Migrations to VMware Cloud Director service

Using VMware Cloud Director Availability

vmware®

Table of contents

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**.

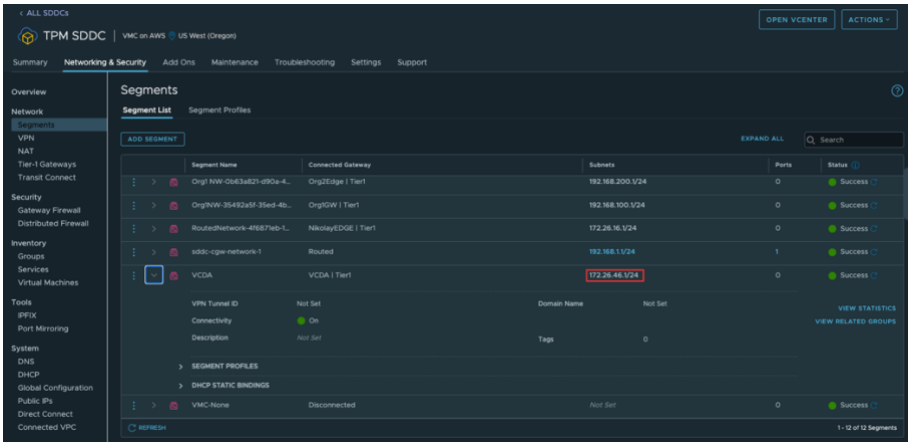


Figure 1 - SDDC Network Segments

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

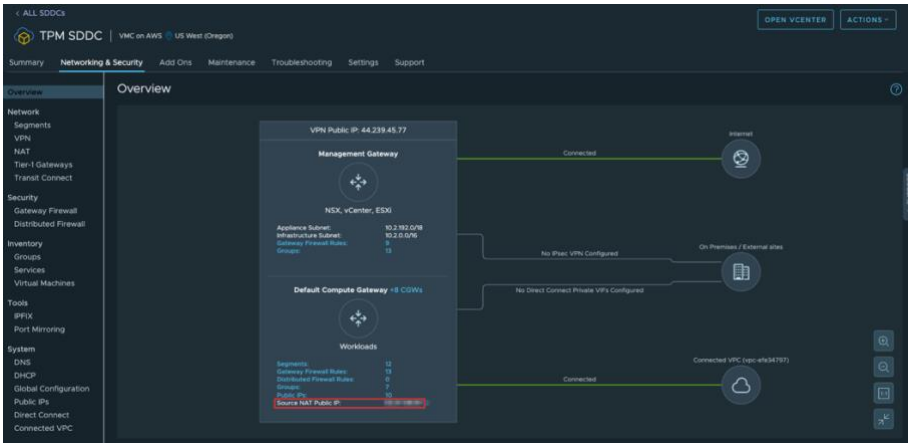


Figure 2 - SDDC Network Overview

7. Obtain the proper **DNS Service IP** of your SDDC from **Networking & Security** → **System** → **DNS.**

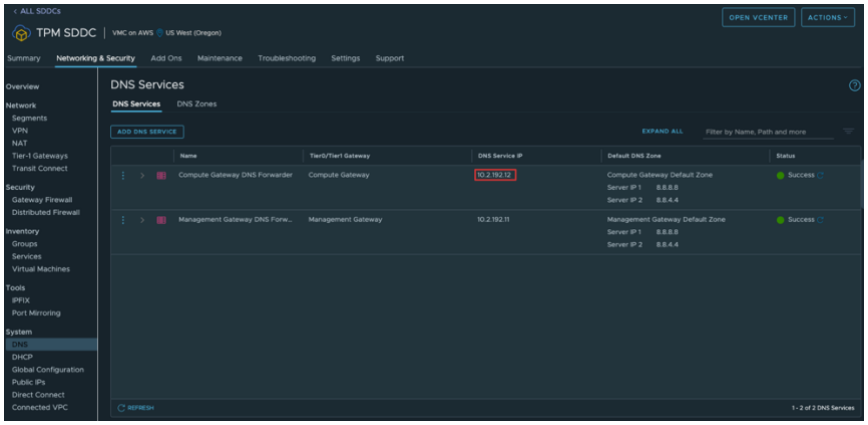


Figure 3 - SDDC DNS Services

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.

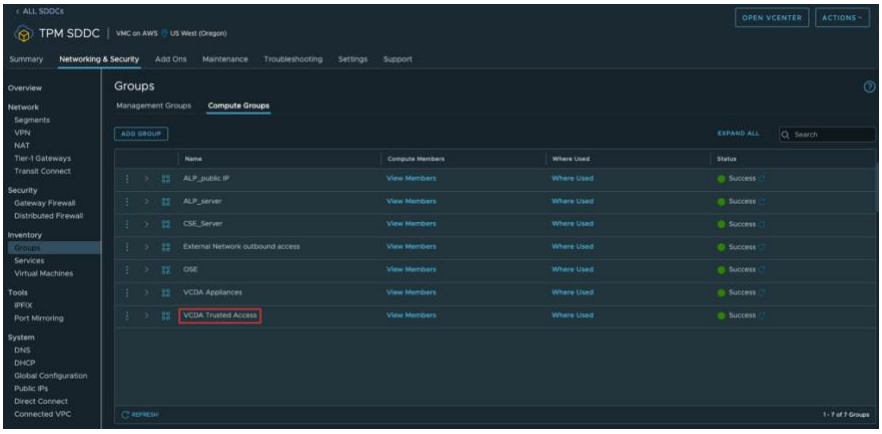


Figure 4 - Compute Groups

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

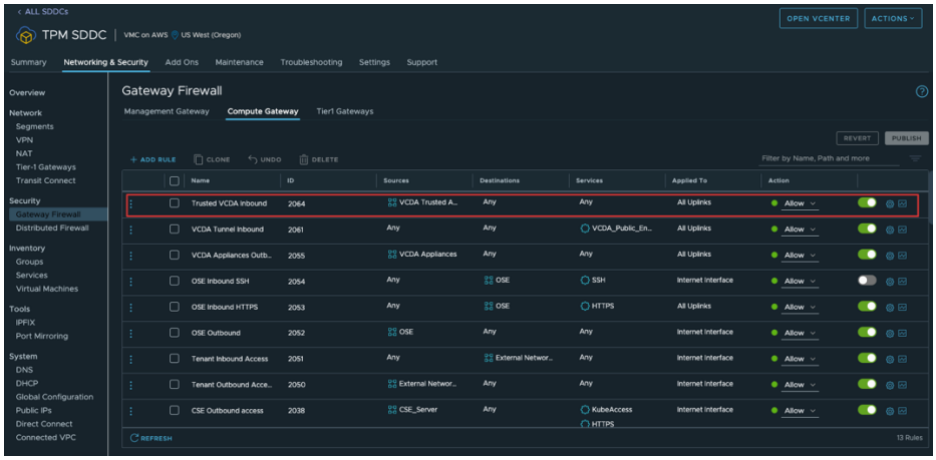


Figure 5 - Compute Gateway Firewall Rules

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

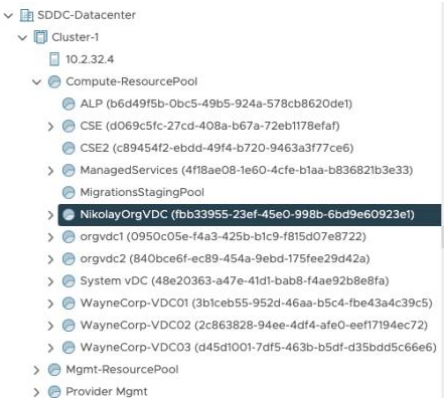


Figure 6 - Dedicated Resource Pool

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**

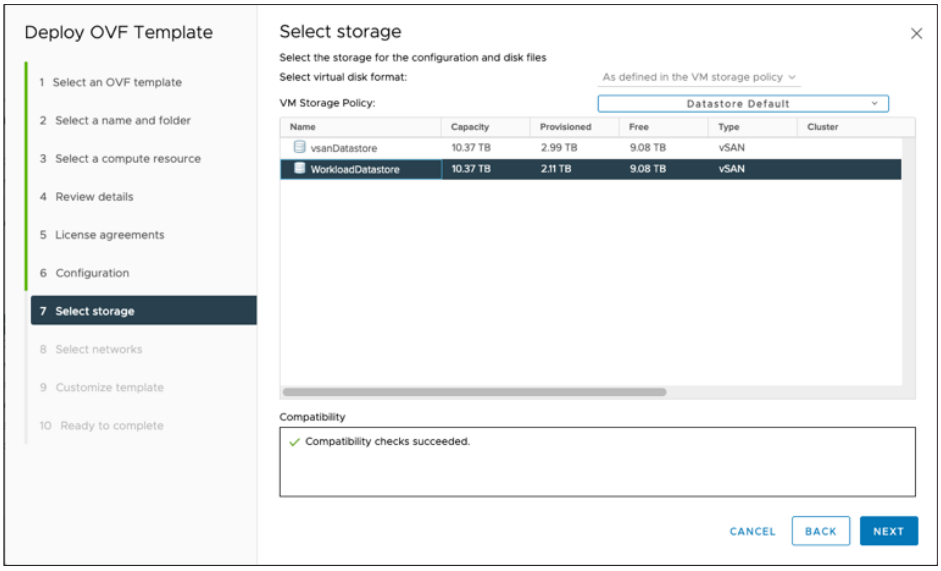


Figure 7 - Datastore selection

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

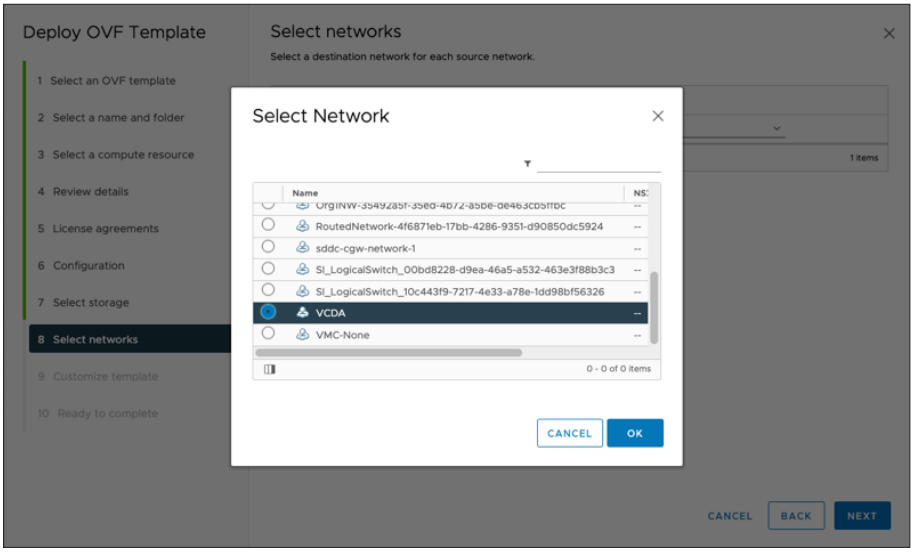


Figure 8 - Network selection

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.

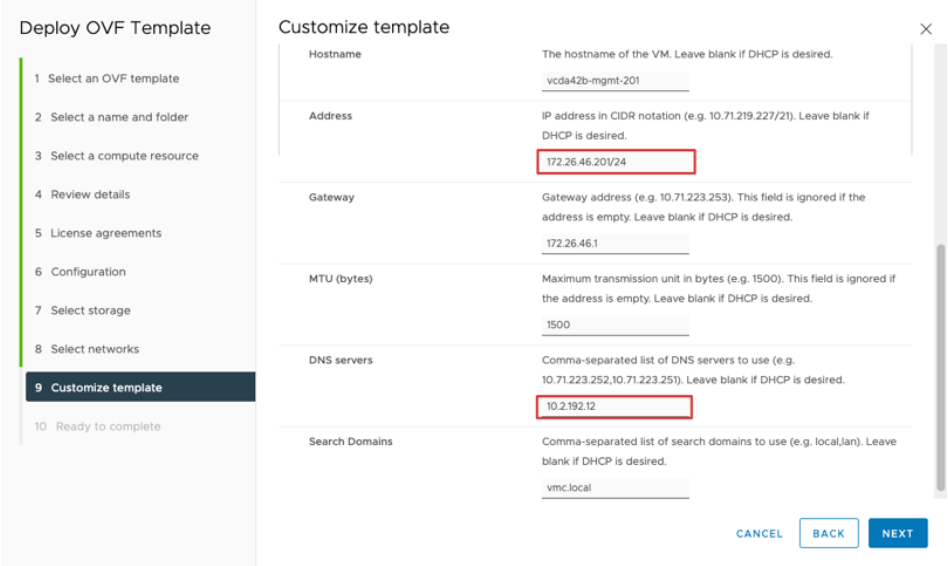


Figure 9 – VMware Cloud Director Availability Network settings

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

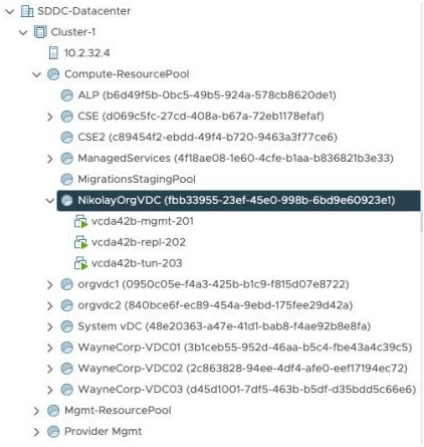


Figure 10 - Deployed appliances view in vCenter

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.
2. 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.

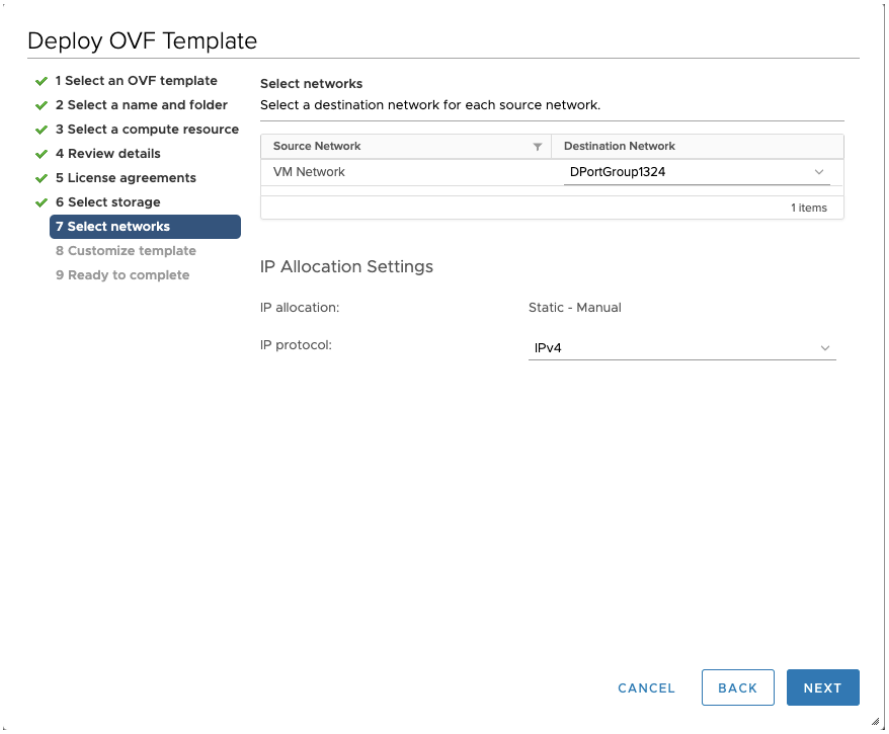


Figure 11 - Deploy OVF Template wizard in vSphere UI

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 → Inventory → Services.**
2. To add the Management Portal service, click on **ADD SERVICE.**
3. Give the service a name.

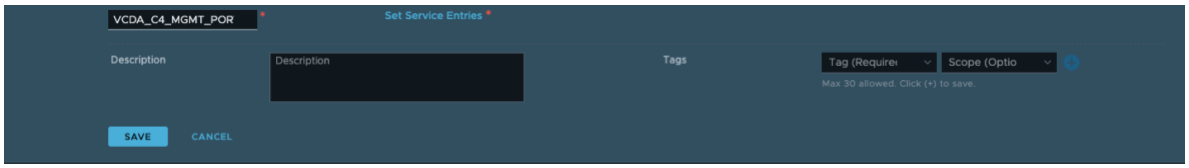


Figure 12 - Add an Inventory Service

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**.

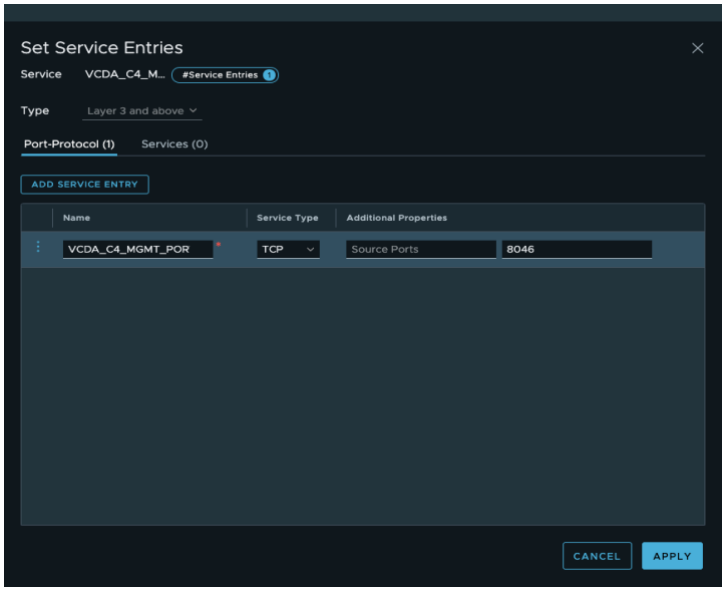


Figure 13 - Set the Inventory Service Members

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

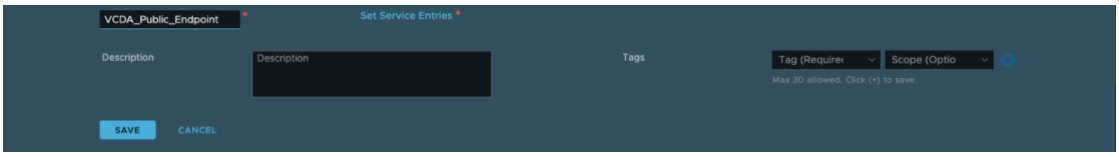


Figure 14 - Add an Inventory Service

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**.

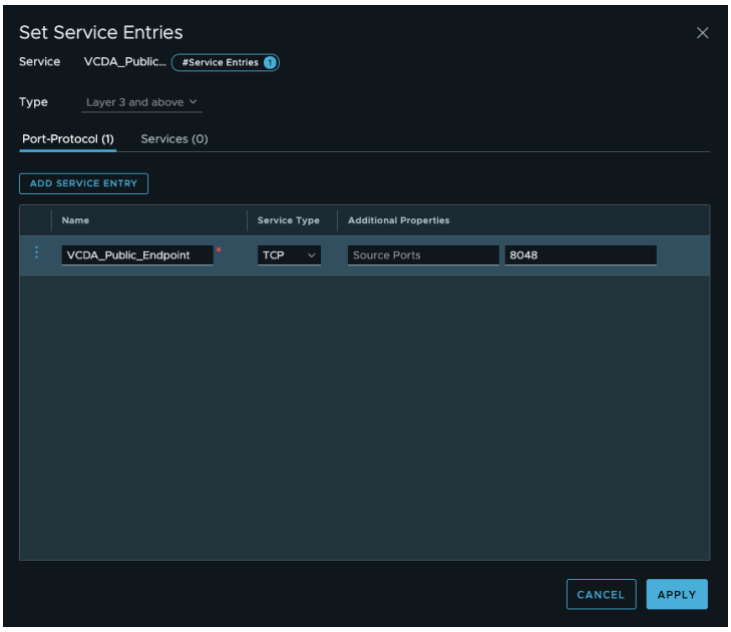


Figure 15 - Set the Inventory Service Members

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** → **System** → **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** → **Inventory** → **Groups** → **Compute Groups**.
2. Click on **ADD GROUP**.
3. Give the Compute Group a meaningful name.

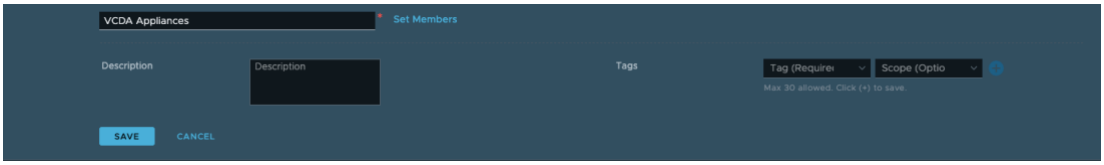


Figure 16 - Add a Compute Group

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

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

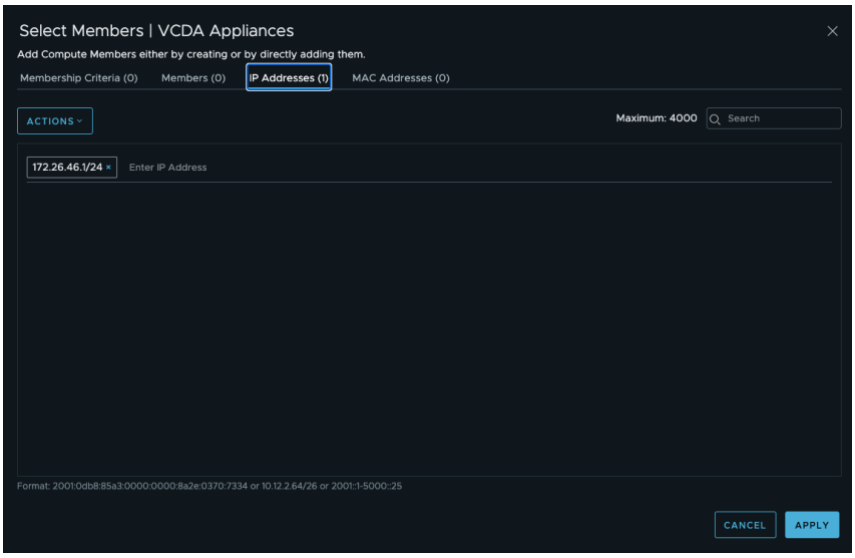


Figure 17 - Add Members to a Compute Group

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

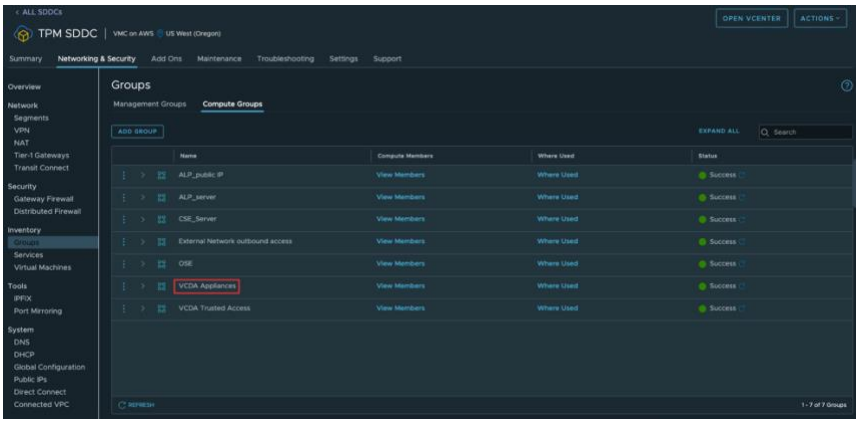


Figure 18 - Compute Groups view

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** → **Inventory** → **Groups** → **Management Groups**.
2. Click on **ADD GROUP**.
3. Give the first Management Group a meaningful name.

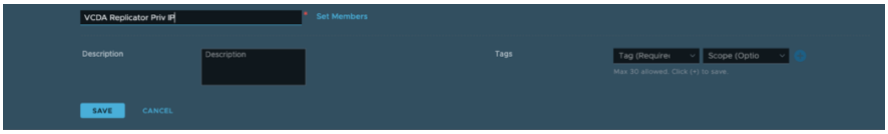


Figure 19 - Add a Management Group

4. Click on **Set Members**.

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

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.

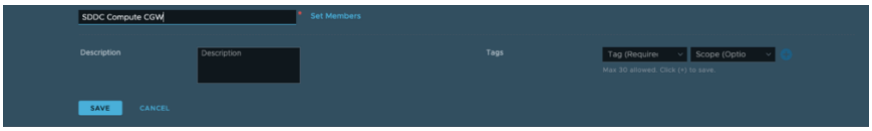


Figure 21 - Add a Management Group

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

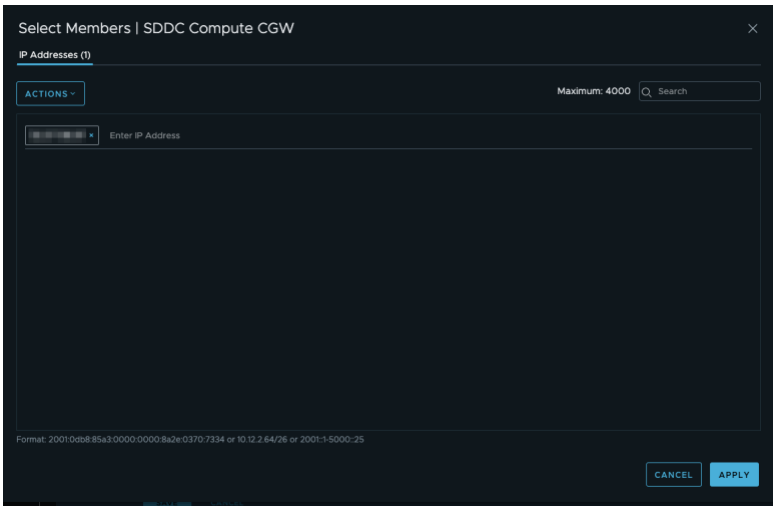


Figure 22 - Select the members of a Management Group

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

12. Your Management Groups are created.

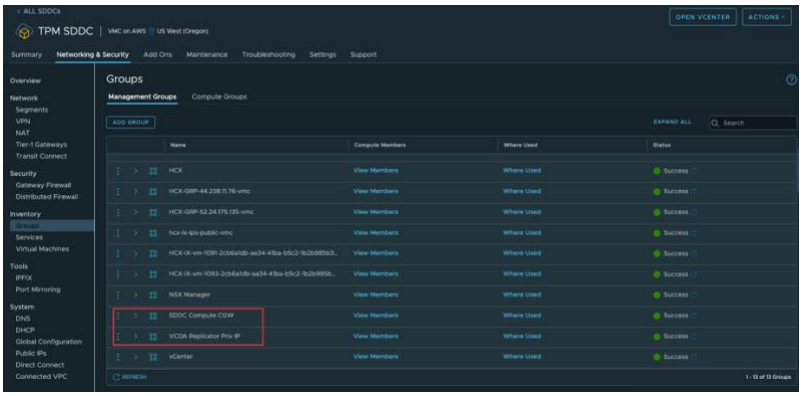


Figure 23 - Management Groups view

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** → **Security** → **Gateway Firewall** → **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.

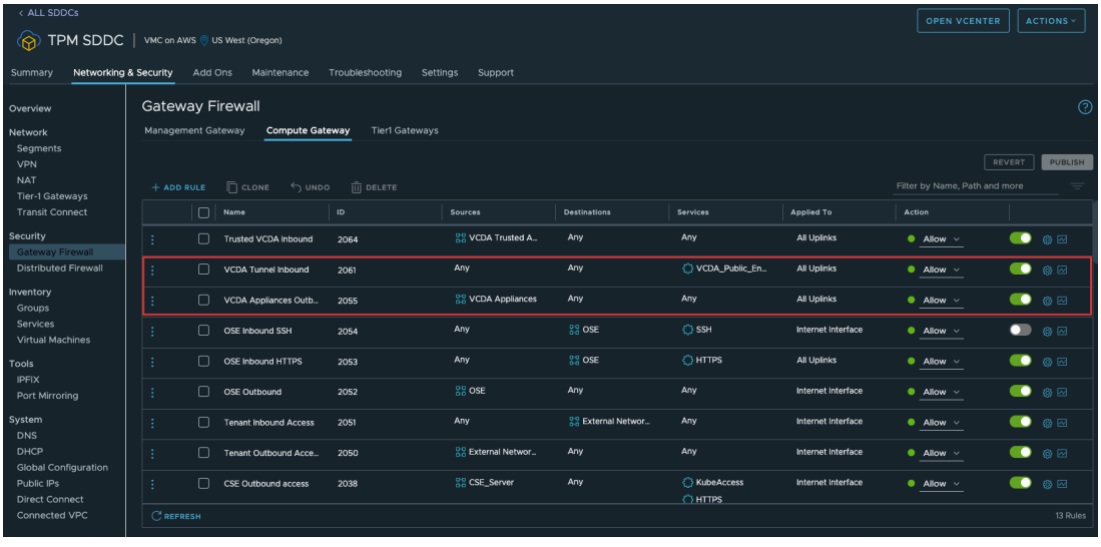


Figure 24 - Compute Gateway Firewall Rules

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** → **Security** → **Gateway Firewall** → **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.

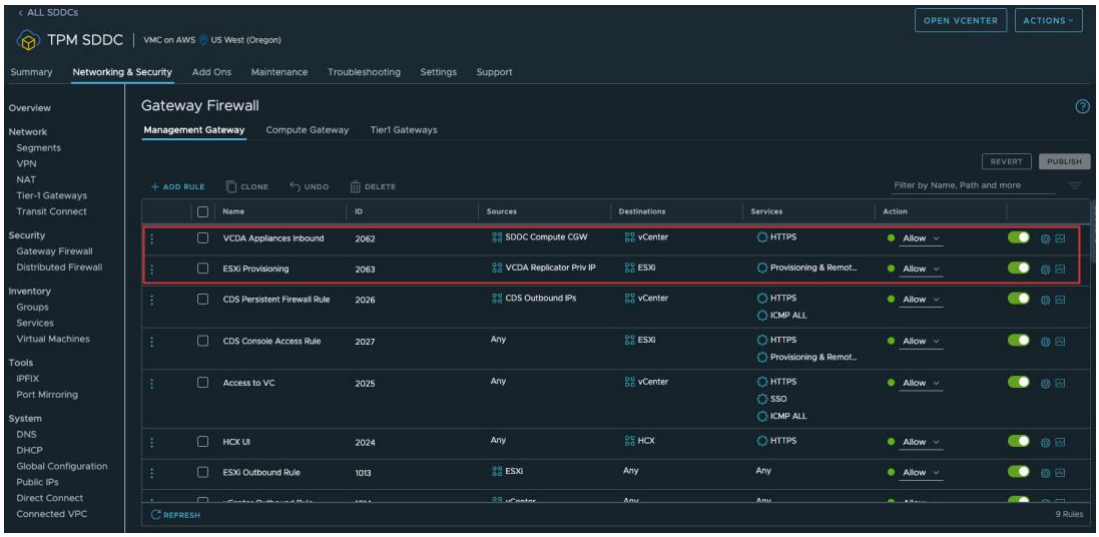


Figure 25 - Management Gateway Firewall Rules

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** → **Network** → **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.

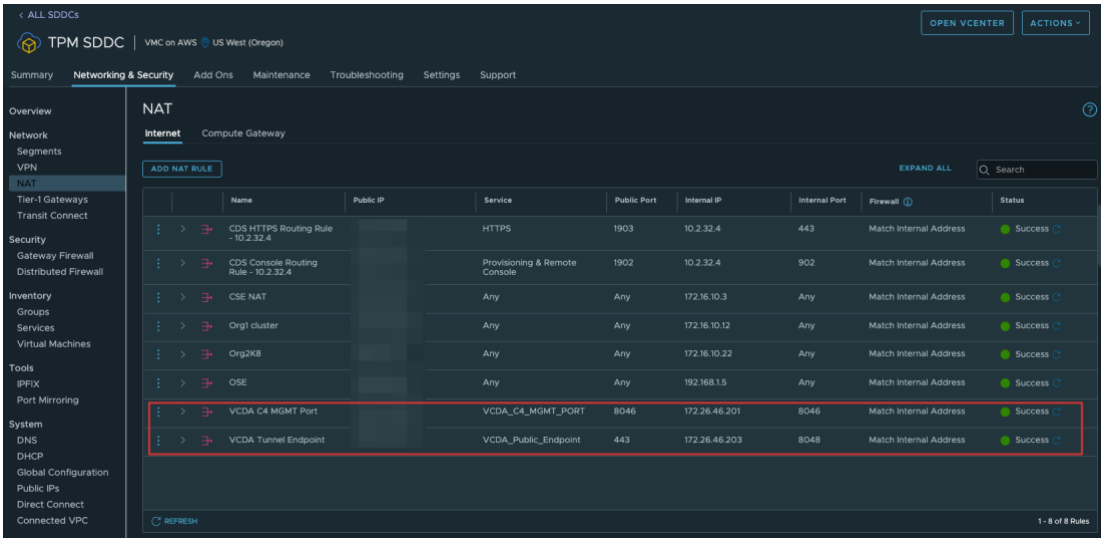


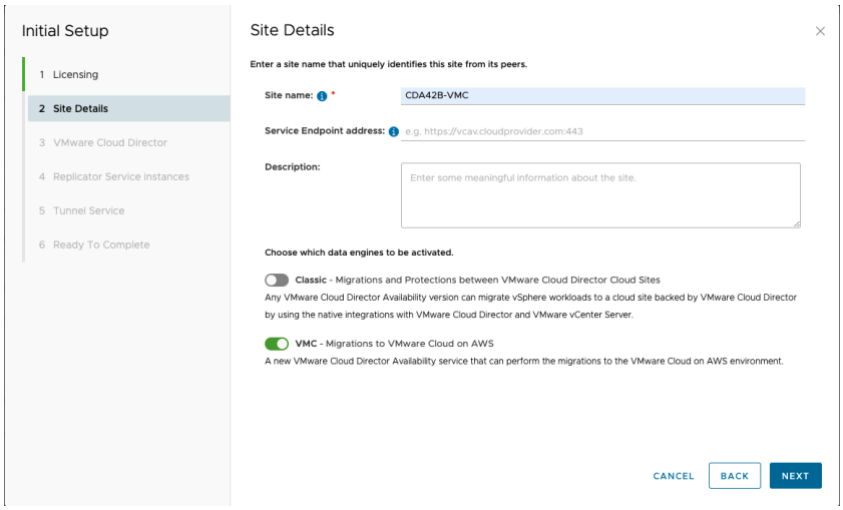
Figure 26 - NAT Rules

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.



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.

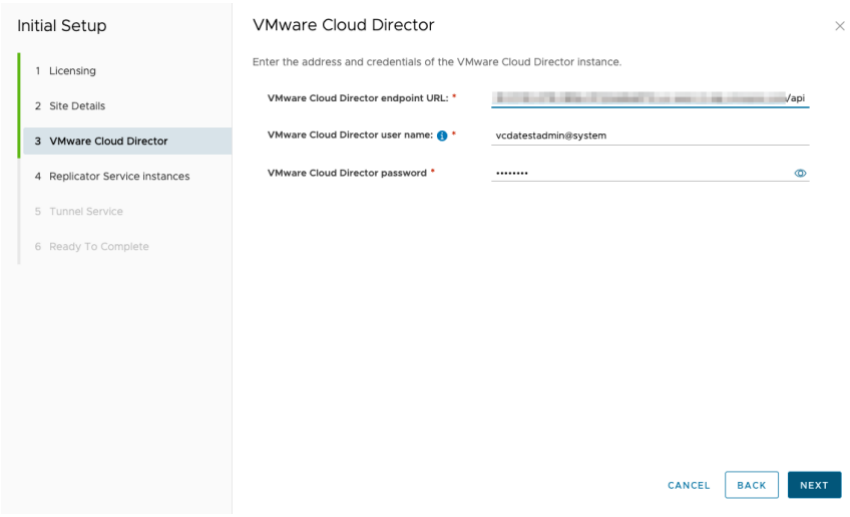


Figure 27 - Provider Setup: Cloud Director service settings

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.

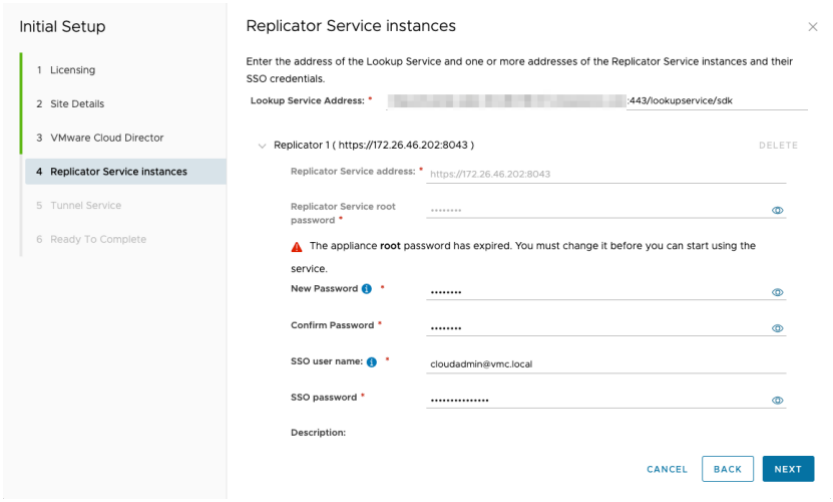


Figure 28 - Provider setup: Replicator settings

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.

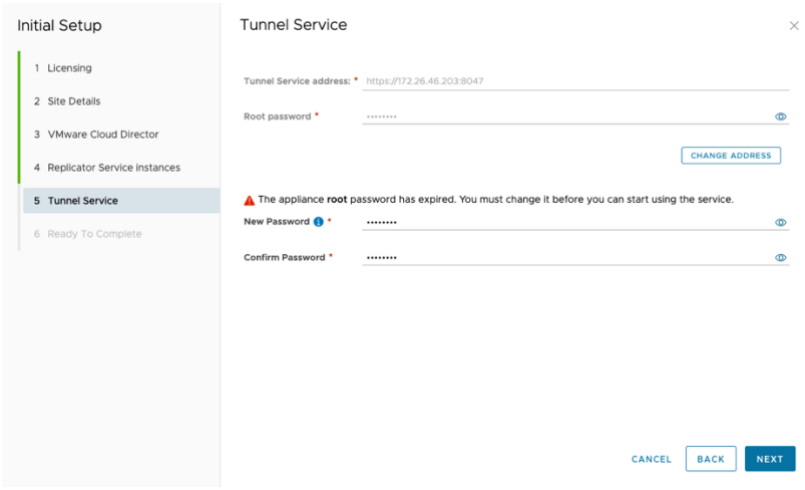


Figure 29 - Provider setup: Tunnel settings

13. Finalize the wizard.

Additional Configuration

1. Assign Replication Policy to your tenants that would allow them to perform migrations.
2. 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** → **Site Settings** → **Data Engine**.

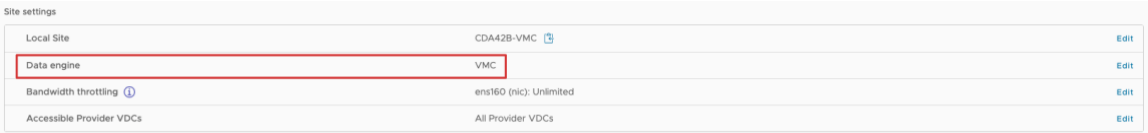


Figure 30 - Change the Data Engine to VMC

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.

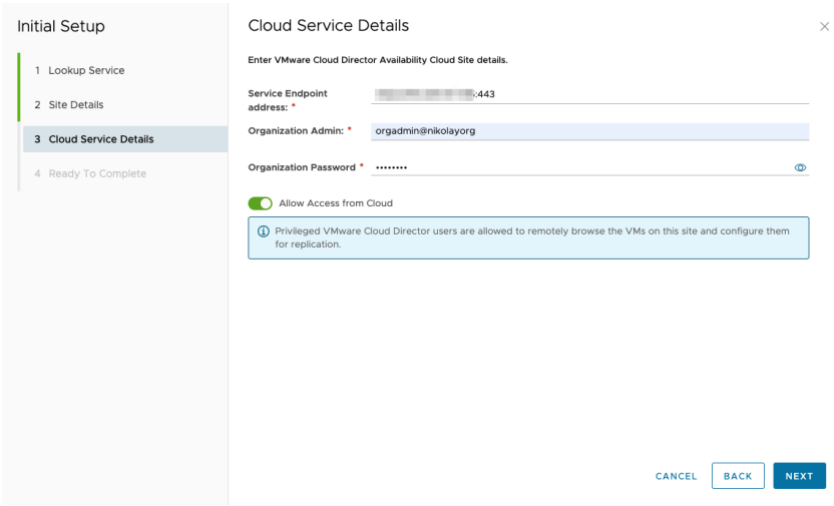


Figure 31 - Tenant setup: Service Endpoint settings

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.

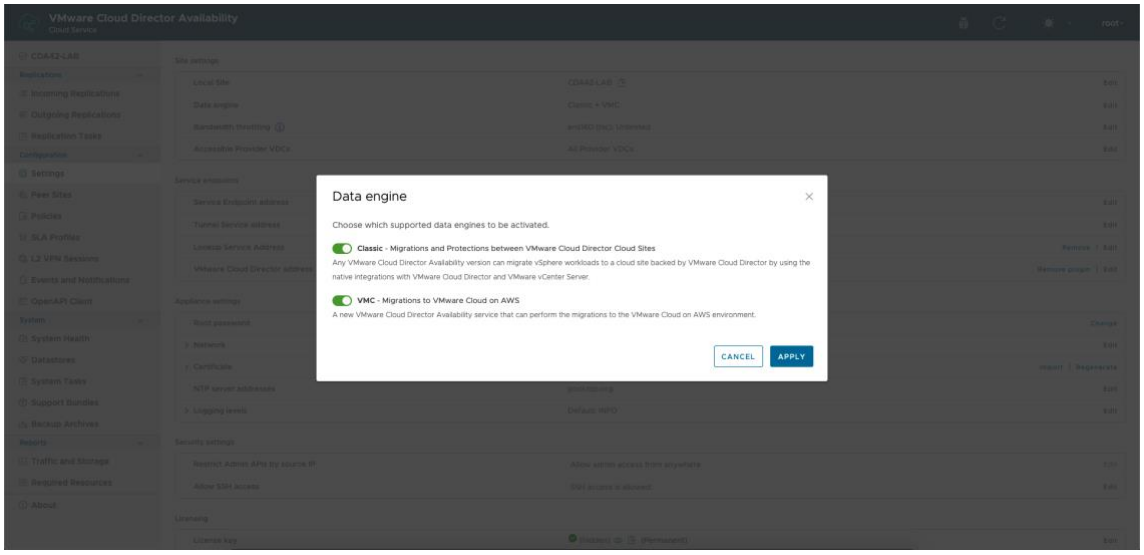


Figure 32 - VMware Cloud Director Availability Data Engine settings in private cloud

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.

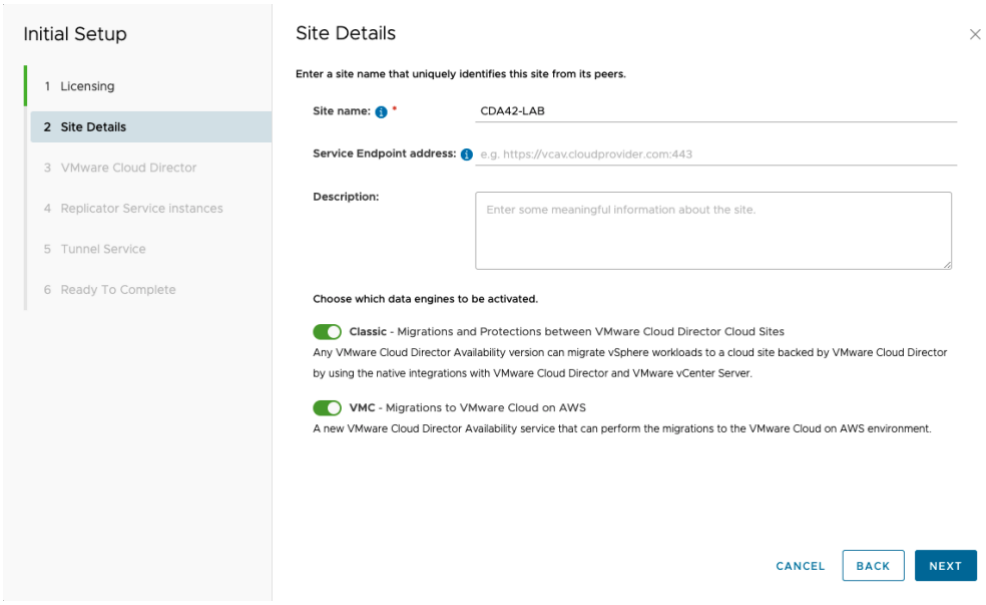


Figure 33 - VMware Cloud Director Availability Data Engine settings in private cloud in the Initial Config Wizard

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**.

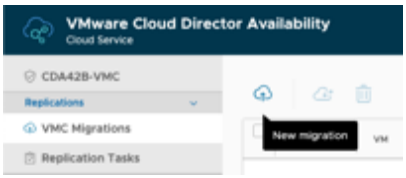


Figure 34 - New migration

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

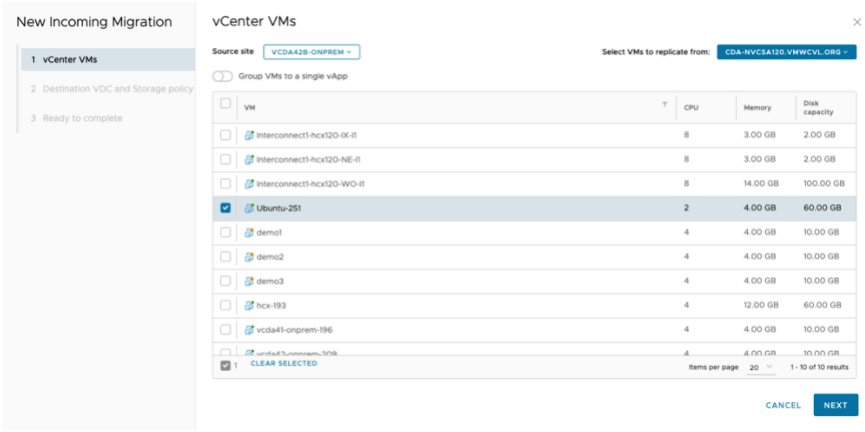


Figure 35 - Select VMs for migration

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

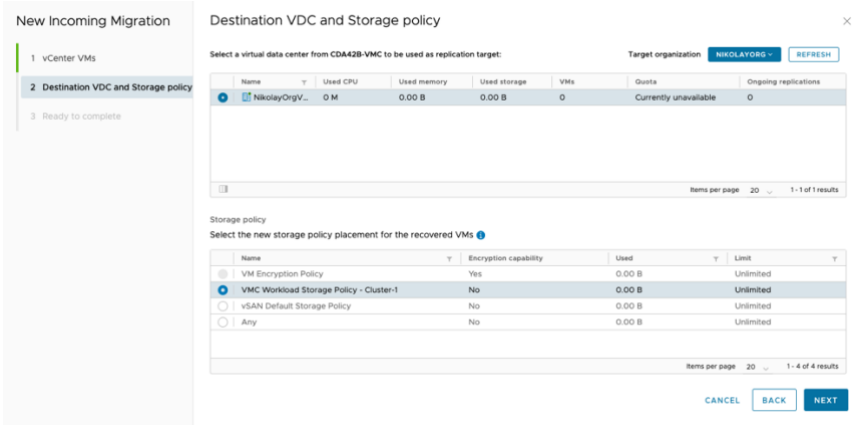


Figure 36 - Select Destination VDC and Storage Policy

6. Finalize the migration.

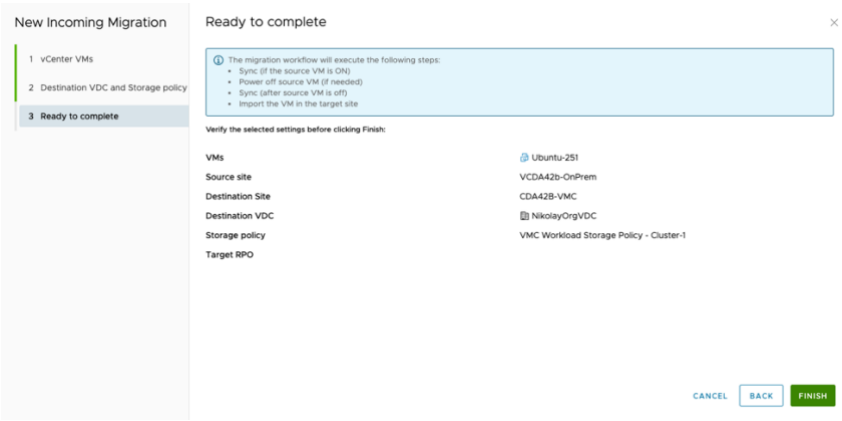


Figure 37 - Migration summary

7. The migration is configured.

Table of Figures

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com