

Installation, Configuration, and Upgrade Guide On-Premises

23 NOV 2021

VMware Cloud Director Availability 4.3

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

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

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

Copyright © 2018-2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	VMware Cloud Director Availability Overview On-Premises	4
2	Deployment Architecture On-Premises	5
3	Installing and Configuring VMware Cloud Director Availability On-Premises Appliance	7
	Deployment Requirements On-Premises	7
	Interoperability and vSphere Product Edition	10
	Deploying the VMware Cloud Director Availability On-Premises Appliance	11
	Deploy the VMware Cloud Director Availability On-Premises Appliance by Using the vSphere Client	11
	Deploying by Using the VMware OVF Tool	13
	Configuring the VMware Cloud Director Availability On-Premises Appliance	15
	Configure the VMware Cloud Director Availability On-Premises Appliance	15
	Configure Local Placement	17
4	Upgrading On-Premises	19
	Management Interface Upgrading On-Premises	21
	Upgrade VMware Cloud Director Availability On-Premises by Using the Default Repository	21
	Upgrade VMware Cloud Director Availability On-Premises by Using a Specified Repository	22
	Upgrade VMware Cloud Director Availability On-Premises by Using an ISO Image	24
	Command-Line Upgrading On-Premises	27
	Command-Line Upgrade On-Premises by Using an ISO Image	27
	Post-Upgrade Configuration On-Premises	29

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

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

- 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.
- 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.
- A single-site VMware Cloud Director Availability can migrate virtual machines and vApps between Virtual Data Centers belonging to a single VMware Cloud Director organization.
- 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.

Deployment Architecture On-Premises

2

To protect or migrate vSphere workloads between cloud sites and on-premises vCenter Server, deploy one or multiple VMware Cloud Director Availability On-Premises 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.

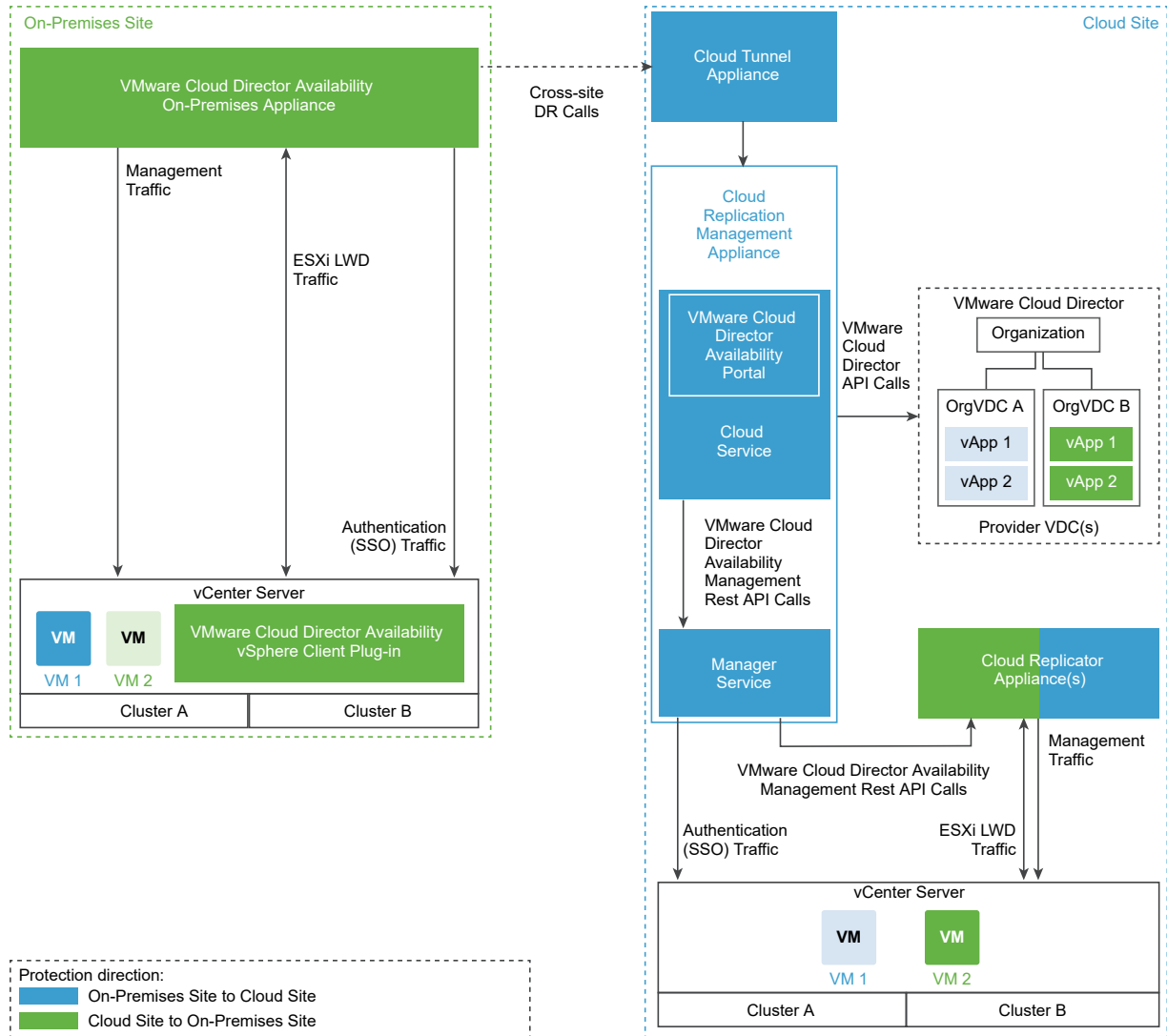
On-premises Appliance Deployment

In the on-premises site, deploy and configure one or more VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance installation and configuration procedures.

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



Installing and Configuring VMware Cloud Director Availability On-Premises Appliance

3

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 VMware Cloud Director Availability On-Premises Appliance role.

This chapter includes the following topics:

- [Deployment Requirements On-Premises](#)
- [Interoperability and vSphere Product Edition](#)
- [Deploying the VMware Cloud Director Availability On-Premises Appliance](#)
- [Configuring the VMware Cloud Director Availability On-Premises Appliance](#)

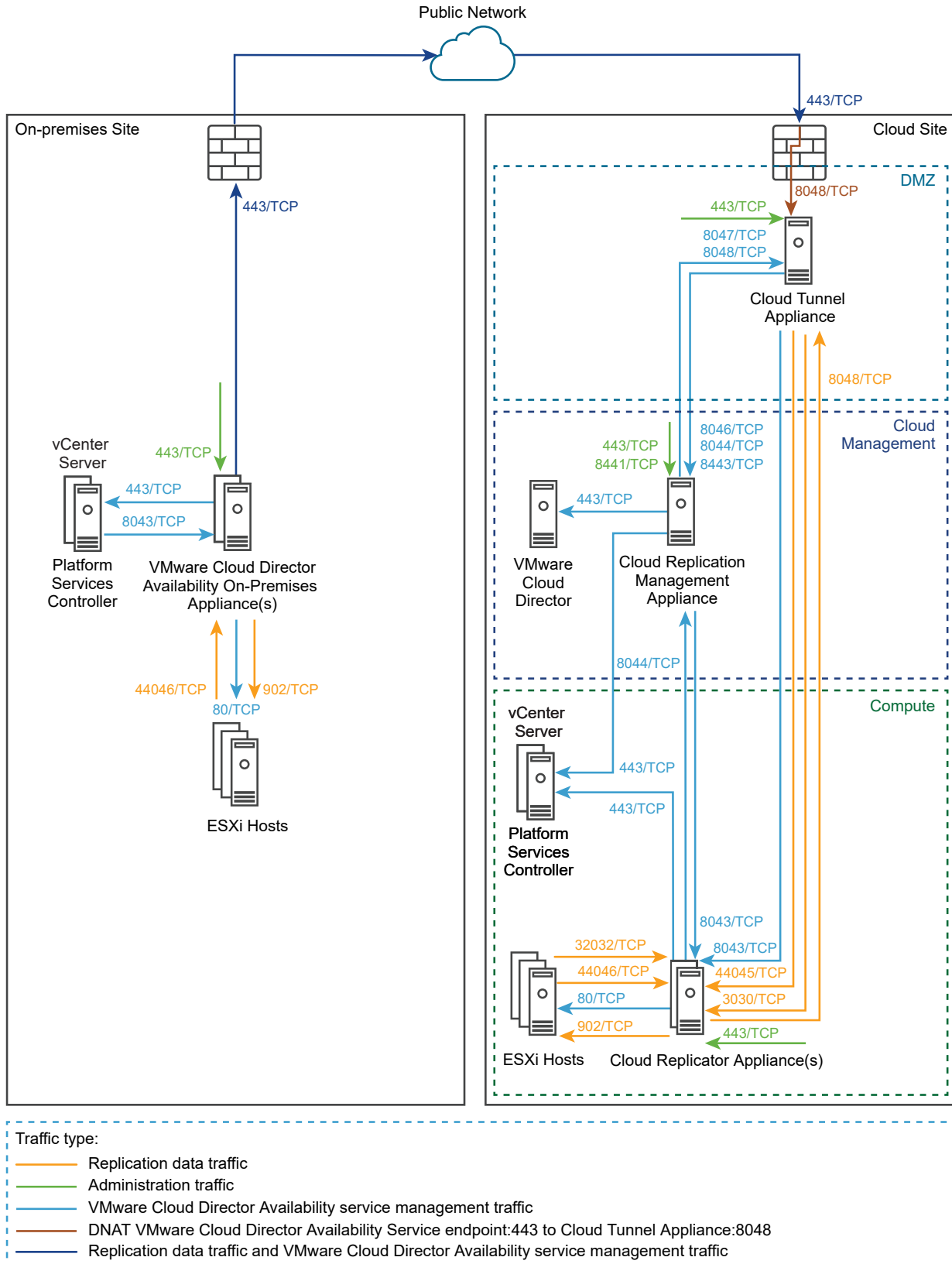
Deployment Requirements On-Premises

Before installing the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance and the disaster recovery infrastructure.



Connectivity Requirements

The VMware Cloud Director Availability appliances must be able to communicate with each other and with the disaster recovery infrastructure. The VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance to the same virtual port group. Using this configuration, the replication traffic between the ESXi hosts and the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance with the vCenter Server Lookup service, provided by the Platform Services Controller used by the resource vCenter Server instances.

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 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, see [Managing Connections Between Cloud Sites](#) in the *Administration Guide*.

Deploying the VMware Cloud Director Availability On-Premises Appliance

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

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

The appliance is distributed with a name of 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.

Deploy the VMware Cloud Director Availability On-Premises Appliance by Using the vSphere Client

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

Prerequisites

- Download the `VMware-Cloud-Director-Availability-On-Premises-release.number.xxxxxx-build_sha_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 **Select storage** page, select the virtual disk format and the storage policy for the appliance and click **Next**.
- 10 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.
- 11 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.

12 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 Provider or On-Premises .
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.
VSPHERE_LOCATOR	<p>The <code>VSPHERE_LOCATOR</code> 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 <code>VSPHERE_LOCATOR</code> value depends on the topology of your vSphere environment. Following are examples for valid <code>VSPHERE_LOCATOR</code> values.</p> <ul style="list-style-type: none"> ■ <code>/data-center-name/host/cluster-1-name/ESXi-host-fully-qualified-domain-name</code> ■ <code>/data-center-name/host/cluster-2-name/ESXi-host-IP-address</code> <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"> ■ <code>/data-center-name/host/ESXi-host-fully-qualified-domain-name</code> ■ <code>/data-center-name/host/ESXi-host-IP-address</code> <p>For more information about the <code>VSPHERE_LOCATOR</code> value, run the <code>./ovftool --help locators</code> command.</p>

Deploy the VMware Cloud Director Availability On-Premises Appliance by Using the OVF Tool

In the VMware OVF Tool console, you can deploy a VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.

The following example script deploys a VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.

Configuring the VMware Cloud Director Availability On-Premises Appliance

After deploying the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance

To configure the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance is installed and powered on. For more information, see [Deploying the VMware Cloud Director Availability On-Premises 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 **Run initial setup wizard**.

The **Initial Setup** wizard opens.

- 5 On the **Site Details** page, enter a **Site Name**, optionally enter a **Site Description**, and click **Next**.

Important The site name is used as an identifier and cannot be changed later without impacting the active replications.

- 6 Optionally, to bypass pairing with the cloud site select **Provide cloud pairing details later** and skip to step 10.

- 7 On the **Lookup Service Details** page, enter the vCenter Server Lookup service details and click **Next**.

- a In the **Lookup Service Address** text box, enter the IP address or the FQDN of the vCenter Server Lookup service.

Note To use the VMware Cloud Director Availability vSphere Client Plug-In without errors, when navigating to the on-premises vSphere Client, use the same method as configured in the **Lookup Service Address** text box - an IP address or an FQDN.

- b Enter the **single sign-on** user credentials for the vCenter Server Lookup service.

- 8 Verify the thumbprint and accept the SSL certificate of the vCenter Server Lookup service and click **Next**.

- 9 On the **Cloud Details** page, pair the on-premises VMware Cloud Director Availability appliance and the cloud provider.

- a Enter the Service Endpoint address, provided by the cloud provider.
- b Enter the VMware Cloud Director **admin@org** organization user credentials.
- c (Optional) Select **Allow Access from Cloud**.

By selecting this option, you allow 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:

- Discover on-premises workloads and replicate them to the cloud.
- Reverse existing replications to the on-premises site.
- Replicate cloud workloads to the on-premises site.

By leaving this option deselected, only users authenticated to the on-premises VMware Cloud Director Availability Tenant Portal can configure new replications and existing replications cannot be reversed from the VMware Cloud Director Availability Tenant Portal.

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

- 10 On the **Ready to complete** page, optionally select to configure the local placement, and to complete the initial setup wizard click **Finish**.

- You can configure on-premises to cloud replications and you can leave **Edit / configure local placement now** deselected.
- To enable the cloud to on-premises replications, select **Edit / configure local placement now**.

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 if you skipped **Configure local placement now** during the initial setup wizard of the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 details**, 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 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 network that the virtual machines connect to after their failover and click **Next**.

If you skip to select a network, the incoming virtual machine replications are recovered with their NICs 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 virtual machines and their disk files and click **Next**.

Datastore clusters are not supported for the on-premises local placement and the clusters are not listed to select.
 - e On the **Ready To Complete** page, verify that the selected configuration is correct and click **Finish**.

Results

To view the placement setup summary, expand the **Placement to newly recovered VMs on this site** section.

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 your vCenter Server by using vSphere Client, authenticate with the Single Sign-On administrator credentials and access the on-premises VMware Cloud Director Availability plugin. For more information, see the *User Guide* document.
- Navigate to the cloud portal Service Endpoint and log in by using the organization administrator credentials.

Upgrading On-Premises

4

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 VMware Cloud Director Availability On-Premises Appliance.

Upgrade Paths

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

Current Version	Next Version	Upgrade Method
4.1.1 or 4.2.1	4.3.x	<ul style="list-style-type: none">■ You can upgrade by using the on-premises appliance management interface, see the updated Management Interface Upgrading On-Premises procedures.■ Alternatively, you can upgrade by using the command-line interface, see the updated Command-Line Upgrading On-Premises procedures.
4.0.x	4.2.1	
3.0.x or 3.5.x	4.0	<ul style="list-style-type: none">■ You can upgrade by using the on-premises appliance management interface, see the legacy Management Interface Upgrading On-Premises procedures.■ Alternatively, you can upgrade by using the command-line interface, see the legacy Command-Line Upgrading On-Premises procedures.
3.0	4.0	You must upgrade only by using the command-line interface, see the legacy Command-Line Upgrading On-Premises procedures.

For more information, see the [Upgrade Path](#) of the VMware Cloud Director Availability On-Premises Appliance in the *VMware Product Interoperability Matrix*.

Important

- Before upgrading the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance to download the upgrade files from one of the following source repositories.

| Repository             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An ISO image           | Use an upgrade ISO file mounted in the virtual appliance CD-ROM drive for environments without an external 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.vmware.com/vcav/4.3.1/</code> as an online upgrade repository.</li> </ul> |

**Note** Cannot upgrade by selecting **Official Online Repository** from versions 4.0.x since Apr 2021. To upgrade by using the management interface, use 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance has an external Internet access to the VMware repository.

### Procedure

- 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-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 VMware Cloud Director Availability On-Premises Appliance by completing the **Update** wizard.

---

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

---

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

The VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 bellow 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 4 Upgrading On-Premises](#).

## Prerequisites

Verify that the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance by completing the **Update** wizard.

---

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

---

- a In the **Repository** page, select **Use Specified Repository**.
- b In 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/4.3`.
  - 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 In the **Available updates** page, select an update and click **Next**.
- d In the **EULA Review** page, to accept the end-user license agreement click **Next**.
- e In the **Ready for update** page, click **Finish** and wait for the installation process to finish.

The VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.
  - a Log in to the on-premises vCenter Server by using the vSphere Client.
  - b Locate the virtual machine that hosts the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.

```
mount /mnt/cdrom
```

- 4 Log in to the management interface of the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance by completing the **Update** wizard.

---

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

---

- a In the **Repository** page, select **Use CDROM Updates** and click **Next**.
- b In the **Available updates** page, select an update and click **Next**.
- c In the **EULA Review** page, to accept the end-user license agreement click **Next**.
- d In 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.

#### What to do next

After you upgrade the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises Appliance command-line 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.

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 VMware Cloud Director Availability On-Premises 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 On-Premises 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 VMware Cloud Director Availability On-Premises Appliance.

---

**Note** Proceed with the upgrade only after taking a snapshot of the VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 the VMware Cloud Director Availability plug-in version 4.1.0 and click **Disable**.

---

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

---

### Results

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