Stretched VRF Use Case

About the Stretched VRF Use Case

Stretched VRF (intra-VRF) is a common use case where a single (common) VRF is defined in a template that is associated to all the sites (on-premises and cloud sites). A separate template is used to deploy networks for the on-premises site since it is not possible to stretch networks between on-premises and cloud sites.

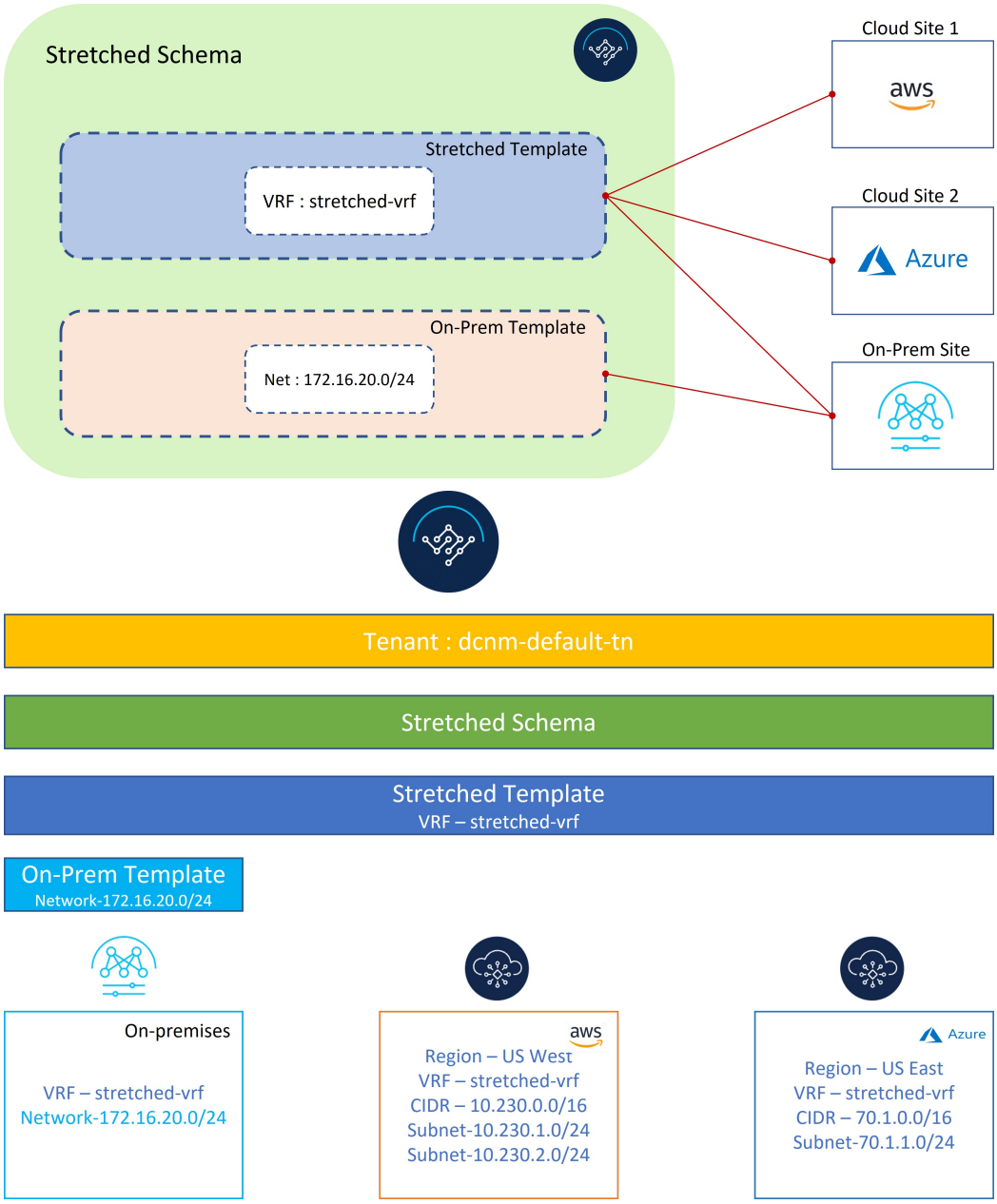
Stretching the same VRF to all the sites enables the exchanging of prefixes between the sites without having the requirement of any additional routing configuration. CIDR blocks (used to provision subnets in cloud VPCs/VNets) are mapped to this stretched VRF.

Note Stretching a Layer 2 subnet across on-premises and cloud sites or between cloud sites is not supported.

The following figure shows two templates being created under the Demo schema:

- The `Stretched Template`, which defines the VRF to be deployed to all three sites. For cloud sites, we define the regions and CIDR blocks under the VRF.
- The `On_Prem Template`, which contains the networks to be deployed to the on-premises VXLAN fabric.

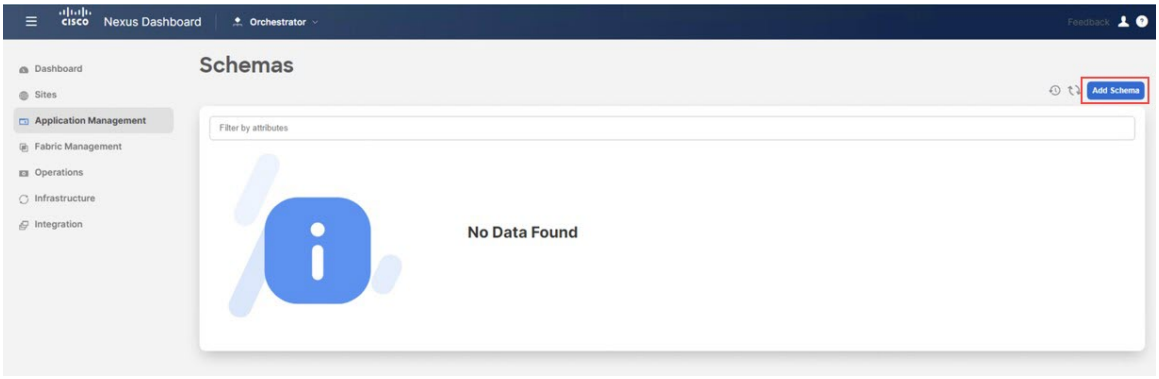
Figure 1:



Configure the Stretched VRF Use Case

Step 1 In NDO, navigate to **Application Management** > **Schemas** and click **Add Schema**.

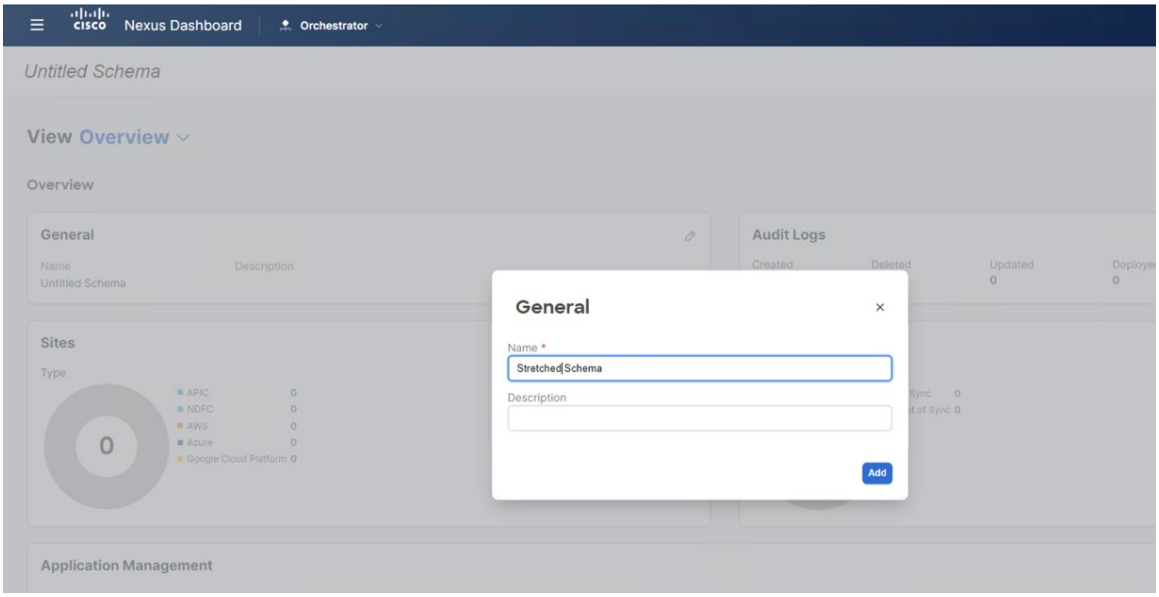
Figure 2:



Step 2 Provide the schema name and click **Add**.

For this use case, we will name the new schema `Stretched Schema`.

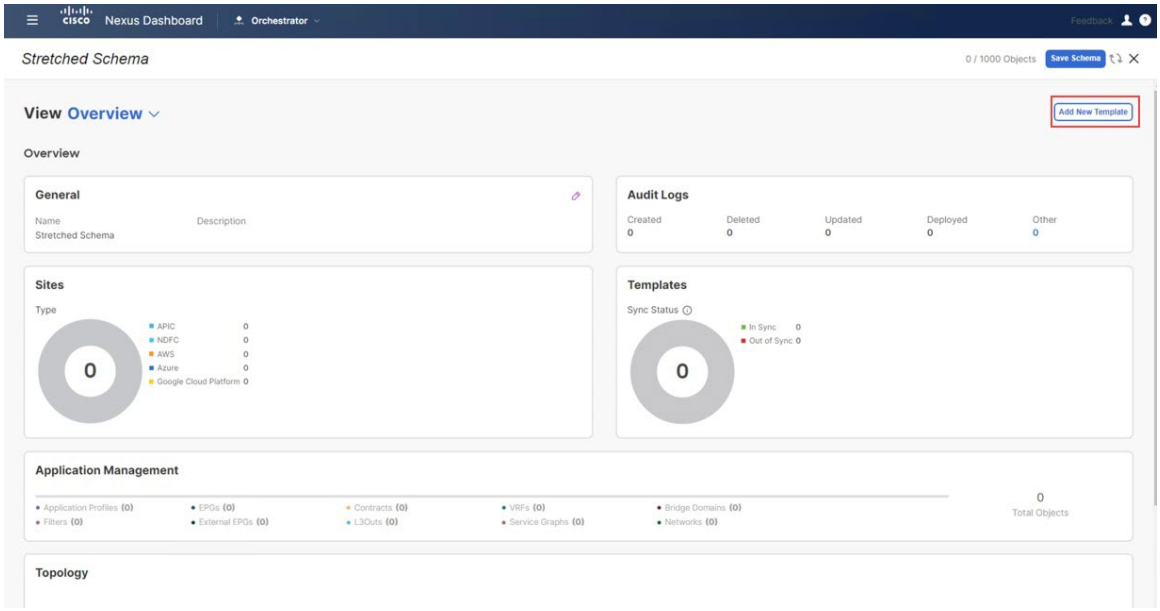
Figure 3:



You are returned to the **Overview** page for the new `Stretched Schema` schema.

Step 3 Click **Add New Template**.

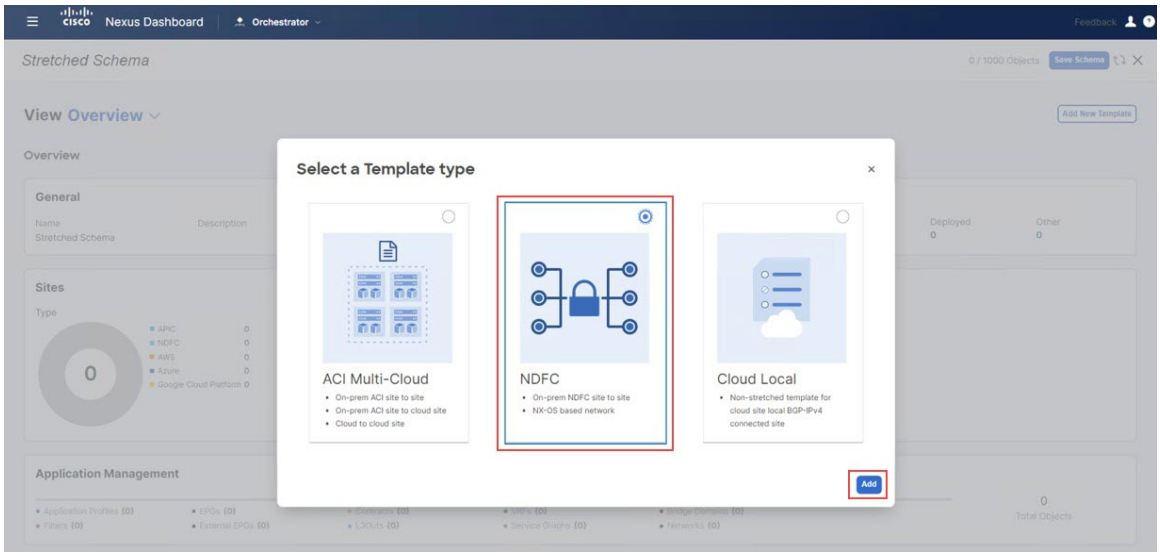
Figure 4:



Step 4 Choose the NDFC template, then click **Add**.

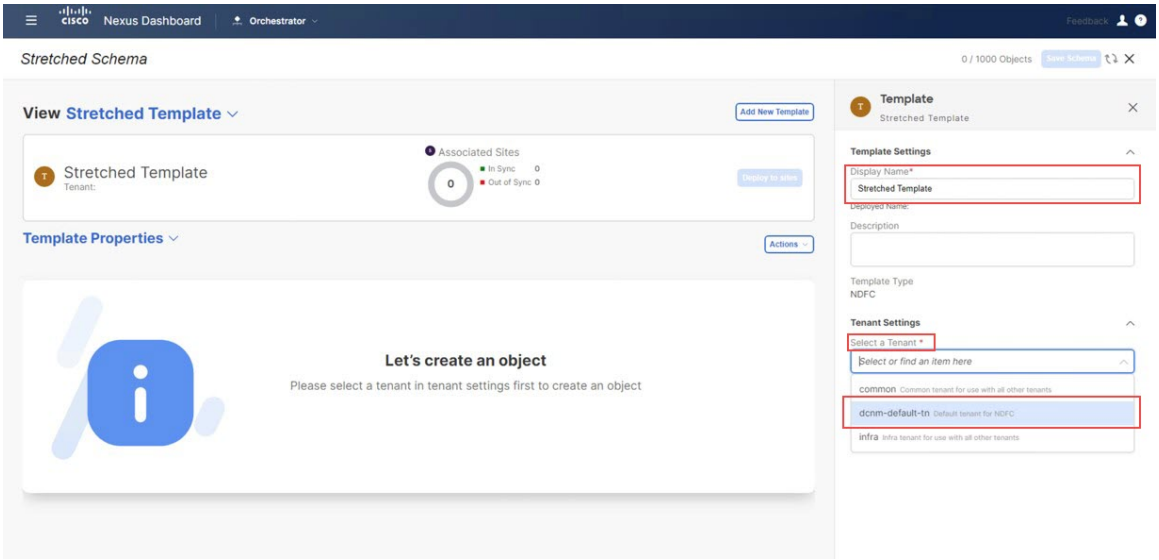
You should use the NDFC template type for on-premises as well as cloud sites.

Figure 5:



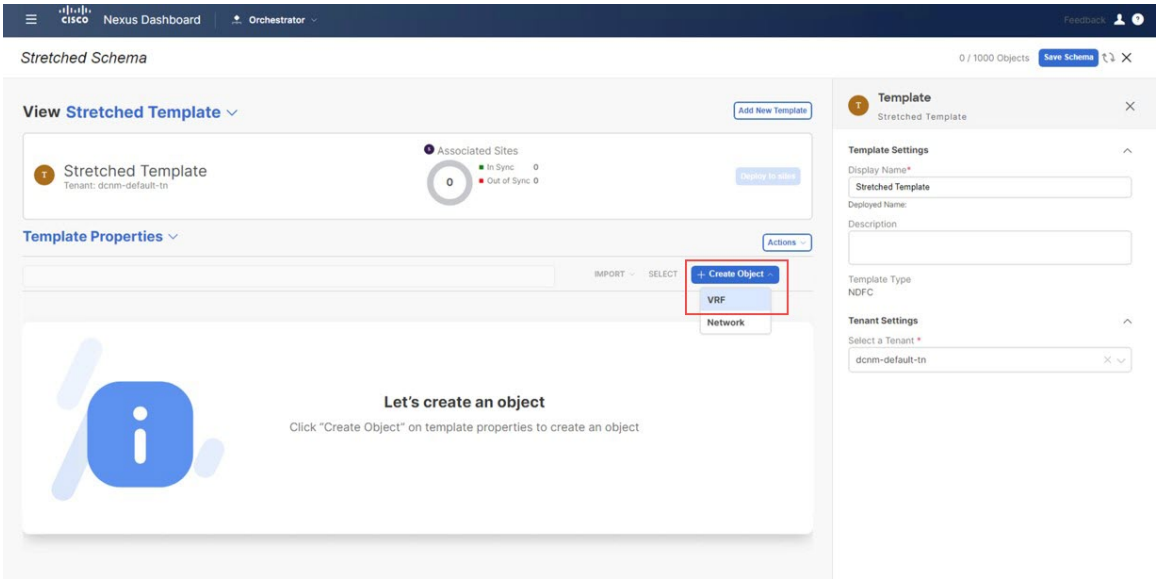
Step 5 Enter a name in the **Display Name** field to create an NDFC-type template (for example, `Stretched Template`) and select the `dcnm-default-tn` tenant in the **Select a Tenant** field to map the template to that tenant.

Figure 6:



Step 6 Under **Template Properties**, click **Create Object** and choose **VRF** to create a VRF that will be stretched to all the sites.

Figure 7:

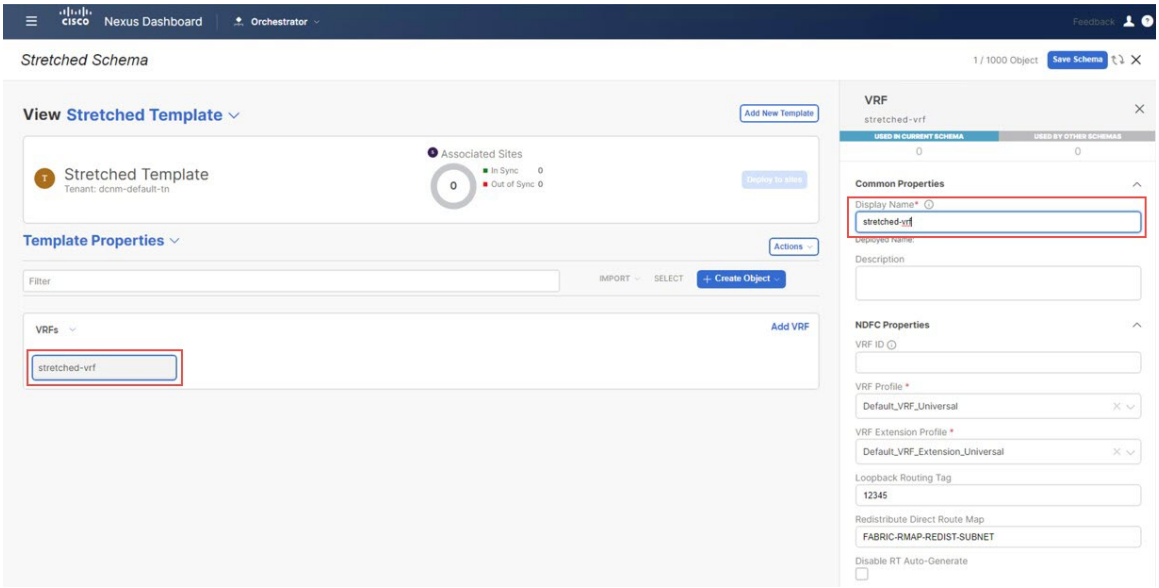


Note If you have an on-premises VRF already created that you want to use instead of creating a new VRF, under **Template Properties**, click **Import**, then import the already-created VRF.

Currently, we only support importing VRFs and networks from on-premises sites.

Step 7 Enter a name in the **Display Name** field for the stretched VRF (for example, `stretched-vrf`).

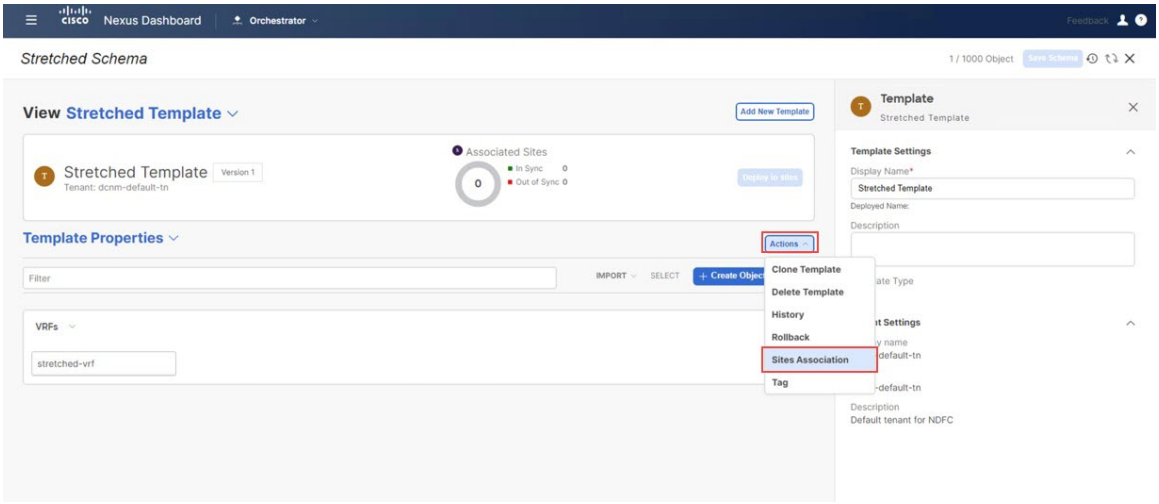
Figure 8:



Step 8 Associate all the sites (on-premises and cloud sites) to `Stretched Template` for the stretched VRF use case.

a) In the **Template Properties** area, click **Actions** > **Sites Association**.

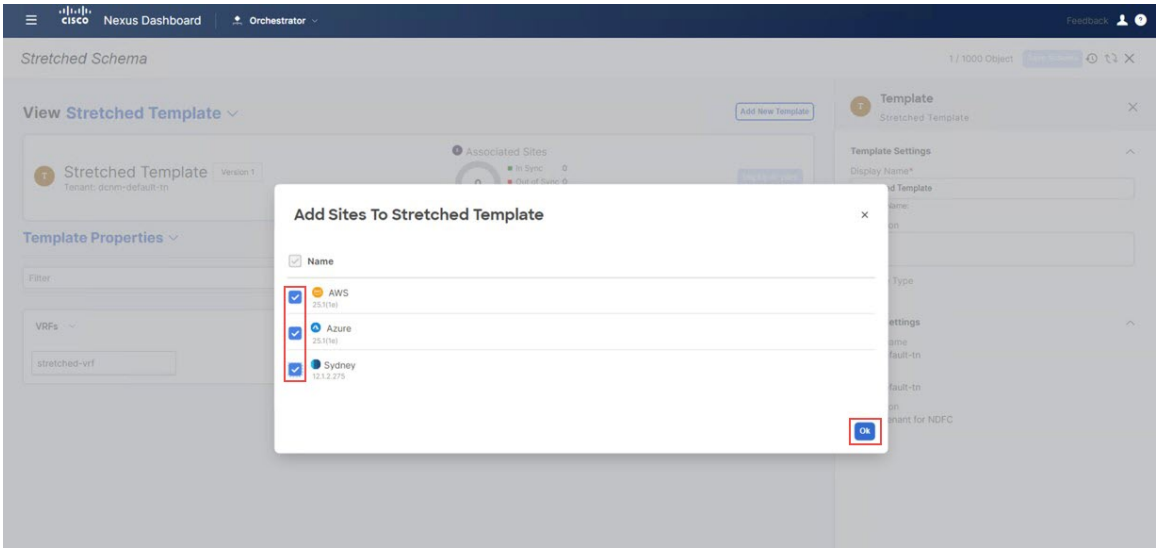
Figure 9:



b) Select all the sites, then click **Ok**.

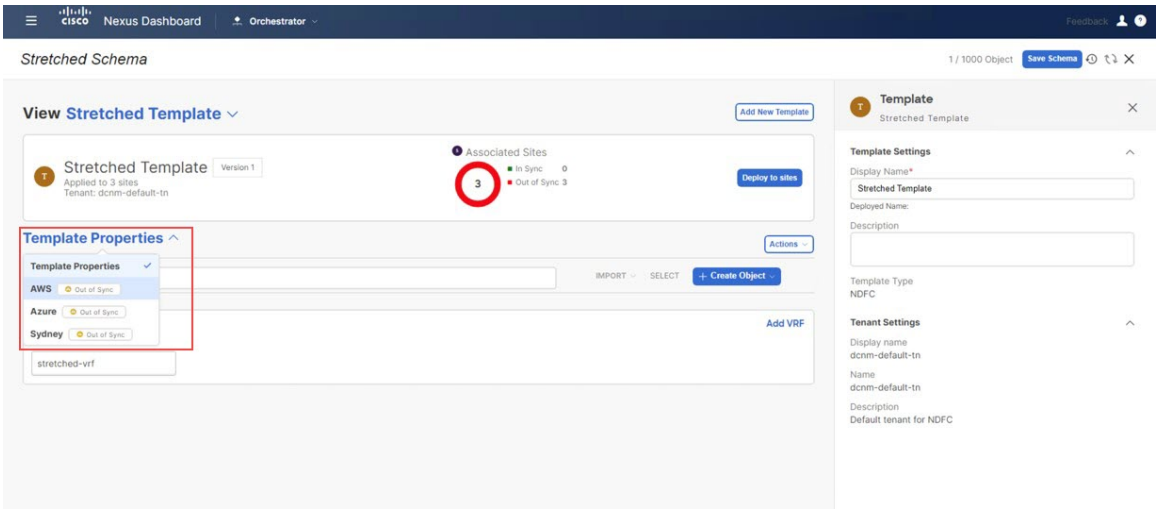
This also allows you to select each site individually to provision site-level configurations for the objects defined in this template (in this specific case, just the stretched VRF).

Figure 10:



Once the sites are associated with the template, they will appear under **Template Properties**.

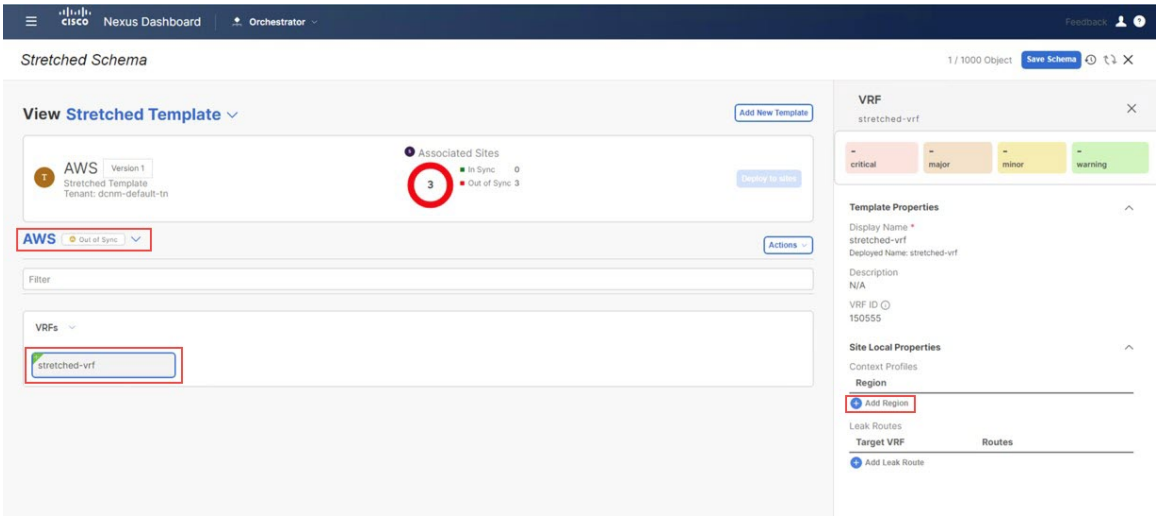
Figure 11:



Step 9 Click **Template Properties** and select the first cloud site (the AWS site in this example use case), then associate the VRF to the appropriate regions to create the VPC.

a) Click the VRF, then click **Add Region** to create the VPC in the selected region.

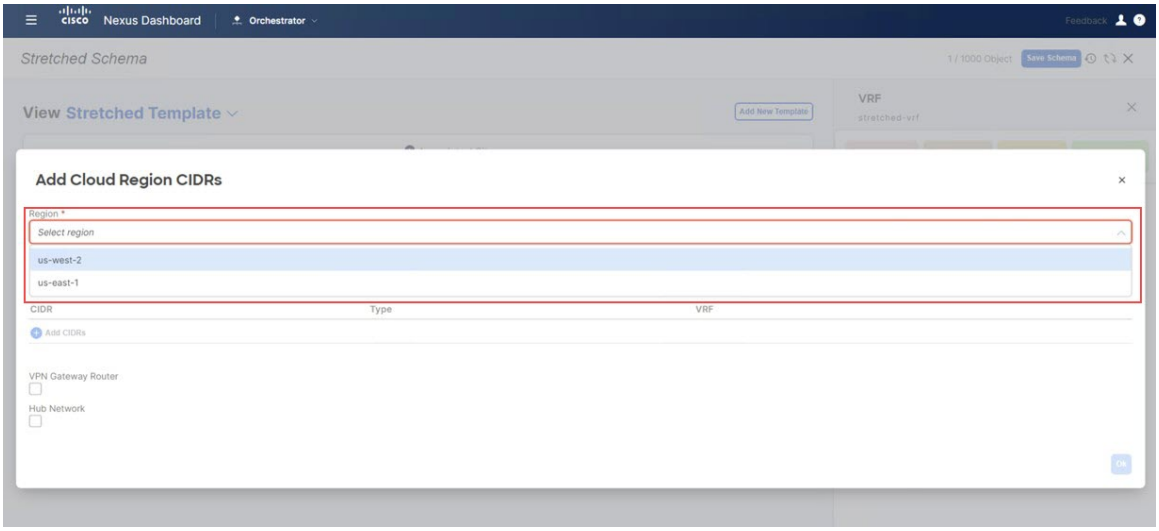
Figure 12:



The **Add Cloud Region CIDRs** window appears.

b) In the **Region** field, choose the region where you want to create the VPC.

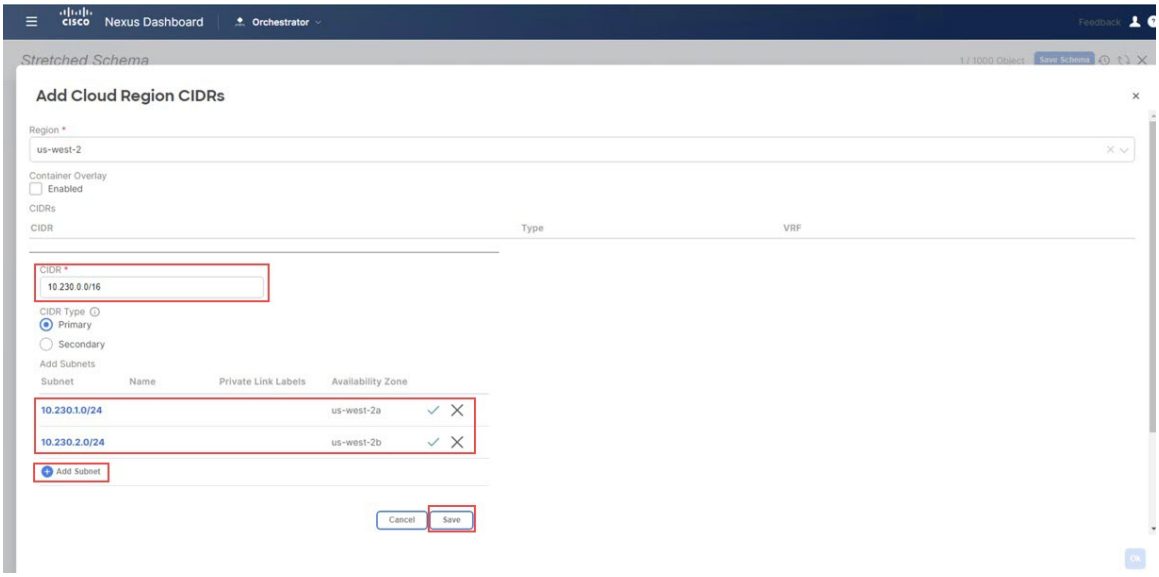
Figure 13:



c) In the **CIDR** field, click **Add CIDRs** and define a CIDR block for the VPC.

d) Click **Add Subnet** to create the subnets and map them to the availability zones, then click **Save**.

Figure 14:



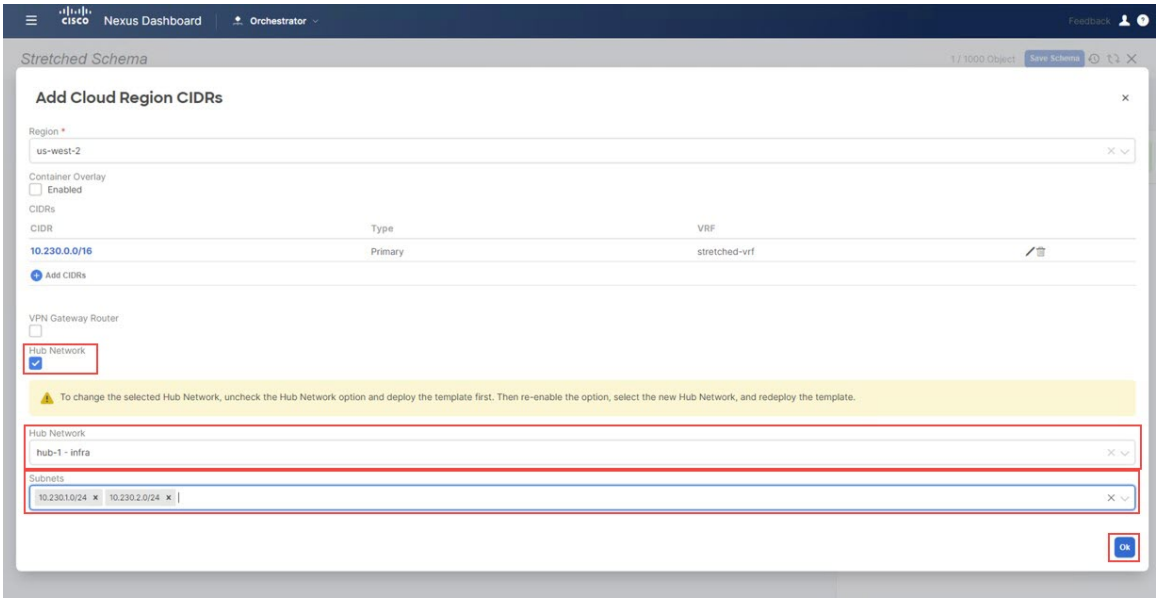
e) Check the box under the **Hub Network** field, then select the hub network that was created on the Cisco Cloud Network Controller for AWS.

This allows the Cisco Cloud Network Controller to attach the subnets onto the transit gateway, which builds the connectivity from those subnets to the transit gateway, where the transit gateway already has the connectivity to the Cisco Catalyst 8000Vs in the cloud.

f) In the **Subnets** field, map the subnets that will be used for the transit gateway.

It is best practice to have a dedicated subnet that will be used for the transit gateway.

Figure 15:



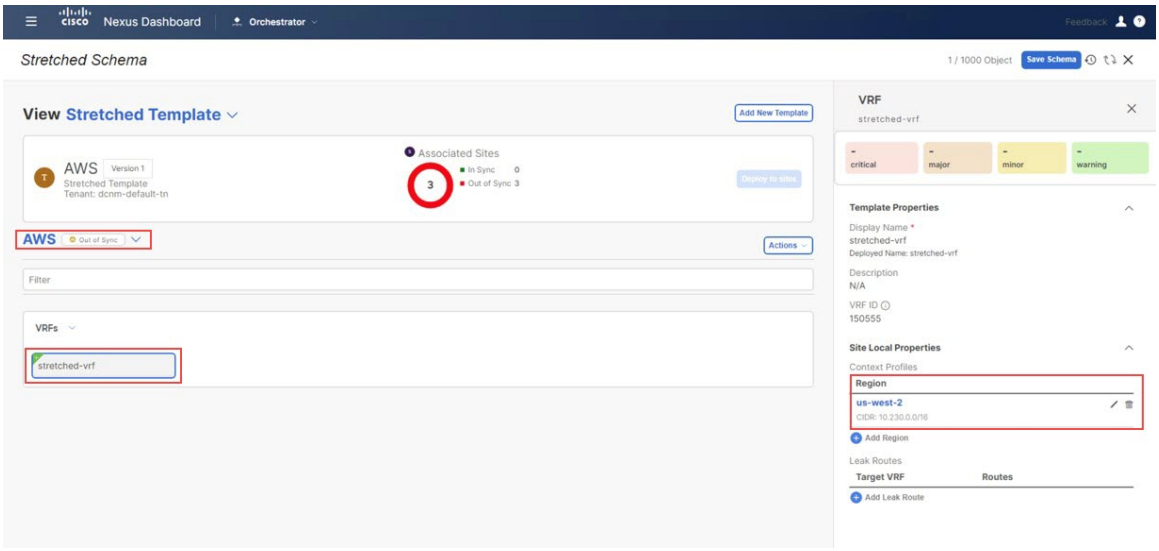
Note Alternatively, a dedicated /25 subnet per availability zone can be used for connectivity to a hub network (TGW). This will allow the entire end-point subnets to be used for end hosts.

g) Click **Ok**.

You are returned to the AWS template window.

When this configuration is deployed, a VPC with CIDR 10.230.0.0/16 will be created in the AWS cloud, stretching between the `us-west-2a` and `us-west-2b` availability zones, with the 10.230.1.0/24 and 10.230.2.0/24 subnets created respectively.

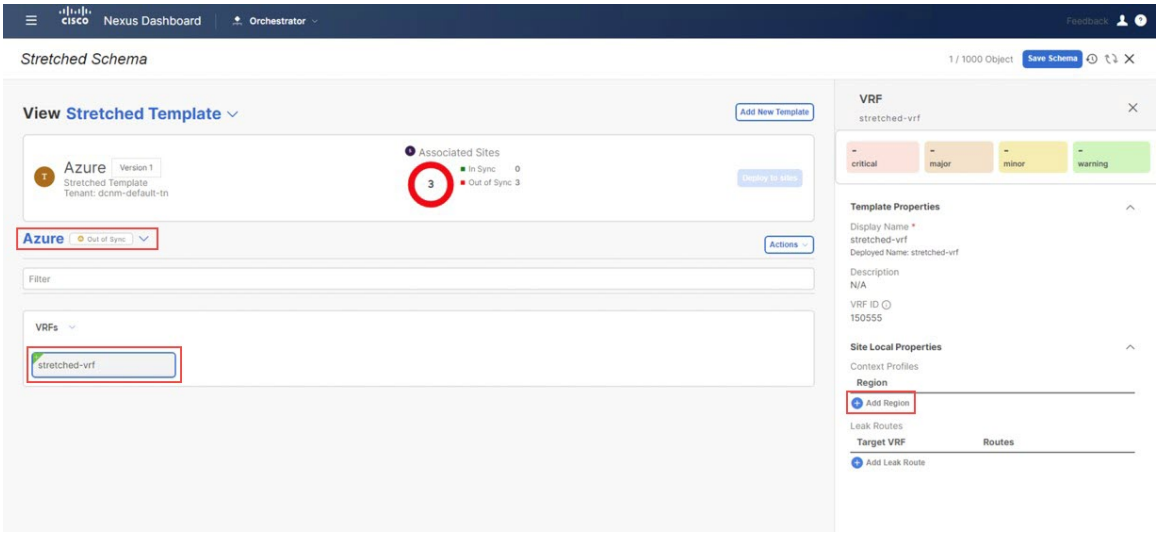
Figure 16:



Step 10 Click **Template Properties** and select the second cloud site (the Azure site in this example use case), then associate the VRF to the appropriate region to create the VNet.

a) Click the VRF, then click **Add Region** to create the VNet in the selected region.

Figure 17:



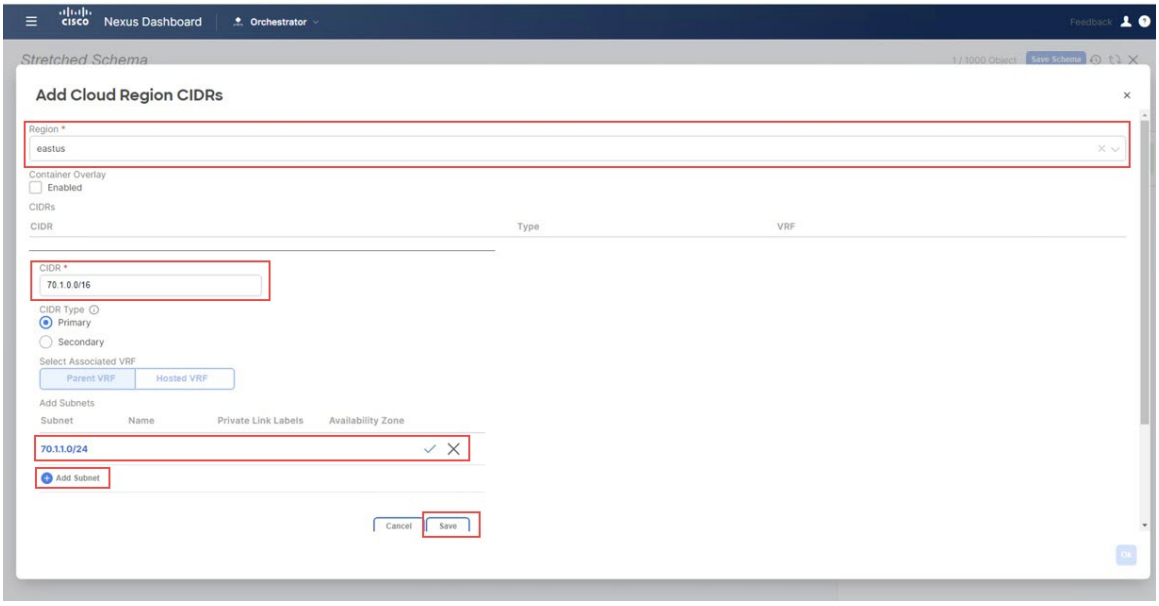
The **Add Cloud Region CIDRs** window appears.

b) In the **Region** field, choose the region where you want to create the VNet.

c) In the **CIDR** field, click **Add CIDRs** and define a CIDR block for the VNet.

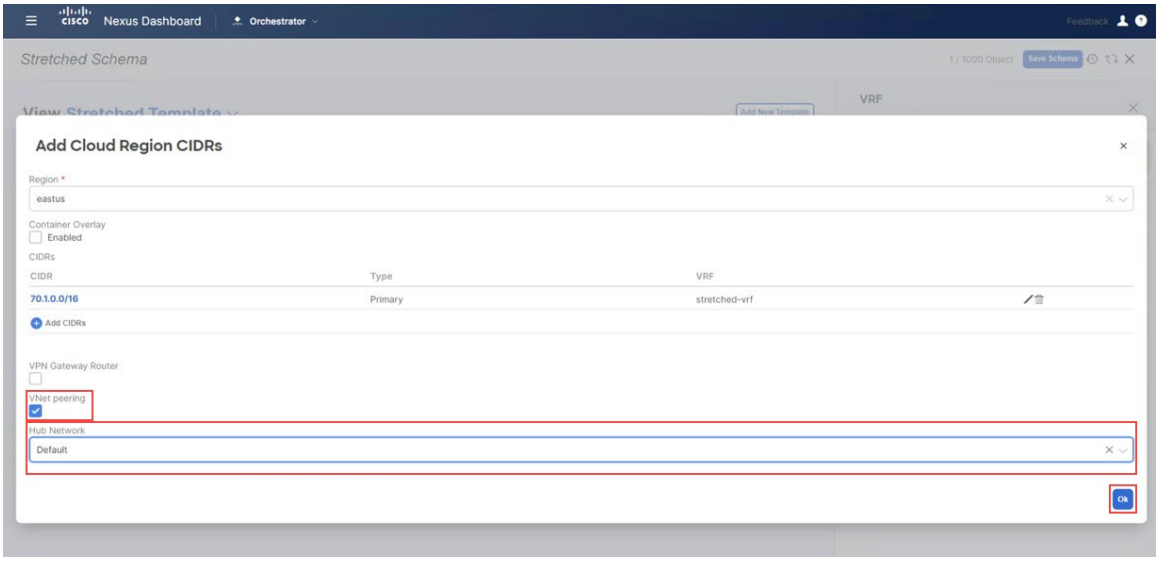
d) Click **Add Subnet** to create the subnets, then click **Save**.

Figure 18:



e) Check the box under the **VNet Peering** field, then select the `Default` hub network that was created on the Cisco Cloud Network Controller for Azure.

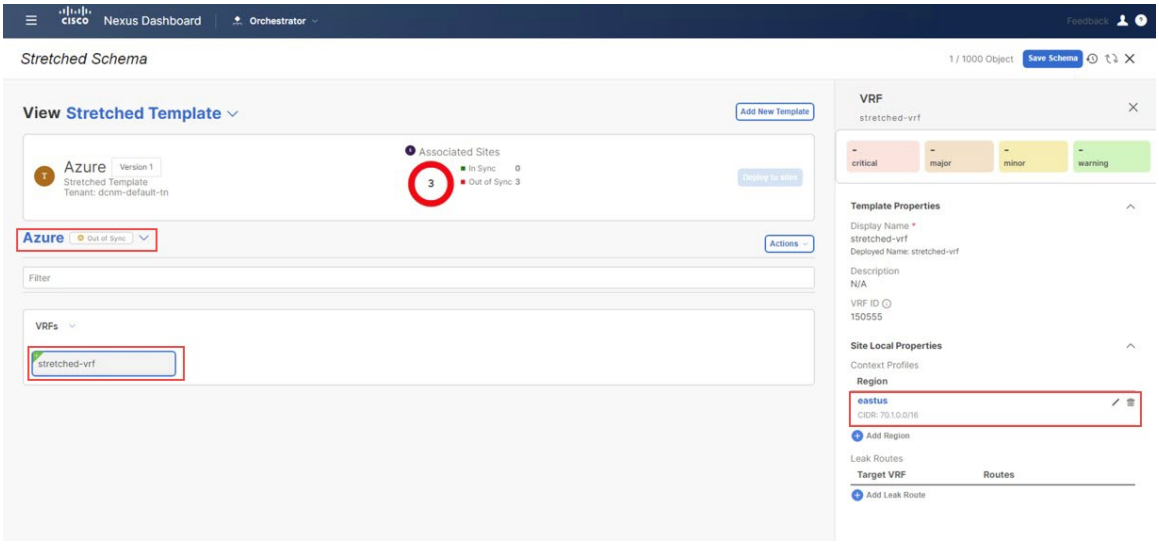
Figure 19:



f) Click **Ok**.

When this configuration is deployed, the VNet that you configured (in this example, 70.1.0.0/16) will be created on the appropriate region in Azure (in this example, the eastus Azure region) and VNet peering is configured to the infra VNet in the infra tenant in Azure.

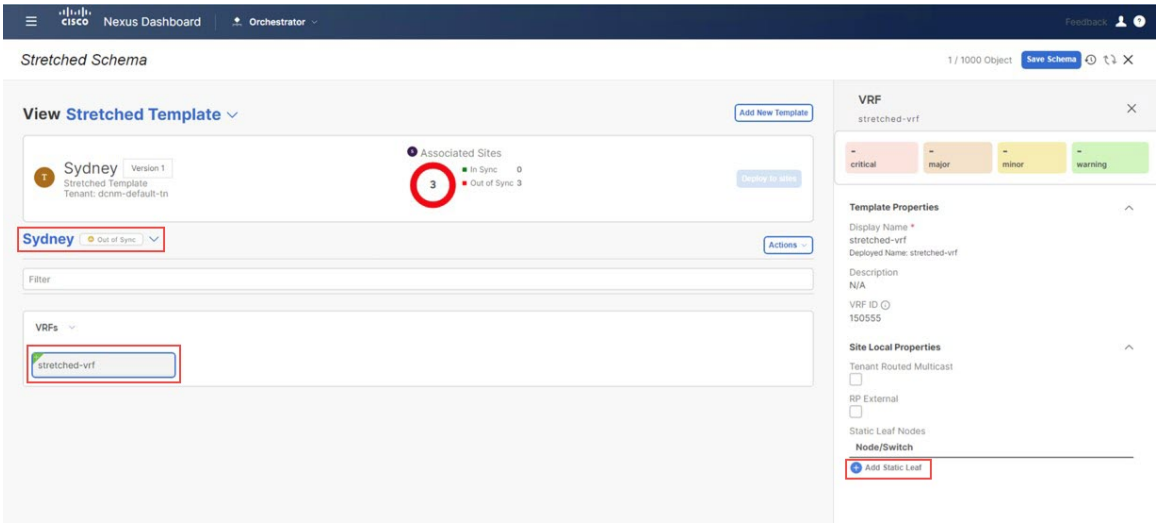
Figure 20:



Step 11 Click **Template Properties** and select the on-premises site (the Sydney site in this example use case), then select the `stretched-vrf` VRF.

Step 12 In the right pane, click **Add Static Leaf**.

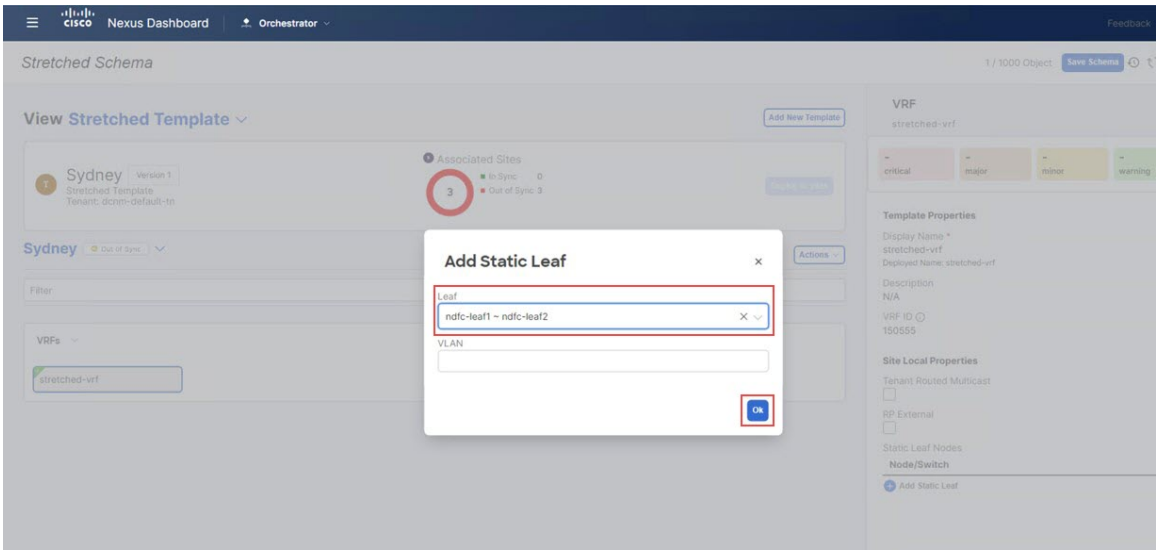
Figure 21:



The **Add Static Leaf** window appears.

Step 13 In the **Leaf** field, select the leaf/border/border gateway device where this VRF is to be deployed and click **Ok**.

Figure 22:

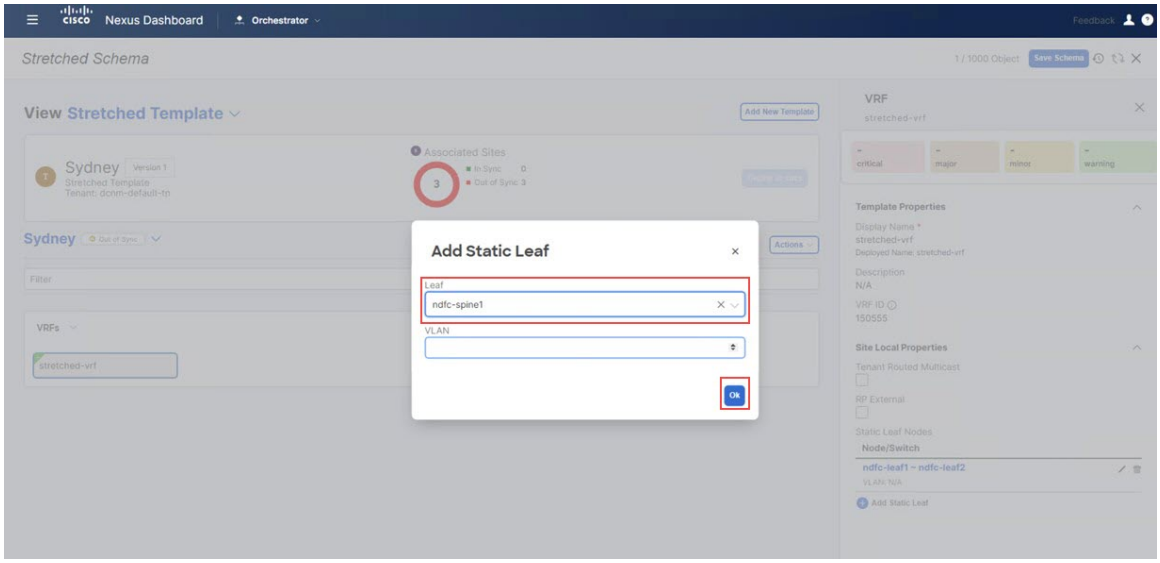


You are returned to the `Stretched Template` page.

Step 14 Click **Add Static Leaf** again to add additional leaf/border/border gateway devices where this VRF is to be deployed.

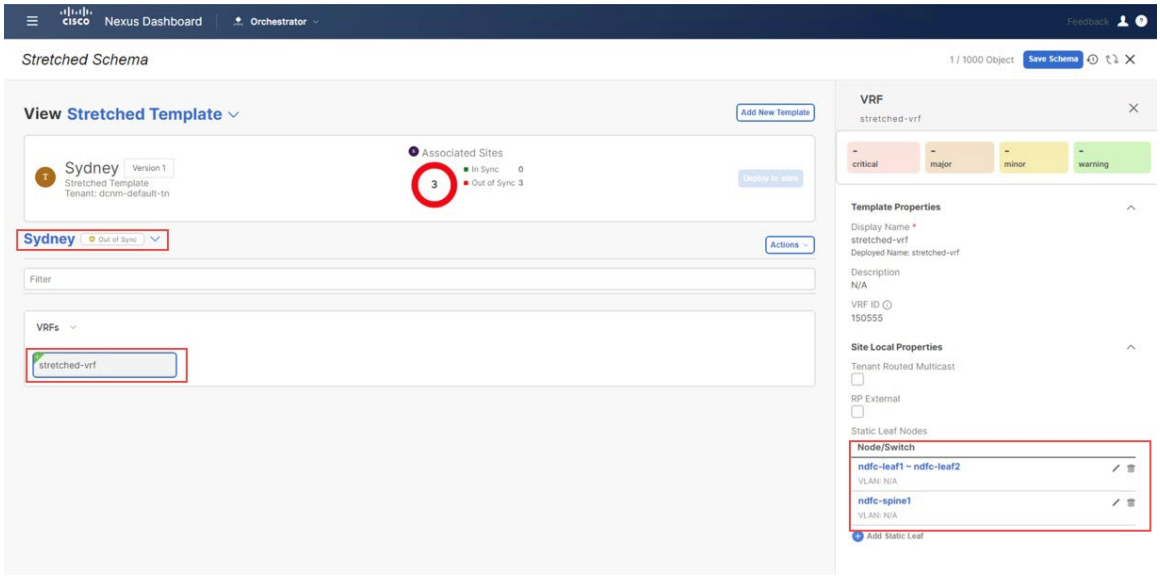
In this example, you need to deploy the VRF on the leaf nodes (where the endpoints part of the network mapped to the VRF will be connected) and on the BGW spine node to be able to extend the Layer 3 connectivity for the VRF towards the cloud sites.

Figure 23:



When you have added all of the leaf/border/border gateway devices where this VRF is to be deployed, they will appear in the **Stretched Template** page.

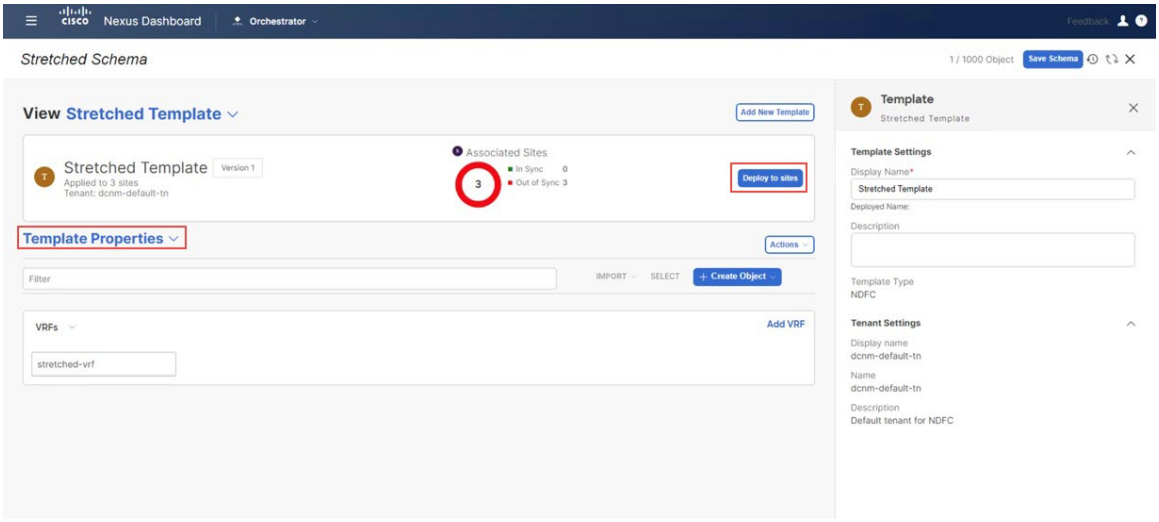
Figure 24:



Step 15 Click the arrow next to the Sydney site, and from the drop-down menu, select **Template Properties**.

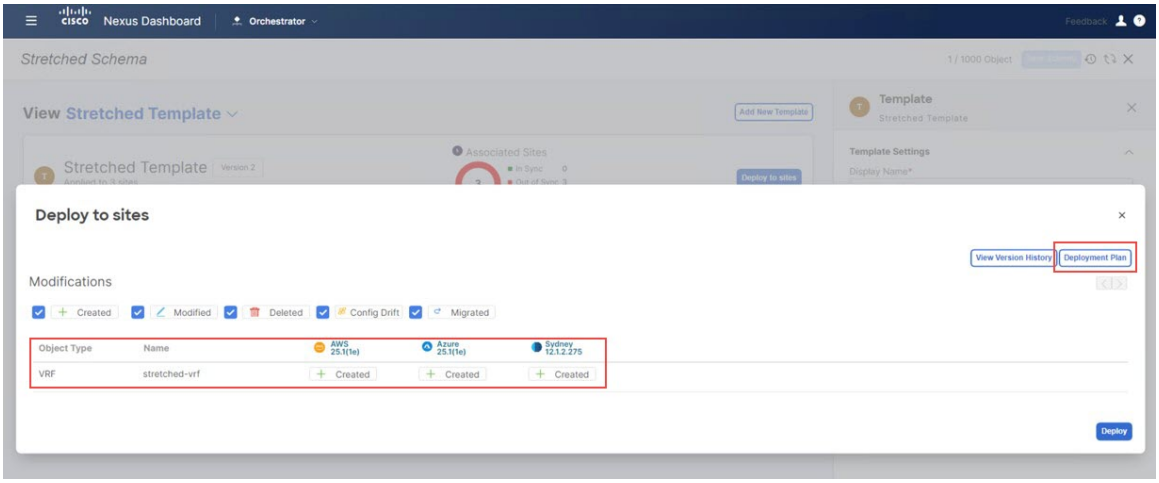
Step 16 Click **Deploy to sites**.

Figure 25:



The **Deploy to Sites** window appears, showing the three sites where the stretched template will be deployed.

Figure 26:



Step 17 Click **Deployment Plan** for additional verification, then click on each site to see the deployment plan for that specific site.

Figure 27:

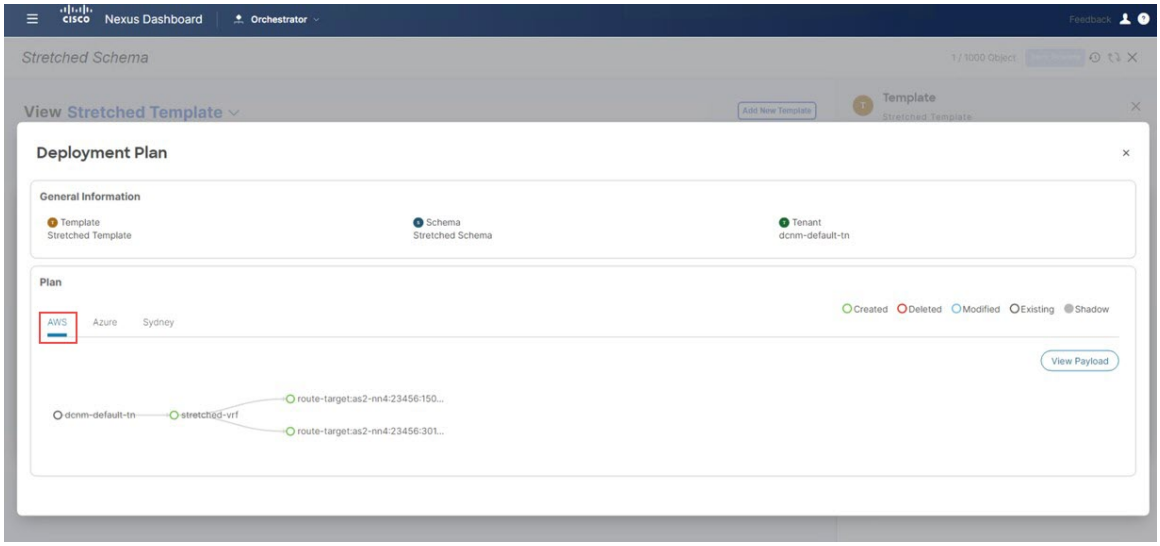


Figure 28:

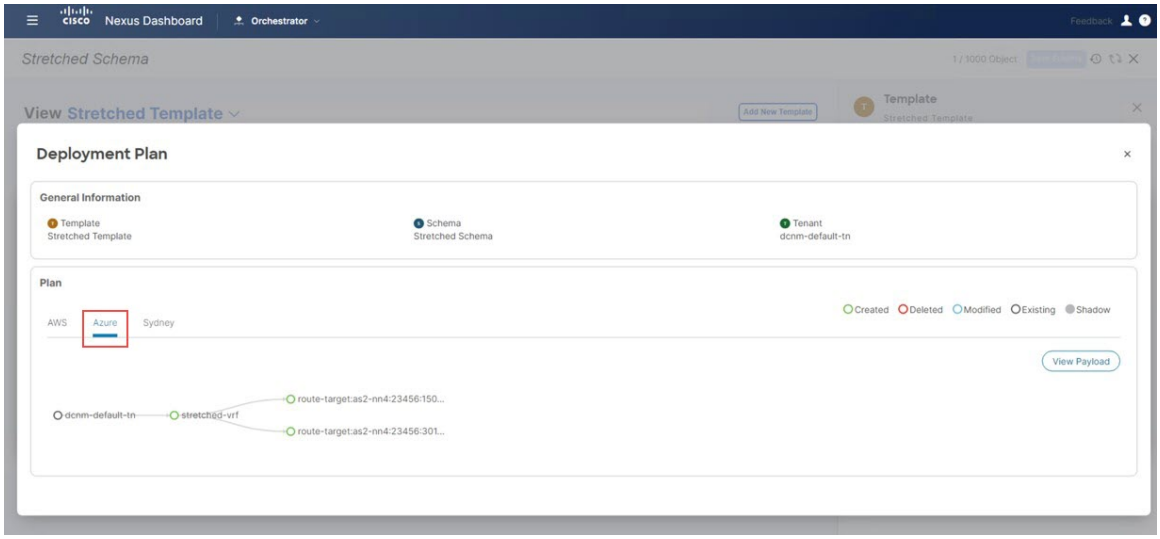
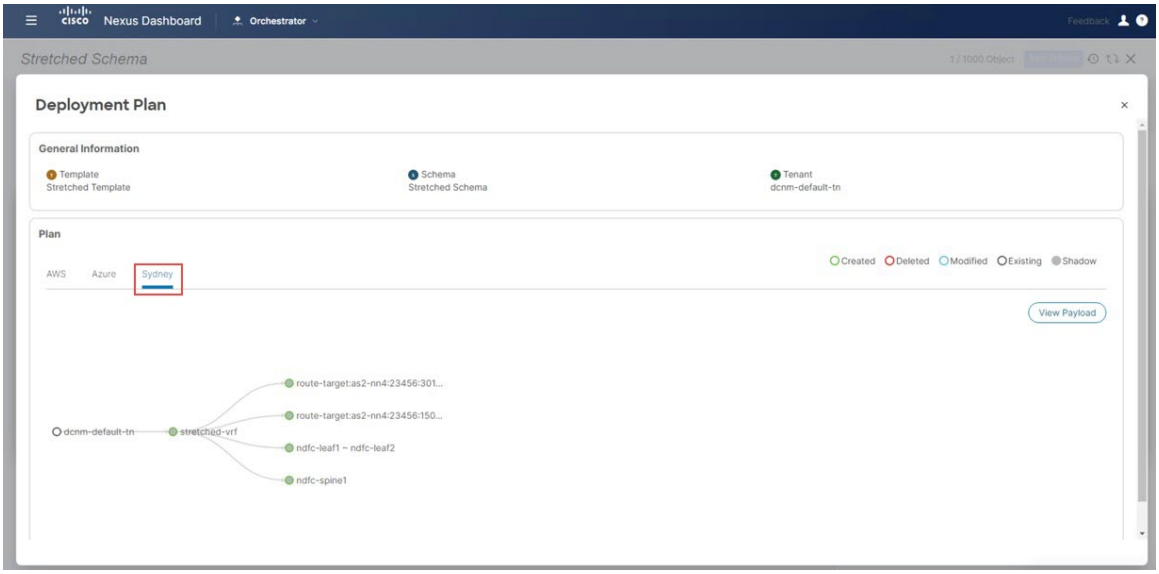
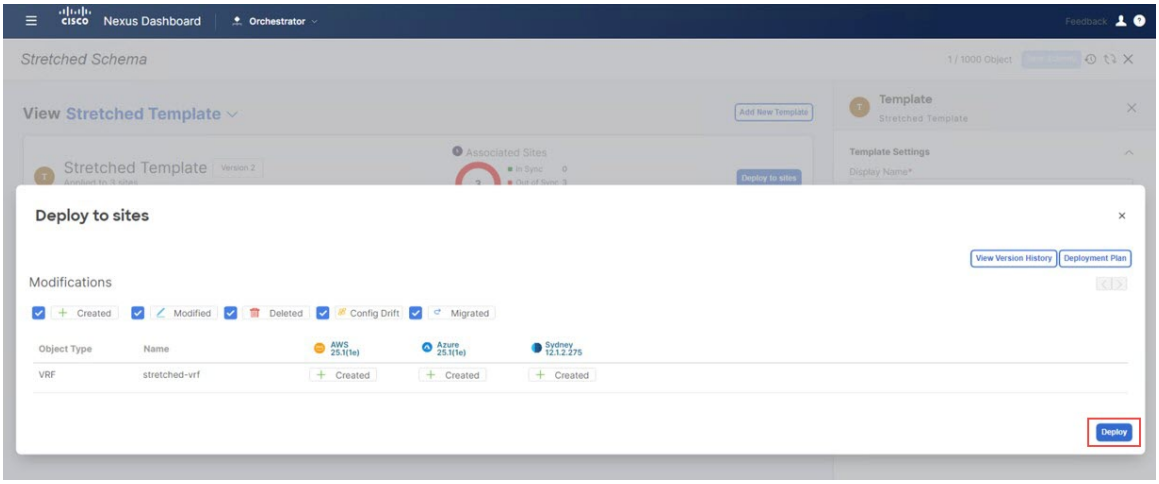


Figure 29:



Step 18 Click **Deploy** to have NDO push the configurations to the site specific controllers (NDFC and Cloud Network Controller).

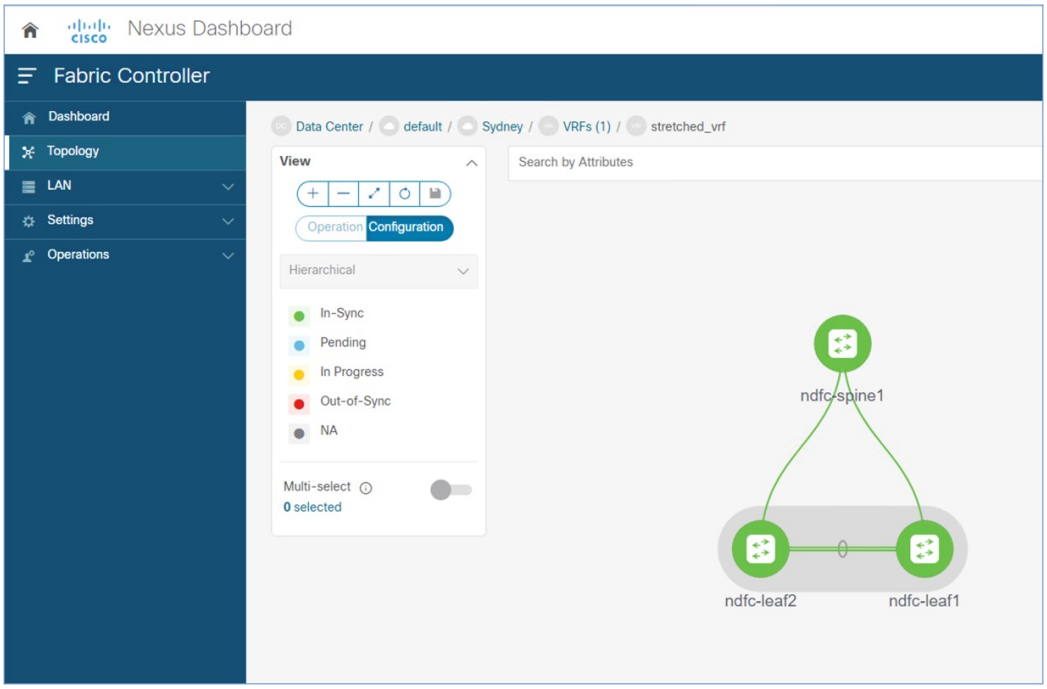
Figure 30:



Step 19 Verify that the configurations were deployed successfully.

- To view the VRF deployment on NDFC, go to the **Topology** view, select the on-premises fabric **Sydney** > **VRFs**, then select `stretched-vrf`.

Figure 31:



- Connect to the Cloud Network Controller deployed on AWS to verify that the configurations for the first cloud site (AWS) were deployed successfully.

  Go to **Application Management** > **VRFs**, locate `stretched-vrf` and click under the column **VPCs**, then go to the **Overview** page and click under **Subnets**.

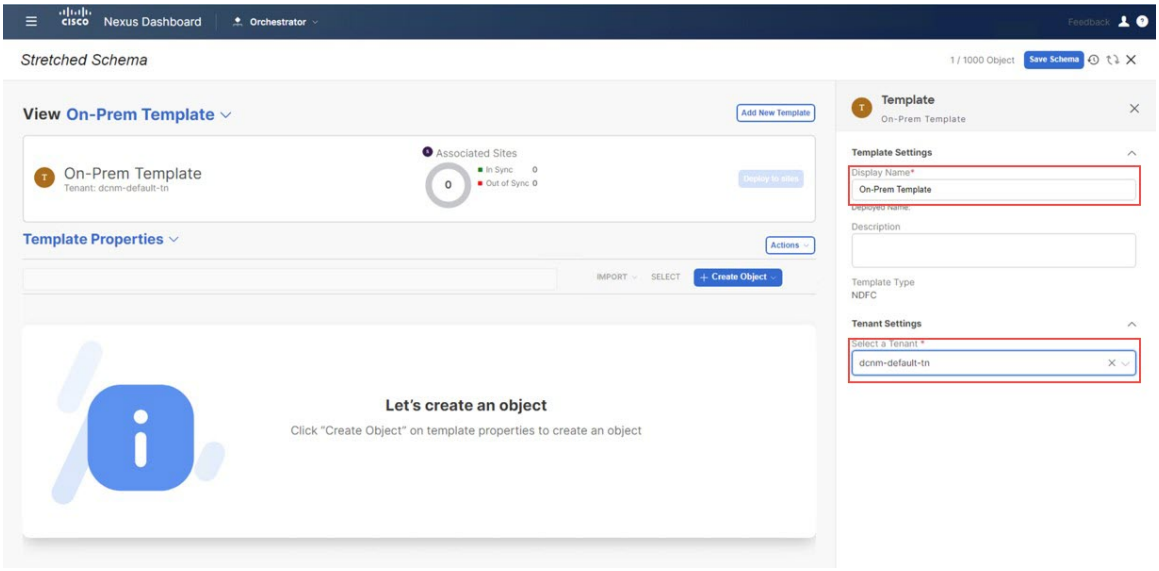
- Connect to the Cloud Network Controller deployed on Azure to verify that the configurations for the second cloud site (Azure) were deployed successfully.

  Go to **Application Management** > **VRFs**, locate `stretched-vrf` and click under the column **Virtual Networks**, then go to the **Overview** page and click under **Subnets**.

Step 20 Create another template under `Demo Schema` for deploying networks on the on-premises site.

a) Under the `Demo Schema` template, click **Add New Template**.
b) Choose the NDFC template.
c) Enter a name in the **Display Name** field to create an NDFC-type template (for example, `On-Prem Template`) and select the `dcnm-default-tn` tenant in the **Select a Tenant** field to map the template to that tenant.

Figure 32:

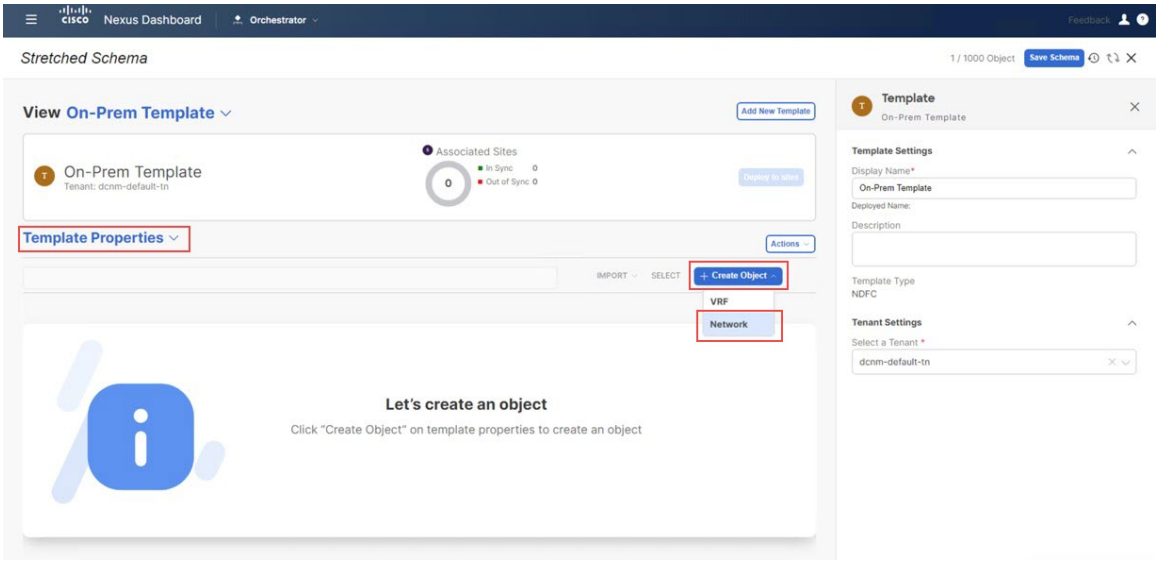


Step 21 Create the `net20` network under the VRF on `On-Prem Template`.

Note If you have a network already created that you want to use instead of creating a new network, under **Template Properties**, click **Import**, then import the already-created network.

a) Under **Template Properties**, click **Create Object** and choose **Network** to create a network.

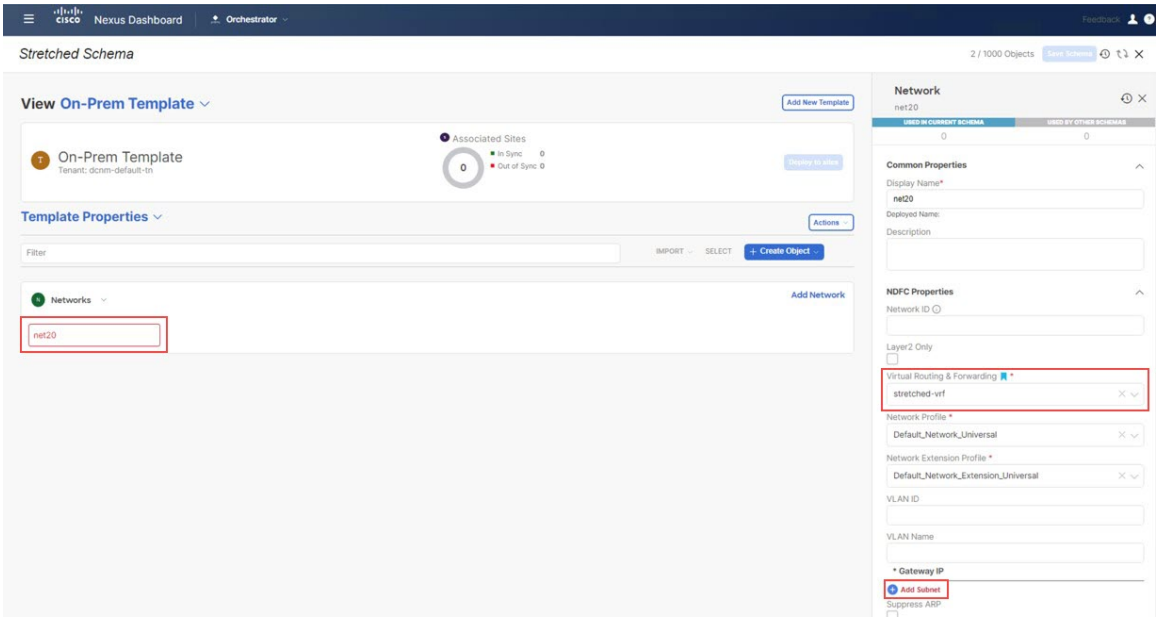
Figure 33:



b) Enter a name in the **Display Name** field for the network (for example, `net20`).

c) In the **Virtual Routing & Forwarding** field, choose the `stretched-vrf` VRF to map `net20` to that VRF.

Figure 34:

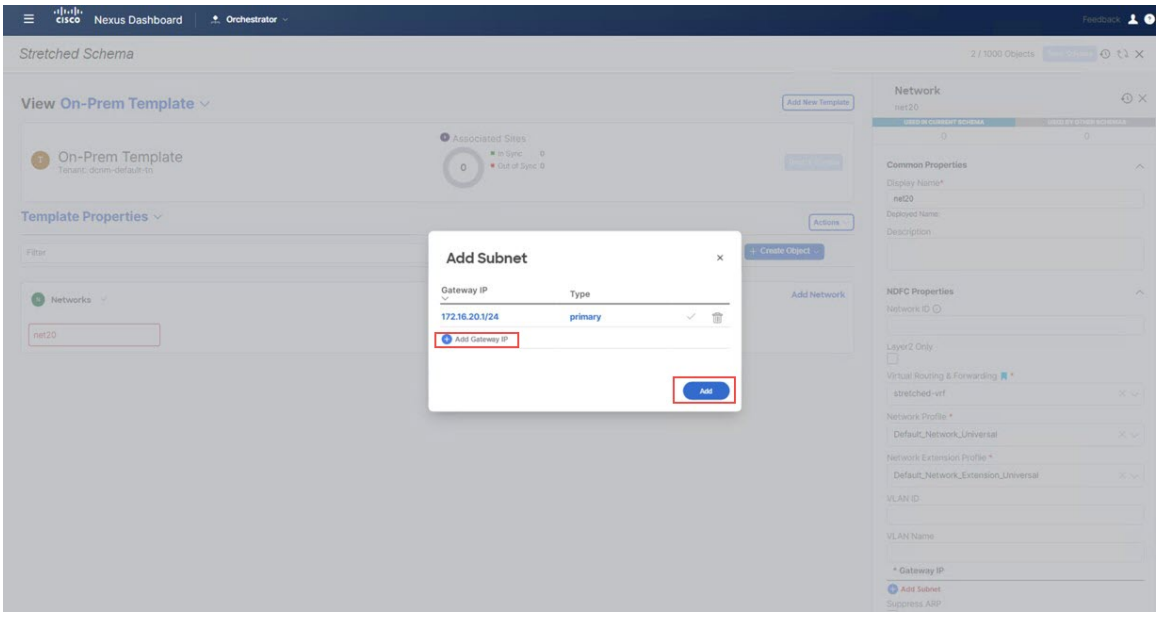


d) In the **Gateway IP** field, click **Add Subnet**.

The Add Subnet window appears.

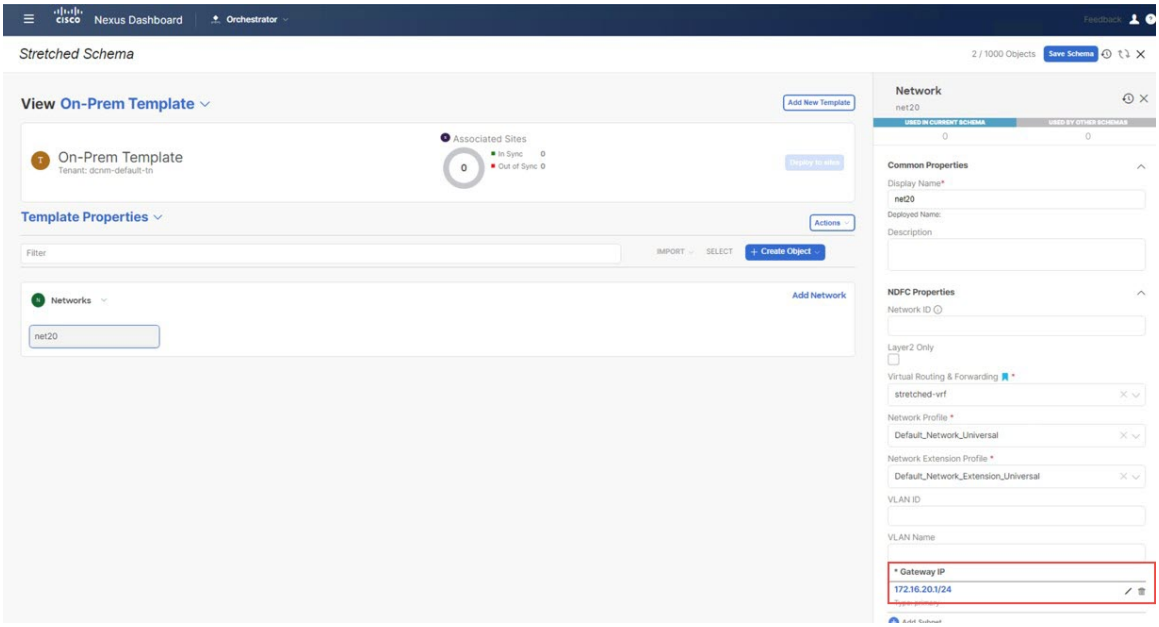
e) Click **Add Gateway IP** and provide the gateway IP address, then click the checkmark to accept the value and click **Add**.

Figure 35:



The gateway IP address is now displayed in the **Gateway IP** field.

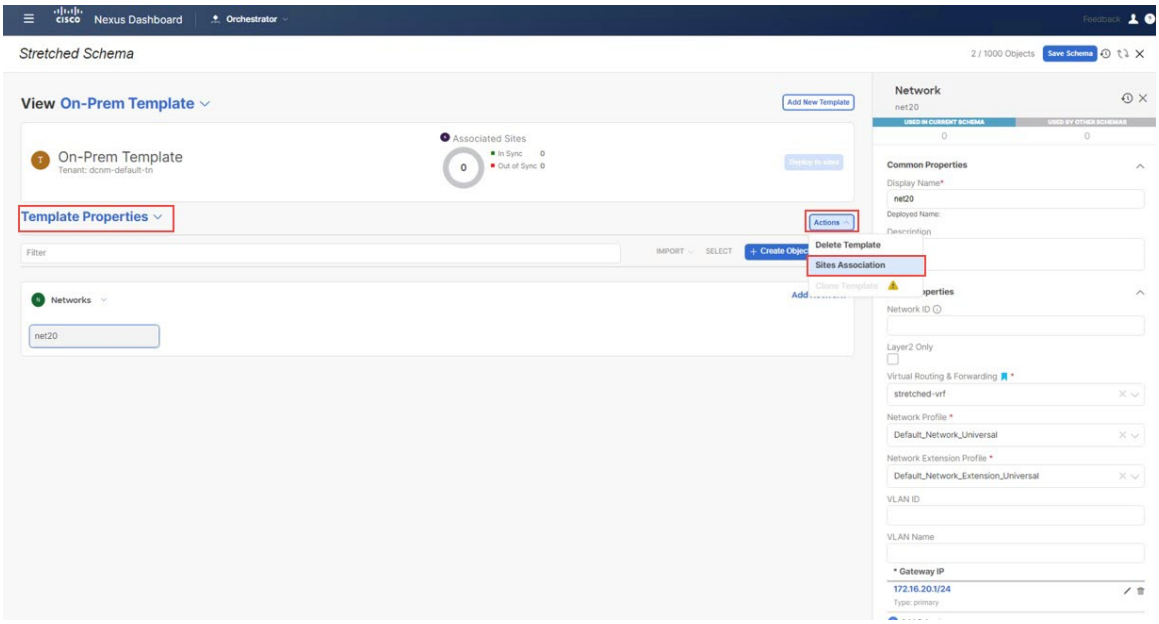
Figure 36:



f) Define other optional parameters for this network, if necessary.

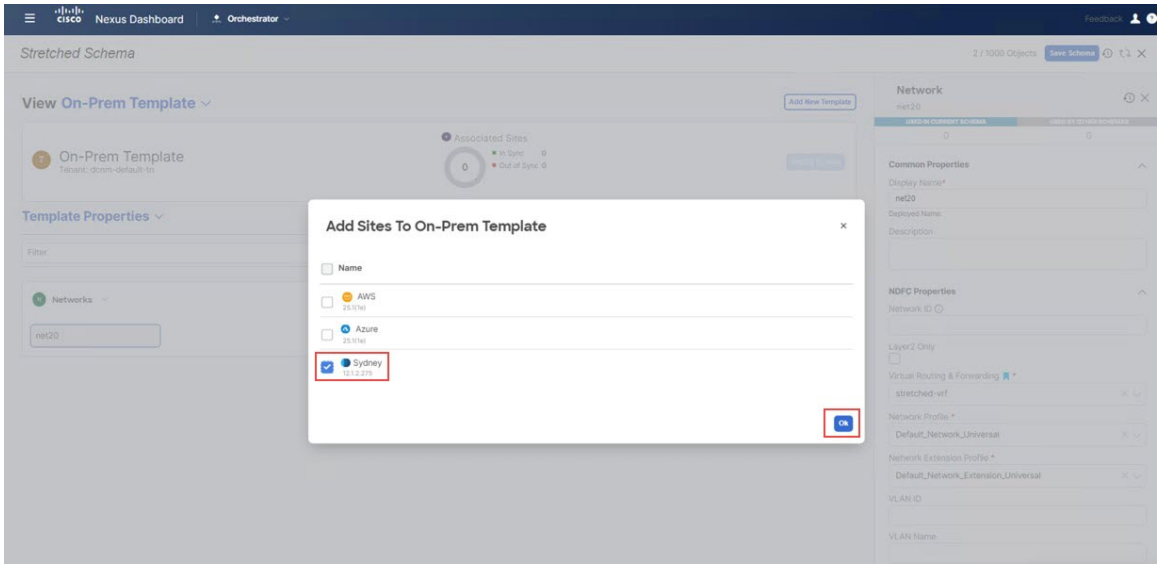
Step 22 In the **Template Properties** area, click **Actions** > **Sites Association**.

Figure 37:



Step 23 Associate this template only to the on-premises site (the Sydney site in this example use case), then click **Ok**.

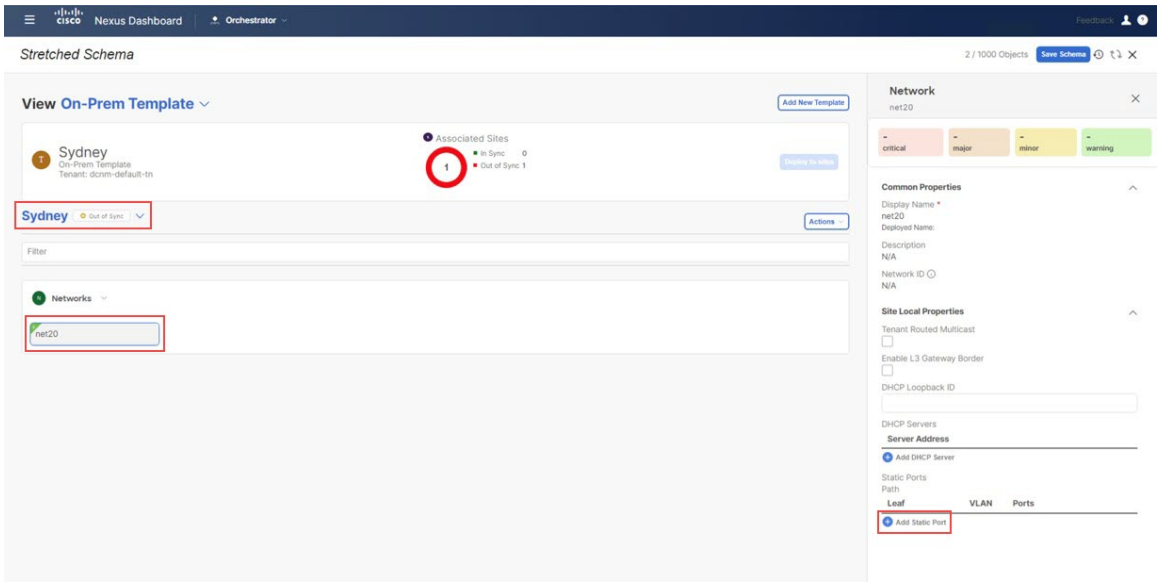
Figure 38:



You are returned to the `On-Prem Template` window.

Step 24 From the **Template Properties** drop-down, select the on-premises site (the `Sydney` site in this example use case), click the `net20` network, then click **Add Static Port** to add the ports where you want to deploy this network.
The **Add Static Port** window appears.

Figure 39:



Step 25 In the **Add Static Port** window, click **Add Path**.
The **Add Static Port** window appears.

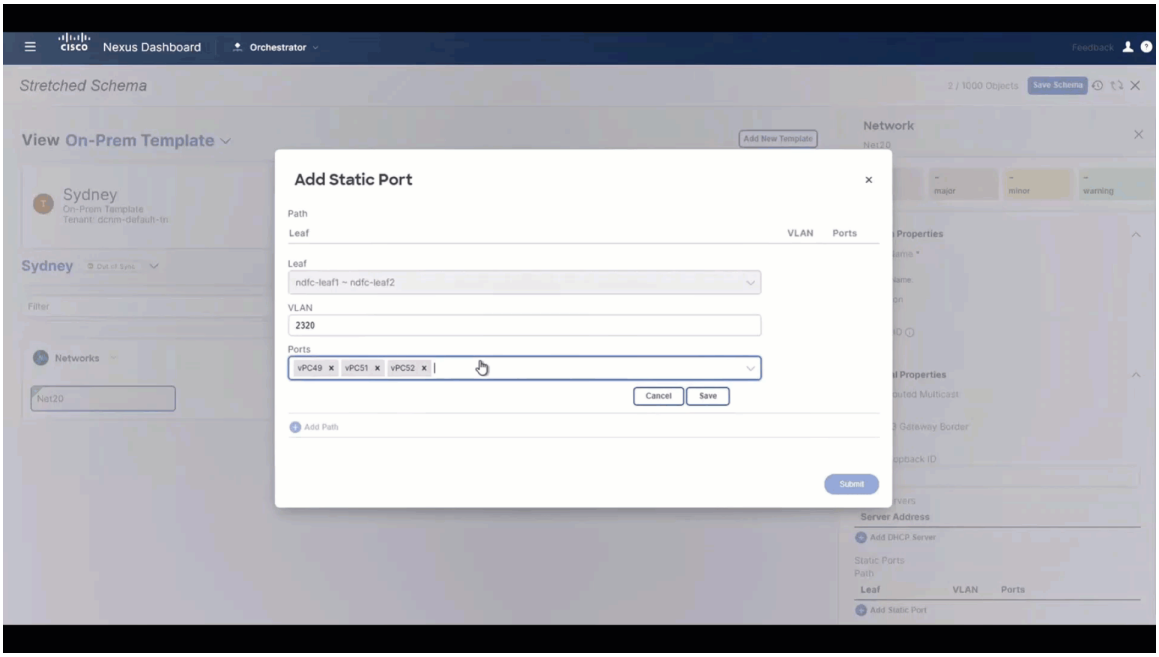
Step 26 In the **Leaf** field, select the device where you want to deploy this network.

Step 27 (Optional) Enter the necessary information in the **VLAN** field.

Step 28 In the **Ports** field, select the ports where you want to deploy this network.

Step 29 Click **Save**.

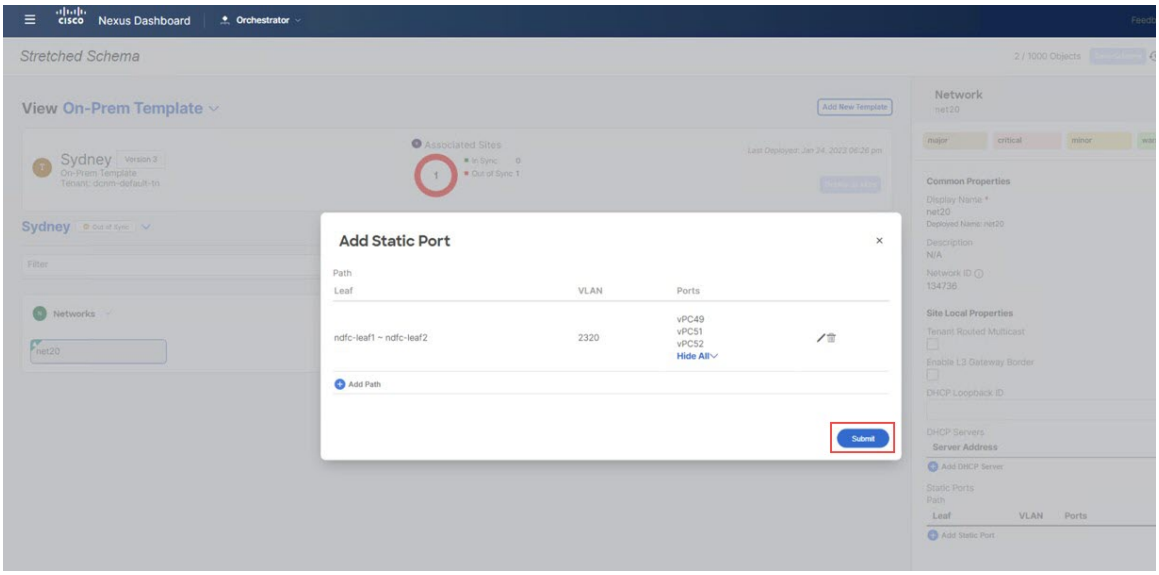
Figure 40:



You are returned to the **Add Static Port** window.

Step 30 In the **Add Static Port** window, click **Submit**.

Figure 41:

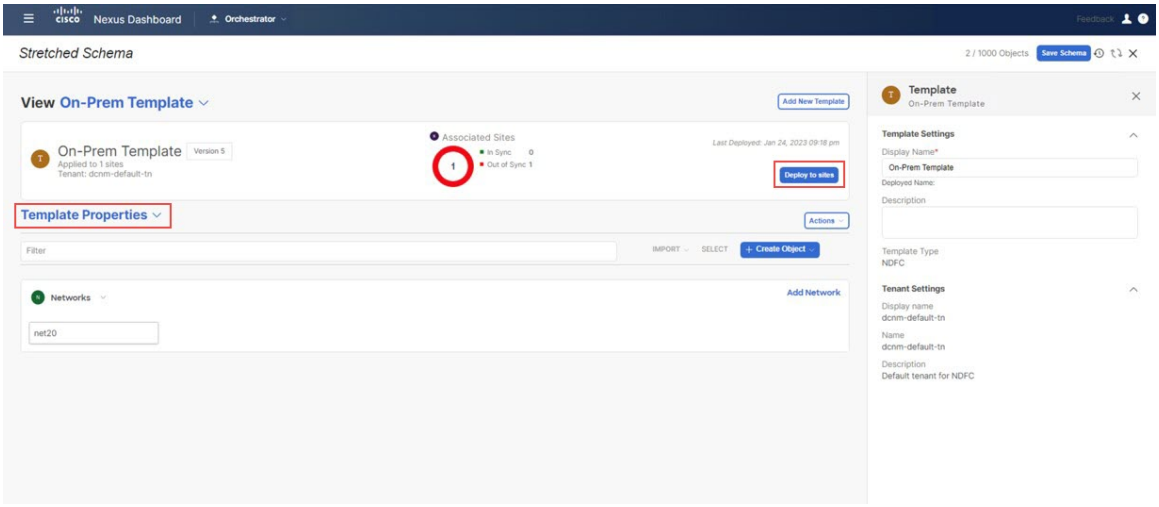


You are returned to the **On-Prem Template** window.

Step 31 Click the arrow next to the on-premises site (the `Sydney` site in this example use case), and from the drop-down menu, select **Template Properties**.

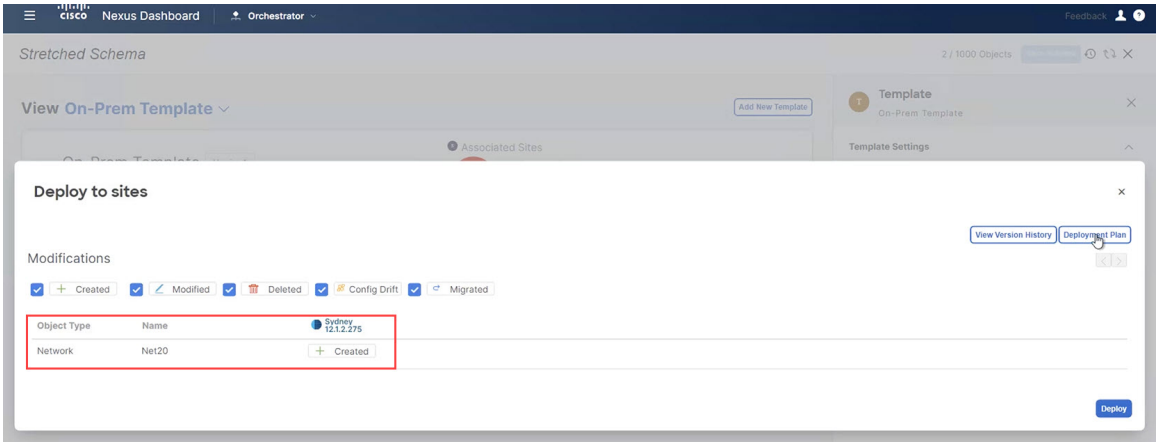
Step 32 Click **Deploy to Sites**.

Figure 42:



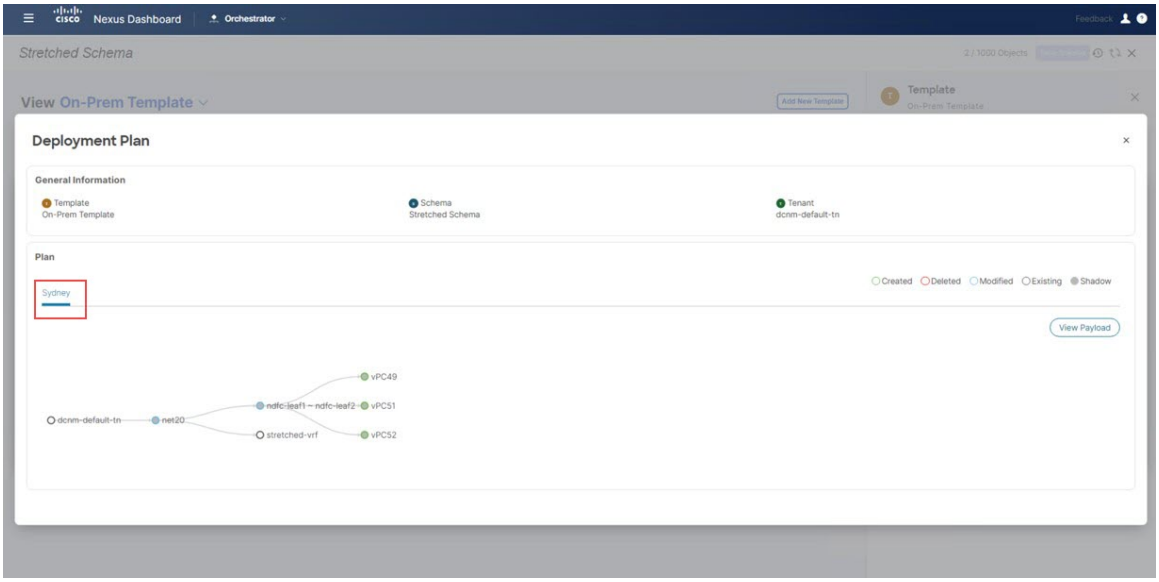
The **Deploy to Sites** window appears, showing the site where the template will be deployed.

Figure 43:



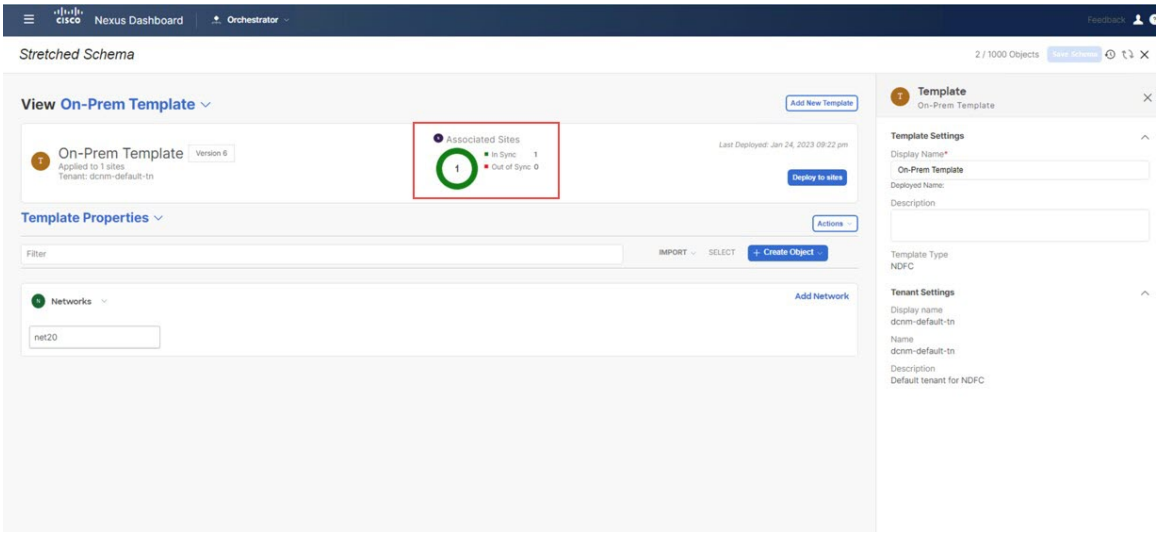
Step 33 Click **Deployment Plan** for additional verification, then click on the on-premises site to see the deployment plan for that specific site.

Figure 44:



Step 34 Click **Deploy** to have NDO push the configurations to NDFC.

Figure 45:



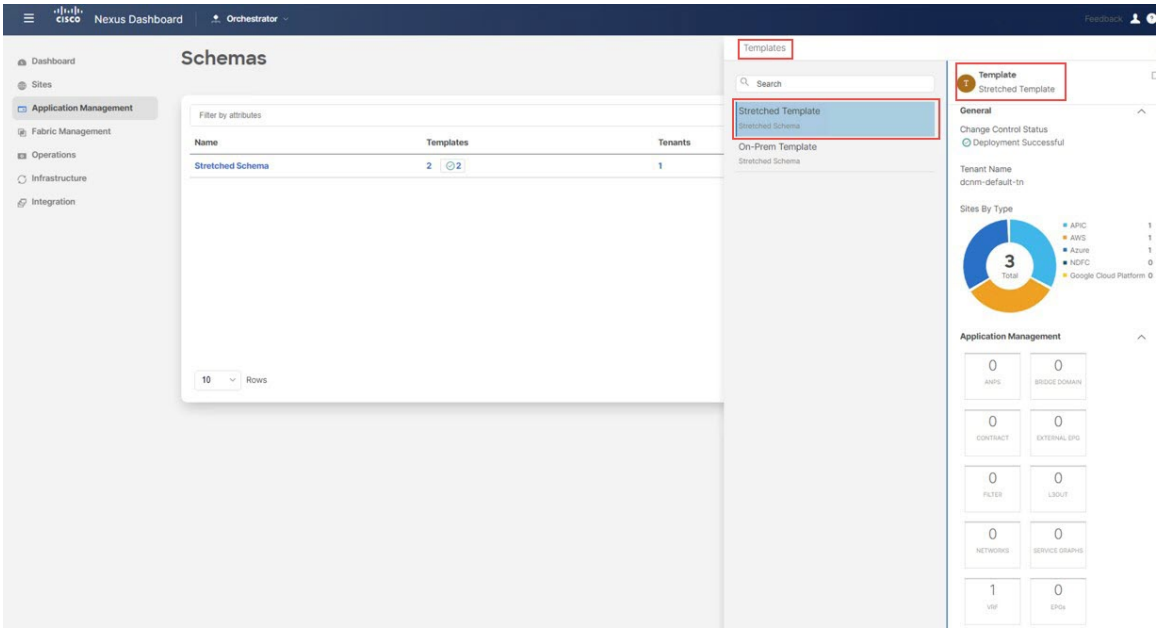
Step 35 Verify that the configurations were deployed successfully.

Note that for each of these verification steps, the exact command that would be used specifically for the configurations in this use case are shown. Replace the appropriate variables in each command based on your configuration.

a) In NDO, verify that the configurations were deployed successfully.

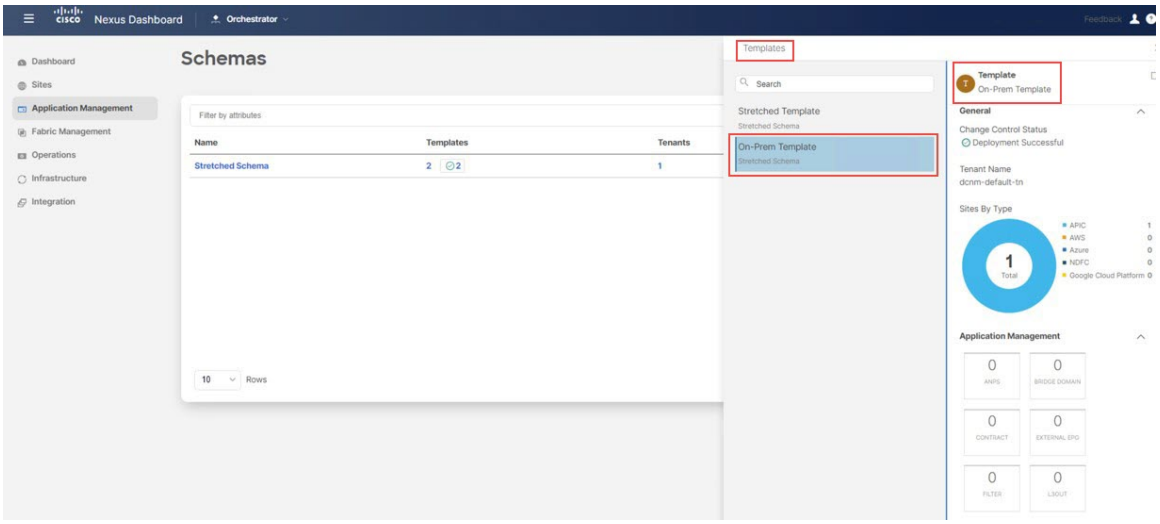
- Verify that the `Stretched Template` was deployed successfully.

Figure 46:



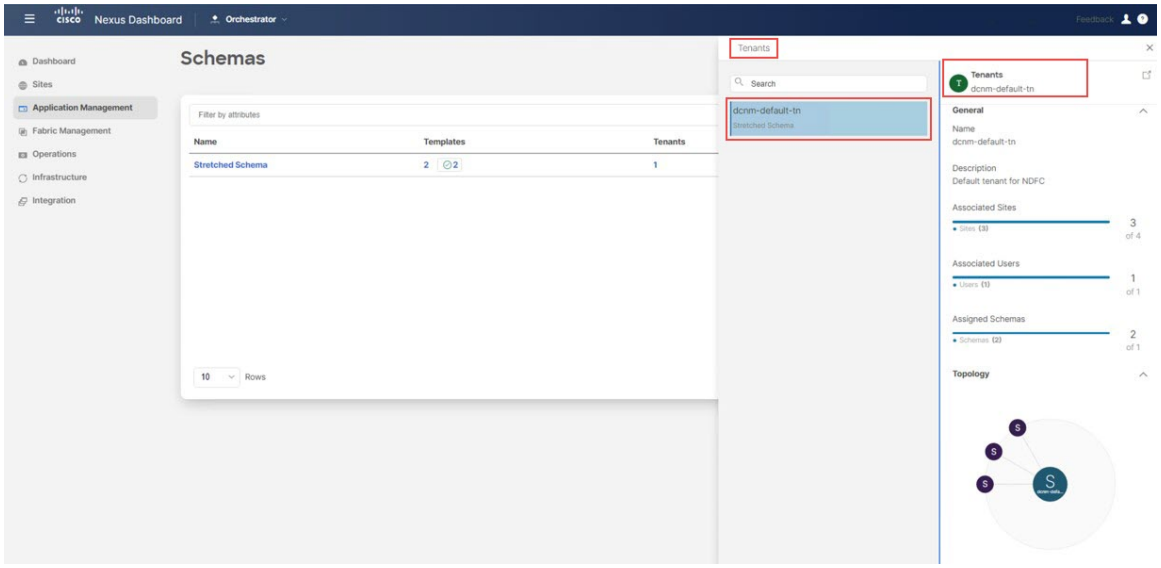
- Verify that the `On-Prem Template` was deployed successfully.

Figure 47:



- Verify that the `dcn-default-tn` tenant was deployed successfully.

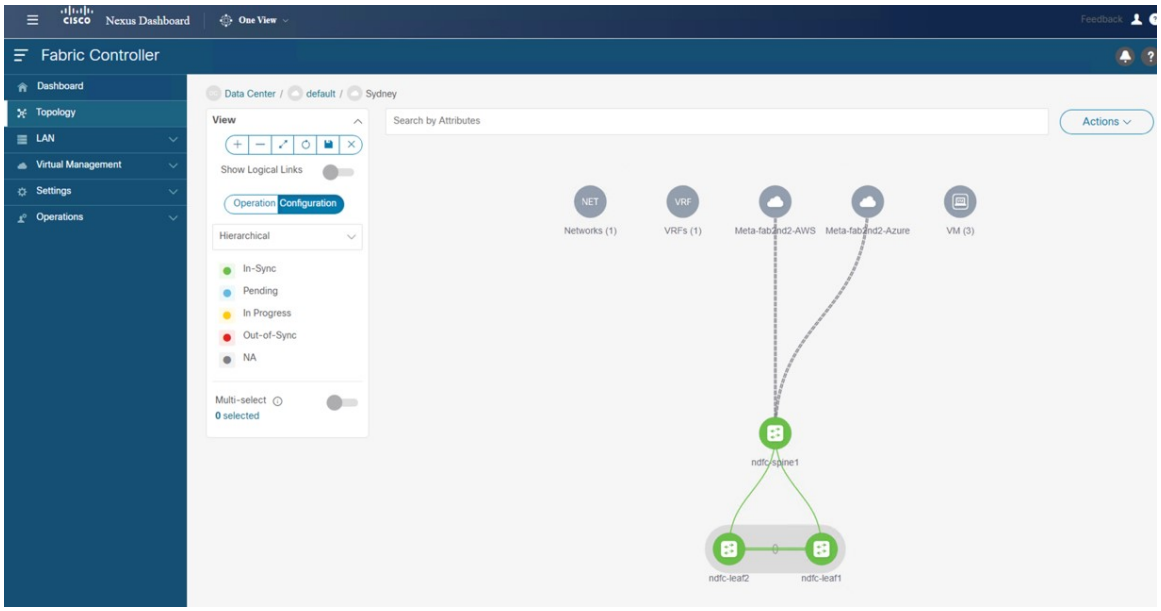
Figure 48:



b) In NDFC, verify that the following were done successfully:

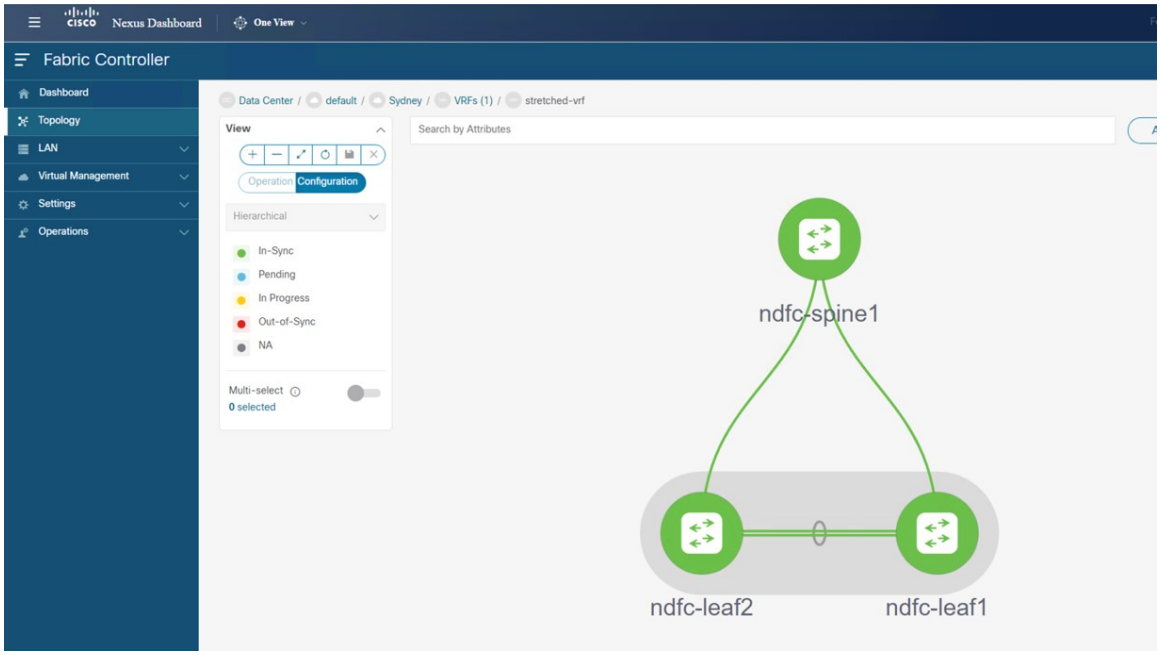
- Verify that one vrf and one network has been created.

Figure 49:



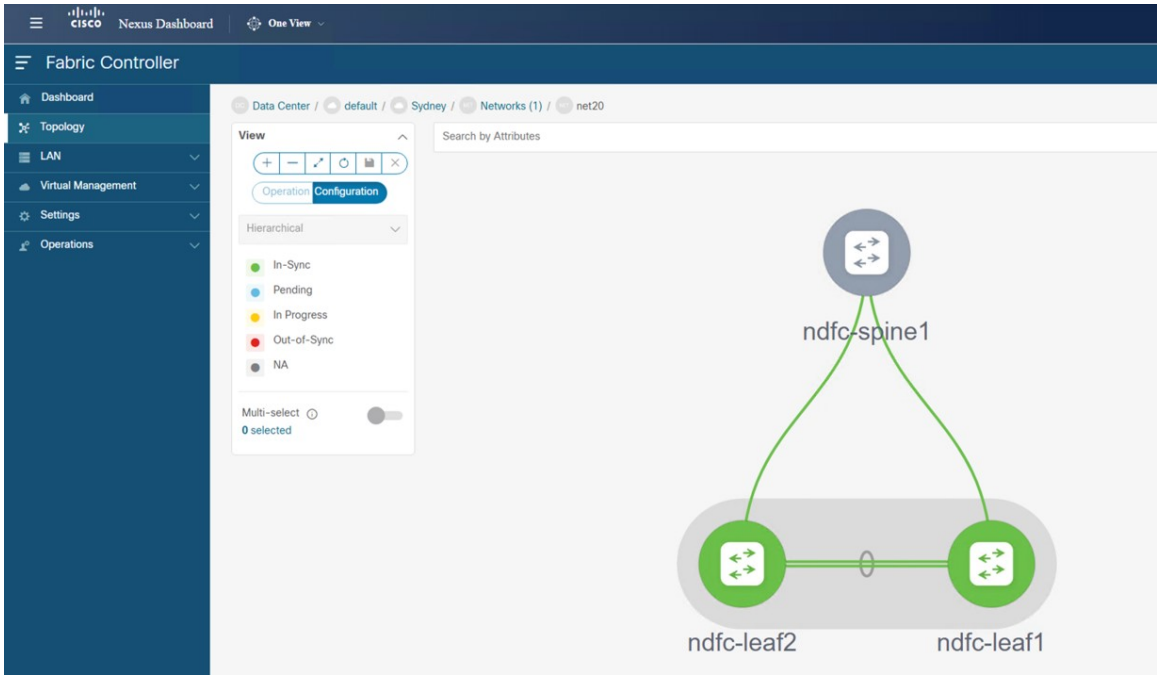
- Verify that the VRF was deployed successfully.

Figure 50:

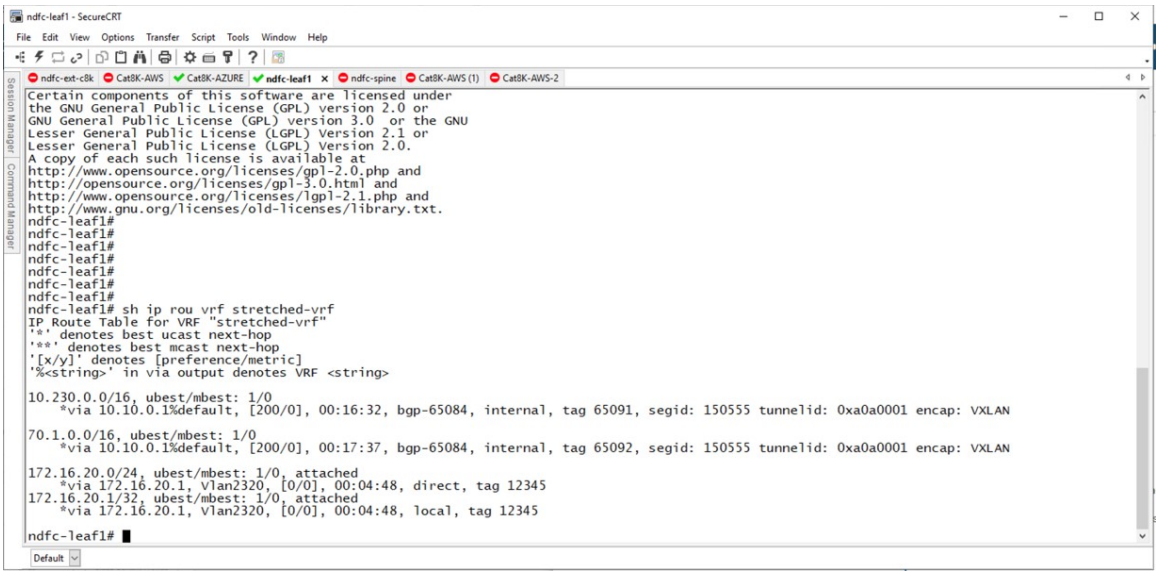


- Verify that the network was deployed successfully.

Figure 51:



c) Enter **sh ip route vrf stretched-vrf** on the on-premises Border Gateway Spine device:

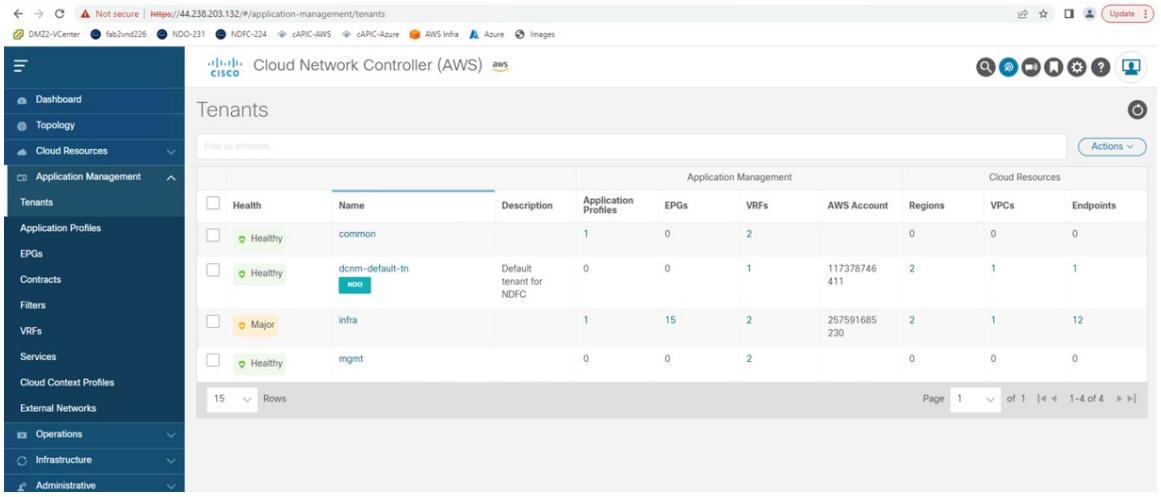


For this use case, using the routing table, you can verify that the NDFC leaf switch can reach out to the following subnets:

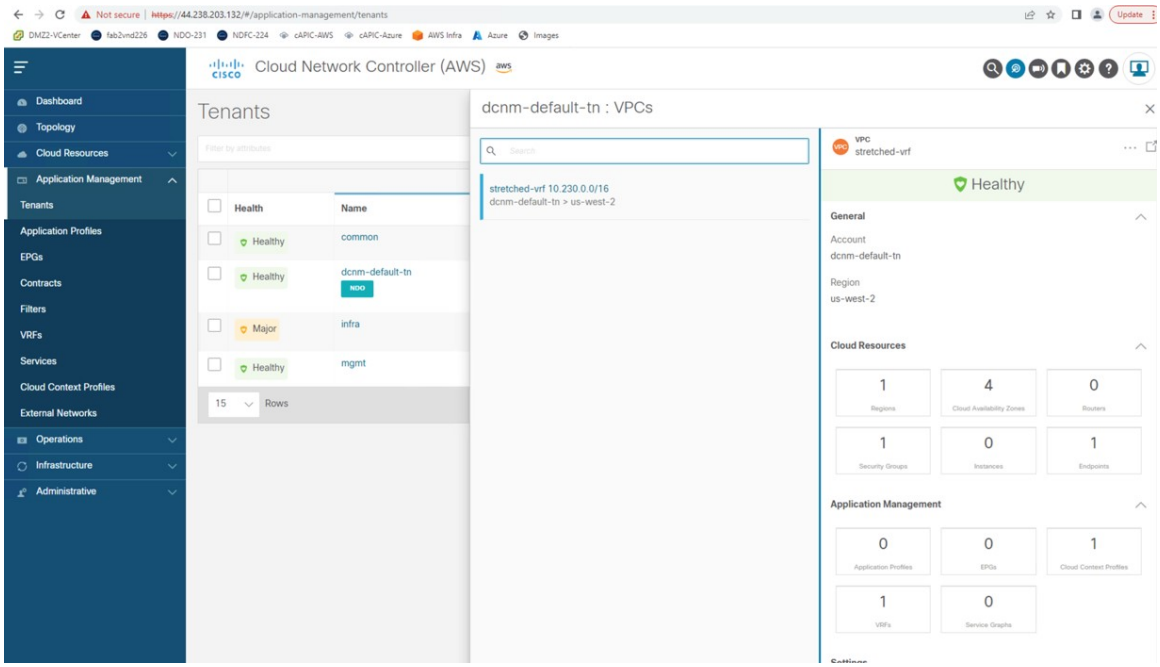
- **AWS**: 10.230.0.0/16
- **Azure**: 70.1.0.0/16

d) Connect to the Cloud Network Controller deployed on AWS and make the following verifications:

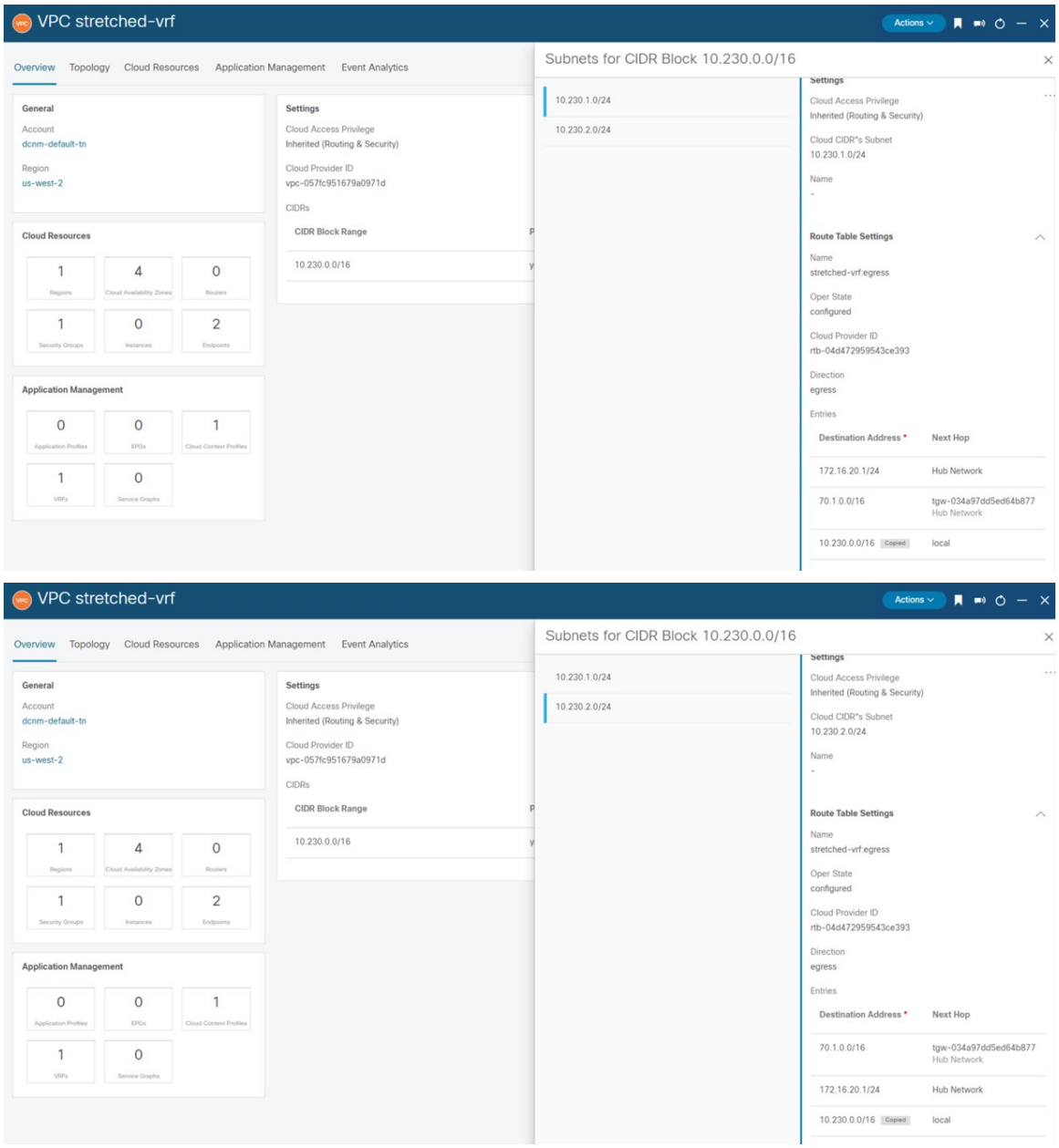
- Verify that the `dcnm-default-tn` tenant is created and one VPC is deployed:



- Verify that the VPC is deployed:

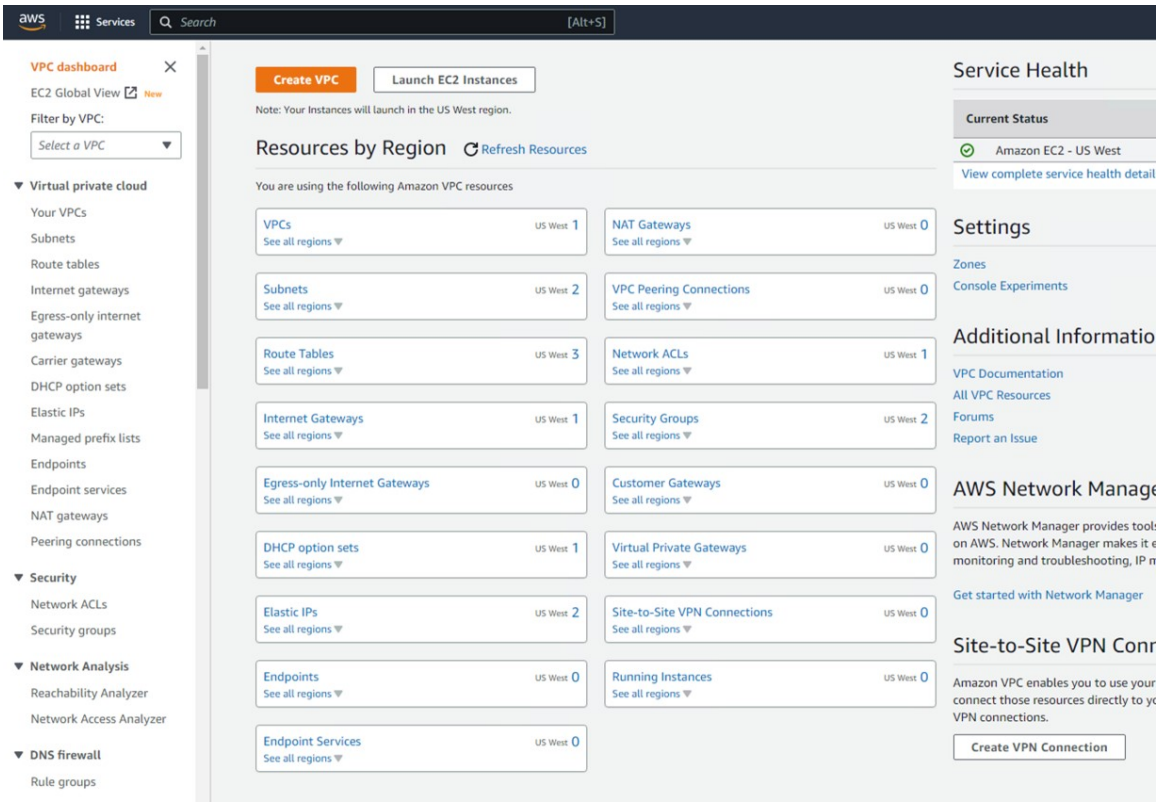


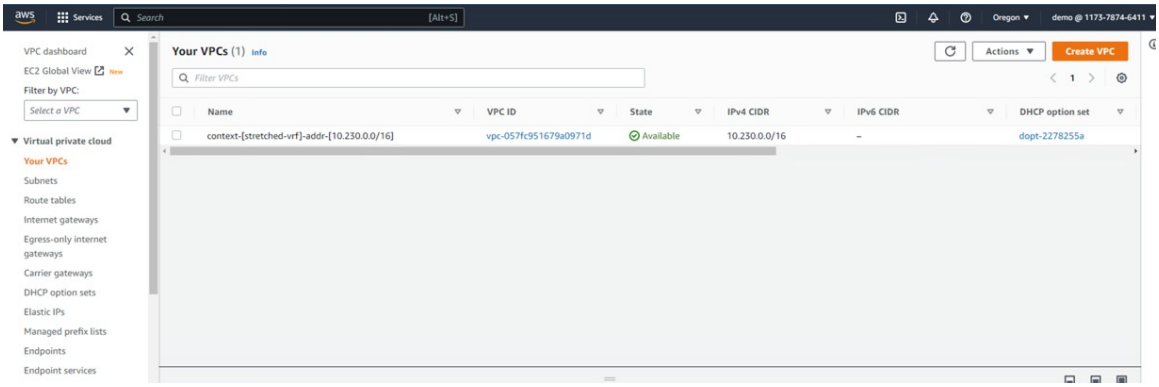
- Using the routing table view from the Cloud Network Controller deployed on AWS, verify that the reachable subnets are:
  - **NDFC**: 172.16.20.0/24
  - **Azure**: 70.1.0.0/16

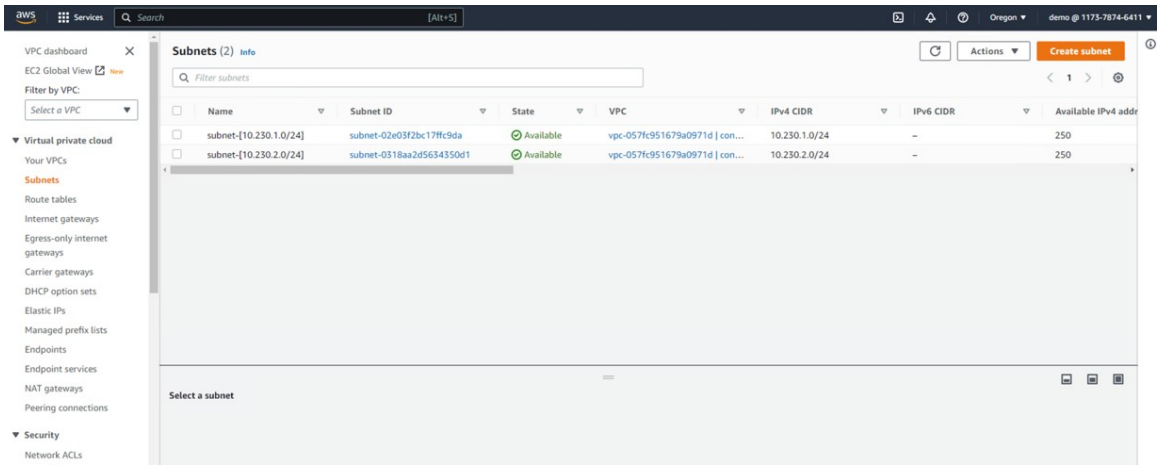


e) In the AWS console, verify the following:

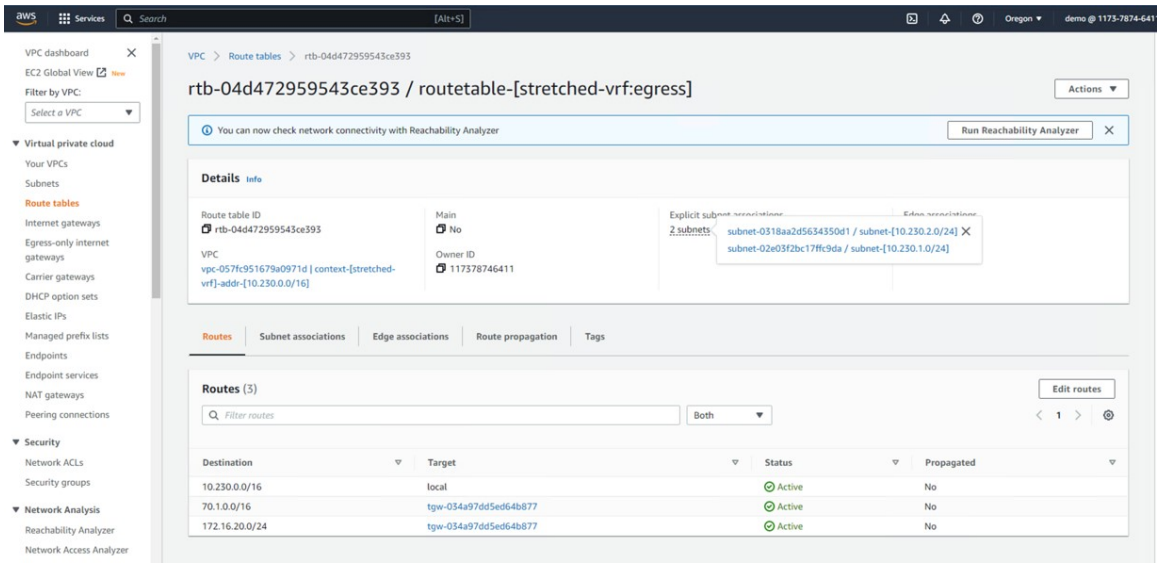
- Verify that you see one VPC and two subnets.


aws
Services
Search
[Alt+S]
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Network Analysis
Reachability Analyzer
Network Access Analyzer
DNS firewall
Rule groups
Create VPC
Launch EC2 Instances
Note: Your Instances will launch in the US West region.
Resources by Region
Refresh Resources
You are using the following Amazon VPC resources
VPCs US West 1 See all regions
NAT Gateways US West 0 See all regions
Subnets US West 2 See all regions
VPC Peering Connections US West 0 See all regions
Route Tables US West 3 See all regions
Network ACLs US West 1 See all regions
Internet Gateways US West 1 See all regions
Security Groups US West 2 See all regions
Egress-only Internet Gateways US West 0 See all regions
Customer Gateways US West 0 See all regions
DHCP option sets US West 1 See all regions
Virtual Private Gateways US West 0 See all regions
Elastic IPs US West 2 See all regions
Site-to-Site VPN Connections US West 0 See all regions
Endpoints US West 0 See all regions
Running Instances US West 0 See all regions
Endpoint Services US West 0 See all regions
Service Health
Current Status
Amazon EC2 - US West
View complete service health detail
Settings
Zones
Console Experiments
Additional Informatio
VPC Documentation
All VPC Resources
Forums
Report an Issue
AWS Network Manage
AWS Network Manager provides tool
on AWS. Network Manager makes it e
monitoring and troubleshooting, IP n
Get started with Network Manager
Site-to-Site VPN Conn
Amazon VPC enables you to use your
connect those resources directly to yo
VPN connections.
Create VPN Connection


aws
Services
Search
[Alt+S]
Oregon
demo @ 1173-7874-6411
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
Your VPCs (1) Info
Filter VPCs
Actions
Create VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
context-[stretched-vrf]-addr-[10.230.0.0/16]
vpc-057fc951679a0971d
Available
10.230.0.0/16
–
dopt-2278255a

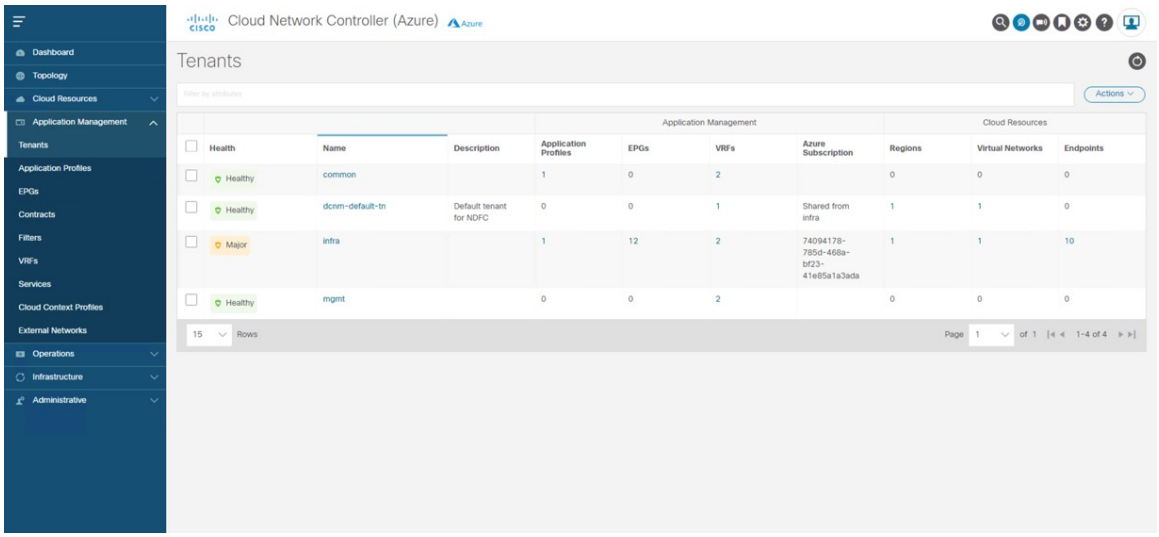


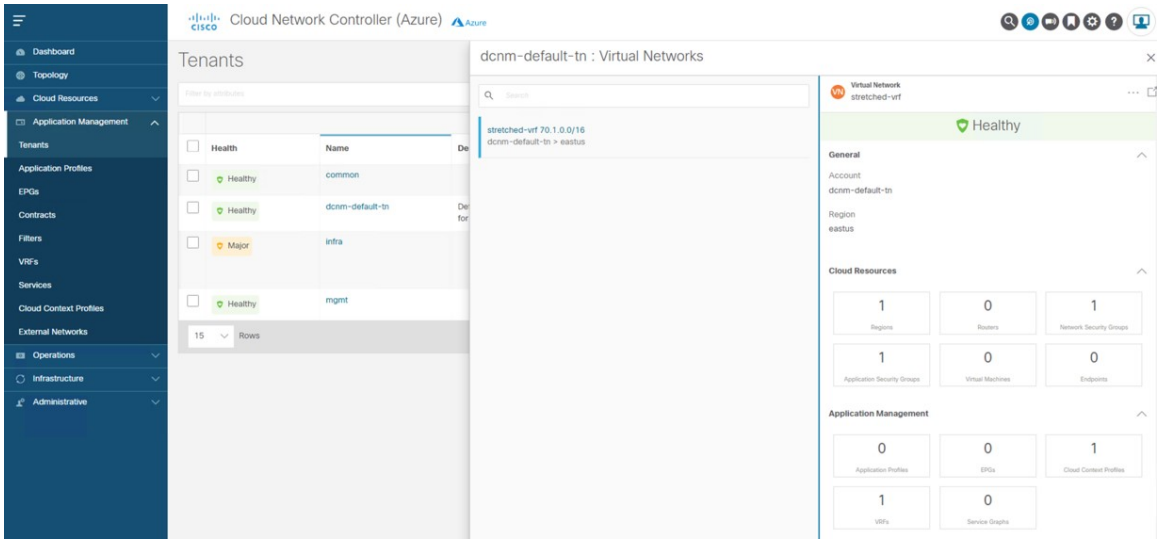
- Verify that you see the routing table.



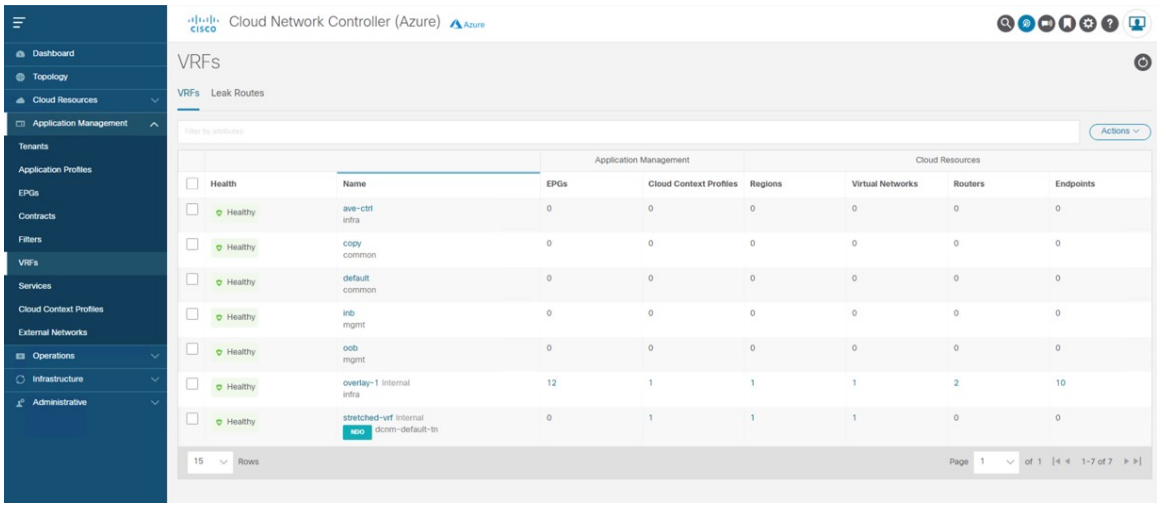
f) Connect to the Cloud Network Controller deployed on Azure and make the following verifications

- Verify that the `dcnm-default-tn` tenant is created:

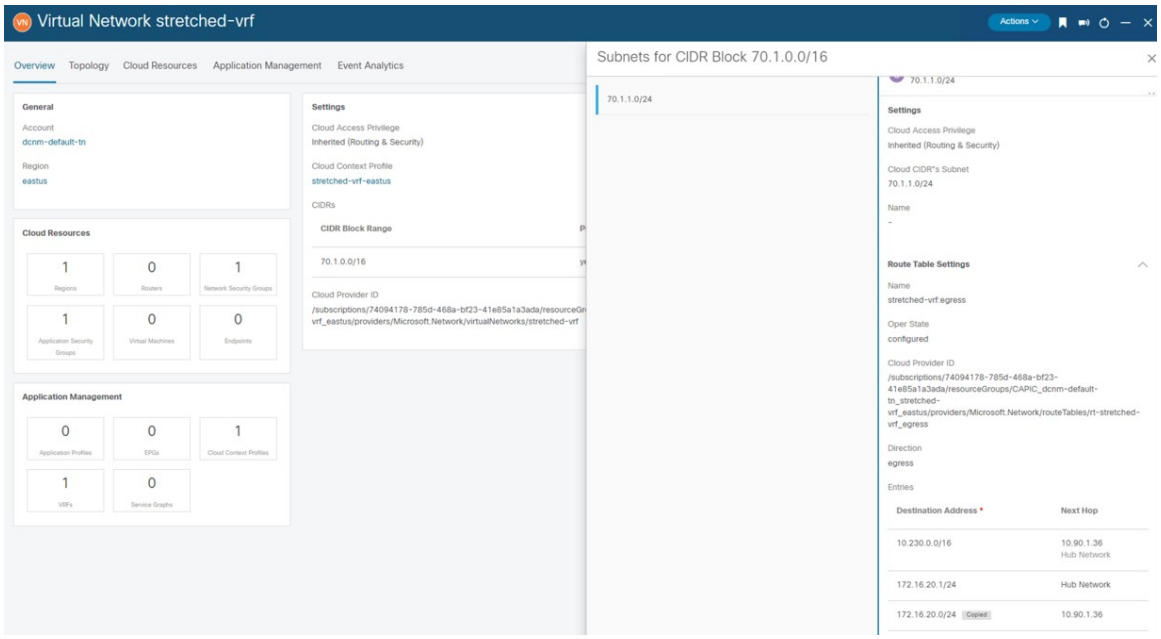




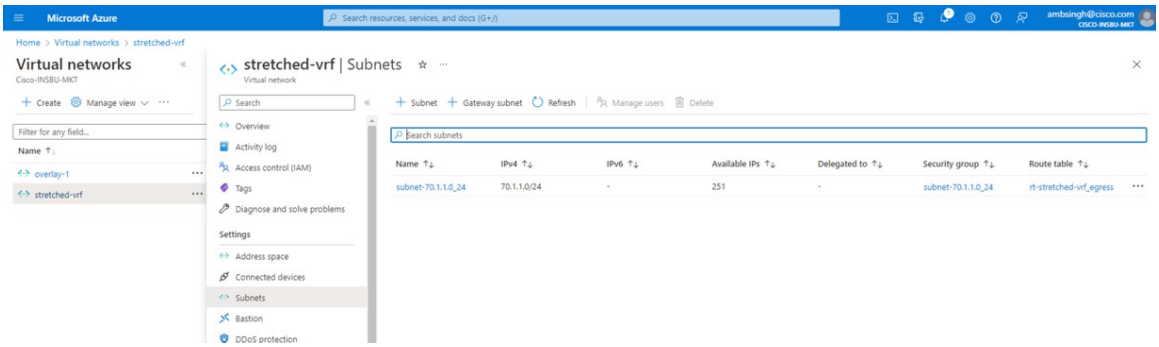
- Verify that the VRF is deployed:



- Using the routing table view from the Cloud Network Controller deployed on AWS, verify that the reachable subnets are:
  - **NDFC**: 172.16.20.0/24
  - **AWS**: 10.230.0.0/16



g) In the Azure console, verify that you can see the subnets:


Microsoft Azure
Search resources, services, and docs (G+/)
ambsingh@cisco.com
CISCO-INSBU-MKT
Home > Virtual networks > stretched-vrf
Virtual networks
Cisco-INSBU-MKT
Create
Manage view
Filter for any field...
Name
overlay-1
stretched-vrf
stretched-vrf | Subnets
Virtual network
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Subnet
Gateway subnet
Refresh
Manage users
Delete
Search subnets
Name
IPv4
IPv6
Available IPs
Delegated to
Security group
Route table
subnet-70.1.1.0_24
70.1.1.0/24
-
251
-
subnet-70.1.1.0_24
rt-stretched-vrf_egress