Save and continue**.  
After providing a valid license key, if you cancel the initial setup wizard, on subsequent attempts the license key is greyed-out and the page does not allow entering it again.
  - b) On the **Site Details** page, configure this Cloud Service instance site and click **Save and continue**.

Site Name	Enter a site name for this Cloud Service instance. <b>IMPORTANT</b> The site name is used as an identifier of this instance of VMware Cloud Director Availability and cannot be changed later without impacting the active replications.
Public Service Endpoint address	Optionally, now enter the Public Service Endpoint address. Alternatively, now you can skip entering this address and provide it later, after you complete the initial configuration.
Description	Optionally, enter a description for this site.
Choose which data engines to be activated	Activate either one or both data engines for replications: <ul style="list-style-type: none"> <li>• <b>Classic</b> data engine supports both migrations and protections.</li> <li>• <b>VMC</b> data engine supports only migrations.</li> </ul> For information about activating the data engines after completing the initial setup, see <i>Activate data engine for replications</i> in the <i>Administration Guide</i> .

- c) On the **VMware Cloud Director** page, register this Cloud Service instance with VMware Cloud Director and click **Save and continue**.

VMware Cloud Director endpoint URL	Enter the address of VMware Cloud Director and press Tab, auto-completing the address as <code>https://VMware-Cloud-Director-IP-Address:443/api</code> .
VMware Cloud Director user name	Enter the user name of a <b>System administrator</b> user in VMware Cloud Director. For example, use <code>administrator@system</code> .

VMware Cloud Director password	Enter the password of the VMware Cloud Director <b>System administrator</b> user.
--------------------------------	---

Verify the thumbprint and accept the SSL certificate of VMware Cloud Director. If you provide a user with insufficient privileges in VMware Cloud Director, it returns an error message: Unexpected VMware Cloud Director error. [ UI-id ] This operation is denied.

When successfully registered in VMware Cloud Director, the Cloud Service installs the plug-ins named Setup DRaaS and Migration and Availability (*localSite*).

- d) On the **Replicator Service instances** page, register this Cloud Service instance with the vCenter Server Lookup service and with one or more Replicator Service instances, then click **Save and continue**.

Option	Description	
<b>Lookup Service address</b>	Enter the address of the vCenter Server Lookup service and press Tab, auto-completing the address as <code>https://Lookup-Service-IP-Address:443/lookupservice/sdk</code> . For information about the supported topologies, see <a href="#">Deployment requirements in the Cloud Director site</a> .	
<b>Replicator 1</b>	<b>Replicator API Service Endpoint</b>	Enter the endpoint address of the first Replicator Service instance and press Tab, auto-completing the address as <code>https://Replicator-IP-Address:8043</code> .
	<b>Replicator Service root password</b>	Enter the password of the <b>root</b> user of the Replicator Appliance instance.
	<b>Test connection</b>	Click to verify the connectivity to this endpoint and its <b>root</b> user password and to save this Replicator Service instance. If the password is not set since deploying the appliance, you must change the initial <b>root</b> user password. When prompted, enter the initial root user password that you set during the OVA deployment. Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: <ul style="list-style-type: none"> <li>• At least one lowercase letter.</li> <li>• At least one uppercase letter.</li> <li>• At least one number.</li> <li>• At least one special character, such as: &amp; # % .</li> </ul>
	<b>SSO user name</b>	Enter a user with administrative privileges in the local site single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
	<b>SSO password</b>	The password for the administrative user.
	<b>Description</b>	Optionally, enter a description for this Replicator Service instance.

Option	Description
<b>Add a Replicator Service instance</b>	Optionally, add more Replicator Service instances.
<b>Use the above Lookup Service address for Cloud, Manager, and Tunnel</b>	<ul style="list-style-type: none"> <li>Since version 4.6, by default this toggle is inactive, meaning the vCenter Server Lookup service address applies only for the Replicator Service instances. <p><b>IMPORTANT</b> By not using this address for the Manager Service, the Cloud Service, and the Tunnel Service where its optional, they show <code>Lookup Service Unconfigured</code>, as expected for vCenter Server Lookup service that is not configured.</p> <p><b>Important:</b> By leaving this toggle inactive does not allow single sign-on (SSO) user authentication for these services. To later configure the vCenter Server Lookup service address for them, see the steps in <i>Configure the services to accept the vCenter Server Lookup service certificate and optionally allow SSO</i> in the <i>Administration Guide</i>.</p> </li> <li>Alternatively, to also use this vCenter Server Lookup service address for the Manager Service, for the Cloud Service, and for the Tunnel Service, and also enable SSO for all these services, activate this toggle.</li> </ul>

Verify the thumbprints and accept the SSL certificates of the vCenter Server Lookup service and of each of the configured Replicator Service instances.

- e) On the **Tunnel Service** page, register this Cloud Service with the primary\* Tunnel Service, test the connection, and click **Save and continue**.

Tunnel Service Address	Enter the API endpoint address of the primary* Tunnel Service and press Tab, auto-completing the address as <code>https://Tunnel-IP-Address:8047</code> .
Root Password	Enter the password of the <b>root</b> user of the Tunnel Appliance.
Test Connection	<p>Click to verify the connectivity to the endpoint and the <b>root</b> user password, and save the Tunnel Service. If the password is not set since deploying the appliance, you must change the initial <b>root</b> user password.</p> <p>Enter the initial root user password that you set during the OVA deployment. Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:</p> <ul style="list-style-type: none"> <li>At least one lowercase letter.</li> <li>At least one uppercase letter.</li> <li>At least one number.</li> <li>At least one special character, such as: &amp; # % .</li> </ul>

\* During the initial configuration, register only the primary Tunnel Appliance. For information about the Tunnel Service high availability and registering a second Tunnel Appliance instance, see [Add a second Tunnel Appliance for HA in the Cloud Director site](#).

Verify the thumbprint and accept the SSL certificate of the Tunnel Service.

- f) On the **Ready To Complete** page, review the Cloud Service configuration summary and click **Finish**.
6. Before pairing, as **provider** you must add each Cloud Service instance for metering in VMware vCloud® Usage Meter.

For information about adding the cloud sites instances in vCloud Usage Meter, see [vCloud Usage Meter Integration](#).

7. Optional: Verify that the Cloud Service configuration is correct.
  - a) In the left pane under **System**, click **System Health**.
  - b) On the **System health** page, ensure that the statuses show as green OK.

After adding the Cloud Service instances in vCloud Usage Meter, you can now pair this Cloud Service instance with cloud sites and with one or more On-Premises to Cloud Director Replication Appliance instances.

For information about pairing and metering the cloud site, see [Managing pairing with Cloud Director sites](#) in the *Administration Guide*.

## Add an additional Replicator Service instance in the Cloud Director site

As a **provider**, depending on the deployment requirements, you can add more Replicator Service instances to the Cloud Director site after configuring the Cloud Service.

- Verify that the Cloud Service in the disaster recovery environment is already configured. For information about configuring the service, see [Configure the Cloud Service in the Cloud Director site](#).
  - Deploy a new Replicator Appliance instance. For more information, see [Deploy VMware vCloud Availability Services Using the vSphere Client](#) and [Deploy VMware vCloud Availability Services Using the OVF Tool](#).
1. Log in to the service management interface of the newly deployed Replicator Appliance instance.
    - a) In a Web browser, go to `https://Replicator-Appliance-IP-Address/ui/admin`.
    - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
    - c) Click **Login**.
  2. If you log in to the appliance for the first time, you must change the initial **root** user password.
    - a) Enter the initial **root** user password that you set during the OVA deployment.
    - b) Enter and confirm a new password.

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

      - At least one lowercase letter.
      - At least one uppercase letter.
      - At least one number.
      - At least one special character, such as & # %.
    - c) Click **Apply**.

The **Getting Started** tab opens.

3. In the left pane, click **Settings** and next to **Lookup Service Address** click **Edit**.
4. In the **Lookup Service Details** window, enter the vCenter Server Lookup service address.
  - a) Press Tab and autocomplete the address as `https://Lookup-Service-IP-address:443/lookupservice/sdk`.
  - b) Click **Apply**.
  - c) Verify and accept the SSL certificate of the vCenter Server Lookup service.
5. Verify that the vCenter Server Lookup service connectivity is operational.
  - a) In the left pane, click **System Monitoring**.
  - b) Under **Service status**, verify that **Lookup Service connectivity** shows a green check status.
6. Log in to the Manager Service service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
7. In the left pane, click **Replicator Services**.
8. On the **Replicator Services administration** page, click **New**.
9. In the **New Local Replicator Service** window, enter the details for the new Replicator Service instance then click **Add**.
  - a) Enter the address and the **root** user password of the new Replicator Appliance then click **Test Connection**.
  - b) Verify and accept the SSL certificate of the new Replicator Service instance.
  - c) Enter the single-sign-on user credentials for the single sign-on domain in the local site.
  - d) Optionally, if you deployed multiple Replicator Appliance instances, to register the additional ones click **Add a Replicator Service instance** then repeat entering the configuration details for each one.

Option	Description
<b>Lookup Service Address</b>	Enter the IP address or the hostname of the vCenter Server Lookup service in the Cloud Director site.
<b>Replicator API Service Endpoint</b>	Enter the IP address and port 8043 of the newly deployed Replicator Appliance instance in the Cloud Director site.  For example, enter <code>https://Replicator-Appliance-IP-address:8043</code> .
<b>Replicator Service Root Password</b>	Enter the <b>root</b> user password for the new Replicator Appliance as set during the OVA deployment of the new appliance then click <b>Test Connection</b> .
<b>New Password</b>	If you did not log in to the new Replicator Appliance, you must now change the initial <b>root</b> user password:  Enter a new password for the <b>root</b> user of the new appliance.  The password that you enter must be a secured password with a minimum of eight characters and it must consist of: <ul style="list-style-type: none"> <li>• At least one lowercase letter.</li> <li>• At least one uppercase letter.</li> <li>• At least one number.</li> <li>• At least one special character, such as &amp; # %.</li> </ul>
<b>Confirm Password</b>	Confirm the new password for the <b>root</b> user of the new appliance, matching the above entry.

Option	Description
SSO User name	Enter a user with administrative privileges in the local site single sign-on domain. For example, enter <i>Administrator@VSPHERE.LOCAL</i> .
SSO password	Enter the password for the single sign-on administrative user.
Description	Optionally, enter a description for the new Replicator Service instance you are registering.

If you enter the FQDN of Replicator Appliance, the management interface always shows the IP address of this Replicator Appliance instance.

On the **Replicator Services administration** page, you now see a green check status for the new Replicator Service instance added to this Manager Service.

10. Verify that the connectivity of the Manager Service to the new instance of Replicator Service is operational.
  - a) In the left pane, click **System Health**.
  - b) Under **Local Replicator Services**, verify that for the new Replicator Service instance **Service connectivity** shows a green check status.

11. To start using the new Replicator Service instance, re-pair this cloud site with all paired cloud sites.

On-premises sites in up to 30 minutes detect the new Replicator Appliance instance and automatically reconfigure the On-Premises to Cloud Director Replication Appliance to start using the new Replicator Service instance. Alternatively, for the on-premises sites to start immediately using the new Replicator Service instance, re-pair these on-premises sites for the On-Premises to Cloud Director Replication Appliance instances to learn about the new Replicator Appliance instance.

A new Replicator Service instance is added to the VMware Cloud Director Availability cloud site.

- To add another Replicator Service instance, repeat this procedure.
- To use the new Replicator Service instance, re-pair all paired cloud sites.

## Add a second Tunnel Appliance for HA in the Cloud Director site

To allow the cloud site to remain operational in case the Tunnel Service becomes unavailable, VMware Cloud Director Availability can operate a couple of Tunnel Service instances in active-active mode per each Cloud Service instance. Since only one Tunnel Service can operate in one Tunnel Appliance, deploy and configure a second Tunnel Appliance in the Cloud Director site for High Availability (HA).

- Verify that all the appliances of VMware Cloud Director Availability 4.6 are successfully deployed, with two Tunnel Appliance instances ready for configuring the second one. For information about deploying all of the appliances, see [Deploying the appliances in the Cloud Director site](#).
- Verify that as **provider** you deploy a load balancer, configured only in TCP mode for both Tunnel Appliance instances.
- Do not register one and the same Tunnel Service instance in the Cloud Service twice.

All incoming and outgoing replication management and data traffic passes through the Tunnel Appliance in the Cloud Director site. If this Tunnel Appliance becomes unavailable for some reason, the paired remote sites cannot communicate with this cloud site, causing disruption for all replications.

### Second Tunnel Appliance:

VMware Cloud Director Availability 4.6 and later can use an optional additional Tunnel Appliance deployed and configured in the Cloud Director site behind an external load balancer. While both Tunnel Service instances are operational, all incoming/outgoing data/management traffic balances between them. If one Tunnel Service instance becomes unavailable, the local and the remote traffic automatically prefer the operational Tunnel Service, provided that both\* sites run version 4.6 or later. For information about the deployment architecture, see [Deploying Two Active-Active Tunnel Appliance Instances](#).

**Active-active mode:**

The following table shows each hop and the order of processing of the incoming and the outgoing external traffic between Internet and the two active-active Tunnel Appliance instances and the order of processing of the internal traffic between the two active-active Tunnel Appliance instances and the Cloud Director Replication Management Appliance and the Replicator Appliance instances:

Traffic direction	Incoming traffic order of processing and hops	Outgoing traffic order of processing and hops
The external traffic, in the order of processing:	<ol style="list-style-type: none"> <li>1. Internet &gt; Public Service Endpoint:443/TCP.</li> <li>2. TCP load balancer:443/TCP &gt; network address translation &gt;:8048/TCP.</li> <li>3. Both Tunnel Appliance instances:8048/TCP.</li> </ol>	<ol style="list-style-type: none"> <li>1. Both Tunnel Appliance instances.</li> <li>2. Firewall (network address translation).</li> <li>3. Public Service Endpoint &gt; Internet.</li> </ol>
Internal traffic:	<ol style="list-style-type: none"> <li>1. Both Tunnel Appliance instances.</li> <li>2. Cloud Director Replication Management Appliance and Replicator Appliance instances.</li> </ol>	<ol style="list-style-type: none"> <li>1. Cloud Director Replication Management Appliance and Replicator Appliance instances.</li> <li>2. TCP load balancer.</li> <li>3. Both Tunnel Appliance instances.</li> </ol>

For a diagram of the hops and the direction of the traffic, see [Deploying Two Active-Active Tunnel Appliance Instances](#).

**Load balancer configuration:**

VMware Cloud Director Availability can operate with any external load balancer configured in application mode: **TCP**. The load balancer must not have TLS/SSL termination proxy, must not perform HTTPS/SSL inspection, and must not use session affinity also known as sticky sessions. The load balancer can choose any of the two active-active Tunnel appliances by using, for example, the round-robin algorithm. For load balancer you can use, for example, haproxy, avi lb, or others without TLS termination. For information about the connectivity between the services and TLS termination, see [VMware Cloud Director Availability Services Connectivity](#).

As **provider**, first configure your TCP load balancer to route the incoming TCP connections towards TCP port 8048 of each of the two Tunnel Appliance instances. Also, ensure that both Tunnel Appliance instances can still make outgoing TCP connections to remote sites, similarly to previous versions with a single Tunnel Appliance. Once the load balancer is configured and routes the incoming and outgoing traffic to and from both Tunnel Appliance instances, enter its IP address in the VMware Cloud Director Availability configuration by following this procedure.

**NOTE**

- VMware Cloud Director Availability does not monitor the TCP load balancer health nor its connectivity.
- Two Tunnel Service instances can operate only in Cloud Director sites.
- The Tunnel Service instances behind the load balancer operate in an active-active mode. Neither Tunnel Appliance is primary or secondary as both Tunnel Appliance instances are considered equal for data routing purposes and do not perform flexible data routing.
- Incoming data bandwidth throttling operates differently with dual Tunnel Appliance instances configured. The throughput value limit applies to each Tunnel Appliance, and since traffic is balanced between both, the aggregate incoming traffic may reach up to twice the configured individual Tunnel Appliance throughput. If one of the Tunnel Appliance instances reaches its cap while the other does not, the busy Tunnel Appliance cannot borrow from the quota of the other.
- \* If only one site is running VMware Cloud Director Availability 4.6 with dual Tunnel Service:
  - Paired cloud sites running earlier versions, for example VMware Cloud Director Availability 4.4 or 4.5, operate as previously when paired with a site running dual Tunnel Service instances, while both instances

are operational. If one instance is down, these sites can experience management traffic issues. However, the data channel automatically recovers and the replication traffic continues without any intervention.

- Paired on-premises sites running version 4.4 or 4.5, may in some cases experience connectivity issues when one of the Tunnel Service instances in the cloud site is not operational.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Tunnel settings** next to **Tunnel HA**, click **Setup**.
4. In the **Tunnel HA TCP Balancer** window, configure the addresses of your TCP load balancer and the second Tunnel Service, then click **OK**.

Option	Description
<b>TCP Balancer address</b>	Enter the <i>IP-address</i> of your load balancer and ensure that it meets all prerequisites.  This is the IP address of the load balancer which resolves to the FQDN of the Public Service Endpoint of VMware Cloud Director Availability.
<b>Port</b>	Enter the <i>TCP-port</i> . This is the port from the Public Service Endpoint.
<b>Tunnel Service Endpoint address</b>	Enter the <i>IP-address</i> of the second Tunnel Appliance instance that you deployed.  <b>NOTE</b> The first Tunnel Appliance instance is already configured during the initial configuration of VMware Cloud Director Availability. For more information see <a href="#">Configure the Cloud Service in the Cloud Director site</a> .
<b>Appliance user</b>	<b>root</b>
<b>Password</b>	Enter the password of the <b>root</b> user of the second Tunnel Appliance instance.

The configured load balancer starts forwarding all the incoming TCP requests to both Tunnel Appliance instances by using the round robin algorithm. Each Tunnel Service instance then passes them to the remaining services of VMware Cloud Director Availability.

You can test that restarting either one of the Tunnel Appliance instances does not interrupt the replications while the other instance is operational.

## Configuring Customer Experience Improvement Program

You can configure VMware Cloud Director Availability™ to participate in the VMware's Customer Experience Improvement Program ("CEIP"). By joining the CEIP, VMware receives anonymous information for improving the quality, reliability, and functionality of VMware products and services.

### VMware Customer Experience Improvement Program

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through the CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

To join or leave the CEIP for this product, see [Join or leave the Customer Experience Improvement Program](#).

## Categories of information that VMware receives

VMware Cloud Director Availability participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <https://www.vmware.com/solutions/trustvmware/ceip.html>.

You can join your VMware Cloud Director Availability to the Customer Experience Improvement Program (CEIP), or decide to leave the CEIP at any time. To leave and rejoin your instance to the CEIP, see [Join or leave the Customer Experience Improvement Program](#).

## Join or leave the Customer Experience Improvement Program

You can configure VMware Cloud Director Availability to join the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

For information about the CEIP Product Table in the Trust & Assurance Center, see <https://www.vmware.com/solutions/trustvmware/ceip-products.html>.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Customer Experience Improvement Program participation**, next to **Participate in CEIP** click **Edit**.
4. In the **Participate in CEIP** window, to join or leave the CEIP for this product configure the following check box then click **Apply**.
  - To join the CEIP, select the **Join the VMware Customer Experience Improvement Program** check box.
  - To leave the CEIP, deselect the **Join the VMware Customer Experience Improvement Program** check box.

## Upgrading in the Cloud Director site

Follow the upgrade path and choose an upgrade method that is available for the currently installed VMware Cloud Director Availability version. After following the prerequisites, choose a source repository for the upgrade files and upgrade each appliance in the Cloud Director site, according to a specific order.

### Upgrade Paths

To upgrade to the latest version of VMware Cloud Director Availability in Cloud Director sites, choose an upgrade method according to the currently installed version in the site.

Current Version	Next Version	Available Upgrade Method
4.5.x or 4.6.x	4.7.x	<ul style="list-style-type: none"> <li>• You can upgrade by using the management interface, see the updated <a href="#">Management interface upgrading</a> procedures.</li> <li>• Alternatively, you can upgrade by using the command-line interface, see the updated <a href="#">Command-line upgrading</a> procedures.</li> </ul>
4.4.x or 4.5.x	4.6.x	
4.3.x or 4.4.x	4.5.x	
4.2.x or 4.3.x	4.4.x	

Current Version	Next Version	Available Upgrade Method
4.0.x or 4.1.x	4.2.1	
3.0.x or 3.5.x	4.0	<ul style="list-style-type: none"> <li>You can upgrade by using the management interface, see the legacy <a href="#">Management Interface Upgrading</a> procedures.</li> <li>Alternatively, you can upgrade by using the command-line interface, see the legacy <a href="#">Command-Line Upgrading</a> procedures.</li> </ul>
3.0	4.0	You must upgrade only by using the command-line interface, see the legacy <a href="#">Command-Line Upgrading</a> procedures.

## IMPORTANT

### Interoperability with paired peer sites running earlier VMware Cloud Director Availability versions:

For information about interoperability between paired sites that run mismatching versions of VMware Cloud Director Availability, see [Paired sites versions interoperability](#).

- Before upgrading each VMware Cloud Director Availability appliance:
  - Ensure to take both backups and snapshots and follow the order of upgrading the cloud appliances, see [Appliances upgrade sequence and prerequisites](#).
  - Ensure that you have not manually enabled the Photon repository on any of the appliances. To verify for enabled repositories, open an SSH connection to each appliance, log in by using the **root** user credentials and run the following command:
 

```
yum -v repolist all | grep enabled
```

 When no repository is active, the command returns no result and you can proceed with the upgrade.
  - Ensure that you have not installed any packages or third-party software or made any manual modifications of `yum` configuration files.
- To complete the upgrade sequence follow [Post-upgrade configuration in the Cloud Director site](#).

## Upgrade Repository

To upgrade to the latest version of VMware Cloud Director Availability in the cloud site, you can configure each appliance to download the upgrade files from one of the following source repositories.

Source Repository	Description
An ISO image	Use an upgrade ISO file mounted in the virtual appliance CD-ROM drive for environments where the network restricts the appliances online Internet access.
A specified repository	<p>To upgrade multiple appliances or after deploying the appliances in different datastores, specify a repository as a content source:</p> <ul style="list-style-type: none"> <li>You can specify a local repository where you can upload the upgrade files, for environments where the network restricts the online Internet access to the appliances.</li> <li>Alternatively, with available Internet access, specify <code>https://packages-prod.broadcom.com/vcav/4.7/</code> as an online upgrade repository.</li> </ul>

## Appliances upgrade sequence and prerequisites

To successfully upgrade VMware Cloud Director Availability, first do all prerequisites steps then upgrade each appliance according to a specific order.

**IMPORTANT**

Verify that before starting the upgrade:

- Verify that the **backups** of all the appliances in the site are recent. For more information, see [Backing up and restoring in the Cloud Director site](#).
- Verify that current **snapshots** of all the appliances exist in the site.  
Take snapshots either with all the VMware Cloud Director Availability services stopped or with the appliances powered off.
- Verify that the sites are prepared for replication interruptions and Recovery Point Objective (RPO) violations.

After taking both backups and snapshots of all appliances, upgrade the sites running VMware Cloud Director Availability in the following order:

1. In the local cloud site, upgrade all the VMware Cloud Director Availability appliances.
2. In remote paired sites, upgrade all the VMware Cloud Director Availability appliances.

**NOTE**

Paired sites interoperability allows for two earlier versions compatibility. Features introduced in later versions cannot interoperate with earlier versions. For more information, see [Paired sites versions interoperability](#).

3. Upgrade all the on-premises appliances. For information about upgrading on-premises, see [Upgrading the on-premises site](#).

In a VMware Cloud Director Availability cloud site, upgrade all the appliances according to the following procedure:

1. Power off the Tunnel Appliance and all Replicator Appliance instances running in the local cloud site.

**NOTE**

Either now power them off when not planning to use the management interface for the upgrade, or alternatively you must power them off after starting the upgrade of the Cloud Director Replication Management Appliance during the **Upgrade** wizard, once the **Compatibility Check** page successfully passes all the checks for the paired sites. When these appliances are powered off before these checks pass, the **Compatibility Check** page shows a warning: *On Premises Replicators are going to become incompatible with this site after upgrade.* Also, on the same page the following expected error message shows for each paired site:

`Generic Network Error occurred on client side.`

2. Upgrade the Cloud Director Replication Management Appliance and after a successful upgrade, power off the appliance.

If the Cloud Director Replication Management Appliance upgrade fails, revert to the latest snapshot.

3. Power on a single Replicator Appliance instance.
  - a) Upgrade the Replicator Appliance instance.
  - b) After a successful upgrade, power off the upgraded Replicator Appliance instance.  
If the upgrade of a Replicator Appliance instance fails, revert to the latest snapshot.
  - c) Repeat this step for all the remaining Replicator Appliance instances in the local cloud site.

4. Power on the Tunnel Appliance.
  - a) Upgrade the Tunnel Appliance.
  - b) After a successful upgrade, power on the upgraded Cloud Director Replication Management Appliance and all the upgraded Replicator Appliance instances.

If the Tunnel Appliance upgrade fails, revert to the latest snapshot.

All the VMware Cloud Director Availability appliances in the local cloud site are upgraded and powered on.

5. Delete all snapshots.

**NOTE**

Any other snapshot operation except the ones described in the first prerequisite and in steps: 2, 3b, 4b, and 5 is not supported and can potentially break VMware Cloud Director Availability.

VMware Cloud Director Availability in the local cloud site is successfully upgraded.

After upgrading the local cloud site, the remote cloud sites, and upgrading the on-premises appliances, you can start using the new features of the upgraded VMware Cloud Director Availability version.

## Management interface upgrading

To upgrade to the latest VMware Cloud Director Availability version, you can use the management interface of each of the appliances, choose an upgrade repository then follow the management interface upgrade procedures according to the chosen repository.

### Upgrade by using the default repository

In the cloud appliances management interface, you can upgrade VMware Cloud Director Availability to the latest version by using the default VMware repository.

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances.
- Verify that each VMware Cloud Director Availability appliance has an external Internet access to the VMware repository.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance.

1. Log in to the service management interface of each VMware Cloud Director Availability appliance.
  - a) Open a Web browser and according to the upgrade order go to each management interface address.

Upgrade Order	VMware Cloud Director Availability Appliance	Management Interface Address
First	Cloud Director Replication Management Appliance	<a href="https://Appliance-IP-Address/ui/admin">https://Appliance-IP-Address/ui/admin</a>
Repeat for all instances	Replicator Appliance	<a href="https://Replicator-IP-Address/ui/admin">https://Replicator-IP-Address/ui/admin</a>
Last	Tunnel Appliance	<a href="https://Tunnel-IP-Address/ui/admin">https://Tunnel-IP-Address/ui/admin</a>

- b) Log in by using the **root** user credentials.
2. In the left pane, click **Settings**.
3. Under **Version**, next to **Product version** click **Check for updates**.
4. Upgrade the cloud appliance by completing the **Update** wizard.
  - a) On the **Repository** page, select **Use Official Online Repository** and click **Next**.
  - b) On the **Available updates** page, select an update and click **Next**.
  - c) On the **Release notes** page, read the notes for this release and click **Next**.
  - d) On the **Compatibility Check** page, check the paired on-premises appliances compatibility with the upgrade version and click **Next**.

If you powered off the Tunnel Appliance and all Replicator Appliance instances before starting the upgrade of the Cloud Director Replication Management Appliance, the following expected error message shows for each paired site:

```
Generic Network Error occurred on client side.
```

If you did not power them off until now, once these compatibility checks pass, power them off.

- e) On the **EULA Review** page, to accept the end user license agreement click **Next**.
- f) On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.

The upgrade process starts. Wait for the installation process to finish.

#### NOTE

If you see either of the following messages, wait a few minutes before attempting to log back in:

```
Timeout has occurred or Operation aborted due to an unexpected error.
```

5. After the appliance restarts, verify that the upgrade is successful.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Open the upgrade log file.
  - c) When upgrading to version 4.6.x, verify that the upgrade log contains the following log entry near the end.

```
'Postupgrade to 4.6.x complete.'
```

Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: `[date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]"), $0 }' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit: run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as unit: run-re595c8a07fe845bbb87e6c36f866caf2.service`

After validating that the upgrade is successful, repeat this procedure for the next appliance, until you upgrade all cloud appliances, according to the upgrade order in the table.

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade by completing the post-upgrade configuration.

## Upgrade by using a specified repository

In the cloud appliances management interface, you can upgrade VMware Cloud Director Availability to the latest version by specifying an online or a local repository that contains the upgrade binaries.

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances.
- Verify that each VMware Cloud Director Availability appliance has a network access to the specified repository.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance.

1. Optional: If the network restricts the appliances online Internet access, prepare a local repository with the upgrade files.
  - a) To host the upgrade files inside the internal network, install and configure a local Web server.
  - b) Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.
  - c) To access the image file contents, mount the downloaded `.iso` file to a local computer.
  - d) Copy the `update` directory to the local Web server.

The `update` directory contains the manifest files and the `dnf` subdirectory.

2. Log in to the service management interface of each VMware Cloud Director Availability appliance.
  - a) Open a Web browser and according to the upgrade order go to each management interface address.

Upgrade Order	VMware Cloud Director Availability Appliance	Management Interface Address
First	Cloud Director Replication Management Appliance	<code>https://Appliance-IP-Address/ui/admin</code>
Repeat for all instances	Replicator Appliance	<code>https://Replicator-IP-Address/ui/admin</code>

Upgrade Order	VMware Cloud Director Availability Appliance	Management Interface Address
Last	Tunnel Appliance	https://Tunnel-IP-Address/ui/admin

b) Log in by using the **root** user credentials.

3. In the left pane, click **Settings**.

4. Under **Version**, next to **Product version** click **Check for updates**.

5. Upgrade the cloud appliance by completing the **Update** wizard.

a) On the **Repository** page, to specify the repository containing the upgrade files select **Use Specified Repository**.

b) On the **Repository URL** text box, specify the repository URL address then click **Next**.

- If the appliance has Internet access, enter the following URL and specify the target version `https://packages-prod.broadcom.com/vcav/4.7/`.
- Alternatively, enter the URL address of the local repository pointing to the `update/dnf` directory of the local Web server. For example, enter `http://local-Web-server-address/update/dnf`.

c) On the **Available updates** page, select an update then click **Next**.

d) On the **Release notes** page, read the notes for this version then click **Next**.

e) On the **Compatibility Check** page, check the paired on-premises appliances compatibility with the upgrade version and click **Next**.

If you powered off the Tunnel Appliance and all Replicator Appliance instances before starting the upgrade of the Cloud Director Replication Management Appliance, the following expected error message shows for each paired site:

```
Generic Network Error occurred on client side.
```

If you did not power them off until now, once these compatibility checks pass, power them off.

f) On the **EULA Review** page, to accept the end-user license agreement click **Next**.

g) On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.

The upgrade process starts. Wait for the installation process to finish.

#### NOTE

If you see either of the following messages, wait a few minutes before attempting to log back in:

```
Timeout has occurred or Operation aborted due to an unexpected error.
```

6. After the appliance restarts, verify that the upgrade is successful.

a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.

b) Open the upgrade log file.

```
less /var/log/upgrade.log
```

c) When upgrading to version 4.6.x, verify that the upgrade log contains the following log entry near the end.

```
'Postupgrade to 4.6.x complete.'
```

```
Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: [date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]"), $0 }' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit: run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as unit: run-re595c8a07fe845bbb87e6c36f866caf2.service
```

```
The upgrade was successful! Scheduling reboot in 15 seconds.
```

After validating that the upgrade is successful, repeat this procedure for the next appliance, until you upgrade all cloud appliances in the cloud site, according to the upgrade order in the above table.

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade by completing the post-upgrade configuration.

## Upgrade by using an ISO image file

In the appliances management interface, you can upgrade VMware Cloud Director Availability to the latest version by using an `.iso` image file containing the upgrade binaries that you mount to the CD-ROM drive of the virtual appliances.

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances.
- Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance.

1. Copy the `.iso` file to a datastore that is accessible from the vCenter Server instance that you use with VMware Cloud Director Availability.
2. Mount the `.iso` file to each of the VMware Cloud Director Availability appliances.
  - a) Log in to the vSphere Client on the site where you want to upgrade VMware Cloud Director Availability.
  - b) Navigate to the virtual machine that hosts the VMware Cloud Director Availability appliance.
  - c) Right-click this virtual machine and select **Edit Settings**.
  - d) On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
  - e) Follow the prompts to add the CD/DVD drive to the VMware Cloud Director Availability virtual machine then select the **Connected** checkbox.
3. By using the appliances console, mount the `.iso` file inside the guest operating system of each of the VMware Cloud Director Availability appliances.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Mount the `.iso` file inside the guest operating system of each appliance.
 

```
mount /mnt/cdrom
```
4. Log in to the service management interface of each VMware Cloud Director Availability appliance.
  - a) Open a Web browser and according to the upgrade order go to each appliance management interface address.

Upgrade Order	VMware Cloud Director Availability Appliance	Management Interface Address
First	Cloud Director Replication Management Appliance	<code>https://Appliance-IP-Address/ui/admin</code>
Repeat for all instances	Replicator Appliance	<code>https://Replicator-IP-Addresses/ui/admin</code>

Upgrade Order	VMware Cloud Director Availability Appliance	Management Interface Address
Last	Tunnel Appliance	<code>https://Tunnel-IP-Address/ui/admin</code>

- b) Log in by using the **root** user credentials.
5. In the left pane, click **Settings**.
6. Under **Version**, next to **Product version** click **Check for updates**.
7. Upgrade this appliance by completing the **Update** wizard.
  - a) On the **Repository** page, select **Use CDROM Updates** then click **Next**.  
If you skipped mounting the image, you see an error message: Could not download the release manifest from file:///mnt/cdrom/update/rel-manifest.json. To continue, perform step 3.
  - b) On the **Available updates** page, select the update then click **Next**.
  - c) On the **Release notes** page, read the notes for this version then click **Next**.
  - d) On the **Compatibility Check** page, verify the paired on-premises appliances compatibility with the upgrade version then click **Next**.  
If you powered off the Tunnel Appliance and all Replicator Appliance instances before starting the upgrade of the Cloud Director Replication Management Appliance, the following expected error message shows for each paired site:  
  
`Generic Network Error occurred on client side.`  
If you did not power them off until now, once these compatibility checks pass, power them off.
  - e) On the **EULA Review** page, to accept the end-user license agreement click **Next**.
  - f) On the **Ready for update** page, confirm creating a backup by selecting the **I have created a backup archive of the appliance** checkbox then click **Finish**.  
The upgrade process starts. Wait for the installation process to finish.

**NOTE**

If you see either of the following messages, wait a few minutes before attempting to log back in:

```
Timeout has occurred OR Operation aborted due to an unexpected error.
```

8. After the upgrade finishes, verify that the upgrade is successful.
  - a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
  - b) Open the upgrade log file.  
`less /var/log/upgrade.log`
  - c) When upgrading to version 4.6.x, verify that the upgrade log contains the following log entry near the end.  
`'Postupgrade to 4.6.x complete.'`  
Once the following tailing lines are logged at the end of the log file, the appliance automatically reboots in 15 seconds: `[date-timestamp] # set -o pipefail; /usr/bin/systemd-run --on-active=15 /usr/sbin/reboot 2>&1 | /usr/bin/gawk '{ print strftime("[%Y-%m-%d %T %Z]", $0 )}' | tee -a /var/log/upgrade.log 1>&2 [date-timestamp] Running timer as unit: run-re595c8a07fe845bbb87e6c36f866caf2.timer [date-timestamp] Will run service as unit: run-re595c8a07fe845bbb87e6c36f866caf2.service`

9. Unmount the `.iso` file.
  - a) In the vSphere Client, shut down the virtual machine that hosts the appliance.
  - b) Right-click the virtual machine and select **Edit Settings**.
  - c) In the **Virtual Hardware** tab, select **CD/DVD Drive** and uncheck the **Connected** and the **Connect At Power On** checkboxes.
  - d) Power on the virtual machine that hosts the appliance.

After validating that the upgrade is successful, repeat this procedure for the next appliance, until you upgrade all appliances, according to the upgrade order in the above table.

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade by completing the post-upgrade configuration.

## Command-line upgrading

To upgrade to the latest VMware Cloud Director Availability version you can use the command-line interface of each of the appliances, choose an upgrade repository then follow the command-line upgrade procedures according to the chosen repository.

### Command-line upgrade by using an ISO image file

From the appliances command-line interface, you can upgrade VMware Cloud Director Availability to the latest version by using an `.iso` file containing the upgrade binaries that you mount to the CD-ROM drive of the virtual appliance.

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances.
- Download the `VMware-Cloud-Director-Availability-release.number.xxxxxxx-build_sha.iso` file, that contains the VMware Cloud Director Availability `release.number` Upgrade Disk Image.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance.

1. Copy the `.iso` file to a datastore that is accessible from the vCenter Server instance that you use with VMware Cloud Director Availability.
2. Mount the `.iso` file in a VMware Cloud Director Availability appliance.
  - a) Log in to the vSphere Client in the site where you want to upgrade VMware Cloud Director Availability.
  - b) On the **Home** page, click **Hosts and Clusters**.
  - c) Right-click the virtual machine that hosts the VMware Cloud Director Availability appliance and select **Edit Settings**.
  - d) On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
  - e) Follow the prompts to add the CD/DVD drive to the VMware Cloud Director Availability virtual machine then select the **Connected** checkbox.

Repeat this step to mount the `.iso` file in all remaining VMware Cloud Director Availability appliances.

3. Upgrade a VMware Cloud Director Availability appliance in the upgrade order from the following table.

#### NOTE

Proceed with the upgrade only after taking a snapshot of each cloud appliance.

Upgrade Order	VMware Cloud Director Availability Appliance
First	Cloud Director Replication Management Appliance
Repeat for all instances	Replicator Appliance

Upgrade Order	VMware Cloud Director Availability Appliance
Last	Tunnel Appliance

- a) Connect to the appliance console either by using a Secure Shell (SSH) client or by using the vSphere Client and log in as the **root** user.
- b) Mount the `.iso` file inside the guest operating system.

```
mount /mnt/cdrom
```

- c) Review the end-user license agreement (EULA) and if you accept the EULA, press `q`.

```
python3 /mnt/cdrom/update/iso-upgrade.py eula | less
```

- d) Install the upgrade.

```
python3 /mnt/cdrom/update/iso-upgrade.py
```

After successfully completing, the upgrade outputs both in the console and in the `/var/log/upgrade.log` file:

```
[date-timestamp] Postupgrade to 4.6.x complete.
Nothing to do.
Loaded plugin: tdnfrepogpgcheck
```

- e) After the upgrade completes, restart the appliance.

```
reboot
```

Repeat this step to upgrade all remaining VMware Cloud Director Availability appliances according the upgrade order.

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade by completing the post-upgrade configuration.

## Post-upgrade configuration in the Cloud Director site

After upgrading all VMware Cloud Director Availability appliances, in VMware Cloud Director reinstall the latest version of the VMware Cloud Director Availability plug-in by reentering the password of the VMware Cloud Director **System administrator** user.

Verify that each of the appliances of VMware Cloud Director Availability are successfully upgraded.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. Reinstall the latest version of the VMware Cloud Director Availability plug-in for VMware Cloud Director.

Skipping the plug-in installation in VMware Cloud Director results in the error message `The requested API version is not supported by the server`.

  - a) In the left pane under **Configuration**, click **Settings**.
  - b) Under **Service endpoints**, next to **VMware Cloud Director address** click **Edit**.
  - c) Enter the VMware Cloud Director endpoint URL as `https://VMware Cloud Director-IP-address:443/api`.
  - d) Enter the VMware Cloud Director **System administrator** user credentials and click **Apply**.  
For example, use `administrator@system`, where `system` is the VMware Cloud Director organization name.
  - e) Verify the thumbprint and accept the VMware Cloud Director SSL certificate.

The upgrade in the cloud site is complete and VMware Cloud Director Availability is ready for replications.

For information about daily operations like replicating workloads, see the *User Guide*.

# Administration Guide

---

VMware Cloud Director Availability™ performs replications at vApp or virtual machine level and is a unified solution, that provides on premises to cloud and cloud to cloud onboarding, migration, and disaster recovery for either multi-tenant Cloud Director sites or for vSphere DR and migration.

## **What is VMware Cloud Director Availability**

VMware Cloud Director Availability offers secure migration and disaster recovery capabilities either between multi-tenant cloud sites backed by VMware Cloud Director™ or between vCenter Server sites. VMware Cloud Director Availability provides simplified onboarding and ensures the continuous availability of VMware vSphere® workloads and automates the recovery operations.

VMware Cloud Director Availability gives the Partner Connect Program providers a converged way to protect and recover their tenants workloads and data and provides flexible workload migration to and from on-premises tenants resources and between provider cloud sites.

VMware Cloud Director Availability is a converged appliance-based solution that provides the following capabilities:

- Dedicated interfaces for the services deployment and for their management.
- For Cloud Director sites, VMware Cloud Director Availability integrates natively with VMware Cloud Director by using the VMware Cloud Director plug-in.
- Access for on-premises tenants by using the VMware Cloud Director Availability vSphere Client Plug-In
- Storage independence from vSphere.

Replication and migration features provided by VMware Cloud Director Availability:

- Full onboarding and migration capabilities from a single management interface.
- Tenant self-service protection, failover, and failback operations for each virtual machine or for each vApp.
- Self-service virtual machine migration from on-premises resources to cloud, cloud to on-premises resources, or cloud to cloud vApp, and virtual machine migrations between sites.
- Symmetrical replication and recovery flow that can be started from either the source or the recovery site.
- Automated inventory collection of virtual data centers, unprotected and protected vApps and virtual machines, storage profiles, and network configuration.
- Managed onboarding and disaster recovery capabilities for on-premises resources to cloud, and cloud to cloud scenarios.
- Automated tenant replication, migration, failover, and failback of vApps and operations after a failover.

When VMware Cloud Director Availability integrates with VMware Cloud Director, it forms a disaster recovery infrastructure where the organization controls operate as an activation-controlled policy that provides the disaster recovery capabilities for each tenant. The organization controls include Recovery Point Objective (RPO), snapshots, and number of permitted replications for the tenant disaster recovery.

Service level agreement (SLA) provided for replications with sites backed by VMware Cloud Director:

- 1 minute of minimum RPO.
- The RPO is customizable by the cloud provider.

Security features provided by VMware Cloud Director Availability:

- Encryption of the replication traffic by using end-to-end TLS encryption.
- The TLS session is terminated at each Replicator Appliance.
- Built-in optional compression of the replication traffic.

Day-2 operations and monitoring of VMware Cloud Director Availability:

- Policy-based management of the disaster recovery capabilities.
- Migration of tenants workloads from one VMware Cloud Director instance to another, for example, to set up a new data center.
- Temporary transfer of workloads to another VMware Cloud Director site, for example, to perform maintenance.
- Certificates and passwords management for the VMware Cloud Director Availability services and for the disaster recovery infrastructure.

### **How Does VMware Cloud Director Availability Work**

- In a cloud site backed by VMware Cloud Director, one or multiple Replicator Service instances, a Manager Service, a Cloud Service, and one or, optionally for high availability - two Tunnel Service instances all operate together to support the replication management, secure communication, and storage of the replicated data. The providers can support recovery for multiple tenant environments that can scale to handle increasing loads for each tenant and for multiple tenants.
- In a cloud vCenter Server site, a Replicator Service, a Manager Service, and a Tunnel Service all operate in a vCenter Replication Management Appliance. Additional Replicator Appliance instances can support performance scaling of the cloud site.
- In an on-premises site, a Replicator Service and a preconfigured Tunnel Service operate in either of the appliances, depending on the remote cloud site:
  - an On-Premises to Cloud Director Replication Appliance paired with a cloud site backed by VMware Cloud Director, or in
  - an On-Premises to Cloud vCenter Replication Appliance paired with a cloud vCenter Server site.
 The on-premises appliances supports replication management by using both the VMware Cloud Director Availability vSphere Client Plug-In and the VMware Cloud Director Availability Tenant Portal, dedicated to tenants.

For more information, go to the [VMware Cloud Director Availability documentation](#) and the [VMware Cloud Director Availability product](#) pages.

## **Administration in the Cloud Director site**

After installing and configuring VMware Cloud Director Availability in the cloud site backed by VMware Cloud Director, you can perform management and administrative tasks. The following tasks include changes to the provisioned environment and routine administration and maintenance procedures.

- **Cloud site backed by VMware Cloud Director:**
  - In a VMware Cloud Director Availability cloud site, backed by VMware Cloud Director, perform the following administration tasks in this current chapter by using the appliances management interface or in the disaster recovery infrastructure.
- **On-premises or provider vCenter Server sites:**
  - For information about VMware Cloud Director Availability in vCenter Server sites, see the [Administration in the on-premises and in the provider sites](#) chapter.

## Activate the data engines for replicating workloads

As **provider**, to replicate workloads between two sites, activate the supported data engines for starting new replications, depending on the source and the destination sites.

- Verify that for activating the **VMC** data engine, VMware Cloud Director Availability 4.2 or later is successfully deployed in the site, as earlier versions only support the **Classic** data engine.
- Verify that all the required network ports are open in the firewalls. For information about the required open ports, see: [VMware Ports and Protocols](#), or [Deployment Requirements On-Premises](#) and [Network Requirements](#).

### IMPORTANT

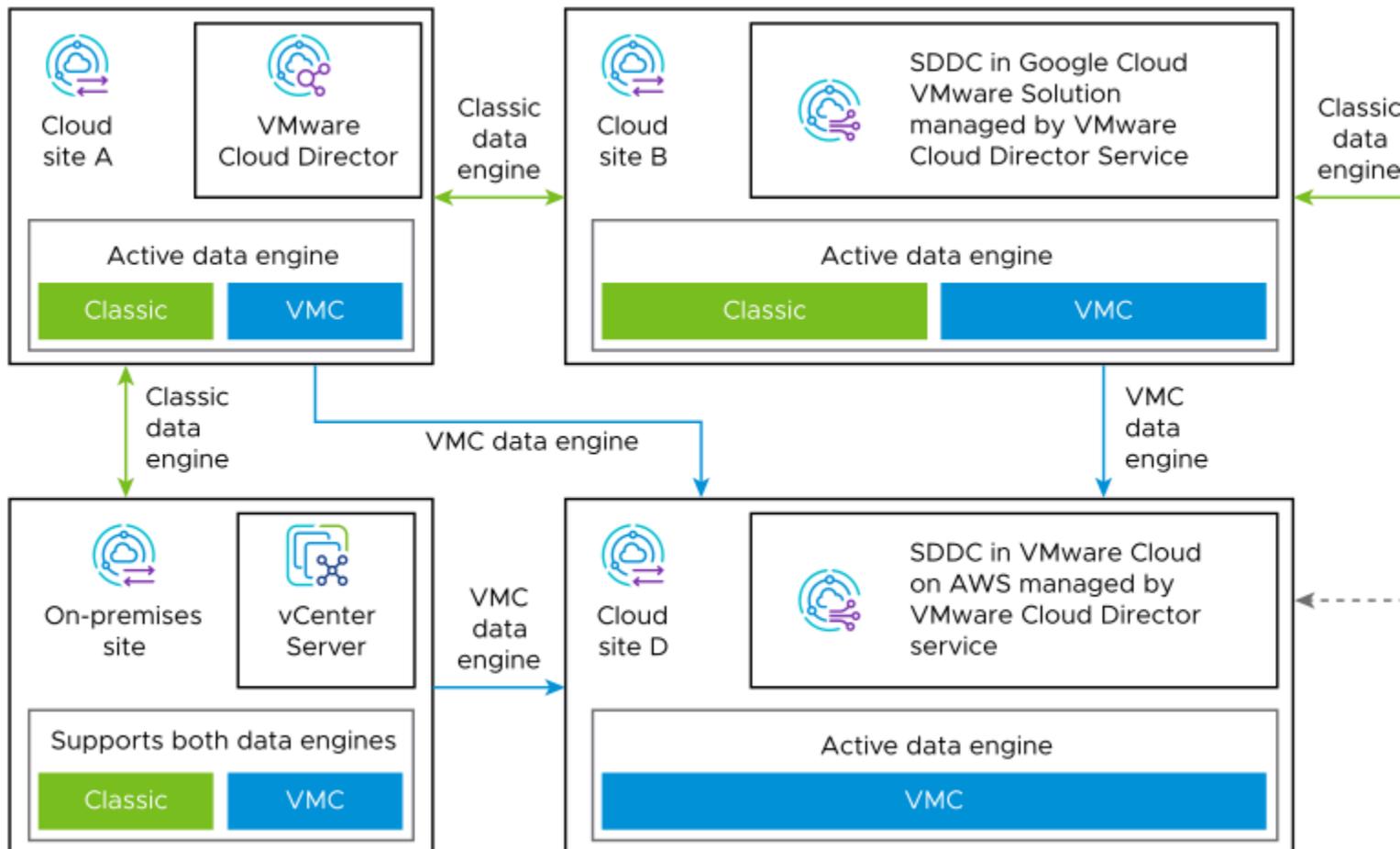
For information about the supported data engines, depending on the source and the destination site, see [Replications use cases](#).

At a replication start, VMware Cloud Director Availability checks whether the currently active data engines match between the source and the destination site:

- If both data engines are activated in both sites, then the **Classic** data engine takes precedence.
- If no available data engine matches between both sites, then the replication fails. In the following example diagram, only **Classic** data engine is active in the source site (Cloud site C) and only **VMC** is active in the destination site (Cloud site D) as is the only supported data engine for this site.

For example, in the following diagram the arrows indicate the replication direction and the used data engine:

**Figure 1: Activated data engines for replications between supported sites**



**NOTE**

Already started replications remain operational regardless of the active data engines. Activating a data engine affects only the start of new replications.

Deactivating a data engine that is used for replications which are already started, has no effect on them.

1. Log in to the management interface of the Cloud Director Replication Management Appliance.
  - a) In a Web browser, go to `https://Cloud-Director-Replication-Management-Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user password.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Site settings**, next to **Data engine** click **Edit**.
  - a) In the **Data engine** window, activate one or both data engines for replications:
    - **Classic** - supports both migrations and protections.
    - **VMC** - supports only migrations.
  - b) Click **Apply**.

The activated data engine in this site becomes available for handling new replications.

Once activated in both sites, you can create new replications that use this data engine between the two sites.

## Managing pairing with Cloud Director sites

The pairing management includes establishing and re-establishing trust with cloud sites backed by VMware Cloud Director. After you initiate pairing from the local site and complete the pairing from the remote site, VMware Cloud Director Availability establishes a trust between the two sites. Re-establish the trust after upgrading VMware Cloud Director Availability, after replacing the Cloud Service certificate, or after registering additional Replicator Service instances.

**REMEMBER**

As **provider** you must add each Cloud Service instance or each vCenter Replication Management Appliance for metering in VMware vCloud® Usage Meter before creating any replications. For information about adding the cloud sites in vCloud Usage Meter, see [vCloud Usage Meter Integration](#).

### Pairing Interoperability with Mismatching VMware Cloud Director Availability Versions

You can pair sites that have different VMware Cloud Director Availability major versions deployed, up to two major versions back, or  $(N-2)$ , where  $N$  is the currently deployed version.

For example, you can pair a site where version 4.7 is running with a site where version 4.5 or later is running, but not with a site where version 4.4 or earlier is running. Mismatching site versions can occur when upgrading the sites one at a time, or when migrating workloads from earlier vSphere and VMware Cloud Director versions to a site with later vSphere and VMware Cloud Director versions.

**NOTE**

When pairing sites with different VMware Cloud Director Availability major versions, only the functionality of the earlier version is supported.

For example, only the functionality and features of VMware Cloud Director Availability 4.5 are supported when pairing a site where version 4.5 is running with a site where version 4.7 is running.

Before pairing VMware Cloud Director Availability sites, verify the interoperability of the versions of VMware Cloud Director Availability between the source site and the destination site in the following tables:

**Table 5: Pairing Interoperability Between the Version of On-Premises to Cloud Director Replication Appliance the Version of the VMware Cloud Director Availability in the Cloud Director Site**

On-Premises to Cloud Director Replication Appliance	Cloud Site 3.0	Cloud Site 3.5	Cloud Site 4.0	Cloud Site 4.1	Cloud Site 4.2	Cloud Site 4.3	Cloud Site 4.4	Cloud Site 4.5	Cloud Site 4.6	Cloud Site 4.7
3.0	Supported	Supported	Supported	Unsupported						
3.5	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
4.0	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
4.1	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported
4.2	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported
4.3	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported
4.4	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported
4.5	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported
4.6	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported
4.7	Unsupported	Supported	Supported	Supported						

**NOTE**

Do not pair sites with more than two major versions apart.

For example, pairing version 4.7 with version 4.5 is supported but pairing version 4.7 with version 4.4 is not supported.

**Table 6: Pairing Interoperability Between the Version of VMware Cloud Director Availability in the Source Cloud Director Site and the Version of the VMware Cloud Director Availability in the Destination Cloud Director Site**

Source Cloud Site VMware Cloud Director Availability	Destination Cloud Site 3.0	Destination Cloud Site 3.5	Destination Cloud Site 4.0	Destination Cloud Site 4.1	Destination Cloud Site 4.2	Destination Cloud Site 4.3	Destination Cloud Site 4.4	Destination Cloud Site 4.5	Destination Cloud Site 4.6	Destination Cloud Site 4.7
3.0	Supported	Supported	Supported	Unsupported						
3.5	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
4.0	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported

Source Cloud Site VMware Cloud Director Availability	Destination Cloud Site 3.0	Destination Cloud Site 3.5	Destination Cloud Site 4.0	Destination Cloud Site 4.1	Destination Cloud Site 4.2	Destination Cloud Site 4.3	Destination Cloud Site 4.4	Destination Cloud Site 4.5	Destination Cloud Site 4.6	Destination Cloud Site 4.7
4.1	Unsup ported	Supported	Supported	Supported	Supported	Supported	Unsup ported	Unsup ported	Unsup ported	Unsup ported
4.2	Unsup ported	Unsup ported	Supported	Supported	Supported	Supported	Supported	Unsup ported	Unsup ported	Unsup ported
4.3	Unsup ported	Unsup ported	Unsup ported	Supported	Supported	Supported	Supported	Supported	Unsup ported	Unsup ported
4.4	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Supported	Supported	Supported	Supported	Supported	Unsup ported
4.5	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Supported	Supported	Supported	Supported	Supported
4.6	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Unsup ported	Supported	Supported	Supported	Supported
4.7	Unsup ported	Supported	Supported	Supported						

### IMPORTANT

When pairing sites, ensure that the latest maintenance patch release for the VMware Cloud Director Availability major version is deployed in each site.

- **Latest release:**

For each major version below, see the latest available release that must be deployed before pairing each site:

- For version 3.0, the site must be running version 3.0.5 or if later is available.
- For version 3.5, the site must be running version 3.5.2 or if later is available.
- For version 4.0, the site must be running version 4.0.1.2 or if later is available.
- For version 4.1, the site must be running version 4.1.1 or if later is available.
- For version 4.2, the site must be running version 4.2.1 or if later is available.
- For version 4.3, the site must be running version 4.3.1 or if later is available.
- For version 4.4, the site must be running version 4.4.1 or if later is available.
- For version 4.5, the site must be running version 4.5.0.1 or if later is available.
- For version 4.6, the site must be running version 4.6.1 or if later is available.

- **vSphere DR and migration between vCenter Server sites:**

This page is dedicated only for sites backed by VMware Cloud Director.

Alternatively, for information about pairing vSphere DR and migration between vCenter Server sites with mismatching VMware Cloud Director Availability versions, see the section [VMware Cloud Director Availability Supported Versions](#).

### **Migrating from Earlier VMware Cloud Director Availability Versions**

By pairing an earlier and later VMware Cloud Director Availability versions, you can migrate workloads from source sites where the later VMware Cloud Director Availability version does not support either the version of vCenter Server or VMware Cloud Director.

VMware Cloud Director Availability is fully capable of migrating workloads running on earlier vSphere and VMware Cloud Director versions that are near or are already EOS. If there is a VMware Cloud Director Availability version compatible with the vSphere and the VMware Cloud Director versions in the source site, you can pair it to VMware Cloud Director Availability 4.0 deployed in a cloud site with later vSphere and VMware Cloud Director versions. For example, see the following table:

**Table 7: Migration Interoperability with Paired Sites with Earlier VMware Cloud Director Availability Versions**

Migration Source Site Early Version	Migration Destination Site Latest Supported Version
On-premises site A, deployed version 3.5 with vSphere 5.5 or later.	Cloud site C, VMware Cloud Director Availability 4.1* with a supported VMware Cloud Director version**.
Cloud site B, deployed version 3.5 with vCloud Director 9.0 or 9.1.	
Cloud site Y, deployed version 3.0 with vCloud Director 8.2, 9.0 or 9.1.	Cloud site Z, VMware Cloud Director Availability 4.0* with a supported VMware Cloud Director version**.

**NOTE**

\* Migrating from a site running earlier version requires a specific version of VMware Cloud Director Availability in the destination site, that may not be the latest currently available, due to the pairing interoperability. For information about the pairing interoperability between the different VMware Cloud Director Availability versions, see the tables in the top section.

- For example, in an on-premises site with vSphere 5.5, deploy an on-premises appliance version 3.5 and pair it to VMware Cloud Director Availability 4.1 deployed in a cloud site with a supported VMware Cloud Director version\*\*. You can then migrate all virtual machines to the later cloud site.
- For example, in a cloud site with vCloud Director 9.0, deploy version 3.0 and pair it to VMware Cloud Director Availability 4.0 deployed in a cloud site with a supported VMware Cloud Director version\*\*. You can then migrate all vApps to the later VMware Cloud Director site.

**Supported Versions**

For the currently supported VMware Cloud Director Availability versions, see the [VMware Cloud Director Availability Documentation](#) page.

**VMware Cloud Director Availability Interoperability Matrices**

\*\* Before deploying VMware Cloud Director Availability in the cloud site, verify the supported versions of VMware Cloud Director and NSX by following the link below.

Before deploying On-Premises to Cloud Director Replication Appliance, verify the supported versions of vCenter Server, ESXi, and NSX by following the link below.

For information about the VMware Cloud Director Availability interoperability with other VMware products, see the [VMware Product Interoperability Matrix](#).

## Pair two Cloud Director sites

To initiate a trust establishment between two cloud sites backed by VMware Cloud Director, where each one runs a VMware Cloud Director Availability instance, first initiate pairing from either of the two sites. Then, to complete establishing the trust, repeat the pairing procedure in the remote site.

- Verify that, before pairing sites, the versions of VMware Cloud Director Availability in both sites can interoperate together. For information about the sites interoperability, see [Managing pairing with Cloud Director sites](#).
- Verify that in both cloud sites, all the VMware Cloud Director Availability appliances are successfully configured:
  - Cloud Director Replication Management Appliance
  - Replicator Appliance instances
  - Tunnel Appliance instances

To pair site A and site B, repeat the steps twice and perform the pairing procedure in both cloud sites:

1. In cloud site A, initiate pairing with a remote cloud site B.
  2. In cloud site B, repeat the procedure to complete pairing with site A.
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/ui/admin`.
    - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
    - c) Click **Login**.
  2. In the left pane under **Configuration**, click **Peer Sites**.
  3. On the **Peer Sites** page, click **New cloud pairing**.
  4. In the **New Cloud Pairing** window, configure the pairing with the remote cloud site, then to initiate the trust between the local and the remote cloud site, click **Pair**.

Option	Description
<b>Site name</b>	Enter a local site name, exactly matching the remote cloud site name.
<b>Public Service Endpoint</b>	<ul style="list-style-type: none"> <li>• Enter the public URL address of the Public Service Endpoint, external for the remote cloud site. For the network port, enter the externally DNAT-ed port, by default port 443. For example, enter <code>https://remote-vcda.provider.com:443</code>.</li> <li>• Only when the Tunnel Service instances are internally visible between both cloud sites, you can enter the internal URL address or the private IP address of the Tunnel Service and enter port 8048 for direct communication across the internal network.</li> </ul>
<b>Description</b>	Optionally, enter a description for the paired cloud site.

5. Complete the first half of the pair process.
  - a) Verify the thumbprint and accept the remote Cloud Service SSL certificate.
  - b) In the **Additional actions** required window, click **OK**.

VMware Cloud Director Availability initiates the trust between the two cloud sites.

Visit the Cloud Service in the *Site name* and repeat these steps to complete the pairing operation.
6. To complete the pairing between both sites, log in to the remote cloud site and repeat this procedure for pairing with the local site.
 

VMware Cloud Director Availability establishes the trust between the two cloud sites.

7. Under **Peer Sites**, verify that the new cloud site is listed and does not show any errors.
8. Before creating any replications, verify that as **provider** you added each Cloud Service instance for metering in VMware vCloud® Usage Meter.

For information about adding the cloud sites instances in vCloud Usage Meter, see [vCloud Usage Meter Integration](#).

After ensuring the Cloud Service instances are metered by vCloud Usage Meter, you can now start creating and managing replications. You can configure new replications, after modifying the default replication policy for both the source and for the destination organization to allow replications. Alternatively, a custom replication policy that is assigned to the source and to the destination organizations must allow replications. For information about the replication policy, see [Configuring replication policies](#) in the *User Guide*.

## Re-pair Cloud Director sites

After registering a Replicator Service instance, replacing the Cloud Service certificate, or upgrading VMware Cloud Director Availability in the local site, go to each paired remote site and re-pair each remote site with the local site backed by VMware Cloud Director.

To re-pair site A with site B, repeat the steps twice and perform the re-pairing procedure in both cloud sites:

1. In cloud site A, initiate re-pairing with a remote cloud site B.
  2. In cloud site B, complete re-pairing with site A.
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/ui/admin`.
    - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
    - c) Click **Login**.
  2. In the left pane under **Configuration**, click **Peer Sites**.
  3. In the **Peer Sites** page, select a remote cloud site for repairing with and click **Repair**.
  4. In the **Update Pairing** window, verify the pairing settings of the remote site and click **Update**.

Option	Description
<b>Site name</b>	Dimmed, as the site name cannot be changed.
<b>Public Service Endpoint</b>	Verify that the both the Public Service Endpoint address and the network port of the remote site are correct.
<b>Description</b>	Optionally, enter a description for the cloud site.

5. To complete the re-pair process, verify the thumbprint and accept the remote Cloud Service SSL certificate. The trust between the two sites is successfully reestablished.
6. Under **Peer Sites**, verify that the remote site shows as *Repaired*.

You reestablished the site trust and can configure new incoming and outgoing replications between the sites. You can configure new replications, after modifying the default replication policy for both the source and for the destination organization to allow replications. Alternatively, a custom replication policy that is assigned to the source and to the destination organizations must allow replications. For information about the replication policy, see [Configuring Replication Policies](#) in the *User Guide*.

## Unpair paired sites from the Cloud Director site

To remove the established trust between a VMware Cloud Director Availability cloud site backed by VMware Cloud Director and a paired cloud or on-premises site, delete the paired site from the cloud site.

Verify that all configured replications with the paired site are deleted.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Peer Sites**.
3. Remove the established trust with a cloud site.
  - a) In the **Cloud sites** page, select a cloud site and click **Delete**.
  - b) In the **Delete Peer Cloud Site** window, to remove the cloud site pairing, click **Delete**.You removed the pairing with the cloud site and removed the trust from both the local and the remote cloud sites.
4. Remove the established trust with an on-premises site from the cloud site.
  - If the on-premises site is still paired, now delete the pairing from the cloud site and then from the on-premises site, unpair the cloud site. For information about unpairing from the on-premises site, see [Unpair a remote site](#).
  - If from the on-premises site the cloud site is already unpaired, delete the remaining record in the cloud site.
  - a) Under **On-premises sites**, click **Delete**.
  - b) In the **Delete On-Premises Site** window, to remove the on-premises site pairing, click **Delete**.Above **On-premises sites** you see a green `On-Premises site deleted successfully` message.

You removed the cloud site trust with the on-premises site. If you performed this procedure from the cloud site first, in the on-premises site the cloud site still shows as paired. For more information, see [Unpair a remote site](#).

## Control the paired sites organization access

As **provider**, you control the peers each tenant sees by hiding certain cloud sites for specific organizations.

Verify that VMware Cloud Director Availability 4.7 is successfully deployed in the cloud site from where you apply the filter.

Tenants using a shared VMware Cloud Director instance usually have access only to some of the cloud sites paired to that instance. They might not be able to log in to those sites, but they see them. As **provider**, you can hide selected cloud peers for organizations that must not see or interact with. Once hidden, that cloud site is filtered from all views. For example, the **Dashboard**, the **Peer Sites** page, and others.

By default, all paired sites are visible for all organizations.

The on-premises sites are paired to certain organizations and are only visible to the respective tenants, therefore need no filtering.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Peer Sites**.
3. Select a remote cloud site to filter, then in the right pane next to **Organization Access**, click **Edit**.
4. In the **Organization Access** window, select the organizations that can access that site, then click **Apply**.
  - a) Optional: To pre-select the organizations that are associated with the remote site in VMware Cloud Director according to the multisite configuration, click **Use associated organization from vCloud**.  
For information about the organization association, see [Configure and Manage Multisite Deployments Using the VMware Cloud Director Tenant Portal](#).
  - b) Select the organizations that should have access to the remote cloud site.  
Only the selected organizations can monitor and manage replications on the filtered cloud site.

The tenants continue to operate only with the paired cloud sites to which you provided them with access.

- You can control the accessible provider virtual data centers for VMware Cloud Director Availability. For more information, see [Control the accessible provider virtual data centers](#).
- You can also control the administrative access to VMware Cloud Director Availability. For more information, see [Restricting the administrative sessions access by source IP](#).

## Restricting the administrative sessions access by source IP

By default, VMware Cloud Director Availability restricts the administrative sessions to all services when originating from public networks. As a **provider**, you can allow the administrative access from public networks.

The restriction applies to the following administrative accounts:

- Login sessions by using the appliance **root** user credentials.
- Login sessions by using VMware Cloud Director **system administrator** credentials.
- Login sessions by using a single sign-on user with vCenter Server **Administrator** credentials.

With restricted external administrative access, attempting to establish a login session from a public IP results in a `401 Not Authenticated` response. This response is identical to a wrong password error. To improve the appliance security further, the appliance denies the external administrative login session without counting it as an unsuccessful login attempt.

## Allow admin access from anywhere

In a dedicated appliance deployment, administrative sessions from public IPs are restricted to all VMware Cloud Director Availability services. If you need external administrative access, you can allow administrative sessions from public IP addresses.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Security settings**, next to **Restrict Admin APIs by source IP**, click **Edit**.
4. In the **Restrict Admin APIs by source IP** window, select **Allow admin access from anywhere** and click **Apply**.  
Under **Security settings**, next to **Restrict Admin APIs by source IP**, you see `Allow admin access from anywhere` listed.

The external administrative sessions to all VMware Cloud Director Availability services are enabled.

Revert the restriction after completing the external administrative operation. For more information, see [Do not allow admin sessions from the Internet](#).

## Do not allow admin sessions from the Internet

If you have enabled administrative access from public IPs, to improve the security you revert the restriction to its default value.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Security settings** next to **Restrict Admin APIs by source IP** click **Edit**.
4. In the **Restrict Admin APIs by source IP** window, select **Do not allow admin sessions from the Internet (recommended)** and click **Apply**.  
Under **Security settings**, next to **Restrict Admin APIs by source IP** you can see `Do not allow admin sessions from the Internet` listed.

The administrative sessions from public IPs to all VMware Cloud Director Availability services are restricted.

## Control the accessible provider virtual data centers

By default, VMware Cloud Director Availability can access all provider virtual data centers (pVDCs) that the VMware Cloud Director instance manages. As a **provider**, you can select the accessible provider VDCs for each VMware Cloud Director Availability instance.

### NOTE

In a multi-site deployment when the vCenter Server instances are in separate data centers but in the same SSO domain, the Replicator Service tries connecting to all vCenter Server instances in the SSO domain, even restricted provider VDCs. If this connectivity is not possible to some remote vCenter Server due to network

restrictions, navigating to **System Health** in the user interface can be slow and the logs can contain messages about connectivity problems.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Site details** next to **Accessible Provider VDCs**, click **Edit**.
4. In the **Accessible Provider VDCs** window, select **VMware Cloud Director Availability can access the following Provider VDCs** and activate the access for each provider VDCs that this VMware Cloud Director Availability instance can access.
 

VMware Cloud Director Availability now limits the visible inventory objects in replication wizards to the selected provider VDCs.

  - Tenants can create replications by using inventory objects that belong only to the selected provider VDCs.
  - You can also control the paired sites each tenant sees by hiding certain cloud sites for specific organizations. For more information, see [Control the paired sites organization access](#).

## Certificates management in the Cloud Director site

In a cloud site backed by VMware Cloud Director, when the SSL certificates are about to expire, the providers can renew or replace the certificates of the VMware Cloud Director Availability services and the certificates in the remaining disaster recovery infrastructure, or optionally, allow single sign-on to the services.

### Replacing the services certificates in the Cloud Director site

Each VMware Cloud Director Availability service uses a unique SSL certificate both for the HTTPS access to the service management interface and in the communication with other services. After renewing or replacing the certificate of a VMware Cloud Director Availability service, configure VMware Cloud Director Availability to trust the certificate.

In a typical cloud deployment, the VMware Cloud Director Availability solution comprises of three types of appliances that operate the following VMware Cloud Director Availability services:

- Cloud Director Replication Management Appliance operating the Cloud Service and the Manager Service.
- Replicator Appliance operating the Replicator Service.
- Tunnel Appliance operating the Tunnel Service.

The Tunnel Service effectively proxies the tenants communication with the Cloud Service. When connecting through the remote Tunnel Service, the On-Premises to Cloud Director Replication Appliance sees only the certificate of the remote Cloud Service and the tenants do not see the certificates of the remote Replicator Service nor the certificate of the remote Tunnel Service.

### Using a CA-Signed Certificate

Each VMware Cloud Director Availability service must have a unique certificate which is different from other services certificates. By default, the certificate is self-signed, or you can use a Certificate Authority (CA)-signed certificate. A

minimum requirement for the trusted communication is to install a trusted CA-signed certificate only for the Cloud Service, while the other services can continue to use self-signed certificates:

- Use a CA-signed certificate only for the Cloud Service. On the same Cloud Director Replication Management Appliance, you must use a self-signed certificate for the Replicator Service.
- Use self-signed certificates for the Tunnel Service and the Replicator Service. If the disaster recovery environment requires using only public certificates, you can also use CA-signed certificates for these two services.

### **Using a Wildcard Certificate**

You can use a wildcard certificate only for the Cloud Service. To keep the certificates unique, you must use self-signed certificates for the remaining VMware Cloud Director Availability services. Do not use the same wildcard certificate for more than one cloud site.

## **Managing the VMware Cloud Director Availability SSL certificates**

Certificates are part of the communication chain used to validate the hosts and are also used for the VMware Cloud Director Availability services management interfaces. To renew or to replace the certificates, you can import a CA-signed certificate or regenerate the self-signed certificate for each service of VMware Cloud Director Availability.

### **Regenerate a self-signed SSL certificate**

When the SSL certificate of a VMware Cloud Director Availability service expires, you can use the service management interface of that service to regenerate the certificate.

1. Log in to the VMware Cloud Director Availability management interface.
  - a) In a web browser, go to `https://Appliance-IP-address/ui/admin`.
  - b) Select **SSO login** or **Appliance login**, and enter the single sign-on or the **root** user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings**, next to **Certificate** click **Regenerate**.
4. In the **Regenerate Certificate** window, click **Apply**.

After the certificate is regenerated, all VMware Cloud Director Availability services that run on the same appliance restart. You can find the old certificate at `/opt/vmware/h4/serviceType/config/keystore.p12.bak`, where `serviceType` is `cloud`, `manager`, `replicator`, or `tunnel`.

### **Upload a CA-signed SSL certificate**

To prevent the Web browser from showing a certificate prompt every time a user opens the VMware Cloud Director Availability interface, you must upload an SSL certificate signed by a trusted certificate authority.

- Verify that the new PKCS#12 (`.pfx`) certificate file and the private key use the same password.
- Verify that the PKCS#12 file contains only one entry: the private key and its corresponding certificate and, optionally, the certificate trust chain. The trust chain must be part of the same keystore entry and must not be provided as separate entries in the PKCS#12 file.
- Verify that the RSA key size is 2048-bit or larger.
- Verify that the certificate does not use insecure hash algorithms, for example SHA1 and MD5.

- If using a wildcard certificate, use it only for the Cloud Service. Do not use the same certificate for any other VMware Cloud Director Availability service. For more information about wildcard certificates, see [Replacing the services certificates in the Cloud Director site](#).
1. Log in to the VMware Cloud Director Availability management interface.
    - a) In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
    - b) Select **SSO login** or **Appliance login**, and enter the single sign-on or the **root** user credentials.
    - c) Click **Login**.
  2. In the left pane under **Configuration**, click **Settings**.
  3. Under **Appliance settings** next to **Certificate**, click **Import**.
  4. In the **Import Certificate** window, enter the certificate details and click **Apply**.
    - a) Enter the password that protects the keystore and the certificate private key.
    - b) Click **Browse** and select the PKCS#12 file.

After you upload the CA-signed certificate, all VMware Cloud Director Availability services that run on the same appliance restart.

You can find the old certificate at `/opt/vmware/h4/serviceType/config/keystore.p12.bak`, where *serviceType* is `cloud`, `manager`, `replicator`, or `tunnel`.

### Replace the SSL certificate of the Cloud Service

Regenerate the Cloud Service self-signed SSL certificate or import a CA-signed certificate. After updating the certificate, re-establish the trust by re-pairing all cloud sites.

In VMware Cloud Director Availability 4.3 and later, replacing the Cloud Service certificate invalidates the trust only with the paired cloud sites. Replacing with a CA-signed certificate does not invalidate the trust with the paired on-premises sites and no longer requires re-pairing with on-premises sites.

To re-establish the trust with the cloud sites after replacing the certificate of the Cloud Service, re-pair with them.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. Replace the SSL certificate of the Cloud Service.
  - a) In the left pane under **Configuration**, click **Settings**.
  - b) Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

Import	Upload a CA-signed certificate.
Regenerate	Generate a new self-signed certificate.

- c) To update the Cloud Service certificate, click **Apply**.

You are logged out and the services automatically restart in a few minutes. After importing a CA-signed certificate, the Cloud Service creates a copy of the old certificate at `/opt/vmware/h4/cloud/config/keystore.p12.bak`.

3. In each paired cloud site, trust this new Cloud Service certificate.
  - a) In the left pane, click **Peer Sites**.
  - b) Select a cloud site and click **Repair**.
  - c) In the **Update Pairing** window, click **Update**.
  - d) To complete the trust re-establishment, accept the remote Cloud Service SSL certificate.

**NOTE**

Repeat this step and re-pair with the remaining cloud sites.

When not using a CA-signed certificate for the Cloud Service, re-pair the paired on-premises sites with this cloud site. For more information, see [Repair with a remote site](#).

**Replace the SSL certificate of the Manager Service**

Regenerate the Manager Service self-signed SSL certificate or import one. After updating this service certificate, repair the trust with the local Replicator Service instances and repair with all cloud sites.

In VMware Cloud Director Availability, replacing the Manager Service certificate:

- Invalidates the trust only:
  - with the paired cloud sites,
  - and with the Replicator Service instances in the local cloud site.
- On-premises sites that are paired automatically reestablish the trust after synchronizing or within 30 minutes. Re-pairing with on-premises sites is not necessary when replacing the SSL certificate of the Manager Service.

**Post-certificate replacement**

To re-establish the trust after replacing the certificate of the Manager Service, re-pair the registration of the Replicator Service instances in the local cloud site and re-pair with the cloud sites.

1. Log in to the Manager Service service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. Replace the SSL certificate of the Manager Service.
  - a) In the left pane under **Configuration**, click **Settings**.
  - b) Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

Import	Upload a certificate.
Regenerate	Generate a new self-signed certificate.

- c) To update the Manager Service certificate, click **Apply**.

You are logged out and the services automatically restart in a few minutes. After importing a certificate, the Manager Service creates a copy of the old certificate at `/opt/vmware/h4/manager/config/keystore.p12.bak`.

After applying the new certificate, all Replicator Service instances and on-premises appliances become offline. Repair all Replicator Service instances in the cloud site. The on-premises appliances restore operations automatically within 30 minutes without additional actions.

- Until the connectivity automatically restores, the tenants see the **Service connectivity** to the Manager Service as offline and all their replications are temporary in red health.
- After re-pairing with all the Replicator Service instances and their connectivity restores, the replications return back to green health.

Tenants do not have to perform additional actions with their on-premises appliances when the provider changes the Manager Service certificate as it only causes a temporary impact on the active replications.

3. Log in to the Manager Service service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
4. Trust the new Manager Service certificate with the remaining Replicator Service instances in the local cloud site.
  - a) In the left pane, click **Replicator Services**.
  - b) In the **Replicator Services administration** page, select each local Replicator Service instance and click **Repair**.
  - c) In the **Details for replicator** window, enter the **root** user password of the Cloud Director Replication Management Appliance, the single sign-on credentials and click **Apply**.
  - d) To complete the trust re-establishment, verify the thumbprint and accept the SSL certificate of this local Replicator Service instance.

**NOTE**

Repeat this step and trust the new certificate of the Manager Service by selecting the remaining Replicator Service instances.

5. Log in to the management interface of the Cloud Director Replication Management Appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
6. In each paired cloud site, trust this new Manager Service certificate.
  - a) In the left pane, click **Peer Sites**.
  - b) Select a cloud site and click **Repair**.
  - c) In the **Update Pairing** window, click **Update**.
  - d) To complete the trust re-establishment, accept the remote Cloud Service SSL certificate.

**NOTE**

Repeat this step and re-pair with the remaining cloud sites.

**Replace the SSL certificate of the Replicator Service**

When the certificate of the Replicator Service expires, you must replace it with the new self-signed or CA-signed certificate.

Verify that you are prepared to follow the steps in these procedures when replacing the certificate:

- [Regenerate a Self-Signed Certificate](#) or [Upload a CA-Signed Certificate](#).

Replacing the SSL certificate of the Replicator Service unregisters it from the Manager Service in the local and in the remote sites. To repair the registration of the Replicator Service to the Manager Service in the remote site, you must re-establish the trust between the cloud sites. For more information, see [Re-Pair Cloud Sites](#).

1. In a Web browser, go to the Replicator Service service management interface for your deployment type.

Deployment type	Service Management Interface
Cloud Director Combined Appliance	<code>https://Appliance-IP-Address:8440/ui/admin</code>
Replicator Appliance	<code>https://Replicator-Appliance-IP-Address/ui/admin</code>

- a) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - b) Click **Login**.
2. Log in as **root**.
  3. Generate or upload a new certificate.
  4. Re-pair the registration of Replicator Service instances to the Manager Service service on the local site.
    - a) Log in again to the Manager Service service management interface at `https://Replication-Manager-IP-address:8441/ui/admin`.  
On the **System Monitoring** tab all Replicator Service instances are *Offline*.
    - b) On the **Replicators** tab, select a Replicator Service instance and click **Repair**.
    - c) Enter the details of the Replicator Service instance and click **Apply**.

Option	Description
Appliance Password	The <b>root</b> user password for the Replicator Service appliance.
SSO User Name	A user name that has administrative privileges for the local site single sign-on domain, for example <i>Administrator@VSPHERE.LOCAL</i> .
SSO Password	The password for the administrative user.

- d) Accept the SSL certificate of the Replicator Service service.
  - e) Repeat steps b to d for all Replicator Service instances that are registered to the Manager Service service in the local site.
  - f) After you repair the registrations for all Replicator Service instances, verify that no connectivity errors are reported on the **System Monitoring** tab.
5. In the service management interface of the Cloud Service appliance, navigate to the **Sites** tab.
  6. Select a cloud site and click **Repair**.

#### NOTE

You must perform this step for each cloud site.

## Replace the SSL certificate of the Tunnel Service

When the certificate of the Tunnel Service expires, you must replace it with a new self-signed or a CA-signed certificate.

Verify that you are prepared to follow the steps in these procedures when replacing the certificate:

- [Regenerate a Self-Signed Certificate](#)
- [Upload a CA-Signed Certificate](#)

Replace the certificate of the Tunnel Service only in cloud sites.

1. In a Web browser, go to the Tunnel Service service management interface for your deployment type.

Deployment type	Service Management Interface
Cloud Director Combined Appliance	<code>https://Appliance-IP-Address:8442/ui/admin</code>
Tunnel Appliance	<code>https://Tunnel-Appliance-IP-Address/ui/admin</code>

- a) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - b) Click **Login**.
2. Log in as **root**.
  3. Generate or upload a new certificate.
  4. Log in to the management interface of the Cloud Director Replication Management Appliance.
    - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
    - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
    - c) Click **Login**.
  5. In the left pane under **Configuration**, click **Settings**.
  6. Under **Service Endpoints** next to **Tunnel Service address**, click **Edit**.
  7. In the **Tunnel Service Settings** window, click **Apply**.
  8. Verify the thumbprint and accept the new Tunnel Service SSL certificate.

After replacing the certificate of the Tunnel Service, on-premises and cloud sites might initially show a `Generic error occurred during TLS handshake` message for this Tunnel Service instance connectivity. Without further actions, within 30 minutes VMware Cloud Director Availability negotiates the certificate and restores the connectivity.

## Replacing external infrastructure certificates in the Cloud Director site

To allow single sign-on for the services or after renewing or replacing the vCenter Server Lookup service SSL certificate, or after changing the VMware Cloud Director endpoint or its certificate, configure the VMware Cloud Director Availability services to work with the new certificates.

### Configure to accept a renewed VMware Cloud Director endpoint or certificate

After changing the VMware Cloud Director endpoint or renewing its SSL certificate, configure VMware Cloud Director Availability to re-establish the trust with the new certificate and communicate securely with VMware Cloud Director.

- Verify that VMware Cloud Director Availability 4.5 or later is deployed for performing full certificate verification when a public certificate authority issued the VMware Cloud Director SSL certificate.
- Verify that the SSL certificate of VMware Cloud Director is successfully renewed. For information about generating and importing SSL certificates in VMware Cloud Director, see [VMware KB 1026309](#).

To re-establish the trust with VMware Cloud Director, in VMware Cloud Director Availability re-apply the endpoint with its address.

**NOTE**

- Since VMware Cloud Director Availability 4.5, when establishing a secure connection to VMware Cloud Director that uses an SSL certificate issued by a public certification authority (CA-issued), the Cloud Service performs complete certificate verification.  
For an existing deployment to use this functionality, first upgrade to version 4.5, then follow this procedure.
- Alternatively, the Cloud Service performs an exact certificate match when the certificate is not CA-issued. All previous VMware Cloud Director Availability versions also use this same behavior with any VMware Cloud Director SSL certificate, regardless of whether it is CA-issued.

1. Log in to the VMware Cloud Director Availability service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
  - b) Select **SSO login** or **Appliance login**, and enter the `single sign-on` or the **root** user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. To re-establish the trust, re-apply the address of the VMware Cloud Director endpoint.
  - a) Under **Service endpoints**, next to the VMware Cloud Director address click **Edit**.
  - b) Verify the URL of the VMware Cloud Director endpoint and click **Apply**.
  - c) Verify the thumbprint of the VMware Cloud Director certificate and click **Accept**.

VMware Cloud Director Availability re-establishes the trust with VMware Cloud Director.

**Configure the services to accept the vCenter Server Lookup service certificate and optionally allow SSO**

To optionally allow single-sign (SSO) on user authentication to the VMware Cloud Director Availability services, or after replacing the vCenter Server Lookup service certificate that is used as a replication source or destination, configure the VMware Cloud Director Availability services to trust the updated certificate.

- Verify that the SSL certificate is successfully renewed, and that the vCenter Server Lookup service is updated to use the renewed certificate.
- Verify that all infrastructure components in your environment that depend on the vCenter Server registration in the vCenter Server Lookup service are configured to trust the renewed certificate. An example of such a component is NSX Manager.
- By default, only the Replicator Service instances are configured with the vCenter Server Lookup service address for allowing single sign-on user authentication. During the initial configuration, the **Use the above Lookup Service address for Cloud, Manager, and Tunnel** toggle is inactive by default. For more information, see [Configure the Cloud Service in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

**NOTE**

To allow single sign-on for these services and resolve the `The service is not configured` message on the dashboard, configure them with the address of the vCenter Server Lookup service as in steps 2-4.

- Alternatively, after replacing the SSL certificate of the vCenter Server Lookup service, you must update all VMware Cloud Director Availability services configured with vCenter Server Lookup service to trust the updated certificate.
1. Configure the Replicator Service instance to work with the renewed vCenter Server Lookup service certificate.  
Repeat this step for all Replicator Service instances.
    - a) In a Web browser, go to the Replicator Service management interface at `https://Replicator-Appliance-instance-X-IP-address/ui/admin`.
    - b) Log in as the **root** user.
    - c) In the left pane, click **Settings**.
    - d) Under **Service endpoints**, next to **Lookup service address** click **Edit**.
    - e) In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.  
The details of the vCenter Server Lookup service certificate appear.

- f) Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.
  - g) In the left pane, click **System Health**.
  - h) To complete the Replicator Service configuration, click **Restart service**.
2. Optional: To allow using SSO login to the Cloud Service, configure it with the vCenter Server Lookup service address.
    - a) In a Web browser, go to the Cloud Service management interface at `https://Cloud-Replication-Management-IP-address/ui/admin`.
    - b) Log in as the **root** user.
    - c) In the left pane under **Configuration**, click **Settings**.
    - d) Under **Service endpoints**, next to **Lookup Service Address** click **Edit**.
    - e) In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.  
The details of the vCenter Server Lookup service certificate appear.
    - f) Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.
    - g) In the left pane, click **System Health**.
    - h) To complete the Cloud Service configuration, click **Restart service**.
  3. Optional: To allow using SSO login to the Manager Service, configure it with the vCenter Server Lookup service address.
    - a) In a Web browser, go to the Manager Service service management interface at `https://Cloud-Replication-Management-IP-address:8441/ui/admin`.
    - b) Log in as the **root** user.
    - c) In the left pane, click **Settings**.
    - d) Under **Service endpoints**, next to **Lookup Service Address** click **Edit**.
    - e) In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.  
The details of the vCenter Server Lookup service certificate appear.
    - f) Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.
    - g) In the left pane, click **System Health**.
    - h) To complete the Manager Service configuration, click **Restart service**.
  4. Optional: To allow using SSO login to the Tunnel Appliance, configure it with the vCenter Server Lookup service address.
    - a) In a Web browser, go to the Tunnel Appliance management interface at `https://Tunnel-Appliance-IP-address/ui/admin`.
    - b) Log in as the **root** user.
    - c) In the left pane, click **Settings**.
    - d) Under **Service endpoints**, next to **Lookup Service Address** click **Edit**.
    - e) In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.  
The details of the vCenter Server Lookup service certificate appear.
    - f) Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.
    - g) In the left pane, click **System Health**.
    - h) To complete the Tunnel Service configuration, click **Restart service**.

## Network settings configuration

After completing a VMware Cloud Director Availability appliance deployment, as a **system administrator** you can modify the network settings of the appliance by using the management interface.

### Host Name Configuration

During the OVF deployment, as a **system administrator**, you can manually provide the appliance host name. If you skip this step, the DHCP server provides the host name. Some DHCP servers are not configured to provide a host name or do

not support host name provisioning. In such cases, the appliance attempts to find the host name and performs a reverse DNS lookup by using the first non-link-local IP address of the default ens160 Ethernet adapter. If the request is successful, the appliance uses the provided domain name as a host name and ignores future host names received over DHCP. If the request is not successful, the appliance uses *photon-machine* as a host name.

After the deployment completes, you can modify the host name of the appliance by using the appliance management interface. Configuring a new host name overwrites the host name that is provided by DHCP.

## **DNS Settings Configuration**

As a **system administrator**, you can configure the provisioning of DNS servers and Domain Search Path in manual or automatic mode.

### **Manual**

As a **system administrator**, you must provide the static DNS settings.

### **Automatic**

The DHCP server or Stateless Address Autoconfiguration (SLAAC) provides the DNS settings.

During the OVF deployment, you can manually provide the DNS settings. If you skip this step, the appliance uses the DNS settings provided by the DHCP server.

After the deployment completes, you can modify the DNS settings of the appliance by using the appliance management interface. When you provide the static DNS settings manually, all network adapters are configured to ignore the DNS settings that are provided by DHCP or SLAAC. Alternatively, you can switch to automatic mode by configuring one or more network adapters to use DHCP or SLAAC. Switching from manual to automatic mode overwrites all static DNS settings.

## **Network Adapter Configuration**

During the OVF deployment, as a **system administrator**, you can provide the network adapter settings. If you do not populate the IP address, the adapter uses DHCPv4. After the deployment completes, you can change the adapter settings provided during deployment.

You can configure the network adapters in VMware Cloud Director Availability to use either IPv4 or IPv6 modes. You can provide the adapter settings manually or alternatively the settings can be received by using one of the following automatic mechanisms.

### **Manual**

The manual adapter configuration requires you to provide a valid Classless Inter-Domain Routing (CIDR) static address. Enter the CIDR address as an IP address, followed by a forward slash and a network mask or a prefix length. You can also set a default gateway, that must be in the same network as the provided IP address. If a second adapter is configured manually with the same IP mode, skip setting the default gateway. You can also configure the maximum transmission unit (MTU), and if omitted, the appliance uses an MTU of 1500 bytes. You can set the static address, gateway, and MTU adapter settings for both IPv4 and IPv6 modes.

### **Automatic**

DHCPv4, DHCPv6, or SLAAC can provide the automatic adapter configuration, depending on the IP mode.

By using DHCPv4 or DHCPv6, the network adapter is configured to:

- Use the DNS servers that are provided by the DHCP server.
- Use the search domains that are provided by the DHCP server.
- Ignore all routes that are provided by the DHCPv4 server, if the appliance has a default gateway configured.
- Remove all manually configured DNS settings such as DNS servers and search domains.
- Remove custom MTU settings.

By using SLAACv6, the network adapter is configured to:

- Enable IPv6 link-local addressing.
- Accept IPv6 Router Advertisement (RA).
- Accept DNS servers and search domains through RA.
- Remove all manually configured DNS settings such as DNS servers and search domains.
- Remove custom MTU settings.

Additional notes for the network adapter configuration:

- If there are multiple sources of DNS settings, for example two NICs that use two different DHCP servers, the DNS requests are sent to all DHCP servers. The appliance uses the first one that responds. To avoid potential issues, you must ensure that there are no conflicting settings. As a best practice, avoid such a configuration.
- To remove the configuration of the network adapter, you must click **Unconfigure** next to the IP mode. This action turns off the adapter and deletes all its settings, including static routes. Later, you can configure the adapter again, which turns it back on. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.
- To change the manually configured default gateway, you must first remove the configuration of the network adapter that is configured with it.
- The upgrade to VMware Cloud Director Availability 4.0 attempts to migrate the network configuration of the old eth0 adapter. If using both IP modes before the upgrade, after the upgrade only one of them is enabled. Also, the upgrade replaces the eth0 adapter with the ens160 adapter.
- The appliance MTU size must match and must not exceed the MTU allowed in the network infrastructure environment.

### **Static Routes Configuration**

VMware Cloud Director Availability 4.0 allows you as a **system administrator** to configure static routes that control how the network packets are sent to the destination.

In a typical environment, there is a default gateway that dynamically routes all the traffic to and from the external networks. Sometimes, you might want to route the traffic through another gateway. For example, you can use static routes when there is no dynamic route to the destination IP address, or when you want to override the dynamically learned route. To address such network setup, you can configure one or more static routes.

#### **NOTE**

Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

### **Configure the network settings of the appliance**

As a **system administrator**, you can modify the host name, the DNS servers, and the Domain Search Path by using the management interface of the VMware Cloud Director Availability appliance.

---

Verify that VMware Cloud Director Availability is successfully deployed.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user password.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings** next to **Network**, click **Edit**.
4. In the **Network Settings** window, configure the network settings and click **Apply**.
  - a) Enter the appliance host name.
  - b) Enter the static DNS servers as a comma-separated list of DNS server addresses.
  - c) Enter the static Domain Search Path as a comma-separated list of search domains.Manually configuring the network settings overwrites the configuration provided by DHCP or by SLAAC.

The VMware Cloud Director Availability appliance now uses the network settings that you configured.

- You can configure the network adapters. For more information, see [Configure a network adapter](#).
- You can use the local domain as a top-level domain in VMware Cloud Director Availability appliances. For more information, see [VMware KB 79088](#).

## Configure a network adapter

As a **system administrator**, you can modify the network adapter settings, such as IP Mode and type, address, gateway, and MTU by using the management interface of the VMware Cloud Director Availability appliance.

Verify that VMware Cloud Director Availability is successfully deployed.

### NOTE

Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Under **Appliance login**, enter the **root** user password.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings**, expand the **Network** section.

You can see all the network adapters that are added to the appliance.

4. Next to the adapter name click **Edit**.
5. In the **Settings** window, configure the network settings and click **Apply**.
  - a) To select an IP mode, click **IPv4**, **IPv6**, or **Unconfigured**.

By selecting **Unconfigured**, you turn off the adapter and delete all its settings, including static routes. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.

- b) Click **Type** and select how to provide the network configuration.

Option	Description
DHCP	If you select DHCP to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed.
SLAAC	If you select SLAAC to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed.
Static	<p>Enter the static configuration.</p> <ol style="list-style-type: none"> <li>1. In the <b>Address/Prefix</b> text box, enter a CIDR address - IP address, followed by a forward slash and a network mask or a prefix length.</li> <li>2. In the <b>Gateway</b> text box, enter a gateway that is in the same network as the provided IP address. For each IP mode, you can use only one default gateway. If you are configuring a second adapter in the same IP mode, you must not enter a default gateway.</li> <li>3. In the <b>MTU (bytes)</b> text box, enter the maximum transmission unit size in bytes. The default is 1500 bytes.</li> </ol>

The selected network adapter of the VMware Cloud Director Availability appliance is configured with the provided settings.

- You can configure the DNS, the appliance host name, and the Domain Search Path. For more information, see [Configure the network settings of the appliance](#).
- You can add additional network adapters to configure. For more information, see [Add an additional network adapter](#).
- You can use the local domain as a top-level domain in VMware Cloud Director Availability appliances. For more information, see [VMware KB 79088](#).

## Configure static routes

To route the network packets through a specific gateway, as a **system administrator** you can configure static routes by using the management interface of the VMware Cloud Director Availability appliance.

Verify that VMware Cloud Director Availability is successfully deployed.

**NOTE**

Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user password.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings**, expand the **Network** section.  
You can see all the network adapters that are added to the appliance.
4. To configure the static routes for a network adapter, next to the adapter name click **Static routes**.  
The static routes are persistent for the selected IP mode of the adapter. If you change the IP mode, all static routes are deleted.
5. In the **Static routes** window, configure the static routes for the selected network adapter.  
The routes that the management interface shows do not contain the whole routing table. The management interface only shows the manually configured routes.
  - a) To add a new static route, enter the following route details and click **Add**.

Option	Description
Destination	You must enter the specific IP address or the whole subnet of the target network.
Gateway	You must enter the IP address of the specific gateway that knows how to route the traffic.
Metric	You can enter a lower value to prioritize the route or a higher value to deprioritize the route. As a best practice, avoid the route prioritization and use the default value of 0.

- b) To remove a static route, click **Delete**.  
To edit a static route entry, you must delete it and add it again.
- c) To apply the network changes, click **Apply**.

The selected network adapter of the VMware Cloud Director Availability appliance is configured with the provided static routes.

You can add additional network adapters to add routes to. For more information, see [Add an additional network adapter](#).

## Add an additional network adapter

As a **system administrator**, you can configure additional network adapters by using the vSphere Client. The newly added adapters can be later configured by using the management interface of the VMware Cloud Director Availability appliance.

Verify that the VMware Cloud Director Availability appliance is successfully deployed.

1. Log in to the vCenter Server instance by using the vSphere Client.
2. Navigate to the VMware Cloud Director Availability virtual machine.
3. Right-click the VMware Cloud Director Availability virtual machine and from the drop-down menu select **Edit Settings**.
4. In the **Edit Settings** window, click **Add new device > Network Adapter**.
5. Select the appropriate network.
6. Select **VMXNET 3** as the adapter type and **Automatic** for the MAC address.
7. Verify that **Connected** is selected and click **OK**.  
The VMware Cloud Director Availability virtual machine is configured with the new adapter.
8. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.  
Use the IP address of the previously existing network adapter.
  - b) Select **Appliance login** and enter the **root** user password.
  - c) Click **Login**.
9. In the left pane, click **Settings**.
10. Under **Appliance settings**, expand the **Network** section.  
You can see all the network adapters that are added to the appliance. The newly added adapter is listed as **Unconfigured**.

You can configure the new network adapter. For more information, see [Configure a network adapter](#).

## Select the endpoint address for each network adapter

Control which network interface the appliance uses for specific communication traffic by selecting the endpoint address. In the Tunnel Appliance, select the address for communication with the local cloud appliances. In each Replicator Appliance instance, select the addresses for management traffic, and for incoming and for outgoing replication traffic.

Verify that VMware Cloud Director Availability 4.3 or later is deployed in the cloud site.

Selecting the endpoint addresses controls the type of traffic the cloud appliances expect on which network interface cards (NICs). The traffic control allows for more specific network topologies and is not intended for traffic isolation between the data and the management network traffic.

### NOTE

- Selecting endpoint address associates it with the IP address. To apply a new endpoint address after the selected IP address changes, manually select the updated IP address for the endpoint re-association.
- The selected IP address for each endpoint must be configured with a static IP address.

### Tunnel Appliance

In the management interface of the Tunnel Appliance, to control the internal traffic in the site you can select an endpoint address for the communication from the Replicator Appliance instances and from the Cloud Director Replication Management Appliance to the Tunnel Appliance, avoiding their communication over the external-facing Tunnel Appliance address. Controlling the Tunnel Appliance traffic avoids routing the traffic from the local cloud appliances through the Internet-facing NIC of the Tunnel Appliance.

### Replicator Appliance instances

In the management interface of each Replicator Appliance instance, to control the traffic you can select the following endpoint addresses.

- For management traffic, between the local cloud appliances in the site.
- For outgoing replication data traffic, to the destination ESXi hosts.
- For incoming replication data traffic, from the source ESXi hosts.

When the Replicator Appliance instances are on a separate network from the ESXi hosts or the Tunnel Appliance, selecting these endpoints directly routes the heavy replication data traffic avoiding the router and reducing the impact over the entire internal infrastructure network.

1. Select the Tunnel Appliance endpoint address for controlling the traffic from the local cloud appliances.
  - a) In a Web browser, go to `https://Tunnel-Appliance-IP-Address`.  
The `https://Tunnel-Appliance-IP-Address/ui/admin` login page opens.
  - b) Enter the password of the **root** user and click **Login**.  
The **Settings** page opens.
  - c) Under **Appliance settings**, click **Edit** next to the **Traffic Control** section.  
The **Traffic Control** window opens.
  - d) From the **Tunnel Address** drop-down menu, select the endpoint IP address for the communication from the local cloud appliances and click **Apply**.
2. Select the Replicator Appliance instance endpoint addresses for controlling the management traffic and the traffic from the local ESXi hosts.
  - a) In a Web browser go to `https://Replicator-Appliance-IP-Address`.  
The `https://Replicator-Appliance-IP-Address/ui/admin` login page opens.
  - b) Enter the password of the **root** user and click **Login**.  
The **System Health** page opens.
  - c) In the left pane, click **Settings**.
  - d) Under **Appliance settings** click **Edit** next to the **Traffic Control** section.  
The **Traffic Control** window opens.
  - e) From the **Management Address** drop-down menu, select the endpoint IP address for the management traffic between the local cloud appliances, where the Tunnel Appliance redirects all traffic when not setting a specific data endpoint.
  - f) From the **NFC Address** drop-down menu select the endpoint IP address for the outgoing Network File Copy (NFC) traffic to the destination ESXi host. All outgoing data traffic to the ESXi hosts goes through this endpoint address.
  - g) From the **LWD Address** drop-down menu select the endpoint IP address for the incoming Lightweight Delta Protocol (LWD) traffic. This endpoint address receives the incoming data traffic from the local source ESXi host.
  - h) To confirm the selected endpoint addresses, click **Apply**.

Repeat this step for the remaining Replicator Appliance instances in the cloud site.

3. After configuring all Replicator Appliance instances, in the Cloud Director Replication Management Appliance enable tunneling to the new Tunnel Appliance endpoint address.
  - a) In a Web browser, go to `https://Cloud-Replication-Management-Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
  - d) In the left pane under the **Configuration** section, click **Settings**.
  - e) Under **Service endpoints**, next to **Tunnel Service address** click **Edit**.
  - f) In the **Tunnel Service Settings** window, enter the **root** user password of the Tunnel Appliance.  
The **Tunnel Service Endpoint address** is already populated and the **Appliance user** is set to **root**.
  - g) Click **Apply**.
  - h) Verify the thumbprint and accept the certificate of the Tunnel Service.

The selected endpoint addresses control the incoming and outgoing traffic.

You can ensure that the selected endpoint addresses do not affect the VMware Cloud Director Availability connectivity. For more information, see [Verify uptime and local and remote connectivity in the Cloud site](#).

## Command-line network configuration

If the management interface is not available, as a **system administrator**, you can configure all network settings by using the command-line interface of the VMware Cloud Director Availability appliance.

- Verify that the VMware Cloud Director Availability appliance is successfully deployed.
- Verify that before running any of the following commands, you understand the general network configuration in VMware Cloud Director Availability. For more information, see [Network settings configuration](#).



### CAUTION

Only use the following `net.py` commands in case you cannot access the management interface.

You must not use any other command-line network configuration, for example: the `ip` command, VAMI scripts, must not manually modify configuration files, and other network settings. Do not automate or use in scripts the `net.py` commands.

You can run the following `net.py` commands in any order.

1. Connect to the VMware Cloud Director Availability by using a Secure Shell (SSH) client.
  - a) Open an SSH connection to `Appliance-IP-Address`.
  - b) Log in as the **root** user.
2. To retrieve all available network adapters, run: `/opt/vmware/h4/bin/net.py nics-status`.

```
$ /opt/vmware/h4/bin/net.py nics-status
[
  {
    "addresses": [
      "fe80::250:56ff:fea9:7c8c/64"
    ],
    "configMode": "SLAAC_V6",
    "gateway": null,
    "mac": "00:50:56:a9:7c:8c",
    "mtu": 1500,
    "name": "ens192",
    "state": "degraded (configured)"
  },
  {
```

```

    "addresses": [
      "10.71.218.128/21"
    ],
    "configMode": "DHCP_V4",
    "gateway": "10.71.223.253",
    "mac": "00:50:56:a9:0e:65",
    "mtu": 1500,
    "name": "ens160",
    "state": "routable (configured)"
  }
]

```

3. To retrieve the status of a specific network adapter, run: `/opt/vmware/h4/bin/net.py nic-status<adapter-name>`.

```

$ /opt/vmware/h4/bin/net.py nic-statusens160
{
  "addresses": [
    "10.71.218.128/21"
  ],
  "configMode": "DHCP_V4",
  "gateway": "10.71.223.253",
  "mac": "00:50:56:a9:0e:65",
  "mtu": 1500,
  "name": "ens160",
  "state": "routable (configured)"
}

```

4. To turn off a specific network adapter and delete all its settings, including static routes, run: `/opt/vmware/h4/bin/net.py unconfigure-nic<adapter-name>`.

```

$ /opt/vmware/h4/bin/net.py unconfigure-nicens192
{
  "addresses": [],
  "configMode": "UNCONFIGURED",
  "gateway": null,
  "mac": "00:50:56:a9:7c:8c",
  "mtu": 1500,
  "name": "ens192",
  "state": "off (unmanaged)"
}

```

5. To configure a specific network adapter to use DHCPv4, run: `/opt/vmware/h4/bin/net.py configure-nic<adapter-name>--dhcp4`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```

$ /opt/vmware/h4/bin/net.py configure-nicens192--dhcp4
{
  "addresses": [],
  "configMode": "DHCP_V4",
  "gateway": null,
  "mac": "00:50:56:a9:7c:8c",
  "mtu": 1500,
  "name": "ens192",

```

```

    "state": "carrier (configuring)"
  }

```

6. To configure a specific network adapter to use DHCPv6, run: `/opt/vmware/h4/bin/net.py configure-nic<adapter-name>--dhcp6`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```

$ /opt/vmware/h4/bin/net.py configure-nicens192--dhcp6
{
  "addresses": [],
  "configMode": "DHCP_V6",
  "gateway": null,
  "mac": "00:50:56:a9:7c:8c",
  "mtu": 1500,
  "name": "ens192",
  "state": "no-carrier (configuring)"
}

```

7. To configure a specific network adapter to use SLAAC, run: `/opt/vmware/h4/bin/net.py configure-nic<adapter-name>--slaac`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```

$ /opt/vmware/h4/bin/net.py configure-nicens192--slaac
{
  "addresses": [],
  "configMode": "SLAAC_V6",
  "gateway": null,
  "mac": "00:50:56:a9:7c:8c",
  "mtu": 1500,
  "name": "ens192",
  "state": "no-carrier (configuring)"
}

```

8. To configure a specific network adapter to use a static IP, run: `/opt/vmware/h4/bin/net.py configure-nic<adapter-name>--static--address<CIDR>--gateway<IP>--mtu<MTU-bytes>`.

```

$ /opt/vmware/h4/bin/net.py configure-nicens192--static--address172.16.0.2/18--gateway172.16.0.1--mtu1400
{
  "addresses": [
    "172.16.0.2/18"
  ],
  "configMode": "DHCP_V4",
  "gateway": "172.16.0.1",
  "mac": "00:50:56:a9:0e:65",
  "mtu": 1400,
  "name": "ens192",
  "state": "routable (configured)"
}

```

9. To see the manually configured static routes list for a specific network adapter, run: `/opt/vmware/h4/bin/net.py list-routes<adapter-name>`.

```

$ /opt/vmware/h4/bin/net.py list-routesens192

```

```
[
  {
    "destination": "1.2.3.4",
    "gateway": "5.6.7.8",
    "metric": 0
  },
  {
    "destination": "10.0.0.0/16",
    "gateway": "9.9.9.9",
    "metric": 0
  },
  {
    "destination": "40.40.40.40",
    "gateway": "50.50.50.50",
    "metric": 0
  }
]
```

10. To add a static route to a specific network adapter, run: `/opt/vmware/h4/bin/net.py add-route<adapter-name> <destination IP or subnet CIDR> <gateway> <optional-metric>`.

```
$ /opt/vmware/h4/bin/net.py add-routeens160 99.99.99.99 10.0.0.42
```

```
[
  {
    "destination": "99.99.99.99",
    "gateway": "10.0.0.42",
    "metric": 0
  }
]
```

11. To remove a static route from a specific network adapter, run: `/opt/vmware/h4/bin/net.py remove-route<adapter-name> <destination IP or subnet CIDR> <gateway> <metric>`.

Ensure that the destination IP, gateway, and metric exactly match the rule to delete.

```
$ /opt/vmware/h4/bin/net.py remove-routeens160 99.99.99.99 10.0.0.42
```

```
[]
```

## Stretching layer 2 networks in the Cloud Director site

During on-premises to the cloud migrations, to allow network connectivity between already migrated and not yet migrated virtual machines as in the same network segment, stretch the on-premises networks across the cloud site. Layer 2 VPN (L2 VPN) stretches the L2 networks across the sites.

### VMware Cloud Director Availability L2 Stretch

By using NSX and its L2 VPN service technology, VMware Cloud Director Availability stretches on-premises L2 networks across the cloud site.

#### Cloud Site

To establish the server L2 VPN session, VMware Cloud Director Availability 4.2 uses VMware NSX. In addition to NSX, VMware Cloud Director Availability 4.2.1 and later also support VMware NSX® Data Center for vSphere® for stretching the L2 network.

#### On-Premises Site

To establish the client L2 VPN session, in a site not managed by NSX download and deploy a standalone VMware® NSX Edge™ appliance, called NSX Autonomous Edge.

To provide self-service for the tenants, VMware Cloud Director Availability manages the entire L2 VPN configuration of the necessary NSX network infrastructure, both in the cloud site and in on-premises sites. As an alternative to using VMware Cloud Director Availability for the L2 stretch, the service provider can perform the entire L2 VPN configuration and management solely in NSX, with the added complexity.

### **L2 Stretch Use Case**

While migrating workloads consisting of several virtual machines, some of the virtual machines can get migrated to the cloud site with the remaining virtual machines of the workload running on-premises. By stretching the network across the two data centers the communication between the migrated and the remaining virtual machines continues as if they operate across the same network segment. The virtual machines remain on the same subnet during the migration between the sites as the stretched network represents a single subnet with a single broadcast domain. When using NSX Autonomous Edge for the L2 stretch, the on-premises virtual machines can only run on VLAN-based networks of distributed switches, that is, distributed port groups.

For the cloud providers, the L2 VPN allows on-boarding tenants without modifying existing IP addresses used by their workloads and applications. Since the IP addresses of the virtual machines do not change upon migration, migrations of the tenants workloads between different network sites are seamless.

In addition to supporting data center migration, on-premises networks stretched with an L2 VPN are useful for disaster recovery plans and dynamically engaging off-premise compute resources and meeting the increased demand.

### **Internet Protocol Security (IPSec) Tunnel**

When using NSX for an L2 stretch, a route-based IPSec tunnel between the server L2 VPN and the client L2 VPN secures the network traffic flowing between the two networks connected over a public network through IPSec gateways called endpoints.

- For information about IPSec VPN when using NSX, see *Understanding IPSec VPN* in the *VMware NSX* documentation.
- For information about IPSec VPN when using NSX Data Center for vSphere, see *IPSec VPN Overview* in the *VMware NSX Data Center for vSphere* documentation.

### **L2 VPN Tunnel**

The L2 VPN tunnel carries only workload traffic and supports network address translation (NAT) through IPSec L2 VPN.

- For information about L2 VPN when using NSX, see *Understanding Layer 2 VPN* in the *VMware NSX* documentation.
- For information about L2 VPN when using NSX Data Center for vSphere, see *IPSec VPN Overview* in the *VMware NSX Data Center for vSphere* documentation.

Multiple client L2 VPN sessions cannot pair to a single server L2 VPN session. An NSX Autonomous Edge can stretch networks from a single vSphere Distributed Switch (VDS), that is, the VDS of the trunk network. To stretch networks from more than one VDS, deploy multiple NSX Autonomous Edge instances.

On-premises, a single NSX Autonomous Edge instance can support a single client L2 VPN session, that can stretch multiple virtual machine networks. To stretch additional client L2 VPN sessions, deploy additional NSX Autonomous Edge instances.

In the cloud site, for information about the scale number of L2 stretched networks to a cloud site, see [VMware Cloud Director Availability Configuration Limits](#).

#### **NOTE**

Cannot establish the L2 VPN tunnel until both the server L2 VPN and the client L2 VPN are configured, and a stretched network is created by selecting client network for each server network. For the procedure steps order, see [On-premises stretching layer 2 networks to the Cloud Director site](#).

## Create a server L2 VPN session with NSX in the Cloud Director site

By using the management interface of VMware Cloud Director Availability in the cloud site backed by NSX, organization administrators create the server side of the L2 VPN session, enabling the L2 stretch of one or more networks across the on-premises site.

- Verify that in both the cloud site and in the on-premises site VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the on-premises site is prepared for an L2 VPN session with NSX Autonomous Edge. For information about the order of the steps of the procedure, see [On-premises stretching layer 2 networks to the Cloud Director site](#).
- Verify that NSX 3.1 or later is deployed in the cloud site to allow stretching of routed and isolated networks.

### NOTE

- Using earlier NSX versions allows only routed networks stretch.
- For NSX Data Center for vSphere (NSX-V), skip this procedure and see [Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site](#).
- Verify that VMware Cloud Director 10.1.0 or 10.2.1 is deployed to allow a single network stretch, or that VMware Cloud Director 10.2.2 or later is deployed to allow multiple networks stretches. The L2 stretch by using NSX does not support VMware Cloud Director versions earlier than 10.2.

### NOTE

VMware Cloud Director 10.3.1 and later do not support isolated networks. To stretch isolated networks use VMware Cloud Director 10.3.0 or earlier.

- Verify that the **Organization Administrator** user has rights to View L2 VPN and Configure L2 VPN. For information about the rights, see [Users and sessions](#) in the *Security Guide*.
- Verify that VMware Cloud Director is prepared to use NSX network resources, after adding an external network backed by a tier-0 gateway, then adding an NSX edge gateway that allows establishing the server L2 VPN session while providing the organization VDC networks with connectivity to external networks:
  - a. Verify that in VMware Cloud Director the NSX backed external network is added. For more information, see [Add a Provider Gateway in Your VMware Cloud Director](#) in the *VMware Cloud Director* documentation.

### NOTE

The VPN service is not supported in an active-active HA (high availability) mode of the tier-0 gateway. For more information, see [Add a Tier-0 Gateway](#) in the *NSX* documentation.

- b. Verify that in VMware Cloud Director the NSX edge gateway is added. For more information, see [Add an Edge Gateway Backed by an NSX Provider Gateway in VMware Cloud Director](#) in the *VMware Cloud Director* documentation.

After preparing VMware Cloud Director with an external network and an edge gateway as per the two steps in the prerequisites, and the on-premises site as per the [On-premises stretching layer 2 networks to the Cloud Director site](#) procedure, follow the procedure below and create the server L2 VPN session.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane, under the **Configuration** section click **L2 Stretch**.
3. Click **L2 VPN Sessions**.
4. From the **Gateway** menu, select the edge gateway and click **New**.

The **NSX Gateway** menu lists both NSX and NSX-V edge gateways that are registered and added in VMware Cloud Director. For information about using NSX-V for server L2 sessions, see [Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site](#).

5. In the **New L2 VPN server session** window, configure the server L2 VPN session and click **Create**.
- In the **Name** text box, enter a name for this server L2 VPN session.
  - In the **Local Address** text box, enter an IP address residing in the IP pool of the edge gateway at the server side of the L2 VPN session.  
The local IP address is a static IP address within the allocated IP range of the NSX edge gateway hosting the server L2 VPN session.
  - In the **Remote Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.  
Usually the remote IP address is the static endpoint IP address of the NSX Autonomous Edge on-premises. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).

**NOTE**

Ensure that the network communication between the local IP address in the cloud and the remote IP address on-premises exists unobstructed.

- In the **Pre-shared Key** text box, enter the pre-shared key as provided by your network administrator.  
Enter only visible ASCII characters, including space, excluding non-printable characters like Null, BEL, and so on. The pre-shared key must meet the following complexity requirements:
  - At least 8 characters
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one digit
  - At least one special character
- In the **Tunnel Interface** text box, enter a private, non-routable subnet address in a CIDR notation.
- Under **Server Network(s)**, to establish an L2 stretch select the server side networks to stretch.  
The number of available server networks to select, depends on the version of VMware Cloud Director. For information about the VMware Cloud Director versions, see the prerequisites above.

**NOTE**

Attempting to delete the server L2 VPN session takes several minutes. Do not attempt to recreate the server L2 VPN session immediately after deletion as it fails due to the deletion progress in the background.

You created the server L2 VPN session in the cloud site.

You can now create the client L2 VPN session that completes the L2 stretch. For more information, see [On-premises stretching layer 2 networks to the Cloud Director site](#).

## Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site

By using the management interface of VMware Cloud Director Availability in the cloud site backed by NSX Data Center for vSphere, the service provider registers the NSX Manager. Then the service provider or the organization administrator creates the server L2 VPN session enabling the L2 stretch of one or more networks across the on-premises site.

- Verify that in both the cloud site and in the on-premises site VMware Cloud Director Availability 4.2.1 or later is successfully deployed.
- Verify that the on-premises site is prepared for an L2 VPN session with NSX Autonomous Edge 3.1.x or 3.2.x only. For more information, see *Understanding Layer 2 VPN* in the *VMware NSX* documentation. For information about the order of the steps of the procedure, see [On-premises stretching layer 2 networks to the Cloud Director site](#).
- Verify that in the cloud site NSX Data Center for vSphere (NSX-V) 6.4.10 or later is deployed to allow stretching of routed networks after registering the NSX Manager.

**NOTE**

- NSX Data Center for vSphere stretches only **Routed** type networks only with interface type **Subinterface**, not **Internal** nor **Distributed**, and cannot stretch **Isolated** nor **Direct** type networks. NSX Data Center for

vSphere can stretch only VXLAN and VLAN Organization VDC routed networks connected to the **Trunk** interface, and cannot stretch networks connected to the **Uplink** nor **Internal** interfaces. **Guest VLAN Allowed** must be deselected and if at some point it was selected, recreate the network for stretch from scratch.

- For NSX, skip this procedure and see [Create a server L2 VPN session with NSX in the Cloud Director site](#).
- Verify that before stretching VLAN routed networks, in vSphere the service provider first created and associated the trunk interface with the edge gateway.
- Verify that VMware Cloud Director 10.0.0.3 or later is deployed in the cloud site.
- Verify that to register the NSX Manager with the Cloud Service for the first time, the service provider authenticates in VMware Cloud Director Availability as a **System Administrator** user.
- Verify that VMware Cloud Director is prepared to use vSphere backed network resources, after adding an external network, then adding an NSX Data Center for vSphere edge gateway that allows establishing the server L2 VPN session while providing the organization VDC networks with connectivity to external networks:
  - a. Verify that in VMware Cloud Director the vSphere backed external network is added. For more information, see [Add an External Network That Is Backed by vSphere Resources to Your VMware Cloud Director](#) in the *VMware Cloud Director* documentation.
  - b. Verify that in VMware Cloud Director the NSX Data Center for vSphere edge gateway is added. For more information, see [Add an NSX Data Center for vSphere Edge Gateway to VMware Cloud Director](#) in the *VMware Cloud Director* documentation.

After preparing VMware Cloud Director with an external network and an edge gateway as per the two steps in the prerequisites, and the on-premises site as per the [On-premises stretching layer 2 networks to the Cloud Director site](#) procedure, follow the procedure below and register the NSX Manager as a service provider. Then as either a service provider or an organization administrator, create the server side of the L2 VPN session.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, under the **Configuration** section click **L2 Stretch**.
3. Click **NSX-V Managers** and select an NSX Manager with an `Unconfigured` status.
4. Click **Edit**.
5. In the **Configure** window, register the NSX Manager with the Cloud Service.
  - a) In the **Password** text box, enter the **admin** user password for the NSX Manager.
  - b) To register the NSX Manager for L2 stretch management by VMware Cloud Director Availability, click **Configure**.  
Verify the thumbprint and accept the SSL certificate of the NSX Manager.  
The NSX Manager is now registered, shows `Up` status, and is ready for creating the server L2 VPN session.
6. Click **L2 VPN Sessions**.
7. From the **NSX Gateway** menu, select the edge gateway and click **New**.  
The **NSX Gateway** menu lists both NSX-V and NSX edge gateways that are registered and added in VMware Cloud Director. For information about using NSX for server L2 sessions, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).

8. In the **New L2 VPN server session** window, configure the server L2 VPN session and click **Create**.
- In the **Name** text box, enter a name for this server L2 VPN session.
  - In the **Local Address** text box, enter an IP address residing in the IP pool of the edge gateway at the server side of the L2 VPN session.  
The local IP address is a static IP address within the allocated IP range of the NSX edge gateway hosting the server L2 VPN session.
  - In the **Remote Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.  
Usually the remote IP address is the static endpoint IP address of the NSX Autonomous Edge on-premises. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).

**NOTE**

Ensure that the network communication between the local IP address in the cloud and the remote IP address on-premises exists unobstructed.

- In the **Pre-shared Key** text box, enter the pre-shared key as provided by your network administrator.  
Enter only visible ASCII characters, including space, excluding non-printable characters like Null, BEL, and so on. The pre-shared key must meet the following complexity requirements:
  - At least 8 characters
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one digit
  - At least one special character
- In the **Tunnel Interface** text box, enter a private, non-routable subnet address in a CIDR notation.
- Under **Server Network(s)**, to establish an L2 stretch select the server side networks to stretch.
  - The available networks for selection are filtered to show only OrgVDC networks connected to the trunk interface of the NSX Data Center for vSphere.
  - The number of available server networks for selection, depends on the version of VMware Cloud Director. For information about the VMware Cloud Director versions, see the prerequisites above.

**NOTE**

- Cannot change or edit the selected networks for stretching when using NSX Data Center for vSphere. To modify the stretched networks, click **Delete** and recreate the server L2 VPN session.
- Attempting to delete the server L2 VPN session takes several minutes. Do not attempt to recreate the server L2 VPN session immediately after deleting as it fails due to the deletion progress in the background.

You created the server L2 VPN session in the cloud site.

You can now create the client L2 VPN session that completes the L2 stretch. For more information, see [On-premises stretching layer 2 networks to the Cloud Director site](#).

## Bandwidth throttling

In VMware Cloud Director Availability, you can configure a global limit on the total incoming replication traffic from all paired sites. For Cloud Director sites, you can also configure a limit for the replication data traffic from on-premises sites to the cloud site. Throttling the network bandwidth can prevent the network saturation and helps to avoid the overloading of the management connections with the replication data traffic that shares the network infrastructure.

In VMware Cloud Director Availability, throttling the network bandwidth to the specified megabits per second limits only the replication data traffic transfer rate. The bandwidth throttling does not limit the transfer rate of other types of network traffic like data and the management traffic.

## **Global Bandwidth Throttling to the Cloud Site**

### **NOTE**

The bandwidth throttle limit to any cloud site requires external Replicator Appliance instances. Since VMware Cloud Director Availability 4.6, you can also apply bandwidth throttle limit for vSphere DR and migration, with the same requirement.

- **Cloud Director sites:**

For Cloud Director sites, external Replicator Appliance instances are expected in production environments. The Cloud Director Combined Appliance does not limit the bandwidth as it is suitable for testing environments only.

For information about adding external Replicator Appliance instances in the Cloud Director site, see [Add an additional Replicator Service instance](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

- **vSphere DR and migration:**

For vSphere DR and migration, external Replicator Appliance instances are optional by default in the cloud site. To apply bandwidth throttle the cloud site must run only external Replicator Appliance instances, in addition to the vCenter Replication Management Appliance.

For information about adding external Replicator Appliance instances for vSphere DR and migration, see [Add an additional Replicator Appliance instance](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

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

## **On-premises Bandwidth Throttling to the Cloud Director Site**

The outbound network bandwidth throttling limit from on-premises sites to the Cloud Director site applies to each individual On-Premises to Cloud Director Replication Appliance instance.

Replication policies configured with bandwidth throttling limit for the traffic from the On-Premises to Cloud Director Replication Appliance instances to the Cloud Director site does not affect the traffic between Cloud Director sites, nor affects the traffic from the Cloud Director site to the On-Premises to Cloud Director Replication Appliance instances.

A replication policy configured with bandwidth throttling limit affects the transfer rate from all On-Premises to Cloud Director Replication Appliance instances, on all on-premises sites that target the respective organization to which the replication policy applies.

## **Configure bandwidth throttling to the cloud site**

To set a global limit for the incoming replication traffic from all peer sites, both remote cloud sites and on-premises sites, you can configure the bandwidth throttling for the cloud site.

- Verify that the cloud site uses only external Replicator Appliance instances.
- Verify that for configuring bandwidth throttle for vSphere DR and migration, VMware Cloud Director Availability 4.6 or later is deployed in the provider cloud site.

The bandwidth throttling to the cloud site is configured and operates the same for both types of cloud sites:

- Cloud Director site
- vSphere DR and migration

For more information, see [Bandwidth throttling](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Tunnel settings** next to **Bandwidth throttling**, click **Edit**.
4. In the **Bandwidth throttling** window, configure the global limit for the incoming traffic from all peer sites.
  - a) To enable bandwidth throttling, select the **Limit all incoming traffic** radio button.
  - b) In the **Maximum** text box, enter a numerical value for the replication traffic limit in megabits per second.
  - c) From the **Tunnel nic** menu, select the network adapter that is connected to the local site components.
  - d) To save the settings, click **Apply**.

## Configure on-premises bandwidth throttling to the Cloud Director site

To set a limit for the replication data traffic from on-premises sites to the cloud site backed by VMware Cloud Director, configure a replication policy. All on-premises sites that target the organization to which this replication policy applies receive and apply this limit.

- Configuring the bandwidth throttling limit in the replication policy affects all On-Premises to Cloud Director Replication Appliance instances, on all on-premises sites that target the organization to which this replication policy applies. For more information, see [Bandwidth throttling](#).
- For information about the replication policies, see [Configuring replication policies](#) in the *User Guide*.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Policies**.
3. Select an existing replication policy and click **Edit**.
4. In the **Edit Policy** window under **General limits**, select **Enable bandwidth throttling**.
5. In the **Max throughput per On-Premises Replicator Appliance** text box, enter the limit in Mbit/s.
6. To save the bandwidth throttling limit, click **Apply**.  
Without re-pairing the on-premises sites, the bandwidth limit applies in 30 minutes.
7. In the list of policies, in the Maximum throughput column you can see the bandwidth limits for each policy.

All On-Premises to Cloud Director Replication Appliance instances in the organization to which the replication policy applies receive and apply the bandwidth throttling limit that you configured.

You can also configure a global limit for the total incoming replication traffic from all cloud sites. For more information, see [Configure bandwidth throttling to the cloud site](#).

## Backing up and restoring in the Cloud Director site

Back up the cloud site and download the backup archive that contains appliance backup files for each appliance in the site. Restore the entire cloud site or only some of the appliances by restoring each appliance in a particular restore order by using its appliance backup file.

## **Backing Up the Cloud Site backed by VMware Cloud Director**

Back up all the cloud appliances in the site by using the Cloud Director Replication Management Appliance management interface. Generating the backup allows downloading a backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file.

This backup archive contains the following information from each appliance in the cloud site:

- Configuration files
- Public certificate
- Keystore
- Database dump

In the backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file, this information is stored as the multiple `.enc` appliance backup files:

- One `cloud-backup_id.tar.bz2.enc` appliance backup file for restoring the Cloud Director Replication Management Appliance.
- One or more `replicator-backup_id-IP_Address.tar.bz2.enc` appliance backup files for restoring each Replicator Appliance instance in the site.
- One `tunnel-backup_id.tar.bz2.enc` appliance backup file for restoring the Tunnel Appliance.

During the backup generation, the provided password encrypts all the `.enc` appliance backup files for preserving any sensitive information.

The backup does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

## **Restoring the Cloud Site**

To restore a VMware Cloud Director Availability cloud site from a backup, use cloud appliances with matching:

- Version
- Appliance roles
- Network settings
- Number of appliances\*

The `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` backup archive contains all the `.enc` appliance backup files that contain the backup information for each appliance in the site.

Follow the order and restore all of the appliances in the cloud site to the `date-timestamp` when the backup was generated, by browsing for the extracted `.enc` appliance backup files.

1. First, for restoring the Tunnel Appliance select the locally extracted `tunnel-backup_id.tar.bz2.enc` appliance backup file and provide the backup password.
2. Then, for restoring the Cloud Director Replication Management Appliance select the locally extracted `cloud-backup_id.tar.bz2.enc` appliance backup file and provide the backup password.
3. Last, for restoring each Replicator Appliance instance select each of the locally extracted `replicator-backup_id-IP_Address.tar.bz2.enc` appliance backup files and provide the backup password.

\* VMware Cloud Director Availability 4.3 introduces in-place restore and restore of a single appliance in the cloud site.

### In-place restore

In VMware Cloud Director Availability 4.3 or later, each appliance supports in-place restore and deploying a new appliance for restoring the backup is no longer necessary. Restoring in-place also does not require powering off of the appliance before the in-place restore.

### Restore of a single cloud appliance

In VMware Cloud Director Availability 4.3 or later, if only a single cloud appliance in the site becomes irrecoverable by other means, you can restore only that appliance instead of restoring all the cloud appliances in the site. Restoring always requires an appliance with exactly the same version as the remaining cloud appliances in the site and with exactly the same version as the downloaded backup archive.

- Restoring a single cloud appliance, without restoring any of the remaining appliances in the site does not require following any restore order.
- Restoring several appliances from the site but not all cloud appliances, requires following the same restore order for restore as restoring the cloud site.
  - a. If restoring the Tunnel Appliance, restore it first.
  - b. If restoring the Cloud Director Replication Management Appliance, ensure that you follow the restore order.
    - a. If restoring Tunnel Appliance as well, then restore the Cloud Director Replication Management Appliance after restoring the Tunnel Appliance.
    - b. If restoring a Replicator Appliance instance as well, restore the Cloud Director Replication Management Appliance before that.
  - c. If restoring a Replicator Appliance instance, restore it as last. If needed, repeat with restoring other Replicator Appliance instances.

## Back up all the appliances in the cloud

In the Cloud Service management interface, as a **service provider** you generate new backup archives of all the VMware Cloud Director Availability appliances in the cloud site. Download the backup archive as a file and then preserve it on an external storage device for future restore of the cloud site to that moment in time.

- Verify that before taking a backup, all VMware Cloud Director Availability services are operational. As exception, unreachable Replicator Service instances without incoming replications do not prevent generating a backup.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least the following amount of free space for each of the VMware Cloud Director Availability appliances in the cloud site:
  - Cloud Director Replication Management Appliance 40%
  - Each Replicator Appliance instance 35%
  - Tunnel Appliance 35%

You generate a backup of all the VMware Cloud Director Availability appliances in the cloud site only by using the management interface of the Cloud Service. This backup archive contains the following information from each appliance in the cloud site:

- Configuration files
- Public certificate
- Keystore
- Database dump

In the backup archive, this information is stored as multiple `.enc` appliance backup files. When generating the backup, you provide a password that encrypts the `.enc` appliance backup files to preserve any sensitive information.

A backup file does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.

- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

Locally, the appliances can store up to 24 backup archives on their internal storage. Past that number, you must delete some of them, or attempting to create another backup, shows `Backup quota exceeded. Number of allowed backups: 24, current backup count: 24`. Such limit does not apply for the **Scheduled backup archives** that are stored on an external SFTP storage. For more information, see [Schedule backup archives](#).

#### NOTE

After evacuating a datastore, all backups taken priorly cannot restore the replications. For information about datastore evacuation, see [Evacuate the replications data from a datastore](#).

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane under the **System** section, click **Backup Archives**.
3. In the top right corner next to **Scheduled backup archives**, click **Manual backup archives**.
4. On the **Manual backup archives** page, to generate a backup archive click **Generate new**.
5. In the **Generate a new backup archive** window, generate the backup archive of the cloud site.
  - a) In the **Password** text box, enter a password that protects and encrypts the backup archive contents.
 

The password that you enter must contain a minimum of eight characters and must consist of:

    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as `& # %`.
  - b) In the **Confirm Password** text box, reenter the password to confirm the password that encrypts the backup.

#### NOTE

Store the backup password in a safe place since it cannot be restored later.

- c) To generate the backup archive, click **Generate**.
- In the **Backup archives** page, you can see the progress of generating the new backup archive.
6. To locally download a generated backup archive, in the Backup Id column click the `backup id` link.
    - a) In the **Download Backup Archive** window, to save the backup file locally click **Download**.
 

In your Web browser, the archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file starts downloading.
    - b) Store the locally downloaded backup archive and its password for future restore of the cloud site to that moment in time.
 

The backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file downloaded, providing a locally-stored backup point in time of the site.
  7. Optional: Remove a backup archive from the appliance.
    - a) Select one or more generated backup archives for removal and click **Delete**.
    - b) In the **Remove Archives** window, to confirm the removal click **Delete**.
 

You deleted the selected backup archives from the appliance. For restoring, use a locally downloaded backup archive.

You can later use a downloaded backup archive to restore all the VMware Cloud Director Availability appliances in the cloud site to that moment in time. For information about restoring from a backup archive, see [Restore the appliances in the cloud](#).

## Restore the appliances in the cloud

As a **provider**, you restore VMware Cloud Director Availability appliances in the cloud site on appliances with the same version, appliance role and network settings and by using a single appliance backup `.enc` file, extracted from the locally downloaded backup archive.

- Verify that VMware Cloud Director Availability 4.3 or later is installed in the cloud site for in-place restore and for restore of a single or several cloud appliances, but not all appliances in the site.
- Verify that you have the backup password and that you locally extract the backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file, resulting in several `.enc` appliance backup files, listed below.
- Verify that the following settings of the cloud appliance for restoring exactly match the backed-up appliance.
  - Version
  - Appliance role
  - Network settings
- Verify that before restoring on a newly deployed appliance, the existing backed-up appliance in the site with the same role is powered off.



### CAUTION

Restoring on a newly deployed appliance while the existing backed-up appliance in the site with the same role is operational might corrupt the replications.

However, for VMware Cloud Director Availability 4.3 or later, when restoring an appliance in-place, where the backed-up appliance matches the appliance on which you restore, do not power it off.

### NOTE

Restoring backups containing deleted replications at the time of restore:

In the management interface of a restored Replicator Service instance, on the **System Tasks** page the **Reload destination** tasks run indefinitely or fail with a `Lock acquisition timed out for object: 'H4-id'` for each replication that is not present since restoring the backup. To manually delete these replications, click the **Emergency Recovery** page, select them then click **Delete**.

- To restore a single appliance in the cloud site, depending on whether restoring on a newly deployed, or restoring in-place over the backed-up appliance:
  - When deploying a new appliance, power off the existing backed-up appliance in the site with the same role.
  - When restoring in-place over the backed-up appliance, without deploying a new appliance, do not power it off.
 Restoring a single appliance does not require following the restore order and can be performed for any of the backed-up cloud appliances. For more information, see [Backing up and restoring in the Cloud Director site](#).
- To restore several of the appliances in the cloud site, but not all, follow the same restore order as with restoring the entire site. For more information, see [Backing up and restoring in the Cloud Director site](#).
- To restore an entire backed-up cloud site, restore the same number of appliances with matching appliance roles. For example, to restore a site consisting of a Tunnel Appliance, a Cloud Director Replication Management Appliance, and a couple of Replicator Appliance instances, you must restore a Tunnel Appliance, a Cloud Director Replication Management Appliance, and a couple of Replicator Appliance instances by following the restore order below.

The backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file contains all of the following password-protected `.enc` appliance backup files for all of the cloud appliances in the site.

1. One `tunnel-backup_id.tar.bz2.enc` appliance backup file for firstly restoring the Tunnel Appliance.
2. One `cloud-backup_id.tar.bz2.enc` appliance backup file for then restoring the Cloud Director Replication Management Appliance.

3. One or more `replicator-backup_id-IP_Address.tar.bz2.enc` appliance backup files for lastly restoring each Replicator Appliance instance in the site.

These appliance backup files contain all the backup information for restoring each of the appliances in the cloud site to the `date-timestamp` point in time when the backup was generated. For more information, see [Back up all the appliances in the cloud](#).

To restore multiple appliances, repeat this procedure multiple times, according to the restore order and restore the appliances in the cloud site by using the appropriate appliance backup file for each appliance role, as extracted from the backup archive.

1. Follow the restore order and log in to the VMware Cloud Director Availability appliances.
  - a) In a Web browser, go to the management interface of the VMware Cloud Director Availability appliances in the following restore order:

Restore Order	Appliance	Service	Management Interface
1	Tunnel Appliance	Tunnel Service	<code>https://Tunnel-Appliance-IP-Address/ui/admin</code>
2	Cloud Director Replication Management Appliance	Cloud Service	<code>https://Replication-Management-Appliance-IP-Address/ui/admin</code>
3	Each Replicator Appliance instance	Replicator Service instances	<code>https://Replicator-Appliance-IP-Address/ui/admin</code>

- b) Log in by entering the **root** user password.
 

If restoring on a newly deployed appliance, this is the password that you set during the OVA deployment.
2. If restoring on a newly deployed appliance, in the **VMware Cloud Director Availability Appliance Password** window, change the initial **root** user password.
  - a) Enter the **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:
    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as & # % .

3. Initiate restoring from the backup archive in the following restore order, according to the appliance role you restore.
  - a) Firstly, for the Tunnel Appliance, in the left pane under the **System** section, click **Backup Archives** then click **Restore**.
  - b) Secondly, repeat the same restore actions for the Cloud Director Replication Management Appliance.
  - c) Lastly, for each Replicator Appliance instance repeat the same restore actions.
4. Following the restore order of the appliances according to their role, browse for the appliance backup file, enter its password, and restore the appliance.
  - a) In the **Restore from a backup archive** window, click **Browse** and select the extracted `.enc` appliance backup file for the appliance role you are restoring.
    - First, for restoring the Tunnel Appliance select the `tunnel-backup_id.tar.bz2.enc` appliance backup file.
    - Then, for restoring the Cloud Director Replication Management Appliance select the `cloud-backup_id.tar.bz2.enc` appliance backup file.
    - Last, for restoring each Replicator Appliance instance select each of the `replicator-backup_id-IP_Address.tar.bz2.enc` appliance backup files.
  - b) In the **Password** text box, enter the password used for encrypting the backup.
  - c) To initiate the restoring of this appliance, click **Restore**.  
Restoring starts and might take a while until complete. While restoring is in progress, you cannot login to this appliance.  
After restoring completes, this appliance restarts.
5. Optional: After the services start, verify that restoring is successful.
  - a) Log in to the management interface of the newly restored appliance.
  - b) In the left pane, click **System Tasks**.  
After the restore, the `Generate backup archive` task, which generated the backup archive used for the restore, shows `Task aborted due to service reboot`.
  - c) Verify the Target of `task.restore.backup`.  
For the Replicator Appliance instances, on the **System tasks** page, you see `Reload replication tasks` for each incoming replication of this Replicator Service instance.

After repeating this procedure multiple times, you restored some or all of the cloud appliances in the site with matching appliance roles.

- The Tunnel Appliance is restored from the backup.
- The Cloud Director Replication Management Appliance is restored from the backup.
- All of the Replicator Appliance instances are restored from the backup.

#### NOTE

- After restore, there might be a misalignment between the replication settings stored in the database and the ones loaded from the backup file. As a result, you might see RPO violations, differing numbers of instances, and others, that you can resolve by reconfiguring the affected replications for reapplying their replication settings.
- After restoring, if an RPO violation is present, the replication might be missing from the source Replicator Service. This situation might happen when the source site is restored to a point in time when the replication is not yet started, leading to not working synchronization. As a workaround, you can attempt manually synchronizing the replication. If the synchronization task fails with `SourceReplicationNotFound`, fail over the replication, stop the replication, then deactivate the replication services for that virtual machine in the source ESXi host, see KB <https://kb.vmware.com/s/article/2106946>. Finally, start a new replication with a seed virtual machine.
- **Instances**

After restore, the instances might disappear for some replications. In most cases, the data is not lost and a subsequent synchronization transfers only a delta. To get an instance, either wait for automatic synchronization, or perform a synchronization manually.

- After evacuating a datastore, all backups taken priorly cannot restore the replications. Take a backup every time the replications are moved from one datastore to another to ensure restoring is successful. For information about datastore evacuation, see [Evacuate the replications data from a datastore](#).

You can perform replication workflows. After confirming that the restored appliances are operational, if you restored on a newly deployed appliances, you can decommission the backed-up appliances that are powered off.

## Maintenance in the Cloud Director site

In cloud sites backed by VMware Cloud Director, perform maintenance operations on a datastore, or on a Replicator Service instance, or rebalance replications across Replicator Service instances, or replace a Tunnel Appliance.

### Evacuate the replications data from a datastore

For performing maintenance operations on a local datastore in the cloud site evacuate all incoming replications and replication data placed on that datastore. To evacuate the replications from the datastore at once, apply an alternative storage policy for all incoming replications that reside on the datastore.

- Verify that before evacuating, any replications that are already failed over or migrated are stopped.
- Verify that before evacuating, any replications that already completed a test failover are cleaned up.

#### NOTE

- Evacuating a datastore invalidates all VMware Cloud Director Availability backups created priorly and they cannot restore the replications.  
To ensure restoring from a backup is successful, create a backup every time the replications are moved from one datastore to another. For information about restoring, see [Restore the appliances in the cloud](#).
- Evacuating a datastore might take several hours until completed and depends on the amount of data for transferring.
- Since VMware Cloud Director Availability 4.4 evacuating replicas from individual members of datastore clusters is supported. Replications on a member datastore can move only to a different (for example, temporary) storage policy, they cannot be rebalanced within the other member datastores within the same cluster. After maintenance completes, the replications can be moved back from the temporary location to the original datastore cluster.

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane under **System**, click **Datastores**.
3. Optional: To show the replications that are placed on a datastore that displays replications counters, click **Preview**.  
For datastore clusters, expand to show the cluster members.

4. Select a local datastore or a cluster member that displays replications counters and click **Evacuate**.
5. In the **Evacuate datastore** window, select the destination storage policy for all incoming replications residing on the datastore and click **Evacuate**.
  - **Reset current storage policy** applies the current storage policy to each matching replication. After removing or adding datastores to the storage policy, to make the matching replications compliant with their storage policy this option can move the replication replica files.
  - **Any** stores all the replications to all the shared datastores that have `Any` storage policy applied.
  - **pVDC Storage policy** applies the selected storage policy to all matching replications. If the `pVDC Storage policy` is not exposed to a tenant data center, the replications of this tenant remain placed on the datastore.

VMware Cloud Director Availability applies the selected storage policy and starts evacuating the incoming replications and replica files from the selected local datastore in the cloud site.

You can track the progress of the `Change storage profiles` task by clicking **System Tasks** in the left pane.

## Replicator Service maintenance mode

To prepare a Replicator Service instance for maintenance without disrupting replications, you can evacuate the incoming replications from the Replicator Service instance to other local Replicator Service instances in the cloud site.

- Verify that VMware Cloud Director Availability is successfully deployed in the cloud site.
- Verify that more than one Replicator Service instance is operational in the cloud site.
- Verify that the clean-up task is complete after using a test failover for any incoming replication. If the Replicator Service contains a test failed over virtual machine, attempting to enter a maintenance mode shows a `Operation aborted due to an unexpected error` message. Before entering maintenance mode, you must perform a test cleanup on the test failed over virtual machine or vApp.

### NOTE

- **Enter Maintenance Mode** auto-rebalances the replications in the local site.
- **Exit Maintenance Mode** does not perform auto-rebalancing. To rebalance the replications after exiting maintenance mode, click **Rebalance**. For more information, see [Rebalance the replications across the Replicator Service instances](#).

The Replicator Service instance must be placed in maintenance mode in each site where it is registered. This procedure is a two-step process, performed first in the local site, then repeated in the remote sites:

1. In the local site, placing the Replicator Service instance in maintenance mode migrates all incoming cloud replications to other Replicator Service instances in the local site. Also, VMware Cloud Director Availability migrates all incoming and outgoing replications from and to on-premises sites.
2. In the remote site, migrate the remaining outgoing cloud replications from this Replicator Service instance to other Replicator Service instances. Log in to the remote site and place in maintenance mode the same Replicator Service instance. Repeat this step in each remote site, where this Replicator Service instance is remotely registered.

New replications are placed on Replicator Service instances that are not in maintenance mode.

1. Log in to the Manager Service service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane, click **Replicators**.
3. To evacuate the incoming replications, select the local Replicator Service instance and click **Enter Maintenance Mode**.
4. To evacuate the outgoing replications from this Replicator Service instance, log in to the Manager Service in the remote site and repeat this procedure.

In the remote site, select the same Replicator Service instance that is remotely registered.

Repeat step 4 for all cloud sites, where the Replicator Service instance is remotely registered.

After placing a Replicator Service instance in maintenance mode from both the local site and all remote sites where it is registered, VMware Cloud Director Availability evacuates all replications from that Replicator Service instance. The Replicator Service instance is ready for maintenance operations.

After performing the maintenance operations, in the local site click **Exit Maintenance Mode**. To repopulate the Replicator Service instance with replications, you must rebalance the replications. For more information, see [Rebalance the replications across the Replicator Service instances](#).

## Rebalance the replications across the Replicator Service instances

To distribute the incoming replications evenly over all Replicator Service instances in the site, you can rebalance the replications. After exiting maintenance mode, you must rebalance the replications.

- Verify that VMware Cloud Director Availability is successfully deployed in the site.
- Verify that more than one Replicator Service instance is operational in the site.

VMware Cloud Director Availability assigns all new replications to the Replicator Service with the fewest number of replications in the site. After adding an extra Replicator Service instance, VMware Cloud Director Availability assigns all new replications to the new Replicator Service instance. Replications that existed before adding the new Replicator Service instance remain assigned to the previous Replicator Service instances. The result is an unequal balance of the number of replications per Replicator Service instance. You can see how many replications are assigned to each Replicator Service instance and rebalance the replications. This operation migrates the replications from Replicator Service instances with more replications to Replicator Service instances with fewer replications.

1. Log in to the Manager Service service management interface.
  - a) In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane, click **Replicators**.
3. To rebalance the replications, click **Rebalance**.
4. In the **Rebalance Site** window, select a site to rebalance and click **Apply**.  
Repeat step 4 for all paired sites.

VMware Cloud Director Availability migrates and evenly distributes the replications to each operational Replicator Service instance in the site.

---

## Replace a Tunnel Appliance instance

To replace or restore a failing Tunnel Appliance, power it off, deploy a new instance of the appliance and enable tunneling to the new appliance.

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that the existing Tunnel Appliance is powered off or that it is disconnected from the port group.

If a backup of the Tunnel Appliance exists, follow the procedure in [Restore the appliances in the cloud](#) instead of the procedure below. To generate a backup in VMware Cloud Director Availability, see [Back up all the appliances in the cloud](#).

1. Deploy a new Tunnel Appliance.
  - a) Use the same host name, IP address, and the remaining settings as the original Tunnel Appliance.
  - b) Power on the new Tunnel Appliance.
2. Log in to the Tunnel Service management interface.
  - a) In a Web browser, go to `https://Tunnel-IP-or-FQDN:8442`.
  - b) Select **Appliance login** and enter the **root** user password that you set during the OVA deployment.
  - c) Click **Login**.
3. If you log in to the appliance for the first time, you must change the initial **root** user password.
  - a) Enter the initial **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password.

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as & # %.
  - c) Click **Apply**.

The **Getting Started** tab opens.

4. Optional: To log in to the Tunnel Service by using vCenter Single Sign-On credentials, you can register the new Tunnel Appliance with the vCenter Server Lookup service.
  - a) In the **Configuration** page, under **Service endpoints**, next to **Lookup Service Address**, click **Edit**.
  - b) In the **Lookup Service Details** window, enter the **Lookup Service Address**.  
Pressing Tab autocompletes the vCenter Server Lookup service address to `https://Lookup-Service-IP-Address:443/lookupservice/sdk`.
  - c) Click **Apply**.
  - d) Verify the thumbprint and accept the certificate of the vCenter Server Lookup service.
5. Log in to the management interface of the Cloud Director Replication Management Appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
6. Enable tunneling to the new Tunnel Appliance instance.
  - a) In the left pane under **Configuration**, click **Settings**.
  - b) Under **Tunnel settings**, next to **Primary Tunnel Service address** click **Edit**.
  - c) In the **Tunnel Service Settings** window, enter the **root** user password.  
The **Appliance user** is already set to **root**.
  - d) Click **Apply**.
  - e) Verify the thumbprint and accept the certificate of the new Tunnel Service instance.

The new Tunnel Appliance starts tunneling for the VMware Cloud Director Availability services communication.

- For the paired cloud sites, you do not need to perform additional operations. In a few minutes, the pairing reports a green status and the replications proceed according to their RPO.
- For the paired on-premises sites, the Cloud Service reports a red status for all the pairings incoming from on-premises and outgoing to on-premises. The paired On-Premises to Cloud Director Replication Appliance instances continue to report a green status for pairing to cloud and the replications from on-premises to cloud proceed according to their RPO. To restore the replications from cloud to on-premises, you can restart the On-Premises to Cloud Director Replication Appliance instances or you can repair all on-premises sites with the cloud site.

You can verify that all services are running correctly. For more information, see [Verify uptime and local and remote connectivity in the Cloud site](#).

## Uninstall VMware Cloud Director Availability from the Cloud Director site

To remove a VMware Cloud Director Availability instance from a cloud site backed by VMware Cloud Director, stop the replications, delete pairing with all peer sites, remove the plug-in from VMware Cloud Director, then remove the cloud appliances.

Verify that VMware Cloud Director Availability is deployed in the cloud site backed by VMware Cloud Director.

When replacing an old VMware Cloud Director Availability instance, to prevent the error message `VM already protected` after installing the new VMware Cloud Director Availability instance, follow the steps in this procedure.

1. Stop all replications from and to the VMware Cloud Director Availability instance you are removing.
  - a) Log in to the VMware Cloud Director Availability instance that you are removing.
  - b) In the left pane, click **Incoming Replications**.
  - c) Select all the replications and click **Delete**.
  - d) Repeat this step in **Outgoing Replications** and delete all the replications.
2. Delete the established trust with all peer sites.
  - a) In the left pane under **Configuration**, click **Peer Sites**.
  - b) In the **Cloud sites** page, select a cloud site, then click **Delete**.
  - c) In the **Delete Peer Cloud Site** window, to delete the cloud site pairing, click **Delete**.  
 You deleted the pairing with the cloud site and removed the trust from both the local and the remote cloud sites.
  - d) Repeat the above steps until you delete the pairing with all peer cloud sites.
  - e) Delete the established trust with all on-premises sites from the cloud site.
    - If the on-premises site is still paired, delete the pairing from the cloud site, then from the on-premises site delete the remaining pairing with the cloud site. For information about deleting pairing from the on-premises site, see [Unpair a remote site](#).
    - If from the on-premises site the cloud site is already unpaired, then delete the remaining record in the cloud site.
  - f) On the **Peer Sites** page, under **On-premises sites**, click **Delete**.
  - g) In the **Delete On-Premises Site** window, to delete the on-premises site pairing, click **Delete**.  
 Above **On-premises sites** you see a green `On-Premises site deleted successfully.` message. You removed the cloud site trust with the on-premises site. If you performed this procedure from the cloud site first, in the on-premises site the cloud site still shows as paired. For more information, see [Unpair a remote site](#).
  - h) Repeat the above step until you delete pairing with all peer on-premises sites.  
 You deleted all peer sites paired with this VMware Cloud Director Availability instance.
3. Remove the VMware Cloud Director Availability plug-in from VMware Cloud Director.
  - a) In the left pane, click **Settings**.
  - b) Under **Service endpoints** next to **VMware Cloud Director Address**, click **Remove plugin**.
  - c) In the **Remove VCD UI plugin** window, click **Remove**.
4. If the management interface of VMware Cloud Director Availability is not available, remove the VMware Cloud Director Availability plug-in from VMware Cloud Director by using its Service Provider Admin Portal.
  - a) Go to `https://vcloud.example.com/provider` and log in to the Service Provider Admin Portal of VMware Cloud Director by using the **system administrator** user credentials.
  - b) From the top navigation bar, select **More > Customize Portal**.
  - c) Select the check box next to the name of the VMware Cloud Director Availability plug-in, then click **Delete**.
  - d) To confirm removing the plug-in, click **Save**.
5. For the VMware Cloud Director Availability instance you are removing, delete all the virtual machines of its appliances from the vCenter Server instance.

This VMware Cloud Director Availability instance is now uninstalled from the cloud site backed by VMware Cloud Director. You can now install a new VMware Cloud Director Availability instance in the same cloud site.

## Administration in the on-premises and in the provider sites

After installing and configuring the VMware Cloud Director Availability appliance in the vCenter Server site, you can perform management and administrative tasks. The following tasks include changes to the provisioned environment and routine administration and maintenance procedures.

- **On-premises or provider vCenter Server sites:**

In either:

- a VMware Cloud Director Availability on-premises vCenter Server site
- or in a provider VMware Cloud Director Availability cloud vCenter Server site,

perform the following administration tasks in this current chapter by using the appliances management interface or in the disaster recovery infrastructure.

- **Cloud site backed by VMware Cloud Director:**

For information about VMware Cloud Director Availability cloud sites, backed by VMware Cloud Director, see the [Administration in the Cloud Director site](#) chapter.

## On-premises stretching layer 2 networks to the Cloud Director site

To prepare the on-premise site for L2 stretch from the Cloud Director site, first deploy NSX Autonomous Edge, then register it and configure its network adapters by using the On-Premises to Cloud Director Replication Appliance. To complete the L2 stretch, in the cloud site, depending on the NSX version create the server L2 VPN session and then create the client L2 VPN session on-premises.

### IMPORTANT

Verify that the prerequisites for NSX and for VMware Cloud Director in the cloud site are met and that you follow the steps in the procedure below in the correct order.

- For information about the L2 stretch, see [Stretching layer 2 networks in the Cloud Director site](#).
  - For the prerequisites for NSX in the cloud site, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).
  - For the prerequisites for NSX Data Center for vSphere in the cloud site, see [Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site](#).

### Procedure Overview

Before stretching the L2 networks, ensure that you follow the procedure in the correct order:

1. Initially, prepare the on-premises site for L2 VPN with NSX Autonomous Edge:

#### NOTE

This on-premises procedure only applies for on-premises sites not managed by NSX. If NSX manages the on-premises site, skip this on-premises section and its subsections and to create a client L2 VPN session and an L2 stretch follow the NSX documentation.

- a. To allow for an L2 stretch on-premises, first deploy an NSX Autonomous Edge appliance. For more information, see [Deploy an NSX Autonomous Edge appliance on-premises](#).
- b. After deploying NSX Autonomous Edge on-premises, register the newly deployed NSX Autonomous Edge by using the On-Premises to Cloud Director Replication Appliance. For more information, see [Register the NSX Autonomous Edge on-premises](#).
- c. After registering the NSX Autonomous Edge, configure its network adapters by using the On-Premises to Cloud Director Replication Appliance. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).

2. Complete the L2 stretch from on-premises to the cloud site by creating the server and the client VPN sessions:
  - a. After configuring the NSX Autonomous Edge on-premises, in the cloud site use its IP address when creating the server L2 VPN session. Depending on the NSX version in the cloud site, follow the correct procedure:
    - When using NSX in the cloud site, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).
    - When using NSX Data Center for vSphere in the cloud site, see [Create a server L2 VPN session with NSX Data Center for vSphere in the Cloud Director site](#).
  - b. Finally, complete the L2 stretch by using the On-Premises to Cloud Director Replication Appliance. For more information, see [Create a client L2 VPN session on-premises](#).

---

## Deploy an NSX Autonomous Edge appliance on-premises

On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that you have access to the NSX Edge OVF file.

In on-premises data centers, you deploy an NSX Autonomous Edge and configure it as on-premises client side of an L2 VPN that connects to the cloud site.

1. Locate the NSX Edge OVF file on the VMware download portal and either copy the download URL or download it locally.
2. By using the vSphere Client, log in to the vCenter Server that manages the non- NSX on-premises site.
3. Select **Hosts and Clusters** and to show the available hosts, expand the clusters.
4. To deploy the NSX Edge, right-click the host where you want it and select **Deploy OVF Template**.
  - a) On the **Select an OVF template** page, to download and deploy the OVF file, paste the URL, or select a locally downloaded OVF file and click **Next**.
  - b) On the **Select a name and folder** page, in the **Virtual machine name** text box enter a name for the NSX Autonomous Edge, select a location for its virtual machine and click **Next**.
  - c) On the **Select a compute resource** page, select the destination compute resource and click **Next**.
  - d) On the **Review details** page, verify the OVF package template details and click **Next**.
  - e) On the **Configuration** page, select a deployment configuration size and click **Next**.
  - f) On the **Select storage** page, select the provisioning, a storage for the configuration and the disk files and click **Next**.
  - g) On the **Select networks** page, for all destination networks select the management network and click **Next**.

After the setup completes, the On-Premises to Cloud Director Replication Appliance takes over managing the network interfaces of the NSX Autonomous Edge. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).

h) On the **Customize template** page, enter the following properties and click **Next**.

**NOTE**

The NSX Edge appliance does not validate the property values such as the passwords before powering on for the first time.

Option	Description
<b>System Root User Password</b>	Enter and confirm the passwords for the system users, that meet the following complexity requirements: <ul style="list-style-type: none"> <li>• At least 12 characters</li> <li>• At least one uppercase letter</li> <li>• At least one lowercase letter</li> <li>• At least one digit</li> <li>• At least one special character</li> <li>• At least five different characters</li> <li>• No dictionary words</li> <li>• No palindromes</li> <li>• No more than four monotonic character in a sequence</li> </ul> <p><b>NOTE</b> NSX Edge core services do not start unless you enter passwords meeting these requirements.</p>
<b>CLI "admin" User Password</b>	
<b>Is Autonomous Edge</b>	Select this property to deploy the NSX Edge node as an autonomous edge in the L2 VPN topology. NSX does not manage NSX Edge nodes determined as autonomous edges.

- You can enable SSH and allow **root** SSH login.
- Skip configuring the remaining properties, like hostname or IP. VMware Cloud Director Availability needs a management IP address for the NSX Autonomous Edge to connect to. If the management network selected during the NSX Autonomous Edge deployment does not grant one, for example via DHCP, you must provide a static one.

i) On the **Ready to complete** page, review the NSX Autonomous Edge settings and click **Finish**.

5. After the deployment completes, power on the NSX Autonomous Edge virtual machine.

The NSX Autonomous Edge appliance deployed successfully on-premises.

Register this newly deployed NSX Autonomous Edge for L2 stretch management by using the management interface of the On-Premises to Cloud Director Replication Appliance. For more information, see [Register the NSX Autonomous Edge on-premises](#).

**Related Links**

[Register the NSX Autonomous Edge on-premises on page 154](#)

On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

[Configure the networks of the NSX Autonomous Edge on-premises on page 155](#)

After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

[Create a client L2 VPN session on-premises on page 156](#)

After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

## Register the NSX Autonomous Edge on-premises

On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
- Verify that an NSX Edge appliance is deployed on-premises, selected as an autonomous edge and configured with passwords for the **root** and the **admin** users that meet the complexity requirements. For more information, see [Deploy an NSX Autonomous Edge appliance on-premises](#).

To complete the L2 stretch configuration entirely by using the management interface of the On-Premises to Cloud Director Replication Appliance, after deploying the NSX Autonomous Edge in the on-premises site you register it by using the On-Premises to Cloud Director Replication Appliance.

1. Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.
  - a) In a Web browser, go to `https://On-Premises-Appliance-IP-address/ui/admin`.
  - b) Log in as the **root** user.
2. In the left pane, under the **System** section click **L2 Stretch**.
3. On the **NSX Autonomous edges** page, click **New**.
4. In the **Register a New NSX Autonomous Edge** window, register the new NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance.
  - a) In the **Name** text box, enter a friendly name for the new NSX Autonomous Edge.
  - b) From the **vCenter Server** drop-down menu, select the vCenter Server instance hosting the NSX Autonomous Edge virtual machine.
  - c) Under **NSX Autonomous Edge VMs**, select the virtual machine of the newly deployed NSX Autonomous Edge.
  - d) In the **Management Address** text box, enter the URL for the NSX Autonomous Edge management.
  - e) In the **User name** and **Password** text boxes, enter the **admin** user credentials for the NSX Autonomous Edge management.
  - f) Optional: In the **Description** text box, enter a description for this NSX Autonomous Edge.
  - g) To register the NSX Autonomous Edge for management, click **Register**.

The On-Premises to Cloud Director Replication Appliance registered the new NSX Autonomous Edge for L2 stretch management.

You can now configure the networks of the newly registered NSX Autonomous Edge by using the On-Premises to Cloud Director Replication Appliance. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).

### Related Links

[Deploy an NSX Autonomous Edge appliance on-premises on page 152](#)

On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

[Configure the networks of the NSX Autonomous Edge on-premises on page 155](#)

After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

[Create a client L2 VPN session on-premises on page 156](#)

After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

## Configure the networks of the NSX Autonomous Edge on-premises

After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
- Verify that the NSX Autonomous Edge in the on-premises site is powered on and registered with the On-Premises to Cloud Director Replication Appliance. For more information, see [Register the NSX Autonomous Edge on-premises](#).

During the NSX Autonomous Edge deployment, its four network adapters are configured with the management network. For more information, see [Deploy an NSX Autonomous Edge appliance on-premises](#). For the L2 stretch to operate, by using the management interface of the On-Premises to Cloud Director Replication Appliance configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

1. Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.
  - a) In a Web browser, go to `https://On-Premises-Appliance-IP-address/ui/admin`.
  - b) Log in as the **root** user.
2. In the left pane, under the **System** section click **L2 Stretch**.
3. On the **NSX Autonomous edges** page, select a newly deployed NSX Autonomous Edge instance.
4. Click **Edit network**.
5. In the **Configure the NSX Autonomous Edge Network Adapters** window, configure the network adapters of the NSX Autonomous Edge and click **Apply**.
 

Cannot select the **Management Network** of the NSX Autonomous Edge preventing the loss of connectivity to it.

  - a) From the **VLAN Trunk Network** drop-down menu, to allow intercepting the on-premises network traffic for the L2 stretch networks by VMware Cloud Director Availability, select a network or a port group allowing VLAN trunking.
  - b) From the **Uplink Network** drop-down menu, to allow the external communication, select a network that can connect to the cloud site NSX Edge.
6. With the newly deployed NSX Autonomous Edge selected, click **Configure the uplink port**.
7. In the **Configure the Uplink Port** window, enter the settings for the external network port and click **Apply**.
  - a) In the **IP Address/Prefix** text box, enter the IP address and the subnet mask of the uplink port.
  - b) In the **VLAN** text box, enter the VLAN of the uplink port.
    - If not using a VLAN port group, enter 0.
    - If using a VLAN port group, it must be within the uplink network connected to the NSX Autonomous Edge.
  - c) Optional: In the **MTU** text box, enter the maximum transmission unit (MTU) of the uplink port or leave the default MTU value of 1500 bytes.
  - d) Optional: In the **Gateway** text box, enter a gateway for the uplink port.

The On-Premises to Cloud Director Replication Appliance configured the NSX Autonomous Edge network on-premises.

You can now create a server L2 VPN session by using the static endpoint IP address of this newly configured NSX Autonomous Edge. For more information, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).

### Related Links

### [Deploy an NSX Autonomous Edge appliance on-premises on page 152](#)

On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

### [Register the NSX Autonomous Edge on-premises on page 154](#)

On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

### [Create a client L2 VPN session on-premises on page 156](#)

After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

## Create a client L2 VPN session on-premises

After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
  - Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
  - Verify that in the cloud site the server L2 VPN session is created. For more information, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).
  - Verify that in the on-premises site the networks of the NSX Autonomous Edge are configured. For more information, see [Configure the networks of the NSX Autonomous Edge on-premises](#).
1. Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.
    - a) In a Web browser, go to `https://On-Premises-Appliance-IP-address/ui/admin`.
    - b) Log in as the **root** user.
  2. In the left pane, under the **System** section click **L2 Stretch**.
  3. On the **NSX Autonomous edges** page, click **L2 VPN Sessions**.
  4. If more than one NSX Autonomous Edge instance is registered with the On-Premises to Cloud Director Replication Appliance, from the **NSX Autonomous Edge** drop-down menu, select the correct NSX Autonomous Edge name to use for the client L2 VPN session.
  5. To create a client L2 VPN session, click **New** and complete the **New Client L2 VPN Session** wizard.
 

If your user session is not currently extended to the cloud site, enter credentials to authenticate to the cloud site.

6. On the **VDC and edge Gateway** page, select the cloud site virtual data center and the edge gateway.
7. On the **Settings and networks** page, configure the L2 VPN and click **Next**.
  - a) In the **Name** text box, enter a name for this client L2 VPN session.
  - b) From the **Server session** drop-down menu, select the cloud side L2 VPN server session.
  - c) In the **Local Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.  
The local IP address must be the same as the uplink port IP address of the NSX Autonomous Edge hosting the client L2 VPN session.
  - d) In the **Remote Address** text box, enter the cloud IP address at the server side of the L2 VPN session.  
Usually the remote IP address is the endpoint IP address of the server L2 VPN session. For more information, see [Create a server L2 VPN session with NSX in the Cloud Director site](#).
  - e) Under the Client Network column, to create an L2 stretch across the networks select an on-premises VLAN network against each server network in the cloud site.  
The number of available client networks for selection, depends on the cloud site version of VMware Cloud Director. For information about the versions of VMware Cloud Director, see the prerequisites in [Create a server L2 VPN session with NSX in the Cloud Director site](#).
8. On the **Ready To Complete** page, to create the L2 VPN stretch click **Finish**.

The client L2 VPN session on-premises is created and the L2 stretch across the cloud site is complete.

You can now use this stretched network when migrating some virtual machines to the cloud that are a part of a single on-premises workload, keeping the network connectivity between the migrated virtual machines in the cloud site and the non-migrated virtual machines on-premises. You can easily manage the L2 stretch by using the management interface of the On-Premises to Cloud Director Replication Appliance, or directly by using the management interface of the NSX Autonomous Edge.

#### Related Links

[Deploy an NSX Autonomous Edge appliance on-premises on page 152](#)

On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

[Register the NSX Autonomous Edge on-premises on page 154](#)

On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

[Configure the networks of the NSX Autonomous Edge on-premises on page 155](#)

After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

## Back up the appliance

In the appliance management interface, you generate new a appliance backup archive. Download the backup archive as a file and then preserve it on an external storage device for future restore of the stack to that moment in time.

- Verify that before taking a backup, the appliance is operational.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least 35%.

Since VMware Cloud Director Availability 4.4, backing up the On-Premises to Cloud Director Replication Appliance can be allowed from the cloud site. Backing up the On-Premises to Cloud vCenter Replication Appliance or the vCenter Replication Management Appliance can only be performed locally from the appliance.

This backup archive contains the following information from the appliance:

- Configuration files
- Public certificate
- Keystore
- Database dump

This information is stored as an `.enc` appliance backup file. When generating the backup, you provide a password that encrypts the appliance backup file to preserve any sensitive information.

The backup does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The time server configuration.

Locally, the appliances can store up to 24 backup archives on their internal storage. Past that number, you must delete some of them, or attempting to create another backup, shows `Backup quota exceeded. Number of allowed backups: 24, current backup count: 24`. Such limit does not apply for the **Scheduled backup archives** that are stored on an external SFTP storage. For more information, see [Schedule backup archives](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, click **Backup Archives**.
3. In the **Backup archives** page, click **Generate new**.
4. In the **Create backup archive** window, create a backup archive of the appliance.
  - a) In the **Password** text box, enter the password to protect and encrypt the backup archive.
 

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as `& # %` .
  - b) In the **Confirm Password** text box, reenter the password to confirm the password that encrypts the backup.
  - c) Store this password in a safe place since it cannot be restored later.
  - d) Click **Create**.

In the **Backup archives** page, you see the progress of generating the new backup archive.

5. To download one of the generated backup archives, in the Backup Id column, click the *backup id* link.
  - a) In the **Download Backup Archive** window, to save the backup file locally click **Download**.
 

In your Web browser, the `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file starts downloading.
  - b) Store the locally downloaded backup file and its password for future restore of the appliance to that moment in time.

The appliance backup `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file downloaded locally.

You can later use one of the locally downloaded backup files to restore the appliance to that moment in time. For more information, see [Restore the appliance](#).

## Restore the appliance

You restore the appliance by deploying a new appliance with the same network settings and by using a single locally downloaded `.enc` backup file.

- Verify that you downloaded the `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file locally and you have the password for the backup.
- Verify that the version and the network settings of the newly deployed appliance exactly match the version and the network settings of the backed-up appliance.
- Verify that before restoring the newly deployed appliance, the existing backed-up on-premises appliance is powered off.



### CAUTION

Restoring while the appliance is operational may corrupt the replications.

The `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file contains all the backup information to restore the appliance to the `date-timestamp`. For information about taking a backup, see [Back up the appliance](#).

### NOTE

Restoring backups containing deleted replications at the time of restore:

Go to the management interface of the restored appliance at `https://Appliance-IP-Address:8043`. On the **System Tasks** page or the **Replication Tasks** page, the **Reload destination** tasks run indefinitely or fail with a `Lock acquisition timed out for object: 'H4-id'` for each replication that is not present since restoring the backup. To manually delete these replications, click the **Emergency Recovery** page, select them then click **Delete**.

1. Log in to management interface of the newly deployed appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Log in by entering the **root** user password that you set during the OVA deployment.
2. In the **VMware Cloud Director Availability Appliance Password** window, change the initial **root** user password.
  - a) Enter the **root** user password that you set during the OVA deployment.
  - b) Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:
    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as `& # %`.
3. Under **Steps to restore from archive**, click **Import the backup archive in...**
4. In the **Restore from backup archive** window, browse for the appliance backup file, enter its password, and restore the appliance.
  - a) Click **Browse** and select the locally downloaded `.enc` appliance backup file.
  - b) In the **Password** text box, enter the password used to encrypt the backup.
  - c) Click **Restore**.

The restore starts and might take a while to complete. You cannot log in to the appliance while the restore is in progress.

After the restore completes, the appliance restarts.

5. Optional: After the services start, verify that the restore is successful.
  - a) Log in to the management interface of the newly restored appliance.

**NOTE**

After restoring, when you have a configured backup schedule the following message appears in the **Backup Archives** page under **Scheduled backup tasks**: `Generate backup archive task`, which generated the scheduled backup archive used for the restore, shows `Task canceled due to service reboot`.

- b) In the left pane, click **System Tasks**.  
After restore, the `Generate backup archive task`, which generated the backup archive used for the restore, also shows `Task canceled due to service reboot`.
- c) Verify the Target of `task.restore.backup`.

A misalignment between the replication settings stored in the database and the ones loaded from the backup might happen. As a result, RPO violations, instances with differing numbers, and others might be present. As a resolution, reapply the replication settings by reconfiguring the affected replications .

**NOTE****Instances**

After restore, the instances might disappear for some replications. In most cases, the data is not lost and a subsequent synchronization transfers only a delta. To get an instance, either wait for automatic synchronization, or perform a synchronization manually.

You can perform replication workflows and after confirming that the newly restored appliance is operational, you can decommission the backed-up appliance that is powered off.

## Managing pairing with on-premises sites and between provider sites

Re-establish the trust between two sites by re-pairing them or break the trust by un-pairing the sites. These pairing procedures between two peer sites apply for any of the following three appliance roles: On-Premises to Cloud Director Replication Appliance, On-Premises to Cloud vCenter Replication Appliance, and vCenter Replication Management Appliance roles.

### Manage an on-premises site pairing with a Cloud Director site

To manage the pairing between an on-premises site and a Cloud Director site, you can perform the following procedures:

**NOTE**

Since VMware Cloud Director Availability 4.7, for pairing the on-premises site with a Cloud Director site, in addition to using a local user, you can alternatively use an API token from VMware Cloud Director. For information about generating the token in VMware Cloud Director, see [Generate an API access token for pairing from VMware Cloud Director](#).

1. Pair an On-Premises to Cloud Director Replication Appliance with the Cloud Director site. For information about the initial pairing, see [Configure the On-Premises to Cloud Director Replication Appliance](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
2. Re-pair the On-Premises to Cloud Director Replication Appliance with the Cloud Director site. For information about re-establishing the trust, see [Repair with a remote site](#).
3. Un-pair the On-Premises to Cloud Director Replication Appliance. For information about removing the trust, see [Unpair a remote site](#).

## Manage pairing for vSphere DR and migration between vCenter sites

To manage the pairing between two vCenter sites for vSphere DR and migration, you can perform the following pairing procedures:

Procedure	vSphere DR and migration between vCenter sites
Initial configure pair	<ul style="list-style-type: none"> <li>• Pair an On-Premises to Cloud vCenter Replication Appliance with the vCenter Replication Management Appliance in the provider cloud site.</li> <li>• Pair between two provider cloud vCenter sites, each running a vCenter Replication Management Appliance.</li> </ul> <p>For information about the initial pairing, see <a href="#">Configure and pair both appliances for vSphere DR and migration</a> in the <i>Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site</i>.</p>
Re-pair	<ul style="list-style-type: none"> <li>• Re-pair the On-Premises to Cloud vCenter Replication Appliance with the vCenter Replication Management Appliance in the provider cloud site.</li> <li>• Re-pair both provider cloud vCenter sites, each running a vCenter Replication Management Appliance.</li> </ul> <p>For information about re-establishing the trust, see <a href="#">Repair with a remote site</a>.</p>
Un-pair	<ul style="list-style-type: none"> <li>• Un-pair the On-Premises to Cloud vCenter Replication Appliance.</li> <li>• Un-pair the two vCenter Replication Management Appliance instances.</li> </ul> <p>For information about removing the trust, see <a href="#">Unpair a remote site</a>.</p>

## Generate an API access token for pairing from VMware Cloud Director

In VMware Cloud Director, once the **provider** allows **tenant** access control on the user's own API token, the **tenant** generates an API token for use in VMware Cloud Director Availability instead of the local user for pairing, re-pairing and removing pairing of an on-premises to a cloud site.

- Verify that the version of VMware Cloud Director is 10.4.1 or later.
- Verify that the version of VMware Cloud Director Availability is 4.7 or later.
- Verify that to allow **tenant** access control on the user's own API token, you can access VMware Cloud Director as a **System Administrator** user.

### NOTE

With version 10.4.1, VMware Cloud Director started the deprecation process for local users. VMware Cloud Director continues to fully support the use of local users while they are under deprecation.

Due to the upcoming deprecation of local users, pairing, re-pairing and removing pairing of an on-premises to a Cloud Director site can also be performed with an API token from VMware Cloud Director. Local users can still be used for these procedures, as long as they are available in VMware Cloud Director.

By default, in VMware Cloud Director the tenants cannot generate API tokens. The **provider** must first allow the **tenant** to generate an API token in VMware Cloud Director that can be then used in VMware Cloud Director Availability for pairing, re-pairing and removing pairing.

For information about the API tokens, see [Generate an API Access Token Using Your VMware Cloud Director Service Provider Admin Portal](#) in the *VMware Cloud Director* documentation.

1. Login in VMware Cloud Director as a **System Administrator** user then click the **Administration** tab.
2. In the left pane, under **Tenant Access Control** click **Rights Bundles**.
3. On the **Rights Bundles** page, click **Add**.
4. In the **Add Rights Bundle** window, configure the following right in the bundle then click **Save**.
  - a) Enter a **Name** and optionally a **Description**.
  - b) Activate the **Show implied rights** toggle.
  - c) Under **Access Control** expand the **User** section.
  - d) Activate the **Manage User's own API token** check box.
5. To publish the new right to all **tenant** users, select the new bundle and click **Publish**.
6. Logout, then log back in VMware Cloud Director as a the **tenant** user to be used for the pairing later.
7. In the top right corner of the navigation bar, click your **tenant user Name** then select **User preferences**.
8. Under the **API Tokens** section, click **New**.
9. In the **Generate General Token** window, create a general token for the currently logged **tenant** user.
  - a) Enter a **Client Name** for the token.
  - b) Click **Create**.
 

You see `Please wait followed by Your token was generated successfully message`.
  - c) Click **Copy** then store the token because it appears only once.
  - d) Once you store the token, click **OK**.

#### NOTE

After you click **OK**, you cannot retrieve this token again, you can only revoke it.

Once used for pairing, the token is not stored anywhere in VMware Cloud Director Availability and you can revoke it without affecting the pairing.

For future pairing, re-pairing, or removing pairing, once revoked, a new token must be generated in VMware Cloud Director and provided to VMware Cloud Director Availability.

The token in your clipboard is ready for using in VMware Cloud Director Availability.

You can use this user token to pair, re-pair, or unpair the on-premises site with a cloud site. For information about the pairing procedures for this token, see the [Manage an on-premises site pairing with a Cloud Director site](#) section.

## Repair with a remote site

To reestablish the trust with a remote site, repair with the remote site by using the management interface of the appliance.

Verify that for vSphere DR and migration, before re-pairing both sites are upgraded to version 4.5 or later.

This procedure applies for the following appliance roles:

- On-Premises to Cloud Director Replication Appliance, see step 2.
- On-Premises to Cloud vCenter Replication Appliance, see step 3.
- vCenter Replication Management Appliance, see step 3.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the `root` or the `single sign-on` user credentials.
  - c) Click **Login**.
2. To re-pair, depending on the appliance role and the remote site choose the appropriate repair method and complete the pairing step.
  - For vSphere DR and migration, to re-establish the trust between vCenter Server sites skip this step and complete step 3.
  - Alternatively, to re-establish the trust with a cloud site backed by VMware Cloud Director follow this step and skip step 3.
  - a) In the left pane, click **Settings**.
  - b) Under **Site settings** next to **Pairing**, click **Repair** then complete the **Update Pairing** wizard.
  - c) On the **Site Details** page, verify this on-premises site name and description then click **Next**.
  - d) On the **Lookup Service** page, enter the `single sign-on` user credentials for the local vCenter Server Lookup service in the on-premises site then click **Next**.
  - e) On the **Cloud Service Details** page, configure the following details then click **Next**.

Option	Description	
Public Service Endpoint address	Enter the address of the cloud site Public Service Endpoint: 443 as given by the provider.	
Authorization type	When using token authentication for VMware Cloud Director, select <b>VCD API Token</b> .	Alternatively, when using local users in VMware Cloud Director, select <b>VCD Local User (DEPRECATED)</b>
	In the <b>Organization</b> text box, enter the name of the organization.	In the <b>Organization Admin</b> text box, enter the user name of a VMware Cloud Director <b>organization administrator</b> user. For example, enter <code>admin1@org</code> .
	In the <b>VCD API Token</b> text box, paste the token from VMware Cloud Director. Once used for pairing, the token is not stored and can be revoked at any time. For more information, see <a href="#">Generate an API access token for pairing from VMware Cloud Director</a> .	In the <b>Organization Password</b> text box, enter the <code>password</code> of the VMware Cloud Director <b>organization administrator</b> user.

Option	Description
Allow access from Cloud	<p><b>Activated access from the cloud site:</b></p> <p>Allows privileged VMware Cloud Director users like the cloud provider and the organization administrators without authenticating to the on-premises site to perform operations from the VMware Cloud Director Availability Tenant Portal.</p> <ul style="list-style-type: none"> <li>• Browse and discover on-premises workloads to replicate them to the cloud site.</li> <li>• Reverse existing replications from the cloud site to the on-premises site.</li> <li>• Replicate cloud site workloads to the on-premises site.</li> </ul> <p><b>Deactivated cloud site access:</b></p> <ul style="list-style-type: none"> <li>• Configuring a new replication requires users to explicitly authenticate to the on-premises VMware Cloud Director Availability Tenant Portal.</li> <li>• Cannot reverse existing replications to the on-premises site.</li> <li>• Allows privileged VMware Cloud Director users to modify existing replications and perform migrate or failover.</li> </ul>
Allow log collection from Cloud	<ul style="list-style-type: none"> <li>• To simplify troubleshooting, activate log collection from the cloud site. This allows the cloud provider and the organization administrators without authenticating to each paired on-premises appliance to obtain its logs.</li> <li>• Leave cloud site log collection deactivated to require authenticating to the on-premises appliance management interface for downloading the on-premises appliance logs.</li> </ul>

If the cloud site does not use a valid CA-signed certificate, verify the thumbprint and accept the SSL certificate of the Public Service Endpoint.

- f) On the **Ready to Complete** page, optionally, reconfigure the on-premises local placement, and to complete the wizard click **Finish**.
- You can use the existing placement of the on-premises replications by leaving the **Configure local placement now** toggle deactivated.
  - To reconfigure the cloud to on-premises placement, activate the **Configure local placement now** toggle then complete the **Configure Placement** wizard.

3. Alternatively, to re-establish the trust with the remote vCenter Server site, complete this step.

On-premises to provider pairing is managed only from the on-premises site.

- a) In the left pane, click **Peer Sites**.
- b) To re-pair, select the site and click **Repair**.
- c) In the **Update Pairing** window, depending on which appliance initiates the repair, enter the following pairing details then click **Update**.
  - As **tenant**, initiate and complete the repair only from the On-Premises to Cloud vCenter Replication Appliance. The On-Premises to Cloud vCenter Replication Appliance does not require a publicly available address.

Public Service Endpoint	<ul style="list-style-type: none"> <li>• Enter the address of the Public Service Endpoint : 443 of the vCenter Replication Management Appliance of the provider.</li> <li>• Alternatively, enter port 8048 only when both appliances reside in the same network.</li> </ul>
SSO Username	<p>Enter the user name of the single-sign-on user from the provider site for the pairing. For example, enter <code>Administrator@vsphere.local</code>.</p> <p>To pair the on-premises appliance with the provider site it is recommended to use a less-privileged user that belongs to the <b>VRUSERS</b> group in the provider site. Alternatively, you can still use a user member of the <b>VRADMINISTRATORS</b> or the <b>ADMINISTRATORS</b> groups in the provider site. For information about these groups, see <a href="#">Users Roles Rights and Sessions</a> in the <i>Security Guide</i>.</p>
SSO Password	Enter the password of the remote single-sign-on user in the provider site.
Description	Optionally, enter a description for this pair.

- As **provider**, when repairing vCenter Replication Management Appliance with vCenter Replication Management Appliance, initiate the pairing by entering:

Public Service Endpoint	<ul style="list-style-type: none"> <li>• Enter the address of the vCenter Replication Management Appliance : 443 in the remote cloud vCenter Server site.</li> <li>• Alternatively, enter port 8048 only when both appliances reside in the same network.</li> </ul>
Description	Optionally, enter a description for this pair.

When repairing two vCenter Replication Management Appliance instances, after initiating pairing from the local site, to complete the pairing log in the remote vCenter Replication Management Appliance and repeat this step to also repair the remote site with the local vCenter Replication Management Appliance.

- d) Verify the thumbprint and accept the SSL certificate of the remote appliance.
4. Verify that the connectivity to the paired site is operational.
- a) In the left pane, click **System Health**.
  - b) Verify that for the site you re-paired, **Service connectivity** shows a green **OK** status.

The pairing between the local and the remote site is re-established.

## Unpair a remote site

To remove the established trust between the local site and a remote site, unpair the remote site from the local site by using the appliance management interface.

Delete all configured replications between the local site and the remote site.

This procedure applies for the following appliance roles:

- On-Premises to Cloud Director Replication Appliance, see step 2.
- On-Premises to Cloud vCenter Replication Appliance, see step 3.
- vCenter Replication Management Appliance, see step 4.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. Remove the established trust between the On-Premises to Cloud Director Replication Appliance and the Cloud Director site.
  - If this On-Premises to Cloud Director Replication Appliance is still paired with the cloud site, first, from the on-premises site unpair the cloud site, then similarly from the cloud site, delete the remaining on-premises site pairing.
  - If from the cloud site this On-Premises to Cloud Director Replication Appliance pairing is already deleted, remove the remaining pairing record in the on-premises site. When done, you see a red `Peer site 'on-prem-site-name' was not found` message because the remote site pairing is removed already.
  - a) In the left pane, click **Settings**.
  - b) Under **Site settings** next to **Pairing**, click **Unpair**.
  - c) In the **Unpair from cloud site** window, authorize with VMware Cloud Director then click **Apply**.
    - When using token authentication for VMware Cloud Director, from the **Authorization type** drop-down menu, select **VCD API Token**, enter the **Organization**, then paste the **VCD API Token**. For more information, see [Generate an API access token for pairing from VMware Cloud Director](#).
    - Alternatively, when using local users in VMware Cloud Director, from the **Authorization type** drop-down menu, select **VCD Local User (DEPRECATED)**, then enter the **Organization Admin** user name and **Organization Password**.

The **Pairing** section shows `Not configured` and the cloud site registration is removed.
3. Remove the established trust between the On-Premises to Cloud vCenter Replication Appliance and the provider cloud site.
  - a) In the left pane, click **Peer Sites**.
  - b) Select the cloud site and click **Delete**.
4. Remove the established trust between two provider vCenter Replication Management Appliance instances.
  - a) In the left pane, click **Peer Sites**.
  - b) Select the remote site and click **Delete**.
  - c) To delete the remaining pairing record, log in to the remote site and repeat this step.

The pairing between this local site and the remote site is removed.

- If you performed this procedure from the on-premises site first, in the cloud site backed by VMware Cloud Director the on-premises site still shows as paired. After unpairing the on-premises site, the **service provider** can remove the

remaining record from the cloud site for the unpaired on-premises site. For more information, see [Unpair paired sites from the Cloud Director site](#).

- You can remove the established connection between the on-premises appliance and vCenter Server, see [Unregister the VMware Cloud Director Availability vSphere Client Plug-In from vCenter Server](#).
- You can repair with the remote site, see [Repair with a remote site](#).

## Replace the SSL certificate of the appliance

In an on-premises or in a cloud vCenter Server site, to replace the SSL certificate of the VMware Cloud Director Availability appliance, use its service management interface.

This procedure applies for any of the following appliance roles:

- **On-premises appliances roles:**
  - On-Premises to Cloud Director Replication Appliance
  - On-Premises to Cloud vCenter Replication Appliance
- **Provider appliances:**
  - vCenter Replication Management Appliance
  - For information about replacing the Replicator Appliance certificate, see [Replace the SSL certificate of the Replicator Service](#).

For information about replacing the certificates in a cloud site backed by VMware Cloud Director, see [Certificates management in the Cloud Director site](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, click **Settings**.
3. Under **Appliance settings**, next to **Certificate** replace the appliance certificate and click **Apply**.
  - To import an SSL certificate, click **Import** and in the **Import Certificate** window, enter the certificate details.
    - a) Enter the password that protects the keystore and the certificate private key.
    - b) Click **Browse** and select the PKCS#12 file.
  - Alternatively, to generate a new self-signed certificate, click **Regenerate**.

After replacing the certificate, the VMware Cloud Director Availability services that run in the appliance restart.

4. After replacing the certificate, redeploy the VMware Cloud Director Availability vSphere Client Plug-In by reapplying the vCenter Server Lookup service address.
  - a) Under **Service endpoints**, next to **Lookup Service Address** click **Edit**.
  - b) Enter the single-sign-on user credentials and click **Apply**.

Option	Description
<b>SSO Admin Username</b>	Enter the vSphere <b>administrator</b> user name for the vCenter Server Lookup service that belongs to the <b>ADMINISTRATORS</b> group.
<b>Password</b>	Enter the vSphere <b>administrator</b> user password for the vCenter Server Lookup service.

5. After replacing either or both of their certificates, repair the On-Premises to Cloud vCenter Replication Appliance and the vCenter Replication Management Appliance.

Skip this step after replacing the certificate of the On-Premises to Cloud Director Replication Appliance.

- a) After replacing the local site certificate, to re-establish the trust log in to the appliance management interface of the remote site.
- b) In the left pane, click **Settings**.
- c) Under **Site settings** next to **Pairing**, click **Repair**.
- d) To re-establish the trust with the site that has a replaced certificate, in the **Update Pairing** window confirm the Public Service Endpoint.

Service Endpoint	<ul style="list-style-type: none"> <li>• Enter the address of the Public Service Endpoint:443 of the remote VMware Cloud Director Availability appliance.</li> <li>• Alternatively, enter port 8048 when both VMware Cloud Director Availability appliances reside in the same network.</li> </ul>
Description	Optionally, enter a description for this vSphere site as an identifier.

Verify the thumbprint and accept the SSL certificate of the Public Service Endpoint in the remote vCenter Server site.

- e) To re-establish the trust after replacing the remote site certificate, log in to the local site appliance management interface and repeat this step.

## Change the IP address of the appliance

By using the appliance management interface, change its IP address. Open the management interface using the new IP address, update the traffic control settings with the new IP address and re-register with the vCenter Server Lookup service. By returning to the appliance management interface, repair the Replicator Service. Finally, repair from the remote site by using the updated Public Service Endpoint address.

Verify that VMware Cloud Director Availability 4.4 or later is deployed in the vCenter Server site.

### NOTE

Applying any network changes leads to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that is being reconfigured.

Perform the exact steps for each appliance role. This procedure applies to the following appliance roles:

- **On-premises appliances roles:**
  - On-Premises to Cloud Director Replication Appliance - perform steps 1-5 only.
  - On-Premises to Cloud vCenter Replication Appliance - perform steps 1-3, then perform steps 5-13.
- **Provider appliances:**
  - vCenter Replication Management Appliance - perform steps 1-3, then perform steps 5-15.
  - Replicator Appliance - perform steps 1-4, then perform steps 12 and 13 only.

For information about configuring the appliance IP address in a cloud site backed by VMware Cloud Director, see [Network settings configuration](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. Change the network adapter IP address of the appliance.
  - a) In the left pane, click **Settings**.
  - b) Under **Appliance settings**, expand the **Network** section.  
You can see all the network adapters that are added to the appliance.
  - c) To change the IP address, next to a network adapter name, for example **ens160**, click **Edit**.
  - d) In the **Settings** window for the selected network adapter, configure its network settings and click **Apply**.

IP Mode	Select either: <ul style="list-style-type: none"> <li>• <b>IPv4</b></li> <li>• <b>IPv6</b></li> <li>• <b>Unconfigured</b> turns off this network adapter and deletes all of its settings, including static routes. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.</li> </ul>
Type:DHCP	<p><b>NOTE</b> After selecting <b>DHCP</b> to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed. To manually add, next to <b>Network</b>, click <b>Edit</b> then enter:</p> <ul style="list-style-type: none"> <li>• <b>DNS servers</b></li> <li>• <b>Domain Search Path</b></li> </ul>
Type: Static	<p>Enter the static configuration.</p> <ol style="list-style-type: none"> <li>1. In the <b>Address/Prefix</b> text box, enter a CIDR address - IP address, followed by a forward slash and a network mask or a prefix length. For example, enter <code>10.20.30.41/21</code>.</li> <li>2. In the <b>Gateway</b> text box, enter a gateway that is in the same network as the provided IP address. For each IP mode, you can use only one default gateway. If you are configuring a second adapter in the same IP mode, you must not enter a default gateway.</li> <li>3. In the <b>MTU (bytes)</b> text box, enter the maximum transmission unit size in bytes. The default is 1500 bytes.</li> </ol>

The updated IP address applies and the management interface keeps showing a continuously spinning progress indicator. After timing out, you see a red error message `Timeout has occurred` indicating you to go to the management interface by using the new IP address.

3. Log back in to the management interface by using the new IP address of the appliance.
  - a) In a Web browser, go to `https://Appliance-New-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
4. Update the **Traffic Control** addresses of the appliance.
  - Perform this step only for On-Premises to Cloud Director Replication Appliance and for Replicator Appliance.
  - Skip this step for On-Premises to Cloud vCenter Replication Appliance and for vCenter Replication Management Appliance.
  - a) In the left pane, click **Settings**.
  - b) Under **Appliance settings**, next to the **Traffic Control** section, click **Edit**.
  - c) In the **Traffic Control** window, select the new IP address of the network adapter then click **Apply**.

Management Address	Select the new IP address for the network adapter.
NFC Address	Select the new IP address for the network adapter.
LWD Address	Select the new IP address for the network adapter.

5. Re-register the appliance with the vCenter Server Lookup service.
  - a) Under **Service endpoints**, next to **Lookup Service Address**, click **Edit**.
  - b) In the **Lookup Service Details** window, re-enter the credentials then click **Apply**.
  - c) Verify the thumbprint and accept the SSL certificate of the vCenter Server Lookup service.

**NOTE**

This step completes changing the IP address of:

- On-Premises to Cloud Director Replication Appliance is now configured with the new IP address.

Proceed with the remaining steps when changing the IP address for one of the following appliance roles:

- On-Premises to Cloud vCenter Replication Appliance
- vCenter Replication Management Appliance

Skip the remaining steps and proceed directly from step 12 when changing the IP of an external:

- Replicator Appliance

6. Log in to the management interface of the internal Replicator Service of the appliance.
  - a) In a Web browser, go to `https://Appliance-New-IP-Address:8440/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
7. Update the **Traffic Control** addresses for the internal Replicator Service.
  - a) In the left pane, click **Settings**.
  - b) Under **Appliance settings**, next to the **Traffic Control** section, click **Edit**.
  - c) In the **Traffic Control** window, select the new IP address of the network adapter then click **Apply**.

Management Address	Select the new IP address for the network adapter.
NFC Address	Select the new IP address for the network adapter.
LWD Address	Select the new IP address for the network adapter.

8. Log in to the management interface of the Tunnel Service in the appliance.
  - a) In a Web browser, go to `https://Appliance-New-IP-Address:8442/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
9. Update the **Traffic Control** addresses for the Tunnel Service.
  - a) In the left pane, click **Settings**.
  - b) Under **Appliance settings**, next to the **Traffic Control** section, click **Edit**.
  - c) In the **Traffic Control** window, select the new IP address of the network adapter then click **Apply**.

Tunnel Address	Select the new IP address for the network adapter.
----------------	--

10. Connect to the VMware Cloud Director Availability appliance by using a Secure Shell (SSH) client.
  - a) Open an SSH connection to *Appliance-IP-Address*.
  - b) Authenticate as the **root** user.
11. Update the appliance IP address in the following configuration file then restart the service.
  - a) Run `vi /opt/vmware/h4/manager/config/application.properties`, press `/` and paste `tunnel.data.endpoint` then press `Insert` and update the appliance IP address.
 

```
tunnel.data.endpoint=https://Appliance-New-IP-Address:port
```
  - b) Restart the service.
 

```
systemctl restart manager
```
12. Log back in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-New-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
13. Repair all Replicator Service instances by updating its Public Service Endpoint address.
  - a) In the left pane, click **Replicator Services**.
  - b) Select a Replicator Service instance listed in red state and click **Repair**.  
Repeat this step and repair each Replicator Service instance that is listed in red state.
  - c) In the **Details for the Replicator Service** window, update the Public Service Endpoint address with the new IP address then click **Apply**.

Endpoint Address	To update the Public Service Endpoint of the Replicator Service, enter the <i>Appliance-New-IP-Address</i> .
Appliance Password	Enter the password for the appliance <b>root</b> user.
SSO Admin Username	Enter the vSphere single-sign-on <b>administrator</b> <i>user name</i> for the vCenter Server Lookup service that belongs to the <b>ADMINISTRATORS</b> group.
SSO Password	Enter the vSphere single-sign-on <b>administrator</b> <i>password</i> for the vCenter Server Lookup service.

- d) Verify the thumbprint and accept the SSL certificate.

**NOTE**

This step completes changing the IP address of the following appliance roles:

- On-Premises to Cloud vCenter Replication Appliance is now configured with the new IP address.
- Replicator Appliance is now configured with the new IP address.

Complete the remaining steps only when not using DNAT when changing the IP address for the following appliance role:

- vCenter Replication Management Appliance.

Skip the remaining steps when using DNAT for the vCenter Replication Management Appliance. Instead, in the provider site you must update the DNAT firewall rule with the new IP address of the vCenter Replication Management Appliance.

- Update the **Public Service Endpoint** of the vCenter Replication Management Appliance with its new IP address.
  - In the left pane, click **Settings**.
  - Under **Service endpoints**, next to **Service Endpoint Address** click **Edit**.
  - In the **Service Endpoint address** window, enter the new IP address and click **Apply**.
- In the remote tenant site, to update the pairing to use the new IP address, re-pair with the provider site.
  - From the remote tenant site, in the left pane click **Peer Sites**.
  - Select the provider site with the updated Public Service Endpoint address and click **Repair**.
  - In the **Update Pairing** window, update the **Public Service Endpoint** with the new IP address and click **Update**.

Public Public Service Endpoint	Enter the updated <i>Appliance-New-IP-Address</i> .
SSO Username	Enter the vSphere single-sign-on <b>administrator</b> <i>user name</i> for the vCenter Server Lookup service that belongs to the <b>ADMINISTRATORS</b> group.
SSO Password	Enter the vSphere single-sign-on <b>administrator</b> <i>password</i> for the vCenter Server Lookup service.
Description	Optionally, enter a description for the pair.

- Verify the thumbprint and accept the SSL certificate of the provider site.

The VMware Cloud Director Availability appliance now uses the new IP address.

## Unregister the VMware Cloud Director Availability vSphere Client Plug-In from vCenter Server

To remove the established connection between the VMware Cloud Director Availability appliance and the vCenter Server instance, you remove the vCenter Server Lookup service registration by using the appliance management interface.

- Log in to the management interface of the VMware Cloud Director Availability appliance.
  - In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - Click **Login**.
- In the left pane, click **Settings**.
- Under **Service endpoints** next to **Lookup Service address**, click **Remove plugin**.
- In the **Remove vSphere Plugin** window click **Remove plugin**.

After you log out and log in to vCenter Server, you can see that the VMware Cloud Director Availability vSphere Client Plug-In is unregistered from the vCenter Server instance.

You can use this appliance again, after running the initial setup wizard. If this site is still paired with a cloud site, use the same vCenter Server Lookup service as in the configuration before the pairing.

## Monitoring and troubleshooting

In the disaster recovery environment, you can configure backup schedule, diagnose and correct problems related to VMware Cloud Director Availability operation, logging, password changes, collect support bundles, and others.

Cloud Director site	On-premises or provider vCenter Server sites
In a VMware Cloud Director Availability cloud site, backed by VMware Cloud Director	In either: <ul style="list-style-type: none"> <li>• a VMware Cloud Director Availability on-premises vCenter Server site</li> <li>• or in a provider VMware Cloud Director Availability cloud vCenter Server site</li> </ul>

Perform the following administration tasks in this current chapter by using the appliances management interface or in the disaster recovery infrastructure.

### Support Knowledge Base

For troubleshooting information from the knowledge base articles for VMware Cloud Director Availability, see the latest [Cloud Director Availability KB articles](#) in the *VMware Knowledge Base*.

## Events and notifications

For auditing purposes, you can monitor the events that VMware Cloud Director Availability generates by using a syslog server, by using email delivery for the notifications, and for Cloud Director sites, you can monitor the events also in VMware Cloud Director.

### Event Notifications Delivery Channels

To aid with auditing and monitoring the cloud site, VMware Cloud Director Availability delivers information about significant events by using the following delivery channels, depending on the cloud site:

Cloud site	Cloud Director sites	vSphere DR and migration sites
Delivery channels	<p><b>Syslog</b></p> <p>As <b>provider</b>, you can use the syslog protocol for delivering the event notifications to a preconfigured syslog server, for example, vRealize Log Insight for auditing.</p> <p>Depending on the cloud site, to enter the syslog server IP address and its UDP port, see either</p> <ul style="list-style-type: none"> <li>• <a href="#">Configure provider event notifications in the Cloud Director site</a></li> <li>• <a href="#">Configure event notifications for vSphere DR and migration</a></li> </ul>	
	<p><b>Email</b></p> <p>This event notification delivery channel is available for both <b>provider</b> and <b>Admin</b>.</p> <p>Either in VMware Cloud Director, as an <b>OrgAdmin</b> user, you can register a Simple Mail Transfer Protocol for the events notifications. VMware Cloud Director Availability can use the SMTP configuration of VMware</p> <ul style="list-style-type: none"> <li>• For information about configuring the email notifications as <b>provider</b>, see <a href="#">Configure the System Email VMware Cloud Director Service Provider Admin Guide</a>.</li> <li>• For information about configuring the email notifications as <b>tenant</b> user, see <a href="#">Modify Your Email Settings Cloud Director Tenant Guide</a>.</li> </ul> <p>Alternatively, since VMware Cloud Director Availability 4.6.1 as <b>provider</b> or as <b>tenant</b> you <b>Set custom SMTP settings</b> and configure the email settings for the selected events notification</p>	<p><b>Email</b></p>

Cloud site	Cloud Director sites	vSphere DR and migration sites
	<p><b>Cloud Director</b></p> <p>For Cloud Director sites, this event notification delivery channel is available for both <b>provider</b> and <b>consumer</b> users. In VMware Cloud Director, as an <b>OrgAdmin</b> user, you can monitor VMware Cloud Director Availability events and also monitor events about user actions for replications owned by the same user. As a <b>System</b> user, you can monitor all events, including the events that <b>OrgAdmin</b> users see, with additional events.</p> <p>VMware Cloud Director maintains an audit log, called <b>Audit Trail</b>, per organization, allowing tenants to inspect the events themselves. For more information, see the <a href="#">Multitenant Logging with VMware Cloud Director</a>.</p> <p>The <b>Audit Trail</b> receives all external events to VMware Cloud Director, including all VMware Cloud Director Availability events, and resides in a designated space, with its own retention rules, separate from the persistence of the conventional events.</p> <p>All events that VMware Cloud Director Availability sends to VMware Cloud Director are marked as <b>audit</b>.</p>	N/A

Each of these delivery channels carries the same notification information, formatted according to the delivery method. To receive events notifications, you can use one or multiple delivery channels simultaneously.

#### NOTE

When sent by email, the events under the **User Activities** section are batched per tenant/activity type and aggregated in one message sent every 60 minutes or every 300 events, whichever comes first.

### Audit Events

The ISO 27001 and PCI-DSS auditing requirements as logged by VMware Cloud Director Availability:

- Logs any administrative, **root**, or elevated access to the system, for example, user *X*, successful login at *timestamp* from *IP-address/FQDN*.
- Logs any unsuccessful login attempts for all users to the system, for example, user *Y*, failed login attempt at *timestamp* from *IP-address/FQDN*.
- Logs any passive operations of all users, for example, running RPO compliance reports, system tasks review, data stores review, and system health review.
- Logs any configuration changes, including creation, modification, and deletion, under the following sections:
  - **Replications** section activities:
    - **Incoming Replications** - logs any user-executed actions, for example, **Migrate**, **Failover**, and **Test**.
    - **Recovery Plans** - logs all recovery plan operations.
    - **Start/Stop** events for replication tasks
  - **Configuration** section activities on the pages:
    - **Settings**
    - **Peer Sites**
    - **Policies**
    - **SLA Profiles**
    - **L2 Stretch**
  - **System** section activities:
    - **Datastores > Evacuate**
    - **Support Bundles**
    - **Backup Archives**
    - **Start/Stop** events for **System** tasks
- **Reports** page logs all report-related activities.

- **Session**-related activities, such as:
  - **Login**
  - **Logout**
  - **Login** to *peer* site
  - **Logout** of *peer* site

### **Weekly Summary Report Subscription**

VMware Cloud Director Availability 4.6 and later allows both providers and their tenants to subscribe for a weekly summary email that contains the numbers of active/new/deleted protections and migrations performed last week.

The subscribers remain informed about what is happening with their replications without logging in. Their weekly summary report:

- Counts only incoming replications using the **Classic** data engine to the cloud site.
- Counts the current state at the report runtime both for active protections and for migrations.
- Counts the following numbers for the week:
  - Performed failovers
  - Performed test failovers
  - Performed migrates
  - New protections and new migrations
  - Deleted protections and migrations

For more information, see [Subscribe for weekly summary email](#).

### **Configure provider event notifications in the Cloud Director site**

As a **provider**, you can forward the VMware Cloud Director Availability provider events notifications to a syslog server, to VMware Cloud Director, and or by using email delivery. All the delivery channels carry the same event information.

- Verify that VMware Cloud Director Availability 4.6.1 or later is deployed in the cloud site to be able to **Set custom SMTP settings**.
- To use the email delivery channel for events notifications, verify that you configured the SMTP settings in VMware Cloud Director. For more information, see [Configure the System Email Settings](#) in the *VMware Cloud Director Service Provider Admin Guide*.

Since VMware Cloud Director Availability 4.6, by default the **Cloud Director events** checkbox is active for all event types.

For information about the events and notifications, see [Events and notifications](#).

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/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, under **Configuration** click **Events and Notifications**.

The **Provider event notifications** page opens.

#### **NOTE**

To forward the provider events to the syslog server and to email, first you as a **provider** must configure these delivery channels. While not yet configured, the **Syslog** and the **Cloud Director email** check boxes display `not configured` and remain dimmed.

3. As a **provider**, to configure the syslog server, under **Receive notifications via the following channels** next to **Syslog** click **Configure**.
  - a) In the **Syslog** window, enter the syslog server address and the UDP port.
  - b) To save the syslog configuration, click **Apply**.
4. Optional: To configure the email delivery channel under **Receive notifications via the following channels** next to **Email** choose one of the following configuration options:
  - To configure the SMTP server by using the VMware Cloud Director Provider Portal, next to **Cloud Director Email** click **Configure in Cloud Director**.  
 VMware Cloud Director Availability reads the following SMTP server configuration from VMware Cloud Director:
    - **SMTP server name** is a required field to save the SMTP configuration.
    - **Sender's email address** is a required field to save the SMTP configuration.
    - Recipients, either explicit email addresses or, by default, the email addresses of all organization administrators.
    - Optionally, the **Email subject prefix**.
  - Alternatively, since version 4.6.1 to configure the SMTP settings directly, click **Set custom SMTP settings**. In the **Configure Email Settings** window, enter the following configuration details then click **Apply**.

Option	Description
<b>SMTP server name</b>	You must enter the IP or hostname of an operational SMTP server.
<b>SMTP server port</b>	You must enter the TCP port of the SMTP server. By default, 25.
<b>SMTP server secure mode</b>	Optionally, select the SMTP encryption mode: <ul style="list-style-type: none"> <li>• <b>None</b>, by default.</li> <li>• <b>SSL</b></li> <li>• <b>Start TLS</b></li> </ul>
<b>SMTP authentication required</b>	Optionally, activate the required SMTP authentication, then you must enter: <ul style="list-style-type: none"> <li>• <b>User name</b></li> <li>• <b>Password</b></li> </ul>
<b>Sender's email address</b>	You must enter the email address of the notifications sender.
<b>Email subject prefix</b>	Optionally, enter the subject of the email notifications.
<b>Recipients' email addresses</b>	You must enter one or multiple recipients that all receive the email notifications.

5. Under **Receive notifications for the following events** configure the delivery channels for each event type.

- To configure all event types at once, click **Quick Activate/Deactivate**, then click **Apply**.
- Alternatively, configure each event type by following the next steps:
  - a) Under the **User Activities** section, to configure each event type click **Edit** then to save the settings click **Apply**.

Event type	Activity triggers	Notifications delivery channels
Replications	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Incoming Replications</b></li> <li>• <b>Recovery Plans</b></li> <li>• and <b>Start/Stop</b> events for replication tasks</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
Configuration	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Settings</b></li> <li>• <b>Peer Sites</b></li> <li>• <b>Policies</b></li> <li>• <b>SLA Profiles</b></li> <li>• <b>L2 Stretch</b></li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
System	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Datastores &gt; Evacuate</b></li> <li>• <b>Support Bundles</b></li> <li>• <b>Backup Archives</b></li> <li>• and <b>Start/Stop</b> events for <b>System</b> tasks</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
Reports	Activities on the <b>Reports</b> page in the left pane.	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
Session	Activities related to users sessions: <ul style="list-style-type: none"> <li>• <b>Login</b></li> <li>• <b>Logout</b></li> <li>• <b>Login</b> to <i>peer</i> site</li> <li>• <b>Logout</b> of <i>peer</i> site</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>

b) Under the **Monitoring Events** section, configure the following two monitoring event types.

c) Next to **Service connectivity and monitoring**, click **Edit**, then to save the settings click **Apply**.

Option	Description
Events types	vCenter Server Lookup service connectivity, database connectivity, certificate expiration, administrative remote access, SSH activation, and others.
Receive notifications via the following channels	Select the notifications delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>

Option	Description
Connectivity poll interval	The time interval between polls for connectivity issues. By default, 30 seconds.
Configuration poll interval	The time interval between polls for configuration issues. By default, 1 day.
Certificate expiry threshold	The time before a certificate expires to start forwarding events. By default, 30 days prior.
Policy compliance poll interval	The time interval between polls for policy compliance issues. By default, 60 minutes.

d) Next to **Replication errors and warnings**, click **Edit**, then to save the settings click **Apply**.

Option	Description
Events types	Any replication errors and RPO violations.
Receive notifications via the following channels	Select the notifications delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
Poll interval	The time interval between polls for replication issues. By default, 5 minutes.
RPO violation threshold time	Only forward events for RPO violation time above this threshold. 0 forwards events for any RPO violation. By default, 30 minutes.
RPO violation threshold count	Only forward events for RPO violations count above this threshold. 0 forwards any number of replications with an RPO violation. By default, 0.

6. Optional: To configure the time before forwarding an event again while the condition is still active, under the **Monitoring Events** section next to **Monitoring events forwarding time**, click **Edit**.

a) In the **Notification settings** window, under **Monitoring events forwarding time** enter the forwarding time.

By default, **Monitoring events forwarding time** is 24 hours.

b) To save the configuration for events notifications reposting, click **Apply**.

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

You can monitor VMware Cloud Director Availability by using the syslog server, VMware Cloud Director, or your email client.

You can also subscribe for a weekly summary email. For more information, see [Subscribe for weekly summary email](#).

## Configure tenant event notifications in the Cloud Director site

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

- Verify that VMware Cloud Director Availability 4.6.1 or later is deployed in the cloud site to be able to **Set custom SMTP settings**.
- To use the email delivery channel for events notifications, verify that you configured the SMTP settings in VMware Cloud Director. For more information, see [Configure the System Email Settings](#) in the *VMware Cloud Director Service Provider Admin Guide*.

Since VMware Cloud Director Availability 4.6, by default the **Cloud Director events** checkbox is active for all event types.

For information about the events and notifications, see [Events and notifications](#).

1. Log in to the tenant interface of the Cloud Director Replication Management Appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/login`.
  - b) Enter the **tenant** user credentials and click **Login**.
2. In the left pane, under **Configuration** click **Events and Notifications**.

**NOTE**

To forward the tenant events by email, first configure this delivery channel. While not yet configured, the **Cloud Director email** check box displays `not configured` and remains dimmed.

3. If you logged in as a **provider**, click **Tenants event notifications** then from the **Organization** drop-down menu, select the organization for which you want to edit the events notifications configuration.  
Skip this step when logged as **tenant**, as you can configure the event notifications only for your organization.
4. Optional: To configure the email delivery channel under **Receive notifications via the following channels** next to **Email** choose one of the following configuration options:

- To configure the SMTP server by using the VMware Cloud Director Tenant Portal, next to **Cloud Director Email** click **Configure in Cloud Director**.

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

- **SMTP server name** is a required field to save the SMTP configuration.
- **Sender's email address** is a required field to save the SMTP configuration.
- Recipients, either explicit email addresses or, by default, the email addresses of all organization administrators.
- Optionally, the **Email subject prefix**.
- Alternatively, since version 4.6.1 to configure the SMTP settings directly, click **Set custom SMTP settings**. In the **Configure Email Settings** window, enter the following configuration details then click **Apply**.

Option	Description
<b>SMTP server name</b>	You must enter the IP or hostname of an operational SMTP server.
<b>SMTP server port</b>	You must enter the TCP port of the SMTP server. By default, 25.
<b>SMTP server secure mode</b>	Optionally, select the SMTP encryption mode: <ul style="list-style-type: none"> <li>• <b>None</b>, by default.</li> <li>• <b>SSL</b></li> <li>• <b>Start TLS</b></li> </ul>
<b>SMTP authentication required</b>	Optionally, activate the required SMTP authentication, then you must enter: <ul style="list-style-type: none"> <li>• <b>User name</b></li> <li>• <b>Password</b></li> </ul>
<b>Sender's email address</b>	You must enter the email address of the notifications sender.
<b>Email subject prefix</b>	Optionally, enter the subject of the email notifications.
<b>Recipients' email addresses</b>	You must enter one or multiple recipients that all receive the email notifications.

5. Under **Receive notifications for the following events** configure the delivery channels for each event type.

- To configure all event types at once, click **Quick Activate/Deactivate**, then click **Apply**.
- Alternatively, configure each event type by following the next steps:
  - a) Under the **User Activities** section, to configure each event type click **Edit** then to save the settings click **Apply**.

Event type	Activity triggers	Notifications delivery channels
Replications	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Incoming Replications</b></li> <li>• <b>Recovery Plans</b></li> <li>• and <b>Start/Stop</b> events for replication tasks</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
Session	Activities related to users sessions: <ul style="list-style-type: none"> <li>• <b>Login</b></li> <li>• <b>Logout</b></li> <li>• <b>Login to <i>peer</i> site</b></li> <li>• <b>Logout of <i>peer</i> site</b></li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>

b) Under the **Monitoring Events** section, configure the following monitoring event type.

c) Next to **Replication errors and warnings**, click **Edit**, then to save the settings click **Apply**.

Option	Description
Events types	Any replication errors and RPO violations.
Receive notifications via the following channels	Select the notifications delivery channels: <ul style="list-style-type: none"> <li>• <b>Cloud Director events</b></li> <li>• <b>Cloud Director email</b></li> </ul>
RPO violation threshold time	Only forward events for RPO violation time above this threshold. 0 forwards events for any RPO violation. By default, 0 minutes.
RPO violation threshold count	Only forward events for RPO violations count above this threshold. 0 forwards any number of replications with an RPO violation. By default, 0.

VMware Cloud Director Availability starts forwarding the events notifications to the tenants by using the selected delivery channels.

Tenants can monitor VMware Cloud Director Availability by using VMware Cloud Director, or their email client.

Tenants can also subscribe for a weekly summary email. For more information, see [Subscribe for weekly summary email](#).

## Configure event notifications for vSphere DR and migration

As a **provider** or an **administrator**, you can forward the VMware Cloud Director Availability events notifications to a syslog server, and or by using email delivery. Both delivery channels carry the same event information.

- Verify that VMware Cloud Director Availability 4.6 or later is deployed for configuring the event notifications for vSphere DR and migration.
- To use the email delivery channel for events notifications, verify that your SMTP server is already configured and that it can accept emails from the VMware Cloud Director Availability appliance.

For information about the events and notifications, see [Events and notifications](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, under **Configuration** click **Events and Notifications**.

### NOTE

To forward the events to the syslog server and to email, first you must configure these delivery channels. While not yet configured, the **Syslog** and the **Email** check boxes display `not configured` and remain dimmed.

3. To configure the syslog server, under **Receive notifications via the following channels** next to **Syslog** click **Configure**.
  - a) In the **Syslog** window, enter the syslog server address and the UDP port.
  - b) To save the syslog configuration, click **Apply**.
4. Optional: To configure the email delivery channel, under **Receive notifications via the following channels** next to **Email** click **Configure**.
  - a) In the **Configure Email Settings** window, enter the following configuration details.

SMTP server name	You must enter the IP or hostname of an operational SMTP server.
SMTP server port	You must enter the TCP port of the SMTP server. By default, 25.
SMTP server secure mode	Optionally, select the SMTP encryption mode: <ul style="list-style-type: none"> <li>• <b>None</b>, by default.</li> <li>• <b>SSL</b></li> <li>• <b>Start TLS</b></li> </ul>
SMTP authentication required	Optionally, activate the SMTP authentication, then you must enter: <ul style="list-style-type: none"> <li>• <b>User name</b></li> <li>• <b>Password</b></li> </ul>
Sender's email address	You must enter the email address of the notifications sender.
Email subject prefix	Optionally, enter the subject of the email notifications.

Recipients' email addresses	You must enter one or multiple recipients that all receive the email notifications.
-----------------------------	---

b) To save the email delivery channel configuration, click **Apply**.

5. Under **Receive notifications for the following events** configure the delivery channels for each event type.

- To configure all event types at once, click **Quick Activate/Deactivate**, then click **Apply**.
- Alternatively, configure each event type by following the next steps:

a) Under the **User Activities** section, to configure each event type click **Edit** then to save the settings click **Apply**.

Event type	Activity triggers	Notifications delivery channels
Replications	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Incoming Replications</b></li> <li>• <b>Recovery Plans</b></li> <li>• and <b>Start/Stop</b> events for replication tasks</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>
Configuration	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Settings</b></li> <li>• <b>Peer Sites</b></li> <li>• <b>Replicator Services</b></li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>
System	Activities on the following pages in the left pane: <ul style="list-style-type: none"> <li>• <b>Support Bundles</b></li> <li>• <b>Backup Archives</b></li> <li>• and <b>Start/Stop</b> events for <b>System</b> tasks</li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>
Session	Activities related to users sessions: <ul style="list-style-type: none"> <li>• <b>Login</b></li> <li>• <b>Logout</b></li> </ul>	Select the delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>

b) Under the **Monitoring Events** section, configure the following two monitoring event types.

c) Next to **Service connectivity and monitoring**, click **Edit**, then to save the settings click **Apply**.

Option	Description
Events types	vCenter Server Lookup service connectivity, database connectivity, certificate expiration, SSH activation, and others.
Receive notifications via the following channels	Select the notifications delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>
Connectivity poll interval	The time interval between polls for connectivity issues. By default, 30 seconds.
Configuration poll interval	The time interval between polls for configuration issues. By default, 1 day.
Certificate expiry threshold	The time before a certificate expires to start forwarding events. By default, 30 days prior.

Option	Description
Policy compliance poll interval	The time interval between polls for policy compliance issues. By default, 60 minutes.

d) Next to **Replication errors and warnings**, click **Edit**, then to save the settings click **Apply**.

Option	Description
Events types	Any replication errors and RPO violations.
Receive notifications via the following channels	Select the notifications delivery channels: <ul style="list-style-type: none"> <li>• <b>Syslog</b></li> <li>• <b>Email</b></li> </ul>
Poll interval	The time interval between polls for replication issues. By default, 5 minutes.
RPO violation threshold time	Only forward events for RPO violation time above this threshold. 0 forwards events for any RPO violation. By default, 30 minutes.
RPO violation threshold count	Only forward events for RPO violations count above this threshold. 0 forwards any number of replications with an RPO violation. By default, 0.

6. Optional: To configure the time before forwarding an event again while the condition is still active, under the **Monitoring Events** section next to **Monitoring events forwarding time**, click **Edit**.

Without any delivery channel selected for **Monitoring Events**, the **Monitoring events forwarding time** displays **N/A** and to configure it, you must select at least one delivery channel for either or for both **Service connectivity and monitoring** and **Replication errors and warnings**.

- a) In the **Notification settings** window, under **Monitoring events forwarding time** enter the forwarding time.  
By default, **Monitoring events forwarding time** is 24 hours.
- b) To save the configuration for events notifications reposting, click **Apply**.

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

You can monitor VMware Cloud Director Availability by using the syslog server, or your email client.

You can also subscribe for a weekly summary email. For more information, see [Subscribe for weekly summary email](#).

## Subscribe for weekly summary email

As either a **provider** or as a **tenant**, subscribe for a summary of the VMware Cloud Director Availability protections and migrations for the week by using the email delivery channel.

- Verify that VMware Cloud Director Availability 4.6 or later is deployed in the cloud site for sending weekly summary emails.
- To use the email delivery channel for weekly summary, verify that the SMTP settings are configured depending on the site:
  - For Cloud Director sites, configure the SMTP settings in VMware Cloud Director. For more information, see [Configure the System Email Settings](#) in the *VMware Cloud Director Service Provider Admin Guide*.
  - For vSphere DR and migration between vCenter Server sites, see [Configure event notifications for vSphere DR and migration](#).

Since VMware Cloud Director Availability 4.6, both providers and their tenants can subscribe for a weekly summary email that contains the numbers of active/new/deleted protections and migrations performed last week.

The subscribers remain informed about what is happening with their replications without logging in. Their weekly summary report:

- Counts only incoming replications\* to the cloud site.
- Counts the current state for active protections and migrations.
- Counts all of the performed: failover, test, migrate, new and deleted replications for the specified period, and the total data transferred this week.
- As **provider**, to see the report in the management interface of VMware Cloud Director Availability, in the left pane click **Reports**. For more information, see [View the activity summary report in the Cloud Director site as a provider](#) in the *User Guide*.

#### NOTE

\* Replications using the **VMC** data engine are not part of the summary report.

- The report can be sent with a date of a maximum of one week earlier than the subscription date.
- The providers see data for each organization and for each replication, while the tenants see data only for their organization and only for replications owned by their organization.

For information about the events and notifications, see [Events and notifications](#).

1. Log in to VMware Cloud Director Availability.
  - a) In a Web browser, go to `https://Appliance-IP-Address`.
  - b) Enter the user credentials and click **Login**.
2. In the left pane, under **Configuration** click **Events and Notifications**.

#### NOTE

To forward the weekly summary events by email, first configure this delivery channel. While not yet configured, the **Weekly summary email** displays `Email is not configured` and **Subscribe** remains dimmed.

3. In Cloud Director sites, to subscribe tenants for weekly summary emails if you logged in as a **provider**, click **Tenants event notifications** then from the **Organization** drop-down menu, select the organization for which you want to edit the weekly summary email configuration.  
Skip this step for vSphere DR and migration or when logged as **atenant**, as you can configure the weekly summary email only for your organization.
4. Optional: Once the email delivery channel is configured, to subscribe for the weekly summary email, next to **Weekly summary email** click **Subscribe**.
5. Optional: In the **Subscribe for weekly summary email** window, schedule the day of the week and the time for sending the weekly summary email then click **Subscribe**.

At the scheduled time, a weekly summary email is sent, containing the unique numbers of protections and of migrations events for the week. For Cloud Director sites, the **provider** receives a summary email containing the numbers of each organization.

## Update the principal user of a Replicator instance

The principal user used for configuring a Replicator instance must be updated by using the service management interface after changing its password or when changing the principal with a user having different set of privileges on the vCenter Server containers.

Verify that VMware Cloud Director Availability is successfully deployed.

When deploying a Replicator instance, after registering it with vCenter Server Lookup service, you configure it with a single sign-on administrative user, also called a principal user for this Replicator instance. Later, this configuration needs updating when you:

- Update the expired password of the principal user.
- Change the principal user to another one with more or less permissions on some vCenter Server containers. For example, for multi-tenancy when two independent entities share the same providers vCenter Server.

Depending on the site, you can also deploy additional Replicator instances:

- For information about adding a new Replicator instance for vSphere DR and migration, see [Add an Additional Replicator Appliance Instance](#).
- Alternatively, for information about adding a new Replicator in the Cloud Director site, see [Add an Additional Replicator Service Instance](#).

1. Depending on the site, log in to the specific service management interface of VMware Cloud Director Availability.

- For vSphere DR and migration, go to `https://Appliance-IP-Address/ui/admin`.
- For a Cloud Director site, go to `https://Appliance-IP-Address:8441/ui/admin`.

- a) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
- b) Click **Login**.

2. In the left pane, click **Replicator Services**.

3. Repair the local Replicator instances with the updated principal user credentials.

- a) On the **Replicator Services administration** page, select a local Replicator instance and click **Repair**.
- b) In the **Details for the Replicator Service** window, enter the following details and click **Apply**.

Option	Description
<b>Endpoint Address</b>	The current IP address of this Replicator instance.
<b>Appliance Password</b>	Enter the root user password of this Replicator Appliance.
<b>SSO Admin Username</b>	Enter the principal user for this Replicator instance.  Requires a user with administrative privileges in the local site single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
<b>SSO Password</b>	Enter the password of the principal user.

Repeat this step for all local Replicator instances.

These Replicator instances start using the newly provided principal user credentials.

## Schedule backup archives

In the management interface of the appliance, create a backup schedule for generating new backup archives of VMware Cloud Director Availability. Connect and authenticate to an external server using Secure File Transfer Protocol (SFTP) for scheduled uploads of the backup archives as files for future restore to that moment in time.

- Verify that VMware Cloud Director Availability 4.6 or later is installed for configuring the backups interval and its retention period.

Alternatively, for information about backing up the appliances to their local internal storage, see [Back Up All Appliances in the Cloud](#) and for all the remaining appliance roles, see [Back Up the Appliance](#).

- Verify that the SFTP server is available and is reachable from VMware Cloud Director Availability.
- Verify that before taking a backup, all VMware Cloud Director Availability services are operational. As exception, unreachable Replicator Service instances without incoming replications do not prevent generating a backup. The scheduled backup generation fails when any other of the services cannot be reached or is not operational.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least 40% amount of free space for each of the VMware Cloud Director Availability appliances in the site. The scheduled backup generation fails when there is insufficient storage.

This procedure is applicable to any the following VMware Cloud Director Availability appliance roles:

- Cloud Director Replication Management Appliance
- Cloud Director Combined Appliance
- On-Premises to Cloud Director Replication Appliance
- vCenter Replication Management Appliance
- On-Premises to Cloud vCenter Replication Appliance

You schedule the backup generation of VMware Cloud Director Availability only by using the management interface of the appliance. The scheduled backup archives contain the following information from each appliance in the site:

- Configuration files
- Public certificate
- Keystore
- Database dump

In the backup archive, this information is stored as multiple `.enc` appliance backup files. When generating the backup, you provide a password that encrypts the `.enc` appliance backup files to preserve any sensitive information.

A backup file does not contain:

- The `applianceroot` user password.
- Any previous backup archives.
- Any support bundles.
- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

#### NOTE

After evacuating a datastore, all backups taken priorly cannot restore the replications. For information about datastore evacuation, see [Evacuate the replications data from a datastore](#).

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the `root` or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane, click **Backup Archives**.
3. On the **Scheduled backup archives** tab, configure or edit the backup schedule.
  - When **Backup schedule** shows `Unconfigured`, click **Configure schedule**.
  - Alternatively, when **Backup schedule** shows `Configured`, click **Edit configuration**.

## 4. Complete the wizard.

a) On the **Server authentication** page, configure the following details then click **Next**.

Server location	Enter <code>sftp://FQDN-or-IP-address:port/destination_folder/subfolder</code> , where the <code>/destination_folder/subfolder</code> path is relative to the root / directory on the server.  <b>NOTE</b> When changing this address to a new server, the backup retention only applies to the newly configured server. No retention applies to any backups stored on the previously configured server.
Authentication method	<ul style="list-style-type: none"> <li>• Select <b>Authenticate using server credentials</b> and enter both <b>Server user name</b> and <b>Server password</b>.</li> <li>• Alternatively, select <b>Authenticate using public key</b> and enter <b>Server user name</b>, click <b>Click to copy public key</b> then paste appending it to the <code>authorized_keys</code> file in the server.</li> </ul>
Server user name	Enter the user for the backup server.
Server password	After selecting <b>Authenticate using server credentials</b> , enter the password for the backup server user.
Test connection	Click to establish a connection with the server, then verify and accept its SSH public key.

b) On the **Settings** page, configure the backup interval, encryption, and retention then click **Next**.

Delay backup start time	Activate this toggle to enter <b>Start time</b> of the backup schedule.
Backup interval	Enter the time interval between each two scheduled backups. The minimum is 30 minutes and the maximum is 1 week. By default, the backup interval is 30 minutes.
Encryption password	Enter a password to protect the contents of the backup archive. The password that you must enter must contain a minimum of eight characters and must consist of: <ul style="list-style-type: none"> <li>• At least one lowercase letter.</li> <li>• At least one uppercase letter.</li> <li>• At least one number.</li> <li>• At least one special character, such as &amp; # % .</li> </ul>

Confirm Password	Confirm the same password to protect the contents of the backup archive.
Retention	<ul style="list-style-type: none"> <li>• Select <b>Retain all backups</b> to never automatically delete any externally stored backups.</li> <li>• Alternatively, select <b>Specify the number of backups to retain</b> to automatically delete backups past the configured <b>Number of retained backups</b>. By default, the appliance keeps 10 backups on the external server. The retention period is 5 hour(s).</li> </ul>

c) On the **Summary** page, verify the selected settings then click **Finish**.

The **Backup schedule** section shows `Configured` and displays:

- **SFTP server location**
- **Authentication method**
- **Backup server user name**
- **Encryption password**
- **Backup interval**
- **Number of retained backups**
- **Start time**
- **Next backup run time**
- **Number of retained backups**

In the **Scheduled backup tasks** table you see a `Generate scheduled backup archive` task progressing.

5. Optional: To modify the backup schedule, click **Edit configuration** then complete the **Edit Backup Schedule** wizard. On the **Server location** page, to select the **Untrust the old SFTP server** check box and remove the established trust with the previously configured SFTP server, first remove the old SFTP server from the list of trusted SSH hosts by going to **Settings > Security settings > Trusted SSH hosts > Remove**.

Alternatively, when using key-based authentication, copy the new public key and paste appending it to the `authorized_keys` file in the SFTP server.

This trust is listed on the **Settings** page, under **Security settings** by expanding the **Trusted SSH hosts** section where you can also optionally click **Copy** or **Regenerate** for the `SSH public key`, or optionally click **Add** and in the **Add SSH host** window enter **Host** and **Port** then verify and accept the SSH server public key.

At the scheduled time, VMware Cloud Director Availability starts backing up then uploads the backup files directly to the SFTP server.

- You can later download one of the scheduled backup files directly from the SFTP server for restoring VMware Cloud Director Availability to that moment in time. For information about restoring from a backup archive, see [Restore the appliances in the cloud](#).
- To manually delete backup files, delete them directly from the SFTP server. This action has no effect on the scheduled backup task in the user interface.
- To automatically delete the oldest backups from the SFTP server, configure **Retention** as shown in step 4.

## Verify uptime and local and remote connectivity in the Cloud site

As a **provider**, check both the services and the appliance uptime, then ensure that the connectivity between all the local services in the cloud site and the paired remote sites is **OK** on the **System Health** page by validating the **Service status** and the **Tunnel connectivity**. `Connection offline` identifies local or remote services that are inaccessible.

Verify that VMware Cloud Director Availability 4.5 or later is deployed for displaying the service uptime.

On the **System Health** page, verify the service uptime and the connectivity in the local cloud site.

### Service uptime

Since VMware Cloud Director Availability 4.5, verify the time elapsed since the services and the appliance started.

- **Service uptime** shows the time that elapsed since all services on the appliance started.
- **Appliance uptime** shows the time that elapsed since the appliance started.

### Service status

Verify the connectivity statuses in the local cloud site to the following infrastructure services.

- Connectivity to the vCenter Server Lookup service.
- Connectivity to the database of VMware Cloud Director Availability.
- Connectivity to VMware Cloud Director.
- Connectivity to the local Tunnel Service.
- Connectivity to the NTP server.

### Tunnel connectivity

The following three sections are available for VMware Cloud Director Availability 4.3 and later for verifying the statuses of the connections from the local Tunnel Service to the following destinations.

- **Local components connectivity** to all the remaining VMware Cloud Director Availability services on the cloud appliances in the local cloud site.
- **Remote cloud sites connectivity** to the remote Tunnel Service instances in all paired remote cloud sites with the local cloud site.
- **On-Prem Incoming connectivity** to all paired On-Premises to Cloud Director Replication Appliance instances with the local cloud site.

Successful connectivity shows a green check icon . Alternatively, a red exclamation icon shows for connections that the Tunnel Service cannot establish. Restoring such connections automatically updates their connectivity status to green check icons .

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the `single sign-on` user credentials.
  - c) Click **Login**.
2. In the left pane, click **System Health**.
3. To verify the elapsed time since the services started and the elapsed time since the appliance started, check both sections.
  - **Service uptime**
  - **Appliance uptime**
4. For the local connectivity in the cloud site with the infrastructure services like vCenter Server Lookup service, VMware Cloud Director, the NTP server, and others, under **Service status** verify that the connectivity reports a green check icon.
5. To verify the local connectivity in the cloud site, under **Tunnel connectivity** expand the **Local components connectivity** section.

This section shows whether the local Tunnel Service successfully connects to the remaining services on the cloud appliances in the local cloud site. If any, the section also shows a red exclamation icon with a number of connections offline.

All the local services to which the local Tunnel Service successfully establishes a connection show a green check icon . Alternatively, a service to which the local Tunnel Service cannot connect shows a red exclamation icon.

If the local Tunnel Service is not operational, the entire **Local components connectivity** sections shows a red exclamation icon `Connection refused`. Also, under **Service status** the **Tunnel Service connectivity** shows a red exclamation icon `Connection refused`.

6. To verify the remote connectivity from the local cloud site to the paired remote cloud sites, under **Tunnel connectivity** expand the **Remote cloud sites connectivity** section.

This section shows whether the local Tunnel Service successfully connects to each remote Tunnel Service in each paired remote cloud site. If any, the section also shows a red exclamation icon with a number of connections offline.

All the remote Tunnel Service instances in paired remote cloud sites to which the local Tunnel Service successfully establishes a connection show a green check icon . Alternatively, a remote Tunnel Service to which the local Tunnel Service cannot connect shows a red exclamation icon.

7. To verify the remote connectivity from the local cloud site to the paired on-premises sites, under **Tunnel connectivity** expand the **On-Prem Incoming connectivity** section.

The **On-Prem Incoming connectivity** section shows whether the local Tunnel Service successfully connects to each remote On-Premises to Cloud Director Replication Appliance in each paired on-premises site. If any, the section also shows a red exclamation icon with a number of connections offline.

All the remote On-Premises to Cloud Director Replication Appliance instances in paired on-premises sites to which the local Tunnel Service successfully establishes a connection show a green check icon . Alternatively, a remote On-Premises to Cloud Director Replication Appliance to which the local Tunnel Service cannot connect shows a red exclamation icon.

You validated that the local cloud site connectivity is .

- For the infrastructure services in the local cloud site.
- For each VMware Cloud Director Availability service in the local cloud site.
- For all the paired remote sites, both cloud sites and on-premises sites.

## Restart the services

As part of the troubleshooting, you can restart all VMware Cloud Director Availability services in the appliance from the **System health** page.

### NOTE

After restarting each service, wait a couple of minutes for the service to become operational and display its service management interface again.

1. Log in to the management interface of each VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. Restart all of the appliance services.
  - a) In the left pane, click **System Health**.
  - b) In the **System health** page, click **Restart service**.
  - c) In the **Restart service** window, to confirm the restart operation click **Restart**.

## Collect support bundles

For troubleshooting purposes, VMware Technical Support might request support bundles that contain product-specific logs, configuration files, and data appropriate to the situation. You can collect the diagnostic information in a support bundle by using a specific management interface or a script.

- Collect a support bundle for each VMware Cloud Director Availability appliance by using its service management interface.
  - a) In a Web browser, go to the management interface of any of the VMware Cloud Director Availability appliances.  
To generate a complete support bundle from a cloud site backed by VMware Cloud Director, go to the management interface of the Cloud Director Replication Management Appliance.

Deployment type	Component	Management Interface
<ul style="list-style-type: none"> <li>• On-Premises to Cloud Director Replication Appliance</li> <li>• On-Premises to Cloud vCenter Replication Appliance</li> <li>• vCenter Replication Management Appliance</li> </ul>	On-Premises	<code>https://Appliance-IP-Address/ui/admin</code>
Cloud Director Replication Management Appliance	Cloud Service	<code>https://Replication-Management-Appliance-IP-Address/ui/admin</code>
Replicator Appliance	Replicator Service	<code>https://Replicator-Appliance-IP-Address/ui/admin</code>
Tunnel Appliance	Tunnel Service	<code>https://Tunnel-Appliance-IP-Address/ui/admin</code>
Cloud Director Combined Appliance	Cloud Service	<code>https://Appliance-IP-Address/ui/admin</code>
	Manager Service	<code>https://Appliance-IP-Address:8441/ui/admin</code>
	Replicator Service	<code>https://Appliance-IP-Address:8440/ui/admin</code>
	Tunnel Service	<code>https://Appliance-IP-Address:8442/ui/admin</code>

- b) Log in as the **root** user.
- c) In the left pane, click **Support Bundles**.
- d) In the **Support bundles** page, click **Generate new**.
- e) In the **Generate a support bundle** window, to initiate creating a support bundle, click **Generate**.

The cloud site provider can also collect on-premises support bundles by activating the **Generate a support bundle from On-Premises site(s)** toggle. Then select the on-premises sites to include in the support bundle. The logs of all the selected on-premises appliances that allow\* log collection from the cloud are included in the `cloud-bundle-id-date-timestamp.tar.bz2` file, under `manager/mgr.tar.bz2/onprems/rtr-id.tar.bz2`.

\*Collecting on-premises logs from the cloud requires version 4.4 or later in both the cloud site and in the on-premises sites and also requires the on-premises administrator to activate the **Allow log collection from Cloud** toggle when initially pairing with the cloud site or during repairing. For information about allowing on-premises log collection from the cloud, see [Repair with a remote site](#).

- f) After generating support bundles, in the **Bundle Id** column, to download a support bundle click the `bundle id` link.
  - g) In the **Download Support Bundle** window, to save the support bundle file locally click **Download**.  
In the Web browser, the `cloud-bundle-id-date-timestamp.tar.bz2` file starts downloading.
  - h) After generating 10 support bundles, to generate new bundle first remove some of the old bundles by selecting them and clicking **Delete**.  
If you attempt to generate an 11th support bundle, after you click **Generate** a **Warning** window shows `Support bundle quota exceeded. Number of allowed bundles: 10, current bundle count: 10.`
- If you cannot access the management interface of the VMware Cloud Director Availability appliance, collect a support bundle by using a Secure Shell (SSH) client.
    - a) Open an SSH connection to the VMware Cloud Director Availability virtual machine and log in by using the **root** user credentials.
    - b) Create a folder for the support bundle.

```
mkdir /opt/vmware/h4/serviceType/support/${uuidgen}
cd /opt/vmware/h4/serviceType
```

For `serviceType`, use one of the arguments: `cloud`, `manager`, `replicator`, or `tunnel`, according to the Component in the above table.

- For On-Premises to Cloud Director Replication Appliance use `replicator`.
  - For On-Premises to Cloud vCenter Replication Appliance use `manager`.
  - For vCenter Replication Management Appliance use `manager`.
- c) To generate the support bundle run the `/opt/vmware/h4/bin/support-bundle.py` script and provide arguments with the deployment type of the appliance and the output folder.
    - In a dedicated appliance deployment type, open an SSH connection to each VMware Cloud Director Availability appliance and run the script
 

```
/opt/vmware/h4/bin/support-bundle.py serviceType $(ls -t /opt/vmware/h4/serviceType/support/ | head -1)
```
    - For the Cloud Service, the following example collects all logs.
 

```
/opt/vmware/h4/bin/support-bundle.py cloud $(ls -t /opt/vmware/h4/cloud/support/ | head -1)
```

- d) Download the `/opt/vmware/h4/serviceType/support/UUID/bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone/serviceType-bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone.tar.bz2` support bundle file.
- Collect a vCenter Server instance support bundle.
    - a) In a Web browser, go to `https://vCenter-Server-FQDN:443/appliance/support-bundle`.
    - b) Log in by using the **root** user credentials, and click **Enter** to start the download of the vCenter Server support bundle.
  - For cloud sites backed by VMware Cloud Director, collect a VMware Cloud Director support bundle by using a Secure Shell (SSH) client.
    - a) Open an SSH connection to the VMware Cloud Director virtual machine and log in by using your user credentials.
    - b) Generate the support bundle file.
 

```
/opt/vmware/vcloud-director/bin/vmware-vcd-support --all --multicell
```
  - c) Download the `vmware-vcd-support-YYYY-MM-DD.NNNN.tgz` support bundle file from the `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support` folder.

After downloading the support bundles, you can provide them to VMware Technical Support.

## Record your screen and browser logs

In your web browser, to assist with live incident reporting you can record a selectable area of your screen and optionally, the microphone and the browser log directly by using VMware Cloud Director Availability.

Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.

The recording contains an encoded video file with your mouse movements, text entries, and all actions performed in the selected screen area, and optionally sound from your microphone.

In addition to the video file, when recording the VMware Cloud Director Availability window, the recording can also optionally contain a browser log file with VMware Cloud Director Availability entries only, with the passwords and the sensitive information censored.

1. Log in to the management interface of VMware Cloud Director Availability.
2. Before using the recording options, access the new recording icons.
  - Depending on the login method, if the top pane of VMware Cloud Director Availability is visible, next to the refresh button and the light/dark theme selector menu, there is a new recording icon.
  - Alternatively, on the **Dashboard** page next to **Topology**, click the **Report Issue** link.
  - Alternatively, to show or hide the new recording icon in the right pane on any VMware Cloud Director Availability page, press **Ctrl + Shift + A**.
3. To start the recording, click either of the new recording icons.
  - a) In the **Before you continue** window, acknowledge the sensitive information message and click **Continue**.
  - b) In the **Live Incident Assistant** window, select at least one recording option and click **Start**.

Capture video	Select to record a motion video track of the selected screen area. The resulting archive contains a <code>video.mp4</code> file with the video track.
Video quality	Select either <b>Low</b> , <b>Medium</b> , or <b>High</b> video encryption quality for the video track.

Capture audio	Select to record the audio track from your microphone. <ul style="list-style-type: none"> <li>• If recording both audio and video, the resulting archive contains a <code>video.mp4</code> file with the video and the audio tracks.</li> <li>• If recording audio without <b>Capture video</b> selected, the resulting archive contains an <code>audio.webm</code> file with the audio track.</li> </ul>
Capture browser logs	Select to record a censored text log with all web browser requests and responses between the VMware Cloud Director Availability portal and the backend server. The resulting archive contains a <code>browser-console.log</code> file.

- c) If you selected **Capture video**, accept your browser request for permission to capture your screen and select a screen recording area.

Depending on your web browser, you can select to share the following area with VMware Cloud Director Availability for recording:

- Your entire screen area, by selecting which monitor to record.
- A specific window, by selecting the application window for recording.
- A specific browser tab, by selecting the tab for recording.

If you cancel, block, or dismiss the screen sharing permissions without explicitly allowing them, an **Error** window shows a message that `Your browser denied the permissions required for capturing the screen.` In the browser, select the screen capture area and allow the request from the appliance to share/see your screen after attempting another capture.

- d) If you selected **Record audio**, accept your browser request for permission to use your microphone.

If you do not permit the audio sharing, an **Error** window shows a message that `Your OS blocks capturing your screen or your microphone.` Allow the requested permissions to your browser before attempting another capture..

4. Perform the actions that you want to be present in the recording.

The maximum session time is 30 minutes. If you do not stop the recording before they pass, you are prompted to download the recording or to discard it.

5. To stop the recording, in the place of the new recording icons, click either of the stop recording buttons or when recording video, you can click the stop sharing browser button.

Your browser downloads the `VCDA UI Support Bundle - hh_mm_ss.zip` file that contains the optional recorded motion video, the optional sound track, and the optional `browser-console.log` file.

You can send the recorded archive to support.

## Allow SSH access to the appliance

By default, VMware Cloud Director Availability does not allow Secure Shell (SSH) access. To connect to the VMware Cloud Director Availability appliance by using an SSH client, first you must allow the SSH access by using the management interface of the appliance.

---

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

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, click **Settings**.
3. Under **Security settings** next to **Allow SSH access**, click **Edit**.
4. In the **Allow SSH access** window, select **Allow SSH access** and click **Apply**.

This VMware Cloud Director Availability appliance now allows SSH connections.

You can connect to the VMware Cloud Director Availability appliance by using an SSH client and authenticating as the **root** user.

## Configure the logging levels

To perform additional troubleshooting, increase the logging level. Use the VMware Cloud Director Availability management interface and set the logging level for each service.

After exhausting the existing logs, advanced troubleshooting might require an extra level of logging detail. To generate the additional level of logging data, configure each VMware Cloud Director Availability service.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
2. In the left pane, click **Settings**.
3. Under **Appliance settings** next to **Logging levels**, click **Edit**.
4. In the **Edit Log Levels** window, for each service you can set the logging level from **Off** to **All**.
5. To apply the configuration, click **Apply**.

The modified logging level of the service persists until this service restarts.

6. Connect to the VMware Cloud Director Availability appliance by using a Secure Shell (SSH) client.
  - a) Open an SSH connection to *Appliance-IP-Address*.
  - b) Authenticate as the **root** user.
7. See the VMware Cloud Director Availability services log files. For information about each service log file, select your version and see [VMware Cloud Director Availability Logs](#) in the *Security Guide*.

## Change the password of the appliance root user

For security reasons, you can change the **root** users passwords of the VMware Cloud Director Availability appliances.

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** enter the **root** user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings**, next to **Root password** click **Change**.
4. In the **VMware Cloud Director Availability Appliance Password** window, change the **root** user password.
  - a) In the **Current Password** text box, you must enter the current password of the **root** user.
  - b) In the **New Password** text box, enter the new password for the **root** user.

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

- At least one lowercase letter.
  - At least one uppercase letter.
  - At least one number.
  - At least one special character, such as & # %.
- c) In the **Confirm Password** text box, enter the same new password.
  - d) To confirm the password change, click **Apply**.

You changed the password of the **root** user of the appliance.

You can change the **root** users passwords of the remaining VMware Cloud Director Availability appliances.

### NOTE

VMware Cloud Director Availability does not store the **root** user password for services communications and operations.

No further actions are required after any of the VMware Cloud Director Availability appliances **root** users passwords changes:

- The **root** user password is used only for administrative logins to the appliance.
- Changing the **root** user password of the Cloud Director Replication Management Appliance in a cloud site does not affect the paired cloud sites and does not affect the paired on-premises sites.
- The Replicator Service instances paired with the Cloud Service continue operating normally after changing the **root** users passwords of the Replicator Appliance instances and the Cloud Director Replication Management Appliance.
- The Cloud Service only uses the Tunnel Appliance**root** user password to enable the Tunnel Service for the first time.
- Changing the **root** user password of the On-Premises to Cloud Director Replication Appliance does not affect the pairing with the cloud site.

## Configure after changing the vCenter SSO credentials

After changing the vCenter Server single sign-on credentials used to register VMware Cloud Director Availability with the vCenter Server Lookup service, in VMware Cloud Director Availability repair the registration with the vCenter Server Lookup service with changed credentials.

After changing the vCenter Server single sign-on credentials, you can perform the following steps in any order.

1. Repair the on-premises appliances that are paired with the vCenter Server Lookup service instance with the changed vCenter Server single sign-on credentials.
  - a) Open a Web browser and go to `https://On-Premises-Appliance-IP-Address`.
  - b) Select **Appliance login** and enter the **root** user credentials.
  - c) Click **Login**.
  - d) In the left pane, click **Settings**.
  - e) Under **Site details**, next to **Pairing** click **Repair**.
  - f) Complete the **Update Pairing** wizard, and in the **Lookup Service** page, enter the new vCenter Server single sign-on credentials.

Repeat this step to repair all on-premises appliances that are paired with the vCenter Server Lookup service instance with changed vCenter Server single sign-on credentials.

2. In the cloud site backed by VMware Cloud Director, repair all Replicator Service instances with the new vCenter Server single sign-on credentials.
  - a) Open a Web browser and go to the Manager Service management interface at `https://Appliance-IP-Address:8441/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user credentials.
  - c) Click **Login**.
  - d) In the left pane, click **Replicator Services**.
  - e) Select each Replicator Service with a site name that matches the current local site name, and click **Repair**.
  - f) In the **Details for the Replicator Service** window, enter the appliance password, the new vCenter Server single sign-on credentials, and click **Apply**.

The selected Replicator Service instance is configured with the new vCenter Server single sign-on credentials. Repeat repairing all remaining Replicator Service instances in the cloud site backed by VMware Cloud Director.

3. Repair all paired cloud sites.
  - a) Open a Web browser and go to the management interface at `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user credentials.
  - c) Click **Login**.
  - d) In the left pane under **Configuration**, click **Peer Sites**.
  - e) Select a remote cloud site and click **Repair**.
  - f) In the **Update Pairing** window, click **Update**.

Repeat this step and repair all paired cloud sites.

The new vCenter Server single sign-on credentials for the vCenter Server Lookup service are propagated after repairing all on-premises appliances, repairing all Replicator Service instances, and repairing all cloud sites.

## Free up VMware Cloud Director Availability appliance disk space

If the available appliance disk space is low, you can remove obsolete or unnecessary files.

After using advanced troubleshooting or if the disk space is low you can regularly clean up the appliance disk space.

1. Clear the VMware Cloud Director Availability appliance service logs.
  - a) Connect to the VMware Cloud Director Availability appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
  - b) Navigate to the following folders and remove the service logs that are old or unnecessary.
    - /opt/vmware/h4/cloud/log
    - /opt/vmware/h4/manager/log
    - /opt/vmware/h4/replicator/log
    - /opt/vmware/h4/tunnel/log
2. Clear the VMware Cloud Director Availability appliance support bundles.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin` and log in as the **root** user or as a single sign on user.
  - b) In the left pane, click **Support** and delete all unnecessary support bundles.
  - c) Log in to the VMware Cloud Director Availability appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
  - d) Navigate to the following folders and remove the support bundles that are not available under the **Support bundles** page.
    - /opt/vmware/h4/cloud/support
    - /opt/vmware/h4/manager/support
    - /opt/vmware/h4/replicator/support
    - /opt/vmware/h4/tunnel/support
3. For dedicated Replicator Appliance instances, remove the core dumps.
  - a) Connect to each Replicator Appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
  - b) Navigate to the `/var/core/` folder and remove the HBR `core*` files.

The available disk space on the VMware Cloud Director Availability appliance is increased.

You can also check the `/var/log` and the `/tmp` folders for unnecessary files and delete them.

## Cannot access the VMware Cloud Director Availability Tenant Portal through VMware Cloud Director

You are unable to access the VMware Cloud Director Availability Tenant Portal through the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal.

- The Availability menu option is not available in the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal, or clicking it does not open the VMware Cloud Director Availability Tenant Portal.
- In the VMware Cloud Director Availability logs, you see an error message such as `Unable to register vCAV plugin in vCD`.

Connectivity problems during the initial configuration of VMware Cloud Director Availability might prevent the VMware Cloud Director Availability plug-in from registering with VMware Cloud Director.

1. Log in to the VMware Cloud Director Availability management interface.
  - a) In a web browser, go to `https://Appliance-IP-address/ui/admin`.
  - b) Select **SSO login** or **Appliance login**, and enter the single sign-on or the **root** user credentials.
  - c) Click **Login**.
2. Re-register the VMware Cloud Director Availability plug-in with VMware Cloud Director.
  - a) In the left pane under **Configuration**, click **Settings**.
  - b) Under **Service endpoints**, next to the **VMware Cloud Director address** click **Edit**.
  - c) In the **VMware Cloud Director Details** window, configure the VMware Cloud Director endpoint.

Option	Description
<b>VMware Cloud Director Endpoint address</b>	Enter the endpoint address as <code>https://VMware-Cloud-Director-IP-Address:443/api</code> .
<b>VMware Cloud Director Username</b>	Enter the <b>system administrator</b> user name, that is used for all administrative operations. For example, <code>administrator@system</code> , where <code>system</code> is the name of the system organization of VMware Cloud Director.
<b>VMware Cloud Director Password</b>	Enter the <b>system administrator</b> password.

- d) Click **Apply**.
  - e) To complete the VMware Cloud Director configuration, verify the thumbprint and accept the VMware Cloud Director SSL certificate.
3. On the **System Monitoring** tab, click **Restart Service** and confirm the operation.

## Unregister the VMware Cloud Director Availability plug-ins from VMware Cloud Director

As **provider** you can remove the plug-ins before removing the VMware Cloud Director Availability appliances, or if you see multiple instances of the plug-ins in VMware Cloud Director.

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

During the initial registration with VMware Cloud Director, the Cloud Service installs the plug-ins in VMware Cloud Director named `Setup DRaaS and Migration and Availability (localSite)`. For more information, see [Configure the Cloud Service](#).

As **provider**, you remove both plug-ins before removing the Cloud Director Replication Management Appliance, or if you see multiple instances of the plug-in.

**NOTE**

If you removed the Cloud Director Replication Management Appliance before following this procedure, see [Delete a Plug-in](#) in the VMware Cloud Director documentation.

1. Log in to the Cloud Service management interface.
  - a) Open a Web browser and go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** and enter the **root** user credentials.
  - c) Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Service endpoints**, next to **VMware Cloud Director address** click **Remove plugin**.
4. In the **Remove VCD UI plugin** window, click **Remove**.

The VMware Cloud Director Availability plug-ins are unregistered from VMware Cloud Director. You can remove the VMware Cloud Director Availability appliances.

## User Guide

---

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

- 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.
- For sites backed by VMware Cloud Director, 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).

For a glossary of the terms in the documentation, see [VMware Cloud Director Availability Terminology](#).

## Accessing VMware Cloud Director Availability

Access either of the VMware Cloud Director Availability interfaces dedicated to providers or to tenants. Alternatively, in VMware Cloud Director you can access either the provider admin portal or the tenant portal. To replicate workloads between an on-premises and a cloud site, access the VMware Cloud Director Availability vSphere Client Plug-In.

### 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.

- Verify that in vSphere your user profile is member of the **ADMINISTRATORS** group, or since VMware Cloud Director Availability 4.5 - member of the **VrOnpremUsers** group, and ensure that the user has sufficient privileges to see and interact with vSphere workloads. For information about the required user roles privileges, see [Users roles rights and sessions](#) in the Security Guide.
- 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](#).

The VMware Cloud Director Availability vSphere Client Plug-In registers in vCenter Server during the initial configuration of the VMware Cloud Director Availability appliance. Since VMware Cloud Director Availability 4.5, once configured with vCenter Server Lookup service, the on-premises appliance creates the **VrOnpremUsers** group in vSphere. Membership of this group grants access to the VMware Cloud Director Availability vSphere Client Plug-In.

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

1. Log in to the vSphere Client.
2. To access the VMware Cloud Director Availability vSphere Client Plug-In, in the top header click **Menu > Cloud Provider DR and Migration**.
3. In the left pane, click the following VMware Cloud Director Availability pages:

Option	Description
<b>Dashboard</b>	See the status of the incoming and outgoing replications, recent tasks, and traffic data and disk usage charts.
<b>Outgoing Replications</b>	Operate with the workloads 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.
<b>Incoming Replications</b>	Operate with the workloads 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.
<b>Replication Tasks</b>	See the replication task name, the target workload, and the start and end time or progress. Filter the tasks by running, succeeded, or failed status in the on-premises site.
<b>Emergency Recovery</b>	Recover or delete the workloads left from other/previous Replicator Service instances.
<b>Source Replications</b>	See the source replications, listed by: VM ID, vCenter ID, Replicator Service ID, and whether it the workload is recovered.
<b>Settings</b>	See and modify the on-premises appliance settings, the cloud site pairing, the workload placement, the vCenter Server Lookup service address, and others. Modify the following 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.
<b>L2 Stretch</b>	Register or modify an NSX autonomous edge, modify the L2 network settings, configure uplink port, modify L2 VPN sessions, and others.
<b>System Health</b>	See the operational status of all internal and external services and reboot the appliance or its services.
<b>System Tasks</b>	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.
<b>Support Bundles</b>	Generate new support bundles, download them, or delete them.
<b>Backup Archives</b>	Schedule or manually generate backups. Restore from a previously taken backup file.
<b>About</b>	See the VMware Cloud Director Availability version or click <b>Check for updates</b> .

## Accessing the VMware Cloud Director Availability Tenant Portal

Tenants log in to the VMware Cloud Director Availability Tenant Portal either 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.

- **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.

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

- 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.
1. In a Web Browser, go to the VMware Cloud Director Availability Tenant Portal at `https://Public 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.

- 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.

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.

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

Providers log in to the VMware Cloud Director Availability Provider Portal either 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.

- **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.

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

- **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.

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.

- 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. For information about the required user roles privileges, see [Users roles rights and sessions](#) in the *Security Guide*.

### 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](#).

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 paired remote cloud sites

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**. 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 roles rights and sessions](#) in the *Security Guide*.
- 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

Replication Operations Not Requiring Authentication: No Credentials Needed	Replication Operations Requiring Authentication: Provide Credentials for the Remote Site
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 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](#).

### 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**.

- 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 [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.

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

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 [Authenticating to paired remote cloud sites](#).

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**.

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 [Authenticating to paired remote cloud 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**.

- 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.

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

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 [Authenticating to paired remote cloud sites](#).

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**.

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 [Authenticating to paired remote cloud sites](#).

## Multisite authentication

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

- Both sites must be running VMware Cloud Director Availability 4.1 or later 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.
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 [Authenticating to paired remote cloud sites](#).
- 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.

## Configure my preferences

As a **user**, you can choose the language of the interface, select the color theme between high-contrast, dark or light, configure the number of displayed items for the table listings like replications and others, and choose the default selection behavior. These preferences persist in the local storage of your browser.

- Verify that VMware Cloud Director Availability 4.7 or later is successfully deployed.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

Since VMware Cloud Director Availability 4.7 you can configure the user interface by selecting your preferences for the current user browser session. For example, to display the interface in your browser by using dimmed palette colors, select the dark theme as on the following screenshot.

Figure 2: My Preferences

## My Preferences

Language English (default) ▾  
Display text content in your preferred language. **Default: English**

Color theme Dark theme ▾  
Show content in your preferred color theme. **Default: Light theme**

Table preferences

Number of items per page 20 (default) ▾  
Set the default page size for top level listings such as replications, recovery plans, etc. **Default: 20**

Selection behavior Replace the selected row (default) ▾  
Set how mouse interaction with listings will behave. **Default: Replace the selected row**

*i* Your browser will refresh to apply the changes to your preferences. ✕

RESET ALL

CANCEL APPLY

1. After you log in, in the top navigation bar, click your user name then select **My Preferences**.
2. In the **My Preferences** window, configure your preferences for the display of the interface.
  - a) From the **Language** drop-down menu, select the display language for the user interface, for example select **English (default)**.
  - b) From the **Color theme** drop-down menu, select one of the user interface themes.
    - **High contrast theme**
    - **Light theme**
    - **Dark theme**

c) Under **Table preferences**, configure the display layout of the user interface tables.

Number of items per page	<p>Select the default page size for top level listings such as replications, recovery plans, and others.</p> <ul style="list-style-type: none"> <li>• 5</li> <li>• 10</li> <li>• 20 (default)</li> <li>• 50</li> <li>• 100</li> </ul>
Selection behavior	<p>Select how mouse interaction with listings behaves.</p> <ul style="list-style-type: none"> <li>• <b>Replace the selected row (default)</b> - clicking another row selects the new row.</li> <li>• <b>Do not replace the default row</b> - clicking another row keeps the previous row selected.</li> </ul>

d) Optional: To revert all these preferences to their default values, click **Reset all**.

e) To save the selected preferences for your browser session, click **Apply**.

Your browser refreshes to apply the changes to your preferences.

The selected preferences apply for the duration of the browser local storage. When its local storage refreshes, for example after clearing the browser cache, the preferences revert to their default values.

You can operate with the replications by using the new display settings. For more information, see [Replicating workloads](#).

## Replicating workloads

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: 

For more information, see [Activate the data engines for replicating workloads](#).

**Table 8: 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							

\* For architecture and for deployment information about the source and destination sites, see the following documentation:

- VMware Cloud Director-backed cloud sites - [Deployment architecture in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- On-premises vCenter Server sites:
  - On-premises vCenter Server site paired with VMware Cloud Director-backed cloud site - [Deployment architecture on-premises](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
  - \*\* vSphere DR and migration between two vCenter Server instances - [Deployment architecture and requirements for vSphere DR and migration](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
- 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) - [Migration with VMware Cloud Director service](#) in the *Migration with 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 - [Migration with VMware Cloud Director service](#) in the *Migration with VMware Cloud Director service Guide*.
- CDS-managed GCVE SDDC - for an SDDC in Google Cloud VMware Solution (GCVE) that is managed by VMware Cloud Director service - [Deployment architecture in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide 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 - [Deployment architecture in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- CDS-managed on-premises pVDC - for an on-premises provider VDC managed by VMware Cloud Director service - [Deployment architecture in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

## **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 9: 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
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, and ESXi 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 in the source site. For information about the instances, see [Using instances](#).

### IOfilters

VMware Cloud Director Availability does not support vSphere APIs for IO Filtering neither in the source site, nor in the destination site. VMware Cloud Director Availability cannot replicate a source virtual machine assigned with a VM Storage Policy that contains IOFilters. You cannot assign such a policy to the destination virtual machine either. Before replicating a virtual machine, ensure its assigned VM Storage Policy does not contain IOFilters. Do not assign VM Storage policies with IOFilters to virtual machines configured for replication.

## 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](#).

## Creating a new replication

To create a new replication, you can choose between either creating a protection or creating a migration. Create a protection when you want to safeguard workloads against disasters and maintain their operation at the source site, and create a migration when you want to move workloads to a new location and make them active there.

### When to create a protection

By creating a protection, you set up a disaster recovery contingency for the selected workloads. Once replicated, the workloads in the source site stay active.

Create a protection to ensure business continuity in case of a disaster at the source site.

### When to create a migration

By creating a migration, you set up the move of the selected workloads to another site. Once replicated, the workloads in the destination site become active.

Create a migration to move the workloads to a new location. For example, create a migration for moving workloads from an on-premises site to a cloud site.

## 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.

- 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 [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 [Authenticating to paired remote cloud sites](#).
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.
      - 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
<b>Use SLA profile</b>	<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>
<b>Target recovery point objective (RPO)</b>	<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="#">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>
<b>Retention policy for point in time instances</b>	<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>
<b>Compress replication traffic</b>	<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>
<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>

Option	Description
	For information about the disk provisioning, see <a href="#">Replicating Thin or Thick Provisioning Virtual Disks</a> .
<b>Delay start synchronization</b>	If you selected <b>Configure settings manually</b> , choose the following option. <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>
<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 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>
<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 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.

- 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**.
- 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**.

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

- 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 [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 [Authenticating to paired remote cloud sites](#).

### NOTE

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

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.
    - 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>	For vSphere DR and migration between vCenter Server sites, select one of the following provisioning formats for the destination disk: <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> For information about the disk provisioning, see <a href="#">Replicating Thin or Thick Provisioning Virtual Disks</a> .
<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> 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> .  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.
<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.

- 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**.
- 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**.

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

### 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 or later 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](https://vCenter_Replication_Management_Appliance_Address:8043/hbr-agent.vib) file.
  - [https://Replicator\\_Appliance\\_Address/hbr-agent.vib](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 [Authenticating to paired remote cloud sites](#).

### 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.

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.

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

## Migrating, failing over, testing failover, and reversing replications

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

- For existing replications, as either a **tenant** or as a **provider**, you can perform migrate, failover, test failover, or reverse by following the procedures in this chapter.
- For information about creating new replications, see [Create a protection](#) or [Create a migration](#).

## Migrate a replication

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

- 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 [Accessing VMware Cloud Director Availability](#).
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> <p><b>NOTE</b> In the source site, all source workloads in the replication power off after a successful recovery.</p>

Option	Description
Network Settings	For migrations to and from cloud sites backed by VMware Cloud Director: <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> 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> . 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.

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.

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.

- 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.

**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 [Accessing VMware Cloud Director Availability](#).
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
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 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>
Power settings	Powers on the recovered workload in the destination site after the failover task completes.

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

- 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.

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

- 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.

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 [Accessing VMware Cloud Director Availability](#).

Perform a test failover for an existing replication, then cleanup the test data.



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
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 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>
Power settings	Powers on the recovered workload in the destination site after the test task completes.

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

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.

- 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.

- 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 [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 disks for 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.

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.

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.

- 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**.

## Replicating with Cloud Director sites

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.

### NOTE

Organization names must not contain the comma character. To avoid errors, rename any organizations that have comma in their name, before applying policies, SLA profiles, and other operations with the organizations.

- 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 [Replicating workloads](#) chapter which are common for replicating with any site.

## Replication tracking placement solution

A replication tracking virtual machine (RT VM) represents a shadow VM for replication placement that allows per-disk placement. An RT vApp is a vApp that consists of RT VMs. As **provider**, you can configure the placement solution of the existing vApp and VM replications to RT VM.

Since VMware Cloud Director Availability 4.7, when using a supported version of VMware Cloud Director in the destination site, then RT VM replaces the independent disk as the placement and reporting solution going forward.

RT VM is a shadow VM residing in the destination VMware Cloud Director that represents the replication. Performing recovery promotes the shadow VM as the workload VM. This recovery process is faster and more robust, allowing for lower RTO. The RT vApp is composed at configuration time instead of recovery time. Also, the recoveries use reload from path, instead of registering a new VM in vCenter, allowing for better RTO and resilience.

A replication that uses RT VM allows placing the replica files in separate data stores for each disk and for the VM itself.

**NOTE**

- Independent disks remain supported for backwards compatibility with VMware Cloud Director 10.5 and earlier VMware Cloud Director Availability versions.
- All new replications automatically use RT VM when using VMware Cloud Director 10.5.1 or later and VMware Cloud Director Availability 4.7 and later.
- With VMware Cloud Director 10.5.1 in the destination site, it is recommended to configure replication tracking placement solution for all the existing replications.

**Configure Replication Tracking****NOTE**

Organization users cannot see nor interact with the RT VM itself in the inventory of VMware Cloud Director. These **tenant** users also do not see Replication Tracking as an option in VMware Cloud Director Availability.

After performing failover, test failover, or migration, then the workload VM becomes available for them in the destination site.

When supported by the version of VMware Cloud Director in the destination site, as **aprovider**, you can configure RT VM placement solution for existing replications. This configuration of the placement solution completes quickly and is irreversible:

- The replica files do not move across data stores during the configuration and the bandwidth is not affected.
- Once configured as replication tracking, the placement solution of a replication cannot revert to independent disk.
- The disk space consumption does not change after upgrading to RT VM.
- All VMs in a vApp replication configure their placement solutions in parallel. vApp replications cannot be recovered when they have Mixed placement solutions, that is some of the VMs use Independent disk, while others use RT VM. To recover such vApp replication, all VM replications must be first configured with RT VM.
- Only providers can see and configure the placement solution.
- Both the source and the destination sites require VMware Cloud Director Availability 4.7 or later and VMware Cloud Director 10.5.1 or later in the destination site for the placement solution configuration.

To configure the placement solution for existing replications:

**NOTE**

Despite recommendations, for existing replications using the **VMC** data engine you cannot use **All Actions > Configure Replication Tracking**. New **VMC** data engine replications use RT VM placement solution. For information about the data engines, see *Activate the data engines for replicating workloads* in the *Administration Guide*.

1. Log in to VMware Cloud Director Availability as **aprovider** then in the left pane click either **Incoming Replications** or **Outgoing Replications**.
2. To configure the existing replications, click the **vApp** tab or the **VM** tab then see the Placement solution column for each replication.
3. Select one or more replications that show *Independent disk* then click **All Actions > Configure Replication Tracking**.

**NOTE**

All VMs in a vApp replication or in a vApp template replication must use the same placement solution. When you click **All Actions > Configure Replication Tracking** for a vApp replication, configure all of its VMs as replication tracking placement solution.

**Configure Replication Tracking** remains inactive when not supported by the version of the destination site VMware Cloud Director.

4. In the **Configure Replication Tracking** window, click **Apply**.

- Optionally, to monitor the progress of the placement solution configuration for the selected replications, in the left pane click **Tasks**.

## 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 [Replicating workloads](#).

#### Events and Notifications

- Activating settings changes allows tenants to manage their own event notifications. For information about the tenants events and notifications, see [Events and notifications](#) 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 10: Default Policy Attributes**

Setting	Default Value
<b>Policy name</b>	Default Policy
<b>Incoming migrations</b>	Activated, by default. In both directions, the migrations are allowed, to both cloud sites and to on-premises sites.
<b>Outgoing migrations to cloud</b>	
<b>Outgoing migrations to On-Premises</b>	
<b>Incoming protections</b>	Deactivated, by default. In both directions, the protections are disallowed.
<b>Outgoing protections</b>	
<b>Custom SLA settings</b>	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.
<b>Allow advanced retention rules</b>	
<b>Max rotated instances per protection</b>	
<b>Max stored instances per protection</b>	
<b>Minimum allowed RPO</b>	
<b>Allow organizations to modify Events and Notifications settings</b>	Activated, by default.
<b>Limit the number of configured replications</b>	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.
<b>Bandwidth throttling</b>	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 organizations can modify their Events and Notifications settings themselves.
- 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.

- 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](#).

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>	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><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="#">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>
<b>Allow organizations to modify Events and Notifications settings</b>	To allow tenants control of the event notification, activate the toggle.
<b>Limit the number of configured replications</b>	If incoming migrations or incoming protections or both are activated, enter the maximum number of replications.

Option	Description
<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.

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

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.

- 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](#).
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**.

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

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.

- 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](#).
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.

Option	Description
<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.  <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="#">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>
<b>Allow organizations to modify Events and Notifications settings</b>	To allow tenants control of the event notification, activate the toggle.
<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.

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.

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

When a replication policy is no longer needed, you can delete it.

- Verify 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 you can access VMware Cloud Director Availability as a **provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).
1. In the left pane under **Configuration**, click **Policies**.
  2. In the **Policies** page, select the replication policy for removal and click **Delete**.
  3. In the **Delete Policy** dialog box, to confirm the deletion click **Delete**.

You removed the selected replication policy.

## Assign a replication policy to organizations

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

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

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

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**.

You assigned the policy to the selected VMware Cloud Director organizations.

- If there are conflicts between the assigned replication policy and the existing replications, you must first resolve the conflicts. For more information, see [Replication policy conflicts](#).
- 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 **provider** you can see the assigned replication policies to all VMware Cloud Director organizations.

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

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

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

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

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

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

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

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, quiesce, compression, and initial synchronization time.

## SLA Settings Enforced by SLA Profiles

As a **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 [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 11: 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 **provider**, you can modify the SLA settings of the predefined SLA profiles, delete them, or create additional SLA profiles.

## Using Custom SLA Settings

To use custom SLA settings instead of selecting an SLA profile in the protections, activate the **Custom SLA settings** toggle 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 **provider**, you can create new SLA profiles.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

1. In the left pane, click **SLA Profiles**.
2. On 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) Optional: Enter the SLA profile description.
  - c) 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 [Replicating workloads](#).

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

- d) 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.
- e) Select whether to activate quiesce.
- f) Select whether to enable compression of the replication traffic.
- g) Select whether to delay the first synchronization and select a timeslot.

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

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 **provider**, you can modify the SLA profiles.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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.

1. In the left pane, click **SLA Profiles**.
2. On the **SLA Profiles** page, 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 [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.

You have modified the SLA profile and on the **SLA Profiles** page you can see the modified SLA settings.

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 **provider** you can delete it.

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

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.

1. In the left pane, click **SLA Profiles**.
2. On the **SLA Profiles** page, select an SLA profile and click **Delete**.
3. In the **Delete SLA profile** window, click **Delete**.

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.

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 **provider**, you can assign one or more SLA profiles to the organization.

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
  - Verify that you can access VMware Cloud Director Availability as a **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).
1. In the left pane, click **SLA Profiles**.
  2. On the **SLA Profiles** page, 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**.

You assigned the selected SLA profile to the selected organizations.

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 machines in a vApp replication to the Cloud Director site

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 Director site

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.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).
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 **Source VMs** page, select one or more virtual machines to replicate as a single vApp replication.
    - b) Select the **Group VMs to a single vApp** checkbox 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.

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

## Modify the settings of vApp replications to the Cloud Director site

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.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).
1. Select a vApp, replicated from an on-premises site to a Cloud Director 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.

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.

## 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.

- 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 [Accessing VMware Cloud Director Availability](#).

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 with 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](#).

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 of the page click the **VM** tab, or to modify vApp replications, stay on the **vApp** tab.
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 **Networks** and **Nics**, see [Configuring network settings of replications to the cloud](#).

a) On the **Guest Customization** page, expand the virtual machine name.

- When the source is a cloud site, by default, the **Use source settings** toggle is activated and the source virtual machine settings apply after the settings from the source replicate. The **Use source settings** toggle is deactivated when no settings come from the source. To allow guest customization, keep the **Use source settings** toggle deactivated.

### NOTE

For information about deactivating **Use source settings** globally and allowing replicating the VMware Cloud Director guest customization settings, see [Replicate source VM guest customization settings](#).

When this replication is deactivated globally, instead of **Use source settings** you can click **Apply source settings** for each replication.

- When the source is an on-premises site, no source settings exist and the toggle does not show.
- b) On the **Guest Customization** page, configure the **General** section for the expanded virtual machine.

The default settings in the following three tables apply for source workloads that do not already use guest customization or when the source is an on-premises site. If the source is a cloud site and the workload already

uses guest customization, by enabling the **Use source settings** toggle, the settings reflect the already customized source workload.

Guest customization	Deactivated by default. To apply any guest customizations, activate this toggle. When the virtual machine uses Guest Properties for customization do not activate the <b>Guest customization</b> toggle.
Computer name	Change the computer name of the destination virtual machine. <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. The computer name and network settings apply to the guest operating system when the virtual machine is powered on.
Change SID	To change the Security ID (SID) for uniquely identifying systems and users, activate this toggle. The SID applies only for virtual machines running a Windows guest operating system. VMware Cloud Director runs <i>sysprep</i> to change the Windows SID. On Windows NT, VMware Cloud Director uses <i>sidgen</i> . Running <i>sysprep</i> is a prerequisite for completing domain join. By not activating this toggle, the destination virtual machine has the same SID as the source virtual machine. 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> .

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**.

Allow local administrator password	Activate this toggle to allow setting an administrator password on the guest operating system.
Require Administrators to change password on first login	Activate this toggle to require administrators to change the password of the guest operating system on the first login.
Auto generate password	Activate this toggle to allow password auto generation.
Specify password	To enter a password, activate the <b>Allow local administrator password</b> toggle and deactivate the <b>Auto generate password</b> toggle.

Number of times to log on automatically	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**.

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 [ x\$1 == x"precustomization" ]; then echo Do Precustomization tasks elif [ x\$1 == x"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**.

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'.

## Replicate source VM guest customization settings

When not using **Recovery Settings**, activating the replication of guest customization settings applies VMware Cloud Director Guest Customization settings per VM.

Verify that VMware Cloud Director Availability 4.6 or later is deployed.

In some cases, replicating the source guest customization settings is not desirable, and you can control it when some environment-specific settings are needed only in the source site and never in the recovery site. For example, having a template to spawn new virtual machines from the source site, might include guest customization script to setup the new VM or apply custom domain settings for Windows VMs. Replicating those customization settings to the recovery site might cause harm and you can deactivate replicating them.

Activating the guest customization settings replication functionality applies VMware Cloud Director guest customization settings per VM when not overwritten by using **Recovery Settings**. Otherwise, guest customization settings need to be specified manually. For information about configuring the **Recovery Settings**, see [Configure recovery settings and guest customization](#).

1. In the left pane, under **Configuration**, click **Settings**.
2. On the **Settings** page, under **Site settings** next to **Replicate Source VM Guest Customization settings**, click **Edit**.
3. In the **Replicate Source VM Guest Customization settings** window, activate or deactivate the toggle whether the guest customization replicates from VMware Cloud Director, then click **Apply**.

## Configuring network settings of replications to the cloud

For both on-premises to cloud and 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.

The virtual machines in a vApp can connect to vApp networks and to organization virtual data center networks. One vApp can include both vApp networks and organization VDC networks. The networks added to the vApp use the network pool that is associated with the organization VDC in which the vApp is created.

A vApp network can be routed, direct, also called bridged, or isolated - a vApp network contained within the vApp.

After creating a vApp network, routing it to an organization VDC network provides connectivity to virtual machines outside of the vApp. The routed vApp networks support network services, such as a firewall and static routing.

- For cloud to cloud replications, VMware Cloud Director Availability replicates all the supported types of source vApp networks in the destination cloud site along with their source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings.

VMware Cloud Director Availability 4.6 or later, backed by VMware Cloud Director 10.3 or later, supports routed vApp networks and vApp network services for virtual data centers backed by NSX, as well as the DHCP service on vApp isolated networks.

#### NOTE

- Fencing a vApp is not supported in virtual data centers backed by NSX. Change the vApp network type to a routed network or to an isolated network.
- A vApp Edge (standalone tier-1 gateway) can only be connected to an overlay organization VDC network: routed, isolated and imported (not VLAN).
- To configure a routed vApp network and use any of the vApp network services, including the DHCP service on vApp isolated networks, the containing organization virtual data center must be configured with an edge cluster. For more information, see the **Prerequisites** in [Add a Network to a vApp](#) in the VMware Cloud Director documentation.

In the previous versions, when replicating from NSX Data Center for vSphere to NSX-backed destination VDC, these networking features cannot be replicated:

- If the NAT-routed vApp networks are attached to an organization VDC network, they are replicated as bridged, also called direct networks in the destination site. The source vApp routed networks are automatically converted to direct (VDC) networks with all of their network services dropped, for example, firewall rules, NAT, DHCP and others.
- Isolated source networks replicate in the destination site as isolated networks with dropped DHCP support.
- For 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.

- Verify that VMware Cloud Director Availability 4.6 or later is deployed in both the on-premises site and in the cloud site for mapping the source and the destination networks per selected replications, similarly to cloud to cloud replications.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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.

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, configure the destination network settings of the selected replications.
  - a) In the left pane, click **Networks**.

### NOTE

**Networks** is available for on-premises to cloud replications since version 4.6.

Source networks	See the name of the networks, and the virtual machine network interface cards (NIC).
Target networks	Click <b>None (not assigned)</b> and select the target network to connect to in the destination site after a migration, failover, or test failover.

- b) In the left pane, click **Nics** and expand a network adapter under a virtual machine.

<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. Then for each NIC, select an organization VDC network to connect to.
Status	To activate the connection for that NIC to the target 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>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 - 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>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> <li>• <b>None</b> selected by default, no IP addressing mode is specified.</li> </ul>

For information about **Guest customization**, see [Configure recovery settings and guest customization](#).

### 3. Click **Apply**.

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.

- Verify that VMware Cloud Director Availability 4.6 or later is deployed in both cloud sites for replicating routed vApp networks with error-free automatic destination network mapping or for replicating the DHCP configuration on isolated networks.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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.

VMware Cloud Director Availability 4.6 or later, when backed by VMware Cloud Director 10.3 or later, supports replicating:

- Routed vApp networks and vApp network services for virtual data centers backed by NSX.
- DHCP service on vApp isolated networks.

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

**Table 12: 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.

Original Network Mapping	Reverse Replication Network Mapping
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.

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**.

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	<p>Select the destination network to connect to in the destination site after a migration, failover, or test failover:</p> <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> <p><b>Automatic destination network mapping</b></p> <p>For vApp routed networks during automatic mapping, VMware Cloud destination organization VDC network by searching for a network with the source router. This automatic mapping requires a powered-on source network.</p> <p>For vApp templates, a routed network cannot automatically be mapped if the template is powered off.</p> <p>For the remaining types of networks, the automatic mapping search is disabled.</p> <p>In previous versions, when NSX is the backing network provider in the destination site, the NSX network is automatically converted to direct VDC networks with all network settings. During failover, test failover, or migration, for example, due to the dropped vApp to remain powered off after the recovery.</p>
-----------------	--

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

<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>

For information about **Guest customization**, see [Configure recovery settings and guest customization](#).

### 3. Click **Apply**.

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.

## Replicating vApp templates between Cloud Director sites

Templates are groups of primary copies of virtual machines, ready for instantiating. Replicating vApp templates to a site allows the tenants there to deploy consistently configured sets of 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 4.6 introduces vApp templates protections with the differences to migrations being options for tracking the source for changes and also once migrated - automatic migration for creating new destination copies on each source change.

### NOTE

The vApp templates protections do not operate with SLA profiles. To protect vApp templates activate the **Custom SLA settings** toggle in the replication policy assigned to the organization. For information about activating this toggle in the policy, see [Edit a replication policy](#).

If the **Custom SLA settings** toggle is not activated in the policy, then the vApp template protection fails at creation with the following error message: `Replication with custom SLA settings can not be configured because it violates policy 'Policy-name' configured at site 'Site-name'`.

### vApp Templates Replications

First, choose a replication direction for the templates:

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

Then, on the *Direction* **Replications** page, for the vApp templates replications click the **Templates** tab.

### Create a New vApp Templates Migration

On the **Templates** tab:

- 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 then click **Next**.

##### 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 later shows an error.

##### b. Select one or more source vApp templates for migrating.

2. On the **Destination VDC and Storage policy** page, configure the destination settings then click **Next**.
  - 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.
3. On the **Settings** page, configure the migration settings then click **Next**.
  - 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 the time for the first synchronization of the templates migration.

**NOTE**

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

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

**Create a New vApp Templates Protection**

On the **Templates** tab:

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

The **New Direction Protection** wizard opens.

1. On the **Catalogs** page, configure the source protection settings then click **Next**.
  - 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 later shows an error.
  - b. Select one or more source vApp templates for protecting.
2. On the **Destination VDC and Storage policy** page, configure the destination settings then click **Next**.
  - 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 protection catalog. Similar to vApp or virtual machine protections, template protections allow changing the storage policy before the recovery.  
The resulting vApp template matches the datastore catalog.

3. On the **Settings** page, configure the protection settings then click **Next**.
  - a. Optionally, leave the **Track source for changes** checkbox activated to track any changes in the source template, then start a new protection for the new version of the template. The protection for the old version automatically stops.
  - b. Optionally, leave the delay and set a time interval for the ongoing automatic synchronization of the templates protection.

**NOTE**

The synchronization could take longer than the configured time window and might finish after the interval is over.

- c. Configure the **Automatic migrate behaviour**:
  - Select **Replace destination template** to keep replicating in one and the same destination template and replace it when new source template versions are detected.
  - Leave **Create a new copy of the destination template and keep the old versions** selected to always replicate to new destination template copies when new source template versions are detected.

**NOTE**

To activate the automatic migrate, first manually perform a migrate. After its initial synchronization, when in the source VMware Cloud Director you select **Overwrite catalog item** for the already protected template, VMware Cloud Director shortly deletes it from its catalog and re-creates it as a new template with a new ID and the same name. Then VMware Cloud Director Availability creates a new template protection, synchronizes it and deletes the old one. This either happens within 5 minutes of the change when no time interval is configured for the synchronization, or with configured time interval - only within it VMware Cloud Director Availability picks the latest source template changes.

- d. 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.

**NOTE**

- If the organization has no SLA profiles assigned, the **Compress replication traffic** toggle shows on the **Settings** page and you can configure it either now when creating the protection, or later by clicking **All Actions > Replication Settings**.
- If the organization has one or more SLA profiles assigned, the **Compress replication traffic** toggle does not show on the **Settings** page. Later, you can still configure it by clicking **All Actions > Replication Settings**.

4. On the **Ready to complete** page, verify the selected protection settings then click **Finish**.

**NOTE**

- With no SLA profiles assigned to the organization, **Compress replication traffic** shows the value that you configured on the **Settings** page.
- With a single SLA profile assigned to the organization, **Compress replication traffic** shows the value according to the already assigned SLA profile.
- With multiple SLA profiles assigned to the organization, **Compress replication traffic** shows the value according to the first SLA profile, counted in alphabetic order.

### **Templates Replication and Recovery Settings**

**NOTE**

Both the network settings and the guest customization settings persist between auto-created template protections only while the names of the virtual machines remain the same between the template versions. By changing the virtual machines names in the source results in copying the network settings from the source template, with no guest customization settings applied in the destination for the next template version.

On the **Templates** tab, select one or more already existing templates replications, then click:

- **All Actions > Replication Settings** and in the **Edit Replication Settings** window configure the available replication settings depending on both the type of the selected replications and whether already migrated, then click **Apply**.

**Table 13: Edit Replication Settings**

Protection	Migration
<p><b>Track source for changes</b> - by leaving this checkbox active tracks any changes in the source template, and starts a new protection for the new version of the template. Then the protection for the old version automatically stops.</p>	Not available for migrations.
<p><b>Set a time interval that is convenient for the automatic synchronization.</b></p> <p><b>NOTE</b> The synchronization can take longer than the configured time window and can finish after the interval is over.</p>	
<p><b>Automatic migrate behaviour:</b></p> <ul style="list-style-type: none"> <li>• Select <b>Replace destination template</b> to keep replicating in one and the same destination template and replace it when new source template versions are detected.</li> <li>• Leave <b>Create a new copy of the destination template and keep the old versions</b> selected to always replicate to new destination template copies when new source template versions are detected.</li> </ul> <p><b>NOTE</b> To activate the automatic migrate, first manually perform a migrate. After its initial synchronization, when in the source VMware Cloud Director you select <b>Overwrite catalog item</b> for the already protected template, VMware Cloud Director shortly deletes it from its catalog and re-creates it as a new template with a new ID and the same name. Then VMware Cloud Director Availability creates a new template protection, synchronizes it and deletes the old one. This either happens within 5 minutes of the change when no time interval is configured for the synchronization, or with configured time interval - only within it VMware Cloud Director Availability picks the latest source template changes.</p>	
<p><b>Compress replication traffic</b> - The traffic compression lowers the network requirements at the expense of higher CPU consumption for the Replicator Appliance instances.</p> <p><b>NOTE</b> After performing migrate, for both protections and migrations the compression can no longer be modified.</p>	

- **All Actions > Recovery settings** then in the **Recovery settings** window click **Networks** and for the vApps and virtual machines configure the source vApp template networks connectivity with the target networks after migrate, then click **Apply**.

**NOTE**

After performing migrate, for both protections and migrations the network settings can no longer be modified.

- **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

On the **Templates** tab, select one or more existing templates protections and 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 Replications**

On the **Templates** tab, 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 usable until the synchronization operation completes.
- **All Actions > Pause** pauses the selected replications and does not send data to the destination site after clicking **Pause**.
- **All Actions > Resume** resumes the selected paused replications and starts sending data again at the configured time after clicking **Resume**.

Performing migrate, 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 cannot replicate templates with one or more encrypted virtual machines. Also, 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](#) or [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 Directors **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](#).

## Configuring settings

Configure advanced settings for the replications: instances, seed, replication settings, storage settings, recovery settings for vSphere DR and migration, or exclude disks from replicating.

## 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.

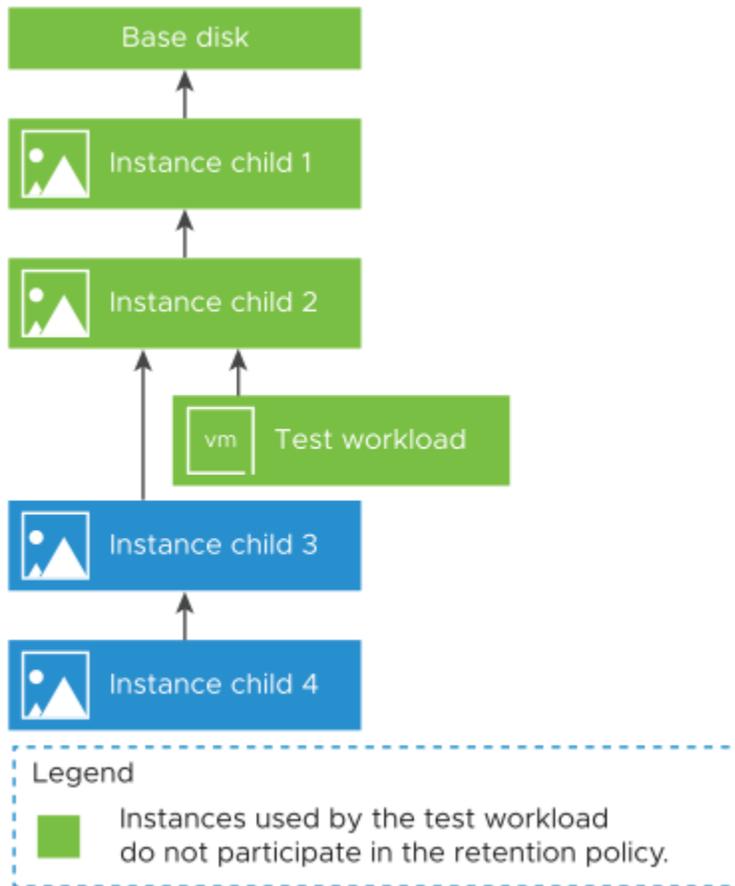
**NOTE**

- Instances cannot interoperate with **Changed Block Tracking (CBT)** enabled for the source virtual machine. For more information, see [Replicating Other Storage](#).
- 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.

- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).
- Verify that before using instances, **Changed Block Tracking (CBT)** is not enabled for the virtual machine. For more information, see [Replicating Other Storage](#).

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.

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**.

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.

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.

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

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.

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.

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.

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

## 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 disks for replication](#).

## Use a vApp as the 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 workloads to removable media for seeding a replication

As a **tenant**, to use a replication seed for configuring a replication, you must first export a virtual machine or a vApp to removable media then give it to your **provider**.

- 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.

1. By using the vSphere Client, power off the virtual machine or the vApp in the source site.
2. Export a virtual machine from vCenter Server to 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 removable media.

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

4. Give the removable media containing the exported files to your **provider**.

### Importing a virtual machine from 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 in VMware Cloud Director

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

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

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=vd-  
c_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.

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

**Import a virtual machine in VMware Cloud Director through vCenter Server**

Import a virtual machine in VMware Cloud Director by using vCenter Server.

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

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

```
ovftool -ds=DATASTORE_NAMEVM_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](#).

You can now configure a replication by using the created seed 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.

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

1. Click either **Incoming Replications** or **Outgoing Replications** then click either **New protection** or **New migration**.
2. On the **Source VMs** page, select the virtual machines or vApps that you want to replicate then click **Next**.
3. On the **Destination VDC and Storage policy** page, select the destination virtual data center to which you want to replicate the workloads and the storage policy then click **Next**.
4. On the **Settings** page, under **Advanced disk settings** select **Configure seed VMs** then click **Next**.
5. On the **Seed VM** page, select the vApp or virtual machine and select the seed virtual machines then 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.

6. On the **Ready to Complete** page, verify that the replication settings are correct then click **Finish**.

The selected seed is used for the new replication.

You can monitor the progress of the replication task by clicking **Replication Tasks** in the left pane.

## Edit replication settings

Modify the settings of any existing incoming or outgoing replications. The protections allow modifying RPO, instances retention rules, quiesce, 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.

- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).
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 <b>Target recovery point objective (RPO)</b>, alternatively for protections to and from cloud sites backed by VMware Cloud Director, you can also select an SLA profile, if configured.</li> <li>• Select the <b>Retention policy for point in time instances</b> . Define rules for instance retention over period of time.</li> <li>• Optionally, <b>Activate quiesce</b>.</li> <li>• Optionally, activate the <b>Compress replication traffic</b> toggle.</li> <li>• For protections to and from cloud sites backed by VMware Cloud Director you can also select the <b>VDC policy settings</b> from the following drop-down menus:               <ul style="list-style-type: none"> <li>– <b>VDC VM placement policy</b></li> <li>– <b>VDC VM sizing policy</b></li> </ul> </li> </ul>
Migration	<ul style="list-style-type: none"> <li>• Optionally, activate the <b>Compress replication traffic</b> toggle.</li> <li>• For protections to and from cloud sites backed by VMware Cloud Director you can also select the <b>VDC policy settings</b> from the following drop-down menus:               <ul style="list-style-type: none"> <li>– <b>VDC VM placement policy</b></li> <li>– <b>VDC VM sizing policy</b></li> </ul> </li> </ul>

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

## 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.

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

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

## 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.

- Verify that VMware Cloud Director Availability 4.6 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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 adapter to 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 the [Replicating with Cloud Director sites](#) chapter.

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 during the recovery of each virtual machine, optionally to select each network for each network adapter activate the **Customize per Network Adapters settings** toggle, then click **Next**.

All network adapters that use a specific source network will be set to the selected target networks.

You can select the target networks to be used per network adapter. For those network adapters that do not have selected target networks, the general mappings will be used.

You can select different target networks to be applied when performing migrate and failover, and for test failover:

- To configure the recovery network settings applied when performing migrate and failover click **Migrate/failover**.
  - To configure the recovery network settings applied when performing test failover click **Test**. Optionally, you can copy the settings from Migrate/failover by clicking the copy settings button.
- d) On the **Network Adapters** page, shown when you activate **Customize per Network Adapters settings** on the previous page, for each network adapter you can select the failover network and the test network then click **Next**.
  - e) 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.

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. When performing migrate, failover, or test failover for the selected replications, on the **Replications** page, to use these newly configured recovery settings, leave the **Use preset recovery settings where possible** toggle activated. For more information, see [Migrating, failing over, testing failover, and reversing replications](#).

## Selecting disks for replication

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 disks for replication

For existing replications you can select which hard disks are replicated.

- 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 **provider**. For more information, see [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.
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 **OK**.

The selected disks are replicated in the destination site.

## Recovery Plans

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.

The recovery plans orchestrate step-by-step the failover or migrations of already created 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

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* replications, then wait *x* seconds) > Completed**
- **Not Started > Delay (Wait *x* seconds) > Prompt (*Message*) > Completed**
- **Not Started > Failover (Failover *x* replications) > 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 workload 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 its type.
- 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

To perform plans operations, log in to the cloud site, then 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 the 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`, or `Completed Test`, or `Suspended . . .` state.

### Delete

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

Deleting a recovery plan also removes all of its reports.

### Suspend

Suspending is available only for plans in a `Running` state. Suspending the selected plan requests pausing its execution after completing the currently running replication task in the current step. 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

- For sites backed by VMware Cloud Director: **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. Change owner is not available for vSphere DR and migration.
- **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** - 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 14: 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

To see reports for each execution of a recovery plan, select the plan and click **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,** depending on the deployment type:
  - Owner: *org@site* for sites backed by VMware Cloud Director.
  - Owner: *System* for vSphere DR and migration.
- **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: *Workload 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 protections for recovery in the step and creates a recovery step.
- For migration plans, completing the **New Migration Step** wizard allows attaching multiple 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 replications for attaching in the selected step.

#### NOTE

For sites backed by VMware Cloud Director:

- 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.

## 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

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

Overall Health	Description
Green	There are no issues with this replication and data is replicated normally.
Yellow	There is a potential issue with this replication that might resolve itself.
Red	The replication is in bad health. 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 this replication.
Complete	Recovery operation is complete. All instances removed.
Test Image Ready	A test failover completed successfully for this replication.
Recovering	Recovery operation is in progress for this replication.
Reversed	This replication is reversed back to the original source site.
Unknown	The recovery status is not known for this replication.

## Monitoring

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.

### View the activity summary report in the Cloud Director site as a provider

As **aprovider**, in the management interface of VMware Cloud Director Availability you can see the activity summary report for the week.

- Verify that VMware Cloud Director Availability 4.6 or later is successfully deployed.
- Verify that you can access VMware Cloud Director Availability as **aprovider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

This activity summary report:

- Counts only incoming replications\* to the cloud site. As **aprovider** you see data for each organization and for each replication.
- Counts the current state for active protections and migrations.
- Counts all of the performed: failover, test, migrate, new or deleted replications for the specified period and the total data transferred this week.

#### NOTE

\* Replications using the **VMC** data engine are not part of the summary report.

1. In the left pane, click **Reports**.

#### NOTE

As **aprovider** you can see **Reports**.

Alternatively, as either **atenant** or **aprovider**, you can subscribe to a weekly email containing the same data. For more information, see [Subscribe for weekly summary email](#) in the *Administration Guide*.

2. On the **Reports** page, click the **Activity Summary** tab.
3. From the **Organization** drop-down menu select an organization for which you want to filter the displayed traffic information.
4. In the top, enter both the beginning and the end dates of the reporting period.

#### NOTE

The selected period can be a maximum of one week earlier than the current date.

In the bottom of the report chart, you can see the activity summary for the selected interval.

5. To open the activity summary report in a new HTML page in printable format, enter the beginning and the end of the reporting period and click **View HTML report file**.

You can subscribe for a weekly email containing the same report. For more information, see [Subscribe for weekly summary email](#) in the *Administration Guide*.

## 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 **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.

- 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](#).

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

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.

You see the historical traffic information for your organization.

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 provider

As a **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.

- Verify that VMware Cloud Director Availability is successfully deployed in the cloud site.
  - Verify that you can access VMware Cloud Director Availability as a **provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).
1. In the left pane, click **Reports**.
  2. On the **Reports** page, click the **Traffic and Storage** tab.
  3. From the **Organization** drop-down menu select an organization for which you want to filter the displayed traffic information.
  4. 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.

5. 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.

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.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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

1. In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
2. To show the virtual machine replications, click the **VM** tab.
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.

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.

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 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**, 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.

- 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](#).

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

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.

You see the disk usage information for your organization.

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 provider

As a **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.

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

1. In the left pane, click **Reports**.
2. On the **Reports** page, click the **Traffic and Storage** tab.
3. From the **Organization** drop-down menu select an organization for which you want to filter the displayed disk usage information.
4. 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.

5. 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.

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.

- 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 **provider**. For more information, see [Accessing VMware Cloud Director Availability](#).

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

1. In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
2. To show the virtual machine replications, click the **VM** tab.
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.

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.

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 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

Since VMware Cloud Director Availability 4.3.1, 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.

- 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](#).

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.

- 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.

- 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](#).

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.

- 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 click the **Organization Resources** tab.

**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 click the **Provider VDC Resources** tab.

**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.

## Modify the VMware Cloud Director Availability License Key

When your VMware Cloud Director Availability license expires or you obtained a new license key with expanded capacity, you can change your license key.

Verify you have a VMware Cloud Director Availability licence key. To obtain a licence key, see [Get Software and License Key for VMware Cloud Director Availability](#).

1. In the left navigation pane of the VMware Cloud Director Availability vSphere Client Plug-In, under **Configuration**, click **Settings**.
2. Under **Licensing**, click **EDIT** to change your license key.
3. In the **License Key** dialog box, enter your new license key and click **APPLY**.

---

# Security Guide

---

This *Security Guide* document provides a reference to the security and the compliance features in VMware Cloud Director Availability™.

To aid with protecting the VMware Cloud Director Availability installation, the *Security Guide* describes the security features in VMware Cloud Director Availability and the measures to take to protect the disaster recovery infrastructure from threats.

- External interfaces, ports, and services required for the correct operation of the VMware Cloud Director Availability appliances.
- The network connectivity between the services and between paired sites.
- The locations on the appliance filesystem of the configuration files for the services.
- The configuration properties of the services with security compliance implications.
- The locations on the appliance filesystem and the purposes of the log files of the services.
- The **theroot** account privileges, the required system user accounts permissions, and the required rights in both VMware Cloud Director™ and in VMware vCenter Server® for their user roles.
- The files locations for the open-source license and for VMware General Terms.
- Obtaining the latest security updates by upgrading the cloud and the on-premises VMware Cloud Director Availability sites.

## **Intended Audience**

The *Security Guide* is intended for cloud architects, infrastructure administrators, cloud administrators, and cloud operators using VMware Cloud Director Availability in a disaster recovery environment that complies with the requirements for capacity, scalability, business continuity, and disaster recovery.

VMware software familiarity is required. The *Security Guide* introduces security and compliance as it relates to the VMware Cloud Director Availability solution.

## **Services and network ports**

When deploying VMware Cloud Director Availability, by selecting the virtual appliance deployment type places the services of VMware Cloud Director Availability on dedicated cloud appliances, or on a combined appliance for testing purposes.

### **VMware Cloud Director Availability Appliance Services**

VMware Cloud Director Availability services provide dedicated management interfaces for configuration and administration. The replication operations depend on the following services that run on each listed VMware Cloud Director Availability virtual appliances in the table.

**Table 15: VMware Cloud Director Availability Services**

Service Name	Service Description
Replicator Service instances	<p>One or, optionally, multiple service instances manage the vSphere Replication Server service and the LWD Proxy service and expose the low-level HBR primitives as a REST API. These instances operate with vCenter Server-level concepts, like virtual machines, folders, datastores.</p> <p>The following VMware Cloud Director Availability appliances each run a single Replicator Service instance, depending on the cloud site:</p> <ul style="list-style-type: none"> <li>• Replicating with a multi-tenant VMware Cloud Director site: <ul style="list-style-type: none"> <li>– Providers deploy multiple Replicator Appliance instances or a single Cloud Director Combined Appliance instance.</li> <li>– Tenants deploy On-Premises to Cloud Director Replication Appliance</li> </ul> </li> <li>• vSphere DR and migration between vCenter Server sites: <ul style="list-style-type: none"> <li>– Providers deploy vCenter Replication Management Appliance and, optionally, multiple Replicator Appliance instances.</li> <li>– Tenants deploy On-Premises to Cloud vCenter Replication Appliance.</li> </ul> </li> </ul>
Manager Service	<p>A service that operates with vCenter Server-level concepts for managing the replication workflow and manages the Replicator Service instances by using REST API calls. The following VMware Cloud Director Availability appliances each run the Manager Service instance, depending on the cloud site:</p> <ul style="list-style-type: none"> <li>• Replicating with a multi-tenant VMware Cloud Director site: <ul style="list-style-type: none"> <li>– Providers deploy Cloud Director Replication Management Appliance or Cloud Director Combined Appliance.</li> </ul> </li> <li>• vSphere DR and migration between vCenter Server sites: <ul style="list-style-type: none"> <li>– Providers deploy vCenter Replication Management Appliance</li> <li>– Tenants deploy On-Premises to Cloud vCenter Replication Appliance</li> </ul> </li> </ul>
Cloud Service	<p>A service that operates with VMware Cloud Director-level concepts, like vApps and virtual machines. Manages the Manager Service by using REST API calls. The following VMware Cloud Director Availability appliances each run the Cloud Service instance:</p> <ul style="list-style-type: none"> <li>• Replicating with a multi-tenant VMware Cloud Director site: <ul style="list-style-type: none"> <li>– Providers deploy Cloud Director Replication Management Appliance or Cloud Director Combined Appliance.</li> </ul> </li> </ul>

Service Name	Service Description
Tunnel Service	<p>A service that orchestrates a secure tunnel creation and as a single endpoint channels both the incoming and outgoing site traffic, and both management data and replication data traffic using Lightweight Delta Protocol (LWD).</p> <p>The following VMware Cloud Director Availability appliances each run the Tunnel Service instance, depending on the cloud site:</p> <ul style="list-style-type: none"> <li>• Replicating with a multi-tenant VMware Cloud Director site: <ul style="list-style-type: none"> <li>– Providers deploy one, or optionally two Tunnel Appliance for HA, or one Cloud Director Combined Appliance. Since VMware Cloud Director Availability 4.6, a second instance can be configured for Tunnel Service high availability. For more information, see <a href="#">Add a second Tunnel Appliance for HA in the Cloud Director site</a> in the <i>Installation, Configuration, and Upgrade Guide in the Cloud Director Site</i>.</li> <li>– Tenants deploy On-Premises to Cloud Director Replication Appliance</li> </ul> </li> <li>• vSphere DR and migration between vCenter Server sites: <ul style="list-style-type: none"> <li>– Providers deploy vCenter Replication Management Appliance</li> <li>– Tenants deploy On-Premises to Cloud vCenter Replication Appliance</li> </ul> </li> </ul>

Table 16: Replication Services

Service Name	Service Description
Lightweight Delta Protocol Service (LWD Proxy)	<p>A proprietary replication protocol service that manages the encryption, compression, and traffic monitoring of the replication traffic. Verifies that each incoming replication data stream comes only from the authorized source LWD Proxy instance. Also verifies that each outgoing replication data stream goes only to an authorized destination LWD Proxy instance.</p> <p>In a site, LWD Proxy operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>• Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance</li> <li>• On-Premises to Cloud Director Replication Appliance</li> <li>• On-Premises to Cloud vCenter Replication Appliance</li> <li>• vCenter Replication Management Appliance</li> </ul>
vSphere® Replication™ service with vSphere Replication filter	<p>For replications using the <b>Classic</b> data engine, a vSphere Replication service called Host-based Replication (HBR) manages the low-level replication operations, creates replication instances, and others. It receives and records the delta information for each replicated workload. During replication, only the delta information is sent from the source site ESXi host to the destination site ESXi host.</p> <p>In a site, vSphere Replication Server operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>• Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance</li> <li>• On-Premises to Cloud Director Replication Appliance</li> <li>• On-Premises to Cloud vCenter Replication Appliance</li> <li>• vCenter Replication Management Appliance</li> </ul> <p><b>NOTE</b> To see the HBR version, see the <b>Caveats</b> section in the <i>VMware Cloud Director Availability Release Notes</i> .</p>

Service Name	Service Description
Data Engine Service	<p>For replications using the <b>VMC</b> replication data engine, VMware Cloud Director Availability 4.2 introduces an alternative service for replicating with the Cloud Director service by using the <b>VMC</b> replication data engine, due to the design specifics of the environment. For more information, see <i>Migration to VMware Cloud Director service</i> in the <i>Migration with VMware Cloud Director service Guide</i>.</p> <p>In a site, a Data Engine Service instance operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>• Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance</li> <li>• On-Premises to Cloud Director Replication Appliance</li> </ul>

The following services run on all VMware Cloud Director Availability appliances.

**Table 17: Other Services**

Service Name	Service Description
sshd	A standard Linux service that provides Secure Shell (SSH) access on port 22 to the VMware Cloud Director Availability appliances. By default, this service is inactive. After explicitly enabling SSH during deployment or in the management interface, this service activates and starts. Only the <b>root</b> user is allowed to authenticate. Three unsuccessful login attempts lock the <b>root</b> user account for 15 minutes.
systemd-timesyncd	A standard Linux service that provides NTP time management. To configure an NTP server, use the management interface. This service is constantly running.
vaos	A VMware service for guest OS initialization, operating VMware infrastructure settings. For example, network settings, hostname settings, creating SSH keys, running boot scripts, accepting EULA, and others. This service runs during the appliance boot.
h4postgresql	An embedded PostgreSQL server, that only listens on the local loopback device. You cannot use an external database and you cannot expose the embedded database externally. This service is constantly running.

## Network Ports

For information about the network ports required for the correct operation of VMware Cloud Director Availability, see [VMware Cloud Director Availability - VMware Ports and Protocols](#).

For information about the services connectivity, see [Services network connectivity](#).

For information about the network requirements and the external interfaces between the paired sites of VMware Cloud Director Availability, select your version and see:

- *Network Requirements in a Cloud backed by Cloud Director* in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- *Deployment Requirements for On-Premises to Cloud Director Appliance* in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
- Since version 4.4, see also *Network Requirements for vSphere and DR* in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

## Services network connectivity

Allow the required TCP access in the site for the correct operation of VMware Cloud Director Availability services.

For information about the network ports required for the correct operation of VMware Cloud Director Availability, see [VMware Cloud Director Availability - VMware Ports and Protocols](#).

For information about the services of VMware Cloud Director Availability, see [Services and network ports](#).

For information about the network requirements and the external interfaces between the paired sites of VMware Cloud Director Availability, select your version and depending on the site, see:

- [Network requirements in the Cloud Director site](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- [Deployment requirements On-Premises](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
- [Deployment architecture and requirements for vSphere DR and Migration](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

### **Services Network Connectivity**

VMware Cloud Director Availability services must be able to communicate with each other and with the following disaster recovery infrastructure.

- The Cloud Service must have TCP access to the Manager Service, to VMware Cloud Director, to vCenter Server, and to the Platform Services Controller, depending on where the vCenter Server Lookup service is hosted.
- The Manager Service must have TCP access to all the Replicator Service instances in both local, and in remote sites and to the vCenter Server Lookup service.
- All the Replicator Service instances must have a TCP access to the Manager Service, to the vCenter Server instance, and to the vCenter Server Lookup service.

#### **NOTE**

The VMware Cloud Director Availability services use end-to-end encryption for the communication across sites. For example, when a Replicator Service on site 1 is communicating to a Replicator Service on site 2, VMware Cloud Director Availability expects that the TLS session is terminated at each Replicator Service.

VMware Cloud Director Availability does not support any TLS terminating products or solutions placed between the appliances, for example, HAProxy, Nginx, Fortinet, and others. If such tools are in place, they must be configured in pass-thru mode, also known as TCP mode, to prevent from interfering with the TLS traffic of VMware Cloud Director Availability.

For more information and a network diagram that shows the connectivity between all VMware Cloud Director Availability components, see *Network Requirements* in *Installation, Configuration, and Upgrade Guide in the Cloud Director Site* and in *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

## **Services configuration files**

VMware Cloud Director Availability services use the following configuration files.

To apply changes in the configuration files, restart the affected service by using the service management interface, or in an SSH session, run the following command.

```
systemctl restart <SERVICE>
```

Service	System Unit	System Unit Location	Configuration File Location
Data Engine Service	h4dm	/usr/lib/systemd/system/h4dm.service	/opt/vmware/h4/h4dm/conf/conf.toml
Replicator Service	replicator	/lib/systemd/system/replicator.service	/opt/vmware/h4/replicator/config/application.properties

Service	System Unit	System Unit Location	Configuration File Location
Manager Service	manager	/lib/systemd/system/manager.service	/opt/vmware/h4/manager/config/application.properties
Cloud Service	cloud	/lib/systemd/system/cloud.service	/opt/vmware/h4/cloud/config/application.properties
Tunnel Service	tunnel	/lib/systemd/system/tunnel.service	/opt/vmware/h4/tunnel/config/application.properties
vSphere Replication Server	hbrsrv	/usr/lib/systemd/system/hbrsrv.service	/etc/vmware/hbrsrv.xml
Lightweight Delta Protocol Service	lwdproxy	/lib/systemd/system/lwdproxy.service	/opt/vmware/h4/lwdproxy/conf/lwdproxy.properties
PostgreSQL database server	h4postgresql	/lib/systemd/system/h4postgresql.service	/opt/vmware/h4/db/postgresql.conf

**NOTE**

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.

For information about configuring the security properties, see [Services security configuration properties](#).

## Services security configuration properties

Configuration properties that relate to security can be modified in the service configuration files.

In the VMware Cloud Director Availability service configuration files, you can modify the following security-related properties. For information about the service configuration files, see [Services configuration files](#).

Property Name	Default Value	Description
<code>session.timeout</code>	1800000	<p>The time in milliseconds to keep inactive sessions active.</p> <p>Each HTTP request resets the timer.</p> <p>The default value is 30 minutes.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>
<code>session.maxage</code>	86400000	<p>The maximum session length in milliseconds.</p> <p>Even if the session is kept alive, after the time specified in this property, the session is terminated.</p> <p>This property prevents attacks based on stolen session cookies.</p> <p>The default value is 24 hours.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>
<code>https.endpoint.protocols</code>	TLSv1.2	<p>Corresponds to <code>sslEnabledProtocols</code> in Apache Tomcat.</p> <p>For more information, see <a href="#">Apache Tomcat Configuration Reference</a> in the <i>Apache Tomcat documentation</i>.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>
<code>https.endpoint.ciphers</code>	 <p><b>CAUTION</b></p> <p>Whilst being able to configure other cipher suites, ensure that you only use secure ciphers.</p> <p>For example, exclude DH and use secure ciphers:  HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:  :!MD5:!kRSA:!DH</p>	<p>Corresponds to <code>ciphers</code> from <code>SSLHostConfig</code> in Apache Tomcat.</p> <p>For information about <code>SSLHostConfig</code>, see <a href="#">Apache Tomcat Configuration Reference</a> in the <i>Apache Tomcat documentation</i>.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>

Property Name	Default Value	Description
<code>vcd.hostnameverifier.noop</code>	<code>false</code>	When set to <code>true</code> , skips the verification of the host name of VMware Cloud Director when establishing a TLS session. Used to prevent an SSL error when the VMware Cloud Director certificate subject or its list of SANs does not contain the provided VMware Cloud Director address. Applies only to the Cloud Service.
<code>web.cors.allowedOrigins</code>	(empty string)	A list of origins (Cross-Origin Resource Sharing (CORS)) that are allowed to access the web resources. Applicable when operating a custom web server serving the plug-in with an iframe. The default value does not allow any origins, but due to the integrated user interface plug-in, the Cloud Service implicitly allows requests from VMware Cloud Director. Applies to the following services: <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>
<code>admin.allow.from</code>	(empty string)	Controls the source IP addresses that are allowed to establish server sessions. In a production environment, deactivate the root access authentication from the Tunnel Service, as requests come from the Internet. The default value states: if the service has tunneling configuration set, reject tunnel requests, otherwise allow all. Applies to the following services: <ul style="list-style-type: none"> <li>• Replicator Service</li> <li>• Manager Service</li> <li>• Cloud Service</li> <li>• Tunnel Service</li> </ul>

## Services logs locations

The log files that contain system messages are located in the VMware Cloud Director Availability virtual appliances.

Each VMware Cloud Director Availability service uses a separate log file, located in the following folders in the VMware Cloud Director Availability appliances.

Service	Default Location	Description
Data Engine Service	/opt/vmware/h4/h4dm/log/h4dm*.log	Contains the Data Engine Service specific logs and security-related messages.
Replicator Service	/opt/vmware/h4/replicator/log/replicator.log	Contains application-specific logs and security-related messages.
	/opt/vmware/h4/replicator/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
Manager Service	/opt/vmware/h4/manager/log/manager.log	Contains application-specific logs and security-related messages.
	/opt/vmware/h4/manager/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
Cloud Service	/opt/vmware/h4/cloud/log/cloud.log	Contains applicationvmware/var/log/-specific logs security-related messages.
	/opt/vmware/h4/cloud/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
Tunnel Service	/opt/vmware/h4/tunnel/log/tunnel.log	Contains entries with the source or destination IP and the source or destination port for newly established TCP connections to and from the Tunnel Service.
	/opt/vmware/h4/tunnel/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
vSphere Replication Server	/var/log/vmware/hbrsrv.log	The log file of the HBR server. Useful for troubleshooting NFC errors other problems.
Upgrade log	/var/log/upgrade.log	Contains the upgrade log entries.

#### NOTE

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.

## Collected Logs Rotation

How many days are collected by default in the logs of VMware Cloud Director Availability:

The main log files for the Cloud Service and the other services rotate due to their amount of logged data, not a static time interval, by first archiving then deleting the oldest archived copies by following these patterns for each of the logs:

- Maximum single log file size reaches 10 MB.
- Archived log file name: *logname.yyyy-MM-dd.number.gz*.
- Maximum number of archived log files reached 30.
- Total size of the archived logs reaches 140 MB.

## Log Messages Related to Security

- Attempting to log in by using an incorrect password for the **root** user account of the appliance shows the following log output.

```
2019-10-22 08:48:29.949 WARN - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10]
c.v.h.c.system.AppliancePasswordHelper : stderr: Unable to authenticate root.
```

```
2019-10-22 08:48:29.950 WARN - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10]
c.v.h.c.system.AppliancePasswordHelper : Incorrect appliance password received!
```

```
2019-10-22 08:48:29.953 ERROR - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10]
c.v.h4.common.config.SecurityConfig : An unauthorized POST request from 127.0.0.1 port 46406 to /ses-
sions failed.
```

```
org.springframework.security.authentication.BadCredentialsException: Login failed
```

```
at com.vmware.spring.security.creds.generic.CredentialsAuthenticationProvider.authenticate(Creden-
tialsAuthenticationProvider.java:84)
```

```
at com.vmware.h4.cloud.security.VcloudCredentialsProvider.authenticate(VcloudCredential-
sProvider.java:40)
```

```
at org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.ja-
va:175)
```

```
at com.vmware.spring.security.creds.JsonCredentialsAuthenticationFilter.attemptAuthentication(Json-
CredentialsAuthenticationFilter.java:140)
```

```
at org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFil-
ter(AbstractAuthenticationProcessingFilter.java:212)
```

- Attempting to log in from the Internet by using the **root** user account of the appliance shows the following log output.

```
2019-10-22 08:51:19.245 ERROR - [6d57eddb-a9d7-4f85-8fec-98503d912c7e_JK] [https-jsse-nio-8043-exec-10]
c.v.spring.security.SourceIpAuthorizer : Authorization by source IP failure: the client IP 127.0.0.1 did
not match the rule Rule{ != 127.0.0.1 }
```

- Attempting to log in by using incorrect single sign-on user credentials shows the following log output.

```
2019-10-22 08:51:59.292 ERROR - [337a5316-56d7-4a28-8991-83911eadbdc9_9W] [https-jsse-nio-8046-exec-3]
c.v.h4.common.config.SecurityConfig : An unauthorized POST request from 127.0.0.1 port 46430 to /ses-
sions failed.
```

```
org.springframework.security.authentication.BadCredentialsException: Login failed
```

```

    at com.vmware.spring.security.creds.SsoCredentialsAuthenticationProvider.authenticate(SsoCredentialsAuthenticationProvider.java:101)

    at com.vmware.h4.cloud.security.VcloudSsoCredentialsProvider.authenticate(VcloudSsoCredentialsProvider.java:44)

    at org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.java:175)

    at com.vmware.spring.security.creds.JsonCredentialsAuthenticationFilter.attemptAuthentication(JsonCredentialsAuthenticationFilter.java:140)

    at org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(AbstractAuthenticationProcessingFilter.java:212)

    ...

```

Caused by: com.vmware.vlsi.client.sso.SsoException: com.vmware.vim.sso.client.exception.AuthenticationFailedException: Provided credentials are not valid.

```

    at com.vmware.vlsi.client.sso.SsoException.toSsoEx(SsoException.java:34)

    at com.vmware.vlsi.client.sso.StsService.acquireBearerToken(StsService.java:90)

    at com.vmware.vlsi.client.sso.StsService.acquireBearer(StsService.java:82)

    at com.vmware.spring.security.creds.SsoCredentialsAuthenticationProvider.authenticate(SsoCredentialsAuthenticationProvider.java:96)

```

- **Certificate mismatch after replacing the certificate of a VMware Cloud Director Availability service. The following log output shows a remote cloud site attempting to connect to the local cloud site, when trust is established with the old certificate.**

```

2019-10-22 09:00:29.748 WARN - [cd88c84a-be07-4ae2-8150-1ba9a3806ad8_Ah] [https-jsse-nio-8046-exec-1]
com.vmware.h4.cloud.peer.PeerRepo : Unrecognized peer certificate: SHA-256:DC:8F:7E:F9:64:E-
F:45:A8:2A:EF:C1:71:E8:03:83:6C:B7:9F:F8:80:86:03:D9:2C:4E:51:E6:1F:B6:9F:BB:10

2019-10-22 09:00:29.749 ERROR - [cd88c84a-be07-4ae2-8150-1ba9a3806ad8_Ah] [https-jsse-nio-8046-exec-1]
c.v.h4.common.config.SecurityConfig : An unauthorized GET request from 172.16.198.49 port 46872 to /
diagnostics/peer-health failed.

org.springframework.security.authentication.BadCredentialsException: Unrecognized client certificate

    at com.vmware.spring.security.clientcert.ClientCertAuthenticationProvider.authenticate(ClientCertAuthenticationProvider.java:47)

    at com.vmware.h4.cloud.peer.PeerClientCertAuthenticationProvider.authenticate(PeerClientCertAuthenticationProvider.java:65)

    at org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.java:175)

    at com.vmware.spring.security.clientcert.impersonate.ImpersonatingClientCertFilter.attemptAuthentication(ImpersonatingClientCertFilter.java:45)

```

```
at org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(
AbstractAuthenticationProcessingFilter.java:212)
```

...

## Users roles rights and sessions

VMware Cloud Director Availability requires the following exact privileges for its specific users roles and rights and establishes the following sessions for performing disaster recovery (DR) operations.

### **VMware Cloud Director Availability Appliance root User Account**

VMware Cloud Director Availability uses the **root** user account for access to both the virtual appliance console and the management interface. The initial deployment of each VMware Cloud Director Availability appliance sets up this account. The **OVF Deployment** wizard requires an initial password for the **root** user account, with an initial requirement being over three characters long. After the initial deployment, VMware Cloud Director Availability forces changing this initial password on the first login by using the **root** user, with the following requirements for the persistent **root** user account password.

- The password must be over eight characters.
- The password must contain digits, upper and lower case letters, and non-alphabetic characters.
- The password cannot match any previous password.
- The password must contain more than four new characters compared to the previous password.

### **VMware Cloud Director Availability Users**

VMware Cloud Director Availability distinguishes users with administrative rights from regular users.

- **Groups in the vCenter single sign-on domain:**

To establish a user session with **administrators** rights in VMware Cloud Director Availability, the credentials for both the source and the destination sites must belong either to the **ADMINISTRATORS** or **VRADMINISTRATORS** groups. Applicable for both types of deployment:

- For vSphere DR and migration between vCenter Server sites.
- For replications with cloud sites backed by VMware Cloud Director.

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

Specifically for vSphere DR and migration, VMware Cloud Director Availability supports users members of the following two groups:

Group membership	In the On-Premises to Cloud vCenter Replication Appliance	In the provider vCenter Replication Management Appliance
<b>ADMINISTRATORS</b> group	On-premises <b>ADMINISTRATORS</b> users allow complete control.	Provider <b>ADMINISTRATORS</b> users allow complete control.
<b>VRUSERS</b> group	<p>On-premises <b>VRUSERS</b> have permissions to only:</p> <ul style="list-style-type: none"> <li>• Monitor replications</li> <li>• Manage replications</li> <li>• Monitor replication tasks</li> <li>• Monitor peer sites. Users members of <b>VRUSERS</b> cannot modify the existing paired sites nor pair new sites.</li> </ul> <p><b>NOTE</b> To pair with a provider site requires entering a provider user that belongs to <b>VRUSERS</b> or <b>ADMINISTRATORS</b> or <b>VRADMINISTRATORS</b> in that provider site. For most tenants, it is recommended to pair by using a user that belongs to the provider <b>VRUSERS</b> group.</p> <p><b>Note:</b> In summary, both users: an on-premises <b>ADMINISTRATORS</b> user plus a provider <b>VRUSERS</b> user are necessary for establishing a pairing from the on-premises site to the provider site.</p>	<p>Provider <b>VRUSERS</b> have permissions to only:</p> <ul style="list-style-type: none"> <li>• Monitor replications</li> <li>• Manage replications</li> <li>• Monitor replication tasks</li> <li>• Monitor peer sites. Users members of <b>VRUSERS</b> cannot pair new sites nor modify the existing paired sites, even for pairings from on-premise sites that use the same provider <b>VRUSERS</b> user for establishing the trust. <b>VRUSERS</b> users have no permission to modify any pairings, regardless of the peer site type.</li> </ul>

- **VMware Cloud Director organization users:**

In Cloud Director sites, the providers manage VMware Cloud Director Availability objects and the local VMware Cloud Director Availability appliances after authenticating as VMware Cloud Director **System Administrator** users. By default, the **System Administrator** role has all VMware Cloud Director rights. Users belonging to that role can manage any local and monitor any remote VMware Cloud Director Availability inventory object. From the local site, to manage remote VMware Cloud Director Availability objects, authenticate as a **System Administrator** to the remote site.

- **Tenant users:**

Tenants perform disaster recovery operations and manage the VMware Cloud Director Availability objects after authenticating as:

- For vSphere DR and migration, as single-sign-on users belonging to the **VRUSERS** group, the tenants can perform disaster recovery operations in the local site, can manage any local VMware Cloud Director Availability object, and can monitor any remote VMware Cloud Director Availability object.
- In Cloud Director sites, as **Organization Administrator** users, tenants can perform disaster recovery operations in the local site, can manage any local VMware Cloud Director Availability object, and can monitor any remote VMware Cloud Director Availability object that belongs to the VMware Cloud Director organization. From the local site, to manage remote VMware Cloud Director Availability objects, authenticate as an **Organization Administrator** user to the remote site.

On-premises, for VMware Cloud Director Availability vSphere Client Plug-In authentication since version 4.5, once configured with vCenter Server Lookup service, the On-Premises to Cloud Director Replication Appliance creates the **VrOnpremUsers** group. Membership of this group allows access to the VMware Cloud Director Availability vSphere Client Plug-In. In previous versions, the tenants authenticate to the VMware Cloud Director Availability vSphere Client Plug-In with a user member of the **Administrators** group.

For vSphere DR and migration, VMware Cloud Director Availability creates both the **VRADMINISTRATORS** and the **VRUSERS** groups in the local vCenter Server instance during the appliance configuration with the vCenter Server Lookup service. In VMware Cloud Director sites, the **VRUSERS** group is not available and the **VRADMINISTRATORS** group must be manually created only if custom permissions are needed for vCenter Server.

## **vSphere Privileges for VMware Cloud Director Availability Administrators**

### **Restricted rights for vSphere DR and migration:**

For vSphere DR and migration, VMware Cloud Director Availability 4.5 and later allow login to the appliance management interface and to the vSphere plug-in by using a monitoring user granted with limited access to the system. The limited user can neither manage the replications nor the service.

After deployment or post-upgrade, registering the VMware Cloud Director Availability appliance with the vCenter Server Lookup service creates two additional new single-sign-on groups in vSphere: **VrMonitoringUsers** and **VrMonitoringAdministrators**.

To use the monitoring-only privileges of these groups, create a new single-sign-on user and make him a member of one of the two groups:

- **VrMonitoringUsers** membership allows the users to monitor replications.
- **VrMonitoringAdministrators** membership allows the administrators to monitor the replications and the system health.

The user privileges are as follows from highest to lowest: **Read-write administrator** > **Read-only administrator** > **Read-write user** > **Read-only user**.

As **provider** or an on-premises **administrator**, allow the least privileges for the roles of the user accounts that register the vCenter Server Lookup service and operate VMware Cloud Director Availability. As **provider** to prevent the tenants access to restricted infrastructure items, only allow the following minimum list of privileges as specified for audit certifications and security compliance of VMware Cloud Director Availability.

When using customized privileges for the **service user** account, the following privileges must apply to the user that operates with VMware Cloud Director Availability and registers it with the vCenter Server Lookup service, depending on the vSphere version:

<b>Privileges in VMware vSphere 7.0</b>	<b>Privileges in VMware vSphere 8.0</b>
<p><b>Cryptographic Operations Privileges</b></p> <ul style="list-style-type: none"> <li>• Cryptographic operations.Manage keys</li> <li>• Cryptographic operations.Register host</li> </ul> <p>Select <b>Cryptographic operations</b> &gt; <b>Manage keys</b>. Select <b>Cryptographic operations</b> &gt; <b>Register host</b>.</p>	<p><b>Cryptographic Operations Privileges</b></p> <ul style="list-style-type: none"> <li>• Cryptographer.ManageKeys</li> <li>• Cryptographer.RegisterHost</li> </ul> <p>Select <b>Cryptographic operations</b> &gt; <b>Manage keys</b>. Select <b>Cryptographic operations</b> &gt; <b>Register host</b>.</p>
<p><b>Datastore Privileges</b></p> <ul style="list-style-type: none"> <li>• Datastore.Browse</li> <li>• Datastore.Configure datastore</li> <li>• Datastore.Low level file operations</li> </ul> <p>Select <b>Datastore</b> &gt; <b>Browse datastore</b>. Select <b>Datastore</b> &gt; <b>Configure datastore</b>. Select <b>Datastore</b> &gt; <b>Low level file operations</b>.</p>	<p><b>Datastore Privileges</b></p> <ul style="list-style-type: none"> <li>• Datastore.Browse</li> <li>• Datastore.Config</li> <li>• Datastore.FileManagement</li> </ul> <p>Select <b>Datastore</b> &gt; <b>Browse datastore</b>. Select <b>Datastore</b> &gt; <b>Configure datastore</b>. Select <b>Datastore</b> &gt; <b>Low level file operations</b>.</p>

Privileges in VMware vSphere 7.0	Privileges in VMware vSphere 8.0
<p><b>Extension Privileges</b></p> <ul style="list-style-type: none"> <li>• Extension.Register extension</li> <li>• Extension.Unregister extension</li> <li>• Extension.Update extension</li> </ul> <p>Select <b>Extension</b> &gt; <b>Register extension</b>.  Select <b>Extension</b> &gt; <b>Unregister extension</b>.  Select <b>Extension</b> &gt; <b>Update extension</b>.</p>	<p><b>Extension Privileges</b></p> <ul style="list-style-type: none"> <li>• Extension.Register</li> <li>• Extension.Unregister</li> <li>• Extension.Update</li> </ul> <p>Select <b>Extension</b> &gt; <b>Register extension</b>.  Select <b>Extension</b> &gt; <b>Unregister extension</b>.  Select <b>Extension</b> &gt; <b>Update extension</b>.</p>
<p><b>Global Privileges</b></p> <ul style="list-style-type: none"> <li>• Global.Disable methods</li> <li>• Global.Enable methods</li> </ul> <p>Select <b>Global</b> &gt; <b>Disable methods</b>.  Select <b>Global</b> &gt; <b>Enable methods</b>.</p>	<p><b>Global Privileges</b></p> <ul style="list-style-type: none"> <li>• Global.DisableMethods</li> <li>• Global.EnableMethods</li> </ul> <p>Select <b>Global</b> &gt; <b>Disable methods</b>.  Select <b>Global</b> &gt; <b>Enable methods</b>.</p>
<p><b>Host Configuration Privileges</b></p> <ul style="list-style-type: none"> <li>• Host.Configuration.Connection</li> </ul> <p>Select <b>Host</b> &gt; <b>Configuration</b> &gt; <b>Connection</b>.</p> <p><b>Host vSphere Replication Privileges</b></p> <ul style="list-style-type: none"> <li>• Host.vSphere Replication.Manage Replication</li> </ul> <p>Select <b>Host</b> &gt; <b>vSphere Replication</b> &gt; <b>Manage replication</b>.</p>	<p><b>Host Configuration Privileges</b></p> <ul style="list-style-type: none"> <li>• Host.Config.Connection</li> </ul> <p>Select <b>Host</b> &gt; <b>Configuration</b> &gt; <b>Connection</b>.</p> <p><b>Host vSphere Replication Privileges</b></p> <ul style="list-style-type: none"> <li>• Host.Hbr.HbrManagement</li> </ul> <p>Select <b>Host</b> &gt; <b>vSphere Replication</b> &gt; <b>Manage replication</b>.</p>
<p><b>Profile-driven Storage Privileges</b></p> <ul style="list-style-type: none"> <li>• Profile-driven storage.Profile-driven storage view</li> </ul> <p>Select <b>Profile-driven storage</b> &gt; <b>Profile-driven storage view</b>.</p>	<p><b>VM Storage Privileges</b></p> <ul style="list-style-type: none"> <li>• StorageProfile.View</li> </ul> <p>Select <b>VM storage policies</b> &gt; <b>View VM storage policies</b>.</p>
<p><b>Resource Privileges</b></p> <ul style="list-style-type: none"> <li>• Resource.Assign virtual machine to resource pool</li> </ul> <p>Select <b>Resource</b> &gt; <b>Assign virtual machine to resource pool</b>.</p>	<p><b>Resource Privileges</b></p> <ul style="list-style-type: none"> <li>• Resource.AssignVMTToPool</li> </ul> <p>Select <b>Resource</b> &gt; <b>Assign virtual machine to resource pool</b>.</p>
<p><b>Storage Views Privileges</b></p> <ul style="list-style-type: none"> <li>• StorageViews.View</li> </ul> <p>Select <b>Storage views</b> &gt; <b>View</b>.</p>	<p><b>Storage Views Privileges</b></p> <ul style="list-style-type: none"> <li>• StorageViews.View</li> </ul> <p>Select <b>Storage views</b> &gt; <b>View</b>.</p>

Privileges in VMware vSphere 7.0	Privileges in VMware vSphere 8.0
<p><b>Virtual Machine Configuration Privileges</b></p> <ul style="list-style-type: none"> <li>Virtual machine.Configuration.Add existing disk</li> <li>Virtual machine.Configuration.Change Settings</li> <li>Virtual machine.Configuration.Remove disk</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Add existing disk</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Change Settings</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Remove disk</b>.</p> <p><b>Virtual Machine Inventory Privileges</b></p> <ul style="list-style-type: none"> <li>Virtual machine.Inventory.Register</li> <li>Virtual machine.Inventory.Unregister</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Edit inventory</b> &gt; <b>Register</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Edit inventory</b> &gt; <b>Unregister</b>.</p> <p><b>Virtual Machine Interaction Privileges</b></p> <ul style="list-style-type: none"> <li>Virtual machine.Interaction.Power Off</li> <li>Virtual machine.Interaction.Power On</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Interaction</b> &gt; <b>Power off</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Interaction</b> &gt; <b>Power on</b>.</p> <p><b>Virtual Machine Snapshot Management Privileges</b></p> <ul style="list-style-type: none"> <li>Virtual machine.Snapshot management.Create snapshot</li> <li>Virtual machine.Snapshot management.Remove snapshot</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Snapshot management</b> &gt; <b>Create snapshot</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Snapshot management</b> &gt; <b>Remove snapshot</b>.</p> <p><b>Virtual Machine vSphere Replication Privileges</b></p> <ul style="list-style-type: none"> <li>Virtual machine.vSphere Replication.Configure Replication</li> <li>Virtual machine.vSphere Replication.Manage Replication</li> <li>Virtual machine.vSphere Replication.Monitor Replication</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Configure replication</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Manage replication</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Monitor replication</b>.</p>	<p><b>Virtual Machine Configuration Privileges</b></p> <ul style="list-style-type: none"> <li>VirtualMachine.Config.AddExistingDisk</li> <li>VirtualMachine.Config.Settings</li> <li>VirtualMachine.Config.RemoveDisk</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Add existing disk</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Change Settings</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Change Configuration</b> &gt; <b>Remove disk</b>.</p> <p><b>Virtual Machine Edit Inventory Privileges</b></p> <ul style="list-style-type: none"> <li>VirtualMachine.Inventory.Register</li> <li>VirtualMachine.Inventory.Unregister</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Edit inventory</b> &gt; <b>Register</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Edit inventory</b> &gt; <b>Unregister</b>.</p> <p><b>Virtual Machine Interaction Privileges</b></p> <ul style="list-style-type: none"> <li>VirtualMachine.Interact.PowerOff</li> <li>VirtualMachine.Interact.PowerOn</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Interaction</b> &gt; <b>Power off</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Interaction</b> &gt; <b>Power on</b>.</p> <p><b>Virtual Machine Snapshot Management Privileges</b></p> <ul style="list-style-type: none"> <li>VirtualMachine.State.CreateSnapshot</li> <li>VirtualMachine.State.RemoveSnapshot</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>Snapshot management</b> &gt; <b>Create snapshot</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>Snapshot management</b> &gt; <b>Remove snapshot</b>.</p> <p><b>Virtual Machine vSphere Replication Privileges</b></p> <ul style="list-style-type: none"> <li>VirtualMachine.Hbr.ConfigureReplication</li> <li>VirtualMachine.Hbr.ReplicaManagement</li> <li>VirtualMachine.Hbr.MonitorReplication</li> </ul> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Configure replication</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Manage replication</b>.</p> <p>Select <b>Virtual machine</b> &gt; <b>vSphere Replication</b> &gt; <b>Monitor replication</b>.</p>

**NOTE**

After adding a custom role in vSphere, the role is created as a Read Only role with three system-defined privileges:

- System.Anonymous
- System.Read
- System.View

These privileges are not visible in the vSphere Client but are used to read specific properties of some managed objects. All the predefined roles in vSphere contain these three system-defined privileges.

For information about the roles privileges in vSphere, see *Defined Privileges* in the vSphere documentation.

## VMware Cloud Director Roles Rights

VMware Cloud Director for users permissions publishes the predefined global tenant roles and the rights they contain to all organizations. **System Administrator** users can modify the rights and the global tenant roles from an individual organization. **System Administrator** users can modify, create, or remove predefined global tenant roles. For more information, see [System Administrator Rights](#) and [Rights in Predefined Global Tenant Roles](#) in the VMware Cloud Director documentation.

### Restricted rights for Cloud Director sites:

VMware Cloud Director Availability 4.5 and later introduce two rights for the cloud site in VMware Cloud Director, according to its version:

User permissions in VMware Cloud Director Availability	VMware Cloud Director 10.4 and earlier	VMware Cloud Director 10.5 and later
Full permission user:	VCDA_MODIFY_RIGHT	View and manage replications
Read-only user:	VCDA_VIEW_RIGHT	View replications

To use these new rights in the cloud site, first the **System Administrator** user must publish the chosen right in a rights bundle in VMware Cloud Director. These rights cannot be used for on-premises users to log in to the On-Premises to Cloud Director Replication Appliance.

- To create or modify an existing rights bundle, in VMware Cloud Director, in the left pane under the **Tenant Access Control** section click **Rights Bundles** then click **Add** or select an existing bundle and click **Edit**.
- In the **Add Rights Bundle** window, under **Rights in Bundle**, under the **Other** category, select the right, according to the version of VMware Cloud Director as per the above table, then click **Save**.
  - **VCDA\_VIEW\_RIGHT** or **View replications**
  - **VCDA\_MODIFY\_RIGHT** or **View and manage replications**
- To publish the rights bundle to all tenants or to specific tenants, select it and click **Publish**.
- In the **Publish Rights Bundle** window, select the tenants to which to publish the new rights bundle and click **Save**.
  - **Publish to Tenants**
  - **Publish to All Tenants**

After the **System Administrator** publishes the rights bundle to one or more organizations, these organizations have access to use those rights when accessing VMware Cloud Director Availability in the cloud site.

### Read-write rights:

VMware Cloud Director Availability allows read-write access to **Organization Administrator** users or to users whose role is assigned with **VCDA\_MODIFY\_RIGHT** or **View and manage replications**.

### Read-only rights:

In the user interface, all management-related actions remain hidden for read-only users. A tenant user whose role is assigned with **VCDA\_VIEW\_RIGHT** or **View replications** is restricted to only viewing his own replications and has no permissions to modify.

### Conflicting rights:

Determining the expected rights if a user role is assigned with conflicting rights, for example, both **VCDA\_VIEW\_RIGHT** or **View replications** and **Organization Administrator**, results in read-write access for that user. Similarly, assigning both **VCDA\_VIEW\_RIGHT** or **View replications** and **VCDA\_MODIFY\_RIGHT** or **View and manage replications** to the same user role again results in read-write access.

As a result:

- Read-write users can either have assigned **VCDA\_MODIFY\_RIGHT** or **View and manage replications** to their custom role, or use the default **Organization Administrator** user.
- Read-only users have assigned **VCDA\_VIEW\_RIGHT** or **View replications** to their role.
- Assigning both **VCDA\_VIEW\_RIGHT** or **View replications** and either (**VCDA\_MODIFY\_RIGHT** or **View and manage replications** or **Organization Administrator**) to the same role results in read-write rights.

**List of the rights of all the users that allow log in to the Cloud Director Replication Management Appliance:**

- Read-write **tenant** users have the same rights as the existing **Organization Administrator** user and allow both managing and monitoring only of their own replications.
- Read-only **tenant** users are introduced with version 4.5 and allow only monitoring of their own replications.
- Read-write **provider** users are the current provider login method and allow both managing and monitoring of all replications and of the system health.
- Read-only **provider** users are introduced with version 4.5 and allow only monitoring of all replications and of the system health.

As a prerequisite, **fortenant** roles that only grant the **VCDA\_MODIFY\_RIGHT** or **View and manage replications** and are different than the default **Organization Administrator**, in VMware Cloud Director at minimum grant exactly the following rights:

- General: Administrator Control
- vApp: Edit VM Compute Policy \*
- vApp: Edit VM Properties
- vApp: Delete
- vApp: Edit VM Network
- vApp: Edit Properties
- vApp: Power Operations
- vApp: View VM metrics
- vApp: View ACL
- Organization: View
- Organization: Edit Association Settings
- Organization Network: View
- Organization vDC Network: View
- Organization vDC Compute Policy: View
- Organization vDC: View ACL
- Access All Organization VDCs
- Catalog: View Private and Shared Catalogs
- Catalog: View ACL
- Organization vDC Named Disk: Delete
- Organization vDC Named Disk: Create
- Organization vDC Named Disk: View Properties
- Organization vDC Named Disk: Edit Properties
- Organization vDC Gateway: View L2 VPN \*\*
- Organization vDC Gateway: Configure L2 VPN \*\*

**NOTE**

- VMware Cloud Director Availability requires each and all of the above rights for the correct operation of the VMware Cloud Director tenant user.
- For the VMware Aria Operations Management Pack for Cloud Director Availability to be able to use auto-discovery of the VMware Cloud Director Availability address, when using a read-only user for the

management pack, you must also add the right View Tenant Portal Plugin, shown in the user interface as UI Plugins: View right.

- \* VMware Cloud Director Availability 4.3 and later require the **vApp: Edit VM Compute Policy** right that is not part of the Default Rights Bundle.
- \*\* In VMware Cloud Director service, to stretch an L2 network to an SDDC in the VMware Cloud™ on AWS, VMware Cloud Director Availability 4.4 and later require both the **Organization vDC Gateway: View L2 VPN** and the **Configure L2 VPN** rights that are not part of the Default Rights Bundle.

### VMware Cloud Director Availability Users Sessions Extension

In Cloud Director sites, each VMware Cloud Director Availability user session must have a VMware Cloud Director user and a VMware Cloud Director organization associated with the session. For more information about the sessions and authenticating to remote sites, see [Extended Session Authentication](#) in the *User Guide*.

See the Cloud Service disaster recovery operations that require an extension of the user session in the following table:

Operation	Incoming Replication		Outgoing Replication	
	Required Session on Source Site	Required Session on Destination Site	Required Session on Source Site	Required Session on Destination Site
start	Yes	Yes	Yes	Yes
stop	No	Yes	Yes	Yes
reconfigure	No	Yes	Yes	Yes
failover	No	Yes	Yes	Yes
migrate	Yes	Yes	Yes	Yes
sync	No	Yes	Yes	Yes
pause	No	Yes	Yes	Yes
resume	No	Yes	Yes	Yes
reverse	Yes	Yes	Yes	Yes
failover test	No	Yes	Yes	Yes
failover test cleanup	No	Yes	Yes	Yes

## VMware General Terms and open-source license

The files containing the VMware General Terms and the VMware Cloud Director Availability open-source license can be located in the VMware Cloud Director Availability virtual appliances.

VMware Cloud Director Availability 4.7 appliances store the files containing the VMware general terms and the open-source license in the following locations in their filesystems:

File	Location
VMware General Terms	/opt/vmware/h4/doc/eula.txt
VMware Cloud Director Availability™ Open Source License	/opt/vmware/h4/doc/open_source_license_VMware_Cloud_Director_Availability_4.7_GA.txt

**NOTE**

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.

## Upgrade for the latest updates

To receive security updates, upgrade all appliances of VMware Cloud Director Availability.

VMware Cloud Director Availability virtual appliances use the VMware Photon OS as the guest operating system.

To receive the latest updates, upgrade each VMware Cloud Director Availability appliance to the latest released version.

### **Cloud Director Site Upgrade**

For information about upgrading VMware Cloud Director Availability in a site backed by VMware Cloud Director, select the version and see [Upgrading in the Cloud](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

When upgrading, currently paired remote Cloud Director sites might cause versions mismatch. For information about pairing with mismatching versions, select the version and see [Managing connections between Cloud Director sites](#) in the *Administration Guide*.

### **On-Premises and Provider Site Upgrade**

For information about upgrading VMware Cloud Director Availability on-premises and in the provider site, select your version and see [Upgrading On-Premises](#) in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

---

# Migration to VMware Cloud Director service Guide

---

VMware Cloud Director Availability™ can migrate workloads both to and from the VMware Cloud Director™ service hosted at VMware Cloud™ on AWS.

## **Classic Migration with Cloud Director Sites**

All versions of VMware Cloud Director Availability can protect or migrate vSphere workloads with a private cloud site backed by VMware Cloud Director by using the native integrations with VMware Cloud Director and VMware vCenter Server®.

## **VMware Cloud on AWS Design Implications**

Due to design specifics of the VMware Cloud Director service hosted at VMware Cloud on AWS, VMware Cloud Director Availability introduces a service named Data Engine Service for performing migrations with VMware Cloud on AWS by using the **VMC** data engine. For information about this service, see [Services and network ports](#) in the *Security Guide*. For information about both the **VMC** and the **Classic** data engines, see [Activate the data engines for replicating workloads](#) in the *Administration Guide*.

By using the Data Engine Service and activating the **VMC** data engine, VMware Cloud Director Availability 4.2 and later can migrate workloads to VMware Cloud Director service. VMware Cloud Director Availability 4.6 and later also allow migrating workloads from VMware Cloud Director service back to the on-premises vCenter Server site. For information about the replications use cases and their cross-site support, see [Replicating workloads](#) in the *User Guide*.

As **provider** in VMware Cloud on AWS you have a VMware Cloud SDDC account and a general AWS account, and the two accounts must be linked for the service to work. Each account has its own virtual private cloud (VPC), and the VMware Cloud VPC contains a management and a compute resource pool. In the management resource pool, VMware has complete administrative control over the management and the infrastructure components. The VMware Cloud Director Availability appliances reside outside the management resource pool, deployed and managed by the **provider**.

## **Migration with VMware Cloud Director service**

Both the providers and their tenants, can use the existing migration flow and migrate their workloads to VMware Cloud Director service in VMware Cloud on AWS after following this *Migration with VMware Cloud Director service Guide*.

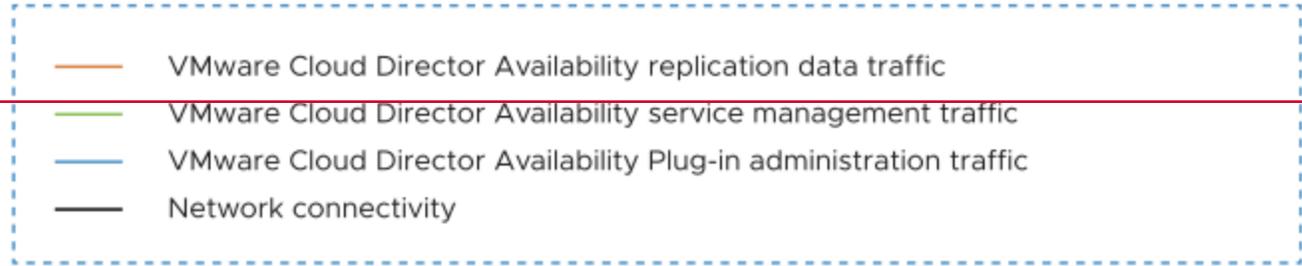
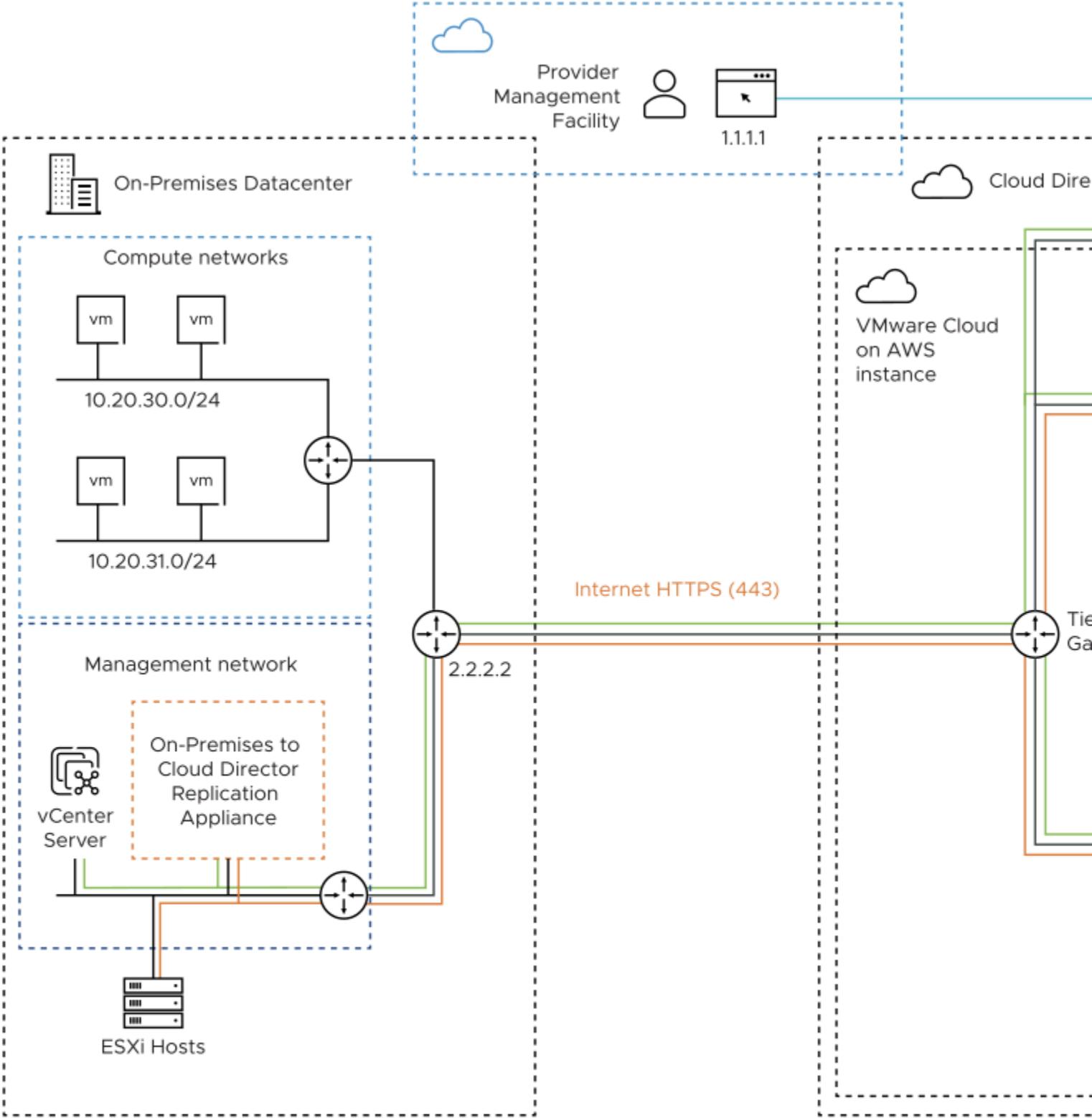
The VMware Cloud Director service pools the resources provided by the SDDC in VMware Cloud on AWS. The following diagrams provide an overview of VMware Cloud Director service after installing VMware Cloud Director Availability and pairing a VMware Cloud on AWS site with an on-premises site and or with a cloud site, backed by VMware Cloud Director.

In VMware Cloud on AWS, VMware Cloud Director Availability resides behind the compute networks compute gateway and firewall and connects with the management components like vCenter Server and ESXi through the management gateway and firewall of the management network. The *Migration with VMware Cloud Director service Guide* covers the necessary configuration in VMware Cloud on AWS allowing the connectivity to and from VMware Cloud Director Availability through the management and the compute gateways.

## **Paired On-Premises Site with VMware Cloud Director Availability in VMware Cloud on AWS**

After pairing the On-Premises to Cloud Director Replication Appliance with VMware Cloud Director Availability in VMware Cloud on AWS, in the following architecture diagram the orange color shows the deployed on-premises and cloud appliances of VMware Cloud Director Availability

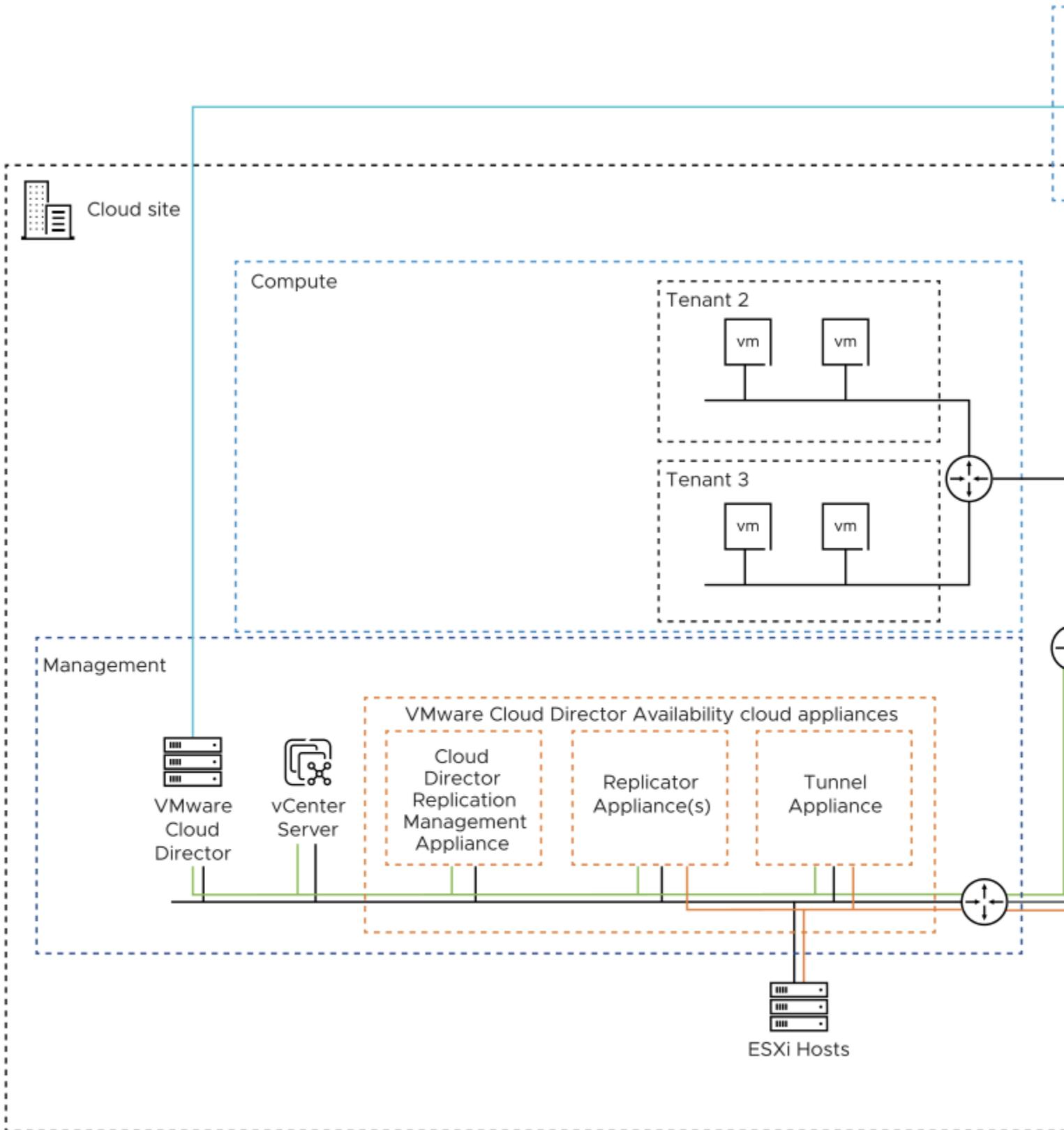
and the replication data traffic between the appliances, with all existing components in black:



**Paired Cloud Site with VMware Cloud Director Availability in VMware Cloud on AWS**

After pairing a cloud site, backed by VMware Cloud Director with VMware Cloud Director Availability in VMware Cloud on AWS, in the following deployment diagram the orange color shows the deployed cloud appliances of

VMware Cloud Director Availability and the replication data traffic between them, with all existing components in black:



- VMware Cloud Director Availability replication data traffic
- VMware Cloud Director Availability service management traffic
- VMware Cloud Director Availability Plug-in administration traffic
- Network connectivity

## Overview of the Configuration

For a summary of all the configured objects in the VMware Cloud on AWS SDDC, see [SDDC network configuration summary](#). VMware Cloud Director Availability resides behind the compute gateway in VMware Cloud on AWS. Configure the SDDC in VMware Cloud on AWS for the following access.

- To access vCenter Server in the management resource pool by administrative users and by VMware Cloud Director Availability.
- To access the management interface of VMware Cloud Director Availability for initial configuration.
- To access the Public Service Endpoint from external VMware Cloud Director Availability sites for pairing and migrations from these sites.

In VMware Cloud on AWS, the SDDC and VMware Cloud Director Availability must be prepared and configured in the following order.

### Procedure outline:

1. Prepare the VMware Cloud on AWS SDDC by creating the following objects. For the detailed SDDC preparation procedure, see [Prepare the SDDC in VMware Cloud on AWS for deployment](#).
  - a. A network segment, connecting all the cloud VMware Cloud Director Availability appliances.
  - b. A trusted management sources group, containing the public IP addresses of the **administrator** users that need access to vCenter Server in VMware Cloud on AWS for installing the cloud VMware Cloud Director Availability appliances.
  - c. A management firewall rule, allowing the trusted management group to access management gateway services like vCenter Server.
  - d. A separate resource pool, dedicated for all the cloud VMware Cloud Director Availability appliances.
2. Deploy the OVA of VMware Cloud Director Availability in the VMware Cloud on AWS SDDC. Alternatively, as a tenant deploy the On-Premises to Cloud Director Replication Appliance in on-premises data centers. For the detailed deployment procedure, see [Deploy VMware Cloud Director Availability in the SDDC](#).
3. Configure the network of the VMware Cloud on AWS SDDC by creating the following objects. For the detailed SDDC configuration procedure, see [Configure the network of the SDDC in VMware Cloud on AWS](#).
  - a. Two inventory services, one for the management interface of VMware Cloud Director Availability and one for the Public Service Endpoint.
  - b. Two public IP addresses requested in the SDDC, one to access the initial setup wizard in the management interface of VMware Cloud Director Availability and one allowing external pairing to the Public Service Endpoint.
  - c. Two NAT rules for forwarding the incoming network traffic to the correct cloud VMware Cloud Director Availability appliances.
  - d. Two management groups, one containing the source NAT public IP address of the SDDC used for bridging the access from the compute gateway VMware Cloud Director Availability appliances and one containing the Replicator Appliance instances.
  - e. Two management firewall rules, one allowing the access from the compute gateway source NAT to the management gateway vCenter Server and one allowing the Replicator Appliance instances access to ESXi datastores for provisioning.
  - f. Four compute groups, one containing the users that can access the management interface of VMware Cloud Director Availability and three groups containing the three types of cloud VMware Cloud Director Availability appliances.
  - g. Another two compute firewall rules, one allowing the access to the management interface of VMware Cloud Director Availability and one allowing the cloud appliances with outbound network access.
4. Configure VMware Cloud Director Availability in VMware Cloud on AWS by completing the initial wizard. For the detailed initial configuration procedure, see [Configure VMware Cloud Director Availability in VMware Cloud on AWS](#).
5. Configure the VMware Cloud on AWS SDDC for pairing with external VMware Cloud Director Availability sites by creating the following objects. For the detailed pairing preparation procedure, see [Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS](#).
  - a. A pairing compute group, containing the public IP addresses of the on-premises tenants and of the private cloud sites, backed by VMware Cloud Director.
  - b. A pairing compute gateway firewall rule, allowing the access from the preceding pairing compute group to the Public Service Endpoint for pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

6. Pair with external VMware Cloud Director Availability sites.
  - a. Optionally, as a tenant configure and pair On-Premises to Cloud Director Replication Appliance instances with VMware Cloud Director Availability in VMware Cloud on AWS. For the detailed initial on-premises configuration and pairing procedure, see [Configure and Pair the On-Premises to Cloud Director Replication Appliance](#).
  - b. Optionally, pair VMware Cloud Director Availability in VMware Cloud on AWS with private cloud sites backed by VMware Cloud Director. For the detailed pairing procedure with cloud sites, see [Pair VMware Cloud Director Cloud Sites](#).

After completing all these steps, by using the existing migration flow in VMware Cloud Director Availability the trusted, allowed, and paired providers and their trusted, allowed, and paired tenants can migrate workloads to VMware Cloud Director service in VMware Cloud on AWS.

- Later, to allow access to perform administrative tasks like certificate replacement by using the three types of management interfaces of the services of VMware Cloud Director Availability:
  - Add three inventory services for each management interface type: Replicator Service, Manager Service, and Tunnel Service.
  - Add three NAT rules, with additional NAT rule for each Replicator Service instance.
  - Modify the existing compute gateway firewall rule that allows access from the trusted compute sources group and include the three additional services, for a total of four inventory services.

For information about adding these networking objects, see [Post-configure the SDDC networking in VMware Cloud on AWS](#).

## Prepare the SDDC in VMware Cloud on AWS for deployment

To deploy and use VMware Cloud Director Availability™ in VMware Cloud™ on AWS for migrations, first prepare the Software-Defined Data Center (SDDC). Create a network segment and allow accessing the management gateway vCenter Server for appliances deployment.

- Verify that the SDDC is successfully deployed at VMware Cloud on AWS, that the cloud administrator user can login to the SDDC, and has permissions to deploy OVF templates.
- Verify that in the VMware Cloud Director service, the Cloud Director instance is deployed at VMware Cloud on AWS in the same AWS region as the SDDC, for example, *US West (Oregon)*, and that the Cloud Director instance is associated with the VMC SDDC.
- Verify that in the Cloud Director instance at least one organization, one organization network, one provider data center (Provider VDC), one organization virtual data center (Organization VDC), and a local administrator user with **CDS Provider Admin Role** exist and that the Cloud Director instance can host migrated virtual machines.

After meeting the SDDC prerequisites, prepare the SDDC for VMware Cloud Director Availability deployment outside the management resource pool. Before deploying the appliances, create a dedicated resource pool.

### NOTE

The access to the management resource pool is limited and the public IP addresses of all the users must be explicitly allowed before accessing the management components in the management resource pool, like vCenter Server for the appliances deployment.

For an overview, see [Migration with VMware Cloud Director service](#).

1. Log in to VMware Cloud on AWS at <https://vmc.vmware.com>.
2. In the VMC console, in the left pane click **SDDCs**.
3. Under the SDDC, click the **View Details** link.
4. Under the SDDC name, click the **Networking & Security** tab.
5. Add a network segment that connects the VMware Cloud Director Availability appliances so they can communicate between themselves and with other network services.
  - a) On the **Networking & Security** tab, in the left pane under the **Network** section, click **Segments**.
  - b) To add a dedicated routed network for the VMware Cloud Director Availability appliances, under **Segment List**, click **Add Segment** and enter the following settings.

Name	Enter a name for the network segment. For example, enter <i>vcda-network-segment</i> .
Type	Routed
Subnets	Enter an IPv4 CIDR subnet for all the VMware Cloud Director Availability appliances.

- c) To save the network segment, click **Save** and to finish configuring the segment click **No**.  
Under the Subnets column, you see the routed network **CIDR** used in the OVF deployment wizard, on the **Select Networks** page.

6. Before accessing the management gateway vCenter Server in VMware Cloud on AWS for deploying the VMware Cloud Director Availability appliances, create a *Trusted Management Sources Group* containing the allowed IP addresses.
  - a) On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.
  - b) To create a management group, click the **Management Groups** tab, click **Add Group** and enter a group name.
  - c) To add trusted members to this new management group, under the Compute Members column, click the **Set Members** link.
  - d) In the **Select Members** window, on the **IP Addresses** tab enter the IP addresses of the trusted users and click **Apply**.

Management Group Name	Management Group Trusted Members IP Addresses
<i>Trusted Management Sources Group</i>	Enter the externally-facing <i>public-IP-addresses</i> of the users granted with access to the vCenter Server management gateway service in VMware Cloud on AWS. <b>IMPORTANT</b> Ensure that you add all the public IP addresses of each user allowed to access vCenter Server in VMware Cloud on AWS or the users have no access.

- e) To save the management group, click **Save**.
7. To allow accessing the management gateway vCenter Server for the cloud appliances deployment, allow access from the trusted management sources group.
    - a) On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.
    - b) Click the **Management Gateway** tab, then click **Add Rule** and configure the following settings.

Name	Enter a name for the compute gateway firewall rule. For example, enter <i>vCenter Inbound From Trusted Management Sources Rule</i> .
Sources	Click <b>Any</b> in the Sources column. In the <b>Set Source</b> window select <b>User Defined Groups</b> , select the trusted IP addresses management group and click <b>Apply</b> . For example, select <i>Trusted Management Sources Group</i> .
Destinations	In the Destinations column click <b>Any</b> , then in the <b>Set Destination</b> window, select <b>System Defined Groups</b> and select <b>vCenter</b> .
Services	In the Services column, select <b>HTTPS (TCP 443)</b> .
Action	Allow

- c) To publish the new management gateway firewall rule, click **Publish**.
8. To obtain permissions for creating new virtual machines, create a separate resource pool dedicated for the multiple cloud VMware Cloud Director Availability appliances, outside the management resource pool.
    - a) Click **Open vCenter** and log in with the cloud admin user credentials.
    - b) Expand **SDDC-Datacenter**, right-click **Cluster-1** and select **New Resource Pool**.
    - c) In the **New Resource Pool** window, enter a name for the resource pool for the VMware Cloud Director Availability appliances. For example, enter *VCDA-Resource-Pool*.
    - d) Configure the **CPU** and the **Memory** sections and click **OK**.

The new resource pool shows under **SDDC-Datacenter > Cluster-1**.

After performing all the steps in this procedure, the SDDC in VMware Cloud on AWS is fully prepared for VMware Cloud Director Availability deployment. For a summary of the configuration, see [SDDC network configuration summary](#).

You can now deploy the VMware Cloud Director Availability appliances in VMware Cloud on AWS. For more information, see [Deploy VMware Cloud Director Availability in the SDDC](#).

## Deploy VMware Cloud Director Availability in the SDDC

In the VMware Cloud on AWS SDDC, as a provider, deploy all cloud VMware Cloud Director Availability appliances from a single `.ova` file. In the tenant data center, as a tenant you can deploy the On-Premises to Cloud Director Replication Appliance by using its dedicated `.ova` file.

- As a provider:
    - Verify that the VMware Cloud on AWS SDDC is prepared for VMware Cloud Director Availability deployment. For more information, see [Prepare the SDDC in VMware Cloud on AWS for deployment](#).
    - Verify that the user you use has permissions to deploy OVF templates. For example, use the `defaultcloudadmin@vmc.local` user that has the required permissions.
    - Download the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
  - As a tenant:
    - Verify that the user you use has the required permissions to deploy an OVF template in the tenant data center.
    - Download the `VMware-Cloud-Director-Availability-On-Premises-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the On-Premises to Cloud Director Replication Appliance.
  - As a provider, after preparing the VMware Cloud on AWS SDDC for deployment, repeat this procedure multiple times and deploy all the cloud appliances of VMware Cloud Director Availability by using the downloaded provider `.ova` file.
  - As a tenant, follow this same procedure once in the tenant data center and deploy the On-Premises to Cloud Director Replication Appliance by using the downloaded on-premises `.ova` file.
1. Navigate to the resource pool for the appliance deployment.
    - As a provider, repeat the steps in this procedure multiple times and deploy the following number of cloud VMware Cloud Director Availability appliances under the dedicated resource pool **SDDC-Datacenter > Cluster-1 > VCDA-Resource-Pool1**, created in [step 10 in Prepare the SDDC for Deployment](#):
      - One or more Replicator Appliance instances.
      - A Cloud Director Replication Management Appliance.
      - A Tunnel Appliance.
    - As a tenant, follow the steps once in your data center and deploy the On-Premises to Cloud Director Replication Appliance.
      - a) Right-click the resource pool for the appliance deployment.
      - b) From the drop-down menu, select **Deploy OVF Template**.
  2. Complete the **Deploy OVF Template** wizard.
    - a) On the **Select an OVF template** page, browse to the `.ova` file location and click **Next**.
    - b) On the **Select a name and folder** page, enter a name for the appliance, select a deployment location, and click **Next**.
    - c) On the **Select a compute resource** page, select a host, or cluster as a compute resource to run the appliance on, and click **Next**.
 

As a provider, select the dedicated resource pool for each appliance, for example select `VCDA-Resource-Pool1`.
    - d) On the **Review details** page, verify the OVF template details and click **Next**.
    - e) On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.
    - f) As a provider, on the **Configuration** page, select an appliance deployment type for each appliance and click **Next**.
      - One or more Replicator Appliance instances.
      - A Cloud Director Replication Management Appliance.
      - A Tunnel Appliance.

For information about the appliance deployment types, see [Deployment Requirements](#) in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

- g) On the **Select storage** page, select **WorkloadDatastore** and click **Next**.
- h) On the **Select networks** page, select the network for the VMware Cloud Director Availability appliance and click **Next**.
  - As a provider, select the dedicated routed network for the VMware Cloud Director Availability appliances. For information about this dedicated routed network, see [step 5.b in Prepare the SDDC for Deployment](#).
  - As a tenant, to ensure a successful pairing select a network with access to the VMware Cloud on AWS SDDC.
- i) On the **Customize template** page, customize the deployment properties of the appliance and click **Next**.

Root password	Enter and confirm the initial password for the appliance <b>root</b> user. Later, when logging in for the first time, this initial password must be changed.
Address	<ul style="list-style-type: none"> <li>• As a provider, enter an IP address in CIDR notation in the <code>vcd a-network-segment</code> dedicated routed network for the cloud VMware Cloud Director Availability appliances. For information about this network, see <a href="#">step 5.b in Prepare the SDDC for Deployment</a>.</li> <li>• As a tenant, enter an IP address in CIDR notation that belongs in the tenant data center network.</li> </ul>
Gateway	<ul style="list-style-type: none"> <li>• As a provider, enter the compute gateway.</li> <li>• As a tenant, enter the tenant data center gateway.</li> </ul>
DNS servers	<ul style="list-style-type: none"> <li>• As a provider, enter the compute gateway DNS service IP address of the SDDC. To obtain it, click the <b>Networking &amp; Security</b> tab, then in the left pane under <b>System</b>, click <b>DNS</b> and next to the <code>Compute Gateway DNS Forwarder</code>, copy its IP address from the <code>DNS Server IP</code> column.</li> <li>• As a tenant, enter the IP address of the DNS server in the tenant data center.</li> </ul>
NTP Server	<p>Enter the address of the NTP server for the VMware Cloud Director Availability appliance to use.</p> <ul style="list-style-type: none"> <li>• As a provider, check the available time servers in the zone of your AWS instance and use the same NTP server as vCenter Server, ESXi, VMware Cloud Director, and all cloud VMware Cloud Director Availability appliances.</li> <li>• As a tenant, use the same NTP server as vCenter Server and ESXi.</li> </ul>

- j) On the **Ready to complete** page, review the settings, optionally select **Power on after deployment** and to begin the OVF deployment, click **Finish**.

The **Recent Tasks** pane shows a new task for initializing the OVF deployment. After the task completes, the new appliance is created in the VMware Cloud Director Availability appliances resource pool.

3. After deployment, power on the appliance.
  - a) Under the resource pool for the appliance deployment, right-click the virtual machine.
  - b) From the context menu, select **Power > Power On**.

The VMware Cloud Director Availability appliances are deployed.

- As a provider, you can now configure the SDDC network. For more information, see [Configure the network of the SDDC in VMware Cloud on AWS](#).
- As a tenant, you can now configure the On-Premises to Cloud Director Replication Appliance. For more information, see [Configure and Pair the On-Premises to Cloud Director Replication Appliance](#).

## Configure the network of the SDDC in VMware Cloud on AWS

To allow pairing with VMware Cloud Director Availability in VMware Cloud on AWS, first configure the network settings of the SDDC.

- Verify that the SDDC is first prepared for VMware Cloud Director Availability deployment. For information about the required steps, see [Prepare the SDDC in VMware Cloud on AWS for deployment](#).
- Verify that VMware Cloud Director Availability 4.2 or later is deployed in VMware Cloud on AWS. For more information, see [Deploy VMware Cloud Director Availability in the SDDC](#).

The access to the resource pools is limited in VMware Cloud on AWS and the private IP addresses of all the cloud appliances of VMware Cloud Director Availability must be explicitly allowed as well as to access the management and infrastructure components in the management resource pool, like vCenter Server and ESXi.

VMware Cloud Director Availability in VMware Cloud on AWS provides two services to the Internet. To use the two services in the configuration of the necessary NAT rules, you explicitly define them since both services internally use non-

standard HTTPS ports. These two services in conjunction with the following two NAT rules translate the network traffic coming to the public IP address on the external port 443/TCP:

- Towards the Cloud Director Replication Management Appliance, internally on port 8046/TCP for management interface network traffic to the Cloud Service.
- Towards the Tunnel Appliance, internally on port 8048/TCP for replication data network traffic to the Public Service Endpoint.

1. Log in to VMware Cloud on AWS at <https://vmc.vmware.com>.
2. Add two new inventory SDDC services, for the management interface and for the Public Service Endpoint.
  - a) In the VMC console, in the left pane click **SDDCs**.
  - b) Under the SDDC click **View Details** and click the **Networking & Security** tab.
  - c) In the left pane under the **Inventory** section, click **Services**.  
Repeat the following steps twice.
    - Add an inventory service for the management interface of the Cloud Director Replication Management Appliance.
    - Add another inventory service for the Public Service Endpoint of the Tunnel Appliance.
  - d) To add an inventory SDDC service, click **Add Service**.
  - e) Enter a name and optionally a description for each service.
  - f) For each service, in the Service Entries column, click the **Set Service Entries** link.
  - g) For each service, in the **Set Service Entries** window, from the **Type** drop down menu select **Layer 3 and above**.
  - h) For each service, on the **Port-Protocol** tab click **Add Service Entry**, enter the details from the respective column, and click **Apply**.

Option	Management Interface Inventory Service	Public Service Endpoint Inventory Service
Name	Enter a name for the service entry of the Cloud Director Replication Management Appliance management interface. For example, enter <i>VCDA-Cloud-Service-Management</i> .	Enter a name for the service entry of the Tunnel Appliance Public Service Endpoint. For example, enter <i>VCDA-Tunnel-Service-Endpoint</i> .
Service Type	Select <b>TCP</b> .	Select <b>TCP</b> .
Additional Properties	Leave the <b>Source Ports</b> text box blank.	Leave the <b>Source Ports</b> text box blank.
	To access the management interface of the Cloud Director Replication Management Appliance in the <b>Destination Ports</b> text box, in enter port 8046.	To access the Public Service Endpoint of the Tunnel Appliance, in the <b>Destination Ports</b> text box enter port 8048.

- i) To save each inventory service, click **Save**.  
On the **Services** page, both services show:

Name	Service Entries
<i>VCDA-Cloud-Service-Management</i>	TCP (Source: Any   Destination: 8046)
<i>VCDA-Tunnel-Service-Endpoint</i>	TCP (Source: Any   Destination: 8048)

3. To later use in NAT rules, request two new public SDDC IP addresses.
  - Request a public IP address to access the initial setup wizard in the management interface of the Cloud Director Replication Management Appliance.
  - Request a public IP address to allow external pairing to the Public Service Endpoint of the Tunnel Appliance.
  - a) On the **Networking & Security** tab, in the left pane under the **System** section click **Public IPs**.
  - b) To request a public IP address for the Cloud Director Replication Management Appliance, click **Request New IP**, enter a note, and click **Save**.  
For example, as a note enter *VCDA-Management-Public-IP-address*.
  - c) To request a public IP address for the Tunnel Appliance, click **Request New IP**, enter a note and click **Save**.  
For example, as a note enter *VCDA-Tunnel-Public-IP-address*.
4. To forward the incoming network traffic to the correct cloud appliances and ports, add two new NAT rules.
  - a) On the **Networking & Security** tab, in the left pane under the **Network** section click **NAT**.  
Repeat the following step twice.
    - Add a NAT rule for the management interface of the Cloud Director Replication Management Appliance.
    - Add another NAT rule for the incoming network traffic to the Public Service Endpoint of the Tunnel Appliance.
  - b) To add a NAT rule, click **Add NAT Rule**, configure the following settings and click **Save**.

Option	Management Interface NAT	Public Service Endpoint NAT
Name	Enter a name for the NAT rule for the Cloud Director Replication Management Appliance management interface. For example, enter <i>VCDA Management Interface NAT</i> .	Enter a name for the NAT rule for the Tunnel AppliancePublic Service Endpoint. For example, enter <i>VCDA Tunnel Service Endpoint NAT</i> .
Public IP	Select the <i>VCDA-Management-Public-IP-addresses</i> .	Select the <i>VCDA-Tunnel-Public-IP-address</i> .
Service	Select the inventory service for the Cloud Director Replication Management Appliance management interface. For example, select <i>VCDA-Cloud-Service-Management</i> .	Select the inventory service for the Tunnel AppliancePublic Service Endpoint. For example, select <i>VCDA-Tunnel-Service-Endpoint</i> .
Public Port	Enter port 443.	Enter port 443.
Internal IP	Enter the <i>private-IP-address</i> of the Cloud Director Replication Management Appliance.	Enter the <i>private-IP-address</i> of the Tunnel Appliance.
Internal Port	8046 (non-editable)	8048 (non-editable)
Firewall	Match Internal Address	Match Internal Address

After completing the initial configuration, to reduce the possible attack surface the NAT rule for the management interface can be disabled or removed. VMware Cloud Director Availability remains accessible from the Cloud Director instance by using the plug-in for VMware Cloud Director Availability.

5. To later create a management group and use it in a management firewall rule, note the compute gateway source NAT *public IP address* of the SDDC.
  - a) On the **Networking & Security** tab, in the left pane click **Overview**.
  - b) Under **Default Compute Gateway** and under **Workloads**, note the **Source NAT Public IP** address of the SDDC.
6. To prepare the cloud appliances access to the management gateway services like vCenter Server and ESXi, add two management groups.
  - a) On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.
  - b) Click the **Management Groups** tab.
 

Repeat the following steps two times.

    - Add a management group, containing the private IP addresses of all the deployed Replicator Appliance instances.
    - Add another management group, containing the compute gateway source NAT.
  - c) To create a management group, click **Add Group** and for each group enter a management group name.
  - d) To add trusted members to each management group, under the Compute Members column, click the **Set Members** link.
  - e) In the **Select Members** window, on the **IP Addresses** tab enter the following IP addresses for each management group and click **Apply**.

Management Group Name	Management Group Trusted Members IP Addresses
<i>SNAT VCDA Management Group</i>	<ul style="list-style-type: none"> <li>• Enter the compute gateway source NAT <i>public-IP-address</i> of the SDDC, as noted in the previous step.</li> <li>• Enter the subnet group of the VMware Cloud Director Availability appliances. For example, enter the <i>vcda-network-segment</i>.</li> </ul>
<i>VCDA Replicators Management Group</i>	Enter the <i>private-IP-addresses</i> reserved within the <i>vcda-network-segment</i> for all the Replicator Appliance instances deployed in VMware Cloud on AWS. All Replicator Appliance instances must access the vCenter Server management gateways services for virtual machines provisioning and performing replication tasks with the ESXi hosts and datastores.

- f) To save each management group, click **Save**.
7. To allow the internal communication from the cloud appliances to the vCenter Server and to the ESXi datastore in the management gateway, add two new management gateway firewall rules.
    - a) On the **Gateway Firewall** page, click the **Management Gateway** tab.
 

Repeat the following steps twice.

      - Add a management firewall rule for allowing the network traffic from the compute gateway source NAT to the management gateway vCenter Server.
      - Add another management firewall rule for allowing the Replicator Appliance instances writing in the destination ESXi datastore.

- b) To create a management firewall rule, click **Add Rule**.
- c) Configure each of the two management firewall rules and click **Apply** when prompted.

Option	vCenter Server Management Gateway Firewall Rule	ESXi Hosts Management Gateway Firewall Rule
Name	Enter a name for the vCenter Server management gateway rule. For example, enter <i>SNAT VCDA to vCenter Rule</i> .	Enter a name for the ESXi management gateway rule. For example, enter <i>VCDA Replicators to ESXi Rule</i> .
Sources	Click <b>Any</b> . In the <b>Set Source</b> window, select <b>User Defined Groups</b> and select the management group for the SNAT. For example, select <i>SNAT VCDA Management Group</i> and click <b>Apply</b> .	Click <b>Any</b> . In the <b>Set Source</b> window, select <b>User Defined Groups</b> and select the management group for the private IP addresses of the Replicator Appliance instances. For example, select <i>VCDA Replicators Management Group</i> and click <b>Apply</b> .
Destinations	Click <b>Any</b> . In the <b>Set Destination</b> window under <b>System Defined Groups</b> , select <b>vCenter</b> and click <b>Apply</b> .	Click <b>Any</b> . In the <b>Set Destination</b> window under <b>System Defined Groups</b> , select <b>ESXi</b> and click <b>Apply</b> .
Services	Click <b>Any</b> and select <b>HTTPS (TCP 443)</b> .	To allow the Data Engine Service of the Replicator Appliance writing in the ESXi datastores, click <b>Any</b> and select <b>HTTPS (TCP 443)</b> and <b>Provisioning &amp; Remote Console (TCP 902)</b> .
Action	Allow	Allow

- d) After creating both management gateway firewall rules, click **Publish**.

8. To prepare for accessing the compute gateway services in VMware Cloud on AWS, create four compute groups.
- a) On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.  
Repeat the following steps four times.
- Add a compute group for the trusted users that need access to the VMware Cloud Director Availability management interface.
  - Add a compute group for the Cloud Director Replication Management Appliance.
  - Add a compute group for all the Replicator Appliance instances.
  - Add a compute group for the Tunnel Appliance.
- b) To create a compute group, under the **Compute Groups** tab, click **Add Group** and enter a group name.
- c) To add trusted members to each compute group, under the Compute Members column, click the **Set Members** link.
- d) In the **Select Members** window, on the **IP Addresses** tab enter the following IP addresses for each compute group and click **Apply**.

Compute Group Name	Compute Group Trusted Members IP Addresses
<i>Trusted Compute Sources Group</i>	Enter the externally-facing <i>public-IP-addresses</i> of the users granted with access to the management interface of VMware Cloud Director Availability. <b>IMPORTANT</b> Ensure that you add all the public IP addresses of each user allowed to access VMware Cloud Director Availability in VMware Cloud on AWS or the users have no access.
<i>VCDA Manager Compute Group</i>	Enter the <i>private-IP-address</i> of the Cloud Director Replication Management Appliance.
<i>VCDA Replicators Compute Group</i>	Enter the <i>private-IP-addresses</i> of all the Replicator Appliance instances.

Compute Group Name	Compute Group Trusted Members IP Addresses
<i>VCDA Tunnel Compute Group</i>	Enter the <i>private-IP-address</i> of the Tunnel Appliance.

e) To save each compute group, click **Save**.

9. To prepare for completing the initial setup wizard, allow accessing the VMware Cloud Director Availability management interface by the trusted compute sources. Also allow the cloud appliances outbound access, both by adding two new compute gateway firewall rules.

a) On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.

Repeat the following steps twice.

- Add a compute gateway firewall rule for allowing the trusted compute sources access to the Cloud Director Replication Management Appliance for completing the initial setup wizard of VMware Cloud Director Availability.
- Add a compute gateway firewall rule for allowing the VMware Cloud Director Availability appliances outbound network traffic from the compute gateway.

b) On the **Compute Gateway** tab, click **Add Rule**.

c) Configure each of the two compute firewall rules and click **Apply** when prompted.

Option	Inbound Compute Gateway Firewall Rule	Outbound Compute Gateway Firewall Rule
Name	Enter a name for the inbound compute gateway rule. For example, enter <i>VCDA Management from Trusted Compute Sources Rule</i> .	Enter a name for the outbound compute gateway rule. For example, enter <i>VCDA Appliances Outbound Compute Rule</i> .
Sources	Click <b>Any</b> . In the <b>Set Source</b> window, select the trusted compute sources group and click <b>Apply</b> . For example, select <i>Trusted Compute Sources Group</i> .	Click <b>Any</b> . In the <b>Set Source</b> window select the three compute groups for the VMware Cloud Director Availability appliances and click <b>Apply</b> . For example, select all three <i>VCDA Manager Compute Group</i> , <i>VCDA Replicators Compute Group</i> , and <i>VCDA Tunnel Compute Group</i> .
Destinations	Click <b>Any</b> . In the <b>Set Destination</b> window, select the Cloud Director Replication Management Appliance compute group and click <b>Apply</b> . For example, select <i>VCDA Manager Compute Group</i> .	Any
Services	Click <b>Any</b> . In the <b>Set Services</b> window, select the Cloud Director Replication Management Appliance management interface service and click <b>Apply</b> . For example, select <i>VCDA-Cloud-Service-Management TCP (Source: Any   Destination: 8046)</i> .	Any
Applied To	All Uplinks	All Uplinks
Action	Allow	Allow

d) After creating both compute gateway firewall rules, click **Publish**.

The SDDC configuration in VMware Cloud on AWS is complete and ready for the initial configuration of VMware Cloud Director Availability. In summary, the SDDC network in VMware Cloud on AWS is configured with:

- ***vcda-network-segment***:  
A dedicated routed network for all the cloud appliances of VMware Cloud Director Availability.
- **Public IP addresses**:

Two requested public IP addresses, for the management interface of the Cloud Director Replication Management Appliance, and for the Public Service Endpoint of the Tunnel Appliance.

- **Management gateway:**
  - Access from the compute gateway source NAT address to the management gateway vCenter Server, used for bridging the access from the compute gateway VMware Cloud Director Availability appliances.
  - Access from the Replicator Appliance to the management gateway ESXi datastore, used for destination of migrations.
- **Compute gateway:**
  - Access from the *Trusted Compute Sources Group* to the management interface of the Cloud Service, used for completing the initial setup. Later, modifying the same rule allows access to all four types of management interfaces of VMware Cloud Director Availability. For more information, see [Post-configure the SDDC networking in VMware Cloud on AWS](#).
  - Access from VMware Cloud Director Availability appliances to Internet, used for the external network traffic from the compute gateway.

For information about the summary of the SDDC network configuration, see [SDDC network configuration summary](#).

You can now configure VMware Cloud Director Availability in VMware Cloud on AWS by completing the initial setup wizard of the Cloud Director Replication Management Appliance. For more information, see [Configure VMware Cloud Director Availability in VMware Cloud on AWS](#).

## Configure VMware Cloud Director Availability in VMware Cloud on AWS

After deploying all the cloud appliances in VMware Cloud on AWS, configure VMware Cloud Director Availability by configuring the Cloud Service instance in the Cloud Director Replication Management Appliance.

- Verify that the *requested-VCDA-public-IP-address* is added as trusted in both the management and in the compute groups.
  - Verify that the network settings of the SDDC are configured. For more information, see [Configure the network of the SDDC in VMware Cloud on AWS](#).
1. Log in to the management interface of the Cloud Director Replication Management Appliance.
    - a) In a Web browser, go to `https://VCDA-management-public-IP-address:443/ui/admin`.  
To ensure your browser redirects you, the NAT rule applies, and the browser trusts the appliance certificate, enter both the `https://` prefix and the `/ui/admin` page suffix.
    - b) If this is the first time you are opening this page in this browser, cancel the certificate prompt for adding the certificate in your browser.
    - c) Select **Appliance login** and enter the **root** user password, set during the initial OVA deployment.
    - d) Click **Login**.

As this Cloud Director Replication Management Appliance is not yet configured, you are redirected to `https://VCDA-management-public-IP-address/ui/portal/initial-config`.

2. In the **VCD A Appliance Password** window, change the initial **root** user password set during the OVA deployment.
  - a) Enter the initial **root** user password as configured during the OVA deployment.
  - b) Enter and confirm a new password.  
The password that you enter must be a secured password with a minimum of eight characters and it must consist of:
    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as: & # % .
  - c) After entering and confirming the new password, click **Apply**.  
The **Getting Started** page opens.
3. Under **Steps for fresh installation**, click the **Run the initial setup wizard** link.  
Under **Deploy the Cloud Replication Management Appliance**, you can see the IP address of this newly deployed Cloud Director Replication Management Appliance.
4. To configure VMware Cloud Director Availability, complete the **Initial Setup** wizard.
  - a) On the **Licensing** page, enter a VMware Cloud Director Availability license key and click **Next**.  
After accepting the license key, if you cancel the wizard, on the next run of the wizard on the **Licensing** page the license key is pre-filled and greyed-out.
  - b) On the **Site Details** page, configure the Cloud Service instance site and click **Next**.

Site Name	Enter a site name for this Cloud Service instance. <b>IMPORTANT</b> The site name is used as an identifier of this instance of VMware Cloud Director Availability and cannot be changed later without impacting the active replications.
Service Endpoint address	Enter <code>https://VCD A-tunnel-public-IP-address:443</code> and ensure that you enter the 443 port.
Description	Optionally, enter a description for this VMware Cloud on AWS site.
Choose which data engines to be enabled.	<ul style="list-style-type: none"> <li>• To enable migrations to VMware Cloud on AWS, select <b>VMC</b>.</li> <li>• To enable migrations to and from private cloud sites, select <b>Classic</b>.</li> </ul>

- c) On the **VMware Cloud Director** page, register the Cloud Service instance with the Cloud Director instance and click **Next**.

VMware Cloud Director endpoint URL	Enter the public address of the Cloud Director instance and to autocomplete it as <code>https://Cloud-Director-service-Public-IPv6-Address/api</code> , press Tab. For example, use the IPv6 IP address you use to browse the Cloud Director instance.
VMware Cloud Director user name	Enter a local user for the Cloud Director instance. Use a <b>System administrator</b> user or a user with the <b>CDS provider admin</b> role, for example enter <code>administrator@system</code> .

VMware Cloud Director password	Enter the password of the Cloud Director instance user.
--------------------------------	---

Verify the thumbprint and accept the SSL certificate of the Cloud Director instance.

- d) On the **Replicator Service instances** page, register the Cloud Service with the vCenter Server Lookup service and with the Replicator Service instances in the SDDC, then click **Next**.

Option	Description	
<b>Lookup Service Address</b>	Enter the public URL address of the VMware Cloud on AWSvCenter Server Lookup service and to autocomplete the address as <code>https://vCenter-Public-URL:443/lookupservice/sdk</code> , press <b>Tab</b> . For example, use the public URL from the vCenter Server you use to browse vSphere in VMware Cloud on AWS and deploy the cloud appliances.	
<b>Use above Lookup Service address for Manager, Cloud and Tunnel</b>	<ul style="list-style-type: none"> <li>By default, the vCenter Server Lookup service address is used only for all the Replicator Service instances. By not using this address for the remaining services, their appliances show a yellow indicator which is expected for the vCenter Server Lookup service that is not configured. By not activating this toggle, single sign-on (SSO) user authentication is not available for the Manager Service, the Cloud Service, and the Tunnel Service. To later configure the vCenter Server Lookup service address for the services, see <a href="#">Configure VMware Cloud Director Availability to Accept the vCenter Server Lookup service Certificate</a> in the <i>Administration Guide</i>.</li> <li>To also use this vCenter Server Lookup service address for the Manager Service, for the Cloud Service, and for the Tunnel Service, and enable SSO for all services, activate this toggle.</li> </ul>	
<b>Replicator 1</b>	<b>Replicator Service address</b>	Enter the private IP address of the Replicator Appliance and to autocomplete the address as <code>https://Replicator-Private-IP-Address:8043</code> , press <b>Tab</b> .
	<b>Replicator Service root password</b>	Enter the password of the <b>root</b> user of the Replicator Service.
	<b>Test Connection</b>	Click to verify the connectivity to the endpoint and the <b>root</b> user password, and save the Replicator Service instance. If the initial <b>root</b> user password of the Replicator Appliance is not changed since deploying the appliance, you must change this password. Enter the initial <b>root</b> user password set during the OVA deployment, then enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: <ul style="list-style-type: none"> <li>At least one lowercase letter.</li> <li>At least one uppercase letter.</li> <li>At least one number.</li> <li>At least one special character, such as: &amp; # % .</li> </ul>
	<b>SSO user name</b>	Enter a <b>cloud admin</b> user with administrative privileges in the single sign-on domain, for example enter <code>cloudadmin@vmc.local</code> . <b>NOTE</b> Cannot use the <b>cloudadmin@vmc.local</b> user for single-sign-on (SSO) user authentication to the Cloud Service or for VMware Cloud Director Availability authentication.
	<b>SSO password</b>	The password for the administrative user.
	<b>Description</b>	Optionally, enter a description for the Replicator Service instance.

Option	Description
<b>Add a Replicator Service Instance</b>	Optionally, add additional Replicator Service instances.

Verify the thumbprints and accept the SSL certificates of the vCenter Server Lookup service in VMware Cloud on AWS and of all the Replicator Service instances.

- e) On the **Tunnel Service** page, register the Cloud Service with the Tunnel Service, test the connection, and click **Next**.

Tunnel Service address	Enter the private IP address of the Tunnel Appliance and to autocomplete the address as <code>https://Tunnel-Private-IP-Address:8047</code> , press Tab.
Root password	Enter the password of the <b>root</b> user of the Tunnel Service.
Test Connection	<p>Click to verify the connectivity to the endpoint and the <b>root</b> user password, and save the Tunnel Service instance. If the initial <b>root</b> user password of the Tunnel Appliance is not changed since deploying the appliance, you must change this password. Enter the initial <b>root</b> user password set during the OVA deployment, then enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:</p> <ul style="list-style-type: none"> <li>• At least one lowercase letter.</li> <li>• At least one uppercase letter.</li> <li>• At least one number.</li> <li>• At least one special character, such as: &amp; # % .</li> </ul>

Verify the thumbprint and accept the SSL certificate of the Tunnel Service.

- f) On the **Ready To Complete** page, review the Cloud Service configuration summary and click **Finish**.
5. To allow the tenants to perform migrations, assign them with a replication policy.
- In the left pane, under **Configuration** click **Policies**.
  - Optional: Create a replication policy or modify the Default policy to allow replications.
  - To assign a replication policy click **Assign** and select the organizations to assign the policy to. Alternatively, click **Organizations** and after selecting the organizations to assign a policy to, click **Assign** and select the policy to assign.

VMware Cloud Director Availability configuration in VMware Cloud on AWS is complete.

You can now configure the network of VMware Cloud on AWS for pairing with on-premises tenants and with remote cloud sites. For more information, see [Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS](#).

## Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS

After deploying and configuring VMware Cloud Director Availability and the external access, the next step is configuring from where VMware Cloud on AWS allows establishing pairings. Create an additional compute group with the public IP

addresses allowed for pairing and an additional firewall rule allowing the access from this new group to the Public Service Endpoint.

- Verify that before pairing, network port 3030/TCP from the remote Tunnel Appliance and the remote On-Premises to Cloud Director Replication Appliance to the Replicator Appliance in VMware Cloud on AWS is allowed. For information about the required network ports, see <https://ports.vmware.com/home/VMware-Cloud-Director-Availability>.
- Verify that VMware Cloud Director Availability in VMware Cloud on AWS is configured. For more information, see [Configure VMware Cloud Director Availability in VMware Cloud on AWS](#).

To allow pairing with VMware Cloud Director Availability in VMware Cloud on AWS, in the compute group below add the public IP addresses of the Public Service Endpoint instances and the on-premises appliances.

1. Log in to VMware Cloud on AWS at <https://vmc.vmware.com>.
2. In the VMC console, in the left pane click **SDDCs**.
3. Under the SDDC click **View Details** and click the **Networking & Security** tab.
4. To allow accessing the Public Service Endpoint compute gateway service in VMware Cloud on AWS, create a compute group containing the remote sites IP addresses.
  - a) On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.
  - b) To create the compute group, under the **Compute Groups** tab, click **Add Group** and enter a group name, for example enter *VCDA Pairing Compute Group*.
  - c) To add trusted sites members to the compute group, under the Compute Members column, click the **Set Members** link.
  - d) In the **Select Members** window, on the **IP Addresses** tab enter the IP addresses of the following site members and click **Apply**.
    - To allow each private cloud site backed by VMware Cloud Director pairing, add the Public Service Endpoint *public-IP-address* of the Tunnel Appliance in the private cloud site.
    - To allow each tenant pairing, add the *public-IP-addresses* of all their On-Premises to Cloud Director Replication Appliance instances.

**IMPORTANT**  
Adding or removing IP addresses from this compute group controls which remote cloud sites and on-premises tenants can establish pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

Before VMware Cloud Director Availability pairs with another site, to allow the pair add the remote site IP address in the *VCDA Pairing Compute Group*.
  - e) To save the pairing compute group, click **Save**.
5. To allow access from the pairing compute group, create a compute gateway firewall rule.
  - a) On the **Networking & Security** tab, in the left pane under the **Security** section, click **Gateway Firewall**.
  - b) On the **Compute Gateway** tab, click **Add Rule** and configure the following settings.

Name	Enter a name for the compute gateway firewall rule, for example enter <i>VCDA Pairing Compute Rule</i> .
Sources	Click <b>Any</b> in the Sources column, then in the <b>Set Source</b> window select <b>User Defined Groups</b> , select the pairing IP addresses compute group, for example select <i>VCDA Pairing Compute Group</i> , and click <b>Apply</b> .

Destinations	Click <b>Any</b> in the Sources column, then in the <b>Set Source</b> window select <b>User Defined Groups</b> , select the Tunnel Appliance IP address compute group, for example select <i>VCDA Tunnel Compute Group</i> , and click <b>Apply</b> .
Services	In the Services column, click <b>Any</b> , then in the <b>Set Source</b> window, select the Public Service Endpoint service, for example select <i>VCD A-Service-Endpoint TCP (Source: Any   Destination: 8048)</i> and click <b>Apply</b> .
Applied To	All Uplinks
Action	Allow

By default, the new compute gateway firewall rule is enabled, allowing the Tunnel AppliancePublic Service Endpoint access from the pairing IP addresses compute group.

- c) To publish the new compute gateway firewall rule, click **Publish**.

The new rule receives an integer ID value, used in the log entries that it generates.

VMware Cloud Director Availability in VMware Cloud on AWS allows pairing with On-Premises to Cloud Director Replication Appliance instances and with VMware Cloud Director Availability instances in private cloud sites backed by VMware Cloud Director.

- Tenants can now configure and pair their On-Premises to Cloud Director Replication Appliance and migrate their workloads to VMware Cloud on AWS. For more information, see [Configure and Pair the On-Premises to Cloud Director Replication Appliance](#).
- You can now pair private cloud sites and migrate cloud workloads to VMware Cloud on AWS. For more information, see [Pair VMware Cloud Director Cloud Sites](#).
- You can allow administrative operations by using the management interfaces of the services of VMware Cloud Director Availability. For more information, see [Post-configure the SDDC networking in VMware Cloud on AWS](#).

## SDDC network configuration summary

After configuring the network of the SDDC and configuring the network of VMware Cloud on AWS for pairing with remote VMware Cloud Director Availability sites, check the summary of the network configuration.

### Management Gateway Firewall Rules

Name	Sources	Destinations	Services	Explanation
<i>vCenter Inbound From Trusted Management Sources Rule</i>	<i>Trusted Management Sources Group</i>	vCenter	HTTPS	Allows the trusted management sources accessing the management gateway vCenter Server for the deployment of the cloud appliances in the compute gateway.
<i>SNAT VCDA to vCenter Rule</i>	<i>SNAT VCDA Management Group</i>	vCenter	HTTPS	Allows the compute gateway source NAT accessing the management gateway vCenter Server for bridging the access from the compute gateway cloud VMware Cloud Director Availability appliances.
<i>VCDA Replicators to ESXi Rule</i>	<i>VCDA Replicators Management Group</i>	ESXi	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• Provisioning &amp; Remote Console</li> </ul>	Allows all the Replicator Appliance instances writing in the destination ESXi datastore.

For information about creating these management firewall rules, see [Prepare the SDDC in VMware Cloud on AWS for deployment](#) and [Configure the network of the SDDC in VMware Cloud on AWS](#).

### Compute Gateway Firewall Rules

Name	Sources	Destinations	Services	Explanation
<i>VCDA Management from Trusted Compute Sources Rule</i>	<i>Trusted Compute Sources Group</i>	<i>VCDA Manager Compute Group</i>	<i>VCDA-Cloud-Service-Management TCP (Source: Any   Destination: 8046)</i>	Allows the trusted compute sources accessing the management interface of the Cloud Service for completing the initial setup. Later, modifying the same rule allows access to all four types of management interfaces of VMware Cloud Director Availability. For more information, see <a href="#">Post-configure the SDDC networking in VMware Cloud on AWS</a> .
<i>VCDA Appliances Outbound Compute Rule</i>	<ul style="list-style-type: none"> <li><i>VCDA Manager Compute Group</i></li> <li><i>VCDA Replicators Compute Group</i></li> <li><i>VCDA Tunnel Compute Group</i></li> </ul>	Any	Any	Allows the VMware Cloud Director Availability appliances to Internet for the external network traffic from the compute gateway.
<i>VCDA Pairing Compute Rule</i>	<i>VCDA Pairing Compute Group</i>	<i>VCDA Tunnel Compute Group</i>	<i>VCDA-Service-Endpoint TCP (Source: Any   Destination: 8048)</i>	Allows the on-premises tenants and the remote cloud sites backed by VMware Cloud Director pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

For information about creating these compute firewall rules, see [Configure the network of the SDDC in VMware Cloud on AWS](#) and [Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS](#).

## Pairing with remote sites

Pair the local site in VMware Cloud on AWS with remote VMware Cloud Director Availability sites for migrating their workloads over. Pair this site with On-Premises to Cloud Director Replication Appliance and with cloud sites backed by VMware Cloud Director.

### Configure and Pair the On-Premises to Cloud Director Replication Appliance

In the tenants data centers, by using the management interface of the On-Premises to Cloud Director Replication Appliance, you must first change the initial `root` user password that you set during the OVA deployment. Then you register the appliance with the local vCenter Server Lookup service and with VMware Cloud Director Availability in VMware Cloud on AWS.

- Verify that before pairing the `tenant-public-IP-address` of the tenant data center where the On-Premises to Cloud Director Replication Appliance is deployed is added as a trusted IP address. As a service provider, for

information about adding the tenants IP addresses, see step 8 in [Prepare the SDDC in VMware Cloud on AWS for deployment](#).

- Verify that before pairing VMware Cloud Director Availability in VMware Cloud on AWS is configured. As a service provider, for more information, see [Configure VMware Cloud Director Availability in VMware Cloud on AWS](#).
1. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
    - a) In a Web browser, go to `https://On-Prem-Appliance-IP-Address/ui/admin`.
    - b) Select **Appliance login** and enter the **root** user password, set during the initial OVA deployment.
    - c) Click **Login**.

As the appliance is not yet configured, it redirects you to the `https://On-Prem-Appliance-IP-Address/ui/portal/initial-config` page.
  2. In the **VCDA Appliance Password** window, change the initial **root** user password set during the OVA deployment.
    - a) Enter the initial **root** user password as configured during the OVA deployment.
    - b) Enter and confirm a new password.
 

The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

      - At least one lowercase letter.
      - At least one uppercase letter.
      - At least one number.
      - At least one special character, such as: & # % .
    - c) After entering and confirming the new password, click **Apply**.
 

The **Getting Started** page opens.
  3. Click the **Run the initial setup wizard** link.
  4. To pair the On-Premises to Cloud Director Replication Appliance with VMware Cloud Director Availability in VMware Cloud on AWS, complete the **Initial Setup** wizard.
    - a) On the **Lookup Service Details** page, enter the local vCenter Server Lookup service and its user credentials, and click **Next**.

Lookup Service Address	Enter the IP address of the local vCenter Server Lookup service in the on-premises data center and to autocomplete the address as <code>https://Lookup-Service-IP-Address:443/lookup-service/sdk</code> , press Tab.
SSO Admin Username	Enter a local user with administrative privileges in the on-premises single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
Password	Enter the password for the administrative user.

Verify the thumbprints and accept the SSL certificates of the on-premises vCenter Server Lookup service.

- b) On the **Site Details** page, enter a name for this on-premises site and click **Next**.

Site Name	Enter a site name for this On-Premises to Cloud Director Replication Appliance.  <b>IMPORTANT</b> The site name is used as an identifier of this on-premises appliance instance and cannot be changed later.
Description	Optionally, enter a description for this site.

- c) On the **Cloud Details** page, pair the on-premises VMware Cloud Director Availability appliance and the VMware Cloud Director Availability in VMware Cloud on AWS.

Service Endpoint address	Enter the public IP address of the Public Service Endpoint of the VMware Cloud Director Availability in VMware Cloud on AWS as supplied by the service provider.
Organization Admin	Enter the <b>organization administrator</b> user of the Cloud Director instance, for example <code>admin@org</code> .
Organization Password	Enter the password for the <b>organization administrator</b> user.
Allow Access from Cloud	Select <b>Allow Access from Cloud</b> . By selecting this option, you allow the cloud provider and the organization administrators without authenticating to the on-premises site to discover on-premises workloads and replicate them to the cloud.

If the VMware Cloud Director Availability cloud site in VMware Cloud on AWS does not use a valid CA-signed certificate, verify the thumbprint and accept the SSL certificate of the Tunnel ServicePublic Service Endpoint at the VMware Cloud Director Availability in VMware Cloud on AWS.

- d) On the **Ready to complete** page, select **Configure local placement now** and click **Finish**.

The On-Premises to Cloud Director Replication Appliance is paired with VMware Cloud Director Availability in VMware Cloud on AWS.

5. To configure the On-Premises to Cloud Director Replication Appliance placement of virtual machines, complete the **Configure Placement** wizard.
- On the **VM Folder** page, browse the location for the recovered virtual machines and click **Next**.
  - On the **Compute Resource** page, browse the destination compute resource for the recovered virtual machines and click **Next**.
  - On the **Default Network** page, browse the network to connect the network interfaces of the virtual machines to after failover and click **Next**.
  - On the **Datastore** page, browse where to store the replicated virtual machines and disk files and click **Next**.
  - On the **Ready To Complete** page, verify the selected configuration and click **Finish**.

The On-Premises to Cloud Director Replication Appliance is configured and paired with VMware Cloud on AWS.

You can now create migrations and migrate workloads from this paired on-premises site to VMware Cloud on AWS. These migrations to VMware Cloud Director service follow the same configuration as the migrations to VMware Cloud Director. For information about creating a migration and migrating the workload, see [Create a Migration](#) and [Perform a Migrate Task](#) in the *User Guide*.

## Pair VMware Cloud Director Cloud Sites

To support migrations from private cloud sites running VMware Cloud Director to VMware Cloud Director service, in the private cloud deploy or upgrade to VMware Cloud Director Availability 4.2, pair the existing instance of VMware Cloud Director Availability operating in this private cloud and enable the VMC data engine.

- Verify that VMware Cloud Director Availability 4.2 is deployed in the private cloud site.
- **IMPORTANT**  
Verify that before pairing a private cloud site, the Public Service Endpoint *public-IP-address* of the Tunnel Appliance in the private cloud site is added as trusted in both the management and in the compute groups in the VMware Cloud on AWS SDDC. For information about adding the IP address in the trusted inventory groups, see [Prepare the SDDC in VMware Cloud on AWS for deployment](#).
- Verify that VMware Cloud Director Availability configuration in the VMware Cloud on AWS environment is complete. For more information, see [Configure VMware Cloud Director Availability in VMware Cloud on AWS](#).

In addition to migrating workloads from on-premises sites to VMware Cloud on AWS, to perform migrations from VMware Cloud Director cloud sites, also called private cloud sites, first pair then configure them with the VMC data engine.

1. Pair the private cloud site. For information about the pairing see [Managing Connections Between Cloud Sites](#) and [Pair Cloud Sites](#) in the *Administration Guide*.

You established trust between VMware Cloud Director Availability in VMware Cloud on AWS and the paired private cloud site.

2. To enable migrations to VMware Cloud on AWS from the paired private cloud site, in VMware Cloud Director Availability in the private cloud site select the VMC data engine.
  - a) In the left pane, under **Configuration** click **Settings**.
  - b) Under **Site settings**, next to **Data engine**, click **Edit**.
  - c) In the **Data engine** window, select **VMC** and click **Apply**.

### NOTE

The existing replications from the private cloud site can continue operating when both the classic and the VMC data engines are selected.

If VMware Cloud Director Availability is only paired with VMware Cloud on AWS and not paired with private cloud sites, do not enable the **Classic** engine.

The private cloud site is paired and prepared to migrate workloads to the VMware Cloud on AWS environment.

You can now create migrations and migrate workloads from the paired private cloud site to VMware Cloud on AWS. These migrations to VMware Cloud Director service follow the same configuration as migrations to VMware Cloud Director. For information about creating a migration and migrating the workload, see [Create a Migration](#) and [Perform a Migrate Task](#) in the *User Guide*.

---

## Post-configure the SDDC networking in VMware Cloud on AWS

To allow access to the management interfaces of the Manager Service, the Replicator Service instances and the Tunnel Service in VMware Cloud on AWS for performing administrative operations like certificate replacement, post-configure the network settings of the SDDC for the additional access to these three types of management interfaces.

- Verify that the SDDC network is already configured for VMware Cloud Director Availability pairing. For information about the required steps, see [Configure the SDDC network for pairing VMware Cloud Director Availability in VMware Cloud on AWS](#).
- Verify that VMware Cloud Director Availability 4.2 or later is deployed in VMware Cloud on AWS. For more information, see [Deploy VMware Cloud Director Availability in the SDDC](#).

By default, the access limited in VMware Cloud on AWS and the public IP addresses of all the cloud appliances of VMware Cloud Director Availability must be explicitly allowed for performing administrative operations.

VMware Cloud Director Availability appliances in VMware Cloud on AWS provide three types of management interfaces for performing administrative tasks like certificate replacement and others. To allow these management interfaces when configuring the necessary NAT rules, you explicitly define them since the three interfaces internally use non-standard

HTTPS ports. These three services in conjunction with the following three NAT rules and a firewall rule translate and allow the network traffic coming to the public IP addresses of the appliances on the external port 443/TCP:

- Towards the Cloud Director Replication Management Appliance, internally on port 8044/TCP for the management interface of the Manager Service.
- Towards all Replicator Appliance instances, internally on port 8043/TCP for the management interfaces of the Replicator Service instances.
- Towards the Tunnel Appliance, internally on port 8047/TCP for the management interface of the Tunnel Service.

1. Log in to VMware Cloud on AWS at <https://vmc.vmware.com>.
2. Add three new inventory SDDC services, for the management interfaces of the Manager Service, Replicator Service, and the Tunnel Service.
  - a) In the VMC console, in the left pane click **SDDCs**.
  - b) Under the SDDC click **View Details** and click the **Networking & Security** tab.
  - c) In the left pane under the **Inventory** section, click **Services**.
 

Repeat the following steps three times:

    - Add an inventory service for the Manager Service of the Cloud Director Replication Management Appliance.
    - Add another inventory service for the Replicator Service of the Replicator Appliance.
    - Add another inventory service for the Tunnel Service of the Tunnel Appliance.
  - d) To add an inventory SDDC service, click **Add Service**.
  - e) Enter a name and optionally a description for each service.
  - f) For each service, in the Service Entries column, click the **Set Service Entries** link.
  - g) For each service, in the **Set Service Entries** window, from the **Type** drop down menu select **Layer 3 and above**.
  - h) For each service, on the **Port-Protocol** tab click **Add Service Entry**, enter the details from the respective column, and click **Apply**.

Option	Manager Service Inventory Service	Replicator Service Inventory Service	Tunnel Service Inventory Service
Name	Enter a name for the management interface service entry of the Cloud Director Replication Management Appliance Manager Service. For example, enter <i>VCDA-Manager-Service-Management</i> .	Enter a name for the management interface service entry of the Replicator Appliance Replicator Service. For example, enter <i>VCDA-Replicator-Service-Management</i> .	Enter a name for the management interface service entry of the Tunnel Appliance Tunnel Service. For example, enter <i>VCDA-Tunnel-Service-Management</i> .
Service Type	Select <b>TCP</b> .	Select <b>TCP</b> .	Select <b>TCP</b> .
Additional Properties	Leave the <b>Source Ports</b> text box blank.	Leave the <b>Source Ports</b> text box blank.	Leave the <b>Source Ports</b> text box blank.

Option	Manager Service Inventory Service	Replicator Service Inventory Service	Tunnel Service Inventory Service
	To access the management interface of the Manager Service in the Cloud Director Replication Management Appliance in the <b>Destination Ports</b> text box, in enter port 8044.	To access the management interface of the Replicator Service in the Replicator Appliance, in the <b>Destination Ports</b> text box enter port 8043.	To access the management interface of the Tunnel Service in the Tunnel Appliance, in the <b>Destination Ports</b> text box enter port 8047.

i) To save each inventory service, click **Save**.

On the **Services** page, the three new services show:

Name	Service Entries
<i>VCDA-Manager-Service-Management</i>	TCP (Source: Any   Destination: <b>8044</b> )
<i>VCDA-Replicator-Service-Management</i>	TCP (Source: Any   Destination: <b>8043</b> )
<i>VCDA-Tunnel-Service-Management</i>	TCP (Source: Any   Destination: <b>8047</b> )

3. To later use in NAT rules, request new public SDDC IP addresses for each of the three types of management interfaces.

- Request a public IP address to access the management interface of the Manager Service in the Cloud Director Replication Management Appliance.
- Request multiple public IP addresses to access the management interface of each Replicator Service in the Replicator Appliance instances.
- Request a public IP address to access the management interface of the Tunnel Service in the Tunnel Appliance.

a) On the **Networking & Security** tab, in the left pane under the **System** section click **Public IPs**.

b) To request a public IP address for the Manager Service, click **Request New IP**, enter a note, and click **Save**.

For example, as a note enter *VCDA-Manager-Public-Management-IP-address*.

Repeat the following step for each instance of the Replicator Service deployed in the SDDC:

c) To request a public IP address for each Replicator Service, click **Request New IP**, enter a note and click **Save**.

For example, as a note enter *VCDA-Replicator-Public-Management-IP-address*. For more Replicator Service instances, for each requested public IP address enter *VCDA-Replicator-X-Public-Management-IP-address*, where *X* marks each instance.

d) To request a public IP address for the Tunnel Service, click **Request New IP**, enter a note and click **Save**.

For example, as a note enter *VCDA-Tunnel-Public-Management-IP-address*.

4. To forward the incoming network traffic to the correct cloud appliances and ports, add new NAT rules.

a) On the **Networking & Security** tab, in the left pane under the **Network** section click **NAT**.

Repeat the following step three times:

- Add a NAT rule for the management interface of the Manager Service in the Cloud Director Replication Management Appliance.
- Add another NAT rule for the management interface of the Replicator Service in the Replicator Appliance. For each additional Replicator Service instance, add another NAT rule.
- Add another NAT rule for the management interface of the Tunnel Service in the Tunnel Appliance.

b) To add a NAT rule, click **Add NAT Rule**, configure the following settings then click **Save**.

Option	Manager Service NAT	Replicator Service NAT	Tunnel Service NAT
Name	Enter a name for the NAT rule for the management interface of the Cloud Director Replication Management ApplianceManager Service. For example, enter <i>VCDA Replication Management NAT</i> .	Enter a name for the NAT rule for the management interface of the Replicator ApplianceReplicator Service. For example, enter <i>VCDA Replicator NAT</i> . For more Replicator Service instances, for each NAT rule enter <i>VCDA Replicator X NAT</i> , where <i>x</i> marks each instance.	Enter a name for the NAT rule for the management interface of the Tunnel ApplianceTunnel Service. For example, enter <i>VCDA Replication Management NAT</i> .
Public IP	Select the <i>VCDA-Manager-Public-Management-IP-address</i> .	Select the <i>VCDA-Replicator-Public-Management-IP-address</i> .	Select the <i>VCDA-Tunnel-Public-Management-IP-address</i> .
Service	Select the inventory service for the Cloud Director Replication Management ApplianceManager Service. For example, select <i>VCDA-Manager-Service-Management</i> .	Select the inventory service for the Replicator ApplianceReplicator Service. For example, select <i>VCDA-Replicator-Service-Management</i> .	Select the inventory service for the Tunnel ApplianceTunnel Service. For example, select <i>VCDA-Tunnel-Service-Management</i> .
Public Port	Enter port 443.	Enter port 443.	Enter port 443.
Internal IP	Enter the <i>private-IP-addresses</i> of the Cloud Director Replication Management Appliance.	Enter all <i>private-IP-addresses</i> of the Replicator Appliance instances.	Enter the <i>private-IP-address</i> of the Tunnel Appliance.
Internal Port	8044 (non-editable)	8043 (non-editable)	8047 (non-editable)
Firewall	Match Internal Address	Match Internal Address	Match Internal Address

5. To allow accessing the VMware Cloud Director Availability management interfaces from the trusted compute sources, add the three new services and destinations in the inbound compute firewall rule.

The compute rule *VCDA Management from Trusted Compute Sources Rule* is created first in [Configure the network of the SDDC in VMware Cloud on AWS](#).

- On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.
- On the **Compute Gateway** tab, click the already created *VCDA Manager from Trusted Compute Sources Rule*.
- Configure the compute firewall rule then click **Apply** when prompted.

Option	Compute Firewall Rule
Name	<i>VCDA Management from Trusted Compute Sources Rule</i> .
Sources	<i>Trusted Compute Sources Group</i> .
Destinations	Click <b>Any</b> . In the <b>Set Destination</b> window, select all the compute groups of the VMware Cloud Director Availability appliances and click <b>Apply</b> . For example, select all three: <ul style="list-style-type: none"> <li><i>VCDA Manager Compute Group</i></li> <li><i>VCDA Replicators Compute Group</i></li> <li><i>VCDA Tunnel Compute Group</i></li> </ul>
Services	Click <b>Any</b> . In the <b>Set Services</b> window, select the three newly created inventory services in addition to the <i>VCDA-Cloud-Service-Management TCP (Source: Any   Destination: 8046)</i> . For example, select additionally: <ul style="list-style-type: none"> <li><i>VCDA-Manager-Service-Management TCP (Source: Any   Destination: 8044)</i></li> <li><i>VCDA-Replicator-Service-Management TCP (Source: Any   Destination: 8043)</i></li> <li><i>VCDA-Tunnel-Service-Management TCP (Source: Any   Destination: 8047)</i></li> </ul> When selected, all four management interface services are now present: Destination: 8046, Destination: 8044, Destination: 8043, and Destination: 8047.
Applied To	All Uplinks
Action	Allow

- After modifying the compute gateway firewall rule, click **Publish**.

The compute firewall rule allows access to the four types of management interfaces of all services of VMware Cloud Director Availability:

- Cloud Service
- Manager Service
- Each Replicator Service instance
- Tunnel Service

The SDDC configuration in VMware Cloud on AWS is complete and ready for administrative operations of the VMware Cloud Director Availability services.

You can now perform administrative tasks for each VMware Cloud Director Availability service. For more information, see the *Administration Guide* for the version of VMware Cloud Director Availability deployed in the SDDC.

---

## VMware Cloud Director Availability Cold Migration

---

Some workloads present challenge for a live migration, like the workload being a physical machine, running on a non-VMware hypervisor, or on a VMware hypervisor where the user lacks the necessary privileges to run the solution. For such workloads you can use the VMware Cloud Director Availability cold migration.

VMware Cloud Director Availability 4.7 introduces the option for a cold migration of the workload to transfer from non-VMware environments, such as KVM, Hyper-V, physical hosts, and others, to a Cloud Director site. The cold migration means that the source machine is powered off and rebooted into an ISO image. As a caveat, workloads to-be migrated which require 24/7 uptime and cannot be powered off cannot use cold migration.

The ISO image for cold migration has the following requirements.

- Minimum 768 MiB of memory (RAM) or more.
- Support for x86-64 architecture from the hypervisor and the CPUs for the physical workloads.

### **Workflow Overview**

1. As **aprovider**, configure a VMware Cloud Director Availability 4.7 site on the destination – either by installing a fresh instance, or by upgrading an existing site. For more information, see [Installing and configuring the appliances in the Cloud Director site](#) or [Upgrading in the Cloud Director site](#).
2. As **aprovider**, activate the cold migration.  
Perform the remaining steps as either **aprovider** or as **atenant** user.
3. Create a cold migration template.
4. Download the ISO image, generated as part of the cold migration template.
5. Power-off the source workload, attach the ISO image to the virtual machine then boot from the ISO image.
6. Once the virtual machine is booted from the ISO image, a new migration appears on the destination site.
7. Depending on the template settings, the migration can either automatically begin or can require an explicit confirmation from the user on the destination site.
8. Once the migration finishes, power-off the original workload manually.

As per steps 4-6, the cold migration requires that the original workload is powered off and booted into a special VMware Cloud Director Availability-generated ISO image that contains the necessary VMware Cloud Director Availability services for the migration. Specifically, the ISO image is based on Debian 12 and contains the VMware Cloud Director Availability Cold Migration Agent (h4dm-agent) that drives the migration process:

- Discover the following hardware information.
  - CPU sockets and cores per socket
  - Physical memory
  - Number of NICs
- Mount all disks into read-only mode.

### **NOTE**

The agent does not make any changes to the underlying disks.

- Discover the guest operating system (OS) type, version, and the computer name for Windows and Linux guest OS. An exception are Linux guests that use Logical Volume Management (LVM) or disk encryption. In case the guest OS cannot be recognized, VMware Cloud Director Availability uses the source workload IP address as the computer name.
- Establish a network connection to VMware Cloud Director Availability.
- Copy each disk over the network to the destination VMware Cloud Director Availability site.

- Create, then optionally power-on the destination virtual machine. Once all of the disks finish copying, a new virtual machine is created in the underlying vCenter Server instance. Then it is imported into the VMware Cloud Director instance and becomes available to the tenant.

#### NOTE

- The ISO image agent (h4dm-agent) is stateless - all of the information that it needs to perform the migration is stored in-memory. This means that the disk copying must happen in a single run; you cannot do a partial sync, power off or reboot, and then resume from the last copied block. Each (re-)boot creates a new migration instance and begins synchronization from scratch.
- If the guest OS is encrypted, for example, by technologies such as `dm-crypt` in Linux and BitLocker in Windows, the disk content is copied as-is, in its encrypted form. Whether it can be decrypted on the destination side, depends on the used encryption technology:
  - If the decryption key is a user-provided password, the decryption is likely to succeed.
  - If the disk encryption key is stored in a Trusted Platform Module (TPM), the data remains unusable in the destination.

## Activate the cold migrations

As a **provider**, first prepare each Replicator Appliance instance with the necessary ISO image for cold migrations. Once ready with all instances, activate the cold migration for all the VMware Cloud Director Availability tenants.

#### NOTE

By default, to preserve disk space on the appliances, the Replicator Appliance does not contain the ISO image with the VMware Cloud Director Availability Cold Migration Agent (h4dm-agent). To obtain it, all Replicator Appliance instances must either have Internet access or you must manually copy-over the ISO image to each instance.

However, not all Replicator Appliance instances handle the incoming cold migration. When activating the cold migration, VMware Cloud Director Availability nominates a random Replicator Appliance instance to handle all cold migrations. In case of failure of this Replicator Appliance instance, all on-going cold migrations are lost.

To nominate another Replicator Appliance instance that is still operational, first deactivate, then activate the cold migration again. All workloads with an on-going migration require starting a new migration by restarting the source machine, except for those workloads that were already successfully migrated before the failure of the previously nominated Replicator Appliance instance. Any successfully-completed migrations, performed by the previously nominated Replicator Appliance instance, no longer show in VMware Cloud Director Availability, but the respective migrated virtual machines remain fully-functional and visible in VMware Cloud Director.

1. Prepare all Replicator Appliance instances for handling the incoming cold migrations.
  - When the Replicator Appliance instances are not connected to the Internet, download the following ISO image file: <https://packages.vmware.com/vcav/cold-mig/4.7.1-d094a2c9/live-image-amd64.hybrid.iso>
  - Once the image downloads, copy it to the appliance by using `scp` or `WinSCP`. As a destination use: `/opt/vmware/h4/h4dm/iso/live-image-amd64.hybrid.iso`. Set the permissions to 400 (read-only access to the owner) and set the owner and group to "h4dm".
  - Alternatively, when the Replicator Appliance instances have Internet access, the ISO image is downloaded to the nominated one automatically, once you activate the cold migration in step 3.

2. Log in to the management interface of the Cloud Director Replication Management Appliance.
  - a) In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
  - b) Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
  - c) Click **Login**.
3. Activate the cold migrations.
  - a) In the left pane under **Settings**, next to **Cold Migrations** click **Edit**.
  - b) In the **Cold Migrations** window, click **Activate**.

Once you activate the cold migration, two new sections appear in the left pane and remain visible to each **tenant**:

  - **Cold Migration Templates**
  - **Cold Migrations**

This VMware Cloud Director Availability site is ready to receive replications from workloads that are booted with the ISO image.

You can now cold migrate the workloads. For more information, see [Cold migrate](#).

## Cold migrate

As either a **provider** or a **tenant**, perform cold migrate in VMware Cloud Director Availability.

- Verify that the respective replication policy for the destination organization allows incoming migrations and also ensure that the **Maximum Incoming Replications** quota for the organization is not exceeded for the cold migrations to operate.
- Verify that VMware Cloud Director Availability 4.7 is operational in the destination site.
- Verify that all Replicator Appliance instances are prepared with the cold migration ISO image. For more information, see [Activate the cold migrations](#).

1. Access VMware Cloud Director Availability as either a **provider** or a **tenant**.
  - Log in to VMware Cloud Director Availability.
  - Alternatively, log in to VMware Cloud Director and open the **Availability** plug-in.
2. Create a new cold migration template.
  - a) In the left pane, click **Cold Migration Templates**.
  - b) Click **New**.
 

The **Create Cold Migration Template** wizard opens.
  - c) On the **Destination settings** page, enter the following settings.

Name	Enter a name for the cold migration template.
Compression	Whether the disk content must be compressed prior to sending it over the network. As a recommendation, enable compression on network links below 1 Gbit/s. For links with bandwidth higher than that, deactivating the compression may result in faster migrations.

Trigger sync	Whether the data synchronization occurs immediately and automatically after booting the source workload from the ISO image, or alternatively after clicking <b>Migrate</b> in the user interface. Selecting manual sync can provide an additional layer of security, as the blue console screen on the source workload shows a confirmation token. The user then finds the migration in the user interface, clicks Migrate and compares the token in the confirmation window with the token on the blue console screen. Alternatively, selecting automatic skips the confirmation step and commences the sync immediately - suitable for automation purposes.
Power on	Whether the recovered virtual machine powers on after the migration finishes.
Max workloads	The number of cold migrations that are allowed as part of this template, or how many times can the generated ISO be used. Migrations that are in-progress and failed migrations count against this quota.
ISO expiration date	A source workload booted from an expired ISO cannot to connect to the destination site. No cold migrations can be created off of an expired ISO.

d) On the **Destination VDC and Storage Policy** page, select:

- The virtual data center to use for the recovery virtual machine.
- The storage policy to use for the recovery virtual machine.

e) On the **VDC Policy Settings** page, select

- The **VM placement policy** to use for the recovery virtual machine.
- The **VM sizing policy** to use for the recovery virtual machine.

f) On the **Ready To Complete** page, see an overview of the previously selected settings and optionally, download the ISO image.

- To trigger the download immediately directly from the **Ready To Complete** page, click **Download ISO**.
- Alternatively, to download the ISO later, in the left pane click **Cold Migration Templates** then select a template and click **Download ISO**.

Once downloaded, you distribute the ISO image and make it available to the hypervisor or the physical machine.

- Once the ISO image is downloaded locally, the user performing the migration must first copy it to the storage of the non-VMware hypervisor, then attach it to the to-be migrated source workload machine and reboot it.

#### NOTE

The source workload machine must be explicitly instructed to boot from the attached ISO image: either through its hypervisor, or alternatively, through its BIOS or UEFI.

- Once the source workload machine boots, the migration starts automatically if the **On boot** option is selected when creating the template. Alternatively, the user performing the migration must access VMware Cloud Director Availability,

as per step 1, then in the left pane click **Cold Migrations**, select the migration and click **Migrate**. To find out which is the migration:

- If the h4dm-agent can determine the hostname of the source workload, filter the rows by the Machine name column.
  - If the h4dm-agent cannot determine the hostname, the Machine name column just displays the IP address, as shown on the blue console screen.
  - Irrespective of the machine name, the h4dm-agent always generates a unique 8-letter confirmation token, shown on the blue console screen, for example, *AB12-CD34*.
- Once all disks are copied to the destination, a new virtual machine is created in the underlying vCenter Server instance. Then it is imported into VMware Cloud Director.

#### IMPORTANT

If the source workload machine uses **IDE** controller type for its boot disk, prior to booting Windows-based guest operating system (OS) on the destination:

1. Power-off the destination virtual machine.
2. Attach the boot disk to the **IDE** controller, for example, attach it to **IDE(0,0)**.
  - If no snapshots exist, remove the boot disk from the destination virtual machine without deleting the boot disk, then attach it to the **IDE** controller.
  - If snapshots exist, attempting to delete the boot disk shows the error message `Invalid configuration for device '0'. Cannot remove virtual disk from the virtual machine because it or one of its parent disks is part of a snapshot of the virtual machine.` As a workaround, in the **Edit Settings** window, under **Hard disk 1 > Virtual Device Node** select **IDE 0** when the machine has snapshots.
3. Power-on the destination virtual machine. After its first successful boot, the Windows **Administrator** installs all necessary drivers and tools.

For Linux-based guest OS, once migrated, perform additional steps for reconstructing its initial ramdisk. For more information, see [Post cold migrate for Linux-based machines](#).

## Post cold migrate

Once a destination virtual machine is created in the inventories of vCenter Server and VMware Cloud Director, you must perform additional steps, depending on the guest operating system.

### Post cold migrate for Windows-based machines

Once a destination virtual machine that runs Windows operating system is created, verify that VMware Tools device drivers are installed.

By running VMware Tools on the machine, you ensure that all devices work properly after the migration. For more information about VMware Tools, see the [official documentation](#).

### Post cold migrate for Linux-based machines

Once a destination virtual machine that runs a Linux operating system is created, you must reconstruct the initial ramdisk, repair missing drivers, and verify that Open VM Tools device drivers are installed on the VM.

- Verify that the workload is successfully cold migrated to the destination site.

To alleviate any missing drivers on your Linux operating system, distributions typically include a bootloader entry which contains all drivers usually called *rescue mode*, where the exact name depends on the specific distribution. The user must boot into this mode then follow the distribution-specific instructions to construct a new initial ramdisk.

After a cold migration, Linux-based machines may need to have their initial ramdisk reconstructed. This is needed so that the ESXi paravirtual drivers are included in the initial ramdisk. This significantly improves the I/O throughput of the migrated VM. The procedure for regenerating the ramdisk is distribution-specific.

By running Open VM Tools on your Linux-based machine, you ensure that all devices work properly after the migration. For more information about Open VM Tools, see the [official documentation](#).

1. Boot the machine into the bootloader that contains all drivers, typically `rescue mode`.
2. Log in as the **root** user.
3. Construct a new initial ramdisk, depending the specific distribution.
  - For distributions that use `dracut`, for example: Red Hat derivatives such as Fedora Linux, Red Hat Enterprise Linux, OpenSUSE, SUSE Linux Enterprise Server, and others, run the following command:
 

```
dracut --regenerate-all --force
```
  - Alternatively, for distributions that use `mkinitcpio`, for example: Arch Linux and its derivatives, run the following command:
 

```
mkinitcpio --allpresets
```
4. After you reconstruct the initial ramdisk, reboot the machine.
5. When the Linux operating system starts, verify that Open VM Tools device drivers are installed.

## Cold migrate support matrix

See a matrix of the supported operating systems and hypervisors or a physical machine.

### Support Matrix

#### NOTE

- `fallback initramfs` and `rescue mode` are standard bootloader options for the target Linux distribution. For information about the additional steps needed for Linux-based machines, see [Post cold migrate for Linux-based machines](#). If such options are not present in your Linux operating system, refer to your distribution's documentation.
- Windows Server 2019 and earlier versions may be unable to connect to a network. For information about the additional steps needed for Windows-based machines, see [Post cold migrate for Windows-based machines](#).
- To successfully start some Windows operating systems after the cold migration, you may need to manually configure their disk controllers.

	ESXi	KVM	Hyper-V	Physical machine
Arch Linux	#	# <code>fallback initramfs</code>	#	Not tested
CentOS 7.9	#	# <code>rescue mode</code>	# <code>rescue mode</code>	Not tested
Fedora 38	#	# <code>rescue mode</code>	# <code>rescue mode</code>	# <code>rescue mode</code>
RHEL 8	#	# <code>rescue mode</code>	# <code>rescue mode</code>	Not tested
Rocky 9.2	#	# <code>rescue mode</code>	# <code>rescue mode</code>	Not tested
Ubuntu Server 22.04	#	#	#	Not tested
Windows Server 2003	#	#	#	Not tested
Windows Server 2008	#	#	# OS starts with Windows Error Recovery screen	Not tested
Windows Server 2012r2	#	#	#	Not tested
Windows Server 2016	#	#	#	Not tested
Windows Server 2019	#	#	#	Not tested

---

	<b>ESXi</b>	<b>KVM</b>	<b>Hyper-V</b>	<b>Physical machine</b>
Windows Server 2022	#	#	#	Not tested

# VMware Cloud Director Availability in Azure VMware Solution

VMware Cloud Director Availability can protect and migrate workloads both to and from the VMware Cloud Director™ service hosted at VMware Cloud™ on Azure VMware Solution.

## **Disaster Recovery and Migration with VMWare Cloud Director Availability**

VMware Cloud Director Availability™ is a Disaster Recovery-as-a-Service (DRaaS) solution. Between providers' clouds or on-premises, with asynchronous replications, VMware Cloud Director Availability protects, migrates, fails over, and reverses failovers of vApps and virtual machines. VMware Cloud Director Availability is available through the Partner Connect Program.

VMware Cloud Director Availability introduces a unified architecture for the disaster recovery protection and migration of VMware vSphere® workloads. In both sites with VMware Cloud Director Availability, formerly known as vCloud Availability, the providers and their tenants can protect and migrate vApps and virtual machines:

- Between an on-premises vCenter Server site and a multi-tenant provider cloud site with VMware Cloud Director™.
- Between multi-tenant provider cloud sites with VMware Cloud Director or/and VMware Cloud Director.

All supported versions of VMware Cloud Director Availability can protect or migrate vSphere workloads with a private Cloud Director site by using the native integration with VMware Cloud Director and VMware vCenter Server®.

## **Azure VMware Solution Design Implications**

To address the design and security implications of the Azure VMware Solution private cloud, VMware Cloud Director Availability 4.7 and later introduces an automation providing capabilities that usually require elevated privileges to install, configure and perform various Day 2 operations, for example, Health Check, Upgrade, Scale, Maintenance Mode, and others, by implementing a suite of PowerShell cmdlets bundled in a suite, also known as Run command for performing any administrative actions with the VMware Cloud Director Availability instance in Azure VMware Solution.

For information about using the Run commands, see [Run Command in Azure VMware Solution](#) in the *Azure VMware Solution* documentation.

For information about the replications use cases and their cross-site support, see [Replicating workloads](#) in the *User Guide*.

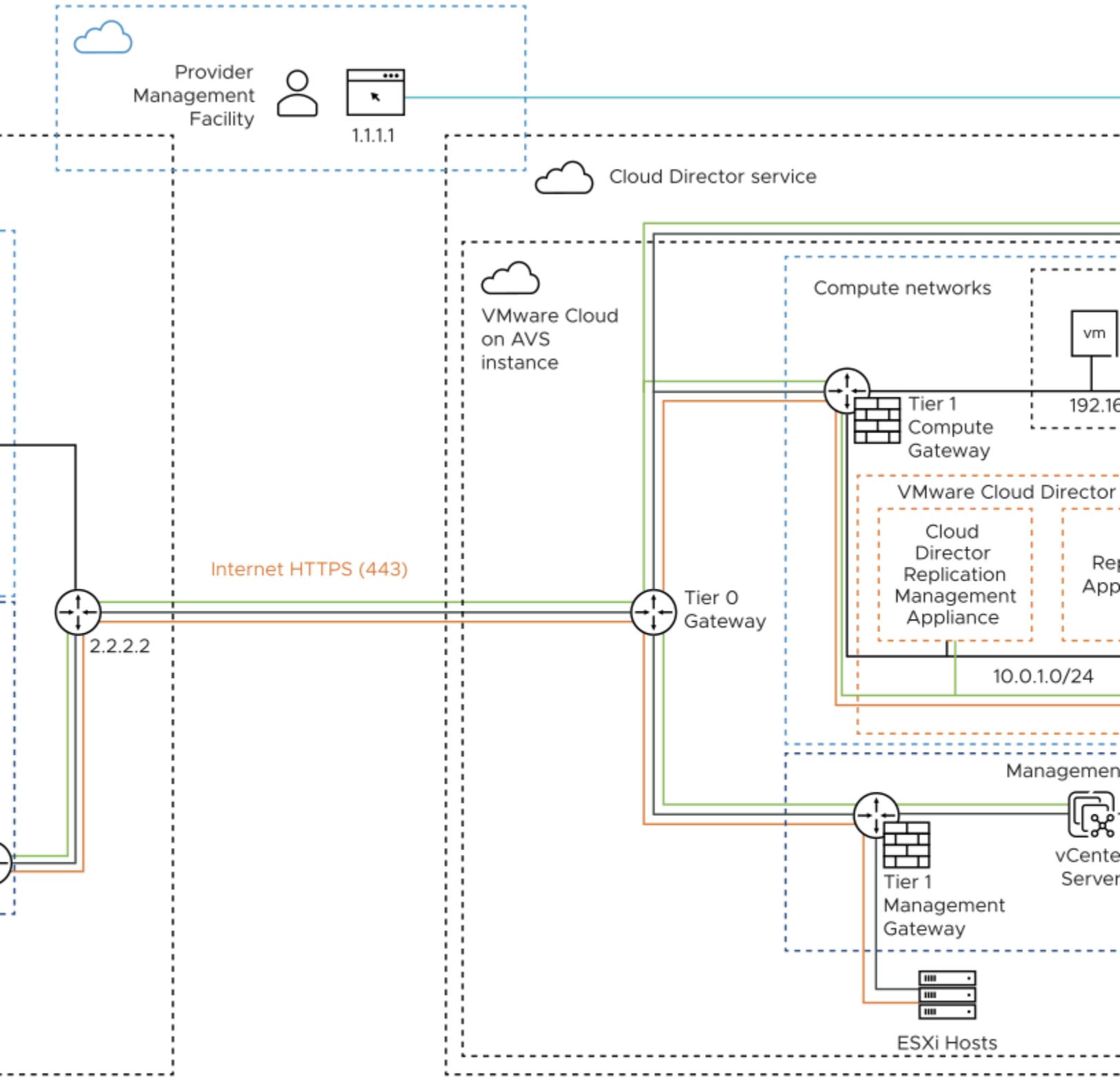
## **Disaster Recovery and Migration with VMware Cloud Director service**

Both the providers and their tenants, can use the existing disaster recovery and migration flow and replicate their workloads to VMware Cloud Director service in Azure VMware Solution after following this *VMware Cloud Director Availability in Azure VMware Solution Guide*.

The VMware Cloud Director service pools the resources provided by the Software-Defined Data Center (SDDC) in Azure VMware Solution. The following diagrams provide an overview of VMware Cloud Director service after installing VMware Cloud Director Availability and pairing an Azure VMware Solution site with an on-premises site and or with a Cloud Director site, either backed by VMware Cloud Director or Cloud Director service.

## **Paired On-Premises Site with VMware Cloud Director Availability in Azure VMware Solution**

After pairing the On-Premises to Cloud Director Replication Appliance with VMware Cloud Director Availability in Azure VMware Solution, in the following architecture diagram the orange color shows the deployed on-premises and cloud appliances of VMware Cloud Director Availability in the VMware Cloud on Azure VMware Solution instance and the replication data traffic between the appliances, with all existing components in black:



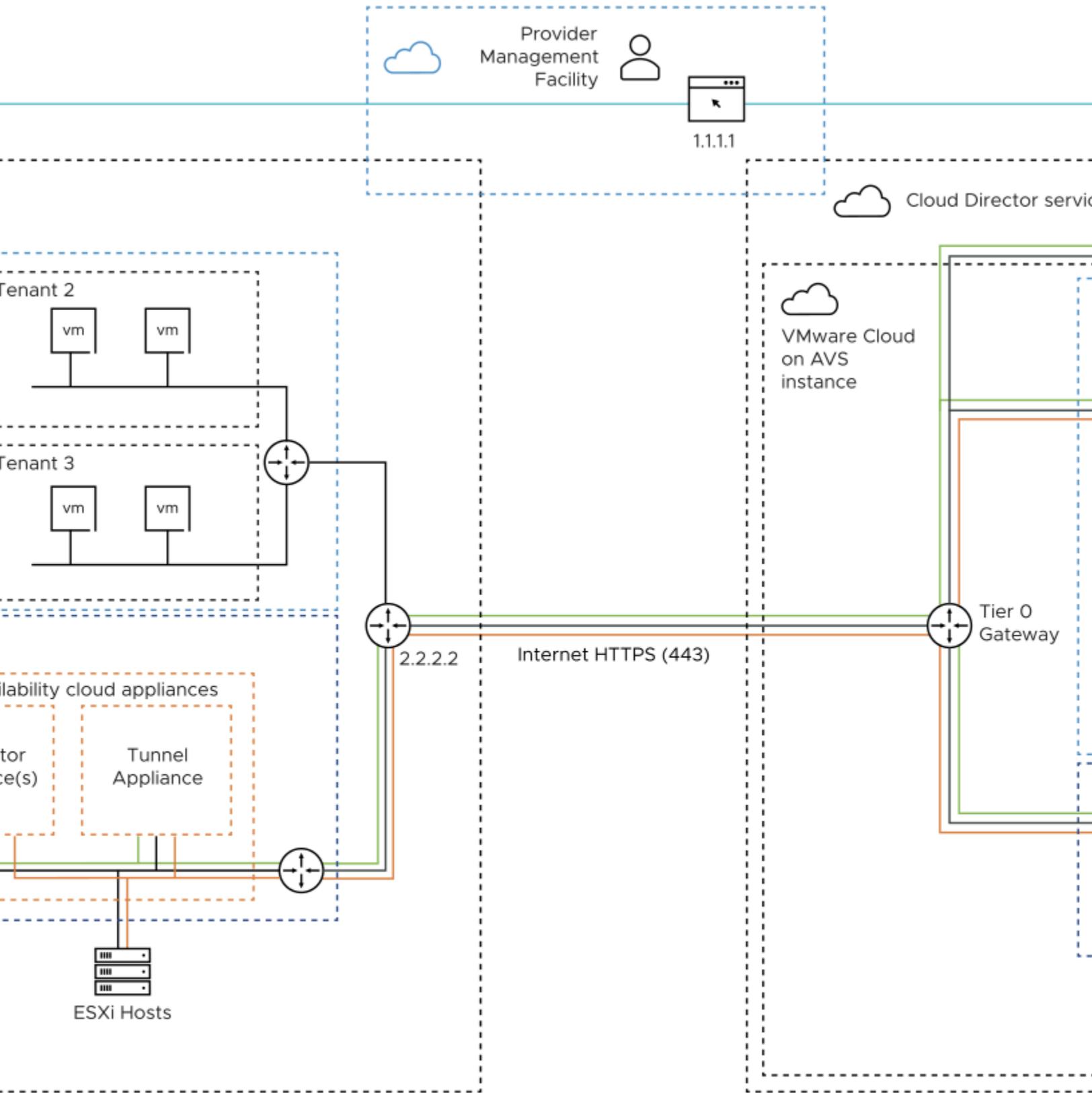
Availability replication data traffic  
Availability service management traffic  
Availability Plug-in administration traffic

**NOTE**

For simplicity, on the above diagram the two Replicator Appliance instances in the VMware Cloud on Azure VMware Solution instance are depicted as a single unit.

**Paired Cloud Site with VMware Cloud Director Availability in Azure VMware Solution**

After pairing a Cloud Director site with VMware Cloud Director Availability in Azure VMware Solution, in the following deployment diagram the orange color shows the deployed cloud appliances of VMware Cloud Director Availability in the VMware Cloud on Azure VMware Solution instance and the replication data traffic between them, with all existing components in black:



**NOTE**

For simplicity, on the above diagram the two Replicator Appliance instances in the VMware Cloud on Azure VMware Solution instance are depicted as a single unit.

**Overview of the Configuration**

VMware Cloud Director Availability resides in Azure VMware Solution private cloud SDDC.

Following access and privileges are required to deploy and configure the VMware Cloud Director Availability service:

- To access Azure VMware Solution private cloud portal with sufficient privileges for using the Azure VMware Solution service.
- To access the Cloud Director service with sufficient privileges for VMware Cloud Director Availability service.
- To access the management interface of VMware Cloud Director Availability for system and maintenance tasks.
- To access the Public Service Endpoint from external VMware Cloud Director Availability sites for pairing and migrations from these sites.

In Azure VMware Solution, the SDDC and VMware Cloud Director Availability must be prepared and configured in the following order. Procedure outline:

1. Prepare the Azure VMware Solution SDDC associated with Cloud Director service by creating the following objects.
  - a. A network segment, connecting all the cloud VMware Cloud Director Availability appliances.
  - b. Outbound internet connectivity to communicate with: VMware Cloud Director service, remote VMware Cloud Director Availability sites and the upgrade repository.
  - c. DNS zone with records for all the VMware Cloud Director Availability appliances.
  - d. DNS zone with forwarding for the public addresses supposed to be reached by VMware Cloud Director Availability outside of the local network segment.
  - e. Public IP and dNAT rule for the Public Service Endpoint of VMware Cloud Director Availability.
  - f. Initialize the Azure VMware Solution site for VMware Cloud Director Availability deployment. The Run command prepares the SDDC by creating a **service account** in vSphere with the corresponding attributes required by VMware Cloud Director Availability.
2. Install and configure VMware Cloud Director Availability instance in Azure VMware Solution SDDC by running the **Initialize-AVSSite** Run command to prepare the SDDC on Azure VMware Solution environment for VMware Cloud Director Availability installation. Once you obtain the required vSphere **service account, role** and **group**, generate password, run the **Install-VCDAAVS** Run command to provision a production-ready disaster recovery and migration service. For the detailed procedure, see *Install and Configure VMware Cloud Director Availability in the SDDC*.
3. Configure the Public Service Endpoint of VMware Cloud Director Availability for pairing with external VMware Cloud Director Availability sites by dNAT rule associating the external IP address with the internal VMware Cloud Director Availability endpoint running on the Tunnel Service port 8048.
4. After performing **Install-VCDAAVS** for the VMware Cloud Director Availability services, to validate that the setup is complete, open the management interface then verify the status of all services by clicking the **System health** page, where the entries show a green health state to indicate successfully configured services.
  - a. To log in to the management interface of the Cloud Director Replication Management Appliance, in a Web browser, go to either of the following addresses:
    - `https://VMware-Cloud-Director-Availability-Public-Service-Endpoint_Public_Address/ui/login`
    - `https://Cloud-Director-Replication-Management-Appliance-IP-Address/ui/login`
    - `https://Cloud-Director-service-Address/provider/plugins/Your-VCDA-Plugin-Id`
  - b. Enter the user name and password of a user with VMware Cloud Director **System** privileges then click **Login**.
5. Once the VMware Cloud Director Availability services are up and in a healthy state, you can use the management interface to proceed with the required management tasks. For information about performing administrative tasks

such as changes to the provisioned environment and routine administration and maintenance procedures, see [Administration in the Cloud Director site](#).

6. Pair with external VMware Cloud Director Availability sites.
  - a. Optionally, the tenants can configure and pair On-Premises to Cloud Director Replication Appliance instances with VMware Cloud Director Availability in Azure VMware Solution. For the detailed initial on-premises configuration and pairing procedure, see [Configure the On-Premises to Cloud Director Replication Appliance](#).
  - b. Optionally, pair VMware Cloud Director Availability in Azure VMware Solution with private Cloud Director sites. For the detailed pairing procedure, see [Pair two Cloud Director sites](#).

After completing all these steps, by using the existing disaster recovery and migration flow in VMware Cloud Director Availability the trusted, allowed, and paired providers and their trusted, allowed, and paired tenants can migrate workloads to and from VMware Cloud Director service in Azure VMware Solution.

- Get familiar with the VMware Cloud Director Availability Run command glossary intended to support you in the process of managing and maintaining the VMware Cloud Director Availability instance.
- Later, to allow access to perform administrative tasks like certificate replacement by using the three types of management interfaces of VMware Cloud Director Availability:
  - Add three inventory services for each management interface type: Replicator Service, Manager Service, and Tunnel Service
  - Add three NAT rules, with additional NAT rule for each Replicator Service instance.
  - Modify the existing compute gateway firewall rule that allows access from the trusted compute sources group and include the three additional services, for a total of four inventory services.

## Run command in Azure VMware Solution

In Azure VMware Solution, as a **provider**, run commands for installing or deleting a VMware Cloud Director Availability instance, for taking and deleting the appliances snapshots, repairing the Replicator Appliance or the vCenter Server Lookup service, or for resetting either the password of the service account or of the **root** user of the appliances.

- Verify that you can access the Microsoft Azure Portal by using an account with sufficient **privileges** for using the Azure VMware Solution service.
- Verify that the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` version 4.7 or later is uploaded under the correct datastore.
- Verify that the subnet, DNS zone and records for the VMware Cloud Director Availability appliances are configured.
- Verify that the subnet has outbound Internet connectivity to communicate with: VMware Cloud Director service, remote VMware Cloud Director Availability sites, and the upgrade repository.
- Verify that the DNS zone has forwarding for the public IP addresses supposed to be reached by VMware Cloud Director Availability outside of the local network segment.
- Verify that the Azure VMware Solution private cloud is configured.
- Verify that the Cloud Director service is associated, and the Transport Proxy is configured with the Azure VMware Solution private cloud SDDC.

Run command for performing any administrative actions with the VMware Cloud Director Availability instance in Azure VMware Solution.

For information about using run command, see [Run Command in Azure VMware Solution](#) in the *Azure VMware Solution* documentation.

1. Run command for VMware Cloud Director Availability in Azure VMware Solution.
  - a) Log in to the Microsoft Azure Portal at <https://portal.azure.com/>.
  - b) In the left pane, under **Operations** click **Run command**.
  - c) Under the **Packages** tab, expand the **VMware.VCDA.AVS** PowerShell Module for Managing VMware Cloud Director Availability on Azure VMware Solution.
2. Select a command from the [VMware Cloud Director Availability Run command glossary](#), enter all of its corresponding properties then click the **Run** button.
3. View these commands execution status and command-line output.
  - a) Click the **Run execution status** tab.
  - b) To see the command-line output, in the right pane click the **Information** tab.

By using the above run command, perform various management operations with VMware Cloud Director Availability in Azure VMware Solution.

You can replicate workloads with VMware Cloud Director Availability in Azure VMware Solution. For more information, see [Replicating workloads](#) in the *User Guide*.

## VMware Cloud Director Availability Run command glossary

Run command can perform operations that normally require elevated privileges through a collection of PowerShell cmdlets. See the following list for VMware Cloud Director Availability, how to use them and a detailed description of the required input parameters.

See the following procedures for how to use each Run command for VMware Cloud Director Availability in the Azure VMware Solution environment.

**Table 18: VMware Cloud Director Availability Run command**

Run command	Description
<b>Get-VCDAReport</b>	Get a status report from VMware Cloud Director Availability.
<b>Initialize-AVSSite</b>	This initial command prepares the SDDC on Azure VMware Solution for VMware Cloud Director Availability installation. Creates vSphere service account, role, group, generate password.
<b>Install-VCDAAVS</b>	Once the Azure VMware Solution site is initialized, install and configure a VMware Cloud Director Availability instance. Finish with a production-ready site, consisting of a Cloud Director Replication Management Appliance, a Tunnel Appliance and two Replicator Appliance instances.
<b>Install-VCDAReplicator</b>	Install and configure additional Replicator Appliance instances in Azure VMware Solution, in addition to the initially-installed two Replicator Appliance instances.
<b>New-VCDAVMSnapshot</b>	Create a snapshot of a VMware Cloud Director Availability virtual machine.
<b>Remove-VCDAVMSnaps hot</b>	Remove a snapshot of a VMware Cloud Director Availability virtual machine.
<b>Repair-LocalReplicator</b>	Repair all local Replicator Appliance instances in the cloud site with the Manager Service. This Run command does not repair any remote Replicator Appliance instances.
<b>Repair-LookupService</b>	Repair vCenter Server Lookup service for all VMware Cloud Director Availability appliances, usually required once the vCenter Server Lookup service certificate or address changes.
<b>Reset-ServiceAccountPa ssword</b>	Reset the password of vSphere service account that is used by VMware Cloud Director Availability, and repair all Replicator Appliance instances with the new password. All Replicator Appliance instances must be in powered-on state.

Run command	Description
<b>Reset-VCDARootPassword</b>	Reset the <b>root</b> user password of all or any given VMware Cloud Director Availability virtual machine. By default the password changes only if it expires within the next 30 days.
<b>Start-VCDAVM</b>	Power on all or given VMware Cloud Director Availability virtual machine in Azure VMware Solution. By default all virtual machines that are not powered-on are powered-on.
<b>Stop-VCDAVM</b>	Stop all (Default) or given VMware Cloud Director Availability virtual machine in Azure VMware Solution. Without any parameter all VMware Cloud Director Availability virtual machines shut down gracefully.
<b>Uninstall-VCDAVS</b>	Delete all VMware Cloud Director Availability virtual machines, any custom roles, folders and accounts used by VMware Cloud Director Availability. All virtual machines must be in powered-off state.

**NOTE**

\* Required field for all the following tables.

**Get-VCDAReport**

Get a VMware Cloud Director Availability status report.

**Table 19: Get-VCDAReport**

Option	Description	Defaults
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status	
Timeout*	Operation timeout	30 min

**Install-VCDAReplicator**

Install and configure new VMware Cloud Director Availability Replicator Appliance virtual machine in the Azure VMware Solution environment.

When installing an additional Replicator Appliance instance, in addition to the first and second instances, you must use one of the predefined virtual machine names:

- VCD-AVS-Replicator-03
- VCD-AVS-Replicator-04
- VCD-AVS-Replicator-05
- VCD-AVS-Replicator-06

**Procedure****Table 20: Install-VCDAReplicator**

Option	Description	Defaults
Datastore*	Name of the datastore to be used for deployment of the appliances. The VMware Cloud Director Availability .ova file must be available in the same Datastore.	
Cluster*	Name of the destination vSphere cluster to be used for deployment of the VMware Cloud Director Availability appliances.	
ReplicatorIPAddress*	IPv4 address in CIDR notation, for example, <i>192.168.0.224/24</i> , to be used for deployment of the first (1st) Replicator Appliance.	
ReplicatorHostname*	Hostname of the first (1st) Replicator Appliance.	

Option	Description	Defaults
ReplicatorGW*	Gateway IP address for the 1st and the 2nd Replicator Appliance instances.	
ReplicatorNetwork*	Name of the vSphere network to be used for deployment of the 1st and the 2nd Replicator Appliance instances.	
NTPServer*	NTP server address to be used for all VMware Cloud Director Availability appliances.	
DNSServer*	Comma-separated list of DNS servers to be used for all appliances, for example, <i>192.168.1.1,192.168.1.2</i> .	
SearchDomain*	List of search domain for all appliances, for example, <i>domain1.local,domain2.local</i> .	
OVAFilename*	Name of the VMware Cloud Director Availability .ova file, located in a folder of the same datastore where the appliances are about to be deployed, for example, <i>VMware-Cloud-Director-Availability-Provider-release.number.xxx-xxxx-build_sha_OVF10.ova</i> .	
VMName	Name of the Replicator Appliance VM, must match any of the predefined virtual machine names: <ul style="list-style-type: none"> <li>• VCD-AMS-Replicator-03</li> <li>• VCD-AMS-Replicator-04</li> <li>• VCD-AMS-Replicator-05</li> <li>• VCD-AMS-Replicator-06</li> </ul>	
AcceptEULA*	Accept the <a href="#">VMware Cloud Director Availability End User License Agreement</a> .	False
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status.	
Timeout*	Operation timeout.	30 min

### **New-VCDAVMSnapshot**

Create a virtual machine snapshot of a VMware Cloud Director Availability virtual machine.

If no VMName is provided it takes snapshots of all the VMware Cloud Director Availability virtual machines.

The limit is two snapshots. If a virtual machine already has two snapshots, then no new snapshots are created.

#### **Procedure**

**Table 21: New-VCDAVMSnapshot**

Option	Description	Defaults
VMName	Name of the VMware Cloud Director Availability virtual machine to snapshot.	
Name	Enter a name for the new snapshot.	
Quisce	If the value is <code>\$true</code> and the virtual machine is powered-on, VMware Tools are used to quiesce the file system of the virtual machine. This assures that a disk snapshot represents a consistent state of the guest file systems. If the virtual machine is powered-off or VMware Tools are not available, the quiesce parameter is ignored.	False
Memory	If the value is <code>\$true</code> and if the virtual machine is powered-on, the memory state of the virtual machine is preserved with the snapshot.	False
Retain up to		60 days

Option	Description	Defaults
Specify name for execution*	Name used to follow the run command execution status.	
Timeout*	Operation timeout	30 min

### **Remove-VCDAVMSnapshot**

Remove a snapshot of a VMware Cloud Director Availability virtual machine, and to get a list of the available snapshots run **Get-VCDAReport**.

By default, this Run command deletes all snapshots from all VMware Cloud Director Availability virtual machines.

To filter which snapshots are removed, use a combination of different parameters.

Running the command without a `Confirm` parameter only lists the snapshots that are to be deleted but does not delete them.

#### **Procedure**

**Table 22: Remove-VCDAVMSnapshot**

Option	Description	Defaults
VMName	Name of the VMware Cloud Director Availability virtual machine to snapshot.	
Name	Name of the snapshots that you want to delete.	
Id	Id of the snapshots that you want to delete.	
Confirm	Confirm that the snapshots of the VMware Cloud Director Availability virtual machines are to be deleted. When not <code>True</code> , the command lists the snapshots that are to be deleted but does not delete any snapshots.	False
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status	
Timeout*	Operation timeout	30 min

### **Repair-LocalReplicator**

Repair all local VMware Cloud Director AvailabilityReplicator Appliance instances in the cloud site with the Manager Service on the Cloud Director Replication Management Appliance.

By default repairs all Replicator Appliance instances. Alternatively, use the `VMName` parameter to repair a specific Replicator Appliance instance. No remote Replicator Appliance instances can be repaired using this Run command.

Use this Run command after the service account password changes or after renewing a Replicator Appliance certificate.

#### **Procedure**

**Table 23: Repair-LocalReplicator**

Option	Description	Defaults
VMName	Name of the Replicator Appliance virtual machine.	
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status.	

Option	Description	Defaults
Timeout*	Operation timeout.	30 min

### **Repair-LookupService**

Repair the vCenter Server Lookup service for the VMware Cloud Director Availability appliances. By default, repairs the service for all of the appliances. Alternatively, to repair a single appliance, specify the `VMName` parameter.

Use this Run command after renewing the certificate of the vCenter Server Lookup service or after its address changes.

#### **Procedure**

**Table 24: Repair-LookupService**

Option	Description	Defaults
VMName	Name of a VMware Cloud Director Availability virtual machine.	
Retain up to		60 days
Specify name for execution*	Name used to follow the Run command execution status.	
Timeout*	Operation timeout.	30 min

#### **What to do next**

- Log in to the VMware Cloud Director Availability management interface and validate the health status of the system services.
- If needed, run the **Repair-LocalReplicator** command.

### **Reset-ServiceAccountPassword**

Reset the password of the vSphere service account that is used by VMware Cloud Director Availability, and repair all Replicator Appliance instances with the new password.

#### **Prerequisites**

Verify that all Replicator Appliance virtual machines are in powered-on state. If any instance is destined to remain unavailable, set the `force` parameter to `True`.

#### **Procedure**

**Table 25: Reset-ServiceAccountPassword**

Option	Description	Defaults
force	Resets the service account password, even when not all Replicator Appliance instances are in powered-on state.	False
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status.	
Timeout*	Operation timeout.	30 min

### **Reset-VCDARootPassword**

Reset the root password of all or any given VMware Cloud Director Availability virtual machine. By default, the password resets only if it expires within the next 30 days, unless you configure the `force` parameter to `True`.

#### **Procedure**

**Table 26: Reset-VCDARootPassword**

Option	Description	Defaults
force	When <code>True</code> , resets the password regardless if it expires in the next 30 days.	False
VMName	Name of the VMware Cloud Director Availability virtual machine on which the password must be reset.	
Retain up to		60 days
Specify name for execution*	Name used to follow the Run command execution status.	
Timeout*	Operation timeout.	30 min

**Start-VCDAVM**

Power-on all or a given VMware Cloud Director Availability virtual machine in the Azure VMware Solution environment.

By default, powers-on all virtual machines that are not in powered-on state. Alternatively, to power-on a specific virtual machine, use the `VMName` parameter.

**Procedure****Table 27: Start-VCDAVM**

Option	Description	Defaults
VMName	Name of the VMware Cloud Director Availability virtual machine to power-on.	
Retain up to		60 days
Specify name for execution*	Name used to follow the Run command execution status.	
Timeout*	Operation timeout.	30 min

**Stop-VCDAVM**

Stop all or a specific VMware Cloud Director Availability virtual machine in the Azure VMware Solution environment.

By default, without any parameter shuts down all the VMware Cloud Director Availability virtual machines gracefully.

**Procedure****Table 28: Stop-VCDAVM**

Option	Description	Defaults
force	<code>True</code> : power-off. <code>False</code> : graceful shutdown.	False
VMName	Name of the VMware Cloud Director Availability virtual machine to shutdown.	
Retain up to		60 days
Specify name for execution*	Name used to follow the Run command execution status.	
Timeout*	Operation timeout.	30 min

## **Uninstall-VCDAAVS**

Delete all VMware Cloud Director Availability virtual machines, any custom roles, folders, and accounts used by VMware Cloud Director Availability. Requires all virtual machines to be in powered-off state.

### **Procedure**

**Table 29: Uninstall-VCDAAVS**

Option	Description	Defaults
AcceptUninstall	Confirm accepting that all VMware Cloud Director Availability virtual machines, any custom roles, folders and accounts used by VMware Cloud Director Availability are all going to be deleted.	False
Retain up to		60 days
Specify name for execution*	Name used to follow the Run command execution status.	
Timeout*	Operation timeout.	30 min

## **Initialize-AVSSite**

Prepare the Azure VMware Solution site to accept the deployment of VMware Cloud Director Availability:

This Run command prepares the SDDC and the Azure VMware Solution environment for VMware Cloud Director Availability installation. Creates and sets vSphere service account, role, group and privileges.

### **Prerequisites**

Verify that you can access the Microsoft Azure Portal by using an account with sufficient privileges for using the Azure VMware Solution service.

### **Procedure**

**Table 30: Initialize-AVSSite**

Option	Description	Defaults
Retain up to		60 days
Specify name for execution*	Name used to follow the run command execution status	
Timeout*	Operation timeout	30 min

### **What to do next**

Install and configure a VMware Cloud Director Availability instance on Azure VMware Solution by running the **Install-VCDAAVS** command.

## **Install-VCDAAVS**

Install and configure a VMware Cloud Director Availability instance in Azure VMware Solution. Before running **Install-VCDAAVS**, the Azure VMware Solution site must be prepared by running the **Initialize-AVSSite** command.

This Run command installs a VMware Cloud Director Availability instance, consisting of a Cloud Director Replication Management Appliance, a Tunnel Appliance and two Replicator Appliance instances. You must Read and Accept the [VMware Cloud Director Availability End User License Agreement](#)

## Prerequisites

- Verify that the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` version 4.7 or later is uploaded and accessible on the datastore.
- Verify that the subnet, DNS zone and records for the VMware Cloud Director Availability appliances are configured.
- Verify that the subnet has outbound internet connectivity to communicate with VMware Cloud Director service, remote VMware Cloud Director Availability sites or/and Upgrade registry.
- Verify that the DNS zone has forwarding for the public addresses supposed to be reached by V VMware Cloud Director Availability outside of the local network segment.
- Verify that the Cloud Director service is associated, and Transport Proxy is configured with the Azure VMware Solution private cloud SDDC.
- Verify that the required system users, roles and privileges are already initialized by **Initialize-AVSSite**.

## Procedure

**Table 31: Install-VCDAAVS**

Option	Description	Defaults
License*	Valid license key for VMware Cloud Director Availability.	
SiteName*	Name of the VMware Cloud Director Availability site, cannot be changed after installation. Only Latin alphanumeric characters and "." are allowed in site name.	
PublicApiEndpoint*	VMware Cloud Director Availability Public Service Endpoint address, for example, <code>https://VCDA-FQDN:443</code> .	
VCDApiEndpoint*	VMware Cloud Director service endpoint URL, for example, <code>https://Cloud-Director-IP-Address:443/api</code> .	
VCDUser*	User name of a <b>System administrator</b> user in VMware Cloud Director service. For example, use <code>administrator@system</code> .	
VCDPassword*	Password of the VMware Cloud Director service <b>System administrator</b> user.	
Datastore*	Name of the datastore to be used for deployment of the appliances. The VMware Cloud Director Availability .ova file must be available in the same datastore.	
Cluster*	Name of the destination vSphere cluster to be used for the deployment of the VMware Cloud Director Availability appliances.	
ManagerIPAddress*	IPv4 address in CIDR notation, for example, <code>192.168.0.222/24</code> to be used for deployment of the Cloud Director Replication Management Appliance.	
ManagerGW*	Gateway IP address for the Cloud Director Replication Management Appliance.	
ManagerHostname*	Hostname of the Cloud Director Replication Management Appliance.	
ManagerNetwork*	Name of the vSphere network to be used for deployment of the Cloud Director Replication Management Appliance.	
TunnelIPAddress*	IPv4 address in CIDR notation, for example, <code>192.168.0.223/24</code> , to be used for deployment of the Tunnel Appliance.	
TunnelGW*	Gateway IP address for the Tunnel Appliance.	
TunnelHostname*	Hostname of the Tunnel Appliance.	
TunnelNetwork*	Name of the vSphere network to be used for deployment of the Tunnel Appliance.	
Replicator1IPAddress*	IPv4 address in CIDR notation, for example, <code>192.168.0.224/24</code> , to be used for deployment of the first (1st) Replicator Appliance instance.	
Replicator1Hostname*	Hostname of the first (1st) Replicator Appliance instance.	
Replicator2IPAddress*	IPv4 address in CIDR notation, for example, <code>192.168.0.225/24</code> to be used for deployment of the second (2nd) Replicator Appliance instance.	
Replicator2Hostname*	Hostname of the second (2nd) Replicator Appliance instance.	
ReplicatorGW*	Gateway IP address for the 1st and the 2nd Replicator Appliance instances.	

Option	Description	Defaults
ReplicatorNetwork*	Name of the vSphere network to be used for deployment of the 1st and the 2nd Replicator Appliance instances.	
NTPServer*	NTP server address to be used for all VMware Cloud Director Availability appliances.	
DNSServer*	Comma-separated list of DNS servers to be used for all appliances, for example, <i>192.168.1.1,192.168.1.2</i> .	
SearchDomain*	List of search domain for all appliances, for example, <i>domain1.local, domain2.local</i> .	
OVAFilename*	Name of the VMware Cloud Director Availability .ova file, located in a folder of the same datastore where the appliances are about to be deployed, for example, <i>VMware-Cloud-Director-Availability-Provider-release.number.xxxxxx-build_sha_OVF10.ova</i> .	
AcceptEULA*	Accept the <a href="#">VMware Cloud Director Availability End User License Agreement</a> .	False
Retain up to		60 days
Specify name for execution*	Name used to follow the execution status of the Run command.	
Timeout*	Operation timeout.	30 min

### What to do next

1. Configure the of for pairing with external sites by dNAT rule associating the external IP address with the internal endpoint running on the port 8048.
2. After performing [Install-VCDAAVS](#) for the services, to validate that the setup is complete, open the management interface then verify the status of all services by clicking the **System health** page, where the entries show a green health state to indicate successfully configured services.
  - a. To log in to the management interface of the , in a Web browser, go to either of the following addresses:
    - [https://VMware-Cloud-Director-Availability-Public-Service-Endpoint\\_Public\\_Address/ui/login](https://VMware-Cloud-Director-Availability-Public-Service-Endpoint_Public_Address/ui/login)
    - <https://Cloud-Director-Replication-Management-Appliance-IP-Address/ui/login>
    - <https://Cloud-Director-service-Address/provider/plugins/Your-VCDA-Plugin-Id>
  - b. Enter the user name and password of a user with VMware Cloud Director **System** privileges then click **Login**.
3. Once the services are up and in a healthy state, you can use the management interface to proceed with the required management tasks. For information about performing administrative tasks such as changes to the provisioned environment and routine administration and maintenance procedures, see [Administration in the Cloud Director site](#).
4. Pair with external sites.
  - a. Optionally, the tenants can configure and pair instances with in Azure VMware Solution. For the detailed initial on-premises configuration and pairing procedure, see [Configure the](#) .
  - b. Optionally, pair in Azure VMware Solution with private Cloud Director sites. For the detailed pairing procedure, see [Pair two Cloud Director sites](#).

### Known problems and solutions

- The Run command **Install-VCDAAVS** fails with the message: `Generic network error occurred at the client side.`

#### Problem resolution:

VMware Cloud Director AvailabilityCloud Director Replication Management Appliance cannot communicate with VMware Cloud Director service Public API endpoint.

#### Synopsis:

The run execution fails with `Generic network error occurred at the client side.`

#### Solution:

Run the **Install-VCDAAVS** command again once you resolved the problem:

1. Open <https://portal.azure.com>.
  2. Navigate to your Azure VMware Solution private cloud **Operations > Run Command**.
  3. Run execution status then pick the most recent `Install-VCDAAVS-ExecXX`.
  4. Click the **Rerun** button.
  5. Validate that the URL set as **VCDApiEndpoint** is correct and has `/api` at the end. For example, `https://Cloud-Director-service-URL:443/api`.
  6. Validate that all the properties are correct then click **Run**.
- The Run command **Install-VCDAAVS** fails with the message: `Could not find SSL/X509 certificate from...`

**Problem resolution:**

VMware Cloud Director Availability Cloud Director Replication Management Appliance cannot establish a connection with VMware Cloud Director service.

**Synopsis:**

The run execution fails with `Could not find SSL/X509 certificate from https://Cloud-Director-service-URL:443/api`.

**Solution:**

1. Validate that the Cloud Director Replication Management Appliance has outbound network connectivity to the VMware Cloud Director service.
2. Run the **Install-VCDAAVS** command again:
  - a. Open <https://portal.azure.com>.
  - b. Navigate to your Azure VMware Solution private cloud **Operations > Run Command**.
  - c. Run execution status then pick the most recent `Install-VCDAAVS-ExecXX`.
  - d. Click the **Rerun** button.
  - e. Validate that the URL set as **VCDApiEndpoint** is correct. For example, `https://Cloud-Director-service-URL:443/api`.
  - f. Validate that all the properties are correct then click **Run**.

## API Guides

---

The programming guides provides information about the VMware Cloud Director Availability REST APIs, including how to use the API services and resources, how to authenticate and construct REST API calls.

### **vSphere DR and Migration API Guide 4.7**

[vSphere DR and Migration API Guide 4.7](#)

### **Cloud Director DR and Migration API Guide 4.7**

[Cloud Director DR and Migration API Guide 4.7](#)

## Terminology

See this glossary for the terms in VMware Cloud Director Availability documentation.

- **Appliance:** VMware Cloud Director Availability consists of one or multiple appliances, depending on the site where they reside in:

Cloud site backed by:	Cloud site appliance roles:	On-premises site appliance roles:
VMware Cloud Director	<ul style="list-style-type: none"> <li>• <b>Cloud Director Replication Management Appliance:</b> An appliance that manages replications in a VMware Cloud Director Availability instance deployed in a cloud site backed by VMware Cloud Director.</li> <li>• <b>Tunnel Appliance instances:</b> One or, two appliances in an active-active mode, that provide the ingress and egress secure SSL communication in a VMware Cloud Director Availability instance.</li> <li>• <b>Replicator Appliance instances:</b> One or more appliances that handle the replication of data in a VMware Cloud Director Availability instance.</li> </ul>	<b>On-premises to Cloud Director Replication Appliance:</b> An appliance that is deployed in the on-premises site to replicate vSphere workloads between an on-premises vCenter Server instance and a provider cloud site backed by VMware Cloud Director.
VMware vCenter Server	<ul style="list-style-type: none"> <li>• <b>vCenter Replication Management Appliance:</b> An appliance that manages replications in a VMware Cloud Director Availability instance deployed in a provider cloud vCenter site.</li> <li>• <b>Replicator Appliance instances:</b> Optionally, one or more appliances handle the replication of data in a VMware Cloud Director Availability instance.</li> </ul>	<b>On-premises to Cloud vCenter Replication Appliance:</b> An appliance that is deployed in the on-premises site to replicate vSphere workloads between an on-premises vCenter Server instance and a provider cloud vCenter Server site.

- **Architectures:**
  - **Cloud Director site:** A multi-tenant provider cloud site backed by VMware Cloud Director to manage and offer disaster recovery and migration services to multiple tenants using VMware Cloud Director Availability instances. These instances consist of a Cloud Director Replication Management Appliance, one or more Replicator Appliances, and one or two Tunnel Appliances for high availability. The Cloud Director sites can interoperate both with other Cloud Director sites and with on-premises sites.
  - **Cloud vCenter site:** A provider cloud site where a cloud service provider deploys a vCenter Server instance to offer disaster recovery and migration services to tenants using a VMware Cloud Director Availability instance. This instance consists of a vCenter Replication Management Appliance and optionally one or more Replicator Appliances. The cloud vCenter sites can interoperate with other cloud vCenter sites or with on-premises sites.
  - **On-premises sites:** Tenants' on-premises vCenter Server sites can protect and migrate their workloads to a provider cloud site using VMware Cloud Director Availability On-Premises Appliance. The tenants deploy the appliance and select its role which can be either an On-Premises to Cloud Director Replication Appliance or an On-Premises to Cloud vCenter Replication Appliance, depending on the type of the provider cloud site. On-premises sites can interoperate only with either a Cloud Director site or a cloud vCenter site.
- **Asynchronous replication:** A data replication method where changes to the primary data are not immediately replicated to the secondary data, but instead are queued and replicated later.
- **Availability cloud site:** A provider cloud site where VMware Cloud Director Availability is deployed to offer disaster recovery and migration services.
- **Backup:** The entire configuration of VMware Cloud Director Availability can be stored in a compressed file, either locally or on an SFTP server.

- **Cloud provider:** Offers cloud-based infrastructure, platform, or software services to customers. These services are accessed by their tenants through a web browser or API. Depending on whether the site is backed by VMware Cloud Director, the provider deploys VMware Cloud Director Availability instances using the appropriate appliances' roles in their vCenter Server instance.
- **Deployment:** The process of installing and configuring the VMware Cloud Director Availability appliances.
- **Deployment topology:** The placement of components in the disaster recovery environment and how they are connected to each other.
- **Destination:** The site to which data is being replicated. The destination can either be the on-premises site, the cloud vCenter Server site, or the multi-tenant cloud site backed by VMware Cloud Director.
- **Disaster recovery:** Refers to an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber attack, or business disruptions. Disaster recovery relies upon the replication of the workload in an off-premises site not affected by the disaster. VMware Cloud Director Availability provides continuous availability of the protected workloads and automates their recovery operations.
- **Disaster recovery protection:** The process of protecting the workloads and their data from disasters by replicating them to a secondary site. Also, see Protection.
- **DRaaS:** Disaster Recovery-as-a-Service, a cloud-based service that provides disaster recovery protection for virtual workloads.
- **ESXi:** An operating system-independent bare-metal hypervisor software installed on servers that can use the physical hardware to create one or more virtual machines (VMs).
- **Failover:** The process of switching to a redundant site in the event of a failure or outage of the primary site.
- **Failover workflows:** Workflows that define the steps to take when failing over workloads to another site in the event of a disaster or outage.
- **In-context integration:** Integration of one product or service with another in a way that is seamless and intuitive for the user. For example, the VMware Cloud Director Availability plug-ins for vSphere and for VMware Cloud Director offer native integration in context without switching interfaces.
- **Migration:** The process of moving data or applications from one location to another. For example, when the primary location is about to be decommissioned.
- **Multi-tenant cloud:** A provider cloud computing architecture where multiple tenants share the same infrastructure and resources but are logically isolated from each other. For example, VMware Cloud Director Availability cloud site, backed by VMware Cloud Director.
- **On-Premises Appliance:** An appliance that enables tenants to protect and migrate their workloads from an on-premises vCenter Server site to a provider cloud site.
- **On-premises site:** A site where VMware Cloud Director Availability and vCenter Server are deployed on-premises within the own facilities of an organization.
- **Partner Connect Program:** A program through which VMware partners can provide VMware Cloud Director Availability.
- **Protection:** The safeguarding of vApps and virtual machines against disasters or unavailability. VMware Cloud Director Availability provides a range of protection services, including disaster recovery, migration, failover, and reverse failover to ensure the continuous availability of the workloads and automate the recovery operations. Protection is achieved through asynchronous replications between cloud sites or between cloud sites and on-premises sites.
- **Provider cloud site:** A site where a cloud service provider offers cloud disaster recovery and migration services to tenant users by using VMware Cloud Director Availability.
- **Quiesce:** The process of pausing or altering a device or application to achieve a consistent state, usually in preparation for a backup or other maintenance. In VMware Cloud Director Availability, quiescing is used to prepare the virtual machines for replication, by creating a snapshot of their memory and then pausing them so that no new data gets written to their disks during replication. The quiescing ensures that the replicated virtual machine is in a consistent state and that no data gets lost during replication.
- **Recovery point objective (RPO):** The maximum amount of data loss acceptable in case of a disaster. The RPO is the maximum amount of time that can elapse between creating a replica and a disaster.
- **Replication:** The process of transferring workload data from the source site to the destination site to allow for protecting, migrating, failing over, and reversing the workload between the two sites.

- Replication policy: A set of rules that define and control the replication settings on a Cloud Director organization level.
- Restore: Once backed up, the appliances configuration can be restored using the interface of VMware Cloud Director Availability.
- Reverse: After performing migration or failover, perform reverse to fallback the workload from the destination site to the original source site.
- Site: A physical location where vSphere workloads are hosted. In VMware Cloud Director Availability, the site can be either an on-premises site or a cloud site.
- Source: The site from which data is being replicated. The source can either be an on-premises vCenter Server instance, a cloud vCenter Server site, or a multi-tenant cloud site backed by VMware Cloud Director.
- Seed: A seed is a vApp or a VM transferred to the destination site before starting a replication to reduce the network traffic and the time for the initial synchronization. The seed is created using different methods, such as offline data transfer, cloning, failover, or copying over the network.
- SLA profile: Service Level Agreement profiles define replication settings, such as recovery point objective (RPO), retention policy for point-in-time instances, quiescing, compression, and initial synchronization time. The provider controls them at once by assigning the SLA profile to multiple VMware Cloud Director organizations.
- Tenant: A customer user of the cloud provider's services to host and run the tenant's applications. In a multi-tenant environment, multiple tenants share the same infrastructure resources, while their data and applications remain isolated from each other ensuring security and privacy. Tenants deploy an On-Premises Appliance in their vCenter Server sites, choosing the appliance role depending on the cloud site type.
- Tenant self-service protection: The ability for tenant users to manage their disaster recovery protection using self-service tools provided by their cloud provider. The tenants can protect their virtual machines or vApps on their own.
- Test failover: Testing allows you to validate that the data from the source site replicates correctly in the destination site.
- Unified architecture: An architecture that integrates multiple components into a single, cohesive system. For example, the appliances of VMware Cloud Director Availability in a cloud site.
- vApp: A virtual application, or vApp, is a container that packages one or more virtual machines along with their associated virtual disks, virtual network interfaces, and other resources. The vApp is a collection of virtual machines that are grouped together for management purposes. In VMware Cloud Director Availability, a vApp can be used to protect and migrate a group of virtual machines as a single unit.
- vCenter Server: A centralized management utility for virtual machines, multiple ESXi hosts, and all dependent components from a single location. Required at each VMware Cloud Director Availability site.
- vCloud Availability: The former name of VMware Cloud Director Availability.
- vCloud Usage Meter: A tool that meters the usage of VMware products and services by providers and tenants.
- VM: A virtual machine is a software-based emulation of a physical computer. It can run its own operating system and applications, like a physical computer. VMs are created and managed by virtualization software, such as vSphere, which allows multiple VMs to run on a single physical host machine. VMware Cloud Director Availability can replicate a virtual machine from a source site to a destination site, allowing failing it over, migrating to another site, or returning it back.
- VMware Cloud Director: A cloud management platform that enables the delivery of infrastructure-as-a-service (IaaS) across multiple clouds.
- VMware Cloud Director Availability: A Disaster Recovery-as-a-Service (DRaaS) solution that protects, migrates, fails-over, and reverses failover of vApps and virtual machines between multi-tenant clouds and on-premises with asynchronous replications.
- vSphere: A cloud computing virtualization platform allowing running application workloads on virtual machines. vCenter Server and ESXi are core components.
- vSphere workloads: Users' workloads that run on the vSphere platform.
- vSphere DR and migration: Disaster recovery and migration capabilities for vSphere workloads between vCenter Server sites using VMware Cloud Director Availability.

## Changelog

This *Changelog* is updated with each release of the product or when necessary.

These tables provide the update history of *VMware Cloud Director Availability* for each version.

### 4.7

**Table 32: VMware Cloud Director Availability 4.7.3 | 18 SEP 2024 | Build 24280288 (Product version: 4.7.3.10534495-154c9f5866)**

Release	Description
18 SEP 2024	VMware Cloud Director Availability 4.7.3 includes important resolved issues and updates of third-party libraries that provide security fixes.
	VMware Cloud Director Availability 4.7.3 supports VMware Cloud Director 10.6.0.1 and VMware vCenter 8.0 Update 3b.
	VMware Cloud Director Availability 4.7.3 supports product activation by using a VMware Live Recovery license key. For more information see <a href="#">Get Software and License Key for VMware Cloud Director Availability</a> .

**Table 33: VMware Cloud Director Availability 4.7.2 | Build 24058656 (Product version:4.7.2.10056114-4ada44c9c3)**

Release	Description
04 JUL 2024	VMware Cloud Director Availability 4.7.2 can now protect and migrate virtual machines with enabled vTPM, and with full, partial, or no encryption of the attached storage disks.
	VMware Cloud Director Availability 4.7.2 can encrypt non-encrypted VMs as a part of the protection and migration processes.
	VMware Cloud Director Availability 4.7.2 supports protection and migration processes with storage policies that use mixed encryption capabilities.

**Table 34: VMware Cloud Director Availability 4.7.1 | Build 23265673 (Product version: 4.7.1.8968498-0422b55a9e)**

Release	Description
15 FEB 2024	VMware Cloud Director Availability 4.7.1 includes important resolved issues and updates of third-party libraries that provide security fixes.
	VMware Cloud Director Availability 4.7.1 can now perform cold migrate for workloads to transfer from non-VMware environments, such as KVM, Hyper-V, physical hosts, and others, to a Cloud Director site. The cold migration means that the source machine is powered-off and rebooted into an ISO image, created by VMware Cloud Director Availability. Once booted from this ISO image, a new migration appears on the destination site.

**Table 35: VMware Cloud Director Availability 4.7 | Build 22817906 (Product version: 4.7.0.8400987-96215f032c)**

Release	Description
23 NOV 2023	Storage policy reassignment during workload recovery - you can activate <b>Change storage placement</b> , then select a different datastore than the selected one in the existing replication, resulting in move of the data after the performed failover or migrate operation completes. All the disks and the vmdk files move to the newly selected storage. For example, the tenants can initially send the replica files to a cheaper and slower storage, where the vmdk gets constructed, then once failed over, the workload moves to expensive and fast storage.
	Security tags - the NSX security tags can be replicated between cloud sites, both running VMware Cloud Director 10.3 and later and VMware Cloud Director Availability 4.7. The security tags apply during the recovery of virtual machine, vApp, and vApp template replications.
	VDC VM policies pre-selected - when creating a replication to a Cloud Director site as a destination, when a VM placement or a VM sizing policy with the same name already applies on the source workload, the matching VDC policy becomes pre-selected, allowing to finish the new replication wizard quicker.
	Recovery plans health validation - after creating a recovery plan, on the <b>Health</b> tab you see a validation of the infrastructure and the data for the replications in the plan to check whether the plan execution might fail on some steps. The validation can show a warning when the observed issues cannot prevent the recovery process, or an error when the issues prevent the recovery process, for example, when the destination storage policy is disabled.
	Flexible storage profile assignment - allows replicating one virtual machine to multiple datastores. For example, place one of its disks on a separate datastore, or split some disks from the .vmx file.
	Pairing sites filtering - the providers can hide some peer sites for certain organizations to prevent every tenant from seeing all paired sites for convenience. The restricted tenants can continue to manage existing incoming replications, but not start new ones as the source site is not visible and cannot see the outgoing replications as they are filtered by site.
	Cloud Director authentication model compliance - prepares VMware Cloud Director Availability for the future deprecation of local users in VMware Cloud Director.
	Replication tracking virtual machine (RT VM) placement solution for Cloud Director replications - now replaces the independent disk and represents a shadow VM for replication placement to allow per-disk placement. The providers can also configure replication tracking for the existing vApp and VM replications. With a supported version of VMware Cloud Director in the destination site, RT VM replaces the independent disk as placement and reporting solution and allows per-disk storage profiles.
	Seed for vSphere DR and migration - using a seed virtual machine is also available for replications between vCenter sites.
	Deactivate protections to on-premises - protections allow for finer control on the allowed destination site, separating on-premises from cloud sites, similarly to controlling migrations separately for on-premises and cloud destinations.
	My Preferences - allows each user to select the language of their interface, dark, light, or high contrast theme, and select number of rows and whether the selected row follows the clicked row.

## 4.6

**Table 36: VMware Cloud Director Availability 4.6.1 | Build 22347688 (Product version: 4.6.1.7681624-a5359f8567)**

Release	Description
31 AUG 2023	VMware Cloud Director Availability 4.6.1 includes important resolved issues and third-party libraries.

Release	Description
	In Cloud Director sites, as <b>aprovider</b> or as <b>atenant</b> you can register a Simple Mail Transfer Protocol (SMTP) server directly in VMware Cloud Director Availability and <b>Set custom SMTP settings</b> as an alternative of <b>Configure in Cloud Director</b> .

**Table 37: VMware Cloud Director Availability 4.6 | Build 21891963 (Product version: 4.6.0.6869101-29b03ba46f)**

Release	Description
15 JUN 2023	Recovery plans can also be created and run for vSphere DR and migration between vCenter Server sites.
	Events and notifications allow auditing the VMware Cloud Director Availability events by using the Cloud Director delivery channel. VMware Cloud Director automatically marks all external events, like the ones received from VMware Cloud Director Availability, as audit events, subject to audit persistence, retention, and export capabilities by using the audit trail system in VMware Cloud Director.
	<p>Recovery Settings Enhancements</p> <ul style="list-style-type: none"> <li>You can map the source and the destination networks per selected replications for on-premises to cloud replications, similarly to the ones from cloud to cloud.</li> <li>vSphere DR and migration validates the recovery settings (data center, VM folder, compute, and others) based on the replication settings (datastore). The network settings are similar to Cloud Director sites, and the source and destination network mappings allow per-virtual machine network mapping.</li> </ul>
	<p>vSphere to vSphere DR and Migration Public API</p> <ul style="list-style-type: none"> <li>VMware Cloud Director Availability provides a step-by-step guide to configure a deployed appliance on <i>developer.vmware.com</i>.</li> <li>In the left pane, under <b>Configuration</b>, click <b>OpenApi Client</b> and select an API. For more information, see <i>developer.vmware.com</i> for the <i>API Programming Guide</i>.</li> </ul>
	<p>NSX-T vApp Edges Support - VMware Cloud Director Availability 4.6, backed by VMware Cloud Director 10.3 or later, supports:</p> <ul style="list-style-type: none"> <li>Replicates routed vApp networks and vApp network services to virtual data centers backed by NSX with error-free automatic destination network mapping.</li> <li>Replicates the DHCP service on vApp isolated networks, bringing parity with NSX for vSphere.</li> <li>To configure a routed vApp network and use any vApp network services, like DHCP in isolated vApp networks, the containing organization's virtual data center must be configured with an edge cluster.</li> </ul>
	Guest Customization Global Setting is a global setting that affects all replications - whether the users need to manually activate or deactivate guest customization on failover.
	Tunnel Appliance High Availability in Cloud Director sites. A second Tunnel Appliance can operate in an active-active mode for high availability of the Tunnel Service, both for new deployments and for upgraded ones.
	Replicating vApp templates between Cloud Director sites includes protecting the vApp templates that permit tracking the source for changes, allowing either creating new destination template versions when the source changes or overwriting the destination.
	<p>Improved Event Notifications</p> <ul style="list-style-type: none"> <li>Events and notifications can also send replication management events by using the email delivery channel.</li> <li>With the email delivery channel configured, tenants and providers can subscribe to a weekly summary email. The subscribers can remain informed about what is happening with their replications without logging in to VMware Cloud Director Availability.</li> <li>In Cloud Director sites, as <b>aprovider</b>, you can see an activity summary report in the management interface.</li> </ul>
	<p>Bandwidth throttling can also apply throttle for vSphere DR and migration sites.</p> <p><b>NOTE</b> Applying the limit requires one or more external Replicator Appliance instances.</p>
	<b>VMC data engine</b> allows creating migrations back to the on-premises vCenter Server site.

---

## Documentation Legal Notice

---

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

