

# Installation, Configuration, and Upgrade Guide On-Premises

23 JUN 2022

VMware Cloud Director Availability 4.4

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

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

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

# Contents

<b>1</b>	<b>VMware Cloud Director Availability Overview On-Premises</b>	<b>4</b>
<b>2</b>	<b>Interoperability and vSphere Product Edition</b>	<b>6</b>
<b>3</b>	<b>Installing and Configuring a vCenter Replication Management Appliance and an On-Premises to Cloud vCenter Replication Appliance</b>	<b>8</b>
	Deployment Architecture and Requirements of vCenter Replication Management Appliance and On-Premises to Cloud vCenter Replication Appliance	8
	Deploy Both Appliances	13
	Configure and Pair Both Appliances	16
<b>4</b>	<b>Installing and Configuring On-Premises to Cloud Director Replication Appliance</b>	<b>20</b>
	Deployment Architecture On-Premises	20
	Deployment Requirements On-Premises	22
	Deploying the On-Premises to Cloud Director Replication Appliance	25
	Deploy the On-Premises to Cloud Director Replication Appliance by Using the vSphere Client	25
	Deploying by Using the VMware OVF Tool	27
	Configuring the On-Premises to Cloud Director Replication Appliance	29
	Configure the On-Premises to Cloud Director Replication Appliance	29
	Configure Local Placement	32
<b>5</b>	<b>Upgrading On-Premises</b>	<b>35</b>
	Management Interface Upgrading On-Premises	37
	Upgrade VMware Cloud Director Availability On-Premises by Using the Default Repository	37
	Upgrade VMware Cloud Director Availability On-Premises by Using a Specified Repository	38
	Upgrade VMware Cloud Director Availability On-Premises by Using an ISO Image	41
	Command-Line Upgrading On-Premises	44
	Command-Line Upgrade On-Premises by Using an ISO Image	44
	Post-Upgrade Configuration On-Premises	46

# VMware Cloud Director Availability Overview On-Premises

# 1

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 cloud vCenter Server site or a multi-tenant cloud site backed by VMware Cloud Director™.

VMware Cloud Director Availability is available through the VMware Cloud Provider 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 to cloud site backed by VMware Cloud Director**

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 On-Premises](#).

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

VMware Cloud Director Availability On-Premises Appliance version 4.4 and later have 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 of vCenter Replication Management Appliance and On-Premises to Cloud vCenter Replication Appliance](#).

Since VMware Cloud Director Availability 4.4, during the on-premises appliance deployment in the on-premises vCenter Server instance, select its role for replicating with a cloud site:

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

Pairs with a cloud site backed by VMware Cloud Director. For more information, see [Chapter 4 Installing and Configuring On-Premises to Cloud Director Replication Appliance](#).

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

Pairs with a cloud vCenter Server site, running vCenter Replication Management Appliance. For more information, see [Chapter 3 Installing and Configuring a vCenter Replication Management Appliance and an On-Premises to Cloud vCenter Replication Appliance](#).

VMware Cloud Director Availability provides:

- Test failover or failover on-premises workloads to the cloud site and failback 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

## 2

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 and the interoperability between the source site and the destination site versions.

## 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 [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 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 sites backed by VMware Cloud Director](#) in the *Administration Guide*.

## Metering cloud sites

As a **provider**, you must meter the consumption data of each cloud site instance of VMware Cloud Director Availability by adding the Service Endpoint of the appliances in VMware vCloud® Usage Meter. For more information, see [Usage Meter integration](#).

# Installing and Configuring a vCenter Replication Management Appliance and an On-Premises to Cloud vCenter Replication Appliance

To replicate vSphere workloads between vCenter Server instances, in the provider vCenter Server instances deploy and license vCenter Replication Management Appliance instances, in the tenants vCenter Server instances deploy VMware Cloud Director Availability On-Premises Appliance instances and during deployment select the On-Premises to Cloud vCenter Replication Appliance role.

- 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 [Chapter 4 Installing and Configuring On-Premises to Cloud Director Replication Appliance](#) chapter.

This chapter includes the following topics:

- [Deployment Architecture and Requirements of vCenter Replication Management Appliance and On-Premises to Cloud vCenter Replication Appliance](#)
- [Deploy Both Appliances](#)
- [Configure and Pair Both Appliances](#)

## Deployment Architecture and Requirements of vCenter Replication Management Appliance and On-Premises to Cloud vCenter Replication Appliance

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**. Deploying the appliances creates the groups **VRADMINISTRATORS** and **VRUSERS** in the vCenter Server instance.

## Appliances Deployment

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

### vCenter Replication Management Appliance

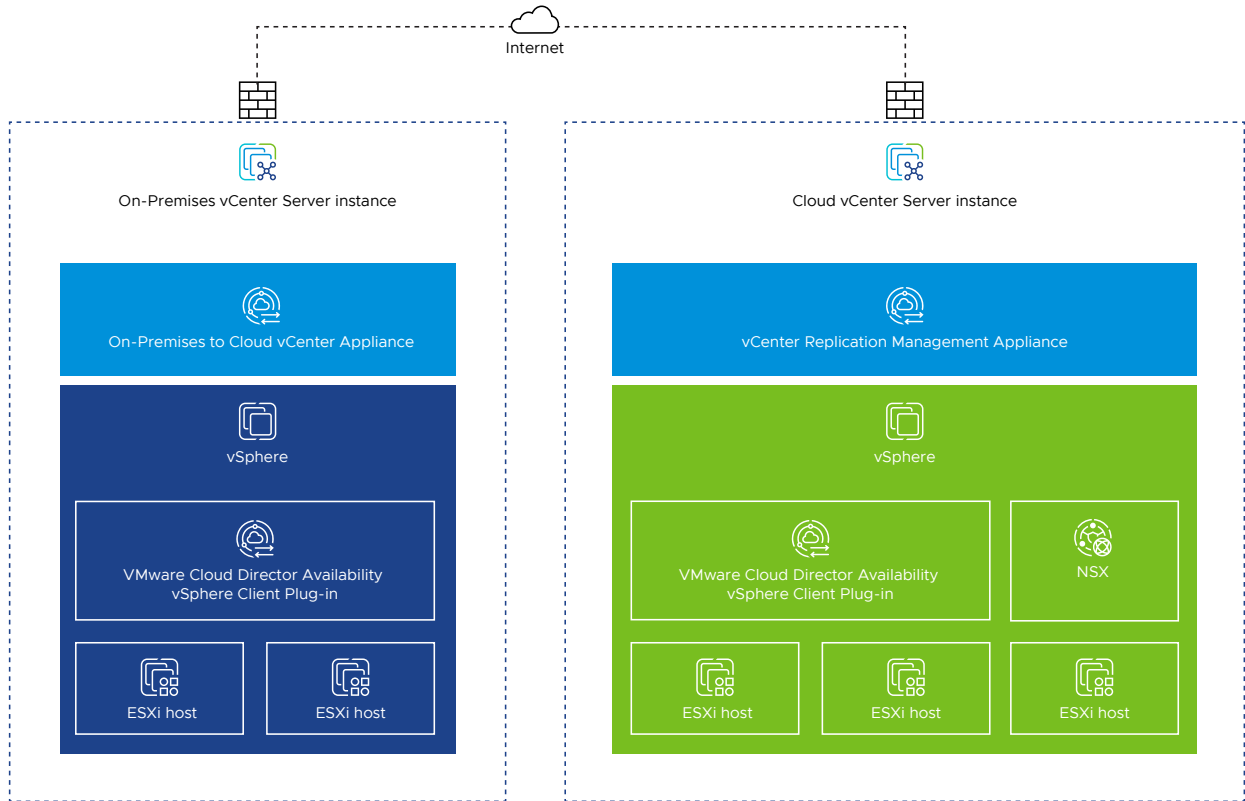
In the provider vCenter Server instance, as a vSphere **administrator** user deploy, license, and configure a vCenter Replication Management Appliance, then add it for metering in VMware vCloud® Usage Meter.

### 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.

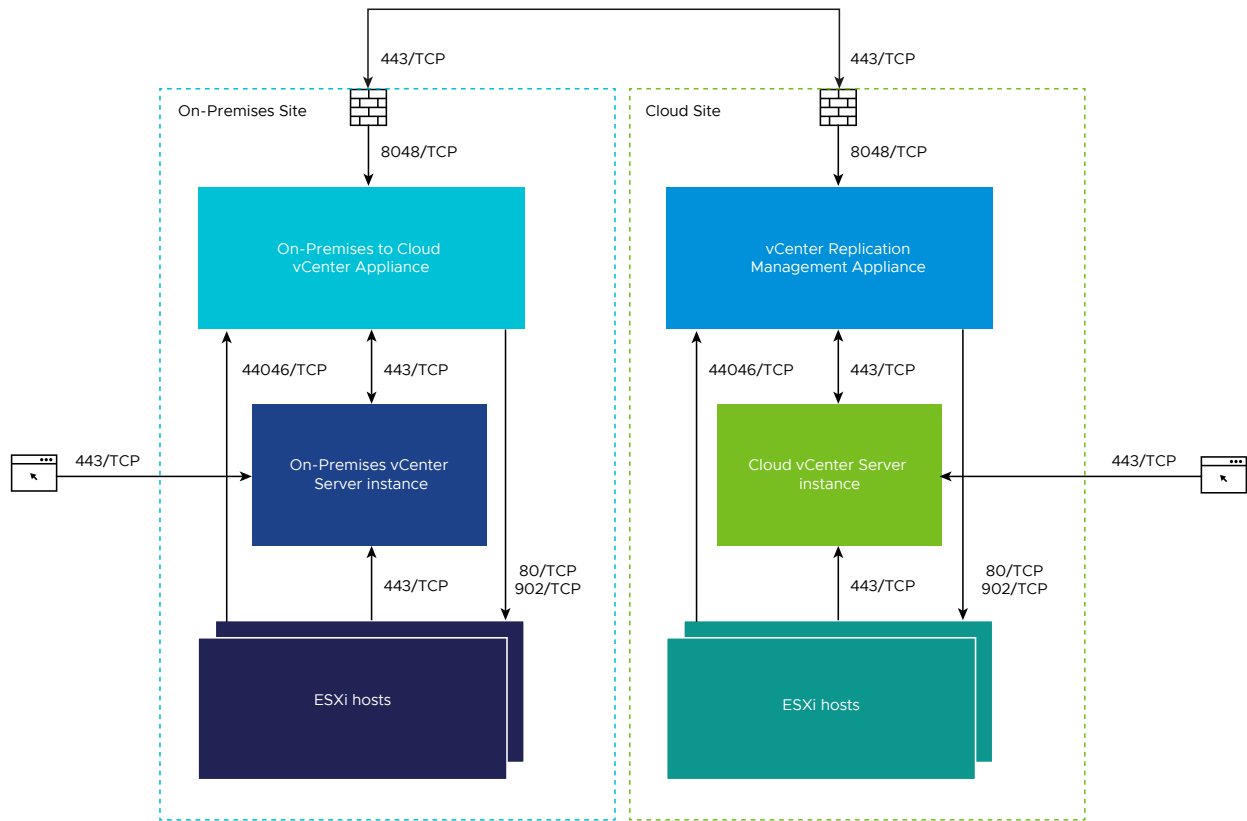
- For information about deploying both appliances in each vCenter Server instance, see [Deploy Both Appliances](#).
- For information about licensing, configuring, metering, and pairing the appliances, see [Configure and Pair Both Appliances](#).
- Alternatively, to replicate workloads between provider 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.

The following architecture diagram shows an On-Premises to Cloud vCenter Replication Appliance and a vCenter Replication Management Appliance, 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 3-1. 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 <b><i>Appliance-IP-address:8048</i></b> .	For <b>Service Endpoint</b> , enter the public <b><i>Service-Endpoint-IP-address:443</i></b> .

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, both appliances are virtual machines with the following hardware requirements.

- 8 vCPUs
- 8 GB RAM
- 10 GB Storage

## 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

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

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.
  - 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.

### Prerequisites

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

## Procedure

- ◆ In a provider vCenter Server instance, deploy a vCenter Replication Management Appliance.
  - a Log in to the provider vCenter Server instance by using the vSphere Client and authenticate as a vSphere **administrator** user.
  - b Navigate to a target object where you want to deploy the vCenter Replication Management Appliance.

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 **vCenter Replication Management Appliance** deployment configuration for the appliance type and click **Next**.

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**.

Option	Description
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	<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 both VMware Cloud Director Availability appliances all use the same NTP server.
Hostname	Enter the appliance hostname.
Address	Enter the IP address of the appliance.
Gateway	Enter the gateway of the appliance network.
MTU	Enter the maximum transmission unit of the network.
DNS servers	Enter DNS servers for the appliance network.
Search domains	Enter the search domains for the appliance network.

- 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 vSphere **administrator** 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 [Chapter 4 Installing and Configuring 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.

## Results

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

## Configure and Pair Both Appliances

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, initiate pairing from one of the appliances, then complete the pairing from the remote appliance.

### Prerequisites

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](#).

### Procedure

- 1 Repeat the following steps for each appliance and configure both appliances.
- 2 In a Web browser, go to **`https://On-Prem-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
Site name	<p>Enter a name for this site.</p> <p><b>Important</b> This site name is used as an identifier and cannot be changed later without impacting the active replications.</p>
Lookup Service Address	<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>
SSO Admin Username	<p>Enter the vSphere <b>administrator single sign-on (SSO)</b> 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>
Password	Enter the vSphere <b>administrator</b> user password for the vCenter Server Lookup service.

- a As a **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 a **provider**, before 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 does not require metering.

- 8 After configuring both appliances, pair them from each of the two sites, regardless which site initiates the pairing process.

**VRUSERS** can also access **Peer Sites** for pairing with the provider.

- First, initiate the pairing process from either of the sites.

- Then complete the pairing process in the remote site.

**Note** You can only pair either two vCenter Replication Management Appliance instances, or one vCenter Replication Management Appliance and one On-Premises to Cloud vCenter Replication Appliance.

Attempting to pair two On-Premises to Cloud vCenter Replication Appliance instances with each other show 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.`

- In the left pane, click **Peer Sites**.
- To initiate the pairing process, on the **Peer Sites** page, click **New pairing**.
- In the **New Pairing** window, configure the appliances pair and click **Pair**.

Option	Description
<b>Service Endpoint</b>	<ul style="list-style-type: none"> <li>■ Enter the address of the Service Endpoint : <b>443</b> of the remote appliance.</li> <li>■ Alternatively, enter port <b>8048</b> when both appliances reside in the same network.</li> </ul>
<b>Description</b>	Optionally, enter a description for this site as an identifier.

- In the **Additional Actions Required** window, to confirm going to the remote appliance interface for completing the pairing process click **OK**.
- In a Web browser, go to the address of the remote appliance and log in as the **root** user.
- In the left pane, click **Peer Sites**.
- To complete the already initiated pairing process, on the **Peer Sites** page, click **New pairing**.
- In the **New Pairing** window, configure the appliances pair and click **Pair**.

Option	Description
<b>Service Endpoint</b>	<ul style="list-style-type: none"> <li>■ Enter the address of the Service Endpoint : <b>443</b> of the remote appliance.</li> <li>■ Alternatively, enter port <b>8048</b> when both appliances reside in the same network.</li> </ul>
<b>Description</b>	Optionally, enter a description for this site as an identifier.

- Verify the thumbprint and accept the SSL certificate of the remote appliance.

Both appliances paired with each other and are ready to integrate with VMware vCloud® Usage Meter for metering. Then the two vCenter Server sites are ready for replications between each other.

## What to do next

After adding the vCenter Replication Management Appliance instances 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 a **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 more information, see the *User Guide*.

# Installing and Configuring On-Premises to Cloud Director Replication Appliance

## 4

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

- 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 [Chapter 4 Installing and Configuring On-Premises to Cloud Director Replication Appliance](#) chapter.

This chapter includes the following topics:

- [Deployment Architecture On-Premises](#)
- [Deployment Requirements On-Premises](#)
- [Deploying the On-Premises to Cloud Director Replication Appliance](#)
- [Configuring the On-Premises to Cloud Director Replication Appliance](#)

## Deployment Architecture On-Premises

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.

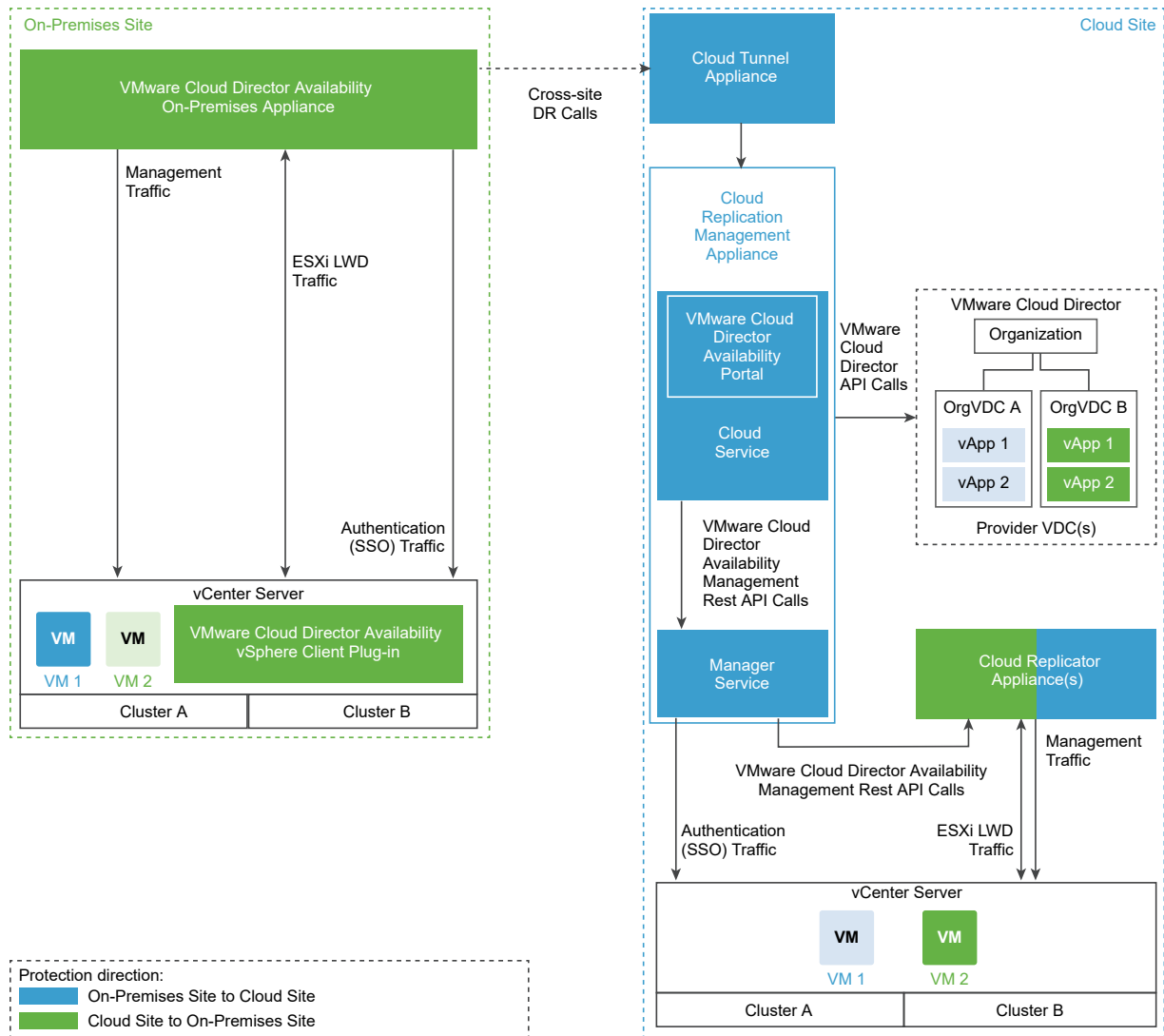
---

**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.



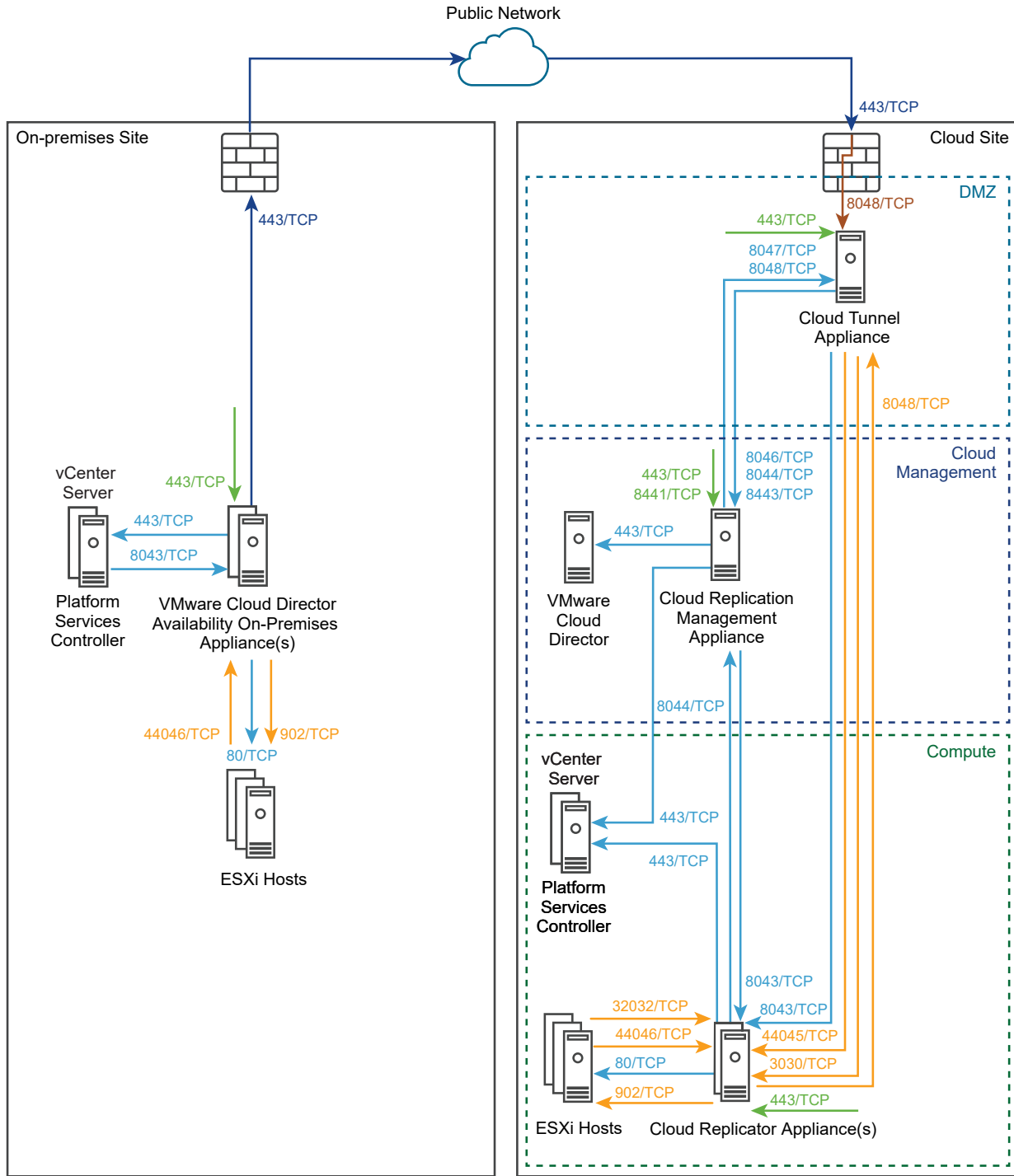
## Deployment Requirements On-Premises

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 Cloud 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.

- 4 vCPUs
- 4 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-yyyyyyyyy_OVF10.ova`, where `x.x.x` represents the product version and `yyyyyyyyy` 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.

### Prerequisites

- 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.

- 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.

#### Procedure

- 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 [Chapter 3 Installing and Configuring a vCenter Replication Management Appliance and an On-Premises to Cloud vCenter Replication Appliance](#).

- 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**.

- a Enter and confirm the initial password for the appliance **root** user.

When you log in for the first time, you must change the initial **root** user password.

- b Select the **Enable SSH** check box.

If you do not enable SSH, you can configure the appliance later. For more information to allow the SSH access, see the *Administration Guide* document.

- c In the **NTP Server** section, enter the NTP server address for the appliance to use.

---

**Important** In your disaster recovery environment, ensure that vCenter Server, ESXi, Platform Services Controller, VMware Cloud Director, and the VMware Cloud Director Availability appliance all use the same NTP server.

---

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

## Results

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.

### Defining the OVF Tool Parameters for 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 <b>Provider</b> or <b>On-Premises</b> .
VMNAME	Virtual machine name.
VSPHERE_DATASTORE	The VSPHERE_DATASTORE 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.

Parameter	Description
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>■ <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 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.

### Prerequisites

- 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 On-Premises](#).

### Procedure

- 1 Log in to a server where the OVF Tool is running, by using a Secure Shell (SSH) client.
- 2 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.

#### Prerequisites

- 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 Service Endpoint address from the cloud provider is obtained.

#### Procedure

- 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
Site name	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.
Description	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
Lookup Service Address	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.
SSO Admin Username	Enter the <b>single sign-on</b> user name for the vCenter Server Lookup service.
Password	Enter the <b>single sign-on</b> 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
Service Endpoint address	Enter the address of the cloud site's Service Endpoint:443 as provided by the cloud provider and press Tab, auto-completing the address as <code>https://Service Endpoint-IP-or-FQDN</code> .
Organization Admin	Enter the user name of a VMware Cloud Director <b>organization administrator</b> . For example, use <b>admin@org</b> .
Organization Password	Enter the <b>password</b> 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 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.

#### What to do next

If you skipped configuring local placement in the last step of the wizard, you can proceed with [Configure Local Placement](#).

## Configure Local Placement

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 [Chapter 3 Installing and Configuring a vCenter Replication Management Appliance and an On-Premises to Cloud vCenter Replication Appliance](#).

---

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

---

#### Procedure

- 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**.

#### Results

The **Placement to newly recovered VMs on this site** section expands, showing the placement configuration.

## What to do next

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 Service Endpoint of the cloud site and log in by using VMware Cloud Director **organization administrator** credentials.

# Upgrading On-Premises

# 5

After the cloud site is upgraded, you can upgrade the on-premises appliance. 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 the On-Premises to Cloud Director Replication Appliance.

## Upgrade Paths

To upgrade to the latest version of the On-Premises to Cloud Director Replication Appliance, use the following upgrade methods, according to the currently installed version.

Current Version	Next Version	Upgrade Method
4.2.x or 4.3.x	4.4.x	<ul style="list-style-type: none"><li>■ You can upgrade by using the on-premises appliance management interface, see the updated <a href="#">Management Interface Upgrading On-Premises</a> procedures.</li><li>■ Alternatively, you can upgrade by using the command-line interface, see the updated <a href="#">Command-Line Upgrading On-Premises</a> procedures.</li></ul>
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 on-premises appliance management interface, see the legacy <a href="#">Management Interface Upgrading On-Premises</a> procedures.</li><li>■ Alternatively, you can upgrade by using the command-line interface, see the legacy <a href="#">Command-Line Upgrading On-Premises</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.

\* To upgrade to the latest version, when performing a two-step upgrade from 4.1.x or from 4.0.x, use 4.2.1 as the intermediate upgrade. For more information, see the [Upgrade Path](#) of the On-Premises to Cloud Director Replication Appliance in the *VMware Product Interoperability Matrix*.

## Important

- Before upgrading the On-Premises to Cloud Director Replication Appliance:
  - 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 On-Premises](#).
- Attempting to upgrade from version 4.0.x directly to version 4.3 appears to proceed with the upgrade while performing no upgrade. The `/var/log/upgrade.log` file shows `Direct upgrades from 4.0.x are not supported! Upgrade to latest from 4.2 code line first and then you'll be able to upgrade to later versions.`

## Upgrade Repository

To upgrade VMware Cloud Director Availability on-premises, you can configure the On-Premises to Cloud Director Replication 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.vmware.com/vcav/4.4/</code> as an online upgrade repository.</li> </ul>

**Note** Cannot upgrade by selecting the option **Official Online Repository** in the management interface of versions 4.0.x since Apr 2021.

To upgrade by using their management interface, either select an ISO image or specify a repository.

This chapter includes the following topics:

- [Management Interface Upgrading On-Premises](#)
- [Command-Line Upgrading On-Premises](#)
- [Post-Upgrade Configuration On-Premises](#)

## Management Interface Upgrading On-Premises

To upgrade from VMware Cloud Director Availability 4.0, you can use the management interface of the On-Premises to Cloud Director Replication Appliance, select an upgrade repository, and follow the updated management interface upgrade procedures for the selected repository.

- If upgrading from version 4.0 or later, you can follow the updated procedures in the current chapter and use the On-Premises to Cloud Director Replication Appliance management interface for the upgrade. Alternatively, you can use the appliance command-line interface for the upgrade by following the updated [Command-Line Upgrading On-Premises](#) procedures.
- If upgrading from version 3.0.x to version 4.0, you can follow the legacy [Management Interface Upgrading On-Premises](#) procedures. Alternatively, you can follow the legacy [Command-Line Upgrading On-Premises](#) procedures.
- If upgrading from version 3.0 to version 4.0, you must follow the legacy [Command-Line Upgrading On-Premises](#) procedures.

## Upgrade VMware Cloud Director Availability On-Premises by Using the Default Repository

In the On-Premises to Cloud Director Replication Appliance management interface, you can upgrade from VMware Cloud Director Availability 4.1.1 and later versions to the latest version by using the default VMware repository.

Follow the updated procedure below only when upgrading from VMware Cloud Director Availability 4.1.1 and later versions. If you are upgrading to version 4.0, follow the legacy [Upgrade On-Premises by Using the Default Repository](#) procedure.

### Prerequisites

Verify that the On-Premises to Cloud Director Replication Appliance has an external Internet access to the VMware repository.

### Procedure

- 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, click **Configuration**.

- 3 Under **Version**, next to **Product version** click **Check for updates**.
- 4 Upgrade the On-Premises to Cloud Director Replication Appliance by completing the **Update** wizard.

---

**Note** Proceed with the upgrade only after taking a snapshot of the On-Premises to Cloud Director Replication Appliance.

---

- 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 **EULA Review** page, to accept the end-user license agreement click **Next**.
- e On the **Ready for update** page, click **Finish** and wait for the installation process to complete.

The On-Premises to Cloud Director Replication Appliance automatically restarts.

- 5 After the appliance restarts, verify that the upgrade is successful.

When the upgrade process finishes, in the left pane in **System Tasks**, you might see a red **Update** task that failed with messages like `Operation aborted due to an unexpected error` or `Task aborted due to service reboot`, while the upgrade is successful.

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

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

- c Verify that the upgrade log finishes with the following log entry.

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

#### What to do next

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 On-Premises](#).

## Upgrade VMware Cloud Director Availability On-Premises by Using a Specified Repository

In the On-Premises to Cloud Director Replication Appliance management interface, you can upgrade from VMware Cloud Director Availability 4.0 and later versions to the latest version by specifying an online or a local repository that contains the upgrade binaries.

Follow the updated procedure below only when upgrading from VMware Cloud Director Availability 4.0 and later versions. If you are upgrading to version 4.0, follow the legacy [Upgrade On-Premises by Using a Specified Repository](#) procedure. For information about the upgrade in the on-premises site, see [Chapter 5 Upgrading On-Premises](#).

### Prerequisites

Verify that the On-Premises to Cloud Director Replication Appliance has a network access to the specified repository.

### Procedure

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

- 5 Upgrade the On-Premises to Cloud Director Replication Appliance by completing the **Update** wizard.

---

**Note** Proceed with the upgrade only after taking a snapshot of the On-Premises to Cloud Director Replication Appliance.

---

- a On the **Repository** page, select **Use Specified Repository**.
- b On the **Repository URL** text box, specify the repository URL address and click **Next**.
  - If the appliance has Internet access, enter the following URL and specify the target version `https://packages.vmware.com/vcav/4.4`.
  - 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 and click **Next**.
- d On the **Release notes** page, read the notes for this release and click **Next**.
- e On the **EULA Review** page, to accept the end-user license agreement click **Next**.
- f On the **Ready for update** page, click **Finish** and wait for the installation process to finish.

The On-Premises to Cloud Director Replication Appliance automatically restarts.

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

When the upgrade process finishes, in the left pane in **System Tasks**, you might see a red **Update** task that failed with messages like `Operation aborted due to an unexpected error` or `Task aborted due to service reboot`, while the upgrade is successful.

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

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

- c Verify that the upgrade log finishes with the following log entry.

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

#### What to do next

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 On-Premises](#).



## Upgrade VMware Cloud Director Availability On-Premises by Using an ISO Image

In the On-Premises to Cloud Director Replication Appliance management interface, you can upgrade from VMware Cloud Director Availability 4.0 and later versions 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 the updated procedure below only when upgrading from VMware Cloud Director Availability 4.0 and later versions. If you are upgrading to version 4.0, follow the legacy [Upgrade On-Premises by Using an ISO Image](#) procedure.

### Prerequisites

- 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.

### Procedure

- 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 On-Premises to Cloud Director Replication Appliance.
  - a Log in to the on-premises vCenter Server by using the vSphere Client.
  - b Locate the virtual machine that hosts the On-Premises to Cloud Director Replication 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 virtual machine and select the **Connected** option.
- 3 By using the virtual appliance console, mount the `.iso` file inside the guest operating system of the On-Premises to Cloud Director Replication Appliance.
  - a Connect to the appliance console either by using a Secure Shell (SSH) client or by using the appliance console in the vSphere Client and log in as the **root** user.
  - b Mount the `.iso` file inside the guest operating system of the On-Premises to Cloud Director Replication 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 **Configuration**.
- 6 Under **Version**, next to **Product version** click **Check for updates**.
- 7 Upgrade the On-Premises to Cloud Director Replication Appliance by completing the **Update** wizard.

---

**Note** Proceed with the upgrade only after taking a snapshot of the On-Premises to Cloud Director Replication Appliance.

---

- a On the **Repository** page, select **Use CDROM Updates** and click **Next**.
- b On the **Available updates** page, select an update and click **Next**.
- c On the **EULA Review** page, to accept the end-user license agreement click **Next**.
- d On the **Ready for update** page, click **Finish** and wait for the installation process to finish.

- 8 After the upgrade finishes, verify that the upgrade is successful On-Premises to Cloud Director Replication Appliance.

When the upgrade process finishes, in the left pane in **System Tasks**, you might see a red **Update** task that failed with messages like `Operation aborted due to an unexpected error` or `Task aborted due to service reboot`, while the upgrade is successful.

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

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

- c Verify that the upgrade log finishes with the following log extract.

- When starting the upgrade from version 4.0.x, the appliance automatically restarts.

```
Complete!
Nothing left to do.
...
The upgrade was successful! Scheduling reboot in 15 seconds..
```

- When starting the upgrade from version 4.0.0.x, after the upgrade finishes you must restart the appliance.

```
Complete!
Verifying... #####
Preparing... #####
    package filesystem-1.1-4.ph3.x86_64 is already installed
Bad exit code: 256
{
  "code": "BadExitCode",
  "msg": "",
  "args": [
    "256"
  ]
}
```

After you see this upgrade log extract, restart the appliance.

```
reboot
```

- 9 Unmount the `.iso` file.

- a In the vSphere Client, shut down the virtual machine that hosts the On-Premises to Cloud Director Replication Appliance.
- b Right-click the virtual machine and select **Edit Settings**.

- c In the **Virtual Hardware** tab, select **CD/DVD Drive** and deselect **Connected** and **Connect At Power On**.
- d Power on the virtual machine that hosts the On-Premises to Cloud Director Replication Appliance.

#### What to do next

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 On-Premises](#).

## Command-Line Upgrading On-Premises

To upgrade from VMware Cloud Director Availability 4.0 by using the command-line interface of the On-Premises to Cloud Director Replication Appliance, select an upgrade repository, and follow the updated command-line procedures for the selected repository.

- If upgrading from version 4.0 or later, you can follow the updated procedures in the current chapter and use the On-Premises to Cloud Director Replication Appliance command-line interface for the upgrade. Alternatively, you can use the appliance management interface for the upgrade by following the updated [Management Interface Upgrading On-Premises](#) procedures.
- If upgrading from version 3.0.x to version 4.0, you can follow the legacy [Management Interface Upgrading On-Premises](#) procedures. Alternatively, you can follow the legacy [Command-Line Upgrading On-Premises](#) procedures.
- If upgrading from version 3.0 to version 4.0, you must follow the legacy [Command-Line Upgrading On-Premises](#) procedures.

## Command-Line Upgrade On-Premises by Using an ISO Image

From the On-Premises to Cloud Director Replication 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.

To upgrade to the latest VMware Cloud Director Availability version, follow this updated procedure below. If you are upgrading to VMware Cloud Director Availability 4.0 or earlier versions, follow the legacy [Command-Line Upgrade On-Premises by Using an ISO Image](#) procedure.

#### Prerequisites

- 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.

**Procedure**

- 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 On-Premises to Cloud Director Replication 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 On-Premises to Cloud Director Replication Appliance and select **Edit Settings**.
  - d On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
  - e Follow the prompts and add the CD/DVD drive to the virtual machine and select the **Connected** option.
- 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 On-Premises to Cloud Director Replication Appliance.

---

**Note** Proceed with the upgrade only after taking a snapshot of the On-Premises to Cloud Director Replication 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 `Complete!` both in the console and in the `/var/log/upgrade.log` file.

- d After the upgrade completes, restart the appliance.

```
reboot
```

## What to do next

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 On-Premises](#).

## Post-Upgrade Configuration On-Premises

After upgrading the On-Premises to Cloud Director Replication Appliance, complete the upgrade by reconfiguring the on-premises appliance with the vCenter Server Lookup service.

### Procedure

- 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 On-Premises to Cloud Director Replication 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**.
- 3 After upgrading to version 4.2 or later, uninstall the version 4.1.0 of VMware Cloud Director Availability vSphere Client Plug-In.
  - a Log in to the vSphere Client as a vCenter Server **Administrator** user.
  - b In the vSphere Client home page, click **Administration > Solutions > Client Plugins**.
  - c Select and deactivate the VMware Cloud Director Availability plug-in version 4.1.0.

---

**Note** The VMware Cloud Director Availability On-Premises Plug-in with the current version remains active, deployed, and ready for use.

---

### Results

The On-Premises to Cloud Director Replication Appliance is successfully upgraded and you can configure new replications. For more information, see the *User Guide*.