VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide in the Cloud

10 JUN 2021

VMware Cloud Director Availability 4.2

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

https://docs.vmware.com/

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

Contents

1 VMware Cloud Director Availability Overview in the Cloud 4

2 Deployment Architecture in the Cloud 6

3 Services 12

4 Installing and Configuring the Cloud Appliances 14

- Installation Requirements in the Cloud 14
  - Interoperability 14
  - Deployment Requirements 15
  - Network Requirements 18
  - Users Requirements 21
- Deploying in the Cloud 22
  - Deploy the Cloud Appliances by Using the vSphere Client 22
  - Deploying by Using the VMware OVF Tool 24
- Configuring the Cloud Appliances 26
  - Configure the Cloud Service 27
  - Add an Additional Replicator Service Instance 30
- Customer Experience Improvement Program 33
  - Categories of Information That VMware Receives 33
  - Join or Leave the Customer Experience Improvement Program 33

5 Upgrading in the Cloud 35

- Upgrade Sequence 36
- Management Interface Upgrading 37
  - Upgrade by Using the Default Repository 38
  - Upgrade by Using a Specified Repository 40
  - Upgrade by Using an ISO Image 42
- Command-Line Upgrading 45
  - Command-Line Upgrade by Using an ISO Image 45
- Post-Upgrade Configuration in the Cloud 47

VMware Cloud Director Availability Overview in the Cloud

1

The VMware Cloud Director Availability™ solution provides replication and failover capabilities for VMware Cloud Director™ and vCenter Server workloads at both 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:

- A single-cloud site supports multiple-tenants.
- 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.
- Single installation package as a Photon-based virtual appliance.
- 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 Cloud Replicator 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.

- A single installation package, distributed as a Photon-based virtual appliance to deploy all VMware Cloud Director Availability components.

Deployment Architecture in the Cloud

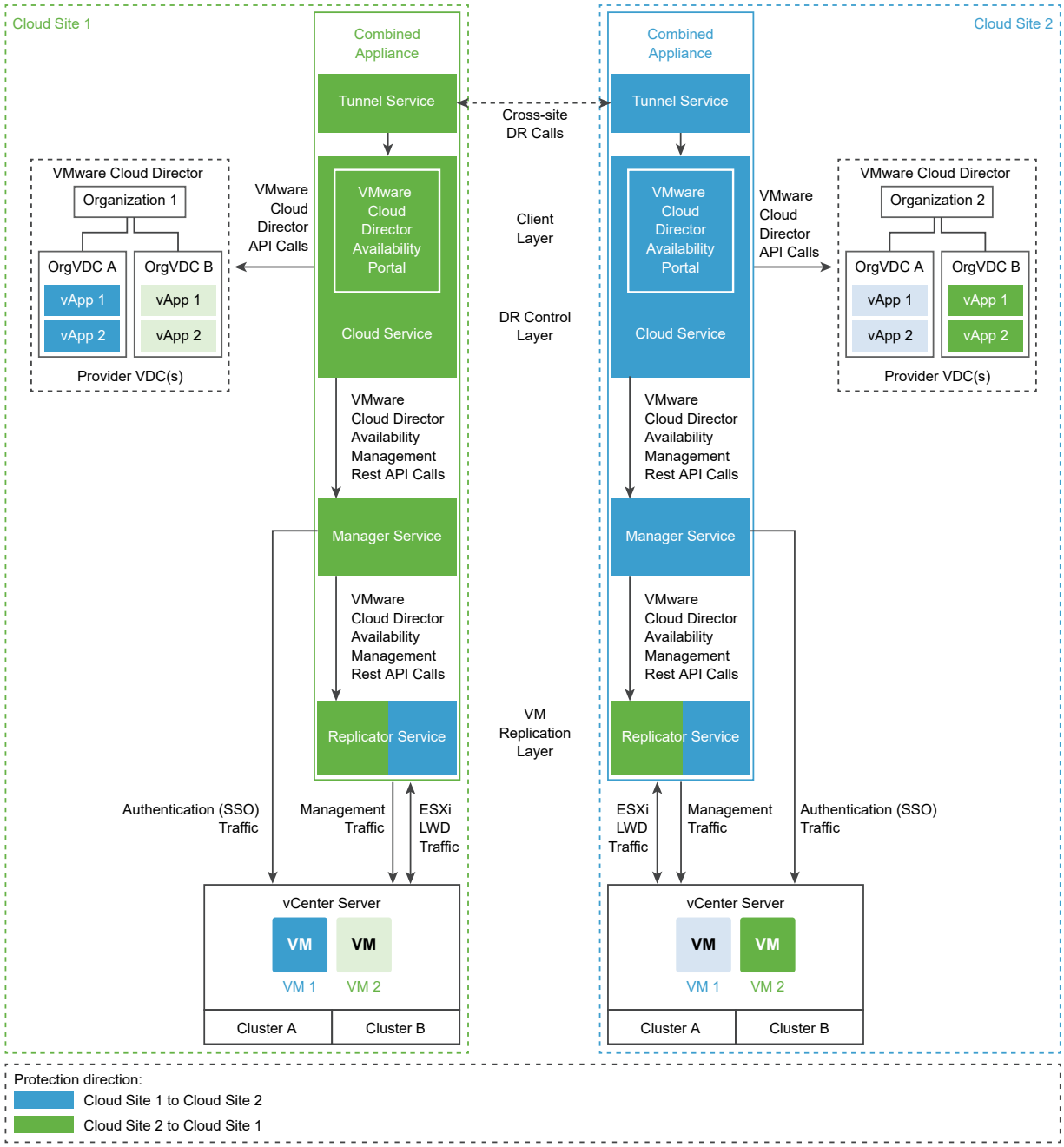
2

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

Test and Development Deployment

In a test and a development VMware Cloud Director site, you can deploy a minimal setup. In the test cloud site, a single Combined Appliance instance can run all the four main VMware Cloud Director Availability services:

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



In the diagram:

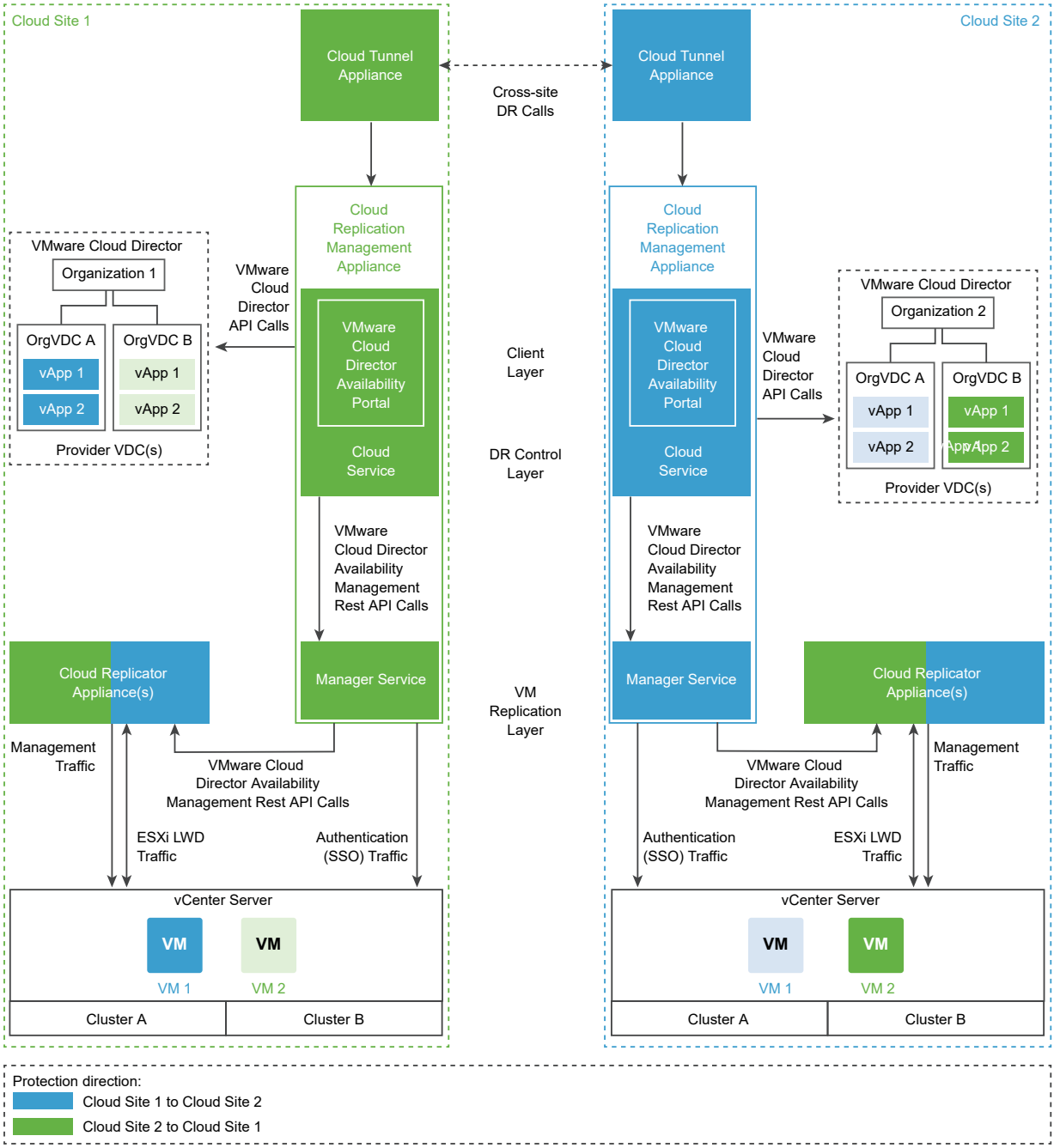
- The colored components inside the two Combined Appliance instances represent the VMware Cloud Director Availability services, deployed during the installation and the initial configuration of the appliances.
- Each component has the color of the replication direction it manages. For example, the protected Organization VDC B vApps and VM 2 from Cloud Site 1 to Cloud Site 2 use the Cloud Site 2 Replicator Service.

- Each replication resides in its destination site. For example, the protections from Cloud Site 1 to Cloud Site 2 reside in Cloud Site 2.
- The components with no color represent existing components in the VMware Cloud Director sites.

Production Deployment

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

- A single Cloud Tunnel Appliance, running the Tunnel Service.
- A single Cloud Replication Management Appliance, running the Cloud Service and the Manager Service.
- One or more Cloud Replicator Appliance instances, each running a Replicator Service instance.



For information about the network connectivity between the services and between the sites, see Network Requirements and for information about each service, see Chapter 3 Services.

Deploying Multiple VMware Cloud Director Availability Instances in VMware Cloud Director

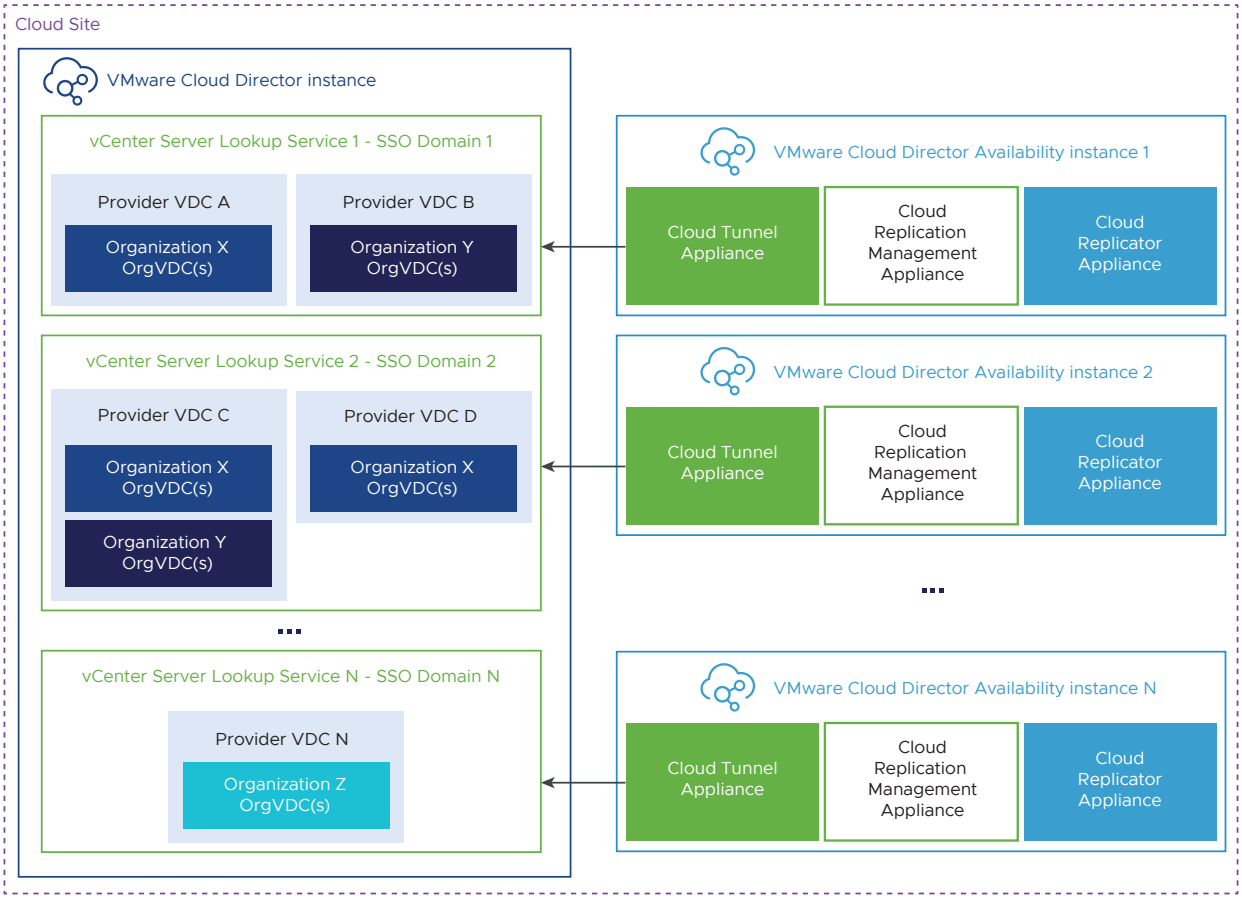
In a production cloud site, you can deploy one or more VMware Cloud Director Availability instances, distributed in provider VDCs.

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

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

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

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



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

Services

3

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

Table 3-1. VMware Cloud Director Availability Services

Service Name	Service Description
Replicator Service	Exposes the low-level Host Based Replication (HBR) primitives as REST API calls.
Manager Service	A management service operating with vCenter Server-level concepts for managing the replication workflow.
Cloud Service with an embedded VMware Cloud Director Availability Tenant Portal	Provides the main interface for replication operations and operates with VMware Cloud Director-level concepts and works with vApps and virtual machines. The embedded VMware Cloud Director Availability Tenant Portal provides the tenants and the service providers of the VMware Cloud Director Availability Provider Portal with a graphic user interface to operate with VMware Cloud Director Availability.
Tunnel Service	The single point that channels all the site traffic: both management and replication data (LWD) traffic.

For information about the VMware Cloud Director Availability appliances, see Deployment Requirements.

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

You perform an initial configuration by using the Manager Service, the Replicator Service, and the Cloud Service service management interfaces. After VMware Cloud Director Availability is deployed and configured, tenants can access the VMware Cloud Director Availability Tenant Portal. For information about the network connectivity between the services, see Network Requirements and for diagrams showing all services in the cloud site and a diagram showing multiple VMware Cloud Director Availability instances, see Chapter 2 Deployment Architecture in the Cloud.

Table 3-2. Replication Services

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

Table 3-3. External Components

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

For information on which VMware Cloud Director Availability appliance each service operates, see Services and Ports in the *VMware Cloud Director Availability Security Guide*.

Installing and Configuring the Cloud Appliances

4

First you deploy the VMware Cloud Director Availability appliances. Then you perform an initial configuration of the Cloud Replication Management Appliance appliance to register with all the components in the disaster recovery infrastructure.

This chapter includes the following topics:

- Installation Requirements in the Cloud
- Deploying in the Cloud
- Configuring the Cloud Appliances
- Customer Experience Improvement Program

Installation Requirements in the Cloud

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

Interoperability

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

You can pair sites that have mismatching VMware Cloud Director Availability versions deployed. For more 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 *VMware Cloud Director Availability Administration Guide*.

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.

Deployment Requirements

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

Deployment Types and Hardware Requirements

In all cloud sites backed by VMware Cloud Director, deploy all cloud appliances of VMware Cloud Director Availability by using a single installation `OVA` file. For information about the cloud appliances location in the disaster recovery infrastructure, see Chapter 2 Deployment Architecture in the Cloud.

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

Table 4-1. Cloud Appliances of VMware Cloud Director Availability

Cloud Appliance Type	Description and Services	Hardware Requirements
Cloud Replication Management Appliance	**Important** As a **provider**, before configuring any replications you must add each instance of Cloud Replication Management Appliance for metering in VMware vCloud® Usage Meter. For information about adding the appliances in vCloud Usage Meter, see vCloud Usage Meter Integration. A dedicated cloud appliance, that runs the following VMware Cloud Director Availability services: ■ Manager Service ■ Cloud Service with embedded VMware Cloud Director Availability Tenant Portal Deploy the Cloud Replication Management Appliance for configuring replications from and to VMware Cloud Director.	■ 2 vCPUs ■ 4 GB RAM ■ 10 GB Storage
Cloud Replicator Appliance	A dedicated cloud appliance for the Replicator Service that handles the replication traffic for a site. For large-scale environments, you can deploy more than one Cloud Replicator Appliance per cloud site.	■ 4 vCPUs ■ 6 GB RAM ■ 10 GB Storage
Cloud Tunnel Appliance	A dedicated cloud appliance for the Tunnel Service.	■ 2 vCPUs ■ 4 GB RAM ■ 10 GB Storage
Combined Appliance	An all-in-one cloud appliance deployment type, only suitable for testing and evaluation environments. The Combined Appliance includes all VMware Cloud Director Availability services: ■ Manager Service ■ Replicator Service ■ Cloud Service with embedded VMware Cloud Director Availability Tenant Portal ■ Tunnel Service	■ 4 vCPUs ■ 6 GB RAM ■ 10 GB Storage

For information about each service, see Chapter 3 Services and for the network connectivity between the services, see Network Requirements.

Deployment Requirements

Deploying VMware Cloud Director Availability in a cloud site backed by VMware Cloud Director requires:

- **Resource vCenter Server Lookup service**

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

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

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

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

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

  For information about deploying multiple instances, see Deploying Multiple VMware Cloud Director Availability Instances in VMware Cloud Director.

- **Certificate of VMware Cloud Director**

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

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

  VMware Cloud Director vApps discovery and adoption must not be active. For more information, see Discovering and Adopting vApps in the VMware Cloud Director documentation.

- **Dedicated ESXi replication VMkernel interfaces**

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

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

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

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

VMware Cloud Director Availability Storage Requirements

For a test failover, the destination storage always must accommodate double the space for the disk size of the source virtual machine during the test failover. Since VMware Cloud Director Availability 4.2, for a failover this does not apply and the storage space equals the source workload size during the failover.

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

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

Supported Topologies

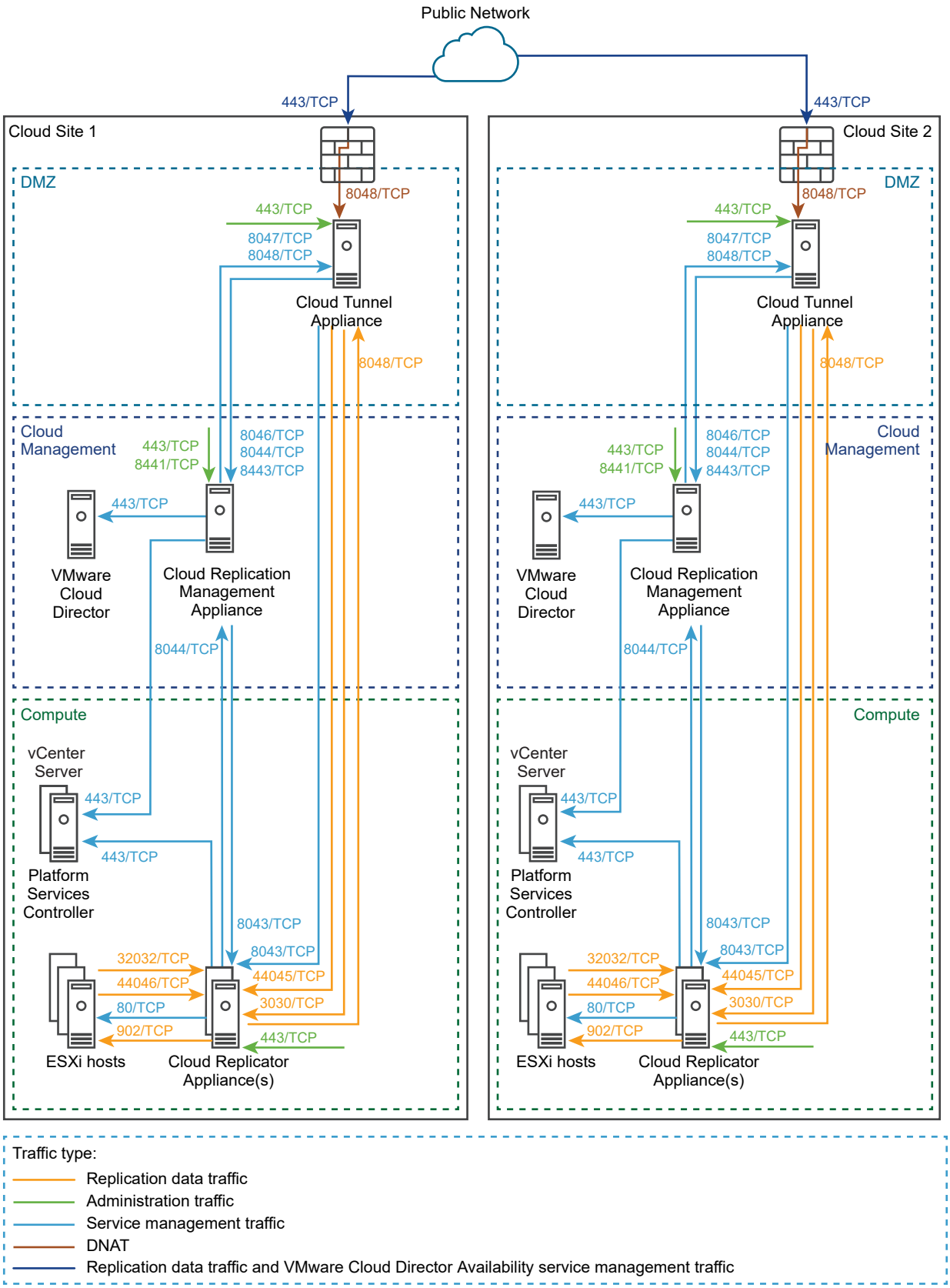
The resource vCenter Server instances within a cloud site backed by VMware Cloud Director must be within the same single sign-on (SSO) domain. All Replicator Service, Manager Service, Cloud Service, and Tunnel Service instances within the respective site must be configured with that same SSO domain. For diagrams showing all services in the cloud site and a diagram showing multiple VMware Cloud Director Availability instances, see Chapter 2 Deployment Architecture in the Cloud.

Network Requirements

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

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

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


Public Network
443/TCP
443/TCP
Cloud Site 1
Cloud Site 2
DMZ
DMZ
8048/TCP
8048/TCP
443/TCP
443/TCP
8047/TCP
8048/TCP
8047/TCP
8048/TCP
Cloud Tunnel Appliance
Cloud Tunnel Appliance
8048/TCP
8048/TCP
Cloud Management
Cloud Management
443/TCP
8441/TCP
443/TCP
8441/TCP
8046/TCP
8044/TCP
8443/TCP
8046/TCP
8044/TCP
8443/TCP
443/TCP
443/TCP
VMware Cloud Director
VMware Cloud Director
Cloud Replication Management Appliance
Cloud Replication Management Appliance
8044/TCP
8044/TCP
Compute
Compute
vCenter Server
vCenter Server
443/TCP
443/TCP
443/TCP
443/TCP
Platform Services Controller
Platform Services Controller
8043/TCP
8043/TCP
8043/TCP
8043/TCP
32032/TCP
44046/TCP
80/TCP
902/TCP
44045/TCP
3030/TCP
443/TCP
32032/TCP
44046/TCP
80/TCP
902/TCP
44045/TCP
3030/TCP
443/TCP
ESXi hosts
Cloud Replicator Appliance(s)
ESXi hosts
Cloud Replicator Appliance(s)
Traffic type:
Replication data traffic
Administration traffic
Service management traffic
DNAT
Replication data traffic and VMware Cloud Director Availability service management traffic

For diagrams showing all services in the cloud site and a diagram showing multiple VMware Cloud Director Availability instances, see Chapter 2 Deployment Architecture in the Cloud.

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

VMware Cloud Director Availability Appliances Connectivity

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

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

VMware Cloud Director Availability Services Connectivity

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

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

For information about each service, see Chapter 3 Services.

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

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

Table 4-2. Firewall Rules for External Communication

Original Destination	Translated Destination	Original Destination Port	DNAT Translated Port	Protocol	Description
Public Network/ Uplink Interface	Cloud Tunnel Appliance	443	8048	TCP	Used for incoming replication management and replication data traffic from public networks to the Tunnel Service. This service then routes the traffic to the local services.

Users Requirements

Before you start deploying and configuring VMware Cloud Director Availability, verify that the service users meet the following requirements.

Cloud Service Users Requirements

The Cloud Service makes a difference between admin users and regular users. To start a session with administrator privileges, the credentials you enter for both of the VMware Cloud Director™ sites must belong to the **ADMINISTRATORS** or **VRADMINISTRATORS** group. For example, the **`Administrator@vsphere.local`** single sign-on user you enter when logging into the management portal, is a member of the **ADMINISTRATORS** group.

VMware Cloud Director Availability User Sessions Requirements

Each VMware Cloud Director Availability user session is guaranteed to have a VMware Cloud Director user and VMware Cloud Director organization associated with the session.

To manage VMware Cloud Director Availability workloads and the local Cloud Service appliance as a service provider, you start a user session as a VMware Cloud Director**system administrator** by using VMware Cloud Director user name and password. **System administrator** users can manage any local and monitor any remote VMware Cloud Director Availability inventory workload. To manage VMware Cloud Director Availability workloads in the remote sites, you must authenticate as a system administrator to the remote site.

For disaster recovery workflows and managing local VMware Cloud Director Availability workloads as a tenant user, you start a user session as a VMware Cloud Director organization administrator by using VMware Cloud Director credentials. As an organization administrator, for disaster recovery workflows in the local site, you can manage any local VMware Cloud Director Availability workload, and can monitor any remote VMware Cloud Director Availability workload that belongs to the respective VMware Cloud Director organization. To manage remote VMware Cloud Director Availability workloads, you must authenticate to the corresponding remote organization.

The following table lists Cloud Service disaster recovery operations that require sessions on either of the sites, or both.

Table 4-3. Cloud Service Replication Operations with Required Sessions

	Incoming Replication		Outgoing Replication	
Operation	Required Session on Source Site	Required Session on Destination Site	Required Session on Source Site	Required Session on Destination Site
`start`	Yes	Yes	Yes	Yes
`stop`	No	Yes	Yes	Yes
`reconfigure`	No	Yes	Yes	Yes
`failover`	No	Yes	Yes	Yes
`migrate`	Yes	Yes	Yes	Yes
`sync`	No	Yes	Yes	Yes
`pause`	No	Yes	Yes	Yes
`resume`	No	Yes	Yes	Yes
`reverse`	Yes	Yes	Yes	Yes
`failover test`	No	Yes	Yes	Yes
`failover test cleanup`	No	Yes	Yes	Yes

For more information about authenticating to remote sites, see *Authenticating to Remote Sites* in the *VMware Cloud Director Availability User Guide*.

Deploying in the Cloud

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

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

The VMware Cloud Director Availability cloud appliances have a name in the form `VMware-Cloud-Director-Availability-Provider-`*`release.number.xxxx-build_number`*`_OVF10.ova`.

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 Cloud Appliances by Using the vSphere Client

In the vSphere Client, you can deploy all VMware Cloud Director Availability appliances from a single `.ova` file.

Prerequisites

- Download the `VMware-Cloud-Director-Availability-Provider-release.number.xxxxxxx-build_sha_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
- If using a version of vSphere earlier than 6.5, install the Client Integration Plug-in to use the **Deploy OVF Template** option in the vSphere Web Client.

Procedure

1. Log in to vCenter Server by using the vSphere Client.
2. Navigate to a target object where you want to deploy the VMware Cloud Director Availability services.

   As a target object you can use a data center, a folder, a cluster, a resource pool, or a host.
3. Right-click the target object and from the drop-down menu select **Deploy OVF Template**.

   The **Deploy OVF Template** wizard opens.
4. On the **Select an OVF template** page, browse to the `.ova` file location and click **Next**.
5. On the **Select a name and folder** page, enter a name for the appliance, select a deployment location, and click **Next**.
6. On the **Select a compute resource** page, select a host, or cluster as a compute resource to run the appliance on, and click **Next**.
7. On the **Review details** page, verify the `OVF` template details and click **Next**.
8. On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.
9. On the **Configuration** page, select the appliance deployment type configuration and click **Next**.

   For more information about the appliance deployment types, see Deployment Requirements.
10. On the **Select storage** page, select the virtual disk format and the storage policy for the appliance and click **Next**.
11. On the **Select networks** page, optionally configure the network settings of the appliance and click **Next**.

    For more information about configuring the network settings after the deployment is complete, see *Network Settings Configuration* in the *VMware Cloud Director Availability Administration Guide* document.

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

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

   You must change the initial **root** user password when you log in for the first time.

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

   If you do not enable SSH, you can configure the appliance later. For more information, see *Allow SSH Access* in the *VMware Cloud Director Availability Administration Guide* document.

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

   Important In the disaster recovery infrastructure, ensure that in the all instances of vCenter Server, ESXi, VMware Cloud Director, Platform Services Controller, and all cloud VMware Cloud Director Availability appliances use the same NTP server.

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

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 `OVA="`*`local_client_path`*`/VMware-Cloud-Director-Availability-`*`Deployment-release.number-xxxx-build_number`*`_OVF10.ova"`, where *Deployment* is **`Provider`** or **`On-Premises`**.
`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.

Parameter	Description
VSPHERE_USER	User name for a vCenter Server administrator.
VSPHERE_USER_PASSWORD	Password for a vCenter Server administrator.
VSPHERE_LOCATOR	The VSPHERE_LOCATOR value contains the target data center name, the tag *host*, 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. ■ */data-center-name*/host/*cluster-1-name*/*ESXi-host-fully-qualified-domain-name* ■ */data-center-name*/host/*cluster-2-name*/*ESXi-host-IP-address* If the target ESXi host is not part of a cluster, skip the *cluster-name* element, as shown in the following examples. ■ */data-center-name*/host/*ESXi-host-fully-qualified-domain-name* ■ */data-center-name*/host/*ESXi-host-IP-address* For more information about the VSPHERE_LOCATOR value, run the `./ovftool --help locators` command.

Deploy the Cloud Appliances by Using the OVF Tool

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

Prerequisites

- Download the `VMware-Cloud-Director-Availability-Provider-`*`release.number.xxxxxxx-build_sha`*`_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
- Verify that the VMware OVF Tool is installed and configured. For more information, see https://code.vmware.com/tool/ovf.

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-Provider-release_number-xxx-
build_number_OVF10.ova"

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

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

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

# VSPHERE_LOCATOR="vSphere-locator"
```

3 Deploy a VMware Cloud Director Availability appliance.

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

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

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

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

Configuring the Cloud Appliances

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

As a best practice, first configure all services in a single cloud site: register the Cloud Service with the VMware Cloud Director, with the vCenter Server Lookup service, with the Replicator Service instances in the same site, and with the Tunnel Service. Then to allow for pairing, perform the initial configuration and the registration in the second cloud site.

After configuring the VMware Cloud Director Availability services, you can validate that the setup is complete by opening the service management interface. In the **System health** page, the entries are green to indicate successfully configured services, and any red entries might indicate an incomplete setup.

Procedure

1 Configure the Cloud Service

Enter a site name as an identifier of the Cloud Service instance and register the Cloud Service with the vCenter Server Lookup service, and with the VMware Cloud Director™ instance. By following the simplified wizard, you can now register the Cloud Service with Replicator Service instances and with the Tunnel Service.

2 Add an Additional Replicator Service Instance

Depending on the deployment requirements, you can add more Replicator Service instances to your disaster recovery environment even after configuring the Cloud Service.

Configure the Cloud Service

Enter a site name as an identifier of the Cloud Service instance and register the Cloud Service with the vCenter Server Lookup service, and with the VMware Cloud Director™ instance. By following the simplified wizard, you can now register the Cloud Service with Replicator Service instances and with the Tunnel Service.

Procedure

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

As the appliance is not yet configured, you are redirected to **`https://Appliance-IP-Address/ui/provider`**.

2 Log in by using the **root** user password that you set during the OVA deployment.

3 If you log in to the appliance for the first time, you must change the initial **root** user password.

a Enter the initial **root** user password that you set during the OVA deployment.

b Enter and confirm a new password.

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

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

c Click **Apply**.

The **Getting Started** tab opens.

4 Under **Steps for configuration** click **Run initial setup wizard**.

Under **Deploy the Cloud Replication Management Appliance**, you see the IP address of this newly deployed Cloud Replication Management Appliance.

5 To set up the Cloud Service instance, complete the **Initial Setup** wizard.

a In the **Licensing** page, you must enter a valid license key for VMware Cloud Director Availability™ and click **Next**.

After providing a valid license key, if you cancel the initial setup wizard, on the next run the **Licensing** page does not show anymore.

b In the **Site Details** page, configure the Cloud Service instance site and click **Next**

Option	Description
Site Name	Enter a site name for this Cloud Service instance. **Important** The site name is used as an identifier of this Cloud Service instance and cannot be changed later.
Service Endpoint address	Optionally, now enter the VMware Cloud Director Availability Service Endpoint address. Alternatively, now you can skip entering this address and provide it after you complete the configuration.
Description	Optionally, enter a description for this site.

c In the **VMware Cloud Director** page, register the Cloud Service instance with a VMware Cloud Director instance and click **Next**.

When registering, the Cloud Service installs the plug-ins named `Setup DRaaS and Migration` and `Availability (localSite)` in VMware Cloud Director

Option	Description
VMware Cloud Director endpoint address	Enter the URL of the VMware Cloud Director instance and to autocomplete the address as `https://VMware-Cloud-Director-IP-Address:443/api`, press Tab.
VMware Cloud Director user name	Enter the VMware Cloud Director **System administrator** user, for example use ***administrator@system***.
VMware Cloud Director password	Enter the VMware Cloud Director **System administrator** password.

Verify the thumbprint and accept the SSL certificate of the VMware Cloud Director instance.

d In the **CEIP** page, optionally, to **Join the VMware Customer Experience Improvement Program**, select the check box and click **Next**.

For more information on the VMware Customer Experience Improvement Program, see Customer Experience Improvement Program.

e In the **Configure Replicator Service instances** page, register the Cloud Service with the vCenter Server Lookup service and with Replicator Service instances, then click **Next**

Option		Description
Lookup Service Address		Enter the address of the vCenter Server Lookup service and to autocomplete the address as `https://Lookup-Service-IP-Address:443/lookupservice/sdk`, press Tab. This address is used for the Cloud Service, for the Manager Service, for all the Replicator Service instances, and for the Tunnel Service.
Replicator 1	**Description**	Optionally enter a description for the instance.
	Replicator Service Address	Enter the API endpoint address of the Replicator Service instance and to autocomplete the address as `https://Replicator-IP-Address:8043`, press Tab.
	Root Password	Enter the password of the **root** user of the Replicator Service.
	Test Connection	Verifies the connectivity to the endpoint and the **root** user password, then saves the Replicator Service instance. If the password is not set since deploying the appliance, you must change the initial **root** user password. Enter the initial root user password that you set during the OVA deployment. Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: ■ At least one lowercase letter. ■ At least one uppercase letter. ■ At least one number. ■ At least one special character, such as: & # % .
	SSO User Name	Enter a user with administrative privileges in the local site single sign-on domain, for example *Administrator@VSPHERE.LOCAL*.
	SSO Password	The password for the administrative user.
Add Replicator		Optionally, add additional Replicator Service instances.

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

f In the **Configure Tunnel Service** page, register the Cloud Service with the Tunnel Service, test the connection, and click **Next**.

Option	Description
Tunnel Service Address	Enter the API endpoint address of the Tunnel Service instance and to autocomplete the address as `https://Tunnel-IP-Address:8047`, press Tab.
Root Password	Enter the password of the **root** user of the Tunnel Service.
Test Connection	Verifies the connectivity to the endpoint and the **root** user password, then saves the Tunnel Service instance. If the password is not set since deploying the appliance, you must change the initial **root** user password. Enter the initial root user password that you set during the OVA deployment. Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: ■ At least one lowercase letter. ■ At least one uppercase letter. ■ At least one number. ■ At least one special character, such as: & # % .

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

g In the **Ready To Complete** page, review the Cloud Service configuration summary and click **Finish**.

6 (Optional) Verify that the Cloud Service configuration is correct.

a In the left pane under **Monitoring**, click **System Health**.

b Under **Service status**, validate that **Lookup Service connectivity** shows a green check status.

c On the **System health** page, you can also see the configuration status of other services.

What to do next

You can now pair this Cloud Service instance with cloud sites and with VMware Cloud Director Availability On-Premises Appliance instances. For more information, see Managing Connections Between Cloud Sites in the *VMware Cloud Director Availability Administration Guide*.

Add an Additional Replicator Service Instance

Depending on the deployment requirements, you can add more Replicator Service instances to your disaster recovery environment even after configuring the Cloud Service.

Prerequisites

- Verify that the Cloud Service in the disaster recovery environment is already configured. For information about configuring the service, see Configure the Cloud Service.
- Deploy a new Cloud Replicator Appliance instance. For more information, see Deploy the Cloud Appliances by Using the vSphere Client and Deploy the Cloud Appliances by Using the OVF Tool.

Procedure

1. Log in to the service management interface of the newly deployed Cloud Replicator Appliance instance.
   a. In a Web browser, go to `https://Cloud-Replicator-Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.
   c. Click **Login**.
2. If you log in to the appliance for the first time, you must change the initial **root** user password.
   a. Enter the initial **root** user password that you set during the OVA deployment.
   b. Enter and confirm a new password.

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

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

   c. Click **Apply**.

      The **Getting Started** tab opens.
3. In the left pane, click **Settings** and next to **Lookup Service Address** click **Edit**.
4. In the **Lookup Service Details** window, enter the vCenter Server Lookup service address.
   a. Press Tab and autocomplete the address as `https://Lookup-Service-IP-address:443/lookupservice/sdk`.
   b. Click **Apply**.
   c. Verify and accept the SSL certificate of the vCenter Server Lookup service.

5 Verify that the vCenter Server Lookup service connectivity is operational.

   a In the left pane, click **System Monitoring**.

   b Under **Service status**, verify that **Lookup Service connectivity** shows a green check status.

6 Log in to the Manager Service service management interface.

   a In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.

   b Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.

   c Click **Login**.

7 In the left pane, click **Replicator Services**.

8 On the **Replicator Services administration** page, click **New**.

9 In the **New Local Replicator Service** window, enter the details for the new Replicator Service instance and click **Add**.

Option	Description
VMware Cloud Director Availability Service Endpoint address	Enter the IP address and port **8043** of the new Cloud Replicator Appliance instance that runs the Replicator Service instance. For example, `https://Cloud-Replicator-Appliance-IP-address:8043`.
Appliance Password	The **root** user password for the new Cloud Replicator Appliance instance as set during the initial Replicator Service configuration.
SSO Admin Username	A user with administrative privileges in the local site single sign-on domain, for example *Administrator@VSPHERE.LOCAL*.
SSO Password	The password for the single sign-on administrative user.
Description	Optionally, enter a description for the new Replicator Service instance you are registering.

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

10 Verify and accept the SSL certificate of the Replicator Service.

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

11 Verify that the connectivity of the Manager Service to the new instance of Replicator Service is operational.

   a In the left pane, click **System Health**.

   b Under **Local Replicator Services**, verify that for the new Replicator Service instance **Service connectivity** shows a green check status.

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

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

Results

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

What to do next

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

Customer Experience Improvement Program

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

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. To join or leave the CEIP for this product, please see Join or Leave the Customer Experience Improvement Program.

Categories of Information That VMware Receives

This product participates in VMware's Customer Experience Improvement Program ("CEIP").

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

To join or leave the CEIP for this product, please see Join or Leave the Customer Experience Improvement Program.

Join or Leave the Customer Experience Improvement Program

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

Procedure

1 Log in to the management interface of the Cloud Replication Management Appliance.

   a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.

   b Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.

   c Click **Login**.

2 In the left pane under **Configuration**, click **Settings**.

3 Under **Customer Experience Improvement Program participation**, next to **Participate in CEIP** click **Edit**.

4 In the **Participate in CEIP** window, to join or leave the CEIP for this product, please configure the following and click **Apply**.

   - To join the CEIP, select the **Join the VMware Customer Experience Improvement Program** check box.
   - To leave the CEIP, deselect the **Join the VMware Customer Experience Improvement Program** check box.

Upgrading in the Cloud

5

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

Upgrade Paths

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

Current Version	Next Version	Available Upgrade Method
4.0.x or 4.1	4.2	■ You can upgrade by using the management interface, see the updated Management Interface Upgrading procedures. ■ Alternatively, you can upgrade by using the command-line interface, see the updated Command-Line Upgrading procedures.
3.5.x 3.0.x	4.0	■ You can upgrade by using the management interface, see the legacy Management Interface Upgrading procedures. ■ Alternatively, you can upgrade by using the command-line interface, see the legacy Command-Line Upgrading procedures.
3.0	4.0	You must upgrade only by using the command-line interface, see the legacy Command-Line Upgrading procedures.

For more information, see the Upgrade Path of VMware Cloud Director Availability in the *VMware Product Interoperability Matrix*.

Important

- Before upgrading, to take snapshots and follow the order of upgrading the appliances, see Upgrade Sequence.
- To complete the upgrade sequence follow Post-Upgrade Configuration in the Cloud.

Upgrade Repository

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

Source Repository	Description
An ISO image	Use an upgrade ISO file mounted in the virtual appliance CD-ROM drive for environments where the network restricts the appliances online Internet access.
A specified repository	To upgrade multiple appliances or when the appliances are deployed in different datastores, specify a repository as a content source: ■ 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. ■ Alternatively, with available Internet access, specify `https://packages.vmware.com/vcav/4.2/` as an online upgrade repository.

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:

- Upgrade Sequence
- Management Interface Upgrading
- Command-Line Upgrading
- Post-Upgrade Configuration in the Cloud

Upgrade Sequence

To successfully upgrade VMware Cloud Director Availability, take snapshots of all the appliances and upgrade each appliance according to a specific order.

Upgrade the sites running VMware Cloud Director Availability in the following order:

1 In the local cloud site, upgrade all the cloud VMware Cloud Director Availability appliances.

2 In remote cloud sites, upgrade all the cloud VMware Cloud Director Availability appliances.

3 Upgrade all the VMware Cloud Director Availability On-Premises Appliance instances.

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

Prerequisites

Important

- Verify that before starting the upgrade, current snapshots of all the appliances exist in the site. Take snapshots only with all the VMware Cloud Director Availability services stopped or with the appliances powered off.
- Verify that before starting the upgrade, 60% free disk space, or more exists on all the appliances in the site.
- Verify that the sites are prepared for replication interruptions and Recovery Point Objective (RPO) violations.

Procedure

1. Power off the Cloud Tunnel Appliance and all Cloud Replicator Appliance instances running in the local cloud site.
2. Upgrade the Cloud Replication Management Appliance and after a successful upgrade, power off the appliance.

   If the Cloud Replication Management Appliance upgrade fails, revert to the latest snapshot.
3. Power on a single Cloud Replicator Appliance instance.
   a. Upgrade the Cloud Replicator Appliance instance.
   b. After a successful upgrade, power off the upgraded Cloud Replicator Appliance instance.

      If the upgrade of a Cloud Replicator Appliance instance fails, revert to the latest snapshot.
   c. Repeat this step for all the remaining Cloud Replicator Appliance instances in the local cloud site.
4. Power on the Cloud Tunnel Appliance.
   a. Upgrade the Cloud Tunnel Appliance.
   b. After a successful upgrade, power on the upgraded Cloud Replication Management Appliance and all the upgraded Cloud Replicator Appliance instances.

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

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

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

Results

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

What to do next

After upgrading the local cloud site, the remote cloud sites, and upgrading the VMware Cloud Director Availability On-Premises Appliance instances, you can start using the new VMware Cloud Director Availability version.

Management Interface Upgrading

To upgrade from VMware Cloud Director Availability 4.0 or later, you can use the management interface of each of the cloud appliances, select an upgrade repository, and follow the updated management interface upgrade procedures for the selected repository.

Verify that you upgrade by following the supported methods in the table, according to the currently installed version.

<table>
<tr><th>Upgrade Method / Starting Version</th><th>Upgrading from Version 3.0</th><th>Upgrading from Version 3.0.x</th><th>Upgrading from Version 4.0 or from Version 4.1</th><th>Upgrading from Version 4.1.x and Later</th></tr>
<tr><td rowspan="3">Upgrade by using the management interface.</td><td rowspan="3">N/A</td><td rowspan="3">Follow the legacy Management Interface Upgrading procedures.</td><td>N/A</td><td>Upgrade by Using the Default Repository</td></tr>
<tr><td colspan="2">Upgrade by Using a Specified Repository</td></tr>
<tr><td colspan="2">Upgrade by Using an ISO Image</td></tr>
<tr><td rowspan="3">Upgrade by using the command-line interface.</td><td colspan="2" rowspan="3">Follow the legacy Command-Line Upgrading procedures.</td><td colspan="2">N/A</td></tr>
<tr><td colspan="2">N/A</td></tr>
<tr><td colspan="2">Command-Line Upgrade by Using an ISO Image</td></tr>
</table>

Upgrade by Using the Default Repository

In the cloud appliances 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.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance. Follow this procedure only when upgrading from VMware Cloud Director Availability 4.1.1 or later. For earlier versions, or alternative upgrade methods, see Chapter 5 Upgrading in the Cloud.

Prerequisites

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances. For more information, see Upgrade Sequence.
- Verify that each VMware Cloud Director Availability appliance has an external Internet access to the VMware repository.

Procedure

1 Log in to the service management interface of each VMware Cloud Director Availability appliance.

a Open a Web browser and according to the upgrade order go to each management interface address.

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

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

2 In the left pane, click **Configuration**.

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

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

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

The VMware Cloud Director Availability 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 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.
```

Results

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

What to do next

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade with a post-upgrade configuration. For more information, see Post-Upgrade Configuration in the Cloud.

Upgrade by Using a Specified Repository

In the cloud appliances 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. If you are upgrading from versions 3.x to 4.0, follow the legacy Upgrade by Using a Specified Repository procedure. For information about the upgrade in the cloud site, see Chapter 5 Upgrading in the Cloud.

Prerequisites

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances. For more information, see Upgrade Sequence.
- Verify that each VMware Cloud Director Availability appliance has a network access to the specified repository.

Procedure

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

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

2 Log in to the service management interface of each VMware Cloud Director Availability appliance.

a Open a Web browser and according to the upgrade order go to each management interface address.

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

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

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

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

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

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

a In the **Repository** page, to specify the repository containing the upgrade files 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/4.2`.
- 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 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 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.
```

Results

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

What to do next

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade with a post-upgrade configuration. For more information, see Post-Upgrade Configuration in the Cloud.

Upgrade by Using an ISO Image

In the cloud appliances management interface, you can upgrade from VMware Cloud Director Availability 4.0 and later versions to the latest version by using an `.iso` image file containing the upgrade binaries that you mount to the CD-ROM drive of the virtual appliances.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance. Follow the updated procedure bellow only when upgrading from VMware Cloud Director Availability 4.0 and later. If you are upgrading from versions 3.x to 4.0, follow the legacy Upgrade by Using an ISO Image procedure.

Prerequisites

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances. For more information, see Upgrade Sequence.
- 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 each of the VMware Cloud Director Availability appliances.

   a Log in to the vSphere Client on the site where you want to upgrade VMware Cloud Director Availability.

   b On the **Home** page, click **Hosts and Clusters**.

   c Right-click the virtual machine that hosts the VMware Cloud Director Availability appliance and select **Edit Settings**.

   d On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.

   e Follow the prompts to add the CD/DVD drive to the VMware Cloud Director Availability virtual machine and select the **Connected** option.

3 By using the cloud appliances console, mount the `.iso` file inside the guest operating system of each of the VMware Cloud Director Availability appliances.

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

   b Mount the `.iso` file inside the guest operating system of each cloud appliance.

```
mount /mnt/cdrom
```

4 Log in to the service management interface of each VMware Cloud Director Availability appliance.

   a Open a Web browser and according to the upgrade order go to each appliance management interface address.

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

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

5 In the left pane, click **Configuration**.

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

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

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

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 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, depending on the version from which you started the upgrade from.

- 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 cloud 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 cloud appliance.

Results

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

What to do next

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade with a post-upgrade configuration. For more information, see Post-Upgrade Configuration in the Cloud.

Command-Line Upgrading

To upgrade from VMware Cloud Director Availability 4.0 you can use the command-line interface of each of the cloud appliances, select an upgrade repository, and follow the updated command-line 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 cloud 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 procedures.
- If upgrading from version 3.0.x to version 4.0, you can follow the legacy Management Interface Upgrading procedures. Alternatively, you can follow the legacy Command-Line Upgrading procedures.
- If upgrading from version 3.0 to version 4.0, you must follow the legacy Command-Line Upgrading procedures.

Command-Line Upgrade by Using an ISO Image

From the cloud appliances 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.

Perform this procedure multiple times, to upgrade each VMware Cloud Director Availability appliance. Follow the updated command-line procedure bellow only when upgrading from VMware Cloud Director Availability 4.0 and later. If you are upgrading from versions 3.x to 4.0, follow the legacy Command-Line Upgrade by Using an ISO Image procedure.

Prerequisites

- Follow a strict order when upgrading the VMware Cloud Director Availability appliances. For more information, see Upgrade Sequence.
- 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 in a VMware Cloud Director Availability appliance.
   a. Log in to the vSphere Client in the site where you want to upgrade VMware Cloud Director Availability.
   b. On the **Home** page, click **Hosts and Clusters**.
   c. Right-click the virtual machine that hosts the VMware Cloud Director Availability appliance and select **Edit Settings**.
   d. On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
   e. Follow the prompts and add the CD/DVD drive to the VMware Cloud Director Availability virtual machine and select the **Connected** option.

   Repeat this step to mount the `.iso` file in all remaining VMware Cloud Director Availability appliances.
3. Upgrade a VMware Cloud Director Availability appliance in the upgrade order from the following table.

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

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

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

```
mount /mnt/cdrom
```

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

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

d Install the upgrade.

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

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

e After the upgrade completes, restart the appliance.

```
reboot
```

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

What to do next

After you upgrade all the VMware Cloud Director Availability appliances, finish the upgrade with a post-upgrade configuration. For more information, see Post-Upgrade Configuration in the Cloud.

Post-Upgrade Configuration in the Cloud

After upgrading all VMware Cloud Director Availability components in both the local and in the remote sites from version 4.0, you perform post-upgrade steps. Reinstall the latest version of the VMware Cloud Director Availability plug-in for VMware Cloud Director by reentering the password of the VMware Cloud Director **System administrator** user.

Prerequisites

Verify that all VMware Cloud Director Availability components in both the local and in the remote sites are successfully upgraded.

Procedure

1 Log in to the management interface of the Cloud Replication Management Appliance.

a In a Web browser, go to `https://`*`Appliance-IP-Address`*`/ui/admin`.

b Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.

c Click **Login**.

2 Reinstall the latest version of the VMware Cloud Director Availability plug-in for VMware Cloud Director.

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

   a In the left pane under **Configuration**, click **Settings**.

   b Under **Service endpoints**, next to **VMware Cloud Director address** click **Edit**.

   c Enter the VMware Cloud Director endpoint URL as `https://`*`VMware Cloud Director-IP-address`*`:443/api`.

   d Enter the VMware Cloud Director **System administrator** user credentials and click **Apply**.

   For example, use *administrator@system*, where *system* is the VMware Cloud Director organization name.

   e Verify the thumbprint and accept the VMware Cloud Director SSL certificate.

Results

The upgrade in the cloud site is complete and VMware Cloud Director Availability is ready for replications. For more information, see the *VMware Cloud Director Availability User Guide*.