# Migrations to VMware Cloud Director service

Using VMware Cloud Director Availability



# Table of contents

Migrations to VMware Cloud Director service	3
Prerequisites	3
Deployment	5
Provider setup	5
Tenant setup	7
Additional SDDC configuration	
Add Inventory Services	8
Request Public IPs	9
Create a Compute Group	9
Create Management Groups	10
Configure the Compute Gateway Firewall	12
Configure the Management Gateway Firewall	13
Add NAT rules	13
Initial setup	
Provider setup	15
Tennant setup	17
Pairing with another Cloud	
Migration	
Table of Figures	21

# Migrations to VMware Cloud Director service

With the native integrations with VMware Cloud Director and vCenter, VMware Cloud Director Availability tenants can easily perform migration and onboarding tasks from their on-premises vCenter environment to your VMware Cloud Director backed cloud. However, due to some design specifics of Cloud Director service hosted at VMC on AWS, there was no option for migrating workloads from on-premises to Cloud Director service.

With VMware Cloud Director Availability 4.2, this scenario is now fully supported. It means you or your tenants, depending on the offered service, can follow the well-known flow used so far and still get their workloads migrated to Cloud Director service.

# Prerequisites

To be able to successfully deploy and run VMware Cloud Director Availability in your VMC on AWS environment, you will need to make sure the following requirements are met:

- 1. Have a properly deployed Software-Defined Data Center (SDDC).
- 2. Have a VMware Cloud Director deployed at VMC on AWS (Cloud Director service) that is linked to the SDDC.
- 3. Have defined at least one Organization, OrgVDC with *Hardware Version* (Default is Hardware Version 14 vCenter 6.7.0) higher than one you have in the vCenter you would like to use as a source location
- 4. Have defined at least one tenant admin user.
- 5. (Recommended) Have a dedicated routed network for the VMware Cloud Director Availability appliances. (You can still use any existing routed network). Obtain its CIDR from **Networking & Security** → **Network** → **Segments**.

< ALL SDDCs								TER ACTIONS -
(in the second of the second o								
Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support								
Overview	Segments							Ø
Network	Segment List	Segment Profiles						
VPN								_ Search
NAT Tigs 1 Categorius								
Transit Connect		Segment Name	Connected Gateway		Subnets		Ports	Status ()
Security		orgi NW-Obesaezi esoa-4	Orgzebge ( Tiert		192.100.200.024			Success C
Gateway Firewall								🍯 Success 🖱
Distributed Firewall								🌕 Success 😋
Inventory Groups								🌕 Success 😋
Services Virtual Machines	i 🖂 🚳							Success C
Tools								
IPFIX								VIEW RELATED GROUPS
Port Mirroring								
System								
DHCP		SEGMENT PROFILES						
Global Configuration		DHCP STATIC BINDINGS						
Public IPs Direct Connect								😑 Success 🖱
Connected VPC								1 - 12 of 12 Segments

Figure 1 - SDDC Network Segments

6. Obtain the proper **Source NAT Public IP** of your SDDC from **Networking & Security** → **Overview**.

	VMC on AWS 💿 US West (Oregon)		OPEN VCENTER	ACTIONS -
Summary Networking	& Security Add Ons Maintenance Overview	Troubleshooting Settings Support		
Network Segments VPN NAT Tier-I Gateways Transit Connect Security		VPN Public IP-44.239.45.77 Management Galeway ++++++++++++++++++++++++++++++++++++	annat S	
Gateway Firewall Distributed Firewall Inventory Groups Services Virtual Machines Tools		NSX, vCenter, ESXI Appliers balanti Inferioritations balanti Origina Default Compute Galaway +8 COWs	Os hemiaes / Ecternal ábes	
IDEA IPFIX Port Mirroring System DHS DHS Global Configuration Public IPs Direct Connect Connected VPC		Worklands Server that a to the server that have the server the server that have the server the serve	Connected VIC (yes: eth28(197)	g g F A

Figure 2 - SDDC Network Overview



7. Obtain the proper DNS Service IP of your SDDC from Networking & Security  $\rightarrow$  System  $\rightarrow$  DNS.

CALL SUDCE					
TPM SDDC					
Summary Networking	& Security Add C				
Overview	DNS Servic	es			0
Network	DNS Services				
Segments VPN NAT					
Tier-1 Gateways					
Transit Connect Security				Compute Gateway Default Zone Server IP 1 8.8.8.8	cess 🖱
Gateway Firewall					
Inventory Groups				Management Gateway Default Zor Server IP 1 8.8.8 Server IP 2 8.8.4.4	ccess 🕑
Services Virtual Machines					
Tools IPFIX Port Mirroring					
System					
DNS					
Global Configuration					
Public IPs					
Direct Connect					2 of 2 PMI Encires
CONTRACTOR VPG					2 of 2 brids services



8. Create a Trusted IPs group from Network & Security → Inventory → Group → Compute Groups where you will add your public IP address so you can access the VMware Cloud Director Availability portal. Then in this group you will need to add all your tenant IP addresses so they can connect their on-premises appliances to your VMware Cloud Director Availability cloud.

< ALL SDDCs			OPEN VCENTER ACTIONS
TPM SDDC			
Summary Networking	8 Security Add Ons Maintenance Troubleshooting Setting		
Overview	Groups		
Network	Management Groups Compute Groups		
Segments VPN NAT			
Tier-1 Gateways		Compute Hembers	
Transit Connect			
Security Gateway Firewall			
Distributed Pirewall			
Groups			
Services Virtual Machines			
Tools			
IPFIX Port Mirroring			
System DNS DHCP Global Configuration Public IPs Direct Connect			
Connected VPC	Canada		1 - 7 of 7 Groups

Figure 4 - Compute Groups

9. Create a Compute Gateway Firewall Rule with the following settings to allow access from your trusted IPs to the environment:

< ALL SDDCs OPEN VCENTER   ACTIONS											
(☆) TPM SDDC   VMCon AWS () US West (Oregon)											
Summary Networking	- Simman Nationalism & Samative And Proc. Maintenainea. Trin Maithendine. Sattlines. Summet										
Overview	Gat	eway f	Firewall								0
Network		gement G	Compute Ga	teway Tier1 Gateways							
Segments VPN										VERT	PUBLISH
NAT											-
Transit Connect											
Security			Trusted VCDA inbound	2064	88 VCDA Trusted A_	Any	Any	All Uplinks	• wolk •		9 🖂
Distributed Firewall		0	VCDA Tunnel Inbound	2061	Any	Any	VCDA_Public_En	All Uplinks	• Allow ~		<b>9</b> 🖸
Inventory Groups			VCDA Appliances Outb	2055	88 VCDA Appliances			All Uplinks	Allow ~		
Services Virtual Machines			OSE Inbound SSH	2054		SS OSE	O SSH	Internet Interface	• Allow ~	•	۵ 🕫
Tools			OSE Inbound HTTPS	2053	Any	88 OSE	O HTTPS	All Uplinks	• wolk_		9 🖂
IPFIX Port Mirroring			OSE Outbound	2052	88 OSE	Any	Any	Internet Interface	• wolk •		9 🖂
System DNS			Tenant Inbound Access	2051	Any	22 External Networ	Any	Internet Interface	• wollA	•	<b>9</b> 62
DHCP Global Configuration			Tenant Outbound Acce	2050	60 External Networ	Any	Any	Internet Interface	• Allow ~		9 69
Public IPs Direct Connect			CSE Outbound access	2038	Stresserver	Any	KubeAccess	Internet Interface	Alow ~	•	9 C
Connected VPC											13 Rules

Figure 5 - Compute Gateway Firewall Rules



10. Create a new Resource Pool for the VMware Cloud Director Availability Appliances under the Compute-Resource Pool.



Figure 6 - Dedicated Resource Pool

# Deployment

To start the deployment process, first download the proper OVA files for provider and on-premises.

#### Provider setup

This guide provides the necessary configuration steps for the separate appliances case and NOT for the combined appliance.

Please repeat the mentioned steps for each of the appliances – Cloud Replication Management appliance, Cloud Replicator appliance and Cloud Tunnel appliance.

- 1. Log in to the vCenter UI from your VMC console.
- 2. Deploy the OVA template in the Resource pool created in Requirement #8 in the Prerequisites section.
- 3. The deployment steps are similar to the VMware Cloud Director Availability 4.1 OVA deployment (*https://blogs.vmware.com/cloudprovider/2020/11/vmware-cloud-director-availability-4-1-initial-setup-improvements.html*). There are only a few considerations to be taken:
  - a. On Step 7 Select Storage: Select Workload Datastore

Deploy OVF Template	Select storage						$\times$
1 Select an OVF template	Select the storage for the co Select virtual disk format:	onfiguration and dis	sk files	As defined in the	VM storage polic	y ~	
	VM Storage Policy:				atastore Defa	ult v	
2 Select a name and folder	Name	Capacity	Provisioned	Free	Туре	Cluster	
2. Select a compute resource	🗐 vsanDatastore	10.37 TB	2.99 TB	9.08 TB	VSAN		
3 Select a compute resource	WorkloadDatastore	10.37 TB	2.11 TB	9.08 TB	VSAN		
4 Review details							
5 License agreements							
6 Configuration							
7 Select storage							
8 Select networks							
9 Customize template							
10. Ready to complete	Compatibility						
	Compatibility checks su	ucceeded.					
					CANCEL	ВАСК	хт

Figure 7 - Datastore selection



b. On Step 8 – Select networks: Select the dedicated network for VMware Cloud Director Availability from Requirement #4 in the Prerequisites section.

Deploy OVF Template	Select networks Select a destination network for each source network.				×
1 Select an OVF template		_			
2 Select a name and folder	Select Network	×		<u>~</u>	
3 Select a compute resource	Ť				1 items
4 Review details	Name	NS:			
5 License agreements	O & RoutedNetwork-4f6871eb-17bb-4286-9351-d90850dc5924				
	O & sddc-cgw-network-1				
6 Configuration	SI_LogicalSwitch_00bd8228-d9ea-46a5-a532-463e3f88b3c3	-			
	O & SI_LogicalSwitch_10c443f9-7217-4e33-a78e-1dd98bf56326				
7 Select storage	💿 🕹 VCDA	-			
8 Select networks	O & VMC-None				
9 Customize template	0 - 0 of 0	Ditems			
10 Ready to complete	CANCEL	ок			
			CANCEL	BACK	NEXT

Figure 8 - Network selection

- c. On Step 9 Customize template:
  - i. In the Address field provide an address in the dedicated network for VMware Cloud Director Availability from Requirement #4 in the Prerequisites section.
  - ii. In the DNS servers field provide the **DNS Service IP** address from Requirement #6 in the Prerequisites section.

Deploy OVF Template	Customize template	×
1 Select an OVF template	Hostname	The hostname of the VM. Leave blank if DHCP is desired. vcda42b-mgmt-201
<ol> <li>Select a name and folder</li> <li>Select a compute resource</li> </ol>	Address	IP address in CIDR notation (e.g. 10.71.219.227/21). Leave blank if DHCP is desired. 172.26.46.201/24
4 Review details 5 License agreements	Gateway	Gateway address (e.g. 10.71.223.253). This field is ignored if the address is empty. Leave blank if DHCP is desired. 172.26.46.1
6 Configuration 7 Select storage	MTU (bytes)	Maximum transmission unit in bytes (e.g. 1500). This field is ignored if the address is empty. Leave blank if DHCP is desired. 1500
8 Select networks 9 Customize template	DNS servers	Comma-separated list of DNS servers to use (e.g. 10.71.223.252,10.71.223.252). Leave blank if DHCP is desired. 10.2.192.12
IV Ready to complete	Search Domains	Comma-separated list of search domains to use (e.g. local,lan). Leave blank if DHCP is desired. vmc.local CANCEL BACK NEXT

Figure 9 – VMware Cloud Director Availability Network settings

4. After you have successfully deployed the 3 appliances, you should see something similar to:



Figure 10 - Deployed appliances view in vCenter

## Tenant setup

Provide the on-premises OVA file to your tenants so they can perform the deployment following these steps:

- 1. Log in to the vCenter UI from your vSphere UI console.
- Deploy the OVA template following the steps from the wizard. There is only one consideration to be taken on Step 7 Select networks: Make sure you pick a network that provides access to your VMC on AWS cloud to ensure the Pairing process will be successful.

1 Select an OVF template 2 Select a name and folder	Select networks Select a destination network for each source network.					
3 Select a compute resource	Source Network T Destination Network					
5 License agreements	VM Network		DPortGroup1324		~	
6 Select storage					1 itoms	
7 Select networks					riterns	
8 Customize template 9 Ready to complete	IP Allocation Settings					
	IP allocation:	Stat	tic - Manual			
	IP protocol:	IPv	4		~	

Figure 11 - Deploy OVF Template wizard in vSphere UI

**vm**ware<sup>®</sup>

# Additional SDDC configuration

To be able to successfully pair any on-premises instance to the VMware Cloud Director Availability cloud instance hosted at VMC on AWS, you need to perform some additional steps and prepare your SDDC network settings.

Please follow the procedures in their exact order as they are listed in this document.

#### Add Inventory Services

You need to define 2 Services that will be later used in the Firewall settings. One is for the Cloud Management Portal and the other one is for the Cloud Tunnel endpoint.

Follow these steps to get your services defined:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Inventory  $\rightarrow$  Services.
- 2. To add the Management Portal service, click on ADD SERVICE.
- 3. Give the service a name.

VCDA_C4_MGMT_POR	Set Service Entries	
	Description	Tag (Requirer V Scope (Optio V )
SAVE CANCEL		

Figure 12 - Add an Inventory Service

- 4. Click on Set Service Entries.
- 5. Enter a name for the entry, select the Service Type to be TCP and the Destination Port to be 8046.

Set Service Entries				
Service VCDA_C4_M #Service Entri	es 1			
Type Layer 3 and above ~				
Port-Protocol (1) Services (0)				
ADD SERVICE ENTRY				
Name	Service Type	Additional Properties		
VCDA_C4_MGMT_POR	TCP ~	Source Ports	8046	
				APPLY

Figure 13 - Set the Inventory Service Members

- 6. Click **Apply** and then **Save**.
- 7. To add the Tunnel endpoint service, click on ADD SERVICE.
- 8. Give the service a name.

VCDA_Public_	Endpoint			
Description	Description		Tag (Require: v     Scope (Optio v       Max 30 allowed. Click (*) to save.	
SAVE	CANCEL			

Figure 14 - Add an Inventory Service

9. Click on Set Service Entries.



10. Enter a name for the entry, select the Service Type to be TCP and the Destination Port to be 8048.

Set Service Entries								
Service VCDA_Public (#Service Entries 1)								
Type Layer 3 and above ~								
Port-Protocol (1) Services (0)								
ADD SERVICE ENTRY								
Name	Service Type	Additional Properties						
VCDA_Public_Endpoint	TCP ~	Source Ports	8048					
				CANCEL	APPLY			

Figure 15 - Set the Inventory Service Members

11. Your services are ready.

## **Request Public IPs**

You will need to request 2 new Public IP addresses – one for the Cloud Management Portal and one for the Cloud Tunnel. To request them, please follow the steps below:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  System  $\rightarrow$  Public Ips.
- 2. Click on **REQUEST NEW IP**.
- 3. Put a meaningful note for your Cloud Management Portal IP.
- 4. Click Save.
- 5. Click on **REQUEST NEW IP**.
- 6. Put a meaningful note for your Cloud Tunnel IP.
- 7. Click Save.
- 8. Your 2 new Public IPs are ready.

#### Create a Compute Group

You need to create a Compute Group that will be later used in the Firewall configuration. To create a Compute Group, please follow the steps below:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Inventory  $\rightarrow$  Groups  $\rightarrow$  Compute Groups.
- 2. Click on ADD GROUP.
- 3. Give the Compute Group a meaningful name.

VCDA Appliances		Set Members	
	Description		Tag (Requires         Scope (Optio         Image: Control of the second s
SAVE CANCEL			

Figure 16 - Add a Compute Group

4. Click on Set Members and select the IP Addresses tab.



5. Enter the network details from Requirement #4 in the Prerequisites section.

Select Members   VCDA Appliances								
Add Compute Members either by creating	or by directly adding t	hem.						
Membership Criteria (0) Members (0)	IP Addresses (1)	MAC Addresses (0)						
ACTIONS ~		Mai	kimum: 4000					
172.26.46.1/24 × Enter IP Address								
				CANCEL	APPLY			

Figure 17 - Add Members to a Compute Group

- 6. Click on **Apply** and then **Save**.
- 7. The Compute Group is now ready.

¢ ALL SDOCS								
TPM SDDC								
Summary Networking	& Security Add Ons Maintenance Troubleshooting Sets							
Overview	Groups			٥				
Network	Management Groups Compute Groups							
Segments VPN NAT								
Tier-1 Gateways	Narra	Compute Members	Where Used	Status				
Transit Connect								
Gateway Firewall								
Inventory								
Crouds								
Services Virtual Machines								
Tools								
Port Mirroring								
System DNS DHCP Global Configuration Public IPs Direct Connect								
Connected VPC				1-7 of 7 Groups				

Figure 18 - Compute Groups view

#### Create Management Groups

For enabling your Cloud Replicator to perform its replication jobs with ESXi, you need to create 2 Management Groups that will be later used in the Management Gateway Firewall configuration. To create them, please follow these steps:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Inventory  $\rightarrow$  Groups  $\rightarrow$  Management Groups.
- 2. Click on ADD GROUP.
- 3. Give the first Management Group a meaningful name.



Figure 19 - Add a Management Group

4. Click on Set Members.



5. Enter the private IP that you will set to the Cloud Replicator.

Select Members   VCDA Replicator Priv IP			
ACTIONS -	Maximum: 4000		
172.26.46.202 * Enter IP Address			
Format: 2001.0db8.85a3:0000.0000.8a2z:0370.7334 or 10.12.2.64/26 or 2001:1-5000::25			
		CANCEL	APPLY

Figure 20- Select the members of a Management Group

- 6. Click on **Apply** and then **Save**.
- 7. Click on ADD GROUP.
- 8. Give the second Management Group a meaningful name.

SDDC Compute CGW						
	Description		Tag (Requires V Scope (Optio V )			
SAVE CANCEL						

Figure 21 - Add a Management Group

- 9. Click on Set Members.
- 10. Enter the Public IP that you collected in Requirement #5 in the Prerequisites section.



Figure 22 - Select the members of a Management Group

11. Click on **Apply** and then **Save**.



12. Your Management Groups are created.

CALL SDOCS						OPEN-VCENTER ACTIONS -
TPM SDDC						
Summary Networking	& Security					
	Gro	ups				
Network	Mana	geme	int Gri	Sups Compute Groups		
Segments VPN						
Tier-1 Gateways Transit Connect					Compute Members	
Security						
Distributed Frewall						
inventory	188					
Services	- EE					
Tools IPFIX						
System DNS						
DHCP Global Configuration				VCDA Replicator Priv IP		
Public IPs Direct Connect						
						1-13 of 13 Groups

Figure 23 - Management Groups view

# Configure the Compute Gateway Firewall

You need to do some configurations to the Compute Gateway Firewall in order to allow the inbound traffic to the Cloud Tunnel and also the outbound traffic from your VMware Cloud Director Availability appliances.

These are the necessary steps:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Security  $\rightarrow$  Gateway Firewall  $\rightarrow$  Compute Gateway.
- 2. Click on ADD RULE.
- 3. Give the Appliances Outbound Rule a meaningful name.
- 4. Select the **Compute Group** that you created in section **Create a Compute Group** in the Sources column. Leave everything else with its default value. Make sure the Rule is enabled.
- 5. Click on ADD RULE.
- 6. Give the Cloud Tunnel Inbound Rule a meaningful name.
- 7. Select the Cloud Tunnel Endpoint service that you created in **Add Inventory Services** section. Leave everything else with its default value. Make sure the Rule is enabled.
- 8. Click on Publish.
- 9. The Firewall Rules are ready.

CALL SDOCS										
(6) TPM SDDC   VMC on AVS () US West (Oregon)										
Summary Networking	& Security	Add	Ons Maintenance	Troubleshooting Setti	nas Support					
Dvers/ew Gateway Firewall C										
Network	Managen		Compute Gate	Tier1 Gateways						
Segments VPN										ERT PUBLISH
NAT										
Tier-1 Gateways Transit Connect			Name			Destinations		Applied To		
Security Galaway Erowall			Trusted VCDA Inbound	2064	28 VCDA Trusted A	Any	Any	All Uplinks	Allow ~	C 🕲 🖂
Distributed Firewall	÷		VCDA Tunnel Inbound	2061	Any	Any	VCDA_Public_En	All Uplinks	Allow ~	•
Inventory Groups			VCDA Appliances Outb	2055	22 VCDA Appliances	Any	Any	All Uplinks	Allow ~	C 🕲 🖸
Services Virtual Machines			OSE Inbound SSH	2054	Any	88 OSE	🔿 SSH	Internet Interface	Allow V	) (¢ 🖂
Tools			OSE Inbound HTTPS	2053	Any	SS OSE	O HTTPS	All Uplinks	Allow v	🔍 🕲 🖂
IPFIX Port Mirroring			OSE Outbound	2052	SS OSE	Any	Any	Internet Interface	Allow 🗸 🕴	🔍 🕲 🖉
System DNS			Tenant Inbound Access	2051	Any	22 External Networ	Any	Internet Interface	Allow v	C 🕲 🖸
DHCP Global Configuration			Tenant Outbound Acce	2050	Se External Networ	Any	Any	Internet Interface	Allow v	🔍 🕲 🖂
Public IPs Direct Connect			CSE Outbound access	2038	SS CSE_Server	Any	C KubeAccess	Internet Interface	Allow ~	C 🕸 🗠
Connected VPC										

Figure 24 - Compute Gateway Firewall Rules

# Configure the Management Gateway Firewall

To enable the internal communication between the different VMware Cloud Director Availability components and the ESXi and vCenter, you need to configure 2 Compute Gateway Firewall rules.

To create them, please follow these steps:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Security  $\rightarrow$  Gateway Firewall  $\rightarrow$  Management Gateway.
- 2. Click on ADD RULE.
- 3. Give the ESXi Provisioning Rule a meaningful name.
- 4. Select as follows:
  - a. Sources the Cloud Replicator Private IP Management Group that you defined in the Create Management Groups section.
  - b. Destinations **ESXi**.
  - c. Services Provisioning and Remote Console (TCP 902).
- 5. Click on ADD RULE.
- 6. Give the Appliances Inbound rule a meaningful name.
- 7. Select as follows:
  - a. Sources the Management Group that has the Public IP as a member that you defined in the **Create** Management Groups section.
  - b. Destinations vCenter.
  - c. Services HTTPS.
- 8. Click on Publish.
- 9. The Firewall Rules are defined.

<all actions="" open="" sddcs="" th="" vcenter="" ~<=""></all>										
TPM SDDC	(m) TPM SDDC   VMC on AWS   US West (Oregon)									
Summary Networking	& Security	Add C	Ons Maintenance Tro	ubleshooting Settings	Support					
Overview	iew Gateway Firewall (2)									
Network	Manage	ment Ga	teway Compute Gatewa	y Tier1 Gateways						l
Segments VPN										PUBLISH
NAT Tier-1 Gateways										
Transit Connect			Name			Destinations	Services			
Security Gateway Firewall	1	0	VCDA Appliances Inbound	2062	SDDC Compute CGW	Be vCenter	O HTTPS	• Allow ~	•	@ @
Distributed Firewall			ESXI Provisioning	2063	22 VCDA Replicator Priv IP	88 ESXI	Provisioning & Remot	Allow 🗸	<b>_</b>	
Inventory Groups Services			CDS Persistent Firewall Rule	2026	器 CDS Outbound IPs	55 vCenter	C HTTPS	Allow -		
Virtual Machines			CDS Console Access Rule	2027	Any	BC ESXI	HTTPS     Provisioning & Remot	• Allow ~	-	
IPFIX Port Mirroring			Access to VC	2025	Any	88 vCenter	C HTTPS SSO	• Allow ~		
System							CMP ALL			
DHCP			HCX UI	2024	Any	BS HCX	O HTTPS	Allow 🗸	-	
Global Configuration Public IPs			ESXi Outbound Rule	1013	SS ESXI	Any	Any	Allow ~	0	
Direct Connect Connected VPC		RESH							-	

Figure 25 - Management Gateway Firewall Rules

# Add NAT rules

NAT rules are necessary to forward the incoming traffic to the correct appliances. You need to add 2 NAT rules – one for the Cloud Management Portal and one for the incoming Cloud Tunnel traffic.

The Cloud Management Portal rule can be removed after the initial configuration is done as the Portal is accessible through the VMware Cloud Director Availability Plug-in in Cloud Director service.

The steps to add NAT rules are:

- 1. Navigate to your SDDC Network & Security  $\rightarrow$  Network  $\rightarrow$  NAT.
- 2. Click on ADD NAT RULE.
- 3. Give the Cloud Management Portal Rule a meaningful name.
- 4. The rule settings should be as follows:
  - a. Public IP the Public IP that you requested for the Cloud Management Portal in the Request Public IPs section.
  - b. Service the Cloud Management Service that you defined in the Add Inventory Services section.
  - c. Public Port 8046.
  - d. Internal IP the Cloud Management Replicator Appliance internal IP address.
  - e. Internal Port **8046**.



- f. Firewall Match Internal Address.
- g. Click Save.
- 5. Click on ADD NAT RULE.
- 6. Give the Cloud Tunnel Inbound Rule a meaningful name.
- 7. The rule settings should be as follows:
  - a. Public IP the Public IP that you requested for the Cloud Tunnel in the **Request Public IPs** section.
  - b. Service the Cloud Tunnel Service that you defined in the Add Inventory Services section.
  - c. Public Port 443.
  - d. Internal IP the Cloud Management Replicator Appliance internal IP address.
  - e. Internal Port 8048.
  - f. Firewall Match Internal Address.
  - g. Click Save.
- 8. The NAT rules are created.

< ALL SDDCs										
TPM SDDC	TPM SDDC   VMC on AWS © US West (Dirigion)									
Summary Networking	summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support									
Overview	NAT ()									
Network	Internet Con	npute Gateway								
VPN NAT									Q Search	
Tier-1 Gateways		Name	Public IP	Service	Public Port	Internal IP	Internal Port	Firewall ()	Status	
Security		CDS HTTPS Routing Rule - 10.2.32.4								iccess 🕐
Gateway Firewall Distributed Firewall		CDS Console Routing Rule - 10.2.32.4		Provisioning & Remote Console						iccess 🕐
Inventory Groups										uccess C
Services										lccess C
Virtual Machines										access C
IPFIX Port Mirroring										iccess 🖱
System		VCDA C4 MGMT Port		VCDA_C4_MGMT_PORT	8046	172.26.46.201	8046	Match Internal Address	SL	iccess C
DNS		VCDA Tunnel Endpoint		VCDA_Public_Endpoint			8048			iccess 🖱
Global Configuration Public IPs Direct Connect										
Connected VPC										1 - 8 of 8 Rules

Figure 26 - NAT Rules

# Initial setup

Even though the initial setup and configuration process is almost the same as the one in VMware Cloud Director Availability 4.1, there are some details that need to be explained further.

#### Provider setup

- 1. Make sure your external IP address is in the Trusted IP list that was defined in Requirement #7 in the Prerequisites section.
- 2. Navigate to https://<Cloud\_Management\_Portal\_Public\_IP>:8046/admin.
- 3. Log in as **root** and change the password when prompted.
- 4. Click on Run the initial setup wizard.
- 5. Provide the VMware Cloud Director Availability license.
- 6. Give the site a meaningful name and check only the VMC data engine to be activated.

Initial Setup	Site Details	×					
1 Licensing	Enter a site name that uniquely identifies this site from its peers.						
2 Site Details	Site name: 🌒 *	CDA42B-VMC					
3 VMware Cloud Director	Service Endpoint address: (	e.g. https://vcav.cloudprovider.com:443					
4 Replicator Service instances	Description:	Enter some meaningful information about the site.					
5 Tunnel Service							
6 Ready To Complete	Choose which data engines to	be activated.					
	Classic - Migrations an Any VMware Cloud Director Av by using the native integrations VMC - Migrations to V A new VMware Cloud Director A	d Protections between VMware Cloud Director Cloud Sites ilability version can migrate vSphere workloads to a cloud site backed by VMware Cloud Director with VMware Cloud Director and VMware vCenter Server. Mware Cloud on AWS vealability service that can perform the migrations to the VMware Cloud on AWS environment.					
		CANCEL BACK NEXT					

- 7. Provide the Cloud Director service public URL in the following format https://CDs\_URL/api.
- 8. Enter a System Administrator or CDS Provider Admin user and its password. For example, vcdaadmin@sytem. Any other user types except Local users are currently not supported.

#### Initial Setup VMware Cloud Director

1 Licensing	Enter the address and credentials of the VMv	vare Cloud Director instance.			
2 Site Details	VMware Cloud Director endpoint URL: *	Accessive and a second			/api
3 VMware Cloud Director	VMware Cloud Director user name: 🚯 *	vcdatestadmin@system			
4 Replicator Service instances	VMware Cloud Director password *				0
5 Tunnel Service					
6 Ready To Complete					
			CANCEL	BACK	NEXT

Figure 27 - Provider Setup: Cloud Director service settings

- 9. Provide the VMC Lookup Service URL which is the vCenter public URL. Use this format *https://vCenter\_URL:443/ lookupservice/sdk.*
- 10. Enter the internal IP address of the Replicator (for example, *https://172.26.46.202:8043*) and its root password. You might be prompted to change the root password, if you haven't done so yet.



11. Enter *cloudadmin@vmc.local* as SSO user name and provide its password.

Initial Setup	Replicator Service instar	nces		×
1 Licensing	Enter the address of the Lookup Serv SSO credentials.	ice and one or more addresses of the Replic	ator Service instances and	their
2 Site Details	Lookup Service Address: *	4	\$3/lookupservice/sdk	
3 VMware Cloud Director	<ul> <li>Replicator 1 ( https://172.26.46.2</li> </ul>	02:8043 )		LETE
4 Replicator Service instances	Replicator Service address: *	https://172.26.46.202:8043		
5 Tunnel Service	Replicator Service root password *			٩
6 Ready To Complete	A The appliance root pass	word has expired. You must change it befor	e you can start using the	
	service.			
	New Password 🚺 📍			0
	Confirm Password *			0
	SSO user name: 🌗 📍	cloudadmin@vmc.local		
	SSO password *			0
	Description:			
			CANCEL BACK	NEXT

Figure 28 - Provider setup: Replicator settings

12. Enter the Cloud Tunnel Appliance internal IP address and its root password. You might be prompted to change the root password, if you haven't done so yet.

Initial Setup	Tunnel Service	×
1 Licensing 2 Site Details 3 VMware Cloud Director 4 Replicator Service instances	Tunnel Service address: • Root password •	https://72.26.46.203.8047
5 Tunnel Service	A The appliance root pa	ssword has expired. You must change it before you can start using the service.
6 Ready To Complete	New Password 🚯 *	
	Confirm Password *	CANCEL BACK NEXT

Figure 29 - Provider setup: Tunnel settings

#### 13. Finalize the wizard.

#### Additional Configuration

- 1. Assign Replication Policy to your tenants that would allow them to perform migrations.
- Change the Service Endpoint to be the https://<Cloud\_Tunnel\_Public\_IP>:443 from Settings → Service Endpoints → Service Endpoint Address.
- 3. Switch the Data Engine to be VMC instead of Classic from Settings  $\rightarrow$  Site Settings  $\rightarrow$  Data Engine.

Si	e settings		
	Local Site	CDA42B-VMC 🗓	Edit
	Data engine	VMC	Edit
	Bandwidth throttling (1)	ens160 (nic): Unlimited	Edit
	Accessible Provider VDCs	All Provider VDCs	Edit

Figure 30 - Change the Data Engine to VMC

Note: When you perform this switch the Outgoing Replications menu will disappear.



#### Tennant setup

- 1. Make sure the external IP address of the Data Center where the On-premises appliance is deployed is in the Trusted IP list that was defined in Requirement #7 in the Prerequisites section.
- 2. Navigate to https://<On\_Premises\_Appliance\_IP/admin.
- 3. Log in as **root** and change the password when prompted.
- 4. Click on Run the initial setup wizard.
- 5. Provide the local vCenter Lookup Service address and credentials.
- 6. Give the site a meaningful name.
- 7. Enter the Service Endpoint address (*https://<Cloud\_Tunnel\_Public\_IP>:443*) that you define in the **Additional Configuration** part of the **Provider Setup** section.
- 8. Enter the credentials for a user with Organization Admin role.

h	nitial Setup	Cloud Service D	etails	$\times$
1	1 Lookup Service	Enter VMware Cloud Direct	or Availability Cloud Site details.	
	2 Site Details	Service Endpoint address: *	:443	
	3 Cloud Service Details	Organization Admin: *	orgadmin@nikolayorg	
	4 Ready To Complete	Organization Password	0	٩
		Allow Access from 0	Cloud	
		Privileged VMware C for replication.	loud Director users are allowed to remotely browse the VMs on this site and configure them	
			CANCEL BACK NE	хт

Figure 31 - Tenant setup: Service Endpoint settings

- 9. Configure the Local placement.
- 10. You are ready to perform your first migration from On-Premises to Cloud Director service.

# Pairing with another Cloud

To enable migrations from private clouds running VMware Cloud Director, you need to upgrade and pair the existing instance of VMware Cloud Director Availability operating in this private cloud.

Once its version is 4.2, you will need to change the Data Engine similarly to what you did in the VMware Cloud Director Availability provider instance running in Cloud Director service (step 3 from the **Additional Configuration** in the **Provider setup** section).

To continue supporting the existing replications, it should have both options selected - Classic and VMC.



Figure 32 - VMware Cloud Director Availability Data Engine settings in private cloud

In cases where you perform a fresh installation of VMware Cloud Director Availability 4.2, you can select both data engines to be enabled during the Initial Config Wizard.

Initial Setup	Site Details		$\times$
1 Licensing	Enter a site name that uniquely ide	entifies this site from its peers.	
2 Site Details	Site name: <b>() *</b>	CDA42-LAB	
3 VMware Cloud Director	Service Endpoint address: 🌗	e.g. https://vcav.cloudprovider.com:443	
4 Replicator Service instances	Description:	Enter some meaningful information about the site.	
5 Tunnel Service			
6 Ready To Complete	Choose which data engines to	be activated.	
	Classic - Migrations an Any VMware Cloud Director Ava by using the native integrations of VMC - Migrations to VI A new VMware Cloud Director A	d Protections between VMware Cloud Director Cloud Sites ilability version can migrate vSphere workloads to a cloud site backed by VMware Cloud Director with VMware Cloud Director and VMware vCenter Server. dware Cloud on AWS vailability service that can perform the migrations to the VMware Cloud on AWS environment.	
		CANCEL BACK NEXT	r

Figure 33 - VMware Cloud Director Availability Data Engine settings in private cloud in the Initial Config Wizard

# Migration

The migrations to Cloud Director service follow the same configuration flow as the migrations to VMware Cloud Director. To create a new one, please follow the steps below:

- 1. Open the VMware Cloud Director Availability UI from the place of your preference (vCenter Plug-In, Cloud Director service Plug-In or On-Premises appliance UI).
- 2. Go to VMC migration under Replications.
- 3. Click on New migration.



Figure 34 - New migration

#### 4. Select the VM(s) to be migrated.

New Incoming Migration	vCenter VMs			×
1 vCenter VMs	Source site VCDA428-ONPREM v	Select VMs to replicate fro	CDA-NVCSA120	VMWCVL.ORG Y
2 Destination VDC and Storage policy	Group VMs to a single vApp	T CPU	Memory	Disk capacity
3 Ready to complete	G InterconnectI-hcx120-0X-II	8	3.00 GB	2.00 GB
	B Interconnect1-hcx120-NE-II	8	3.00 GB	2.00 GB
	Binterconnect1-hcx120-WO-I1	8	14.00 GB	100.00 GB
	C & Ubuntu-251	2	4.00 GB	60.00 GB
	🗌 🐉 demot	4	4.00 GB	10.00 GB
	C 🚱 demo2	4	4.00 GB	10.00 GB
	□ 🚱 demo3	4	4.00 GB	10.00 GB
	□ 🐉 hcx-193	4	12.00 GB	60.00 GB
	G vcda41-onprem-196	4	4.00 GB	10.00 GB
	Rundat2.contem.209	4	4.00 GR	10.00.GR
	CLEAR SELECTED	te	ms per page 20 V	1 - 10 of 10 results
			CAN	CEL NEXT

Figure 35 - Select VMs for migration

5. Select the **Destination VDC** and **Storage Policy**.

New Incoming Migration	Des	tination VDC	and Stora	ige policy						×
1 vCenter VMs	Select	a virtual data center f	rom CDA42B-VMC	to be used as replicat	ion target:		Target organization	NIKOLAYOR	G ~ REFRESH	כ
2 Destination VDC and Storage policy		Name T	Used CPU	Used memory	Used storage	VMs	Guota	Ong	poing replications	
2 Destination VDC and Storage poincy	0	NikolayOrgV	O M	0.00 B	0.00 B	0	Currently unavailab	le O		
3 Ready to complete										
							tems	per page 20	<ul> <li>1-1 of 1 result</li> </ul>	15
	Storag									
	Select	t the new storage n	olicy placement	for the recovered V	Me 🙆					
		Name		Ψ	Encryption capability		Used	T Limit		r
		VM Encryption Pol	icy		Yes		0.00 B	Unlimit	ed	
	0	VMC Workload Sto	rage Policy - Clus	ter-1	No		0.00 B	Unlimit	ed	
		vSAN Default Store	age Policy		No		0.00 B	Unlimit	ed	
		Any			No		0.00 B	Unlimit	ed	
							items p	er page 20	U 1-4 of 4 result	15
								_		_
							c	ANCEL	BACK	r

Figure 36 - Select Destination VDC and Storage Policy

6. Finalize the migration.

New Incoming Migration	Ready to complete	×
1 vCenter VMs	The migration workflow will execute the following steps:         Sync (if the source VM is ON)	
2 Destination VDC and Storage policy	<ul> <li>Power off source VM (if needed)</li> <li>Sync (after source VM is off)</li> <li>Import the VM in the target site</li> </ul>	
3 Ready to complete	Verify the selected settings before clicking Finish:	
	VMs	👌 Ubuntu-251
	Source site	VCDA42b-OnPrem
	Destination Site	CDA42B-VMC
	Destination VDC	NikolayOrgVDC
	Storage policy	VMC Workload Storage Policy - Cluster-1
	Target RPO	
		CANCEL BACK FINISH

Figure 37 - Migration summary

7. The migration is configured.

# **vm**ware<sup>®</sup>

# Table of Figures

3
З
4
4
4
5
5
6
6
7
7
8
8
8
9
9
10
10
10
11
11
11
12
12
13
14
15
16
16
16
17
18
18
19
19
19
. 20





VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-wp-tech-temp-a4-word-101-proof 6/20