Migration to VMware Cloud Director service Guide

23 JUN 2022

VMware Cloud Director Availability 4.4

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

https://docs.vmware.com/

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

Contents

Migration to VMware Cloud Director service

1

VMware Cloud Director Availability™ 4.2 and later can migrate workloads to the VMware Cloud Director™ service hosted at VMware Cloud™ on AWS.

Classic Migrations to VMware Cloud Director Cloud Sites

Any VMware Cloud Director Availability version can migrate vSphere workloads to a private cloud site backed by VMware Cloud Director by using the native integrations with VMware Cloud Director and VMware vCenter Server®.

VMware Cloud on AWS Design Implications

Due to design specifics of the VMware Cloud Director service hosted at VMware Cloud on AWS, a new VMware Cloud Director Availability 4.2 service, named VMware Cloud on AWS Data Engine Service performs the migrations to VMware Cloud on AWS by using the new VMC data engine. By using the Data Engine Service and selecting the **VMC** data engine, VMware Cloud Director Availability can migrate workloads to VMware Cloud Director service. For more information about this service, see Services and Network Ports in the *Security Guide*.

The service providers in VMware Cloud on AWS have a VMware Cloud SDDC account and a general AWS account, and the two accounts must be linked for the service to work. Each account has its own virtual private cloud (VPC), and the VMware Cloud VPC contains a management and a compute resource pool. In the management resource pool, VMware has complete administrative control over the management and the infrastructure components. The VMware Cloud Director Availability appliances reside outside the management resource pool, deployed and managed by the service provider.

Migrations to VMware Cloud on AWS

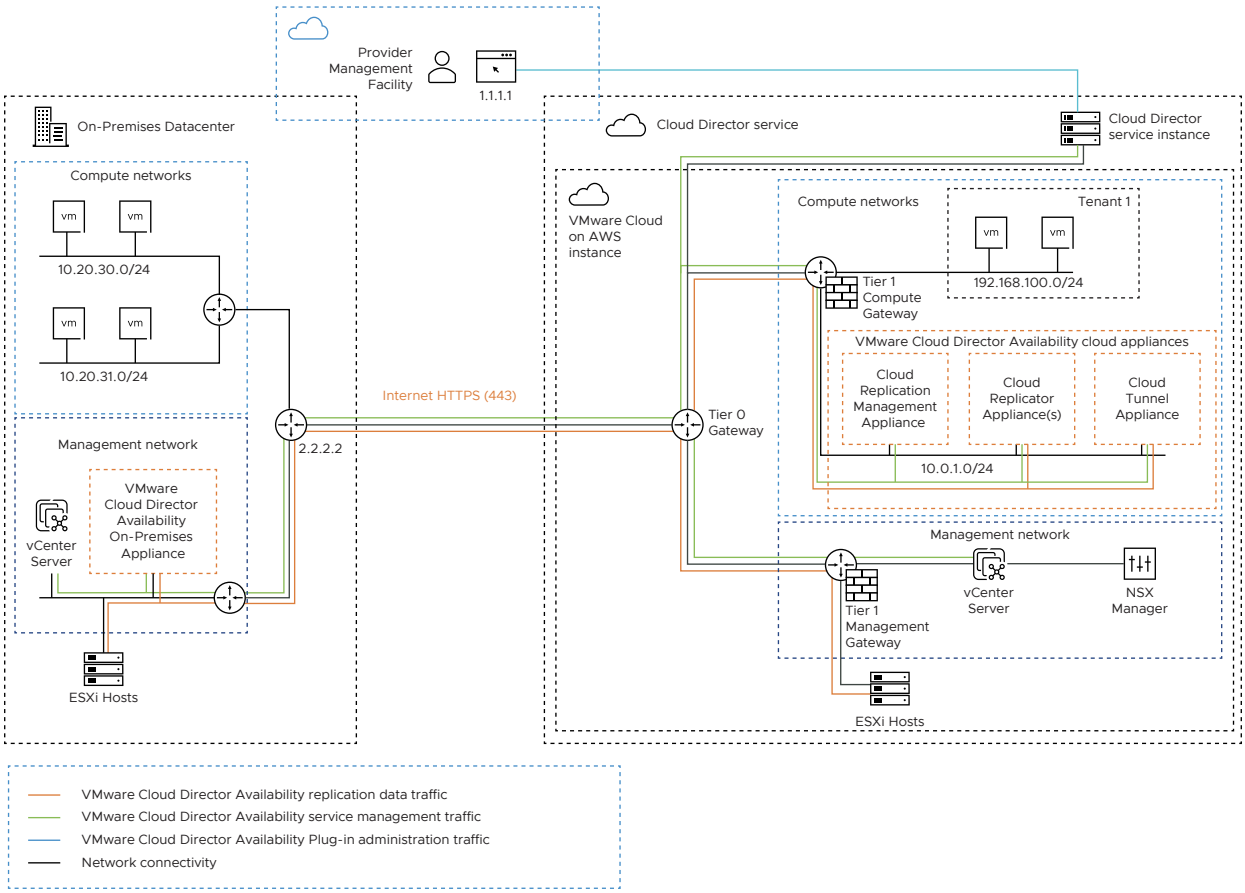
Both the service providers and their tenants, can use the existing migration flow and migrate their workloads to VMware Cloud Director service in VMware Cloud on AWS after following this *Migration to VMware Cloud Director service Guide*.

VMware Cloud Director service pools resources provided by the SDDC in VMware Cloud on AWS. The following diagrams provide an overview of VMware Cloud Director service after installing VMware Cloud Director Availability and pairing VMware Cloud on AWS with an on-premises site and or with a cloud site, backed by VMware Cloud Director.

In VMware Cloud on AWS, VMware Cloud Director Availability resides behind the compute networks compute gateway and firewall and connects with the management components like vCenter Server and ESXi trough the management gateway and firewall of the management network. The *Migration to VMware Cloud Director service Guide* covers the necessary configuration in VMware Cloud on AWS allowing the connectivity to and from VMware Cloud Director Availability trough the management and the compute gateways.

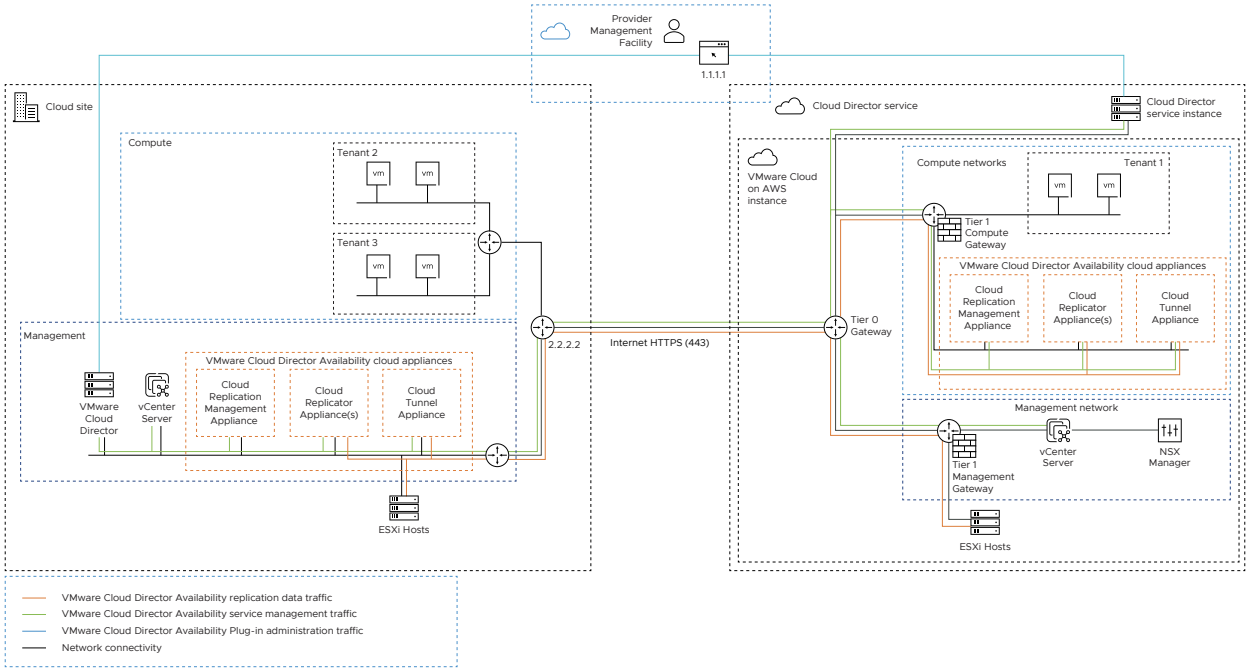
Paired On-Premises Site with VMware Cloud Director Availability in VMware Cloud on AWS

After pairing the On-Premises to Cloud Director Replication Appliance with VMware Cloud Director Availability in VMware Cloud on AWS, in the following architecture diagram the orange color shows the deployed on-premises and cloud appliances of VMware Cloud Director Availability and the replication data traffic between the appliances, with all existing components in black:



Paired Cloud Site with VMware Cloud Director Availability in VMware Cloud on AWS

After pairing a cloud site, backed by VMware Cloud Director with VMware Cloud Director Availability in VMware Cloud on AWS, in the following deployment diagram the orange color shows the deployed cloud appliances of VMware Cloud Director Availability and the replication data traffic between them, with all existing components in black:



Overview of the Configuration

For a summary of all the configured objects in the VMware Cloud on AWS SDDC, see Chapter 7 SDDC Network Configuration Summary. VMware Cloud Director Availability resides behind the compute gateway in VMware Cloud on AWS. Configure the SDDC in VMware Cloud on AWS for the following access.

- To access vCenter Server in the management resource pool by administrative users and by VMware Cloud Director Availability.
- To access the management interface of VMware Cloud Director Availability for initial configuration.
- To access the Service Endpoint from external VMware Cloud Director Availability sites for pairing and migrations from these sites.

In VMware Cloud on AWS, the SDDC and VMware Cloud Director Availability must be prepared and configured in the following order.

1 Prepare the VMware Cloud on AWS SDDC by creating the following objects. For the detailed SDDC preparation procedure, see Chapter 2 Prepare the SDDC in VMware Cloud on AWS for Deployment.

   a A network segment, connecting all the cloud VMware Cloud Director Availability appliances.

   b A trusted management sources group, containing the public IP addresses of the **administrator** users that need access to vCenter Server in VMware Cloud on AWS for installing the cloud VMware Cloud Director Availability appliances.

   c A management firewall rule, allowing the trusted management group to access management gateway services like vCenter Server.

   d A separate resource pool, dedicated for all the cloud VMware Cloud Director Availability appliances.

2 Deploy the OVA of VMware Cloud Director Availability in the VMware Cloud on AWS SDDC. Alternatively, as a tenant deploy the On-Premises to Cloud Director Replication Appliance in on-premises data centers. For the detailed deployment procedure, see Chapter 3 Deploy VMware Cloud Director Availability in the SDDC.

3 Configure the network of the VMware Cloud on AWS SDDC by creating the following objects. For the detailed SDDC configuration procedure, see Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS .

   a Two inventory services, one for the management interface of VMware Cloud Director Availability and one for the Service Endpoint.

   b Two public IP addresses requested in the SDDC, one to access the initial setup wizard in the management interface of VMware Cloud Director Availability and one allowing external pairing to the Service Endpoint.

   c Two NAT rules for forwarding the incoming network traffic to the correct cloud VMware Cloud Director Availability appliances.

   d Two management groups, one containing the source NAT public IP address of the SDDC used for bridging the access from the compute gateway VMware Cloud Director Availability appliances and one containing the Cloud Replicator Appliance instances.

   e Two management firewall rules, one allowing the access from the compute gateway source NAT to the management gateway vCenter Server and one allowing the Cloud Replicator Appliance instances access to ESXi datastores for provisioning.

   f Four compute groups, one containing the users that can access the management interface of VMware Cloud Director Availability and three groups containing the three types of cloud VMware Cloud Director Availability appliances.

   g Another two compute firewall rules, one allowing the access to the management interface of VMware Cloud Director Availability and one allowing the cloud appliances with outbound network access.

4 Configure VMware Cloud Director Availability in VMware Cloud on AWS by completing the initial wizard. For the detailed initial configuration procedure, see Chapter 5 Configure VMware Cloud Director Availability in VMware Cloud on AWS.

5 Configure the VMware Cloud on AWS SDDC for pairing with external VMware Cloud Director Availability sites by creating the following objects. For the detailed pairing preparation procedure, see Chapter 6 Configure the SDDC Network for Pairing VMware Cloud Director Availability in VMware Cloud on AWS.

   a A pairing compute group, containing the public IP addresses of the on-premises tenants and of the private cloud sites, backed by VMware Cloud Director.

   b A pairing compute gateway firewall rule, allowing the access from the preceding pairing compute group to the Service Endpoint for pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

6 Pair with external VMware Cloud Director Availability sites.

   a Optionally, as a tenant configure and pair On-Premises to Cloud Director Replication Appliance instances with VMware Cloud Director Availability in VMware Cloud on AWS. For the detailed initial on-premises configuration and pairing procedure, see Configure and Pair the On-Premises to Cloud Director Replication Appliance.

   b Optionally, pair VMware Cloud Director Availability in VMware Cloud on AWS with private cloud sites backed by VMware Cloud Director. For the detailed pairing procedure with cloud sites, see Pair VMware Cloud Director Cloud Sites.

After completing all these steps, by using the existing migration flow in VMware Cloud Director Availability the trusted, allowed, and paired service providers and their trusted, allowed, and paired tenants can migrate workloads to VMware Cloud Director service in VMware Cloud on AWS.

- Later, to allow access to perform administrative tasks like certificate replacement by using the three types of management interfaces of the services of VMware Cloud Director Availability:
  - Add three inventory services for each management interface type: Replicator Service, Manager Service, and Tunnel Service.
  - Add three NAT rules, with additional NAT rule for each Replicator Service instance.
  - Modify the existing compute gateway firewall rule that allows access from the trusted compute sources group and include the three additional services, for a total of four inventory services.

  For information about adding these networking objects, see Chapter 9 Post-configure the SDDC Networking in VMware Cloud on AWS.

Prepare the SDDC in VMware Cloud on AWS for Deployment

2

To deploy and use VMware Cloud Director Availability™ in VMware Cloud™ on AWS for migrations, first prepare the Software-Defined Data Center (SDDC). Create a network segment and allow accessing the management gateway vCenter Server for appliances deployment.

After meeting the SDDC prerequisites, prepare the SDDC for VMware Cloud Director Availability deployment outside the management resource pool. Before deploying the appliances, create a dedicated resource pool.

Note The access to the management resource pool is limited and the public IP addresses of all the users must be explicitly allowed before accessing the management components in the management resource pool, like vCenter Server for the appliances deployment.

For an overview, see Chapter 1 Migration to VMware Cloud Director service.

Prerequisites

- Verify that the SDDC is successfully deployed at VMware Cloud on AWS, that the cloud administrator user can login to the SDDC, and has permissions to deploy OVF templates.
- Verify that in the VMware Cloud Director service, the Cloud Director instance is deployed at VMware Cloud on AWS in the same AWS region as the SDDC, for example, *US West (Oregon)*, and that the Cloud Director instance is associated with the VMC SDDC.
- Verify that in the Cloud Director instance at least one organization, one organization network, one provider data center (Provider VDC), one organization virtual data center (Organization VDC), and a local administrator user with **CDS Provider Admin Role** exist and that the Cloud Director instance can host migrated virtual machines.

Procedure

1. Log in to VMware Cloud on AWS at https://vmc.vmware.com.
2. In the VMC console, in the left pane click **SDDCs**.
3. Under the SDDC, click the **View Details** link.
4. Under the SDDC name, click the **Networking & Security** tab.

5 Add a network segment that connects the VMware Cloud Director Availability appliances so they can communicate between themselves and with other network services.

a On the **Networking & Security** tab, in the left pane under the **Network** section, click **Segments**.

b To add a dedicated routed network for the VMware Cloud Director Availability appliances, under **Segment List**, click **Add Segment** and enter the following settings.

Option	Description
Name	Enter a name for the network segment. For example, enter ***vcda-network-segment***.
Type	Routed
Subnets	Enter an **IPv4 CIDR subnet** for all the VMware Cloud Director Availability appliances.

c To save the network segment, click **Save** and to finish configuring the segment click **No**.

Under the Subnets column, you see the routed network **CIDR** used in the OVF deployment wizard, on the **Select Networks** page.

6 Before accessing the management gateway vCenter Server in VMware Cloud on AWS for deploying the VMware Cloud Director Availability appliances, create a *Trusted Management Sources Group* containing the allowed IP addresses.

a On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.

b To create a management group, click the **Management Groups** tab, click **Add Group** and enter a group name.

c To add trusted members to this new management group, under the Compute Members column, click the **Set Members** link.

d In the **Select Members** window, on the **IP Addresses** tab enter the IP addresses of the trusted users and click **Apply**.

Management Group Name	Management Group Trusted Members IP Addresses
Trusted Management Sources Group	Enter the externally-facing ***public-IP-addresses*** of the users granted with access to the vCenter Server management gateway service in VMware Cloud on AWS. **Important** Ensure that you add all the public IP addresses of each user allowed to access vCenter Server in VMware Cloud on AWS or the users have no access.

e To save the management group, click **Save**.

7 To allow accessing the management gateway vCenter Server for the cloud appliances deployment, allow access from the trusted management sources group.

a On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.

b Click the **Management Gateway** tab, then click **Add Rule** and configure the following settings.

Option	Description
Name	Enter a name for the compute gateway firewall rule. For example, enter ***vCenter Inbound From Trusted Management Sources Rule***.
Sources	Click **Any** in the Sources column. In the **Set Source** window select **User Defined Groups**, select the trusted IP addresses management group and click **Apply**. For example, select ***Trusted Management Sources Group***.
Destinations	In the Destinations column click **Any**, then in the **Set Destination** window, select **System Defined Groups** and select **vCenter**.
Services	In the Services column, select **HTTPS (TCP 443)**.
Action	Allow

c To publish the new management gateway firewall rule, click **Publish**.

8 To obtain permissions for creating new virtual machines, create a separate resource pool dedicated for the multiple cloud VMware Cloud Director Availability appliances, outside the management resource pool.

a Click **Open vCenter** and log in with the cloud admin user credentials.

b Expand **SDDC-Datacenter**, right-click **Cluster-1** and select **New Resource Pool**.

c In the **New Resource Pool** window, enter a name for the resource pool for the VMware Cloud Director Availability appliances. For example, enter ***VCDA-Resource-Pool***.

d Configure the **CPU** and the **Memory** sections and click **OK**.

The new resource pool shows under **SDDC-Datacenter > Cluster-1**.

Results

After performing all the steps in this procedure, the SDDC in VMware Cloud on AWS is fully prepared for VMware Cloud Director Availability deployment. For a summary of the configuration, see Chapter 7 SDDC Network Configuration Summary.

What to do next

You can now deploy the VMware Cloud Director Availability appliances in VMware Cloud on AWS. For more information, see Chapter 3 Deploy VMware Cloud Director Availability in the SDDC.

Deploy VMware Cloud Director Availability in the SDDC 3

In the VMware Cloud on AWS SDDC, as a service provider, deploy all cloud VMware Cloud Director Availability appliances from a single `.ova` file. In the tenant data center, as a tenant you can deploy the On-Premises to Cloud Director Replication Appliance by using its dedicated `.ova` file.

- As a service provider, after preparing the VMware Cloud on AWS SDDC for deployment, repeat this procedure multiple times and deploy all the cloud appliances of VMware Cloud Director Availability by using the downloaded provider `.ova` file.
- As a tenant, follow this same procedure once in the tenant data center and deploy the On-Premises to Cloud Director Replication Appliance by using the downloaded on-premises `.ova` file.

Prerequisites

- As a service provider:
  - Verify that the VMware Cloud on AWS SDDC is prepared for VMware Cloud Director Availability deployment. For more information, see Chapter 2 Prepare the SDDC in VMware Cloud on AWS for Deployment.
  - Verify that the user you use has permissions to deploy OVF templates. For example, use the default **cloudadmin@vmc.local** user that has the required permissions.
  - Download the `VMware-Cloud-Director-Availability-Provider-`*`release.number.xxxxxxx-build_sha`*`_OVF10.ova` file, containing the binaries for the VMware Cloud Director Availability cloud appliances.
- As a tenant:
  - Verify that the user you use has the required permissions to deploy an OVF template in the tenant data center.
  - Download the `VMware-Cloud-Director-Availability-On-Premises-`*`release.number.xxxxxxx-build_sha`*`_OVF10.ova` file, containing the binaries for the On-Premises to Cloud Director Replication Appliance.

Procedure

1 Navigate to the resource pool for the appliance deployment.

- As a service provider, repeat the steps in this procedure multiple times and deploy the following number of cloud VMware Cloud Director Availability appliances under the dedicated resource pool **SDDC-Datacenter > Cluster-1 > *VCDA-Resource-Pool***, created in step 10 in Prepare the SDDC for Deployment:
  - One or more Cloud Replicator Appliance instances.
  - A Cloud Replication Management Appliance.
  - A Cloud Tunnel Appliance.
- As a tenant, follow the steps once in your data center and deploy the On-Premises to Cloud Director Replication Appliance.

a Right-click the resource pool for the appliance deployment.

b From the drop-down menu, select **Deploy OVF Template**.

2 Complete the **Deploy OVF Template** wizard.

a On the **Select an OVF template** page, browse to the `.ova` file location and click **Next**.

b On the **Select a name and folder** page, enter a name for the appliance, select a deployment location, and click **Next**.

c On the **Select a compute resource** page, select a host, or cluster as a compute resource to run the appliance on, and click **Next**.

As a service provider, select the dedicated resource pool for each appliance, for example select ***VCDA-Resource-Pool***.

d On the **Review details** page, verify the `OVF` template details and click **Next**.

e On the **License agreements** page, select the **I accept all license agreements** check box and click **Next**.

f As a service provider, on the **Configuration** page, select an appliance deployment type for each appliance and click **Next**.

- One or more Cloud Replicator Appliance instances.
- A Cloud Replication Management Appliance.
- A Cloud Tunnel Appliance.

For information about the appliance deployment types, see Deployment Requirements in the *Installation, Configuration, and Upgrade Guide in the Cloud*.

g On the **Select storage** page, select **WorkloadDatastore** and click **Next**.

h On the **Select networks** page, select the network for the VMware Cloud Director Availability appliance and click **Next**.

- As a service provider, select the dedicated routed network for the VMware Cloud Director Availability appliances. For information about this dedicated routed network, see step 5.b in Prepare the SDDC for Deployment.
- As a tenant, to ensure a successful pairing select a network with access to the VMware Cloud on AWS SDDC.

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

Option	Description
Root password	Enter and confirm the initial password for the appliance **root** user. Later, when logging in for the first time, this initial password must be changed.
Address	■ As a service provider, enter an IP address in CIDR notation in the *vcda-network-segment* dedicated routed network for the cloud VMware Cloud Director Availability appliances. For information about this network, see step 5.b in Prepare the SDDC for Deployment. ■ As a tenant, enter an IP address in CIDR notation that belongs in the tenant data center network.
Gateway	■ As a service provider, enter the compute gateway. ■ As a tenant, enter the tenant data center gateway.
DNS servers	■ As a service provider, enter the compute gateway DNS service IP address of the SDDC. To obtain it, click the **Networking & Security** tab, then in the left pane under **System**, click **DNS** and next to the `Compute Gateway DNS Forwarder`, copy its IP address from the DNS Server IP column. ■ As a tenant, enter the IP address of the DNS server in the tenant data center.
NTP Server	Enter the address of the NTP server for the VMware Cloud Director Availability appliance to use. ■ As a service provider, check the available time servers in the zone of your AWS instance and use the same NTP server as vCenter Server, ESXi, VMware Cloud Director, and all cloud VMware Cloud Director Availability appliances. ■ As a tenant, use the same NTP server as vCenter Server and ESXi.

j On the **Ready to complete** page, review the settings, optionally select **Power on after deployment** and to begin the OVF deployment, click **Finish**.

The **Recent Tasks** pane shows a new task for initializing the OVF deployment. After the task completes, the new appliance is created in the VMware Cloud Director Availability appliances resource pool.

3 After deployment, power on the appliance.

a Under the resource pool for the appliance deployment, right-click the virtual machine.

b From the context menu, select **Power > Power On**.

Results

The VMware Cloud Director Availability appliances are deployed.

What to do next

- As a service provider, you can now configure the SDDC network. For more information, see Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS .
- As a tenant, you can now configure the On-Premises to Cloud Director Replication Appliance. For more information, see Configure and Pair the On-Premises to Cloud Director Replication Appliance.

Configure the Network of the SDDC in VMware Cloud on AWS

4

To allow pairing with VMware Cloud Director Availability in VMware Cloud on AWS, first configure the network settings of the SDDC.

The access to the resource pools is limited in VMware Cloud on AWS and the private IP addresses of all the cloud appliances of VMware Cloud Director Availability must be explicitly allowed as well as to access the management and infrastructure components in the management resource pool, like vCenter Server and ESXi.

VMware Cloud Director Availability in VMware Cloud on AWS provides two services to the Internet. To use the two services in the configuration of the necessary NAT rules, you explicitly define them since both services internally use non-standard HTTPS ports. These two services in conjunction with the following two NAT rules translate the network traffic coming to the public IP address on the external port 443/TCP:

- Towards the Cloud Replication Management Appliance, internally on port 8046/TCP for management interface network traffic to the Cloud Service.
- Towards the Cloud Tunnel Appliance, internally on port 8048/TCP for replication data network traffic to the Service Endpoint.

Prerequisites

- Verify that the SDDC is first prepared for VMware Cloud Director Availability deployment. For information about the required steps, see Chapter 2 Prepare the SDDC in VMware Cloud on AWS for Deployment.
- Verify that VMware Cloud Director Availability 4.2 or later is deployed in VMware Cloud on AWS. For more information, see Chapter 3 Deploy VMware Cloud Director Availability in the SDDC.

Procedure

1. Log in to VMware Cloud on AWS at https://vmc.vmware.com.
2. Add two new inventory SDDC services, for the management interface and for the Service Endpoint.
   a. In the VMC console, in the left pane click **SDDCs**.
   b. Under the SDDC click **View Details** and click the **Networking & Security** tab.

c In the left pane under the **Inventory** section, click **Services**.

Repeat the following steps twice.

- Add an inventory service for the management interface of the Cloud Replication Management Appliance.
- Add another inventory service for the Service Endpoint of the Cloud Tunnel Appliance.

d To add an inventory SDDC service, click **Add Service**.

e Enter a name and optionally a description for each service.

f For each service, in the Service Entries column, click the **Set Service Entries** link.

g For each service, in the **Set Service Entries** window, from the **Type** drop down menu select **Layer 3 and above**.

h For each service, on the **Port-Protocol** tab click **Add Service Entry**, enter the details from the respective column, and click **Apply**.

Option	Management Interface Inventory Service	Service Endpoint Inventory Service
Name	Enter a name for the service entry of the Cloud Replication Management Appliance management interface. For example, enter ***VCDA-Cloud-Service-Management***.	Enter a name for the service entry of the Cloud Tunnel Appliance Service Endpoint. For example, enter ***VCDA-Tunnel-Service-Endpoint***.
Service Type	Select **TCP**.	Select **TCP**.
Additional Properties	Leave the **Source Ports** text box blank.	Leave the **Source Ports** text box blank.
	To access the management interface of the Cloud Replication Management Appliance in the **Destination Ports** text box, in enter port **8046**.	To access the Service Endpoint of the Cloud Tunnel Appliance, in the **Destination Ports** text box enter port **8048**.

i To save each inventory service, click **Save**.

On the **Services** page, both services show:

Name	Service Entries
VCDA-Cloud-Service-Management	TCP (Source: Any | Destination: 8046)
VCDA-Tunnel-Service-Endpoint	TCP (Source: Any | Destination: 8048)

3 To later use in NAT rules, request two new public SDDC IP addresses.

- Request a public IP address to access the initial setup wizard in the management interface of the Cloud Replication Management Appliance.

- Request a public IP address to allow external pairing to the Service Endpoint of the Cloud Tunnel Appliance.

a On the **Networking & Security** tab, in the left pane under the **System** section click **Public IPs**.

b To request a public IP address for the Cloud Replication Management Appliance, click **Request New IP**, enter a note, and click **Save**.

For example, as a note enter ***VCDA-Management-Public-IP-address***.

c To request a public IP address for the Cloud Tunnel Appliance, click **Request New IP**, enter a note and click **Save**.

For example, as a note enter ***VCDA-Tunnel-Public-IP-address***.

4 To forward the incoming network traffic to the correct cloud appliances and ports, add two new NAT rules.

   a On the **Networking & Security** tab, in the left pane under the **Network** section click **NAT**.

   Repeat the following step twice.

   - Add a NAT rule for the management interface of the Cloud Replication Management Appliance.
   - Add another NAT rule for the incoming network traffic to the Service Endpoint of the Cloud Tunnel Appliance.

   b To add a NAT rule, click **Add NAT Rule**, configure the following settings and click **Save**.

Option	Management Interface NAT	Service Endpoint NAT
Name	Enter a name for the NAT rule for the Cloud Replication Management Appliance management interface. For example, enter ***`VCDA Management Interface NAT`***.	Enter a name for the NAT rule for the Cloud Tunnel Appliance Service Endpoint. For example, enter ***`VCDA Tunnel Service Endpoint NAT`***.
Public IP	Select the ***VCDA-Management-Public-IP-address***.	Select the ***VCDA-Tunnel-Public-IP-address***.
Service	Select the inventory service for the Cloud Replication Management Appliancemanagement interface. For example, select ***VCDA-Cloud-Service-Management***.	Select the inventory service for the Cloud Tunnel Appliance Service Endpoint. For example, select ***VCDA-Tunnel-Service-Endpoint***.
Public Port	Enter port **`443`**.	Enter port **`443`**.
Internal IP	Enter the ***`private-IP-address`*** of the Cloud Replication Management Appliance.	Enter the ***`private-IP-address`*** of the Cloud Tunnel Appliance.
Internal Port	8046 (non-editable)	8048 (non-editable)
Firewall	Match Internal Address	Match Internal Address

   After completing the initial configuration, to reduce the possible attack surface the NAT rule for the management interface can be disabled or removed. VMware Cloud Director Availability remains accessible from the Cloud Director instance by using the plug-in for VMware Cloud Director Availability.

5 To later create a management group and use it in a management firewall rule, note the compute gateway source NAT *public IP address* of the SDDC.

   a On the **Networking & Security** tab, in the left pane click **Overview**.

   b Under **Default Compute Gateway** and under **Workloads**, note the **Source NAT Public IP** address of the SDDC.

6 To prepare the cloud appliances access to the management gateway services like vCenter Server and ESXi, add two management groups.

a On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.

b Click the **Management Groups** tab.

Repeat the following steps two times.

- Add a management group, containing the private IP addresses of all the deployed Cloud Replicator Appliance instances.
- Add another management group, containing the compute gateway source NAT.

c To create a management group, click **Add Group** and for each group enter a management group name.

d To add trusted members to each management group, under the Compute Members column, click the **Set Members** link.

e In the **Select Members** window, on the **IP Addresses** tab enter the following IP addresses for each management group and click **Apply**.

Management Group Name	Management Group Trusted Members IP Addresses
SNAT VCDA Management Group	■ Enter the compute gateway source NAT ***public-IP-address*** of the SDDC, as noted in the previous step. ■ Enter the subnet group of the VMware Cloud Director Availability appliances. For example, enter the ***vcda-network-segment***.
VCDA Replicators Management Group	Enter the ***private-IP-addresses*** reserved within the *vcda-network-segment* for all the Cloud Replicator Appliance instances deployed in VMware Cloud on AWS. All Cloud Replicator Appliance instances must access the vCenter Server management gateways services for virtual machines provisioning and performing replication tasks with the ESXi hosts and datastores.

f To save each management group, click **Save**.

7 To allow the internal communication from the cloud appliances to the vCenter Server and to the ESXi datastore in the management gateway, add two new management gateway firewall rules.

a On the **Gateway Firewall** page, click the **Management Gateway** tab.

Repeat the following steps twice.

- Add a management firewall rule for allowing the network traffic from the compute gateway source NAT to the management gateway vCenter Server.
- Add another management firewall rule for allowing the Cloud Replicator Appliance instances writing in the destination ESXi datastore.

b To create a management firewall rule, click **Add Rule**.

c Configure each of the two management firewall rules and click **Apply** when prompted.

Option	vCenter Server Management Gateway Firewall Rule	ESXi Hosts Management Gateway Firewall Rule
Name	Enter a name for the vCenter Server management gateway rule. For example, enter ***SNAT VCDA to vCenter Rule***.	Enter a name for the ESXi management gateway rule. For example, enter ***VCDA Replicators to ESXi Rule***.
Sources	Click **Any**. In the **Set Source** window, select **User Defined Groups** and select the management group for the SNAT. For example, select ***SNAT VCDA Management Group*** and click **Apply**.	Click **Any**. In the **Set Source** window, select **User Defined Groups** and select the management group for the private IP addresses of the Cloud Replicator Appliance instances. For example, select ***VCDA Replicators Management Group*** and click **Apply**.
Destinations	Click **Any**. In the **Set Destination** window under **System Defined Groups**, select **vCenter** and click **Apply**.	Click **Any**. In the **Set Destination** window under **System Defined Groups**, select **ESXi** and click **Apply**.
Services	Click **Any** and select **HTTPS (TCP 443)**.	To allow the Data Engine Service of the Cloud Replicator Appliance writing in the ESXi datastores, click **Any** and select **HTTPS (TCP 443)** and **Provisioning & Remote Console (TCP 902)**.
Action	Allow	Allow

d After creating both management gateway firewall rules, click **Publish**.

8 To prepare for accessing the compute gateway services in VMware Cloud on AWS, create four compute groups.

a On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.

Repeat the following steps four times.

- Add a compute group for the trusted users that need access to the VMware Cloud Director Availability management interface.
- Add a compute group for the Cloud Replication Management Appliance.
- Add a compute group for all the Cloud Replicator Appliance instances.
- Add a compute group for the Cloud Tunnel Appliance.

b To create a compute group, under the **Compute Groups** tab, click **Add Group** and enter a group name.

c To add trusted members to each compute group, under the Compute Members column, click the **Set Members** link.

d In the **Select Members** window, on the **IP Addresses** tab enter the following IP addresses for each compute group and click **Apply**.

Compute Group Name	Compute Group Trusted Members IP Addresses
Trusted Compute Sources Group	Enter the externally-facing ***public-IP-addresses*** of the users granted with access to the management interface of VMware Cloud Director Availability. **Important** Ensure that you add all the public IP addresses of each user allowed to access VMware Cloud Director Availability in VMware Cloud on AWS or the users have no access.
VCDA Manager Compute Group	Enter the ***private-IP-address*** of the Cloud Replication Management Appliance.
VCDA Replicators Compute Group	Enter the ***private-IP-addresses*** of all the Cloud Replicator Appliance instances.
VCDA Tunnel Compute Group	Enter the ***private-IP-address*** of the Cloud Tunnel Appliance.

e To save each compute group, click **Save**.

9 To prepare for completing the initial setup wizard, allow accessing the VMware Cloud Director Availability management interface by the trusted compute sources. Also allow the cloud appliances outbound access, both by adding two new compute gateway firewall rules.

a On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.

Repeat the following steps twice.

- Add a compute gateway firewall rule for allowing the trusted compute sources access to the Cloud Replication Management Appliance for completing the initial setup wizard of VMware Cloud Director Availability.
- Add a compute gateway firewall rule for allowing the VMware Cloud Director Availability appliances outbound network traffic from the compute gateway.

b On the **Compute Gateway** tab, click **Add Rule**.

c Configure each of the two compute firewall rules and click **Apply** when prompted.

Option	Inbound Compute Gateway Firewall Rule	Outbound Compute Gateway Firewall Rule
Name	Enter a name for the inbound compute gateway rule. For example, enter ***`VCDA Management from Trusted Compute Sources Rule`***.	Enter a name for the outbound compute gateway rule. For example, enter ***`VCDA Appliances Outbound Compute Rule`***.
Sources	Click **Any**. In the **Set Source** window, select the trusted compute sources group and click **Apply**. For example, select ***Trusted Compute Sources Group***.	Click **Any**. In the **Set Source** window select the three compute groups for the VMware Cloud Director Availability appliances and click **Apply**. For example, select all three ***VCDA Manager Compute Group***, ***VCDA Replicators Compute Group***, and ***VCDA Tunnel Compute Group***.
Destinations	Click **Any**. In the **Set Destination** window, select the Cloud Replication Management Appliance compute group and click **Apply**. For example, select ***VCDA Manager Compute Group***.	Any
Services	Click **Any**. In the **Set Services** window, select the Cloud Replication Management Appliance management interface service and click **Apply**. For example, select ***VCDA-Cloud-Service-Management*** **TCP (Source: Any | Destination: 8046)**.	Any
Applied To	All Uplinks	All Uplinks
Action	Allow	Allow

d After creating both compute gateway firewall rules, click **Publish**.

Results

The SDDC configuration in VMware Cloud on AWS is complete and ready for the initial configuration of VMware Cloud Director Availability. In summary, the SDDC network in VMware Cloud on AWS is configured with:

- ***vcda-network-segment*:**

  A dedicated routed network for all the cloud appliances of VMware Cloud Director Availability.

- **Public IP addresses:**

  Two requested public IP addresses, for the management interface of the Cloud Replication Management Appliance, and for the Service Endpoint of the Cloud Tunnel Appliance.

- **Management gateway:**
  - Access from the compute gateway source NAT address to the management gateway vCenter Server, used for bridging the access from the compute gateway VMware Cloud Director Availability appliances.
  - Access from the Cloud Replicator Appliance to the management gateway ESXi datastore, used for destination of migrations.
- **Compute gateway:**
  - Access from the *Trusted Compute Sources Group* to the management interface of the Cloud Service, used for completing the initial setup. Later, modifying the same rule allows access to all four types of management interfaces of VMware Cloud Director Availability. For more information, see Chapter 9 Post-configure the SDDC Networking in VMware Cloud on AWS.
  - Access from VMware Cloud Director Availability appliances to Internet, used for the external network traffic from the compute gateway.

For information about the summary of the SDDC network configuration, see Chapter 7 SDDC Network Configuration Summary.

What to do next

You can now configure VMware Cloud Director Availability in VMware Cloud on AWS by completing the initial setup wizard of the Cloud Replication Management Appliance. For more information, see Chapter 5 Configure VMware Cloud Director Availability in VMware Cloud on AWS.

Configure VMware Cloud Director Availability in VMware Cloud on AWS

5

After deploying all the cloud appliances in VMware Cloud on AWS, configure VMware Cloud Director Availability by configuring the Cloud Service instance in the Cloud Replication Management Appliance.

Prerequisites

- Verify that the *requested-VCDA-public-IP-address* is added as trusted in both the management and in the compute groups. For information about requesting and adding this public IP address in the trusted inventory groups, see step 8 in Prepare the SDDC for Deployment.
- Verify that the network settings of the SDDC are configured. For more information, see Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS .

Procedure

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

   a In a Web browser, go to `https://VCDA-management-public-IP-address:443/ui/admin`.

   To ensure your browser redirects you, the NAT rule applies, and the browser trusts the appliance certificate, enter both the `https://` prefix and the `/ui/admin` page suffix.

   b If this is the first time you are opening this page in this browser, cancel the certificate prompt for adding the certificate in your browser.

   c Select **Appliance login** and enter the **root** user password, set during the initial OVA deployment.

   d Click **Login**.

   As this Cloud Replication Management Appliance is not yet configured, you are redirected to `https://VCDA-management-public-IP-address/ui/portal/initial-config`.

2 In the **VCDA Appliance Password** window, change the initial **root** user password set during the OVA deployment.

   a Enter the initial **root** user password as configured during the OVA deployment.

   b Enter and confirm a new password.

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

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

   c After entering and confirming the new password, click **Apply**.

   The **Getting Started** page opens.

3 Under **Steps for fresh installation**, click the **Run the initial setup wizard** link.

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

4 To configure VMware Cloud Director Availability, complete the **Initial Setup** wizard.

   a On the **Licensing** page, enter a VMware Cloud Director Availability license key and click **Next**.

   After accepting the license key, if you cancel the wizard, on the next run of the wizard on the **Licensing** page the license key is pre-filled and greyed-out.

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

Option	Description
Site Name	Enter a site name for this Cloud Service instance. **Important** The site name is used as an identifier of this instance of VMware Cloud Director Availability and cannot be changed later without impacting the active replications.
Service Endpoint address	Enter `https://VCDA-tunnel-public-IP-address:443` and ensure that you enter the **443** port.
Description	Optionally, enter a description for this VMware Cloud on AWS site.
Choose which data engines to be enabled.	■ To enable migrations to VMware Cloud on AWS, select **VMC**. ■ To enable migrations to and from private cloud sites, select **Classic**.

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

Option	Description
VMware Cloud Director endpoint URL	Enter the public address of the Cloud Director instance and to autocomplete it as `https://Cloud-Director-service-Public-IPv6-Address/api`, press Tab. For example, use the IPv6 IP address you use to browse the Cloud Director instance.
VMware Cloud Director user name	Enter a local user for the Cloud Director instance. Use a **System administrator** user or a user with the **CDS provider admin** role, for example enter ***administrator@system***.
VMware Cloud Director password	Enter the password of the Cloud Director instance user.

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

d On the **Replicator Service instances** page, register the Cloud Service with the vCenter Server Lookup service and with the Replicator Service instances in the SDDC, then click **Next**.

Option		Description
Lookup Service Address		Enter the public URL address of the VMware Cloud on AWS vCenter Server Lookup service and to autocomplete the address as `https://vCenter-Public-URL:443/lookupservice/sdk`, press Tab. For example, use the public URL from the vCenter Server you use to browse vSphere in VMware Cloud on AWS and deploy the cloud appliances.
Use above Lookup Service address for Manager, Cloud and Tunnel		■ By default, the vCenter Server Lookup service address is used only for all the Replicator Service instances. By not using this address for the remaining services, their appliances show a yellow indicator which is expected for the vCenter Server Lookup service that is not configured. By not activating this toggle, single sign-on (SSO) user authentication is not available for the Manager Service, the Cloud Service, and the Tunnel Service. To later configure the vCenter Server Lookup service address for the services, see Configure VMware Cloud Director Availability to Accept the vCenter Server Lookup service Certificate in the *Administration Guide*. ■ To also use this vCenter Server Lookup service address for the Manager Service, for the Cloud Service, and for the Tunnel Service, and enable SSO for all services, activate this toggle.
Replicator 1	**Replicator Service address**	Enter the private IP address of the Cloud Replicator Appliance and to autocomplete the address as `https://Replicator-Private-IP-Address:8043`, press Tab.
	Replicator Service root password	Enter the password of the **root** user of the Replicator Service.
	Test Connection	Click to verify the connectivity to the endpoint and the **root** user password, and save the Replicator Service instance. If the initial **root** user password of the Cloud Replicator Appliance is not changed since deploying the appliance, you must change this password. Enter the initial **root** user password set during the OVA deployment, then enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: ■ 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 **cloud admin** user with administrative privileges in the single sign-on domain, for example enter ***cloudadmin@vmc.local***. **Note** Cannot use the **cloudadmin@vmc.local** user for single-sign-on (SSO) user authentication to the Cloud Service or for VMware Cloud Director Availability authentication.

Option		Description
	SSO password	The password for the administrative user.
	Description	Optionally, enter a description for the Replicator Service instance.
Add a Replicator Service Instance		Optionally, add additional Replicator Service instances.

Verify the thumbprints and accept the SSL certificates of the vCenter Server Lookup service in VMware Cloud on AWS and of all the Replicator Service instances.

e On the **Tunnel Service** page, register the Cloud Service with the Tunnel Service, test the connection, and click **Next**.

Option	Description
Tunnel Service address	Enter the private IP address of the Cloud Tunnel Appliance and to autocomplete the address as `https://Tunnel-Private-IP-Address:8047`, press Tab.
Root password	Enter the password of the **root** user of the Tunnel Service.
Test Connection	Click to verify the connectivity to the endpoint and the **root** user password, and save the Tunnel Service instance. If the initial **root** user password of the Cloud Tunnel Appliance is not changed since deploying the appliance, you must change this password. Enter the initial **root** user password set during the OVA deployment, then enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of: ■ 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.

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

5 To allow the tenants to perform migrations, assign them with a replication policy.

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

b (Optional) Create a replication policy or modify the Default policy to allow replications.

c To assign a replication policy click **Assign** and select the organizations to assign the policy to.

Alternatively, click **Organizations** and after selecting the organizations to assign a policy to, click **Assign** and select the policy to assign.

Results

VMware Cloud Director Availability configuration in VMware Cloud on AWS is complete.

What to do next

You can now configure the network of VMware Cloud on AWS for pairing with on-premises tenants and with remote cloud sites. For more information, see Chapter 6 Configure the SDDC Network for Pairing VMware Cloud Director Availability in VMware Cloud on AWS.

Configure the SDDC Network for Pairing VMware Cloud Director Availability in VMware Cloud on AWS

6

After deploying and configuring VMware Cloud Director Availability and the external access, the next step is configuring from where VMware Cloud on AWS allows establishing pairings. Create an additional compute group with the public IP addresses allowed for pairing and an additional firewall rule allowing the access from this new group to the Service Endpoint.

To allow pairing with VMware Cloud Director Availability in VMware Cloud on AWS, in the compute group below add the public IP addresses of the Service Endpoint instances and the on-premises appliances.

Prerequisites

- Verify that before pairing, network port 3030/TCP from the remote Cloud Tunnel Appliance and the remote On-Premises to Cloud Director Replication Appliance to the Cloud Replicator Appliance in VMware Cloud on AWS is allowed. For information about the required network ports, see https://ports.vmware.com/home/VMware-Cloud-Director-Availability.
- Verify that VMware Cloud Director Availability in VMware Cloud on AWS is configured. For more information, see Chapter 5 Configure VMware Cloud Director Availability in VMware Cloud on AWS.

Procedure

1. Log in to VMware Cloud on AWS at https://vmc.vmware.com.
2. In the VMC console, in the left pane click **SDDCs**.
3. Under the SDDC click **View Details** and click the **Networking & Security** tab.
4. To allow accessing the Service Endpoint compute gateway service in VMware Cloud on AWS, create a compute group containing the remote sites IP addresses.
   a. On the **Networking & Security** tab, in the left pane under the **Inventory** section click **Groups**.
   b. To create the compute group, under the **Compute Groups** tab, click **Add Group** and enter a group name, for example enter ***`VCDA Pairing Compute Group`***.
   c. To add trusted sites members to the compute group, under the Compute Members column, click the **Set Members** link.

d In the **Select Members** window, on the **IP Addresses** tab enter the IP addresses of the following site members and click **Apply**.

- To allow each private cloud site backed by VMware Cloud Director pairing, add the Service Endpoint ***public-IP-address*** of the Cloud Tunnel Appliance in the private cloud site.
- To allow each tenant pairing, add the ***public-IP-addresses*** of all their On-Premises to Cloud Director Replication Appliance instances.

Important Adding or removing IP addresses from this compute group controls which remote cloud sites and on-premises tenants can establish pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

Before VMware Cloud Director Availability pairs with another site, to allow the pair add the remote site IP address in the *VCDA Pairing Compute Group*.

e To save the pairing compute group, click **Save**.

5 To allow access from the pairing compute group, create a compute gateway firewall rule.

a On the **Networking & Security** tab, in the left pane under the **Security** section, click **Gateway Firewall**.

b On the **Compute Gateway** tab, click **Add Rule** and configure the following settings.

Option	Description
Name	Enter a name for the compute gateway firewall rule, for example enter ***VCDA Pairing Compute Rule***.
Sources	Click **Any** in the Sources column, then in the **Set Source** window select **User Defined Groups**, select the pairing IP addresses compute group, for example select ***VCDA Pairing Compute Group***, and click **Apply**.
Destinations	Click **Any** in the Sources column, then in the **Set Source** window select **User Defined Groups**, select the Cloud Tunnel Appliance IP address compute group, for example select ***VCDA Tunnel Compute Group***, and click **Apply**.
Services	In the Services column, click **Any**, then in the **Set Source** window, select the Service Endpoint service, for example select ***VCDA-Service-Endpoint*** **TCP (Source: Any | Destination: 8048)** and click **Apply**.
Applied To	All Uplinks
Action	Allow

By default, the new compute gateway firewall rule is enabled, allowing the Cloud Tunnel Appliance Service Endpoint access from the pairing IP addresses compute group.

c To publish the new compute gateway firewall rule, click **Publish**.

The new rule receives an integer ID value, used in the log entries that it generates.

Results

VMware Cloud Director Availability in VMware Cloud on AWS allows pairing with On-Premises to Cloud Director Replication Appliance instances and with VMware Cloud Director Availability instances in private cloud sites backed by VMware Cloud Director.

What to do next

- Tenants can now configure and pair their On-Premises to Cloud Director Replication Appliance and migrate their workloads to VMware Cloud on AWS. For more information, see Configure and Pair the On-Premises to Cloud Director Replication Appliance.
- You can now pair private cloud sites and migrate cloud workloads to VMware Cloud on AWS. For more information, see Pair VMware Cloud Director Cloud Sites.
- You can allow administrative operations by using the management interfaces of the services of VMware Cloud Director Availability. For more information, see Chapter 9 Post-configure the SDDC Networking in VMware Cloud on AWS.

SDDC Network Configuration Summary

7

After configuring the network of the SDDC and configuring the network of VMware Cloud on AWS for pairing with remote VMware Cloud Director Availability sites, check the summary of the network configuration.

Management Gateway Firewall Rules

Name	Sources	Destinations	Services	Explanation
vCenter Inbound From Trusted Management Sources Rule	*Trusted Management Sources Group*	vCenter	HTTPS	Allows the trusted management sources accessing the management gateway vCenter Server for the deployment of the cloud appliances in the compute gateway.
SNAT VCDA to vCenter Rule	*SNAT VCDA Management Group*	vCenter	HTTPS	Allows the compute gateway source NAT accessing the management gateway vCenter Server for bridging the access from the compute gateway cloud VMware Cloud Director Availability appliances.
VCDA Replicators to ESXi Rule	*VCDA Replicators Management Group*	ESXi	■ HTTPS ■ Provisioning & Remote Console	Allows all the Cloud Replicator Appliance instances writing in the destination ESXi datastore.

For information about creating these management firewall rules, see Chapter 2 Prepare the SDDC in VMware Cloud on AWS for Deployment and Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS .

Compute Gateway Firewall Rules

Name	Sources	Destinations	Services	Explanation
VCDA Management from Trusted Compute Sources Rule	*Trusted Compute Sources Group*	*VCDA Manager Compute Group*	*VCDA-Cloud-Service-Management* TCP (Source: Any | Destination: 8046)	Allows the trusted compute sources accessing the management interface of the Cloud Service for completing the initial setup. Later, modifying the same rule allows access to all four types of management interfaces of VMware Cloud Director Availability. For more information, see Chapter 9 Post-configure the SDDC Networking in VMware Cloud on AWS.
VCDA Appliances Outbound Compute Rule	■ *VCDA Manager Compute Group* ■ *VCDA Replicators Compute Group* ■ *VCDA Tunnel Compute Group*	Any	Any	Allows the VMware Cloud Director Availability appliances to Internet for the external network traffic from the compute gateway.
VCDA Pairing Compute Rule	*VCDA Pairing Compute Group*	*VCDA Tunnel Compute Group*	*VCDA-Service-Endpoint* TCP (Source: Any | Destination: 8048)	Allows the on-premises tenants and the remote cloud sites backed by VMware Cloud Director pairing with VMware Cloud Director Availability in VMware Cloud on AWS.

For information about creating these compute firewall rules, see Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS and Chapter 6 Configure the SDDC Network for Pairing VMware Cloud Director Availability in VMware Cloud on AWS.

Pairing with Remote Sites

8

Pair the local site in VMware Cloud on AWS with remote VMware Cloud Director Availability sites for migrating their workloads over. Pair this site with On-Premises to Cloud Director Replication Appliance and with cloud sites backed by VMware Cloud Director.

This chapter includes the following topics:

Configure and Pair the On-Premises to Cloud Director Replication Appliance

In the tenants data centers, by using the management interface of the On-Premises to Cloud Director Replication Appliance, you must first change the initial **root** user password that you set during the OVA deployment. Then you register the appliance with the local vCenter Server Lookup service and with VMware Cloud Director Availability in VMware Cloud on AWS.

Prerequisites

- Verify that before pairing the *tenant-public-IP-address* of the tenant data center where the On-Premises to Cloud Director Replication Appliance is deployed is added as a trusted IP address. As a service provider, for information about adding the tenants IP addresses, see step 8 in Prepare the SDDC for Deployment.
- Verify that before pairing VMware Cloud Director Availability in VMware Cloud on AWS is configured. As a service provider, for more information, see Chapter 5 Configure VMware Cloud Director Availability in VMware Cloud on AWS.

Procedure

1. Log in to the management interface of the On-Premises to Cloud Director Replication Appliance.
   a. In a Web browser, go to `https://On-Prem-Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** and enter the **root** user password, set during the initial OVA deployment.
   c. Click **Login**.

As the appliance is not yet configured, it redirects you to the **https://*On-Prem-Appliance-IP-Address*/ui/portal/initial-config** page.

2 In the **VCDA Appliance Password** window, change the initial **root** user password set during the OVA deployment.

a Enter the initial **root** user password as configured during the OVA deployment.

b Enter and confirm a new password.

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

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

c After entering and confirming the new password, click **Apply**.

The **Getting Started** page opens.

3 Click the **Run the initial setup wizard** link.

4 To pair the On-Premises to Cloud Director Replication Appliance with VMware Cloud Director Availability in VMware Cloud on AWS, complete the **Initial Setup** wizard.

a On the **Lookup Service Details** page, enter the local vCenter Server Lookup service and its user credentials, and click **Next**.

Option	Description
Lookup Service Address	Enter the IP address of the local vCenter Server Lookup service in the on-premises data center and to autocomplete the address as `https://Lookup-Service-IP-Address:443/lookupservice/sdk`, press Tab.
SSO Admin Username	Enter a local user with administrative privileges in the on-premises single sign-on domain, for example *Administrator@VSPHERE.LOCAL*.
Password	Enter the password for the administrative user.

Verify the thumbprints and accept the SSL certificates of the on-premises vCenter Server Lookup service.

b On the **Site Details** page, enter a name for this on-premises site and click **Next**.

Option	Description
Site Name	Enter a site name for this On-Premises to Cloud Director Replication Appliance. **Important** The site name is used as an identifier of this on-premises appliance instance and cannot be changed later.
Description	Optionally, enter a description for this site.

c On the **Cloud Details** page, pair the on-premises VMware Cloud Director Availability appliance and the VMware Cloud Director Availability in VMware Cloud on AWS.

Option	Description
Service Endpoint address	Enter the public IP address of the Service Endpoint of the VMware Cloud Director Availability in VMware Cloud on AWS as supplied by the service provider.
Organization Admin	Enter the **organization administrator** user of the Cloud Director instance, for example **`admin@org`**.
Organization Password	Enter the password for the **organization administrator** user.
Allow Access from Cloud	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 discover on-premises workloads and replicate them to the cloud.

If the VMware Cloud Director Availability cloud site in VMware Cloud on AWS does not use a valid CA-signed certificate, verify the thumbprint and accept the SSL certificate of the Tunnel Service Service Endpoint at the VMware Cloud Director Availability in VMware Cloud on AWS.

d On the **Ready to complete** page, select **Configure local placement now** and click **Finish**.

The On-Premises to Cloud Director Replication Appliance is paired with VMware Cloud Director Availability in VMware Cloud on AWS.

5 To configure the On-Premises to Cloud Director Replication Appliance placement of virtual machines, complete the **Configure Placement** wizard.

a On the **VM Folder** page, browse the location for the recovered virtual machines and click **Next**.

b On the **Compute Resource** page, browse the destination compute resource for the recovered virtual machines and click **Next**.

c On the **Default Network** page, browse the network to connect the network interfaces of the virtual machines to after failover and click **Next**.

d On the **Datastore** page, browse where to store the replicated virtual machines and disk files and click **Next**.

e On the **Ready To Complete** page, verify the selected configuration and click **Finish**.

Results

The On-Premises to Cloud Director Replication Appliance is configured and paired with VMware Cloud on AWS.

What to do next

You can now create migrations and migrate workloads from this paired on-premises site to VMware Cloud on AWS. These migrations to VMware Cloud Director service follow the same configuration as the migrations to VMware Cloud Director. For information about creating a migration and migrating the workload, see Create a Migration and Perform a Migrate Task in the *User Guide*.

Pair VMware Cloud Director Cloud Sites

To support migrations from private cloud sites running VMware Cloud Director to VMware Cloud Director service, in the private cloud deploy or upgrade to VMware Cloud Director Availability 4.2, pair the existing instance of VMware Cloud Director Availability operating in this private cloud and enable the VMC data engine.

In addition to migrating workloads from on-premises sites to VMware Cloud on AWS, to perform migrations from VMware Cloud Director cloud sites, also called private cloud sites, first pair then configure them with the VMC data engine.

Prerequisites

- Verify that VMware Cloud Director Availability 4.2 is deployed in the private cloud site.
- **Important** Verify that before pairing a private cloud site, the Service Endpoint *public-IP-address* of the Cloud Tunnel Appliance in the private cloud site is added as trusted in both the management and in the compute groups in the VMware Cloud on AWS SDDC. For information about adding the IP address in the trusted inventory groups, see Chapter 2 Prepare the SDDC in VMware Cloud on AWS for Deployment.
- Verify that VMware Cloud Director Availability configuration in the VMware Cloud on AWS environment is complete. For more information, see Chapter 5 Configure VMware Cloud Director Availability in VMware Cloud on AWS.

Procedure

1. Pair the private cloud site. For information about the pairing see Managing Connections Between Cloud Sites and Pair Cloud Sites in the *Administration Guide*.

   You established trust between VMware Cloud Director Availability in VMware Cloud on AWS and the paired private cloud site.

2 To enable migrations to VMware Cloud on AWS from the paired private cloud site, in VMware Cloud Director Availability in the private cloud site select the VMC data engine.

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

   b Under **Site settings**, next to **Data engine**, click **Edit**.

   c In the **Data engine** window, select **VMC** and click **Apply**.

   Note The existing replications from the private cloud site can continue operating when both the classic and the VMC data engines are selected.

   If VMware Cloud Director Availability is only paired with VMware Cloud on AWS and not paired with private cloud sites, do not enable the **Classic** engine.

Results

The private cloud site is paired and prepared to migrate workloads to the VMware Cloud on AWS environment.

What to do next

You can now create migrations and migrate workloads from the paired private cloud site to VMware Cloud on AWS. These migrations to VMware Cloud Director service follow the same configuration as migrations to VMware Cloud Director. For information about creating a migration and migrating the workload, see Create a Migration and Perform a Migrate Task in the *User Guide*.

Post-configure the SDDC Networking in VMware Cloud on AWS

9

To allow access to the management interfaces of the Manager Service, the Replicator Service instances and the Tunnel Service in VMware Cloud on AWS for performing administrative operations like certificate replacement, post-configure the network settings of the SDDC for the additional access to these three types of management interfaces.

By default, the access limited in VMware Cloud on AWS and the public IP addresses of all the cloud appliances of VMware Cloud Director Availability must be explicitly allowed for performing administrative operations.

VMware Cloud Director Availability appliances in VMware Cloud on AWS provide three types of management interfaces for performing administrative tasks like certificate replacement and others. To allow these management interfaces when configuring the necessary NAT rules, you explicitly define them since the three interfaces internally use non-standard HTTPS ports. These three services in conjunction with the following three NAT rules and a firewall rule translate and allow the network traffic coming to the public IP addresses of the appliances on the external port 443/TCP:

- Towards the Cloud Replication Management Appliance, internally on port 8044/TCP for the management interface of the Manager Service.
- Towards all Cloud Replicator Appliance instances, internally on port 8043/TCP for the management interfaces of the Replicator Service instances.
- Towards the Cloud Tunnel Appliance, internally on port 8047/TCP for the management interface of the Tunnel Service.

Prerequisites

- Verify that the SDDC network is already configured for VMware Cloud Director Availability pairing. For information about the required steps, see Chapter 6 Configure the SDDC Network for Pairing VMware Cloud Director Availability in VMware Cloud on AWS.
- Verify that VMware Cloud Director Availability 4.2 or later is deployed in VMware Cloud on AWS. For more information, see Chapter 3 Deploy VMware Cloud Director Availability in the SDDC.

Procedure

1 Log in to VMware Cloud on AWS at https://vmc.vmware.com.

2 Add three new inventory SDDC services, for the management interfaces of the Manager Service, Replicator Service, and the Tunnel Service.

   a In the VMC console, in the left pane click **SDDCs**.

   b Under the SDDC click **View Details** and click the **Networking & Security** tab.

   c In the left pane under the **Inventory** section, click **Services**.

      Repeat the following steps three times:

      - Add an inventory service for the Manager Service of the Cloud Replication Management Appliance.
      - Add another inventory service for the Replicator Service of the Cloud Replicator Appliance.
      - Add another inventory service for the Tunnel Service of the Cloud Tunnel Appliance.

   d To add an inventory SDDC service, click **Add Service**.

   e Enter a name and optionally a description for each service.

   f For each service, in the Service Entries column, click the **Set Service Entries** link.

   g For each service, in the **Set Service Entries** window, from the **Type** drop down menu select **Layer 3 and above**.

h For each service, on the **Port-Protocol** tab click **Add Service Entry**, enter the details from the respective column, and click **Apply**.

Option	Manager Service Inventory Service	Replicator Service Inventory Service	Tunnel Service Inventory Service
Name	Enter a name for the management interface service entry of the Cloud Replication Management Appliance Manager Service. For example, enter ***VCDA-Manager-Service-Management***.	Enter a name for the management interface service entry of the Cloud Replicator Appliance Replicator Service. For example, enter ***VCDA-Replicator-Service-Management***.	Enter a name for the management interface service entry of the Cloud Tunnel Appliance Tunnel Service. For example, enter ***VCDA-Tunnel-Service-Management***.
Service Type	Select **TCP**.	Select **TCP**.	Select **TCP**.
Additional Properties	Leave the **Source Ports** text box blank.	Leave the **Source Ports** text box blank.	Leave the **Source Ports** text box blank.
	To access the management interface of the Manager Service in the Cloud Replication Management Appliance in the **Destination Ports** text box, in enter port **8044**.	To access the management interface of the Replicator Service in the Cloud Replicator Appliance, in the **Destination Ports** text box enter port **8043**.	To access the management interface of the Tunnel Service in the Cloud Tunnel Appliance, in the **Destination Ports** text box enter port **8047**.

i To save each inventory service, click **Save**.

On the **Services** page, the three new services show:

Name	Service Entries
VCDA-Manager-Service-Management	TCP (Source: Any | Destination: **8044**)
VCDA-Replicator-Service-Management	TCP (Source: Any | Destination: **8043**)
VCDA-Tunnel-Service-Management	TCP (Source: Any | Destination: **8047**)

3 To later use in NAT rules, request new public SDDC IP addresses for each of the three types of management interfaces.

- Request a public IP address to access the management interface of the Manager Service in the Cloud Replication Management Appliance.
- Request multiple public IP addresses to access the management interface of each Replicator Service in the Cloud Replicator Appliance instances.

- Request a public IP address to access the management interface of the Tunnel Service in the Cloud Tunnel Appliance.

a On the **Networking & Security** tab, in the left pane under the **System** section click **Public IPs**.

b To request a public IP address for the Manager Service, click **Request New IP**, enter a note, and click **Save**.

For example, as a note enter ***VCDA-Manager-Public-Management-IP-address***.

Repeat the following step for each instance of the Replicator Service deployed in the SDDC:

c To request a public IP address for each Replicator Service, click **Request New IP**, enter a note and click **Save**.

For example, as a note enter ***VCDA-Replicator-Public-Management-IP-address***. For more Replicator Service instances, for each requested public IP address enter ***VCDA-Replicator-X-Public-Management-IP-address***, where *X* marks each instance.

d To request a public IP address for the Tunnel Service, click **Request New IP**, enter a note and click **Save**.

For example, as a note enter ***VCDA-Tunnel-Public-Management-IP-address***.

4 To forward the incoming network traffic to the correct cloud appliances and ports, add new NAT rules.

a On the **Networking & Security** tab, in the left pane under the **Network** section click **NAT**.

Repeat the following step three times:

- Add a NAT rule for the management interface of the Manager Service in the Cloud Replication Management Appliance.
- Add another NAT rule for the management interface of the Replicator Service in the Cloud Replicator Appliance. For each additional Replicator Service instance, add another NAT rule.
- Add another NAT rule for the management interface of the Tunnel Service in the Cloud Tunnel Appliance.

b To add a NAT rule, click **Add NAT Rule**, configure the following settings then click **Save**.

Option	Manager Service NAT	Replicator Service NAT	Tunnel Service NAT
Name	Enter a name for the NAT rule for the management interface of the Cloud Replication Management Appliance Manager Service. For example, enter ***`VCDA Replication Management NAT`***.	Enter a name for the NAT rule for the management interface of the Cloud Replicator Appliance Replicator Service. For example, enter ***`VCDA Replicator NAT`***. For more Replicator Service instances, for each NAT rule enter ***`VCDA Replicator X NAT`***, where *X* marks each instance.	Enter a name for the NAT rule for the management interface of the Cloud Tunnel Appliance Tunnel Service. For example, enter ***`VCDA Replication Management NAT`***.
Public IP	Select the *VCDA-Manager-Public-Management-IP-address*.	Select the *VCDA-Replicator-Public-Management-IP-address*.	Select the *VCDA-Tunnel-Public-Management-IP-address*.
Service	Select the inventory service for the Cloud Replication Management ApplianceManager Service. For example, select *VCDA-Manager-Service-Management*.	Select the inventory service for the Cloud Replicator Appliance Replicator Service. For example, select *VCDA-Replicator-Service-Management*.	Select the inventory service for the Cloud Tunnel ApplianceTunnel Service. For example, select *VCDA-Tunnel-Service-Management*.
Public Port	Enter port **`443`**.	Enter port **`443`**.	Enter port **`443`**.
Internal IP	Enter the ***`private-IP-address`*** of the Cloud Replication Management Appliance.	Enter all ***`private-IP-addresses`*** of the Cloud Replicator Appliance instances.	Enter the ***`private-IP-address`*** of the Cloud Tunnel Appliance.
Internal Port	8044 (non-editable)	8043 (non-editable)	8047 (non-editable)
Firewall	Match Internal Address	Match Internal Address	Match Internal Address

5 To allow accessing the VMware Cloud Director Availability management interfaces from the trusted compute sources, add the three new services and destinations in the inbound compute firewall rule.

The compute rule *VCDA Management from Trusted Compute Sources Rule* is created first in Chapter 4 Configure the Network of the SDDC in VMware Cloud on AWS .

a On the **Networking & Security** tab, in the left pane under the **Security** section click **Gateway Firewall**.

b On the **Compute Gateway** tab, click the already created ***VCDA Manager from Trusted Compute Sources Rule***.

c Configure the compute firewall rule then click **Apply** when prompted.

Option	Compute Firewall Rule
Name	***VCDA Management from Trusted Compute Sources Rule***.
Sources	***Trusted Compute Sources Group***.
Destinations	Click **Any**. In the **Set Destination** window, select all the compute groups of the VMware Cloud Director Availability appliances and click **Apply**. For example, select all three: ■ ***VCDA Manager Compute Group*** ■ ***VCDA Replicators Compute Group*** ■ ***VCDA Tunnel Compute Group***
Services	Click **Any**. In the **Set Services** window, select the three newly created inventory services in addition to the ***VCDA-Cloud-Service-Management TCP (Source: Any | Destination: 8046)***. For example, select additionally: ■ ***VCDA-Manager-Service-Management*** **TCP (Source: Any | Destination: 8044)** ■ ***VCDA-Replicator-Service-Management*** **TCP (Source: Any | Destination: 8043)** ■ ***VCDA-Tunnel-Service-Management*** **TCP (Source: Any | Destination: 8047)** When selected, all four management interface services are now present: `Destination: 8046`, `Destination: 8044`, `Destination: 8043`, and `Destination: 8047`.
Applied To	All Uplinks
Action	Allow

d After modifying the compute gateway firewall rule, click **Publish**.

The compute firewall rule allows access to the four types of management interfaces of all services of VMware Cloud Director Availability:

- Cloud Service
- Manager Service
- Each Replicator Service instance
- Tunnel Service

Results

The SDDC configuration in VMware Cloud on AWS is complete and ready for administrative operations of the VMware Cloud Director Availability services.

What to do next

You can now perform administrative tasks for each VMware Cloud Director Availability service. For more information, see the *Administration Guide* for the version of VMware Cloud Director Availability deployed in the SDDC.