Global Load-Balancing for VMware Multi-Cloud SDDC Using Avi

VMware Architecture

Table of contents

Global Load-Balancing for VMware Multi-Cloud SDDC Using Avi

Summary

AVI GSLB provides load balancing of applications across multiple geographically dispersed locations (typically, multiple data centers and/or public clouds), while providing centralized configuration, application monitoring, and analytics.

However, most of the AVI GSLB deployments was done for applications hosted in the public-Cloud with Public-IP access (AWS, GCP, Azure or OCI).

This article was created to show that AVI Global load-balancing can be used to load-balance application workloads with Private-IPs, hosted in multiple VMware SDDCs in public-Cloud providers (i.e,. AWS, Google, Azure and Oracle Cloud).

Users attempting to access a particular application will be routed using advanced AVI load-balancing algorithm to a VMware private SDDC.

In this paper, we have two sections. Section 1 will walk-you through the architecture of AVI GSLB for multi-cloud VMware SDDC and Section 2 will walk-you through the implementation of AVI-GSLB multi-cloud architecture in details and explain all the necessary steps required for a successful implementation.

Overview

It is important to start by explaining how AVI GSLB works at a high level, once this is out of the way, I will explain the architecture of the public and private Cloud environments required to implement a successful Multi-Cloud AVI GSLB deployment.

AVI GSLB

AVI GSLB provides load balancing of applications across multiple geographically dispersed locations, while providing centralized configuration, application monitoring, and analytics.

What is GSLB?

Global Server Loading Balancing (GSLB) is the act of balancing an application's load across instances of the application that have been deployed to multiple locations (typically, multiple data centers and/or public clouds). Application load at any one of those locations is usually managed by a "local" load balancer, which could be AVI Vantage or a third-party ADC solution.

GSLB is usually implemented to achieve one or more of the following goals for an application:

- Provide optimal application experience to users/clients who are in geographically distributed areas
- Offer resilience to loss of a data center or a network connection
- Perform non-disruptive migration to or addition of another data center

GSLB High-Level Functionality

To achieve these goals AVI GSLB performs the following functions:

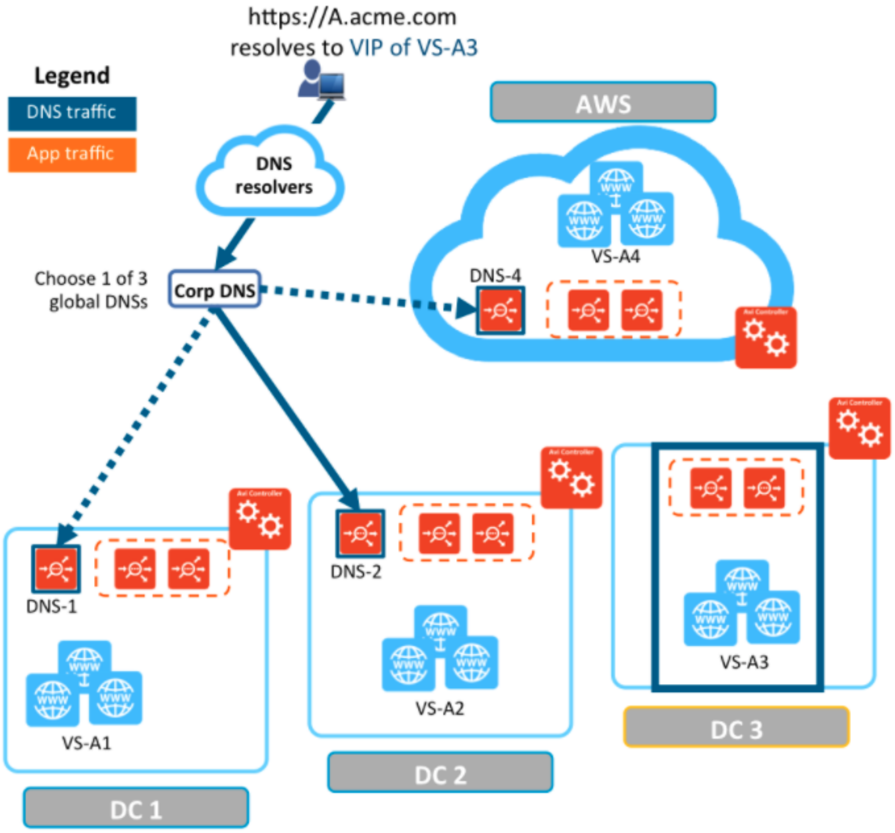
1. It chooses the location (Data Center/Cloud) to which to steer the client's requests
2. It monitors health of the virtual services so that it can choose the best location (i.e., rule out unhealthy ones)
3. It synchronizes configuration and state across GSLB sites, so that #1 and #2 can continue despite certain failures

Functions 2 and 3 are performed by AVI GSLB in a fashion that is totally opaque to end-users. AVI uses the Domain Name System (DNS) for providing the optimal destination information to the user clients. When a client (typically a browser) performs a DNS query on fully qualified domain names (FQDNs), AVI GSLB responds with the IP address (VIP) of the *optimal* application instance. The optimal address can and will change based on the load balancing algorithm, health of the application instances, and the location of the clients.

How AVI GSLB Works

As an example, refer to the setup in the following diagram:

- AVI Vantage is running in four locations (GSLB sites), three on-premises and one in AWS. Each site has its own AVI Controller cluster (represented by a single Controller icon).
- Application "A" has virtual services running in all four locations. These virtual services are identified by VS-A1 through VS-A4.
- Three of the four locations (DC-1, DC-2, and AWS) have global DNS services (DNS-1, DNS-2, and DNS4) that are synchronized. They are all equally authoritative for the subdomain A.acme.com.
- The fourth site (DC3) does not run a global DNS service and therefore can't provide request-steering information.



Now that we understand how AVI GSLB work, we can now apply the same concepts for workloads hosted in VMware SDDCs, however, before diving in, let's first discuss the multi-cloud environment that we will apply this architecture to. For more details, please read the next section.

The VMware Multi-Cloud Lab

The VMware Multi-Cloud Lab is a world class lab connecting multiple Public Cloud providers together.

It is a collection of public cloud platforms and VMware services that are meant to drive multi-cloud and hybrid cloud reference architectures, showcase VMware multi-cloud capabilities in practice and drive innovation via BU collaboration or feedback. Due to the broad range of platforms and services available in the lab, almost any use case or solution is possible, however, we limit the use cases to be focused on multi-cloud or hybrid-cloud. A few examples are below.

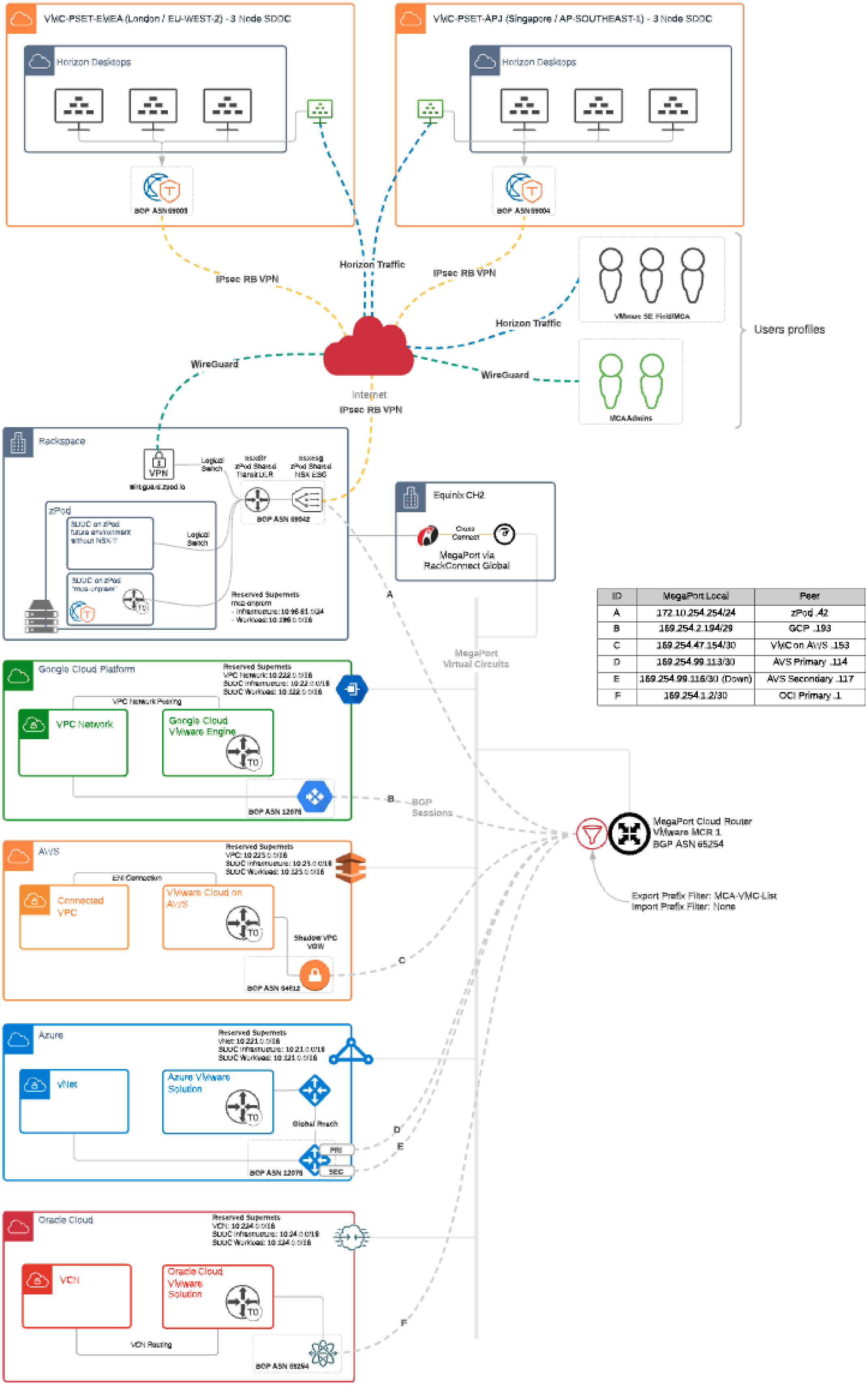
- Deploying or operating Hybrid-Cloud environment (e.g. VMC on AWS on Premises, GCVE + VMC on AWS, AVS + GCVE, etc...)
- Cloud migration (premises to VMware Cloud on AWS)
- Managing a multi-cloud application with Wavefront
- Deploying a multi-cloud application using Tanzu on EC2 and AVS

One of the unique features in the multi-cloud lab is its advanced subnet routing between the different cloud providers, in other words, the lab administrators have granular control of which subnets are permitted between different cloud platforms.

As mentioned above, the VMware multi-cloud lab hosts multiple VMware SDDCs, VMC on AWS, Google Cloud VMware Solution, Azure Cloud VMware Solution and Oracle Cloud VMware Solution. This VMware SDDCs host the VMware Workloads which are used to test AVI GSLB.

Each SDDC has the basic VCF building blocks, vCenter, NSX, HCX, vSAN, ESXi hosts.

The following diagram shows the Multi-Cloud architecture.



ID	MegaPort Local	Peer
A	172.10.254.254/24	zPod .42
B	169.254.2.194/29	GCP .193
C	169.254.47.154/30	VMC on AWS .153
D	169.254.99.113/30	AVS Primary .114
E	169.254.99.116/30 (Down)	AVS Secondary .117
F	169.254.1.2/30	OCI Primary .1

The Multi-Cloud Router (Mega-Port)

If you are wondering how the VMware SDDCs communicating with each other, then it is time to talk about the Mega-Port Router (MCR). However, before explaining the MCR method of operation, it is important to know that you can use multiple different vendors to facilitate the communication between your Cloud SDDCs, the multi-cloud lab is using Mega-Port for this purpose.

MCR Overview

The MCR is a managed virtual router service that establishes Layer 3 connectivity on the worldwide Megaport software-defined network (SDN). MCR instances are preconfigured in data centers in key global routing zones. An MCR enables data transfer between multi-cloud or hybrid cloud networks, network service providers, and cloud service providers.

An MCR instance is not physically cross-connected like a Port in the Megaport network. However, it can host Layer 2 VXC connections just like a physical Port and it can extend to any other Port in the Megaport network or another MCR.

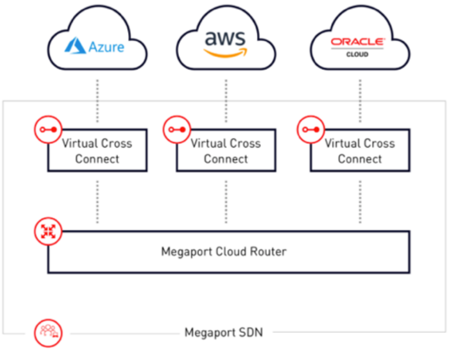
How it works

An MCR joins two or more independent Virtual Cross Connect (VXC) services into a single routing domain, providing connectivity between all the VXCs attached to the MCR.

Without physical infrastructure, you can leverage cloud-to-cloud networking, private peering between leading public Cloud, IaaS, and SaaS providers, and direct connectivity to any provider on the Megaport Software Defined Network (SDN). There is no need to own and maintain equipment. MCR removes the complexity of getting connected at Layer 3 and opens new possibilities for virtualized networking.

You can use an MCR instance either with or without a physical Port in the Megaport network. If you want to configure multi-region deployments with a single cloud service provider (CSP), or a multi-cloud deployment with multiple CSPs, MCR can enable both functionalities. Combining MCR functionality with a physical Port in the Megaport network has added benefits:

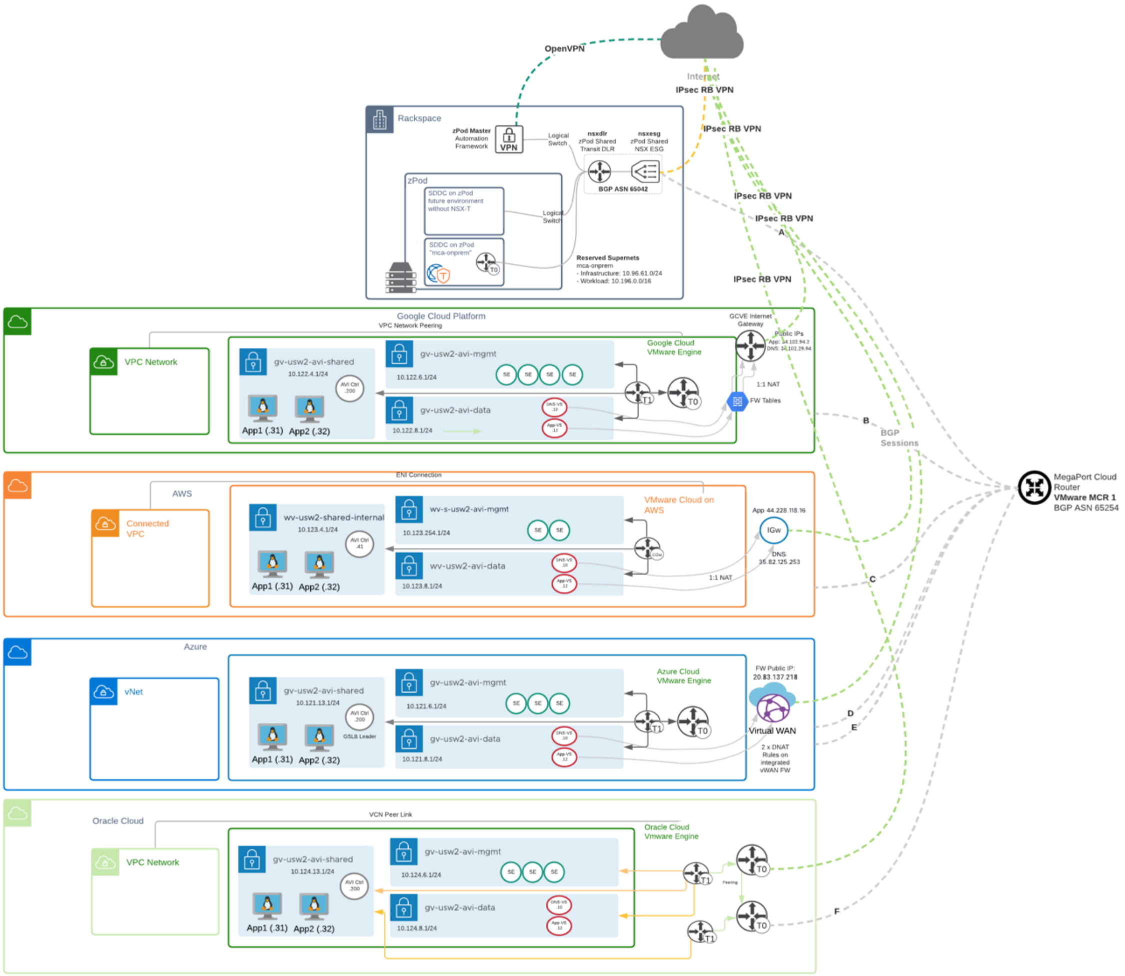
- Reduced latencies by enabling direct connections among cloud providers.
- Inter-region or inter-cloud connectivity to control and localize traffic.



Section 1: AVI-GSLB SDDC Architecture

Before diving into the details, let's start with the following architecture diagram which illustrates a detailed view of the AVI-GSLB multi-cloud architecture.

I will break down the architecture into its basic building blocks in the next few sections of this document.



Each SDDC in the above diagram has few components that build the SDDC architecture, in the next few lines I will share the required components that are used to build the architecture.

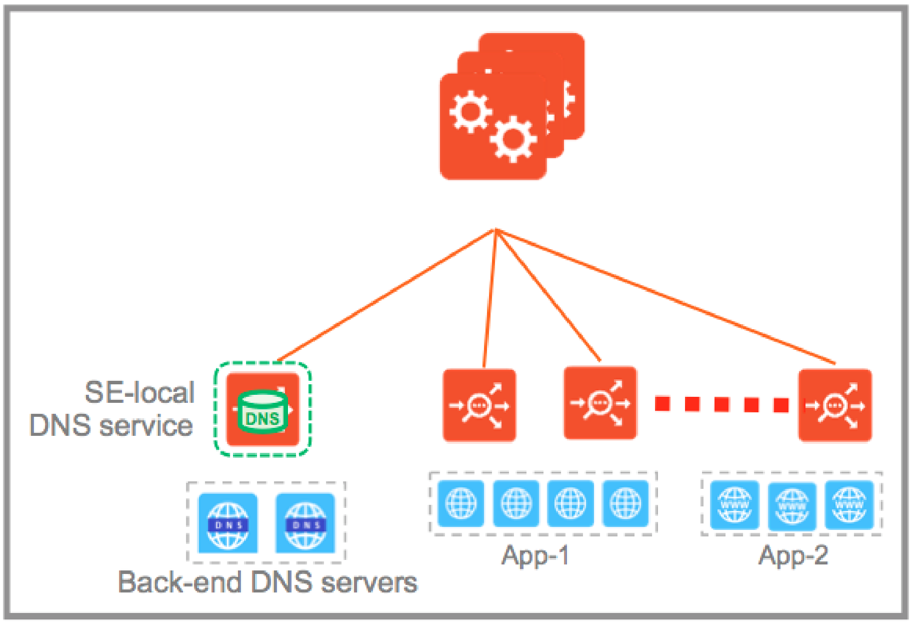
DNS Load Balancing

Let's now dive into the concept of DNS load balancing, this is the concept used by AVI for GSLB.

Avi Service Engines proxy DNS requests to a back-end pool of DNS servers. A virtual service with a System-DNS (or similar) application profile is defined as usual. For this, a pool of back-end servers loaded with DNS software packages must be assigned.

Avi DNS runs a virtual service with System-DNS application profile type and a network profile using per-packet load balancing.

Referring to the diagram below, a DNS service — represented in green— is hosted on the leftmost Service Engine. The DNS virtual service responds to DNS queries if there is a matching entry. If a matching entry is not found and if pool members are configured, the DNS virtual service forwards the request to the back-end DNS pool servers (represented in blue).

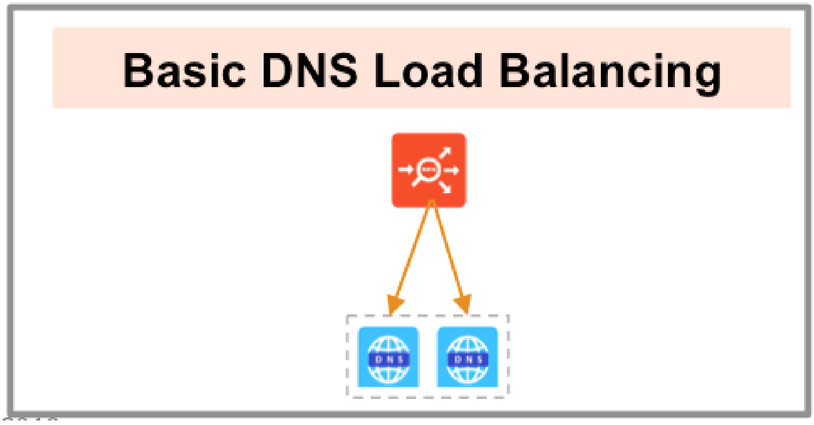


An Avi DNS virtual service can act as an authoritative DNS server for one or more subdomains (zones) and all analytics and client logs are supported.

Deployment Scenario – Authoritative Name Server for Subdomain (Zone)

In this scenario, the corporate name server delegates one or more subdomains to the Avi DNS service, which in turn acts as an authoritative DNS server for them. In the example shown below, avi.mcsa.cloud and mcsa.cloud are the subdomains. Typically, the corporate name server will have a NS record pointing to the Avi DNS service. Client queries for these subdomains are sent directly to Avi Vantage, whereas all DNS requests outside of mcsa.cloud are instead sent to the external ".cloud" name server.

For load balancing to work, the corporate DNS servers are pooled together and exposed by an Avi SE group as a single, scaled DNS service



All clients queries for the subdomains that are sent directly to AVI Vantage are NAT'd at each Cloud provider edge (AWS, GCP, Azure & OCI) and forwarded to DNS Virtual Service inside each VMware SDDC.

Now, let's apply this load-balancing concept to a multi-Cloud architecture, however, let me walk you through the building block of the architecture for each SDDC.

The building blocks of the Multi-Cloud Architecture

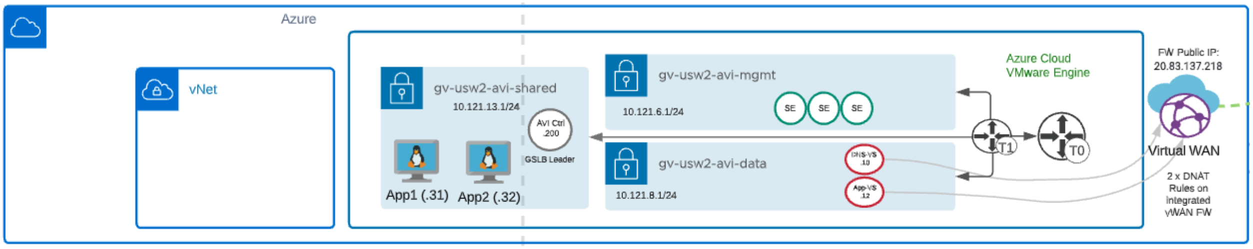
If you look deeply into the architecture diagram at the beginning of section 1, you will notice some common components in each SDDC, you will also notice some differences as well, let's discuss this in more details in the next section.

Azure VMware Solution building Blocks:

- VMware SDDC - AVS

- vCenter
- vSAN
- NSX
  - Management Network for AVI Service Engine Management – wv-s-usw2-avi-mgmt (10.121.6.1/24)
  - Data Network for AVI Virtual Services (DNS and Application VIPs) – wv-usw2-avi-data (10.121.8.1/24)
  - Shared Network for AVI Controller and application hosts – wv-usw2-shared-internal (10.121.13.1/24)
- HCX for workload mobility – Not a requirement for AVI GSLB
- AVI Controller – GSLB Leader – 10.121.13.200
- AVI Service Engines
- AVI Virtual Service
  - DNS-VS – 10.121.8.1.10
  - Application-VS – 10.121.8.12
- Two copies of an application running on two different ESXi hosts.
  - App1 – 10.121.13.31
  - App2 – 10.121.13.32

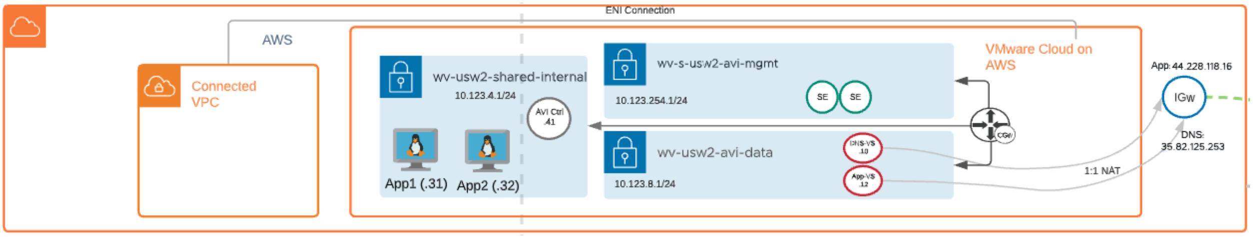
- Azure
  - Azure vWAN** - Please refer to future work section for more details.
  - Azure Firewall
    - Azure Firewall Manager
      - Firewall Tables
    - Destination NAT
  - Azure Internet Gateway
  - Azure VPC
  - Azure Public IP Address (20.83.137.218)
- Global DNS Configuration – Route53 - http://global.demoavi.mcsa.cloud/



VMware Cloud on AWS:

- VMware SDDC - VMC
  - vCenter
  - vSAN
  - VMC Networking and Security
    - Segments
      - Management Network for AVI Service Engine Management – wv-s-usw2-avi-mgmt (10.123.254.1/24)
      - Data Network for AVI Virtual Services (DNS and Application VIPs) – wv-usw2-avi-data (10.123.8.1/24)
      - Shared Network for AVI Controller and application hosts – wv-usw2-shared-internal (10.123.4.1/24)
    - Public IPs
      - AVI-Public-App-Traffic – 44.228.118.16
      - AVI-GSLB-DNS-Load-Balancing – 35.82.125.253

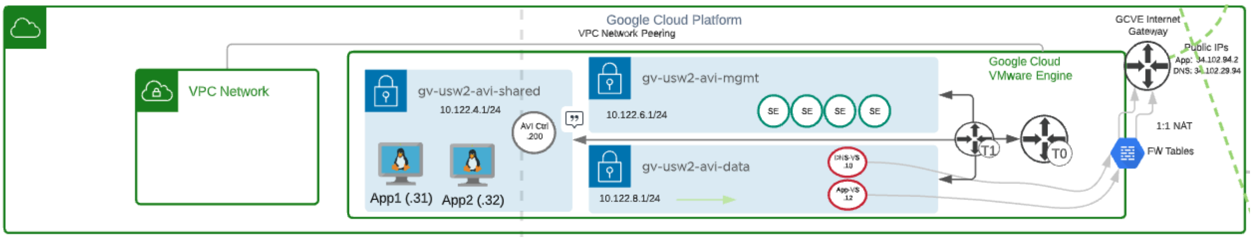
        - Security – Gateway Firewall
            - AVI-DNS-Inbound – Allow traffic to AVI-DNS-VS for the following services (ICMP, DNS-UDP and DNS)
            - Internet Inbound – Allow internet inbound traffic for AVI-DNS-VS and Applications. Use Inventory Group configuration for better management of traffic.
    - HCX for Workload mobility – Not a requirement for AVI GSLB
    - AVI Controller – 10.123.4.41
    - AVI Service Engines
    - AVI Virtual Service
        - DNS-VS – 10.123.8.1.10
        - Application-VS – 10.123.8.12
    - Two copies of an application running on two different ESXi hosts.
        - App1 – 10.123.4.31
        - App2 – 10.123.4.32
- AWS
    - Route53 for DNS management – Applies for all clouds.
- Global DNS Configuration – Route53 - http://global.demoavi.mcsa.cloud/



Google Cloud VMware Solution:

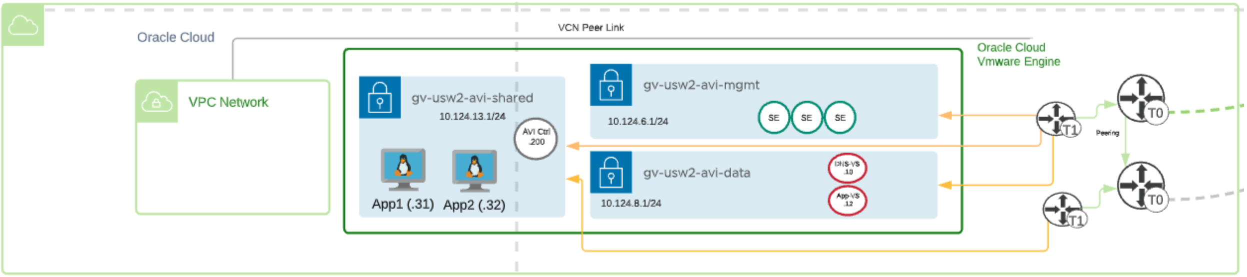
- VMware SDDC - GCVE
    - vCenter
    - vSAN
    - NSX
        - Management Network for AVI Service Engine Management – gv-usw2-avi-mgmt (10.122.6.1/24)
        - Data Network for AVI Virtual Services (DNS and Application VIPs) – gv-usw2-avi-data (10.122.8.1/24)
        - Shared Network for AVI Controller and application hosts – gv-usw2-shared-internal (10.122.4.1/24)
    - HCX for workload mobility – Not a requirement for AVI GSLB
    - AVI Controller – 10.122.4.200
    - AVI Service Engines
    - AVI Virtual Service
        - DNS-VS – 10.122.8.1.10
        - Application-VS – 10.122.8.12
    - Two copies of an application running on two different ESXi hosts.
        - App1 – 10.122.4.31
        - App2 – 10.122.4.32
    - GCvE internal Internet Gateway**
    - Public IPs
        - Avi-app-public-ip – 34.102.94.2 (Google cloud does 1:1 Natting by default for public IPs to a private SDDC IP – 10.122.8.12 for application VIP)

        - Avi-dns-ip – 34.102.29.94 (Nat'd to 10.122.8.10)
    - Firewall Tables
        - Allow inbound TCP traffic to AVI from any source to 34.102.94.2/32 for Ports 443 and 80
        - Allow inbound UDP traffic from any source to 34.102.29.94/32 for all ports
- Google Cloud
    - Google Cloud VPC
- Global DNS Configuration – Route53 - http://global.demoavi.mcsa.cloud/



Oracle Cloud VMware Solution:

- VMware SDDC - OCVS
    - vCenter
    - vSAN
    - NSX
        - Management Network for AVI Service Engine Management – gv-usw2-avi-mgmt (10.124.6.1/24)
        - Data Network for AVI Virtual Services (DNS and Application VIPs) – gv-usw2-avi-data (10.124.8.1/24)
        - Shared Network for AVI Controller and application hosts – gv-usw2-shared-internal (10.124.13.1/24)
    - HCX for workload mobility – Not a requirement for AVI GSLB
    - AVI Controller – 10.124.13.200
    - AVI Service Engines
    - AVI Virtual Service
        - DNS-VS – 10.124.8.1.10
        - Application-VS – 10.124.8.12
    - Two copies of an application running on two different ESXi hosts.
        - App1 – 10.124.13.31
        - App2 – 10.124.13.32
    - Public IPs – WiP for this section
- Oracle Cloud – WiP for this section
- Global DNS Configuration – Route53 - http://global.demoavi.mcsa.cloud/



Section 2: AVI-GSLB SDDC Configuration Guide

Deploy AVI-GSLB on Azure Cloud VMware Solution

Before deploying AVI-GSLB we must fully deploy an AVI Controller and AVI Service Engines on AVS. The process of deploying AVI is straightforward and similar a typical AVI deployment on vSphere, I will walk you through the process once in this section and highlight any additional requirements on future sections.

The deployment architecture is discussed in an earlier section on this document, please reference it for more information.

Prerequisites

Role Requirement

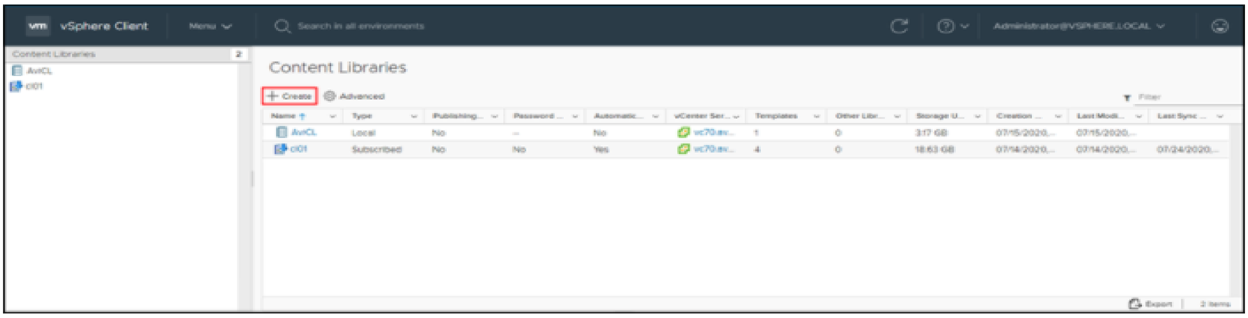
The AVI Controller requires:

- The NSX Network Engineer role or higher
- VMware vCenter Permissions as defined in Roles and Permissions for vCenter and NSX-T Users (https://avinetworks.com/docs/latest/roles-and-permissions-for-vcenter-nsx-t-users/)
- You can use the cloudadmin user and credential provided for AVS. This user has a role which is a superset of the required permissions and is sufficient for the integration.

Content Library

The AVI Controller uploads the Service Engine image to the content library on the vCenter server and uses this to create new virtual machine (VM) every time a new Service Engine is required. The content library must be created on vCenter before configuring the NSX-T cloud. In the vCenter vSphere client:

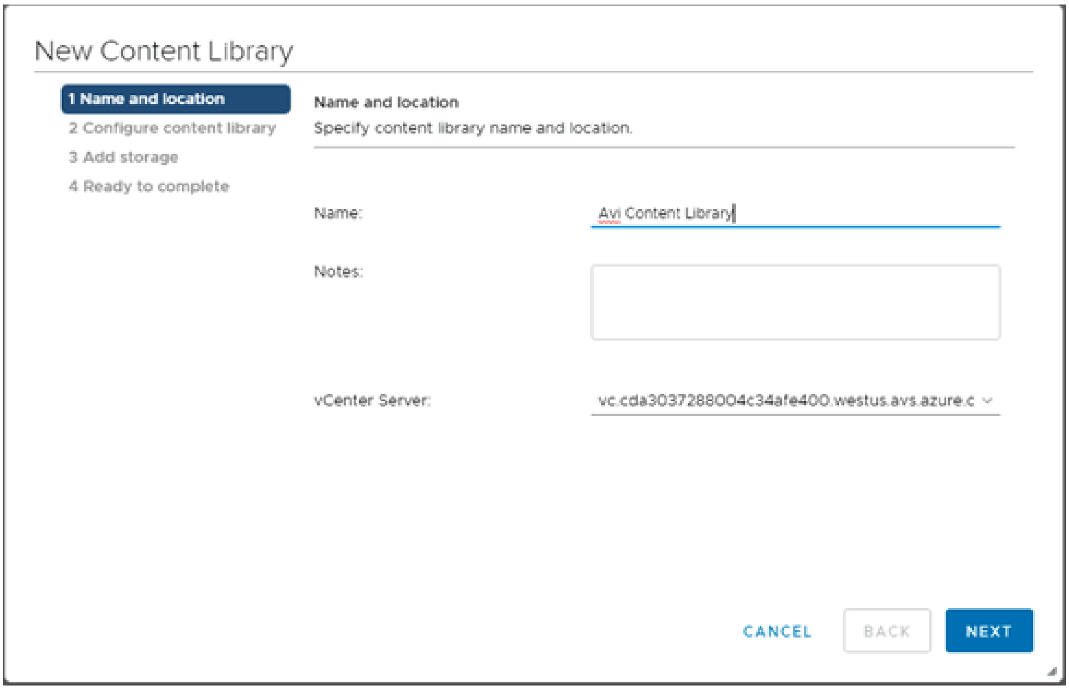
1. Navigate to **Content Libraries**.
2. Click on **Create**.



Content Libraries

Name	Type	Publishing...	Password ...	Automatic...	vCenter Ser...	Templates	Other Libr...	Storage U...	Creation ...	Last Modi...	Last Sync ...
AviCL	Local	No	--	No	vc70.av...	1	0	3.17 GB	07/15/2020,...	07/15/2020,...	
cl01	Subscribed	No	No	Yes	vc70.av...	4	0	18.63 GB	07/14/2020,...	07/14/2020,...	07/24/2020,...

3. The New Content Library wizard opens. In the Name and location page, enter the Name and select a vCenter Server instance for the content library as shown below:



New Content Library

1 Name and location
2 Configure content library
3 Add storage
4 Ready to complete

Name and location

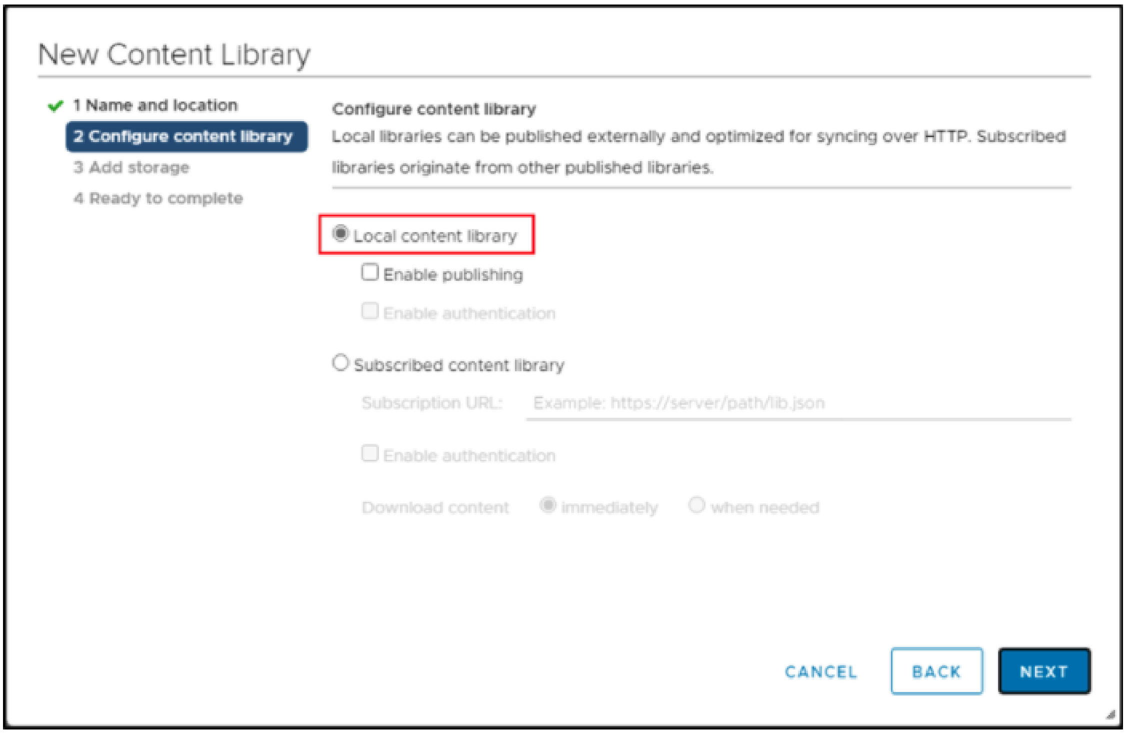
Specify content library name and location.

Name: Avi Content Library

Notes:

vCenter Server: vc.cda3037288004c34afe400.westus.avs.azure.c

4. Click on **Next**.
5. In the **Configure content library page, select Local content library**.



New Content Library

✓ 1 Name and location
2 Configure content library
3 Add storage
4 Ready to complete

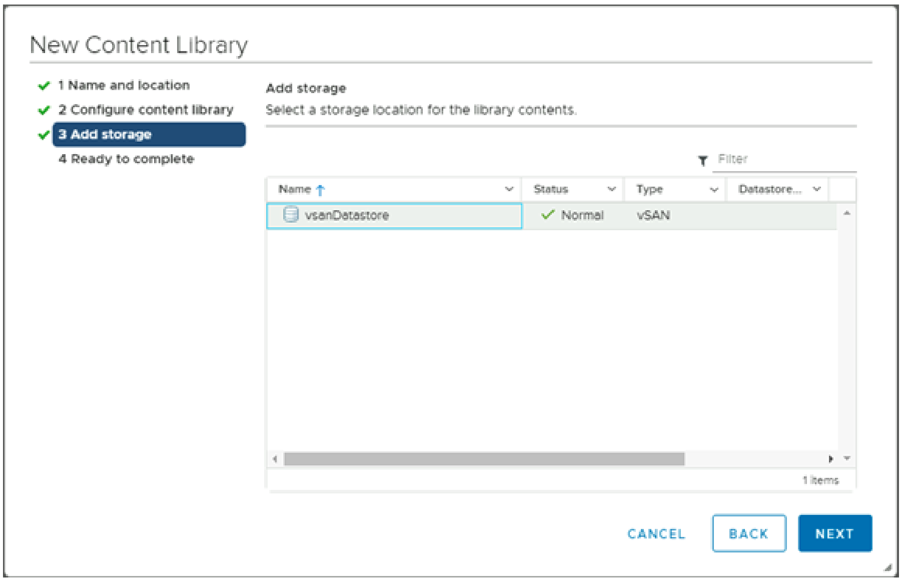
Configure content library

Local libraries can be published externally and optimized for syncing over HTTP. Subscribed libraries originate from other published libraries.

● Local content library
□ Enable publishing
□ Enable authentication

○ Subscribed content library
Subscription URL: Example: https://server/path/lib.json
□ Enable authentication
Download content ● immediately ○ when needed

6. Click on **Next**.
7. In the **Add storage** page, select a datastorage location for the contents of the content library.



New Content Library

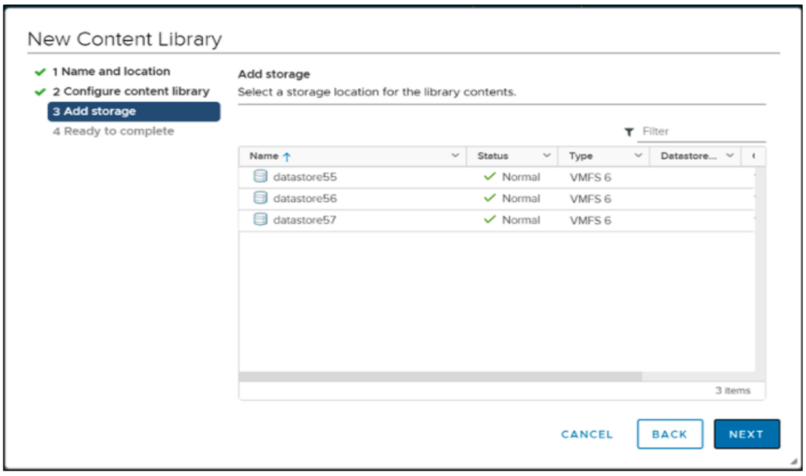
- ✓ 1 Name and location
- ✓ 2 Configure content library
- ✓ 3 Add storage
- 4 Ready to complete

Add storage

Select a storage location for the library contents.

Name ↑	Status	Type	Datastore...
vsanDatastore	✓ Normal	vSAN	

1 items



New Content Library

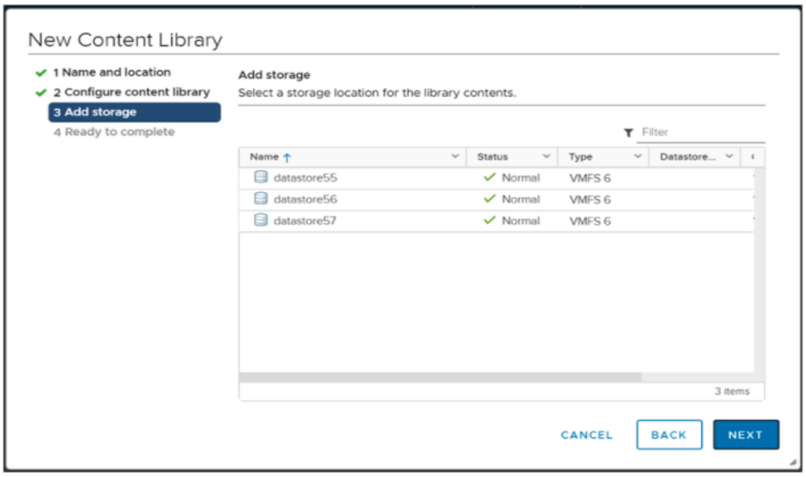
- ✓ 1 Name and location
- ✓ 2 Configure content library
- 3 Add storage
- 4 Ready to complete

Add storage

Select a storage location for the library contents.

Name ↑	Status	Type	Datastore...
datastore55	✓ Normal	VMFS 6	
datastore56	✓ Normal	VMFS 6	
datastore57	✓ Normal	VMFS 6	

3 items



New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library
- 3 Add storage
- 4 Ready to complete

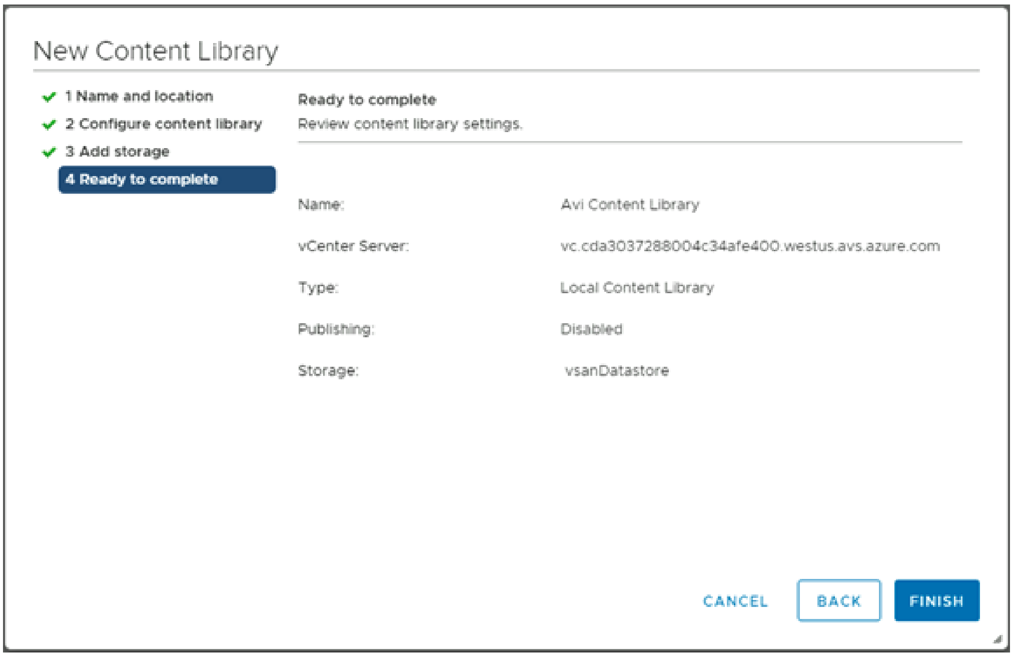
Add storage

Select a storage location for the library contents.

Name ↑	Status	Type	Datastore...
datastore55	✓ Normal	VMFS 6	
datastore56	✓ Normal	VMFS 6	
datastore57	✓ Normal	VMFS 6	

3 items

8. Click on **Next**.
9. In the **Ready to complete page**, review the details.



New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library
- ✓ 3 Add storage
- 4 Ready to complete

Ready to complete
Review content library settings.

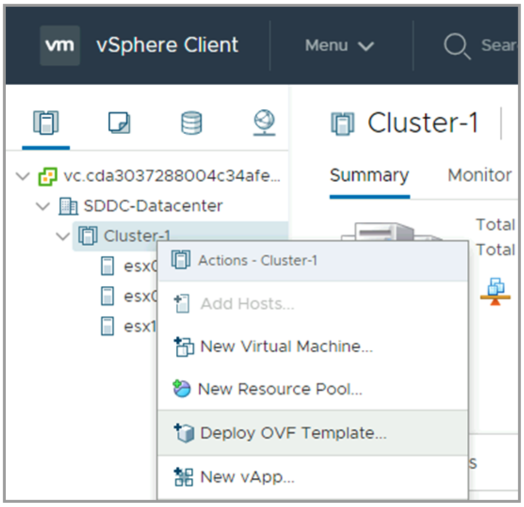
Name:	Avi Content Library
vCenter Server:	vc.cda3037288004c34afe400.westus.avs.azure.com
Type:	Local Content Library
Publishing:	Disabled
Storage:	vsanDatastore

10. Click on **Finish**.

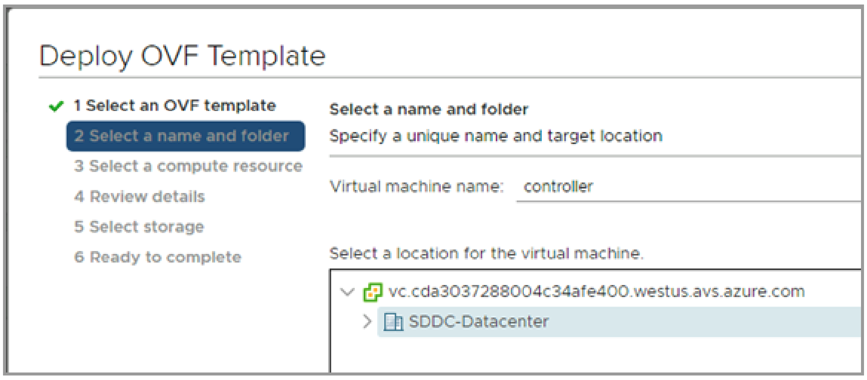
Deploying the AVI Controller OVA

To deploy the AVI Controller OVA:

1. Login to the vCenter server through a vCenter client, using the fully qualified domain name (FQDN).
2. From the **File** menu, select **Deploy OVF Template**.



3. Select the controller.ova file from your local machine.
4. In the **Deploy OVF Template** wizard, select the VM name and the location to deploy.



Deploy OVF Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

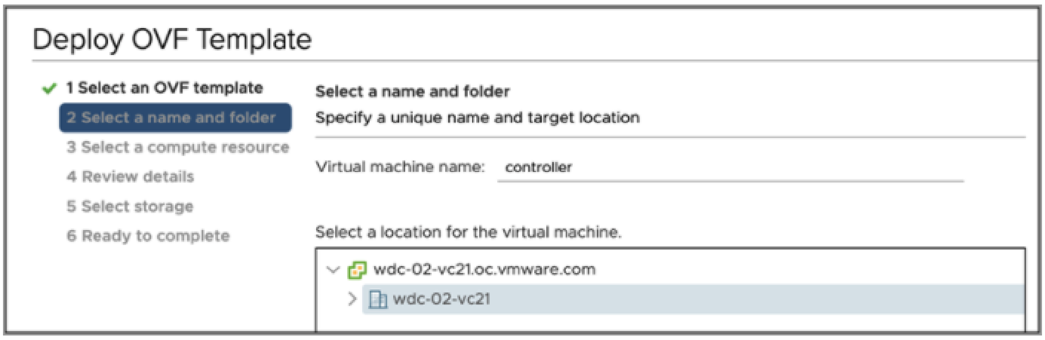
Select a name and folder

Specify a unique name and target location

Virtual machine name: controller

Select a location for the virtual machine.

vc.cda3037288004c34afe400.westus.avs.azure.com
SDDC-Datacenter



Deploy OVF Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

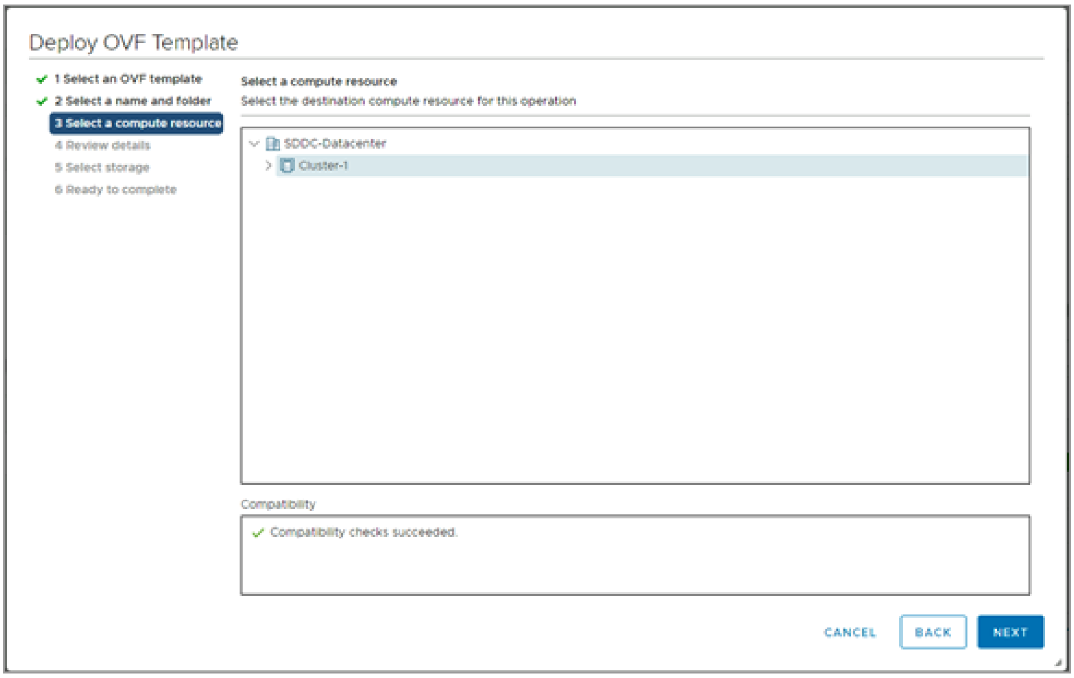
Specify a unique name and target location

Virtual machine name: controller

Select a location for the virtual machine.

wdc-02-vc21.oc.vmware.com
wdc-02-vc21

5. Select the compute resource.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource

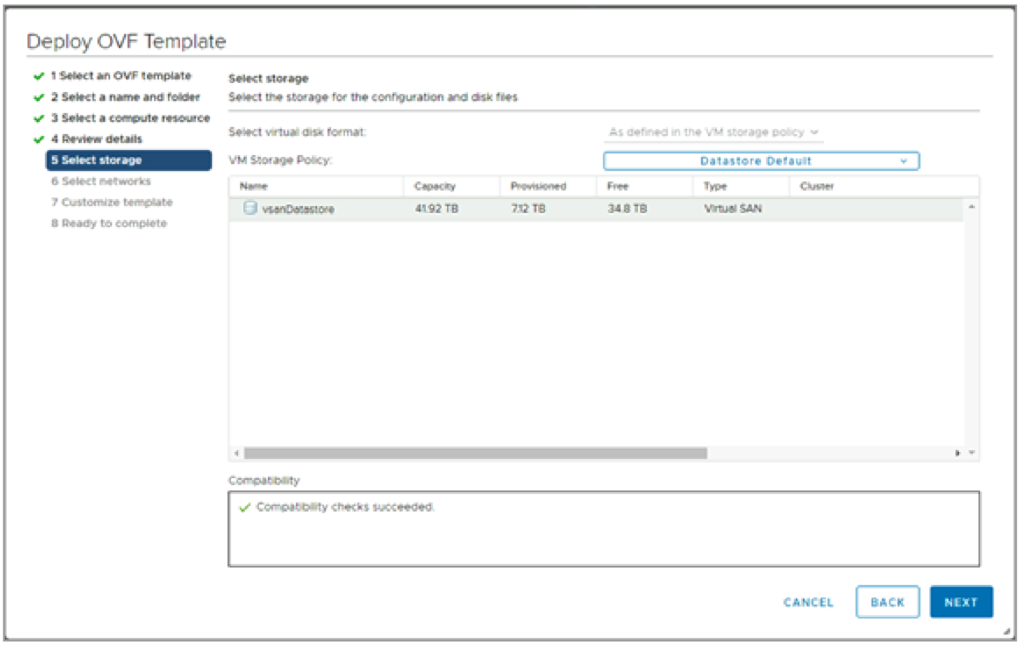
Select the destination compute resource for this operation

SDDC-Datacenter
Cluster-1

Compatibility

✓ Compatibility checks succeeded.

6. Review the details.
7. Select storage.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

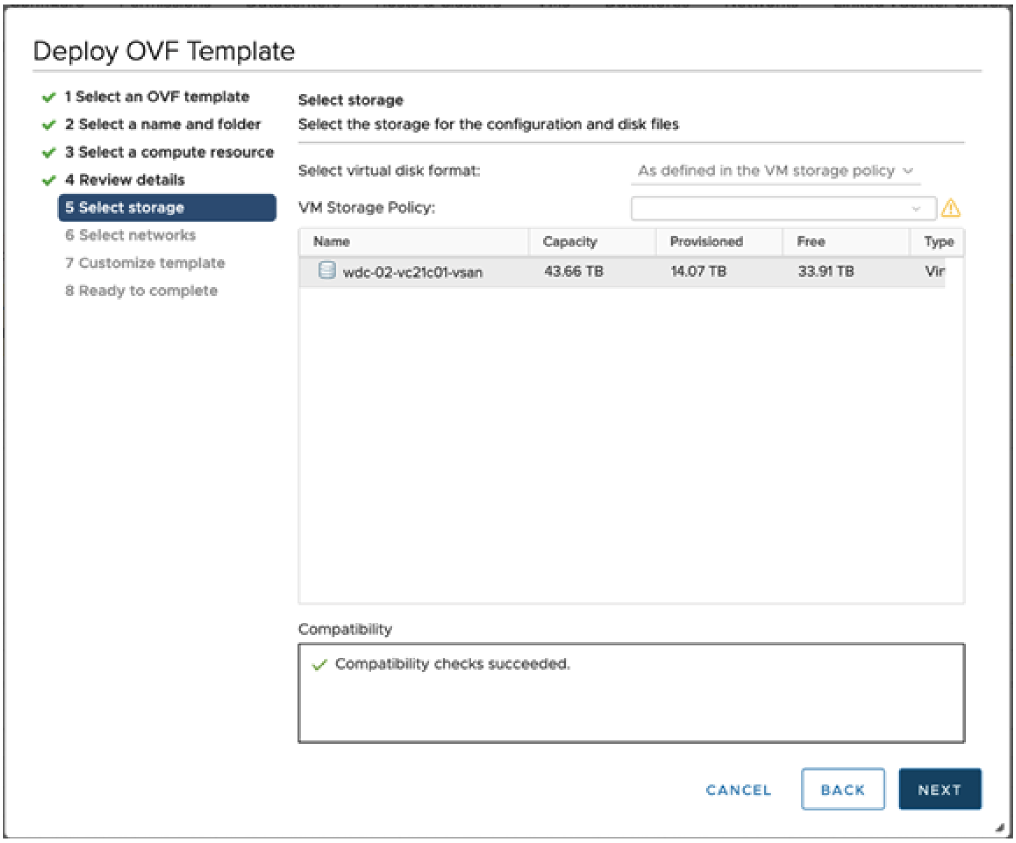
Select virtual disk format: As defined in the VM storage policy

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
vsanDatastore	41.92 TB	7.12 TB	34.8 TB	Virtual SAN	

Compatibility

✓ Compatibility checks succeeded.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

Select virtual disk format: As defined in the VM storage policy

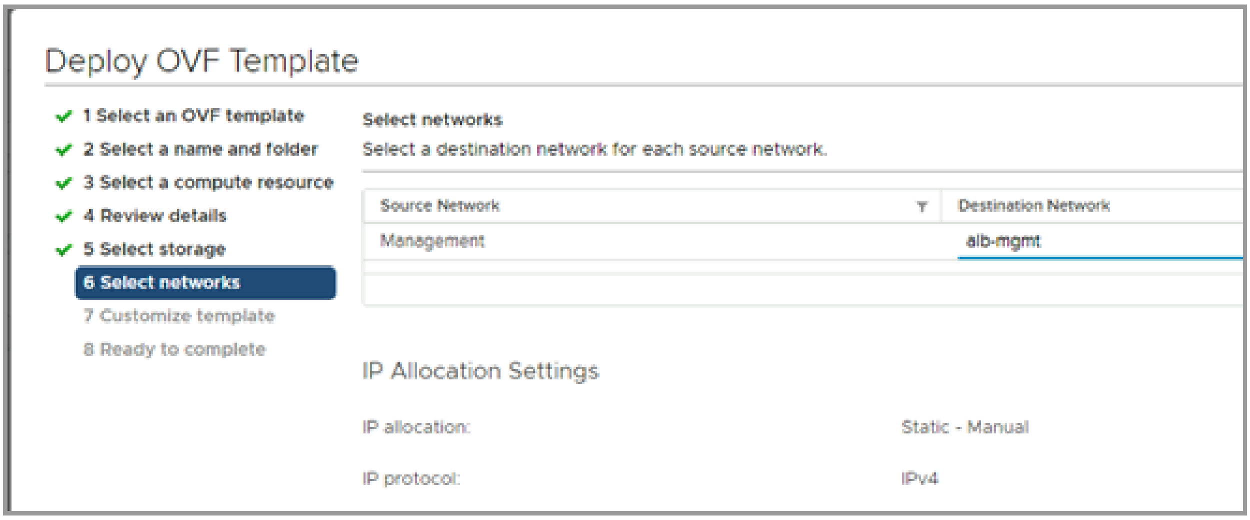
VM Storage Policy: ⚠

Name	Capacity	Provisioned	Free	Type
wdc-02-vc21c01-vsan	43.66 TB	14.07 TB	33.91 TB	Vir

Compatibility

✓ Compatibility checks succeeded.

8. Choose a management network for the Avi Controller.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management	alb-mgmt

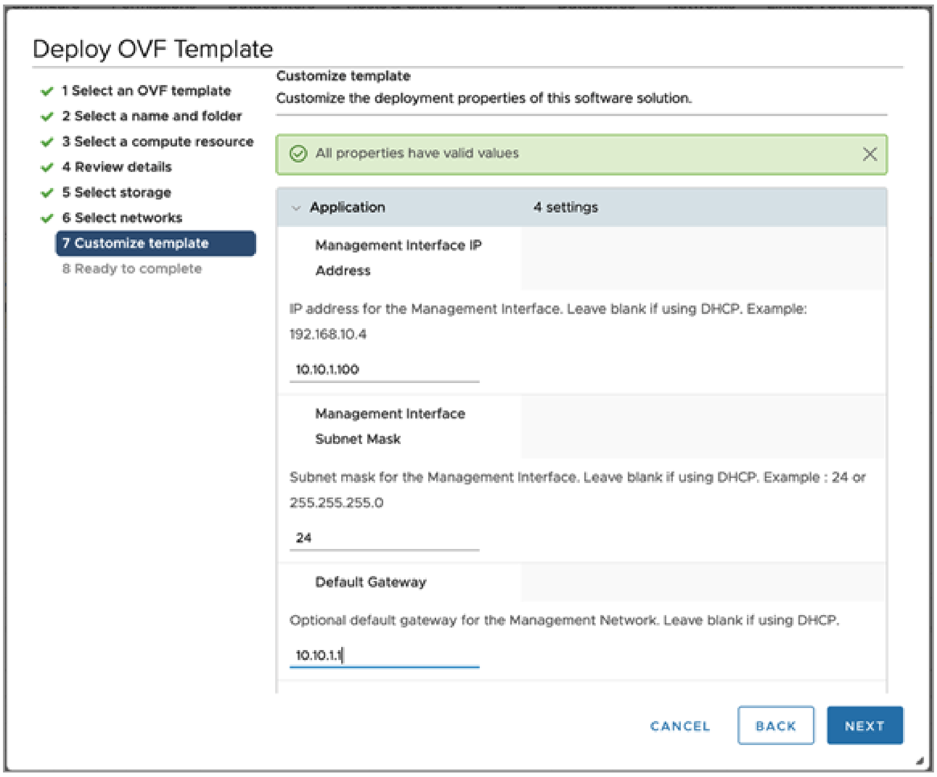
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

9. Enter the management IP address, subnet mask and default gateway. In the case of DHCP, leave this field empty.

Note: Using static IP address is recommended for production setups.



Deploy OVF Template

Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Application 4 settings

Management Interface IP Address

IP address for the Management Interface. Leave blank if using DHCP. Example: 192.168.10.4

10.10.1.100

Management Interface Subnet Mask

Subnet mask for the Management Interface. Leave blank if using DHCP. Example : 24 or 255.255.255.0

24

Default Gateway

Optional default gateway for the Management Network. Leave blank if using DHCP.

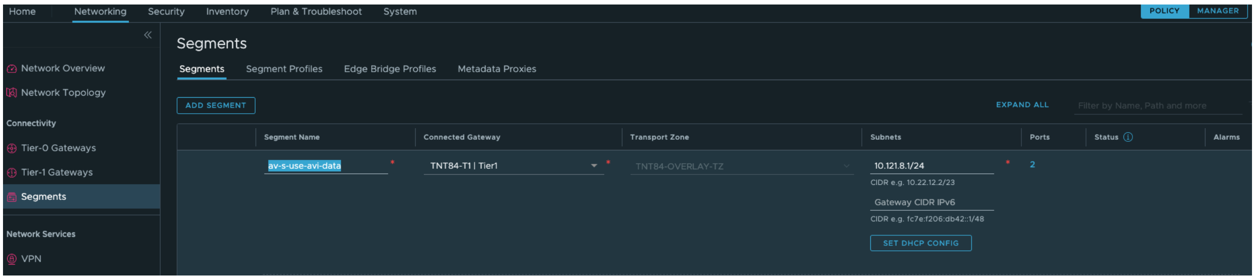
10.10.1.1

10. Review the settings and click on **Finish**. After this, power on the virtual machine.

Configuring AVI Network Segments in NSX-T

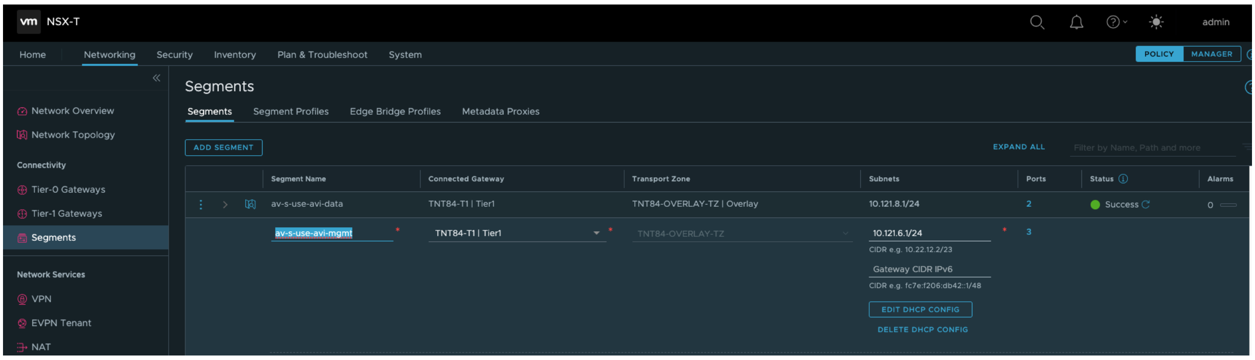
Assuming your NSX-T is up and running for your Azure VMware Solution SDDC, you should be able to navigate to Networking > Segments and add your data, management and shared networks.

This is a very important step to allow proper traffic routing between your different AVI components.



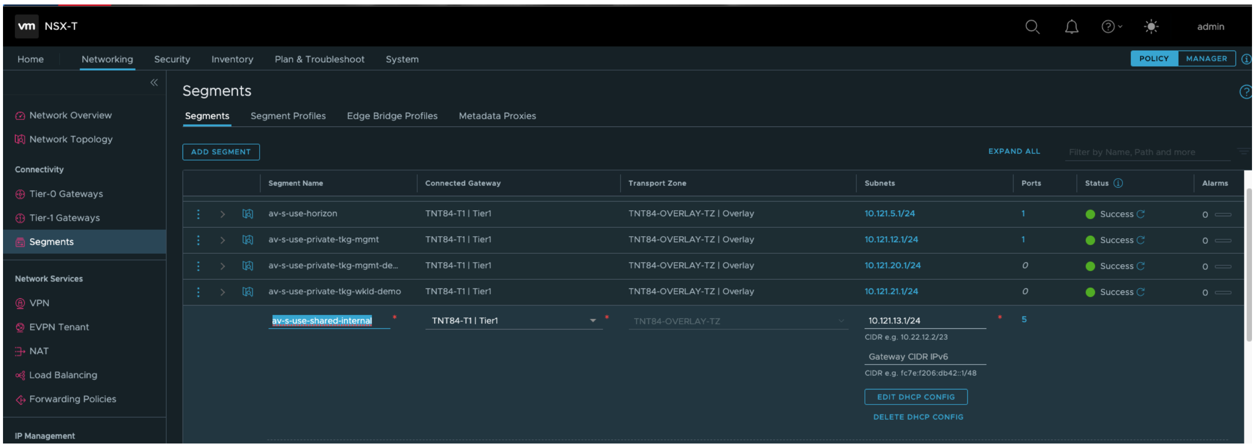
Segments

Segment Name	Connected Gateway	Transport Zone	Subnets	Ports	Status	Alarms
av-s-use-avi-data	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ	10.121.8.1/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48	2		



Segments

Segment Name	Connected Gateway	Transport Zone	Subnets	Ports	Status	Alarms
av-s-use-avi-data	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ | Overlay	10.121.8.1/24	2	● Success	0
av-s-use-avi-mgmt *	TNT84-T1 | Tier1 *	TNT84-OVERLAY-TZ	10.121.6.1/24 * CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48	3		



Segments

Segment Name	Connected Gateway	Transport Zone	Subnets	Ports	Status	Alarms
av-s-use-horizon	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ | Overlay	10.121.5.1/24	1	● Success	0
av-s-use-private-tkg-mgmt	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ | Overlay	10.121.12.1/24	1	● Success	0
av-s-use-private-tkg-mgmt-de...	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ | Overlay	10.121.20.1/24	0	● Success	0
av-s-use-private-tkg-wkld-demo	TNT84-T1 | Tier1	TNT84-OVERLAY-TZ | Overlay	10.121.21.1/24	0	● Success	0
av-s-use-shared-internal *	TNT84-T1 | Tier1 *	TNT84-OVERLAY-TZ	10.121.13.1/24 * CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48	5		

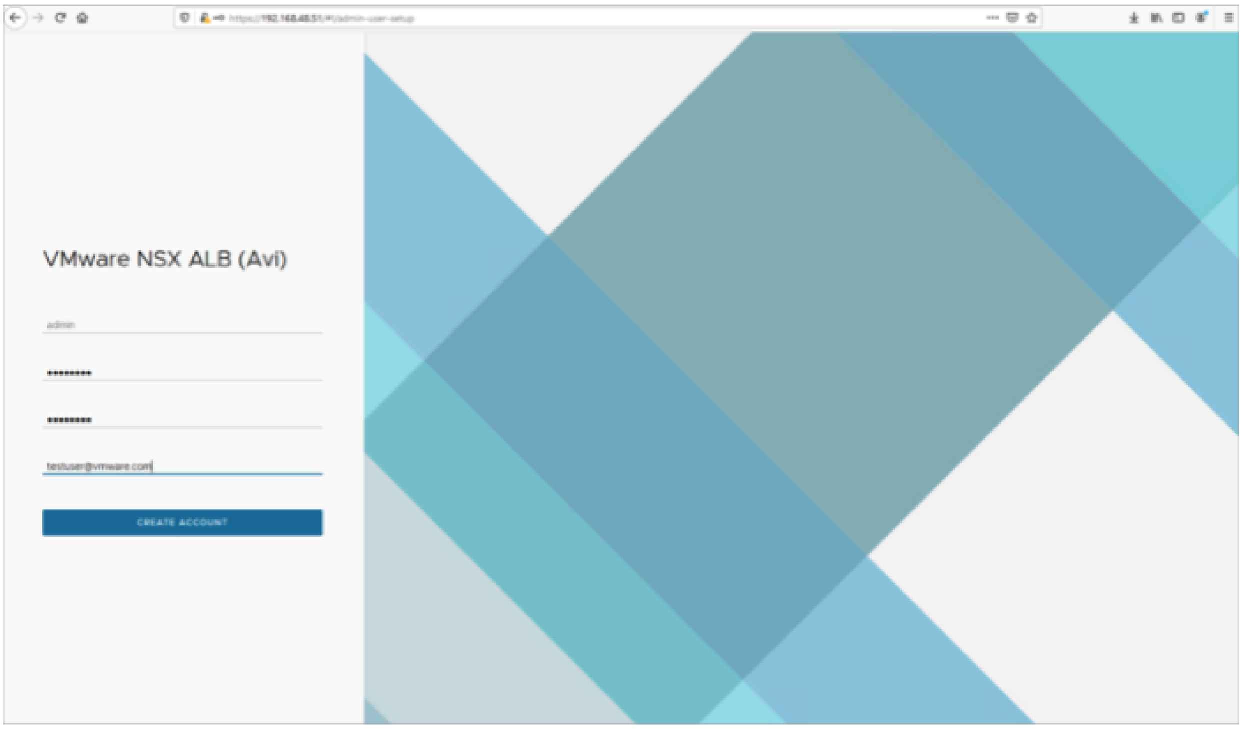
Setting up the Avi Controller

This section shows the steps to perform initial configuration of the Avi Controller using its deployment wizard. You can change or customize settings following initial deployment using the Avi Controller’s web interface.

1. To complete the setup, navigate to the Avi Controller IP via a browser.

Note: While the system is booting up, a 503 status code or a page with following message will appear, “Controller is not yet ready. Please try again after a couple of minutes”. Wait for about 5 to 10 minutes and refresh the page. Then follow the instructions below for the setup wizard.

2. Enter the admin details as shown below:



VMware NSX ALB (Avi)

admin

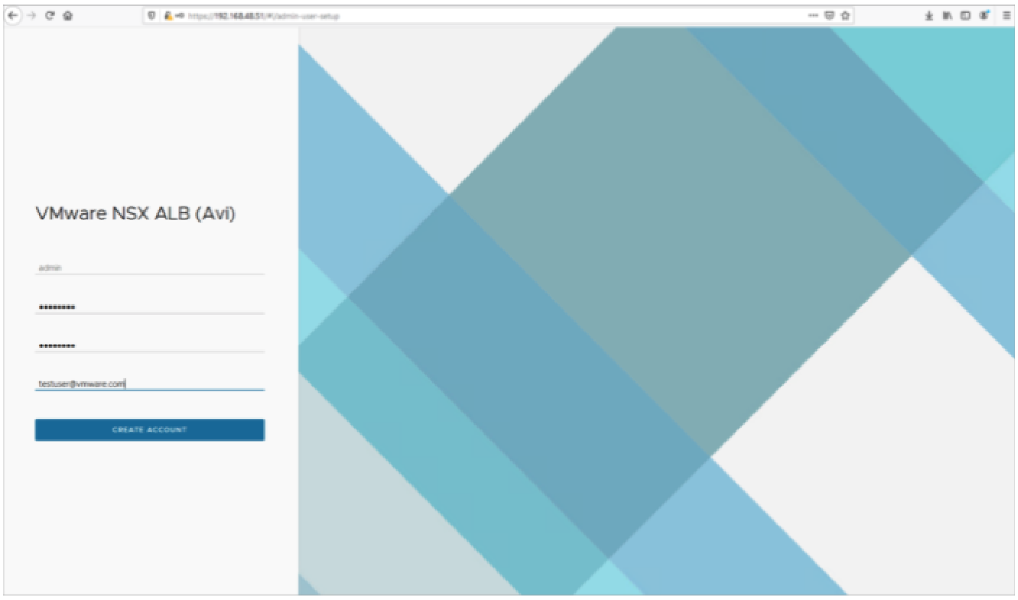
****

****

testuser@vmware.com

Note: This e-mail address is required for admin password reset in case of lockout.

3. Enter the backup passphrase, DNS server information.
4. Configure the Email/SMTP information.



https://192.168.48.51/#/admin-user-setup

VMware NSX ALB (Avi)

admin

•••••••••

•••••••••

testuser@vmware.com

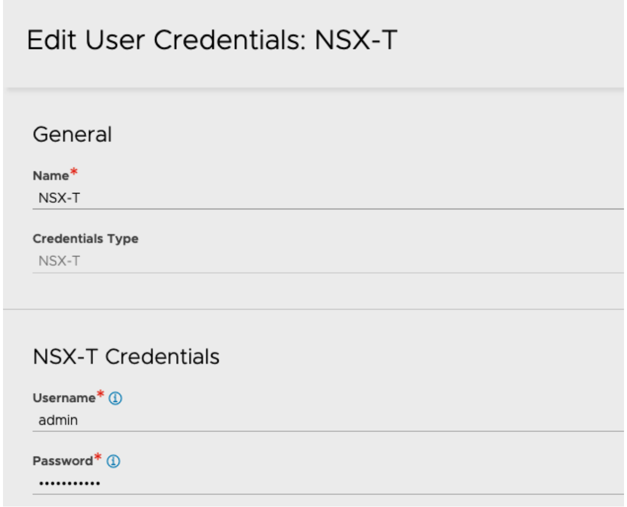
5. Click on Save.

Creating an NSX-T Cloud

To create an NSX-T cloud, log in into the Avi Controller and follow the steps given below:

Create Credentials

1. In the Avi UI, Navigate to **Administration** > **User Credentials**.
2. Click on **Create**.
3. Provide a **Name** for the credential.
4. Select *NSX-T* as the **Credentials Type**.
5. Provide the NSX **Username** and **Password**



Edit User Credentials: NSX-T

General

Name* NSX-T

Credentials Type NSX-T

NSX-T Credentials

Username* admin

Password* •••••••••••

6. Click on **Save**

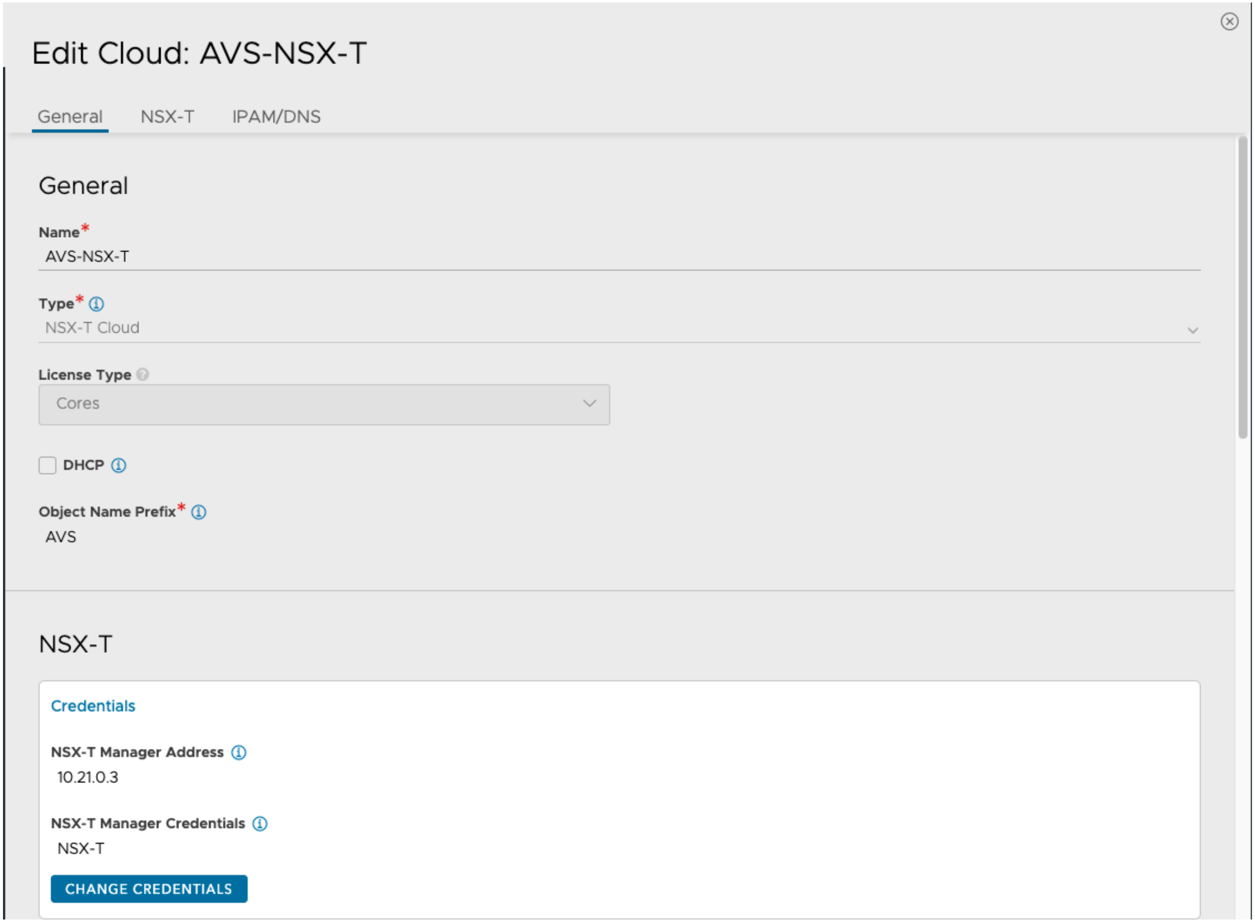
Similarly, create the vCenter credentials.

Configure the Cloud

To configure the cloud:

1. Navigate to **Infrastructure > Clouds**.
2. Click on **Create** and select the **NSX-T Cloud**.
3. Enter the **Name** of the NSX-T cloud.

4. Check the **DHCP** option if SE management segment has DHCP enabled.
5. Enter a prefix string. The prefix string must only have letters, numbers, and underscore. This field cannot be changed once the cloud is configured.
6. Enter the NSX-T manager hostname or IP address as the **NSX-T Manager Address** and select the **NSX-T Manager Credentials**.
7. Click on Connect to authenticate with the NSX-T manager.



Edit Cloud: AVS-NSX-T

General

Name* AVS-NSX-T

Type* NSX-T Cloud

License Type Cores

□ DHCP

Object Name Prefix* AVS

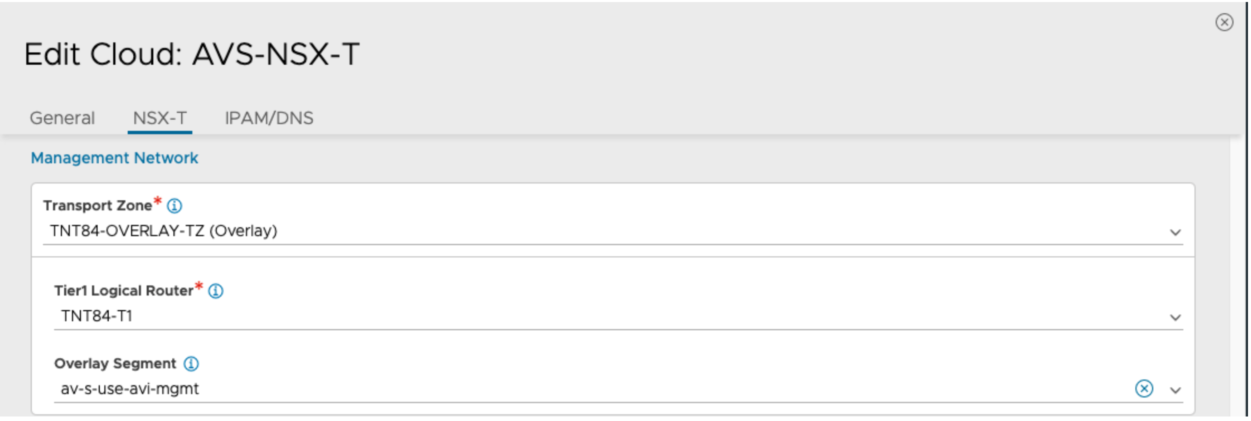
NSX-T

Credentials

NSX-T Manager Address 10.21.0.3

NSX-T Manager Credentials NSX-T

8. Select the **Transport Zone** required from the drop-down.
9. Under **Management Network Segment**, select the **Tier1 Logical Router ID** and **Segment ID**.
10. Select the Tier-1 gateway and logical switch for VIP placement.
11. Click on **Add** to select one more Tier-1 router and a connected logical segment for VIP placement.



Edit Cloud: AVS-NSX-T

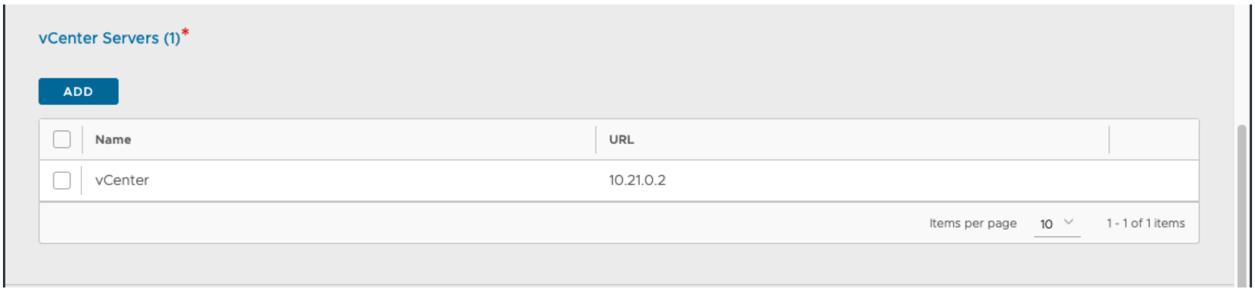
Management Network

Transport Zone* TNT84-OVERLAY-TZ (Overlay)

Tier1 Logical Router* TNT84-T1

Overlay Segment av-s-use-avi-mgmt

12. Under vCenter Servers, click on **Add**.
13. Enter the vCenter server **Name** and configure the credentials.
14. Click on **Connect**.
15. Select the Content Library and click on **Done**.



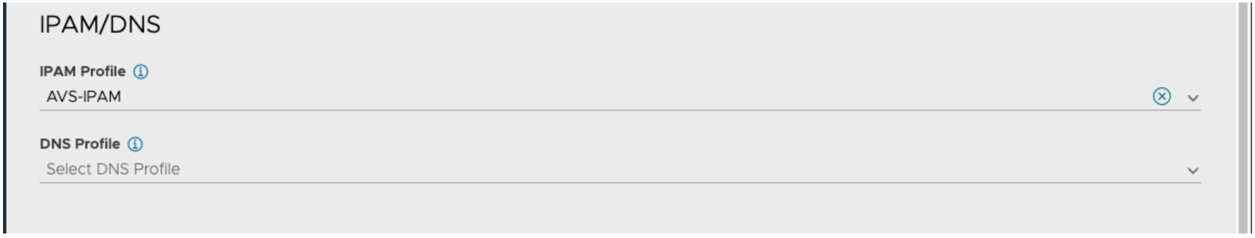
vCenter Servers (1)*

ADD

Name	URL
vCenter	10.21.0.2

Items per page 10 1 - 1 of 1 items

16. Select the IPAM/DNS Profile, as required.



IPAM/DNS

IPAM Profile: AVS-IPAM

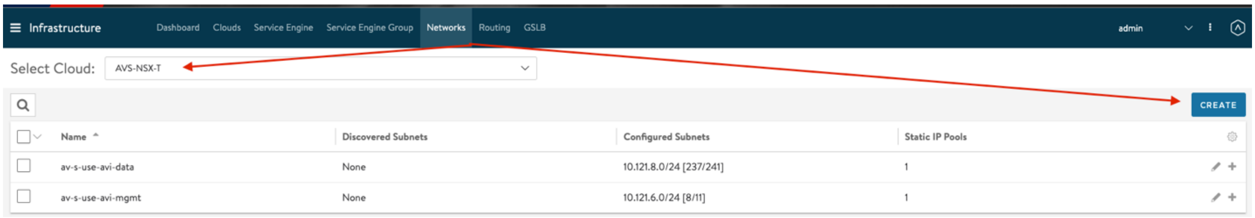
DNS Profile: Select DNS Profile

Note: you might need to go and create an IPAM and DNS profiles before going through the previous step

17. Click on **Save** to create the NSX-T cloud.
The Cloud Connector Status will turn green, and the system is ready for creation of a virtual Service.

Configure Networks

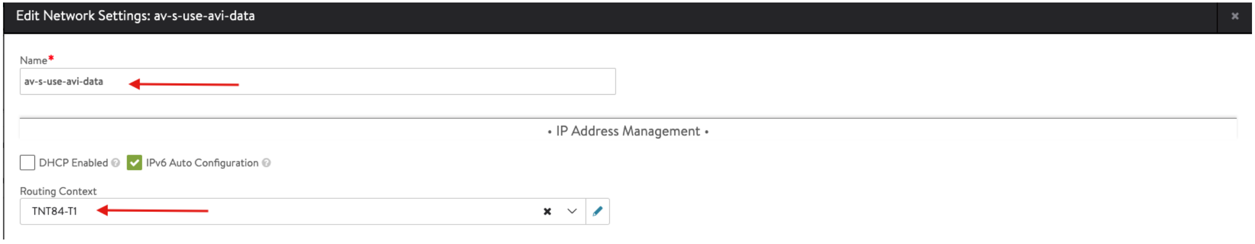
1. From the Controller UI, navigate to **Infrastructure** > **Networks**
2. Select the cloud (AVS-NSX-T)
3. Select **Create**



Select Cloud: AVS-NSX-T

Name	Discovered Subnets	Configured Subnets	Static IP Pools
av-s-use-avi-data	None	10.121.8.0/24 [237/241]	1
av-s-use-avi-mgmt	None	10.121.6.0/24 [8/11]	1

4. Enter the details as per the following image



Edit Network Settings: av-s-use-avi-data

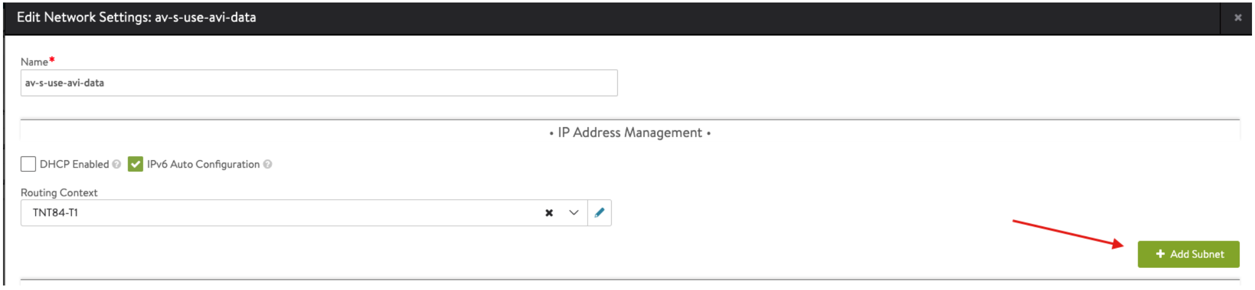
Name*: av-s-use-avi-data

• IP Address Management •

□ DHCP Enabled ☑ IPv6 Auto Configuration

Routing Context: TNT84-T1

5. Select Add Subnet and insert the following details



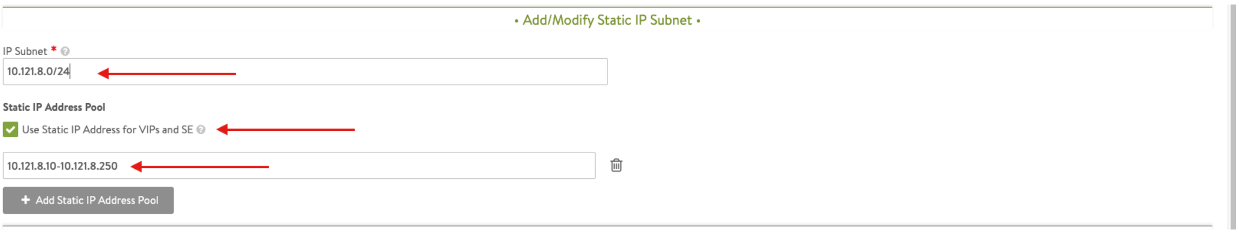
Edit Network Settings: av-s-use-avi-data

Name*: av-s-use-avi-data

• IP Address Management •

□ DHCP Enabled ☑ IPv6 Auto Configuration

Routing Context: TNT84-T1



• Add/Modify Static IP Subnet •

IP Subnet *

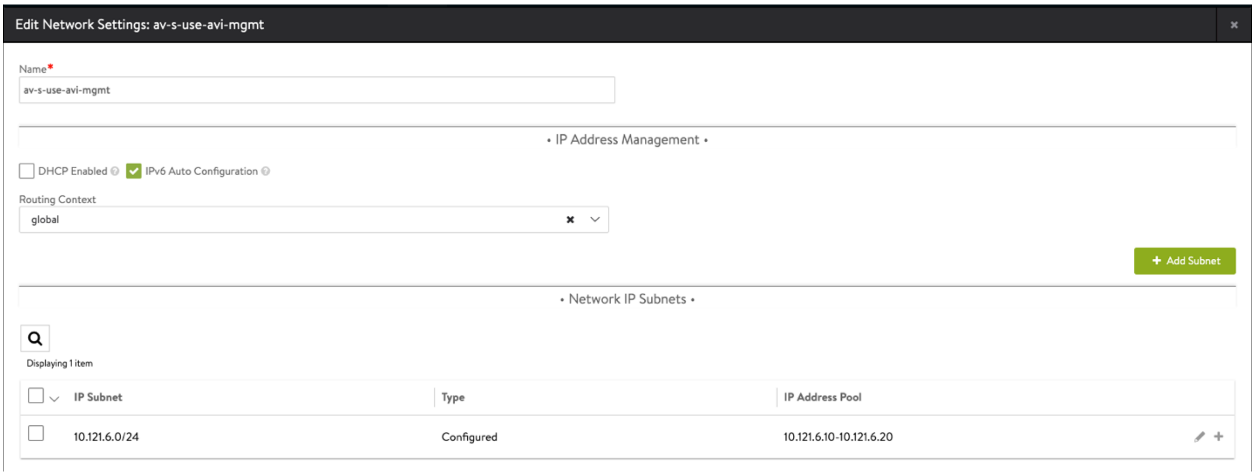
10.121.8.0/24

Static IP Address Pool

☑ Use Static IP Address for VIPs and SE

10.121.8.10-10.121.8.250

Apply the same previous steps to create the AVI management network.



Edit Network Settings: av-s-use-avi-mgmt

Name*

av-s-use-avi-mgmt

• IP Address Management •

□ DHCP Enabled ☑ IPv6 Auto Configuration

Routing Context

global

• Network IP Subnets •

Displaying 1 item

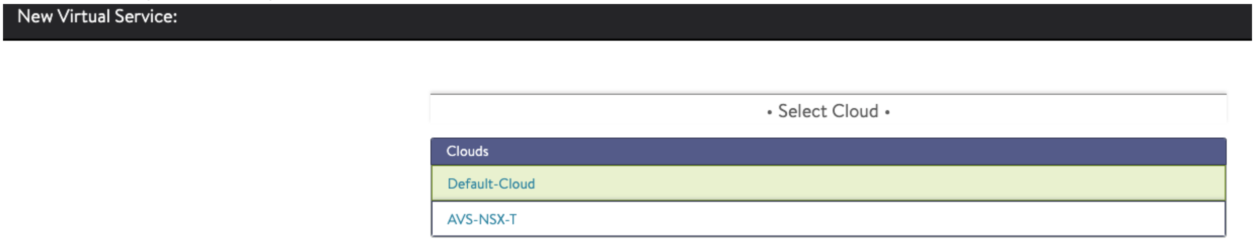
□	IP Subnet	Type	IP Address Pool
□	10.121.6.0/24	Configured	10.121.6.10-10.121.6.20

Note: The av-s-use-avi-data network will be used by AVI for application VIPs, the av-s-use-avi-mgmt will be used by AVI for the Service Engines

Creating Virtual Services (DNS and Application VIPs)

DNS Virtual Service

1. From the Controller UI, navigate to **Applications** > **Create Virtual Service** (Advanced Setup).
2. Select the cloud (AVS-NSX-T)



New Virtual Service:

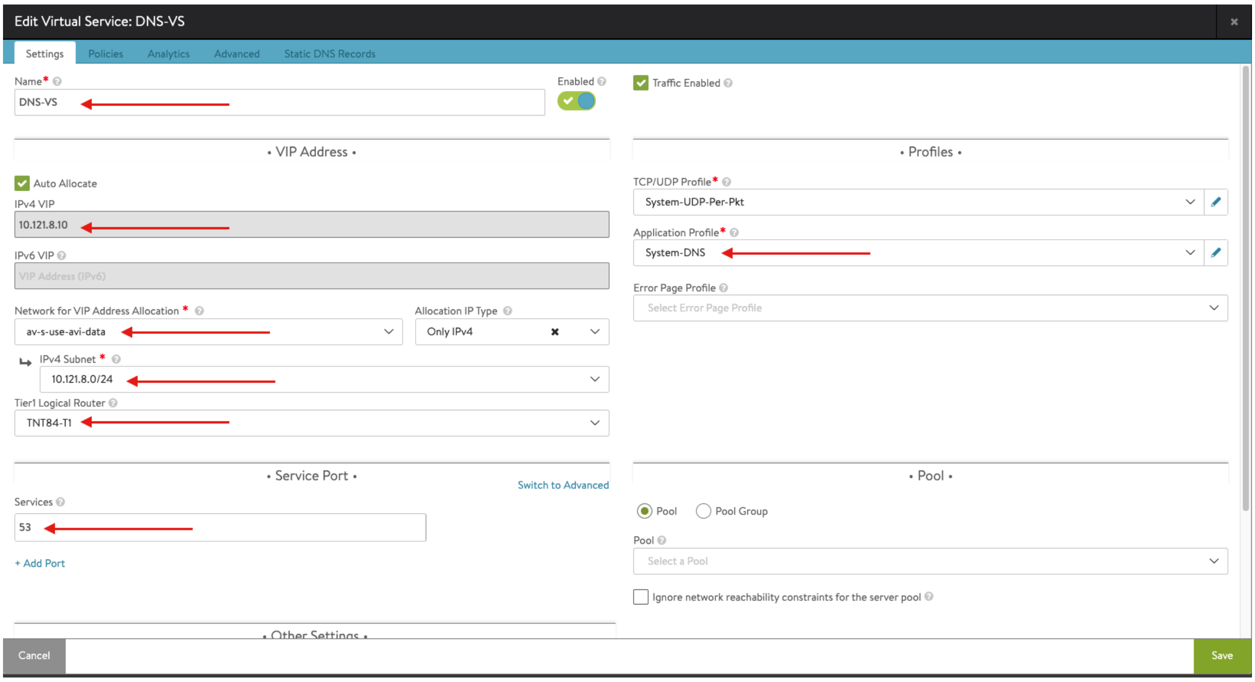
• Select Cloud •

Clouds

Default-Cloud

AVS-NSX-T

3. Enter the details related to the VS IP, Pool members, Tier 1 Logical Router, etc.



Edit Virtual Service: DNS-VS

Name*: DNS-VS

Enabled

☑ Traffic Enabled

• VIP Address •

☑ Auto Allocate

IPv4 VIP: 10.121.8.10

IPv6 VIP: VIP Address (IPv6)

Network for VIP Address Allocation *: av-s-use-avi-data

Allocation IP Type: Only IPv4

IPv4 Subnet *: 10.121.8.0/24

Tier1 Logical Router: TNT84-T1

• Profiles •

TCP/UDP Profile*: System-UDP-Per-Pkt

Application Profile*: System-DNS

Error Page Profile: Select Error Page Profile

• Service Port •

Switch to Advanced

Services: 53

+ Add Port

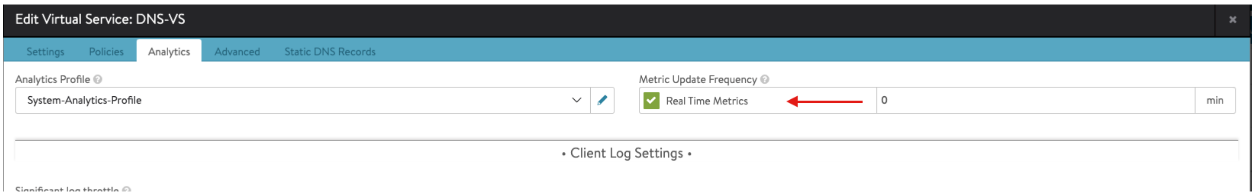
• Pool •

● Pool ○ Pool Group

Pool: Select a Pool

□ Ignore network reachability constraints for the server pool

• Other Settings •



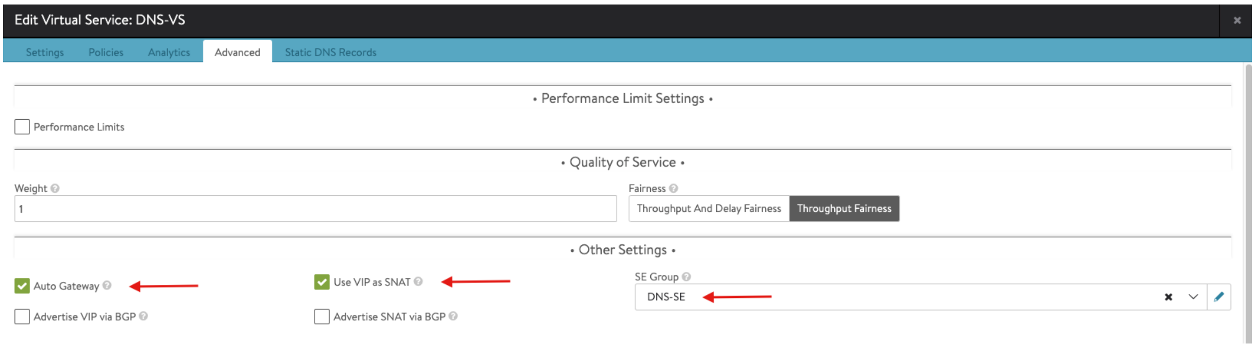
Edit Virtual Service: DNS-VS

Analytics Profile: System-Analytics-Profile

Metric Update Frequency: ☑ Real Time Metrics 0 min

• Client Log Settings •

Significant log throttle



Edit Virtual Service: DNS-VS

• Performance Limit Settings •

□ Performance Limits

• Quality of Service •

Weight: 1

Fairness: Throughput And Delay Fairness [✓ Throughput Fairness]

• Other Settings •

☑ Auto Gateway

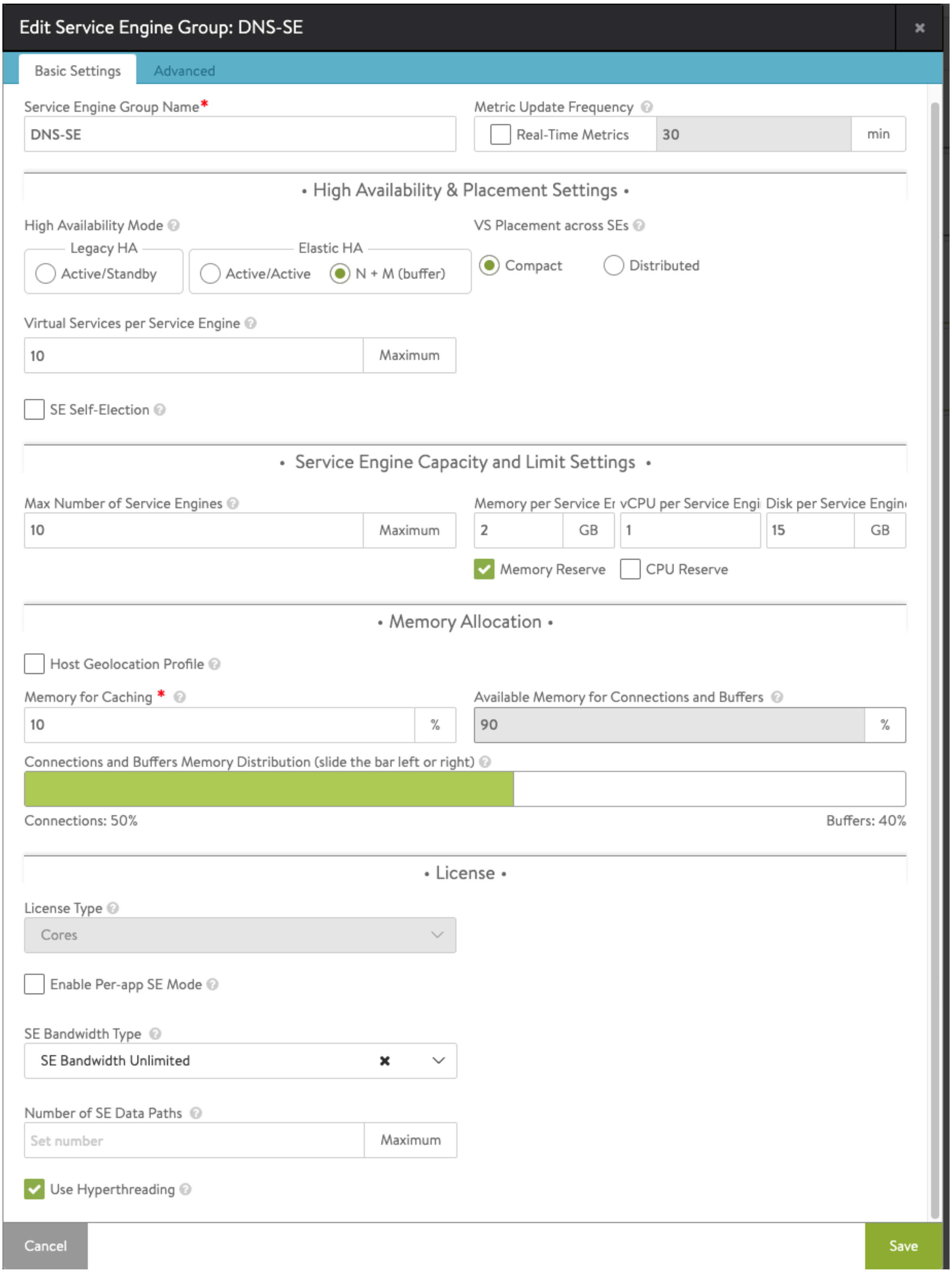
□ Advertise VIP via BGP

☑ Use VIP as SNAT

□ Advertise SNAT via BGP

SE Group: DNS-SE

Note: you need to configure the DNS-SE group shown in the above snapshot, you can do sy by clicking on the pencil symbol associated with SE-Group and apply the following configuration.



Edit Service Engine Group: DNS-SE

Service Engine Group Name*: DNS-SE

Metric Update Frequency: □ Real-Time Metrics 30 min

• High Availability & Placement Settings •

High Availability Mode
Legacy HA: ○ Active/Standby
Elastic HA: ○ Active/Active ● N + M (buffer)

VS Placement across SEs: ● Compact ○ Distributed

Virtual Services per Service Engine: 10 Maximum

□ SE Self-Election

• Service Engine Capacity and Limit Settings •

Max Number of Service Engines: 10 Maximum

Memory per Service Engine: 2 GB

vCPU per Service Engine: 1

Disk per Service Engine: 15 GB

☑ Memory Reserve □ CPU Reserve

• Memory Allocation •

□ Host Geolocation Profile

Memory for Caching *: 10 %

Available Memory for Connections and Buffers: 90 %

Connections and Buffers Memory Distribution (slide the bar left or right)

Connections: 50%

Buffers: 40%

• License •

License Type: Cores

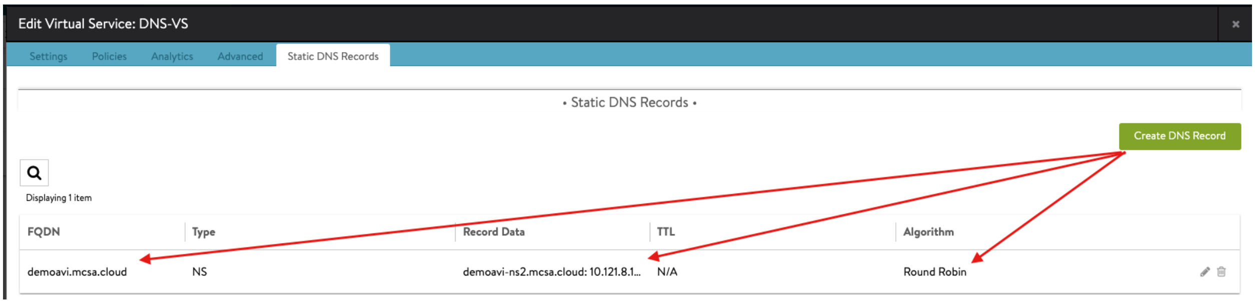
□ Enable Per-app SE Mode

SE Bandwidth Type: SE Bandwidth Unlimited

Number of SE Data Paths: Set number Maximum

☑ Use Hyperthreading

Once this is done, hit save and resume the configuration.



• Static DNS Records •

FQDN	Type	Record Data	TTL	Algorithm
demoavi.mcsa.cloud	NS	demoavi-ns2.mcsa.cloud: 10.121.8.1...	N/A	Round Robin

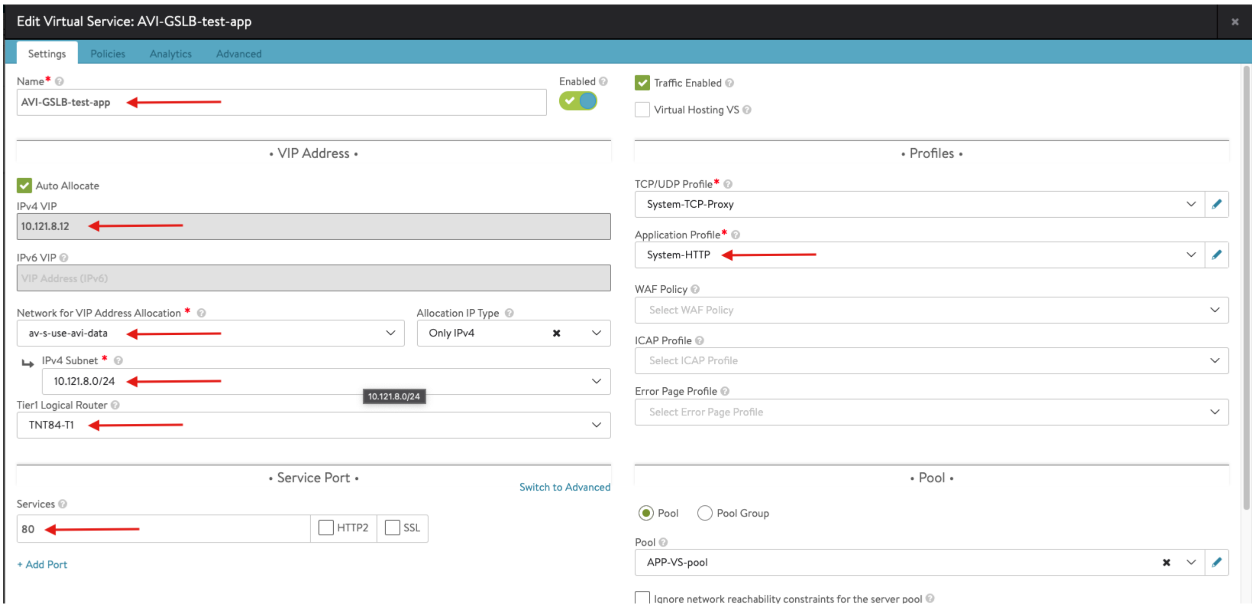
4. click on Save to create the virtual service.

On successful creation of a Service Engine, the virtual service will come up and will be ready to process traffic.

Application Virtual Service

Go through the same steps to configure the application virtual service, however, apply the following configurations this time:

1. Enter the details related to the VS IP, Pool members, Tier 1 Logical Router, etc. Note the pool configuration is show in the next screenshot.



Name* AVI-GSLB-test-app

Enabled

☑ Traffic Enabled

□ Virtual Hosting VS

• VIP Address •

☑ Auto Allocate

IPv4 VIP 10.121.8.12

IPv6 VIP VIP Address (IPv6)

Network for VIP Address Allocation * av-s-use-avi-data

Allocation IP Type Only IPv4

IPv4 Subnet * 10.121.8.0/24

Tier1 Logical Router TNT84-T1

• Service Port •

Services 80 □ HTTP2 □ SSL

• Profiles •

TCP/UDP Profile* System-TCP-Proxy

Application Profile* System-HTTP

WAF Policy Select WAF Policy

ICAP Profile Select ICAP Profile

Error Page Profile Select Error Page Profile

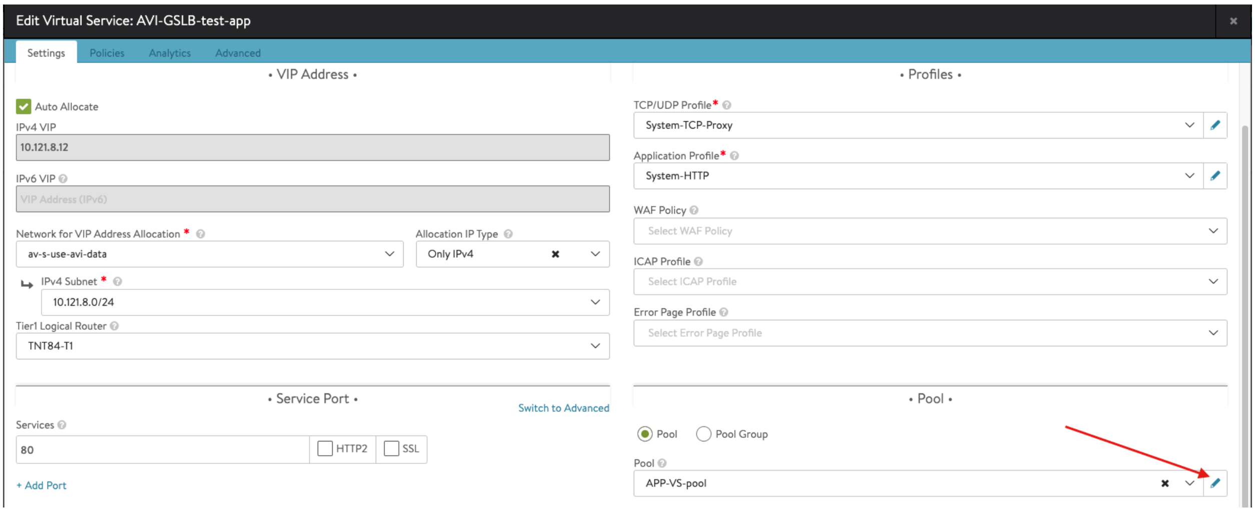
• Pool •

● Pool ○ Pool Group

Pool APP-VS-pool

□ Ignore network reachability constraints for the server pool

2. Create a Pool



• VIP Address •

☑ Auto Allocate

IPv4 VIP 10.121.8.12

IPv6 VIP VIP Address (IPv6)

Network for VIP Address Allocation * av-s-use-avi-data

Allocation IP Type Only IPv4

IPv4 Subnet * 10.121.8.0/24

Tier1 Logical Router TNT84-T1

• Service Port •

Services 80 □ HTTP2 □ SSL

• Profiles •

TCP/UDP Profile* System-TCP-Proxy

Application Profile* System-HTTP

WAF Policy Select WAF Policy

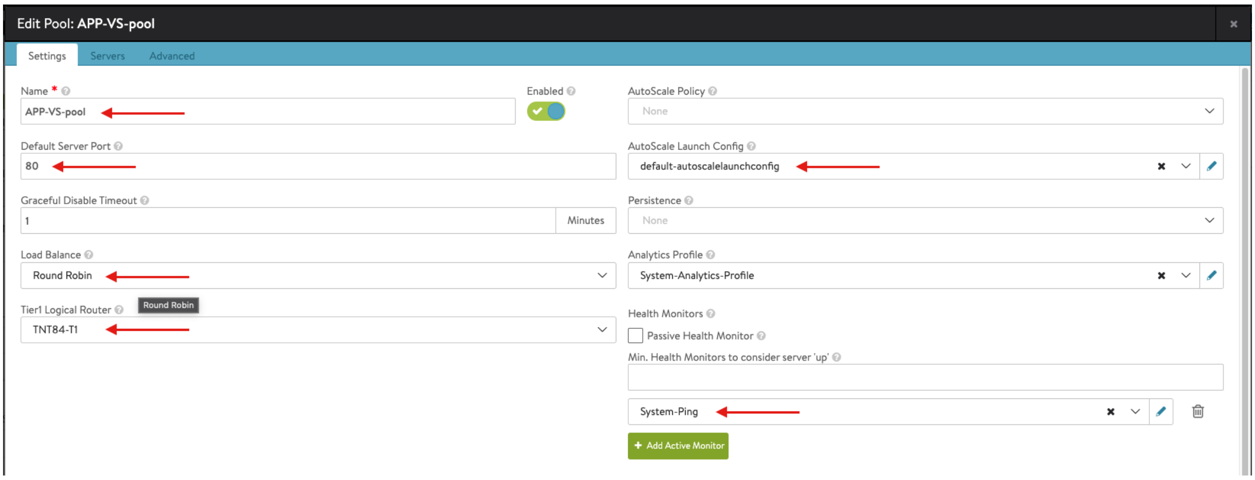
ICAP Profile Select ICAP Profile

Error Page Profile Select Error Page Profile

• Pool •

● Pool ○ Pool Group

Pool APP-VS-pool



Edit Pool: APP-VS-pool

Name *: APP-VS-pool

Enabled: ✓

AutoScale Policy: None

Default Server Port: 80

AutoScale Launch Config: default-autoscalelaunchconfig

Graceful Disable Timeout: 1 Minutes

Persistence: None

Load Balance: Round Robin

Analytics Profile: System-Analytics-Profile

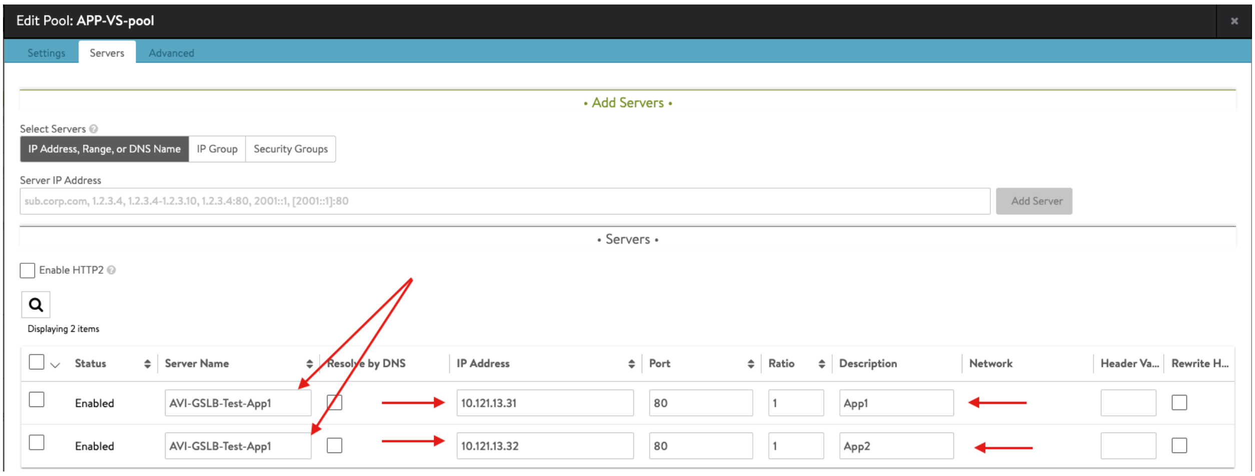
Tier1 Logical Router: TNT84-T1

Health Monitors

□ Passive Health Monitor

Min. Health Monitors to consider server 'up'

System-Ping



Edit Pool: APP-VS-pool

Select Servers: IP Address, Range, or DNS Name | IP Group | Security Groups

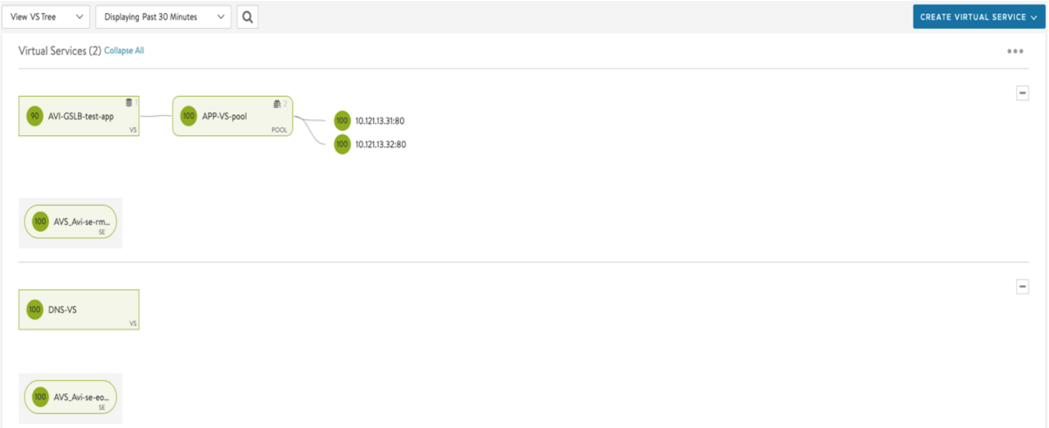
Server IP Address: sub.corp.com, 1.2.3.4, 1.2.3.4-1.2.3.10, 1.2.3.4:80, 2001::1, [2001::1]:80

□ Enable HTTP2

Displaying 2 items

□	Status	Server Name	Resolve by DNS	IP Address	Port	Ratio	Description	Network	Header Va...	Rewrite H...
□	Enabled	AVI-GSLB-Test-App1	□	10.121.13.31	80	1	App1			□
□	Enabled	AVI-GSLB-Test-App1	□	10.121.13.32	80	1	App2			□

3. Once you complete the Pool configuration, hit Save to complete the Virtual Service configuration
4. Once you completed the configuration you should have something like the following:



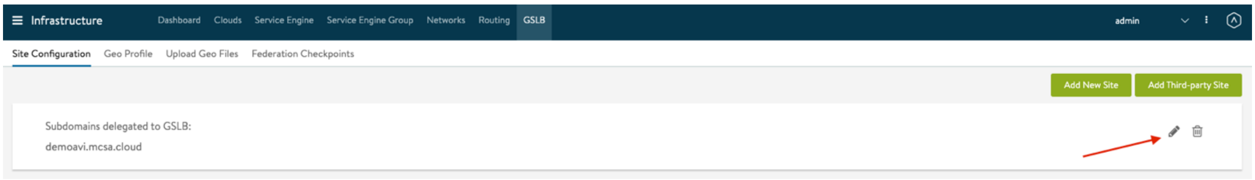
Configure Global Load Balancing for Azure VMware Solution

Once all the previous steps were completed successfully, you can move ahead with the GSLB configuration. First, we need to enable GSLB service as per below

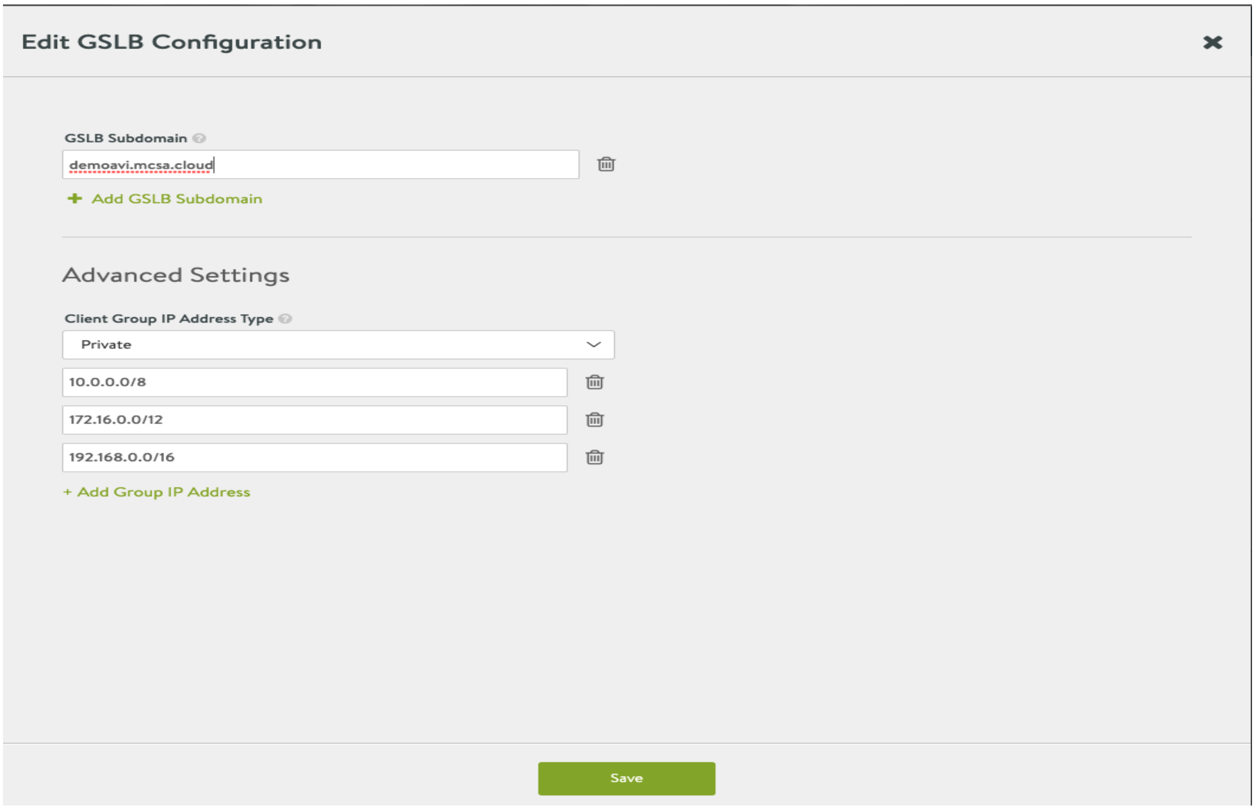
I have selected the AVI Controller in AVS to be my leader GSLB controller, you can select only one leader controller in your setup.

let us first add your GSLB members to the GSLB leader (which is your AVS Controller)

1. From the Controller UI, navigate to **Infrastructure** > **GSLB**
2. Select **Create**
3. Select Edit for your Subdomains delegated to GSLB and insert all the following information, once done hit save



Subdomains delegated to GSLB:
demoavi.mcsa.cloud



Edit GSLB Configuration

GSLB Subdomain: demoavi.mcsa.cloud

Advanced Settings

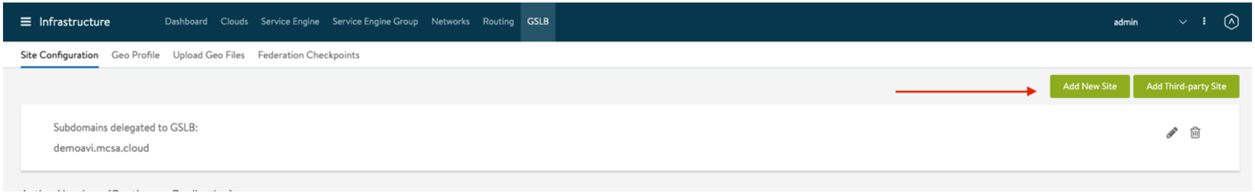
Client Group IP Address Type: Private

10.0.0.0/8

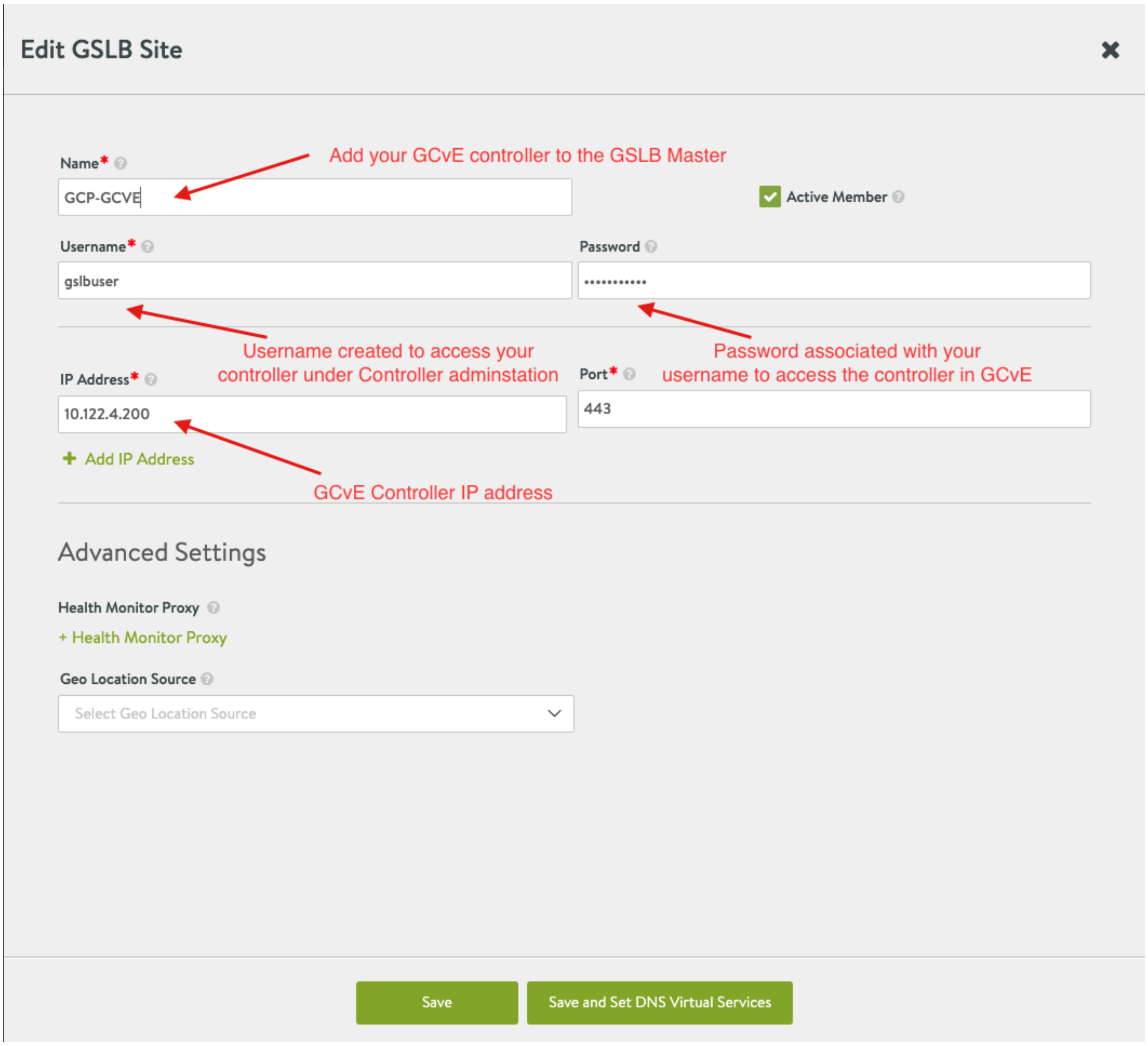
172.16.0.0/12

192.168.0.0/16

4. Next select Add New Site to add the following sites to GSLB



Subdomains delegated to GSLB:
demoavi.mcsa.cloud



Edit GSLB Site

Name*: GCP-GCVE

☑ Active Member

Username*: gslbuser

Password: •••••••••••

IP Address*: 10.122.4.200

Port*: 443

Add your GCvE controller to the GSLB Master

Username created to access your controller under Controller adminstation

Password associated with your username to access the controller in GCvE

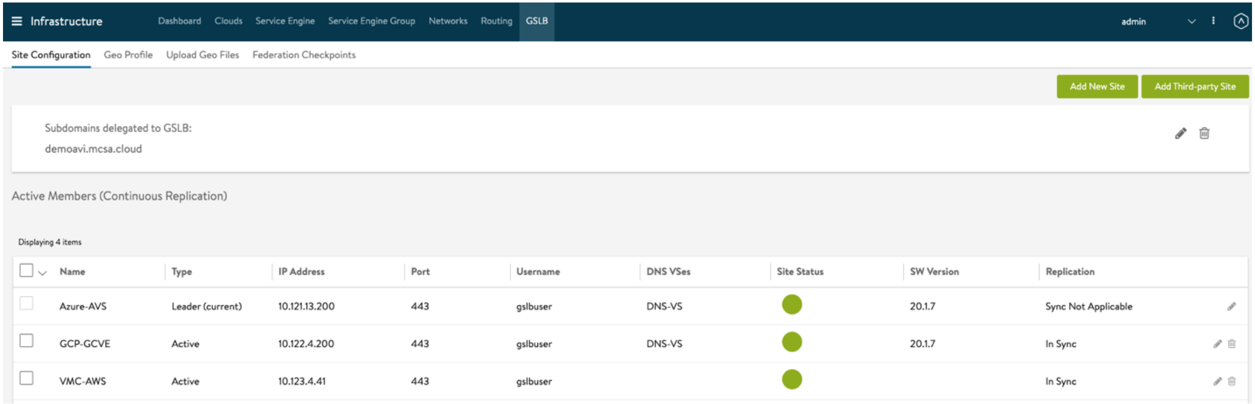
GCvE Controller IP address

Advanced Settings

Health Monitor Proxy

Geo Location Source: Select Geo Location Source

5. Repeat the configurations in step 4 for all the other GSLB Sites. Once done, you should get a similar view, please note that Azure-AVS site is Leader and Sync Not applicable.



Subdomains delegated to GSLB:
demoavi.mcsa.cloud

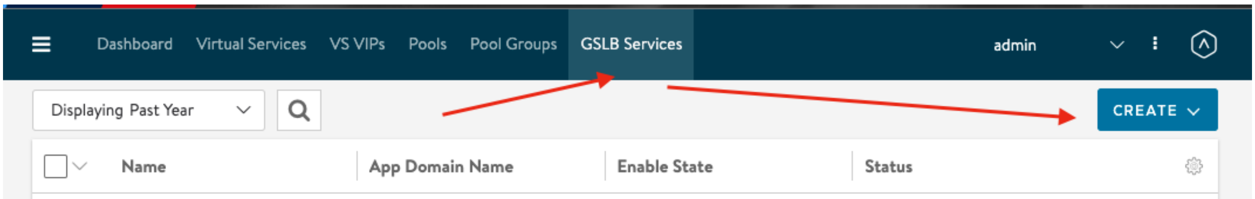
Active Members (Continuous Replication)

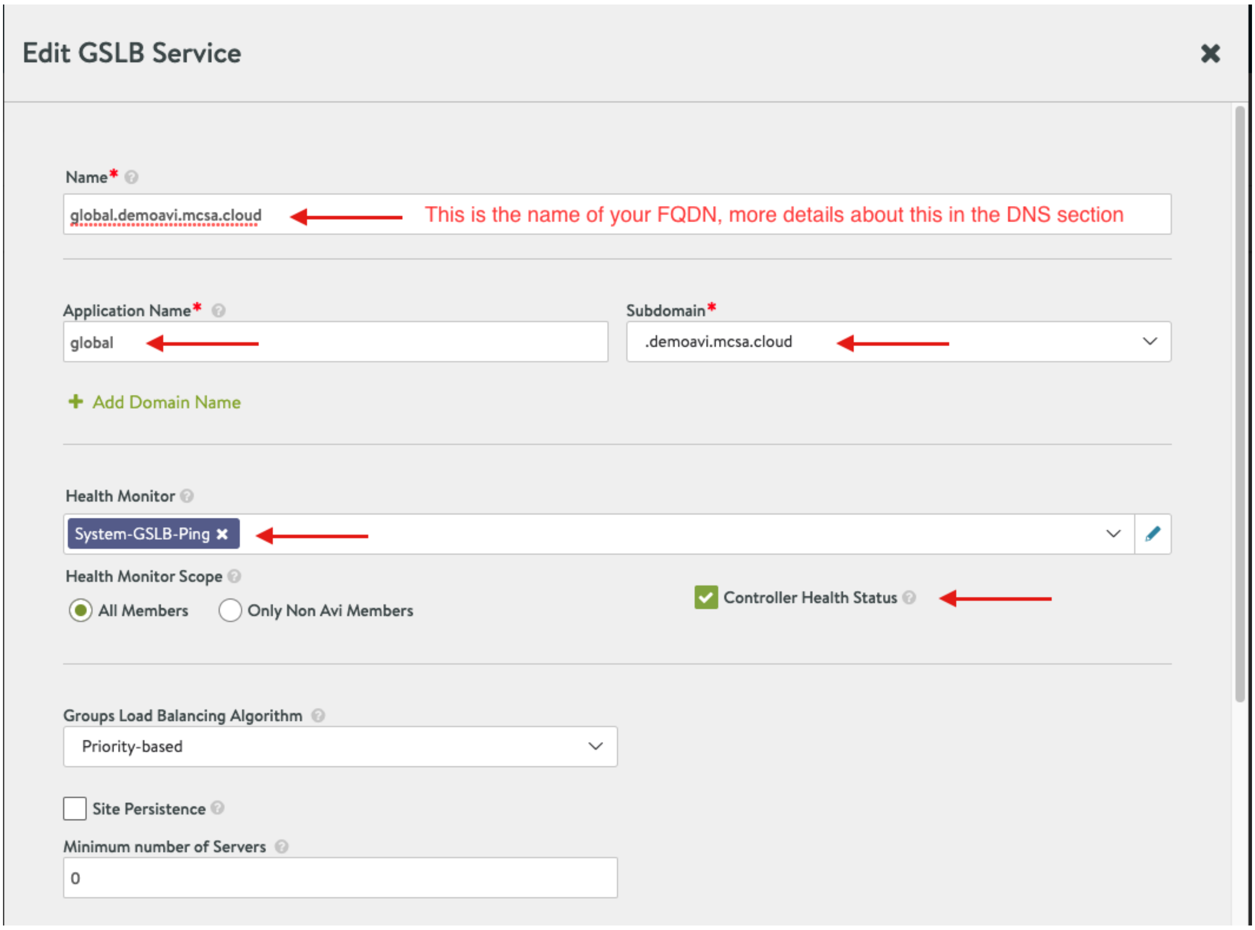
Displaying 4 items

	Name	Type	IP Address	Port	Username	DNS VSes	Site Status	SW Version	Replication
□	Azure-AVS	Leader (current)	10.121.13.200	443	gslbuser	DNS-VS	●	20.1.7	Sync Not Applicable
□	GCP-GCVE	Active	10.122.4.200	443	gslbuser	DNS-VS	●	20.1.7	In Sync
□	VMC-AWS	Active	10.123.4.41	443	gslbuser		●		In Sync

Next, You will apply your GSLB configuration for all the other SDDCs in the leader GSLB controller.

1. From the Controller UI, navigate to **Applications** > **GSLB Services**
2. Select **Create**




Edit GSLB Service

Name*: global.demoavi.mcsa.cloud

This is the name of your FQDN, more details about this in the DNS section

Application Name*: global

Subdomain*: .demoavi.mcsa.cloud

Health Monitor: System-GSLB-Ping

Health Monitor Scope: ● All Members ○ Only Non Avi Members

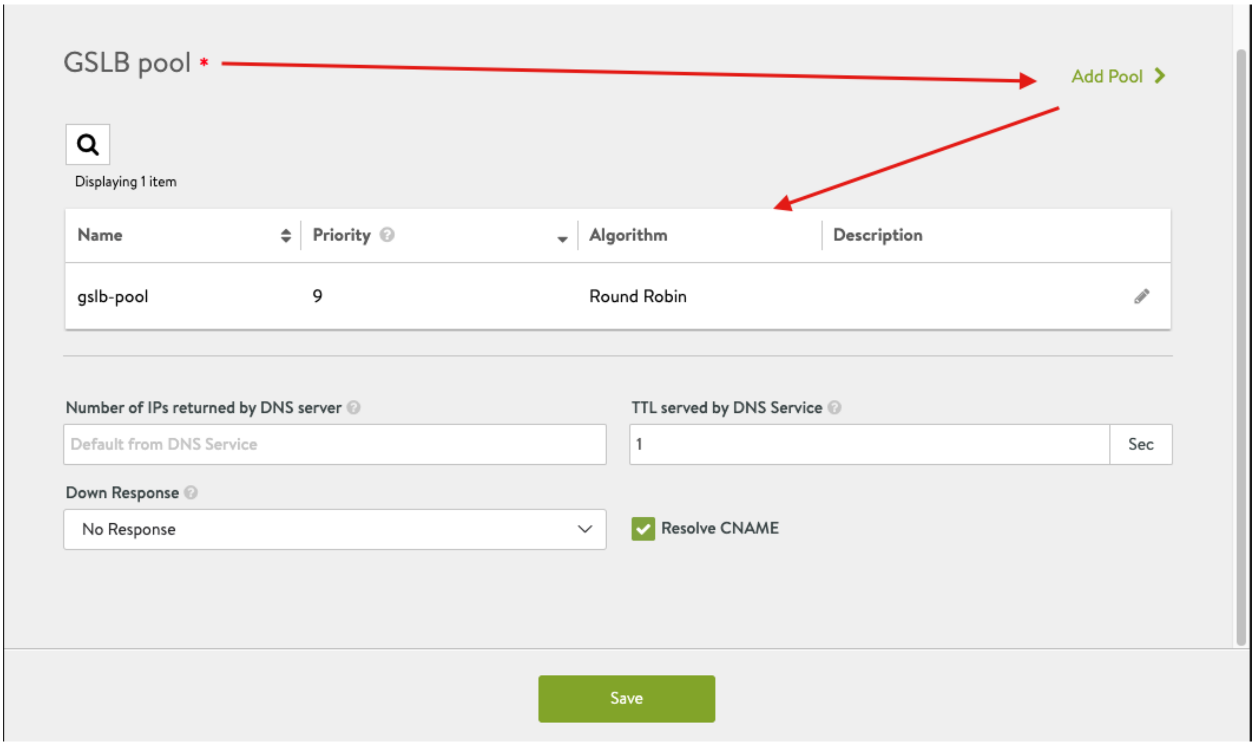
☑ Controller Health Status

Groups Load Balancing Algorithm: Priority-based

□ Site Persistence

Minimum number of Servers: 0

3. Scroll down to GSLB Pools and select Add Pool



GSLB pool *

Add Pool

Displaying 1 item

Name	Priority	Algorithm	Description
gslb-pool	9	Round Robin	

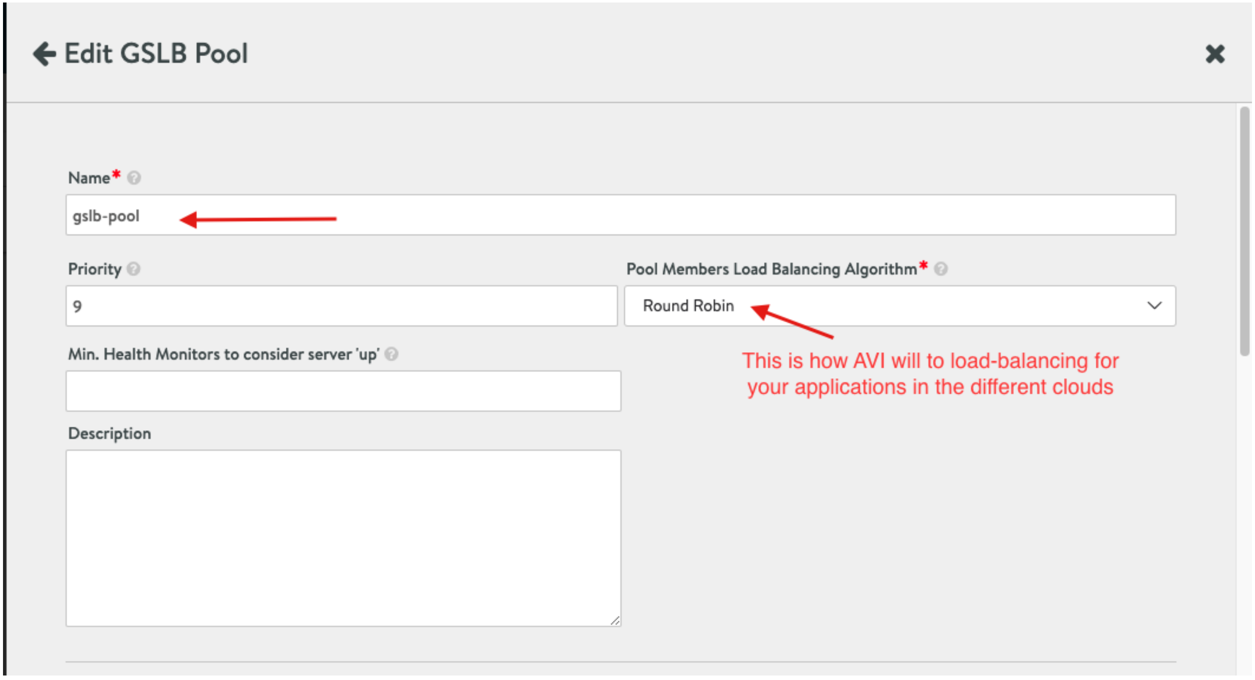
Number of IPs returned by DNS server: Default from DNS Service

TTL served by DNS Service: 1 Sec

Down Response: No Response

☑ Resolve CNAME

4. Apply the following configuration, however, please note that you might need to revisit this section after completing your VMC, GCvE and OCvS sections to populate the required information.



Edit GSLB Pool

Name*: gslb-pool

Priority: 9

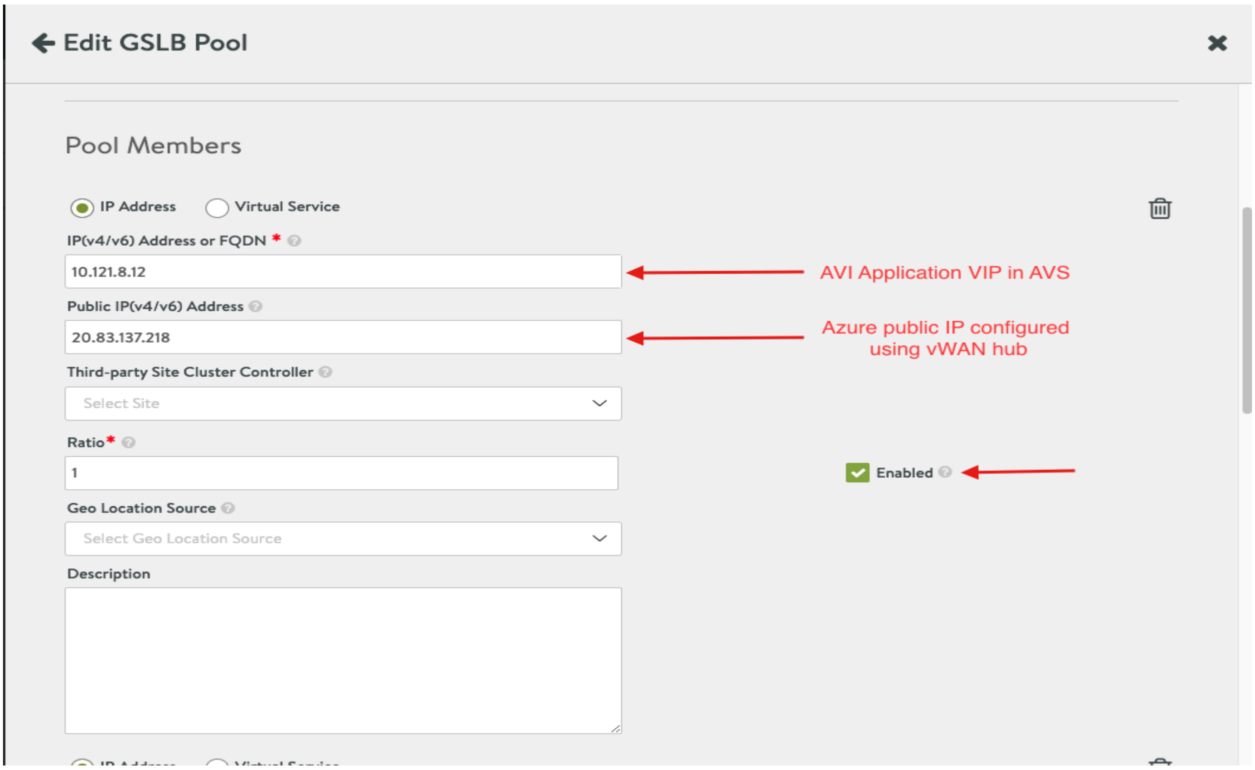
Pool Members Load Balancing Algorithm*: Round Robin

Min. Health Monitors to consider server 'up':

Description:

This is how AVI will to load-balancing for your applications in the different clouds

Please note, you have two options of adding Pool Member, I chose the IP Address, however, best practice is to add Pool members as Virtual service, my intention was to show you the IP addresses applied for each service.



Edit GSLB Pool

Pool Members

● IP Address ○ Virtual Service

IP(v4/v6) Address or FQDN *: 10.121.8.12

Public IP(v4/v6) Address: 20.83.137.218

Third-party Site Cluster Controller: Select Site

Ratio*: 1

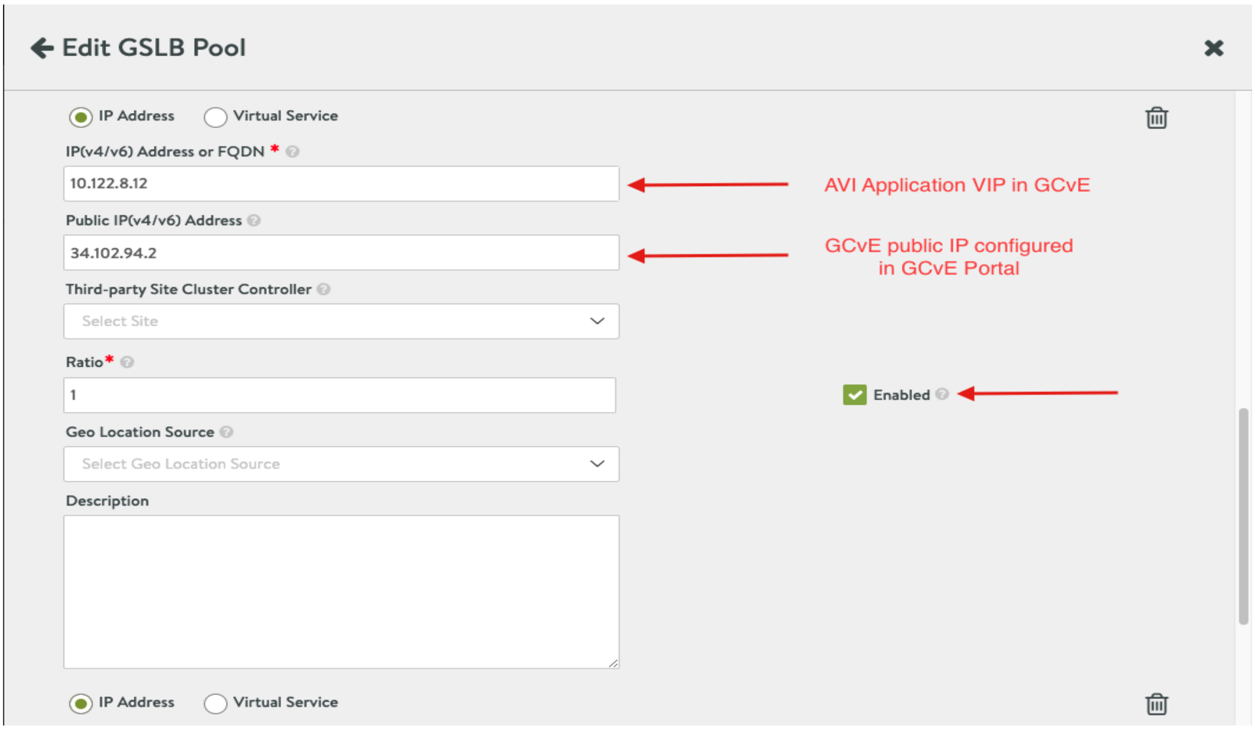
☑ Enabled

Geo Location Source: Select Geo Location Source

Description:

AVI Application VIP in AVS

Azure public IP configured using vWAN hub



Edit GSLB Pool

● IP Address ○ Virtual Service

IP(v4/v6) Address or FQDN *: 10.122.8.12

Public IP(v4/v6) Address: 34.102.94.2

Third-party Site Cluster Controller: Select Site

Ratio*: 1

☑ Enabled

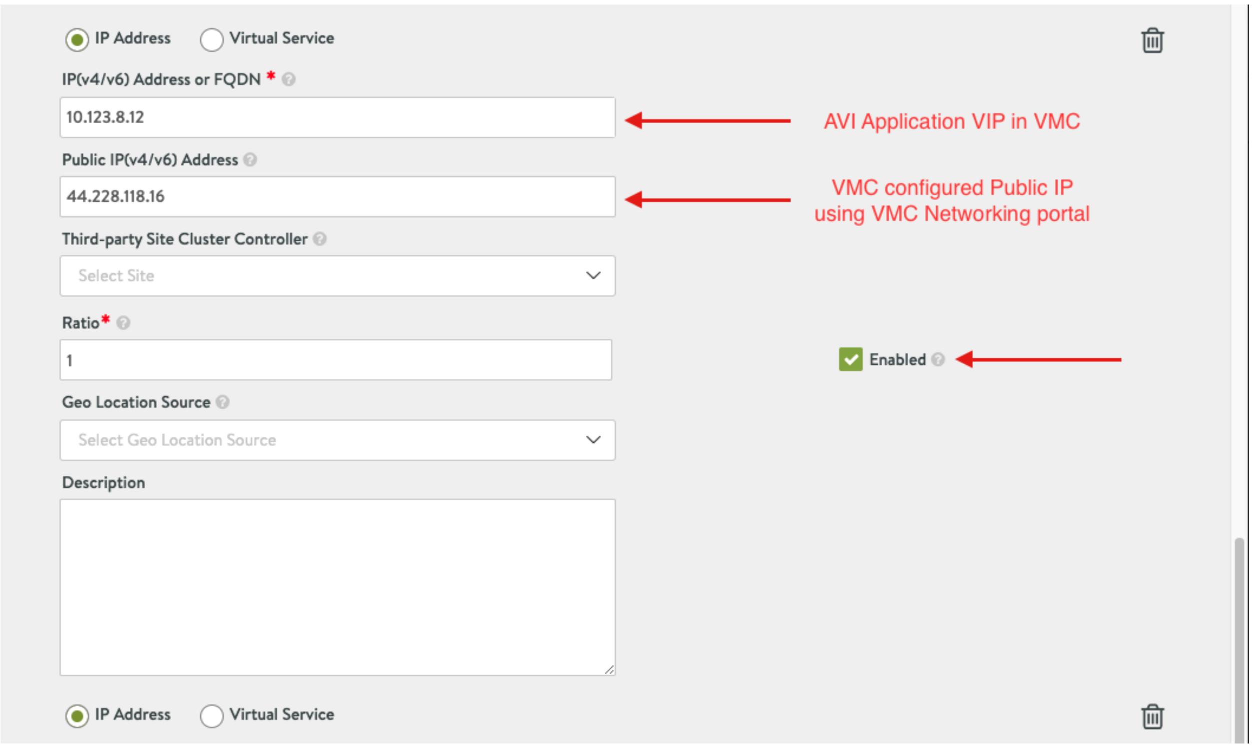
Geo Location Source: Select Geo Location Source

Description:

● IP Address ○ Virtual Service

AVI Application VIP in GCvE

GCvE public IP configured in GCvE Portal



● IP Address ○ Virtual Service

IP(v4/v6) Address or FQDN *

10.123.8.12

AVI Application VIP in VMC

Public IP(v4/v6) Address

44.228.118.16

VMC configured Public IP using VMC Networking portal

Third-party Site Cluster Controller

Select Site

Ratio*

1

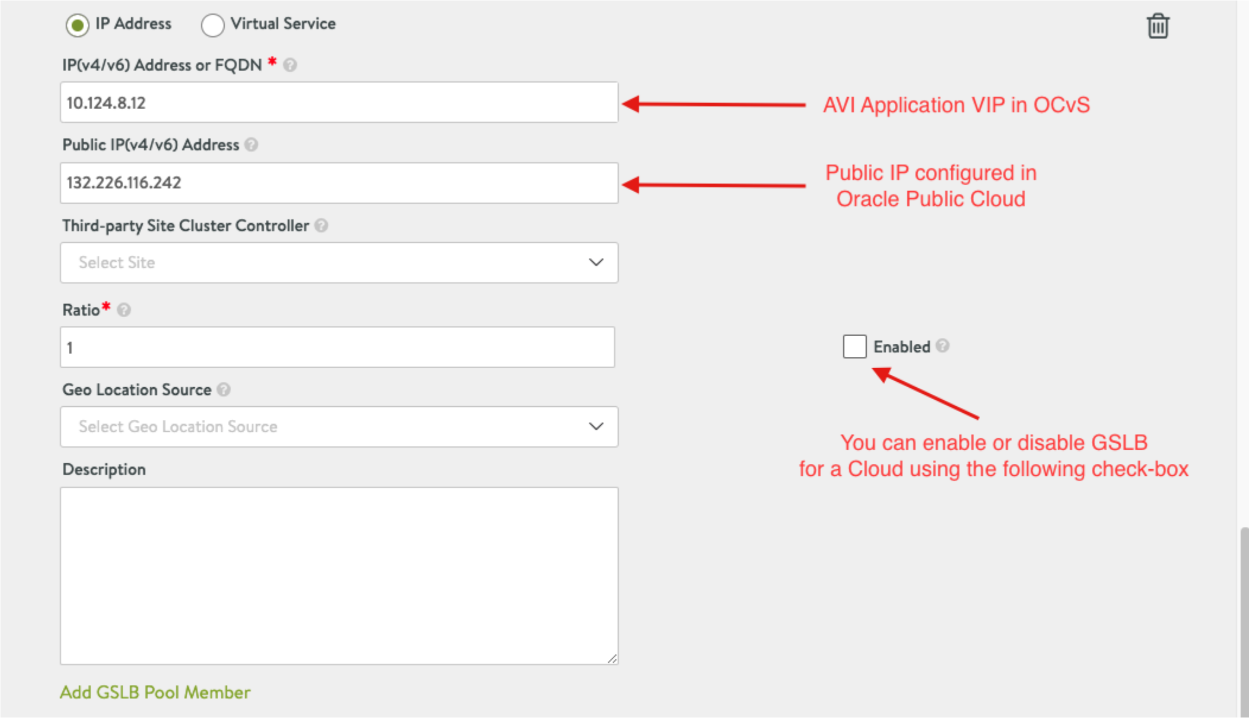
☑ Enabled

Geo Location Source

Select Geo Location Source

Description

● IP Address ○ Virtual Service



● IP Address ○ Virtual Service

IP(v4/v6) Address or FQDN *

10.124.8.12

AVI Application VIP in OCvS

Public IP(v4/v6) Address

132.226.116.242

Public IP configured in Oracle Public Cloud

Third-party Site Cluster Controller

Select Site

Ratio*

1

☐ Enabled

You can enable or disable GSLB for a Cloud using the following check-box

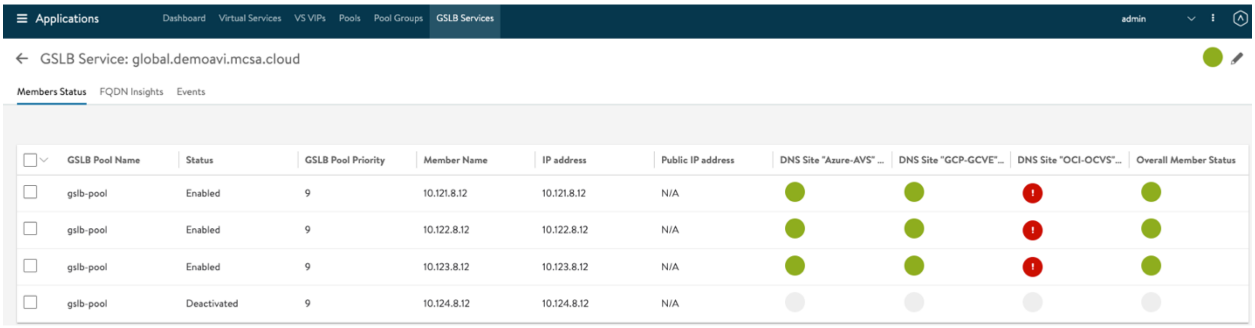
Geo Location Source

Select Geo Location Source

Description

Add GSLB Pool Member

5. Once all the Cloud configuration has been applied you can select **done**.
6. Hit the GSLB Service link created after your last configuration, you should have a similar view to the following image, please note if any of your clouds are still initializing or running into some errors you should see Location un-available, in my case below my Oracle cloud is still initializing. Please do not move on unless all your clouds are green.

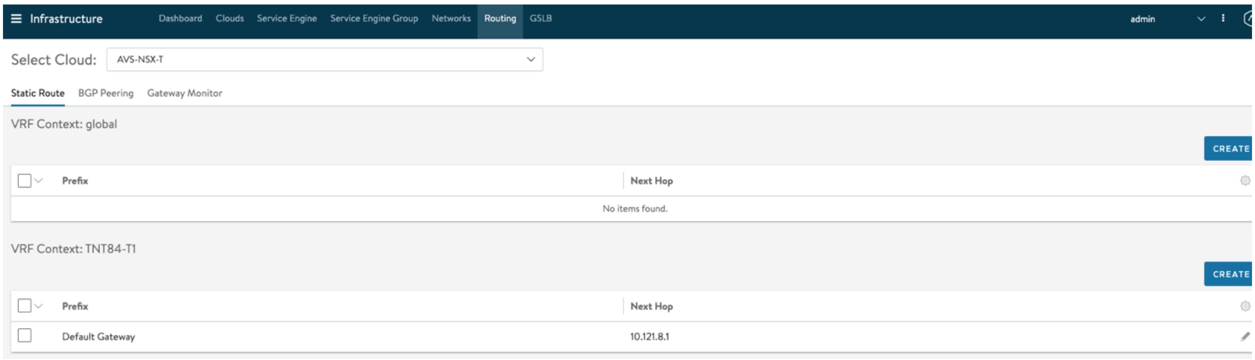


GSLB Service: global.demoavi.mcsa.cloud

	GSLB Pool Name	Status	GSLB Pool Priority	Member Name	IP address	Public IP address	DNS Site "Azure-AVS" ...	DNS Site "GCP-GCVE"...	DNS Site "OCI-OCVS"...	Overall Member Status
□	gslb-pool	Enabled	9	10.121.8.12	10.121.8.12	N/A	●	●	!	●
□	gslb-pool	Enabled	9	10.122.8.12	10.122.8.12	N/A	●	●	!	●
□	gslb-pool	Enabled	9	10.123.8.12	10.123.8.12	N/A	●	●	!	●
□	gslb-pool	Deactivated	9	10.124.8.12	10.124.8.12	N/A	○	○	○	○

In some cases, you might need to configure Routing for your default Gateway in AVI, this configuration routes all your traffic to the AVI VIP.

To apply this configuration, navigate to Infrastructure > Routing. Make sure to Select your AVS-NSX-T Cloud. Under VRF Context, Select Create and configure 10.121.8.1 as the Next Hop for your default Gateway



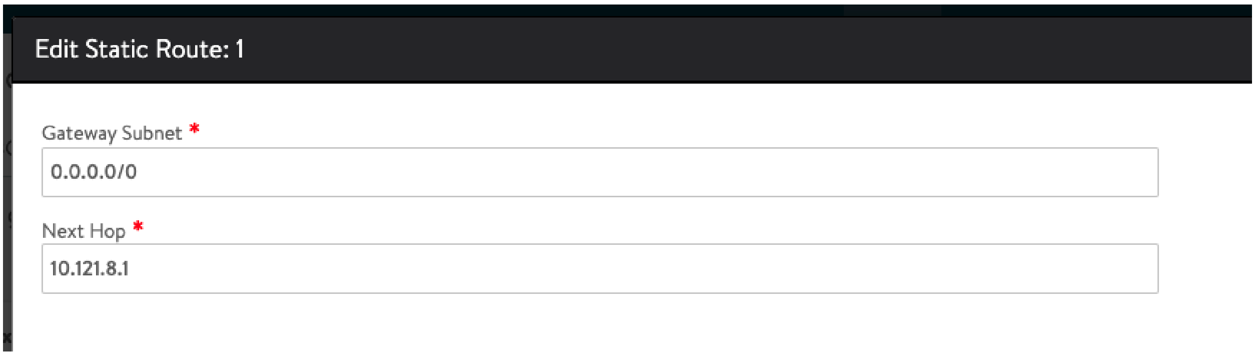
Select Cloud: AVS-NSX-T

VRF Context: global

Prefix	Next Hop
No items found.	

VRF Context: TNT84-T1

Prefix	Next Hop
Default Gateway	10.121.8.1



Edit Static Route: 1

Gateway Subnet *
0.0.0.0/0

Next Hop *
10.121.8.1

Azure Configuration requirements for GSLB

One of the key AVI-GSLB requirements for multi-cloud VMware SDDC architecture, is to allow ingress and egress traffic from Azure to VMware SDDC and vice versa. But why is this a requirement? To understand this concept please read the following lines.

Think of VMware's SDDC in Azure as a private isolated network that requires egress and ingress traffic management. Then, think of AVI GSLB as a network solution that allows users coming from external networks or even the internet and trying to access private workloads or applications in your isolated VMware SDDC in Azure.

Based on the previous statements and to make GSLB work we will need to allow external public traffic into the VMware private SDDC, this association requires some configuration on the public cloud side to allow traffic coming from the internet into Azure, then from Azure to VMware SDDC in the same for the opposite direction.

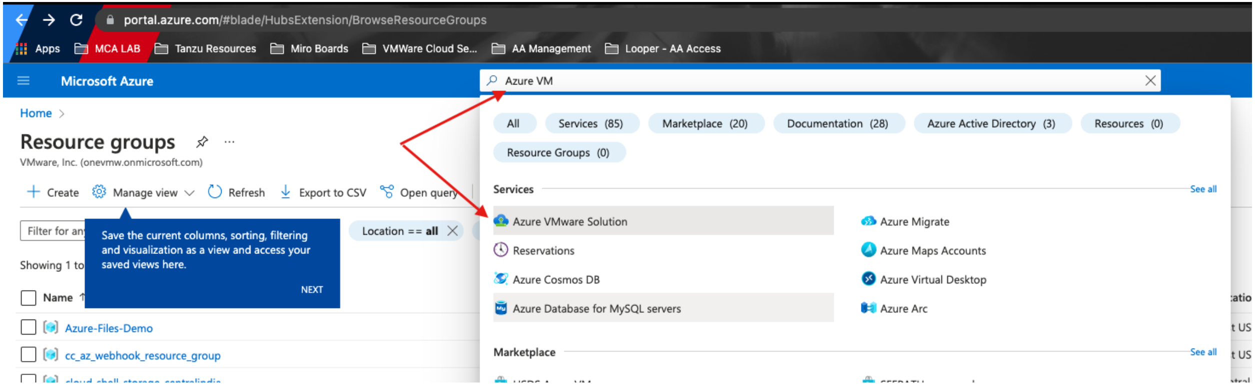
The association of public to private traffic is done using NAT'ing of public IPs to private IPs.

Please note, in this section I will only explain the configuration requirements for Azure, this configuration is **not** the same for all other public-cloud providers, for more information about each public cloud please see the dedicated section for each cloud.

** Azure does not allow public-IP configuration for Azure VMware Solution (AVS), for this reason I had to create a vWAN hub, on the vWAN hub I enabled a Firewall with a public-ip and couple Destination NAT rules.

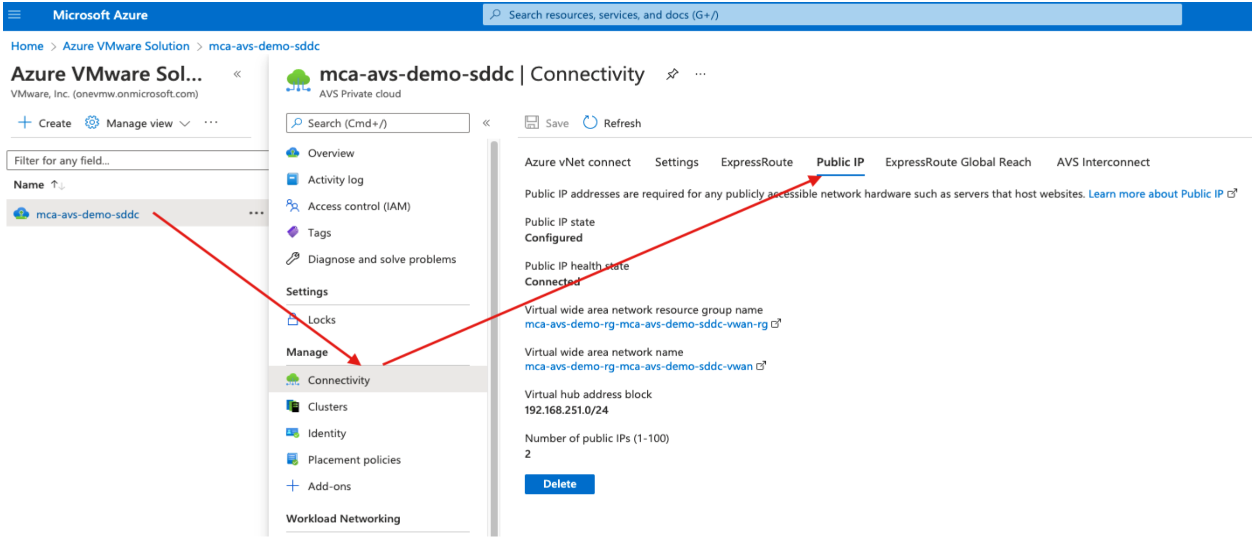
This is the only available way **today** to allow public traffic into the private VMware SDDC. Please visit the future work section for more information. **

1. Open your Azure portal, use the following link: portal.azure.com
2. In search bar, search for Azure VMware Solution (assuming you already configured AVS)



Save the current columns, sorting, filtering and visualization as a view and access your saved views here.

3. Select your SDDC
4. Under **Manage**, select **Connectivity** and select the **Public IP** tab



Public IP addresses are required for any publicly accessible network hardware such as servers that host websites. Learn more about Public IP

Public IP state
Configured

Public IP health state
Connected

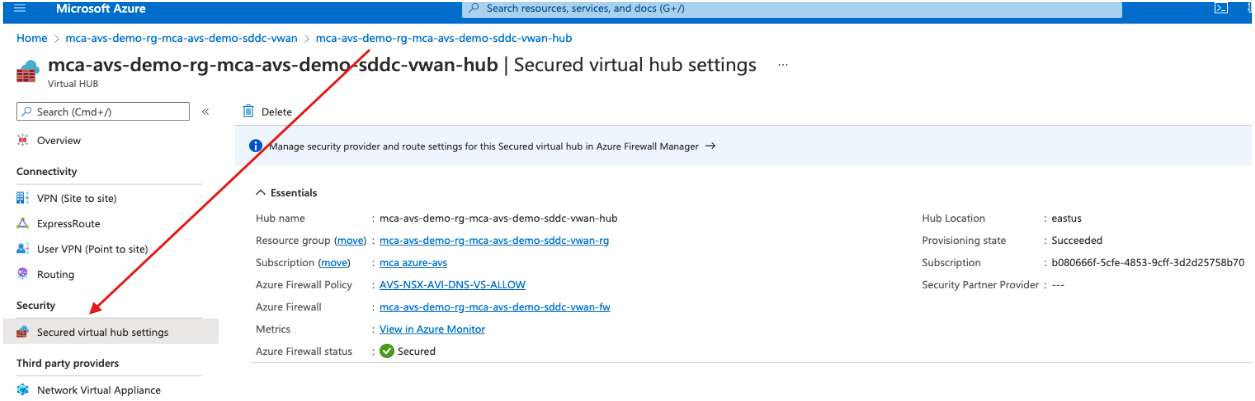
Virtual wide area network resource group name
mca-avs-demo-rg-mca-avs-demo-sddc-vwan-rg

Virtual wide area network name
mca-avs-demo-rg-mca-avs-demo-sddc-vwan

Virtual hub address block
192.168.251.0/24

Number of public IPs (1-100)
2

5. If you are configuring a public-ip for the first time you will see the option of configuring a public-ip, in my case this configuration was already done.
6. Click configure Public-ip, as mentioned previously, Azure will force you to configure a vWAN hub to all a public-ip for your SDDC. Starting April/May 2022, Azure will allow you to configure a public-ip without using vWAN hub, for more information check the future section on this document.
7. Go through the vWAN hub configuration, for more information about vWAN hub configuration please use the following link: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about
8. Once your vWAN hub is fully configured, you can now navigate to your hub to configure a vWAN Firewall, please note you will need this firewall to control ingress and egress traffic and to create DNAT (Destination NAT) rules to map your Public to private IP address.
9. In your vWAN hub, navigate to Security and select Secured virtual hub settings.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > mca-avs-demo-rg-mca-avs-demo-sddc-vwan > mca-avs-demo-rg-mca-avs-demo-sddc-vwan-hub
mca-avs-demo-rg-mca-avs-demo-sddc-vwan-hub | Secured virtual hub settings
Virtual HUB
Search (Cmd+/)
Overview
Connectivity
VPN (Site to site)
ExpressRoute
User VPN (Point to site)
Routing
Security
Secured virtual hub settings
Third party providers
Network Virtual Appliance
Delete
Essentials

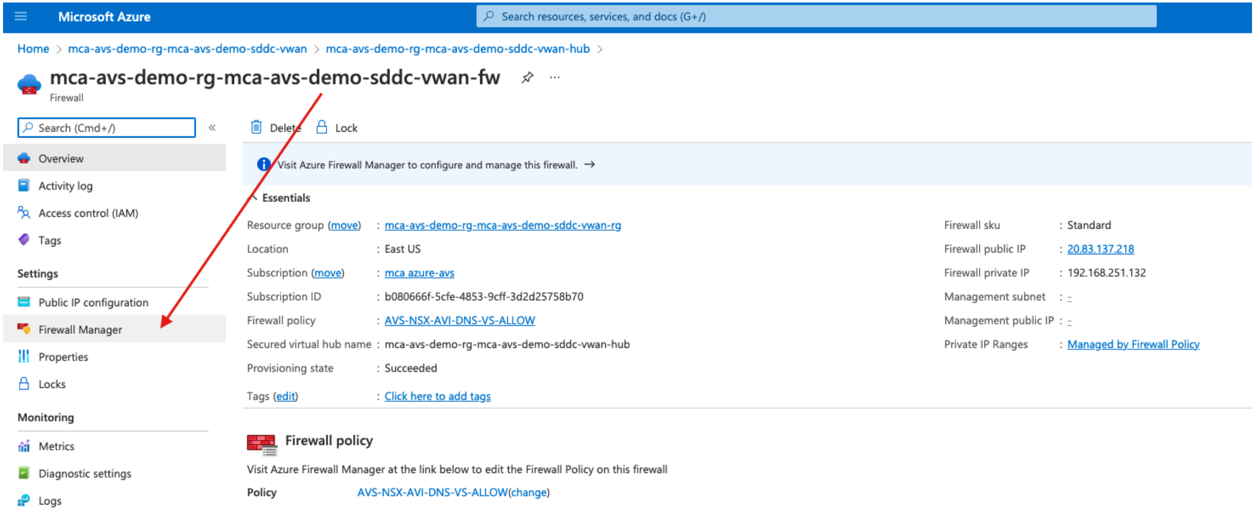
Manage security provider and route settings for this Secured virtual hub in Azure Firewall Manager →

Hub name : mca-avs-demo-rg-mca-avs-demo-sddc-vwan-hub
Resource group (move) : mca-avs-demo-rg-mca-avs-demo-sddc-vwan-rg
Subscription (move) : mca azure-avs
Azure Firewall Policy : AVS-NSX-AVI-DNS-VS-ALLOW
Azure Firewall : mca-avs-demo-rg-mca-avs-demo-sddc-vwan-fw
Metrics : View in Azure Monitor
Azure Firewall status : Secured

Hub Location : eastus
Provisioning state : Succeeded
Subscription : b080666f-5cfe-4853-9cff-3d2d25758b70
Security Partner Provider : ---

10. Navigate to vWAN FW on the right side, if you don't have the same view, use the search bar to find your vWAN FW, from there

navigate to Firewall Manager.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > mca-avs-demo-rg-mca-avs-demo-sddc-vwan > mca-avs-demo-rg-mca-avs-demo-sddc-vwan-hub
mca-avs-demo-rg-mca-avs-demo-sddc-vwan-fw
Firewall
Search (Cmd+/)
Delete
Lock
Overview
Activity log
Access control (IAM)
Tags
Settings
Public IP configuration
Firewall Manager
Properties
Locks
Monitoring
Metrics
Diagnostic settings
Logs
Visit Azure Firewall Manager to configure and manage this firewall. →
Essentials

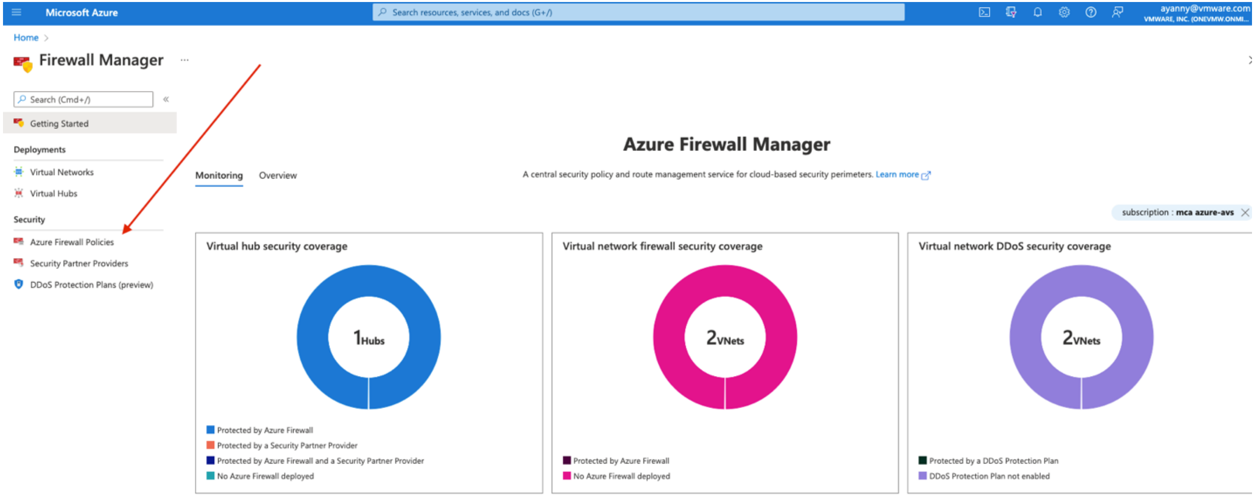
Resource group (move)	: mca-avs-demo-rg-mca-avs-demo-sddc-vwan-rg	Firewall sku	: Standard
Location	: East US	Firewall public IP	: 20.83.137.218
Subscription (move)	: mca azure-avs	Firewall private IP	: 192.168.251.132
Subscription ID	: b080666f-5cfe-4853-9cff-3d2d25758b70	Management subnet	: -
Firewall policy	: AVS-NSX-AVI-DNS-VS-ALLOW	Management public IP	: -
Secured virtual hub name	: mca-avs-demo-rg-mca-avs-demo-sddc-vwan-hub	Private IP Ranges	: Managed by Firewall Policy
Provisioning state	: Succeeded		
Tags (edit)	: Click here to add tags		

Firewall policy

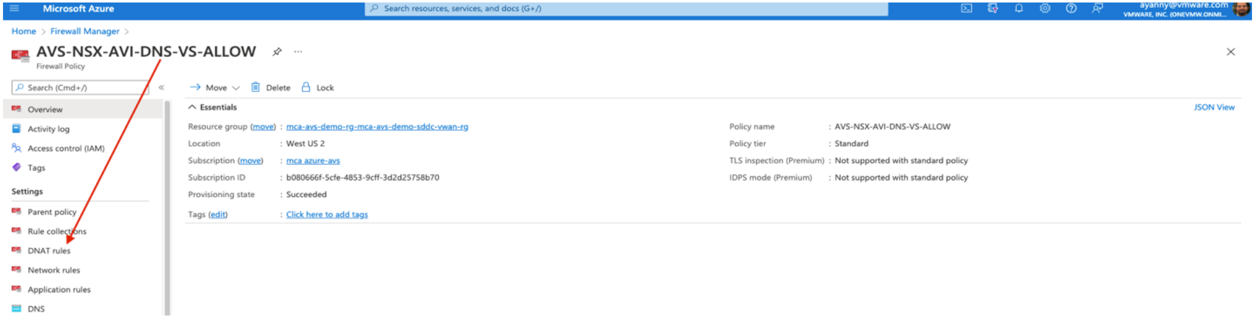
Visit Azure Firewall Manager at the link below to edit the Firewall Policy on this firewall

Policy AVS-NSX-AVI-DNS-VS-ALLOW(change)

11. Under Firewall manager navigate to Azure Firewall policies.

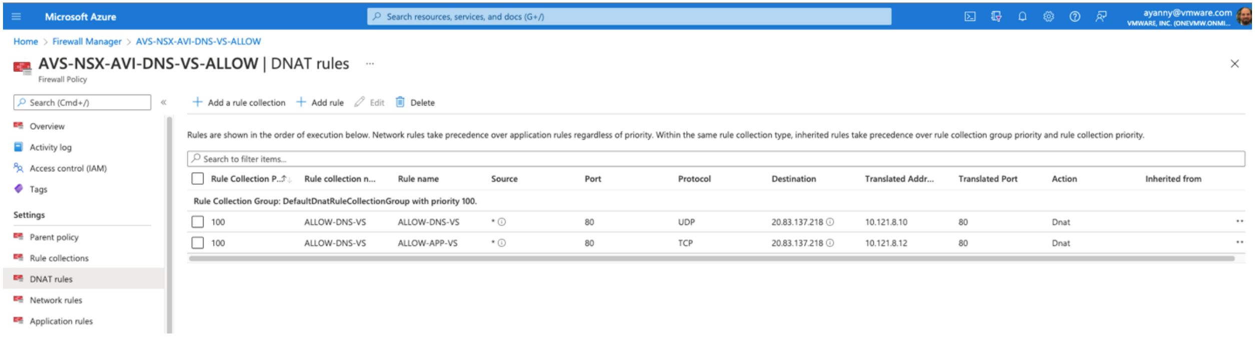

Microsoft Azure
Search resources, services, and docs (G+/)
ayanny@vmware.com
VMWARE, INC. (ONEVMW.ONMI...
Home >
Firewall Manager
Search (Cmd+/)
Getting Started
Deployments
Virtual Networks
Virtual Hubs
Security
Azure Firewall Policies
Security Partner Providers
DDoS Protection Plans (preview)
Azure Firewall Manager
Monitoring
Overview
A central security policy and route management service for cloud-based security perimeters. Learn more
subscription : mca azure-avs
Virtual hub security coverage
1Hubs
Protected by Azure Firewall
Protected by a Security Partner Provider
Protected by Azure Firewall and a Security Partner Provider
No Azure Firewall deployed
Virtual network firewall security coverage
2VNets
Protected by Azure Firewall
No Azure Firewall deployed
Virtual network DDoS security coverage
2VNets
Protected by a DDoS Protection Plan
DDoS Protection Plan not enabled

12. Select Create Azure Firewall Policy. Make sure to create the following DNAT rules to manage egress/ingress mapping once you create the Firewall policy.



Resource group (move)	: mca-avs-demo-rg-mca-avs-demo-sddc-vwan-rg	Policy name	: AVS-NSX-AVI-DNS-VS-ALLOW
Location	: West US 2	Policy tier	: Standard
Subscription (move)	: mca azure-avs	TLS inspection (Premium)	: Not supported with standard policy
Subscription ID	: b080666f-5cfe-4853-9cff-3d2d25758b70	IDPS mode (Premium)	: Not supported with standard policy
Provisioning state	: Succeeded		
Tags (edit)	: Click here to add tags		

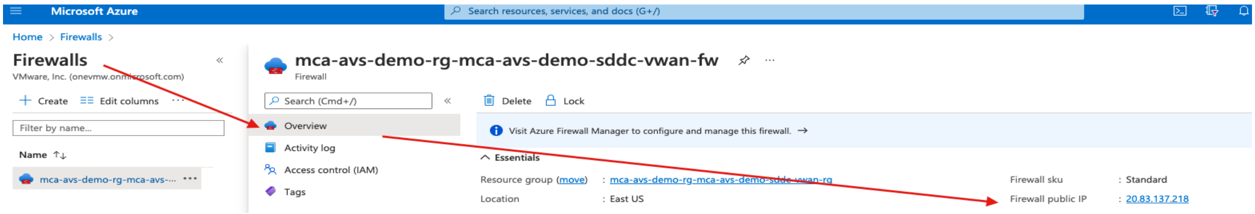
13. Apply the following DNAT configuration, make sure to apply the proper IPs as per your configurations.



Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

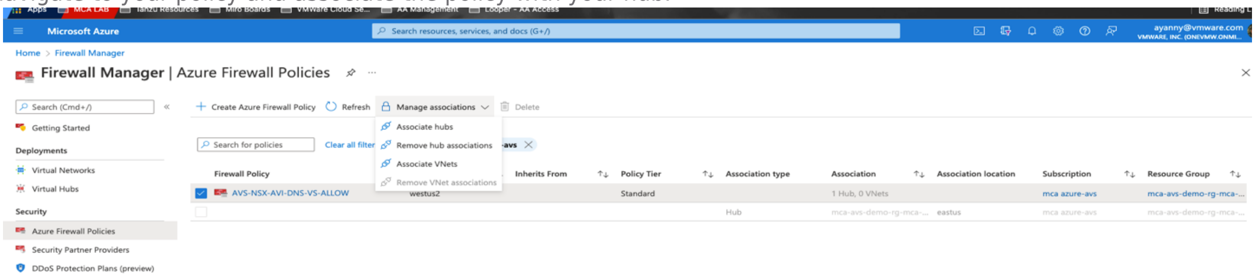
□ Rule Collection P...	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Translated Addr...	Translated Port	Action	Inherited from
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.										
□ 100	ALLOW-DNS-VS	ALLOW-DNS-VS	*	80	UDP	20.83.137.218	10.121.8.10	80	Dnat	
□ 100	ALLOW-DNS-VS	ALLOW-APP-VS	*	80	TCP	20.83.137.218	10.121.8.12	80	Dnat	

Please note, you can find the public-IP of your Firewall if you navigate to **firewall** and select **Overview**


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Firewalls >
Firewalls
VMware, Inc. (onevmw.onmicrosoft.com)
Create
Edit columns
Filter by name...
Name
mca-avs-demo-rg-mca-avs-...
mca-avs-demo-rg-mca-avs-demo-sddc-vwan-fw
Firewall
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Delete
Lock
Visit Azure Firewall Manager to configure and manage this firewall. →
Essentials

Resource group (move) : mca-avs-demo-rg-mca-avs-demo-sddc-vwan-rg
Location : East US
Firewall sku : Standard
Firewall public IP : 20.83.137.218

14. Finally navigate to your policy and associate the policy with your hub.



Firewall Policy		Inherits From	Policy Tier	Association type	Association	Association location	Subscription	Resource Group
☑ AVS-NSX-AVI-DNS-VS-ALLOW	westus2		Standard		1 Hub, 0 VNets		mca azure-avs	mca-avs-demo-rg-mca-...
□				Hub	mca-avs-demo-rg-mca-...	eastus	mca azure-avs	mca-avs-demo-rg-mca-...

Assuming your Global DNS configuration is fully completed, if you navigate to http://global.demoavi.mcsa.cloud/ you should be able to reach your AVS private workload

Deploy AVI-GSLB on Google Cloud VMware Solution

To deploy AVI-GSLB on Google Cloud VMware Solution you will need to follow similar steps discussed on the following location on this document here

Configure NSX-T networking as per instructions show in here

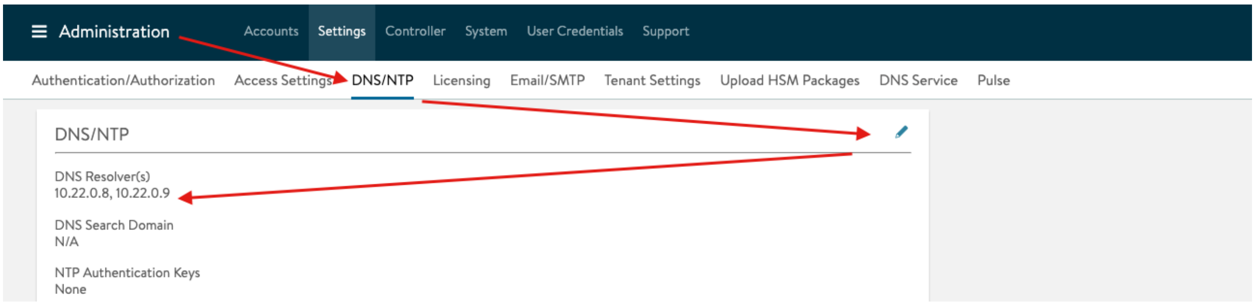
Once AVI is installed, you can configure AVI GSLB, for more information follow steps discuss in the following location on this document here

AVI general Installation and initial configuration guide here or follow the following link: https://avinetworks.com/docs/21.1/avi-deployment-guide-for-google-cloud-platform-gcp/

Note, although GSLB configuration is very similar on most of the SDDCs, you will notice that GSLB configuration is **only** allowed at the Azure VMware Solution because it is the GSLB leader.

DNS Configuration Tip:

In some cases, you will need to configure DNS resolvers for your AVI controller. The required DNS resolvers are the Google Cloud VMware Solution DNS IPs. To apply the following configuration, you need to access your AVI controller and navigate to Administration > DNS/NTP, then add the GCvE private DNS resolvers:



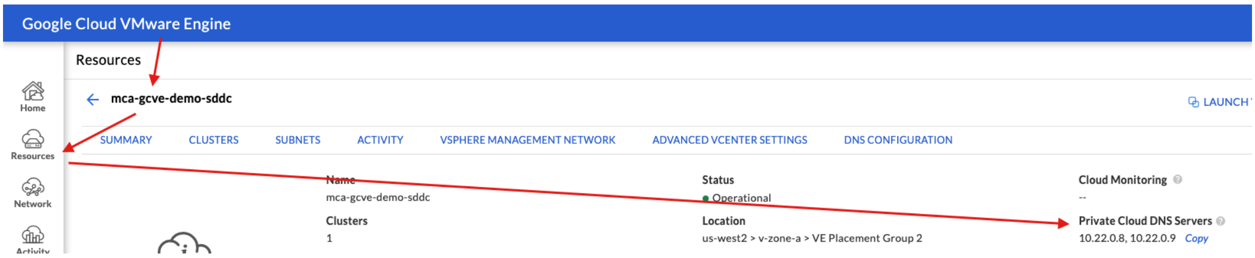
DNS/NTP

DNS Resolver(s)
10.22.0.8, 10.22.0.9

DNS Search Domain
N/A

NTP Authentication Keys
None

You can locate the GCvE DNS resolvers by accessing your GCvE Solution in GCP, then navigate to **Resources** > **Summary**



Name
mca-gcve-demo-sddc

Clusters
1

Status
● Operational

Location
us-west2 > v-zone-a > VE Placement Group 2

Cloud Monitoring
--

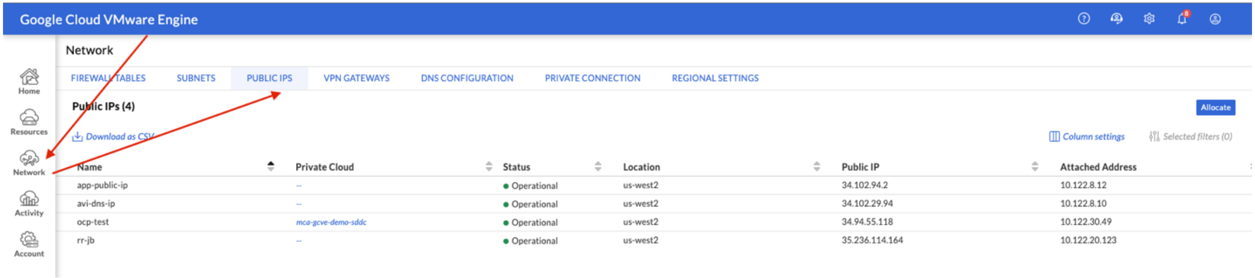
Private Cloud DNS Servers
10.22.0.8, 10.22.0.9 Copy

Google Configuration requirements for GSLB

As previously discussed, public cloud configurations for the VMware SDDCs are different for each cloud. That being said, we will discuss the required configuration to enable AVI GSLB for Google Cloud.

Assuming you already have Google Cloud VMware Solution already deployed

1. Navigate to your Google Cloud platform and search for Google Cloud VMware Solution in the search bar.
2. Navigate to Networks on the left side Menu and select Public IP, you need to create two public-ips and map the public-ips to two private-ips. One public-ip is required for the application VIP and the other public-ip is required for the DNS VIP.

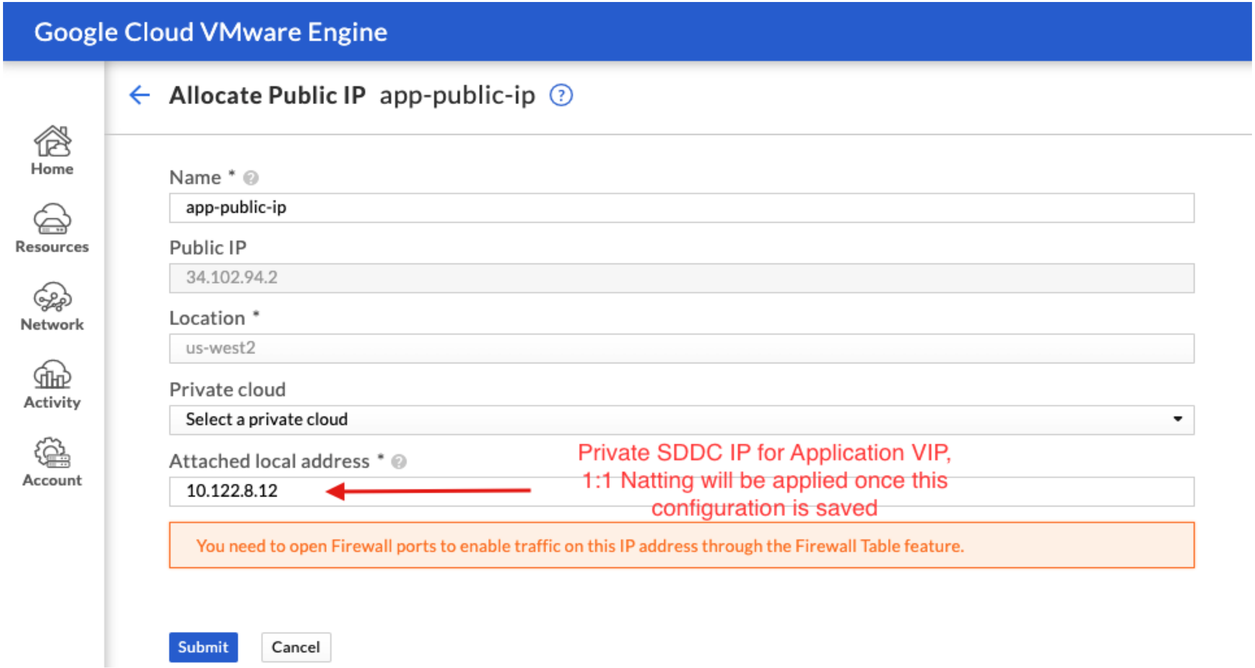


Public IPs (4)

Name	Private Cloud	Status	Location	Public IP	Attached Address
app-public-ip	--	● Operational	us-west2	34.102.94.2	10.122.8.12
avi-dns-ip	--	● Operational	us-west2	34.102.29.94	10.122.8.10
ocp-test	mca-gcve-demo-sddc	● Operational	us-west2	34.94.55.118	10.122.30.49
rr-jb	--	● Operational	us-west2	35.236.114.164	10.122.20.123

3. Select Allocate and apply the following configuration. By default, GCP will allocate a public IP for you, you need to add a Name

and Attach a local address. Google does 1:1 NATing by default once you apply this configuration. Once you apply the below configuration hit submit



Allocate Public IP app-public-ip

Name *
app-public-ip

Public IP
34.102.94.2

Location *
us-west2

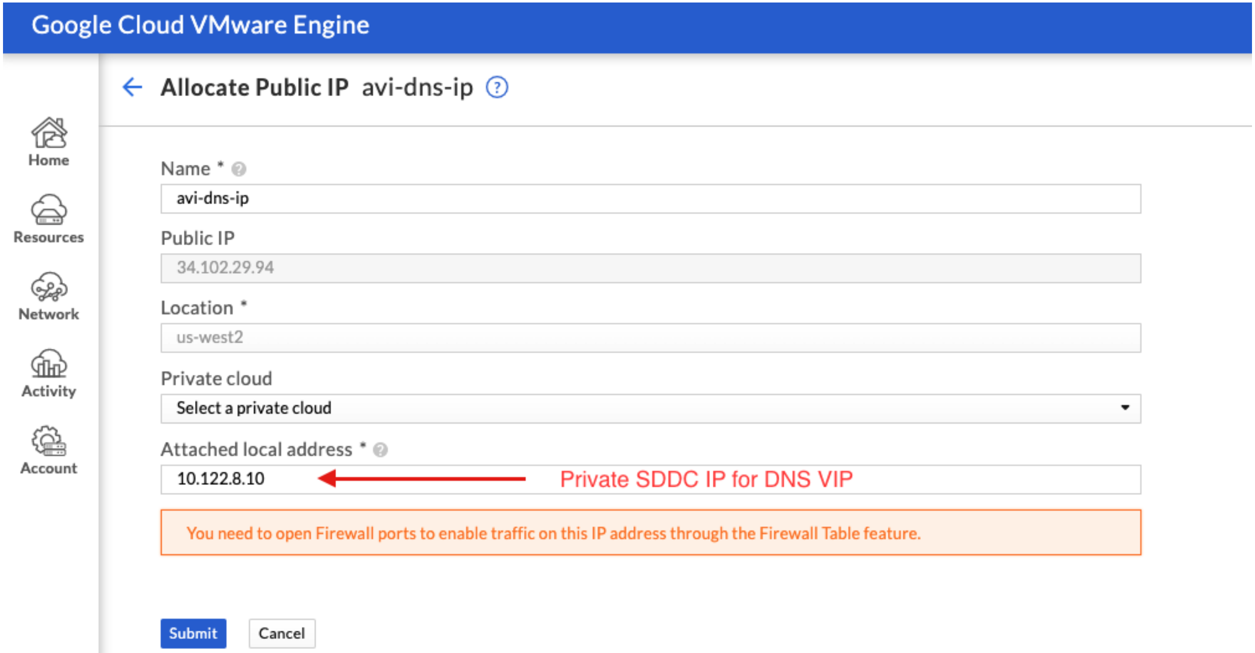
Private cloud
Select a private cloud

Attached local address *
10.122.8.12

Private SDDC IP for Application VIP, 1:1 Natting will be applied once this configuration is saved

You need to open Firewall ports to enable traffic on this IP address through the Firewall Table feature.

4. Select Allocation again and configure a DNS Public-ip mapping, once you apply the below configuration hit submit



Allocate Public IP avi-dns-ip

Name *
avi-dns-ip

Public IP
34.102.29.94

Location *
us-west2

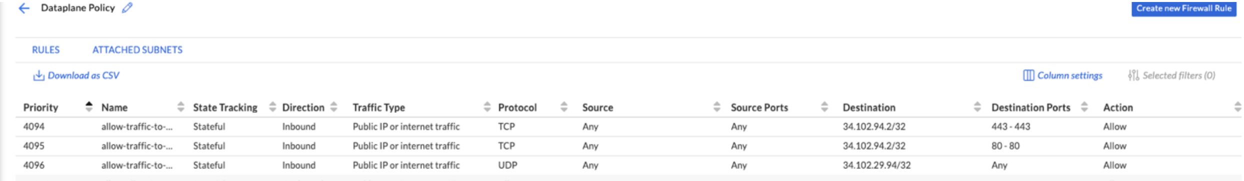
Private cloud
Select a private cloud

Attached local address *
10.122.8.10

Private SDDC IP for DNS VIP

You need to open Firewall ports to enable traffic on this IP address through the Firewall Table feature.

5. Next, we will need to allow traffic to flow between GCP and GCvE, this is the traffic coming from internet or external networks to our SDDC. To allow this, you need to navigate to **Firewall Tables** > **Create New Firewall Table** and allow traffic for the public/private IPs you created in the previous steps. Please make sure you allow traffic for ports 443 and port 80 as per below.



Priority	Name	State Tracking	Direction	Traffic Type	Protocol	Source	Source Ports	Destination	Destination Ports	Action
4094	allow-traffic-to-...	Stateful	Inbound	Public IP or internet traffic	TCP	Any	Any	34.102.94.2/32	443 - 443	Allow
4095	allow-traffic-to-...	Stateful	Inbound	Public IP or internet traffic	TCP	Any	Any	34.102.94.2/32	80 - 80	Allow
4096	allow-traffic-to-...	Stateful	Inbound	Public IP or internet traffic	UDP	Any	Any	34.102.29.94/32	Any	Allow

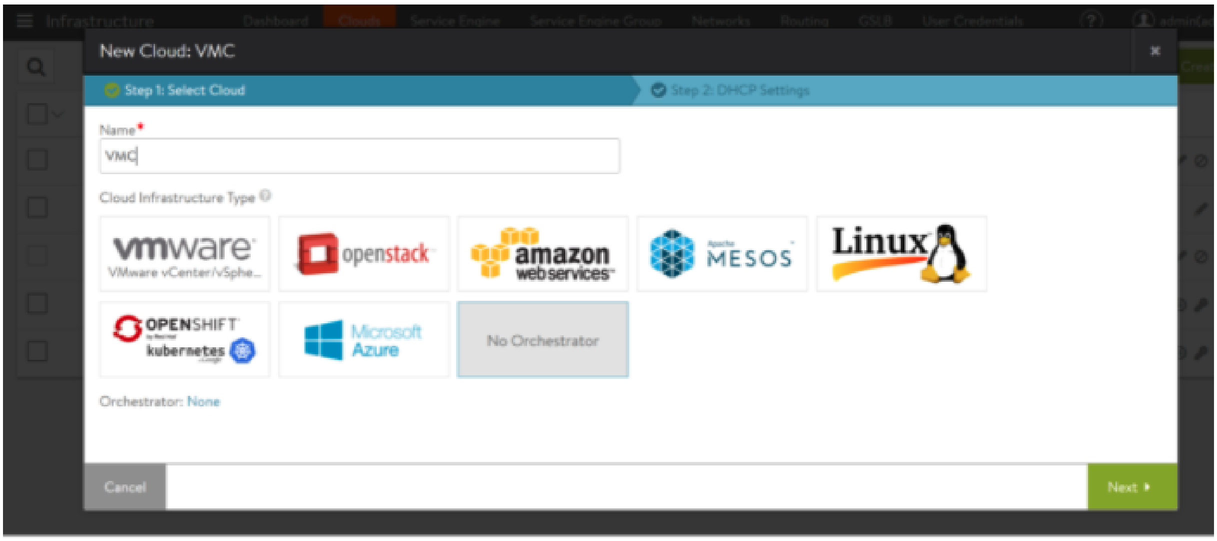
Assuming your DNS configuration is fully configured, if you navigate to your application address, you should be able to reach your AVS private workload. In my case (http://global.demoavi.mcsa.cloud/)

Architecture Note: GCP creates a small internet Gateway when you deploy Google Cloud VMware Solution. This Internet Gateway is what I used to control egress and ingress internet traffic to the VMware SDDC. It is not recommended to use this internet Gateway for your traffic, but rather deploy a GCP internet Gateway and use it for your SDDC ingress/egress traffic. For more information, please review the future work section.

Deploy AVI-GSLB on VMware Cloud on AWS

Deploying AVI on VMC on AWS is a slightly different process that the one explained for Azure (here). I recommend you visit the following link and follow the process to download, install and configure AVI: https://avinetworks.com/docs/20.1/avi-vantage-integration-with-vmware-cloud-on-aws/

You will find that the AVI Configuration process is straightforward, however, one thing to keep in mind is that you will need to choose the **No Orchestrator** Cloud for your VMC deployment.


New Cloud: VMC

Step 1: Select Cloud

Step 2: DHCP Settings

Name*

VMC

Cloud Infrastructure Type

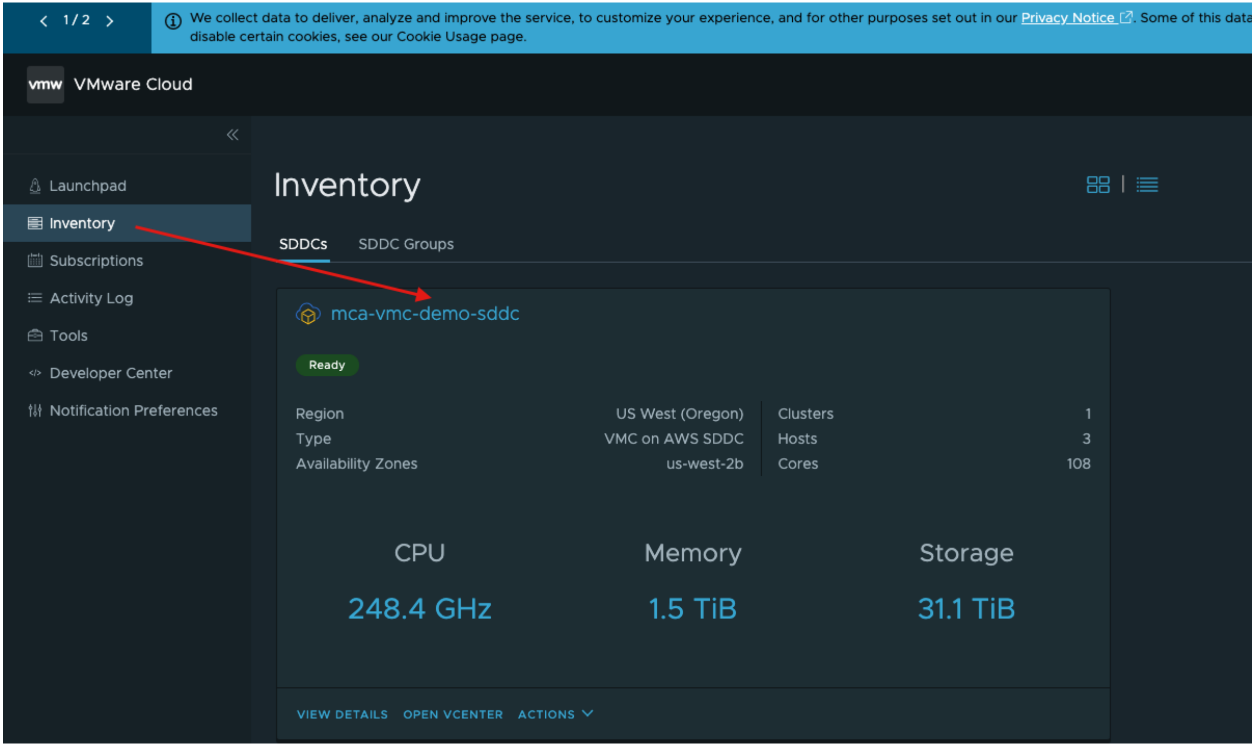
Orchestrator: None

VMware Cloud on AWS Networking and Security Configuration for AVI

After installing AVI in your VMC environment, you will need to configure networking and security in VMC to ensure that AVI can communicate with applications in your SDDC and the public networks and/or Internet.

Here are all the required steps you need on VMC on AWS.

1. Navigate to your SDDC in your vmc.vmware.com portal


We collect data to deliver, analyze and improve the service, to customize your experience, and for other purposes set out in our Privacy Notice. Some of this data disable certain cookies, see our Cookie Usage page.

Inventory

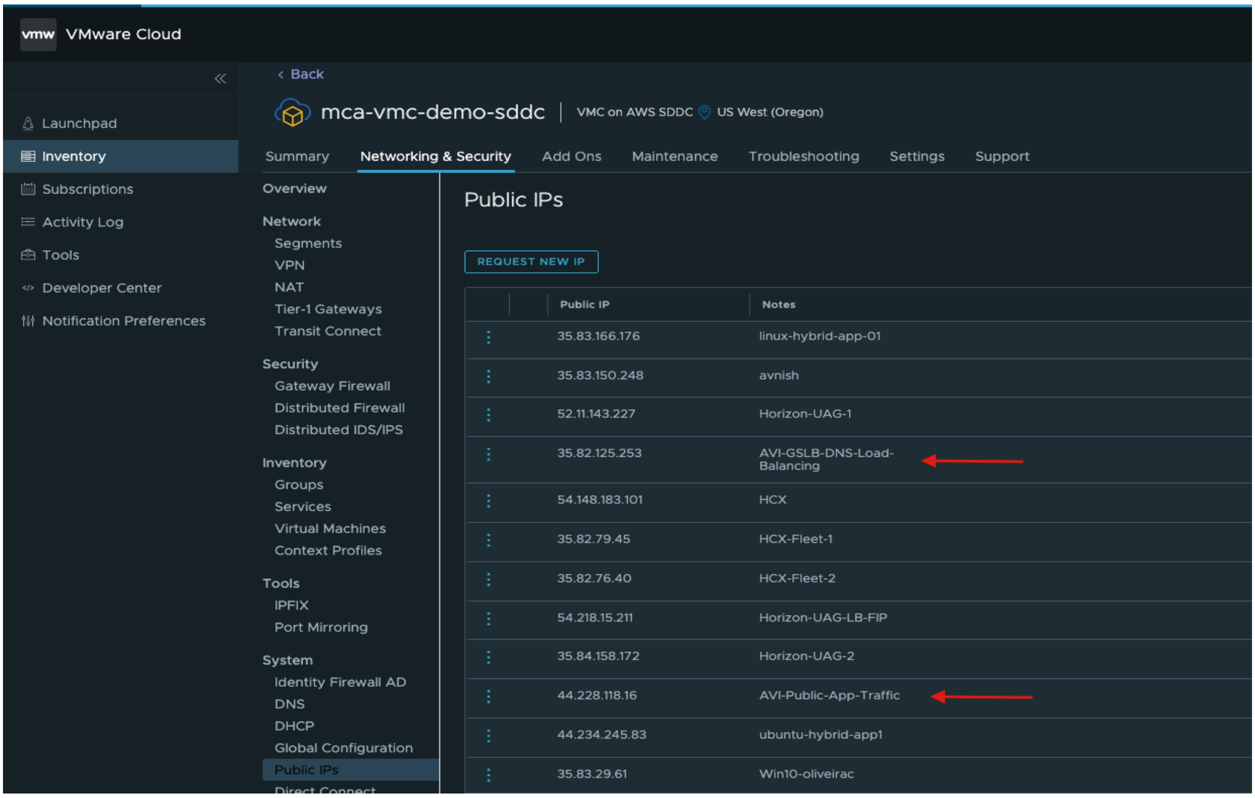
mca-vmc-demo-sddc

Ready

Region	US West (Oregon)	Clusters	1
Type	VMC on AWS SDDC	Hosts	3
Availability Zones	us-west-2b	Cores	108

CPU	Memory	Storage
248.4 GHz	1.5 TiB	31.1 TiB

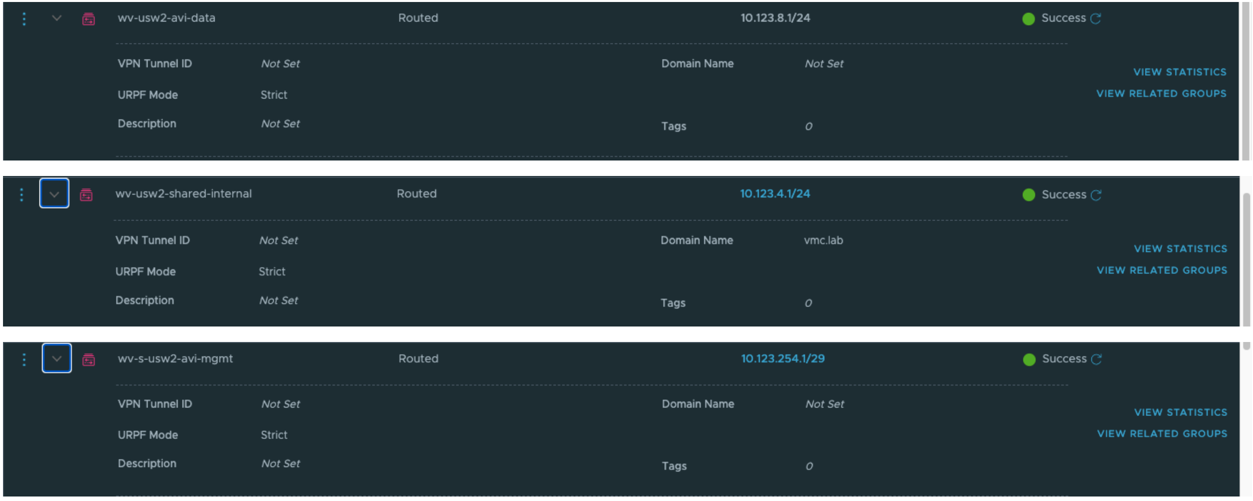
2. Select the **Networking & Security** tab then select **Public IPs**. Select Request New IP and add two IPs, one for your DNS-VS and a second one for the Application VS



Public IPs

Public IP	Notes
35.83.166.176	linux-hybrid-app-01
35.83.150.248	avnish
52.11.143.227	Horizon-UAG-1
35.82.125.253	AVI-GSLB-DNS-Load-Balancing
54.148.183.101	HCX
35.82.79.45	HCX-Fleet-1
35.82.76.40	HCX-Fleet-2
54.218.15.211	Horizon-UAG-LB-FIP
35.84.158.172	Horizon-UAG-2
44.228.118.16	AVI-Public-App-Traffic
44.234.245.83	ubuntu-hybrid-app1
35.83.29.61	Win10-oliveirac

3. Navigate to **Networking & Security** > **Segments**. We will need to configure NSX Segments for AVI. Wv-usw2-avi-data (10.123.8.1/24), wv-usw2-shared-internal (10.123.4.1/24) and wv-s-usw-avi-mgmt (10.123.254.1/29). Configuring segments is as easy as selecting Add Segment.


wv-usw2-avi-data Routed 10.123.8.1/24 Success

VPN Tunnel ID: Not Set
URPF Mode: Strict
Description: Not Set
Domain Name: Not Set
Tags: 0

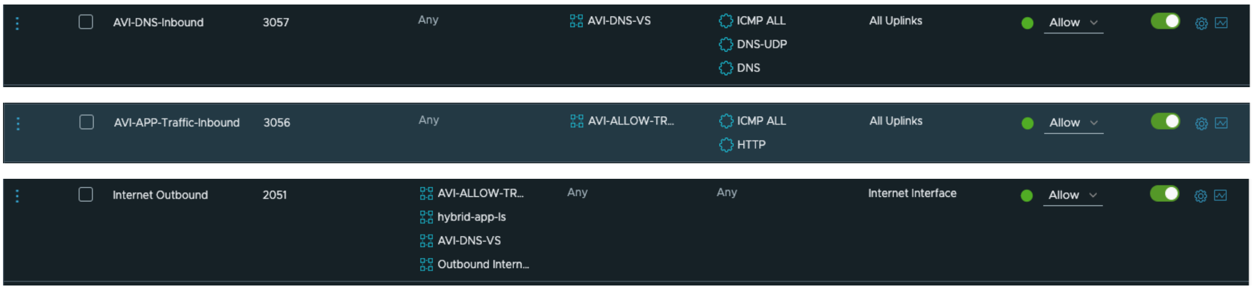
wv-usw2-shared-internal Routed 10.123.4.1/24 Success

VPN Tunnel ID: Not Set
URPF Mode: Strict
Description: Not Set
Domain Name: vmc.lab
Tags: 0

wv-s-usw2-avi-mgmt Routed 10.123.254.1/29 Success

VPN Tunnel ID: Not Set
URPF Mode: Strict
Description: Not Set
Domain Name: Not Set
Tags: 0

4. Next, we will need to configure Security to manage our egress and ingress traffic for our SDDC. Navigate to **Network & Security** > **Security** > **Gateway Firewall**. Select Add Rule and create the following rules to allow inbound and outbound traffic.

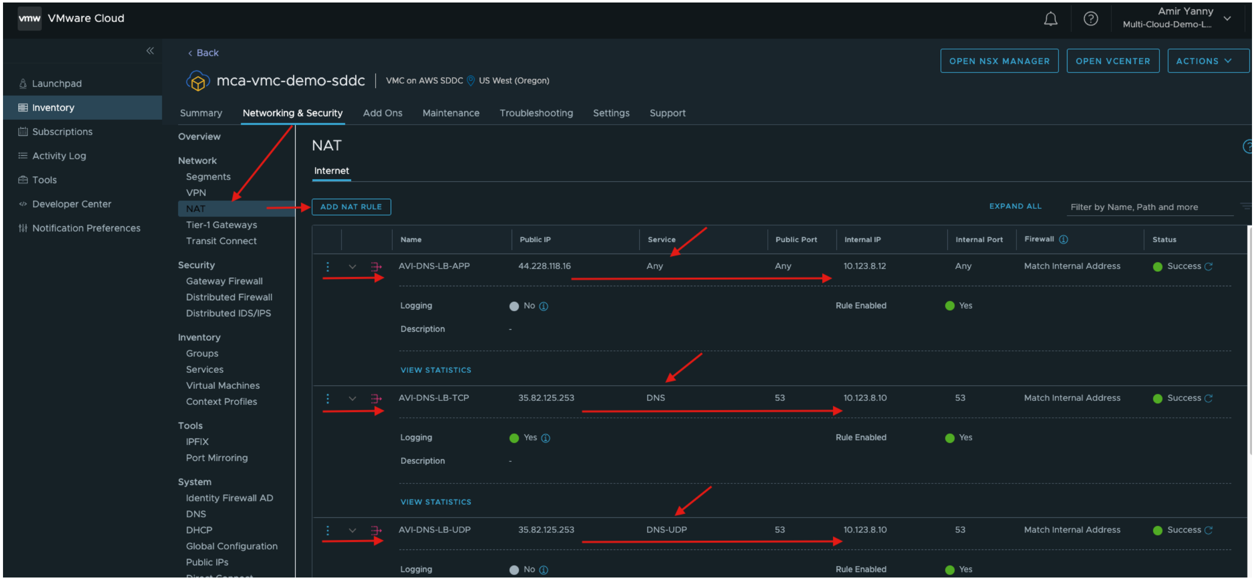


□	AVI-DNS-Inbound	3057	Any	AVI-DNS-VS	ICMP ALL DNS-UDP DNS	All Uplinks	● Allow
□	AVI-APP-Traffic-Inbound	3056	Any	AVI-ALLOW-TR...	ICMP ALL HTTP	All Uplinks	● Allow
□	Internet Outbound	2051	AVI-ALLOW-TR... hybrid-app-ls AVI-DNS-VS Outbound Intern...	Any	Any	Internet Interface	● Allow

Note, it is recommended to configure Groups under Inventory for ease of management.

5. Finally, we need to configure NAT, to map the external IPs to the internal IPs. Navigate to Networking & Security > Network >

NAT > ADD NAT RULE and add the following NAT Rules.



NAT

Name	Public IP	Service	Public Port	Internal IP	Internal Port	Firewall	Status
AVI-DNS-LB-APP	44.228.118.16	Any	Any	10.123.8.12	Any	Match Internal Address	● Success
AVI-DNS-LB-TCP	35.82.125.253	DNS	53	10.123.8.10	53	Match Internal Address	● Success
AVI-DNS-LB-UDP	35.82.125.253	DNS-UDP	53	10.123.8.10	53	Match Internal Address	● Success

AVI-DNS-LB-APP: Logging ● No; Rule Enabled ● Yes; Description -

AVI-DNS-LB-TCP: Logging ● Yes; Rule Enabled ● Yes; Description -

AVI-DNS-LB-UDP: Logging ● No; Rule Enabled ● Yes

For more information on AVI virtual services and pool configurations, please follow instructions in here.

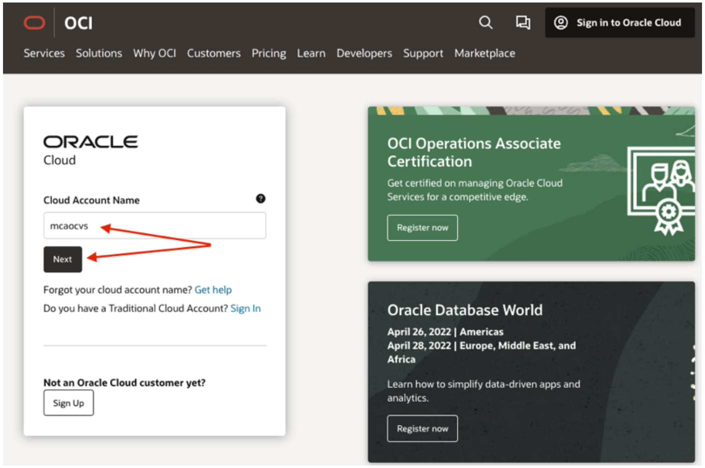
Assuming your DNS configuration is fully configured, if you navigate to your application address, you should be able to reach your VMC private workload. In my case (http://global.demoavi.mcsa.cloud/)

Deploy AVI-GSLB on Oracle Cloud VMware Solution

As previously discussed, public cloud configurations for the VMware SDDCs are different for each cloud. That being said, we will discuss the required configuration to enable AVI GSLB for Oracle Cloud Infrastructure.

Assuming you already have OCVS (Oracle Cloud VMware Solution) already deployed

1. Navigate to your OCI and access your Cloud Account Name (mcaocvs) and hit next



ORACLE Cloud

Cloud Account Name

mcaocvs

Next

Forgot your cloud account name? Get help

Do you have a Traditional Cloud Account? Sign In

Not an Oracle Cloud customer yet?

Sign Up

OCI Operations Associate Certification

Get certified on managing Oracle Cloud Services for a competitive edge.

Register now

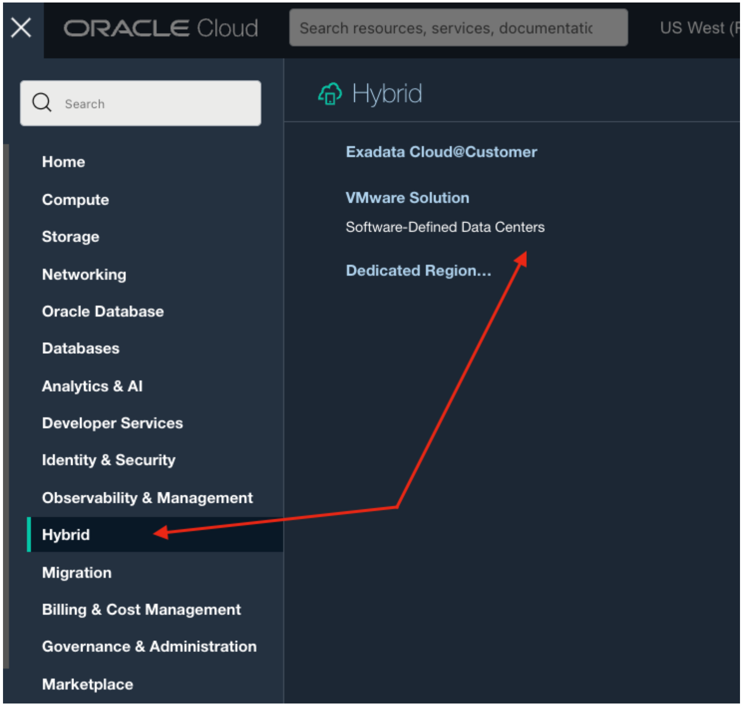
Oracle Database World

April 26, 2022 | Americas
April 28, 2022 | Europe, Middle East, and Africa

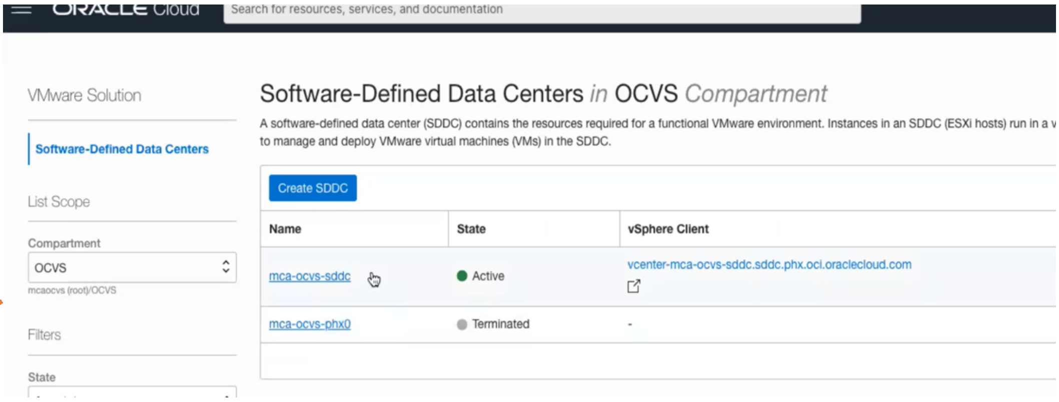
Learn how to simplify data-driven apps and analytics.

Register now

2. Using the Hamburger menu on the top left navigate to hybrid



3. Access your SDDC

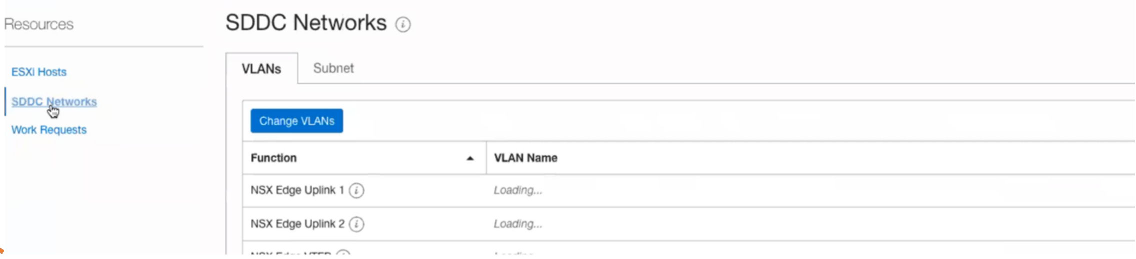


Software-Defined Data Centers *in* OCVS *Compartment*

A software-defined data center (SDDC) contains the resources required for a functional VMware environment. Instances in an SDDC (ESXi hosts) run in a v to manage and deploy VMware virtual machines (VMs) in the SDDC.

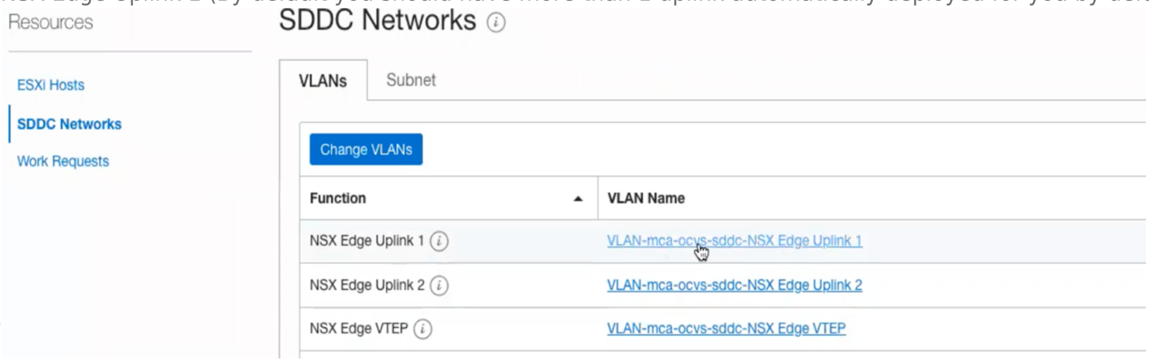
Name	State	vSphere Client
mca-ocvs-sddc	Active	vcenter-mca-ocvs-sddc.sddc.phx.oci.oraclecloud.com
mca-ocvs-phx0	Terminated	-

4. Scroll down and click on the networks tab (SDDC Networks)



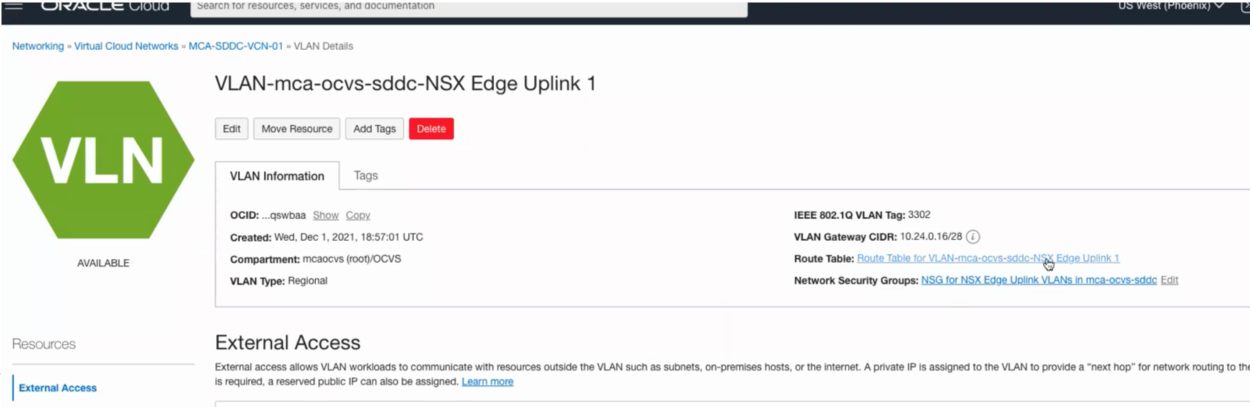
Function	VLAN Name
NSX Edge Uplink 1	*Loading...*
NSX Edge Uplink 2	*Loading...*

5. Now, click on NSX Edge Uplink 1 (By default you should have more than 1 uplink automatically deployed for you by default)



Function	VLAN Name
NSX Edge Uplink 1	VLAN-mca-ocvs-sddc-NSX Edge Uplink 1
NSX Edge Uplink 2	VLAN-mca-ocvs-sddc-NSX Edge Uplink 2
NSX Edge VTEP	VLAN-mca-ocvs-sddc-NSX Edge VTEP

6. Now, navigate to the route table on the right-hand side, we need to set a route a default route to send all traffic from our SDDC to hit the Internet Gateway.


ORACLE Cloud
Search for resources, services, and documentation
US West (Phoenix)
Networking » Virtual Cloud Networks » MCA-SDDC-VCN-01 » VLAN Details
VLN
AVAILABLE
Edit
Move Resource
Add Tags
Delete
VLAN Information
Tags
Resources
External Access

VLAN-mca-ocvs-sddc-NSX Edge Uplink 1

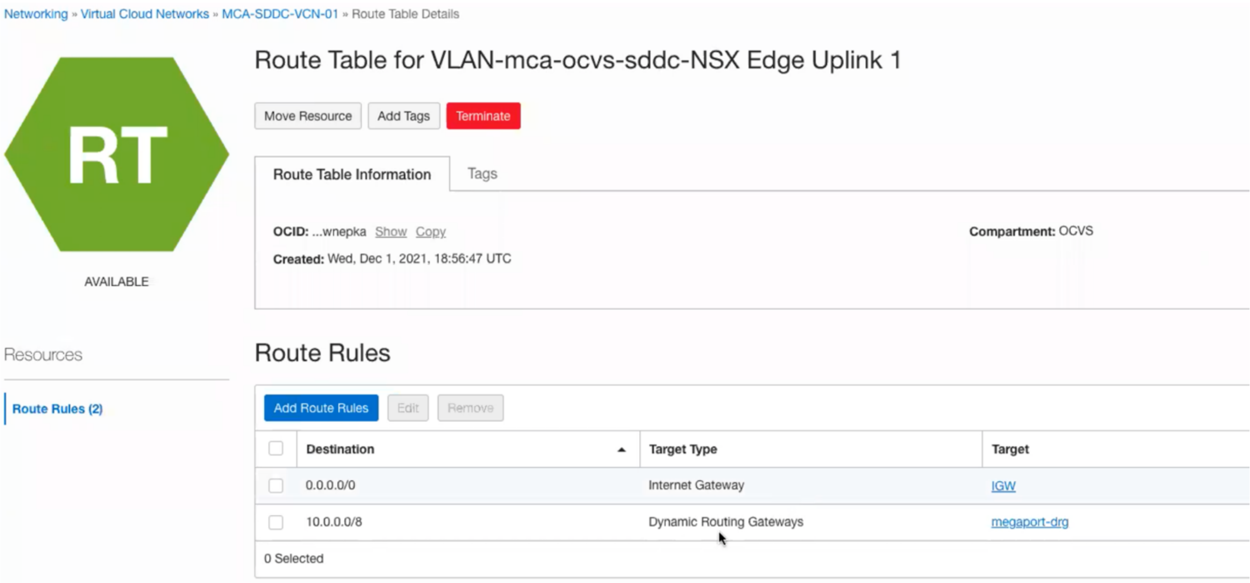
OCID: ...qswbaa Show Copy
Created: Wed, Dec 1, 2021, 18:57:01 UTC
Compartment: mcaocvs (root)/OCVS
VLAN Type: Regional

IEEE 802.1Q VLAN Tag: 3302
VLAN Gateway CIDR: 10.24.0.16/28
Route Table: Route Table for VLAN-mca-ocvs-sddc-NSX Edge Uplink 1
Network Security Groups: NSG for NSX Edge Uplink VLANs in mca-ocvs-sddc Edit

External Access

External access allows VLAN workloads to communicate with resources outside the VLAN such as subnets, on-premises hosts, or the internet. A private IP is assigned to the VLAN to provide a "next hop" for network routing to the is required, a reserved public IP can also be assigned. Learn more

7. Navigate to Add Route Rules and add a quad zero (0.0.0.0/0) with a next hop as IGW as per below



Networking » Virtual Cloud Networks » MCA-SDDC-VCN-01 » Route Table Details

Route Table for VLAN-mca-ocvs-sddc-NSX Edge Uplink 1

OCID: ...wnepka Show Copy

Created: Wed, Dec 1, 2021, 18:56:47 UTC

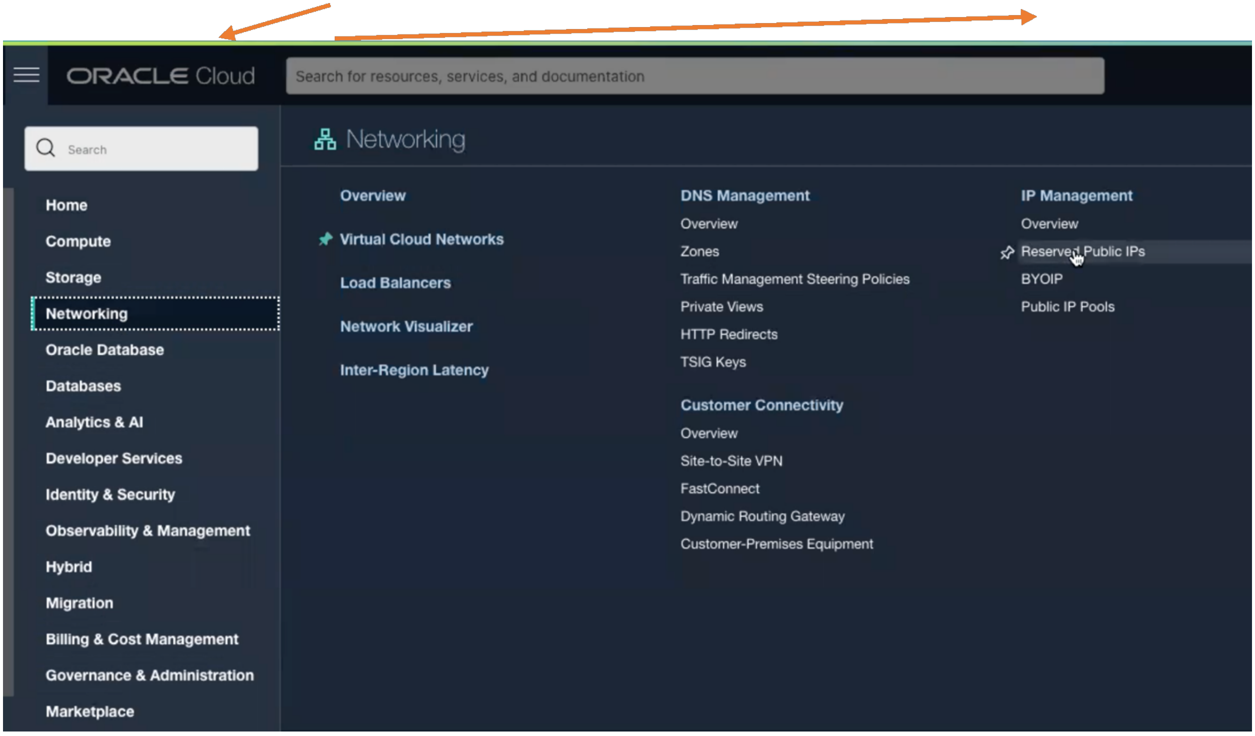
Compartment: OCVS

Route Rules

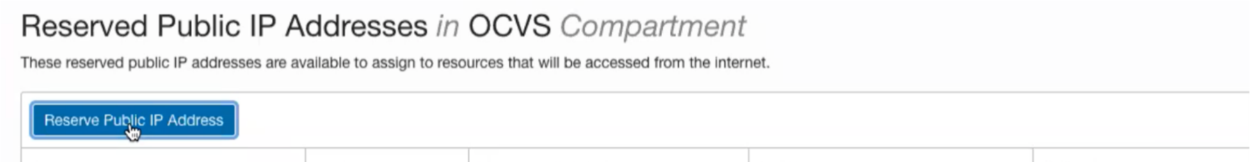
□	Destination	Target Type	Target
□	0.0.0.0/0	Internet Gateway	IGW
□	10.0.0.0/8	Dynamic Routing Gateways	megaport-drg

0 Selected

8. Now click again on the hamburger menu, go to networking and click on Reserved Public IP’s on the right hand side.



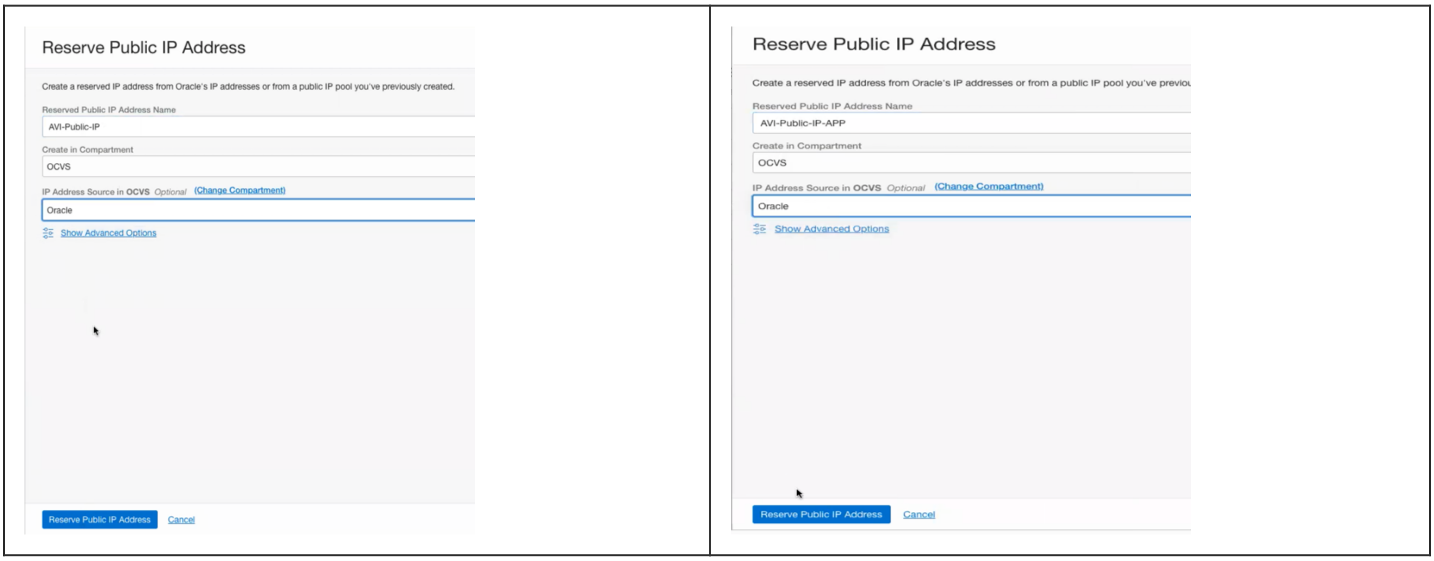
9. Click on Reserve Public IP address



Reserved Public IP Addresses *in* OCVS *Compartment*

These reserved public IP addresses are available to assign to resources that will be accessed from the internet.

10. Reserve two Public facing IP address, one for your Application Virtual Service and one for your DNS Virtual Service.



Reserve Public IP Address

Create a reserved IP address from Oracle's IP addresses or from a public IP pool you've previously created.

Reserved Public IP Address Name: AVI-Public-IP

Create in Compartment: OCVS

IP Address Source in OCVS *Optional* (Change Compartment): Oracle

Show Advanced Options

Reserve Public IP Address Cancel

Reserve Public IP Address

Create a reserved IP address from Oracle's IP addresses or from a public IP pool you've previou

Reserved Public IP Address Name: AVI-Public-IP-APP

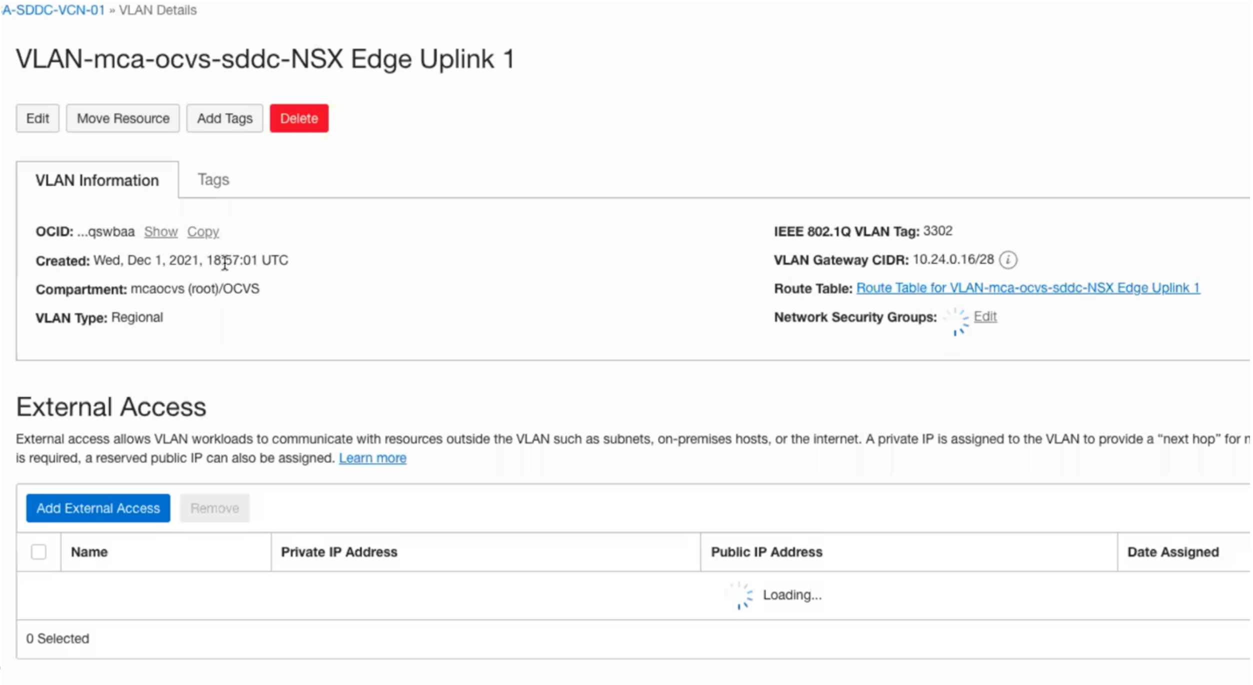
Create in Compartment: OCVS

IP Address Source in OCVS *Optional* (Change Compartment): Oracle

Show Advanced Options

Reserve Public IP Address Cancel

11. Now repeat steps 2, 3, 4, 5, then click on Add External Access



A-SDDC-VCN-01 » VLAN Details

VLAN-mca-ocvs-sddc-NSX Edge Uplink 1

OCID: ...qswbaa Show Copy

Created: Wed, Dec 1, 2021, 18:57:01 UTC

Compartment: mcaocvs (root)/OCVS

VLAN Type: Regional

IEEE 802.1Q VLAN Tag: 3302

VLAN Gateway CIDR: 10.24.0.16/28

Route Table: Route Table for VLAN-mca-ocvs-sddc-NSX Edge Uplink 1

Network Security Groups: Edit

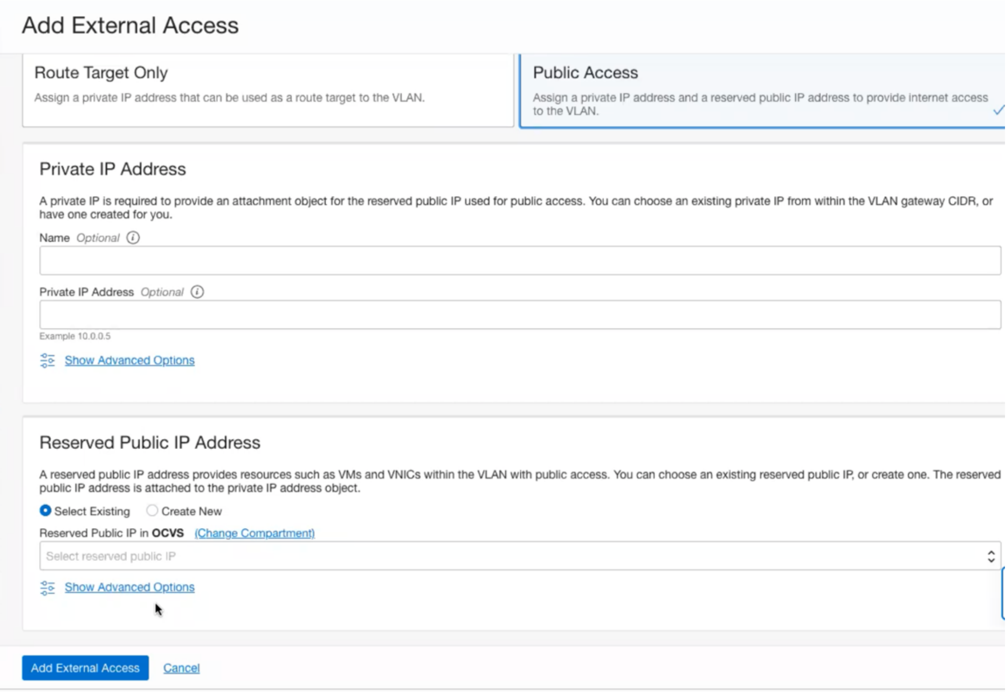
External Access

External access allows VLAN workloads to communicate with resources outside the VLAN such as subnets, on-premises hosts, or the internet. A private IP is assigned to the VLAN to provide a "next hop" for r is required, a reserved public IP can also be assigned. Learn more

□	Name	Private IP Address	Public IP Address	Date Assigned
			Loading...	

0 Selected

12. Choose Public Access then click Reserve Public IP, and choose the Public IP created in the previous steps.



Add External Access

Route Target Only
Assign a private IP address that can be used as a route target to the VLAN.

Public Access ✓
Assign a private IP address and a reserved public IP address to provide internet access to the VLAN.

Private IP Address

A private IP is required to provide an attachment object for the reserved public IP used for public access. You can choose an existing private IP from within the VLAN gateway CIDR, or have one created for you.

Name *Optional*

Private IP Address *Optional*

Example 10.0.0.5

Show Advanced Options

Reserved Public IP Address

A reserved public IP address provides resources such as VMs and VNICs within the VLAN with public access. You can choose an existing reserved public IP, or create one. The reserved public IP address is attached to the private IP address object.

● Select Existing ○ Create New

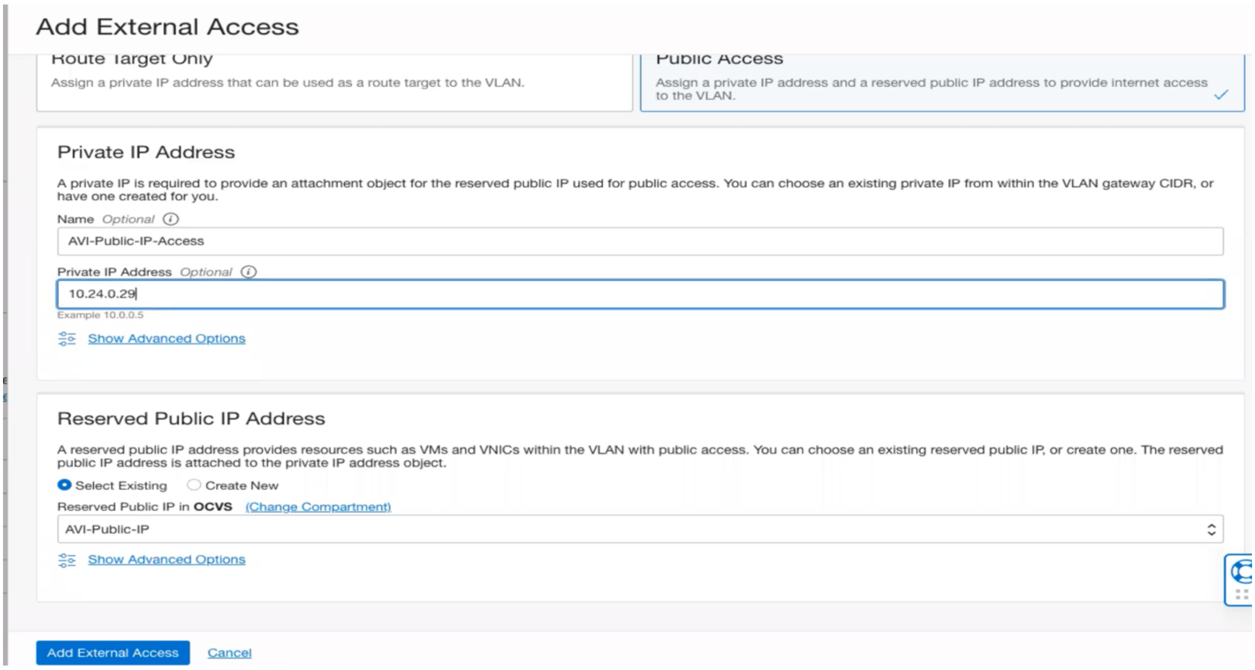
Reserved Public IP in **OCVS** (Change Compartment)

Select reserved public IP

Show Advanced Options

Add External Access Cancel

13. In the Private IP Address section, give your private IP a name and then choose a free IP in your VLAN Gateway CIDR block (check the screen shot in step 11, this is where you see your Gateway CIDR block), in my case I will choose 10.24.0.29 for the DNS-VS, then Click Add External Access.



Add External Access

Route Target Only
Assign a private IP address that can be used as a route target to the VLAN.

Public Access ✓
Assign a private IP address and a reserved public IP address to provide internet access to the VLAN.

Private IP Address

A private IP is required to provide an attachment object for the reserved public IP used for public access. You can choose an existing private IP from within the VLAN gateway CIDR, or have one created for you.

Name *Optional*: AVI-Public-IP-Access

Private IP Address *Optional*: 10.24.0.29

Example 10.0.0.5

Show Advanced Options

Reserved Public IP Address

A reserved public IP address provides resources such as VMs and VNICs within the VLAN with public access. You can choose an existing reserved public IP, or create one. The reserved public IP address is attached to the private IP address object.

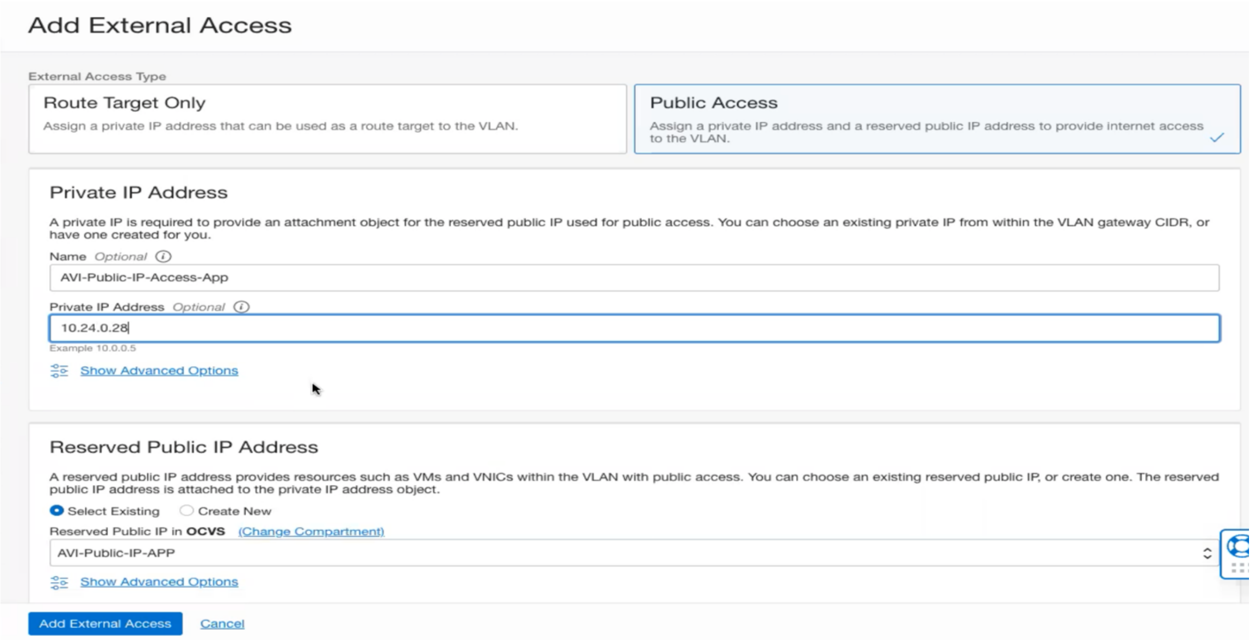
● Select Existing ○ Create New

Reserved Public IP in **OCVS** (Change Compartment): AVI-Public-IP

Show Advanced Options

Add External Access Cancel

14. Repeat the previous step and add external access for the application virtual service, the will map the internal IP 10.24.0.28 to the public ip assigned for the application.



Add External Access

External Access Type

○ Route Target Only
Assign a private IP address that can be used as a route target to the VLAN.

● Public Access ✓
Assign a private IP address and a reserved public IP address to provide internet access to the VLAN.

Private IP Address

A private IP is required to provide an attachment object for the reserved public IP used for public access. You can choose an existing private IP from within the VLAN gateway CIDR, or have one created for you.

Name *Optional*: AVI-Public-IP-Access-App

Private IP Address *Optional*: 10.24.0.28
Example 10.0.0.5

Show Advanced Options

Reserved Public IP Address

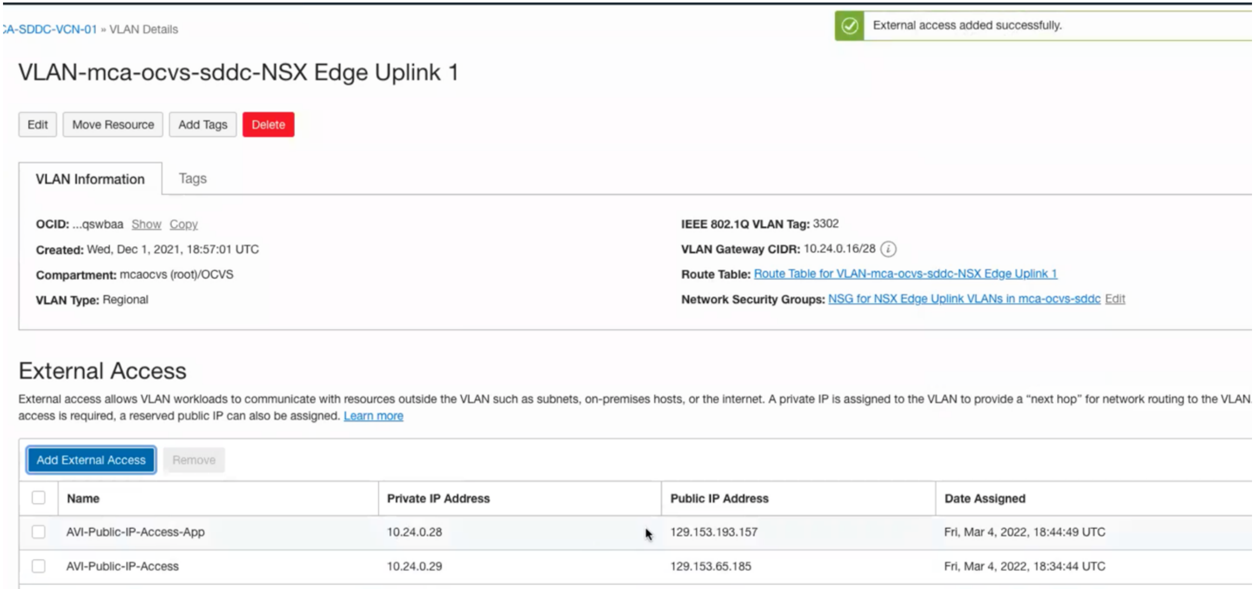
A reserved public IP address provides resources such as VMs and VNICs within the VLAN with public access. You can choose an existing reserved public IP, or create one. The reserved public IP address is attached to the private IP address object.

● Select Existing ○ Create New

Reserved Public IP in **OCVS** (Change Compartment): AVI-Public-IP-APP

Show Advanced Options

15. You should see a similar view to the below snap-shot



CA-SDDC-VCN-01 » VLAN Details

✓ External access added successfully.

VLAN-mca-ocvs-sddc-NSX Edge Uplink 1

OCID: ...qswbaa Show Copy
Created: Wed, Dec 1, 2021, 18:57:01 UTC
Compartment: mcaocvs (root)/OCVS
VLAN Type: Regional

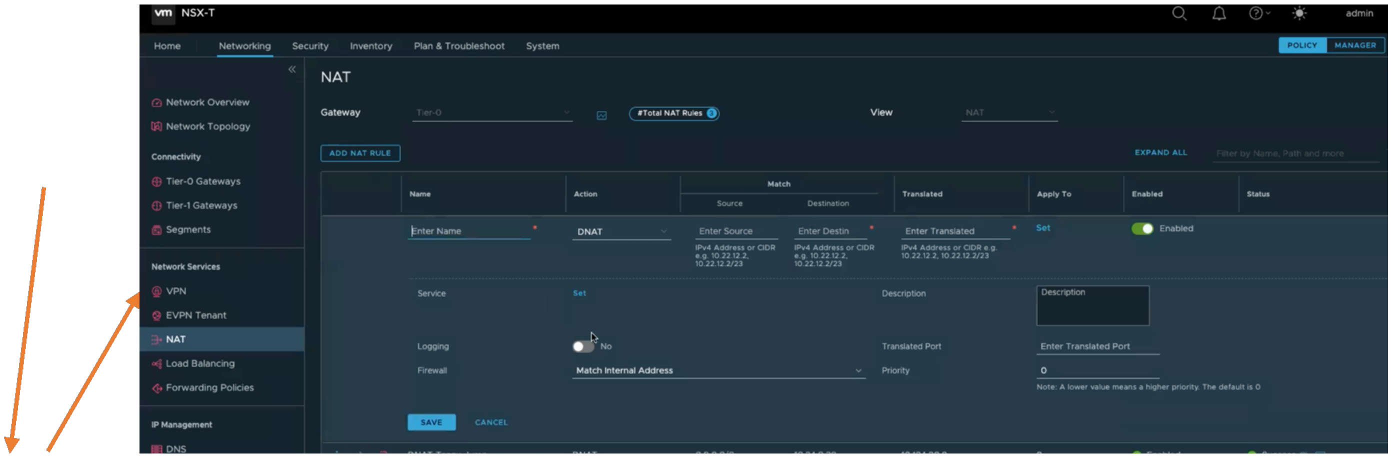
IEEE 802.1Q VLAN Tag: 3302
VLAN Gateway CIDR: 10.24.0.16/28
Route Table: Route Table for VLAN-mca-ocvs-sddc-NSX Edge Uplink 1
Network Security Groups: NSG for NSX Edge Uplink VLANs in mca-ocvs-sddc Edit

External Access

External access allows VLAN workloads to communicate with resources outside the VLAN such as subnets, on-premises hosts, or the internet. A private IP is assigned to the VLAN to provide a "next hop" for network routing to the VLAN access is required, a reserved public IP can also be assigned. Learn more

□	Name	Private IP Address	Public IP Address	Date Assigned
□	AVI-Public-IP-Access-App	10.24.0.28	129.153.193.157	Fri, Mar 4, 2022, 18:44:49 UTC
□	AVI-Public-IP-Access	10.24.0.29	129.153.65.185	Fri, Mar 4, 2022, 18:34:44 UTC

16. Now go ahead and open the SDDC manager for this SDDC. Once you open NSX, go to the networking tab and click on NAT then Add NAT Rule.



NAT

Gateway: Tier-0 #Total NAT Rules 3 View: NAT

Filter by Name, Path and more

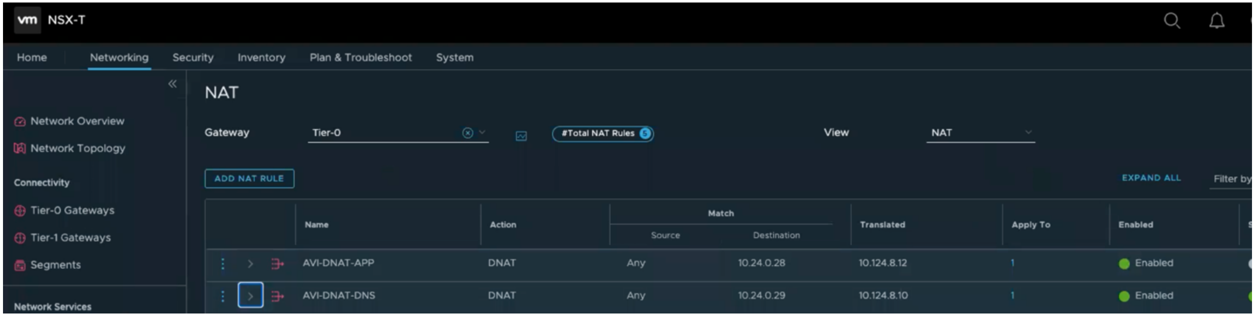
Name	Action	Match Source	Match Destination	Translated	Apply To	Enabled	Status
Enter Name	DNAT	Enter Source IPv4 Address or CIDR e.g. 10.22.12.2, 10.22.12.2/23	Enter Destin IPv4 Address or CIDR e.g. 10.22.12.2, 10.22.12.2/23	Enter Translated IPv4 Address or CIDR e.g. 10.22.12.2, 10.22.12.2/23	Set	Enabled	

Service: Set
Description: Description
Logging: No
Translated Port: Enter Translated Port
Firewall: Match Internal Address
Priority: 0
Note: A lower value means a higher priority. The default is 0

17. Apply the following configuration to create a DNAT Rule to NAT traffic for DNS Virtual Service:
    a. Name: AVI-DNAT-DNS

    b. Source: leave it blank (Represents Any)
    c. Destination: 10.24.0.29
    d. Translated: 10.124.8.10 (AVI IP address of the DNS-Virtual Service)
    e. Apply to: Hit Set and choose NSX-Edge-Uplink-1
    f. Hit Save

18. Apply the following configuration to create a DNAT Rule to NAT traffic for Application Virtual Service:
    a. Name: AVI-DNAT-App
    b. Source: leave it blank (Represents Any)
    c. Destination: 10.24.0.28
    d. Translated: 10.124.8.12 (AVI IP address of the Application-Virtual Service)
    e. Apply to: Hit Set and choose NSX-Edge-Uplink-1
    f. Hit Save
19. Once you finish the previous two steps you should get a similar view to the following image



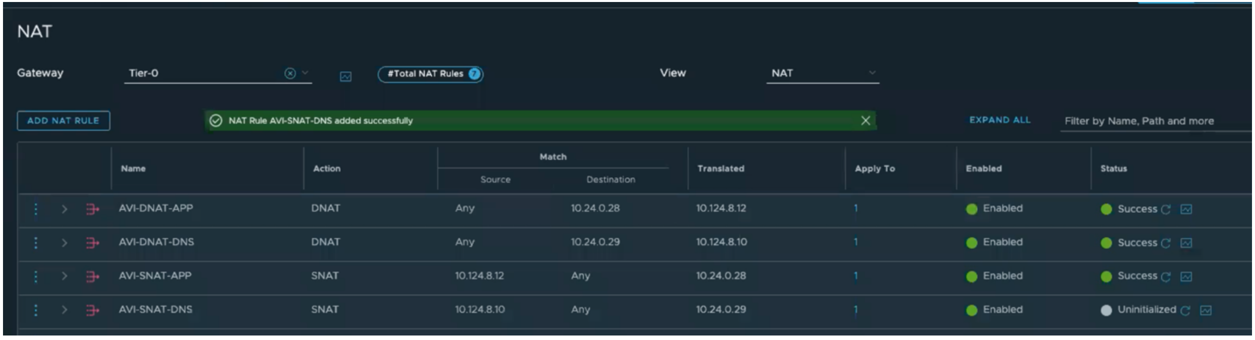
NAT

Gateway: Tier-0

View: NAT

Name	Action	Match		Translated	Apply To	Enabled
		Source	Destination			
AVI-DNAT-APP	DNAT	Any	10.24.0.28	10.124.8.12	1	Enabled
AVI-DNAT-DNS	DNAT	Any	10.24.0.29	10.124.8.10	1	Enabled

20. Now we need to create couple outgoing Source NAT rules
    a. Rule1:
        1. Name: AVI-SNAT-DNS
        2. Source: 10.124.8.10
        3. Destination: Any
        4. Translated: 10.24.0.29
        5. Apply to: Hit Set and choose NSX-Edge-Uplink-1
        6. Hit Save
    b. Rule2:
        1. Name: AVI-SNAT-APP
        2. Source: 10.124.8.12
        3. Destination: Any
        4. Translated: 10.24.0.28
        5. Apply to: Hit Set and choose NSX-Edge-Uplink-1
        6. Hit Save
21. Once you completed the previous step you see a similar view



NAT

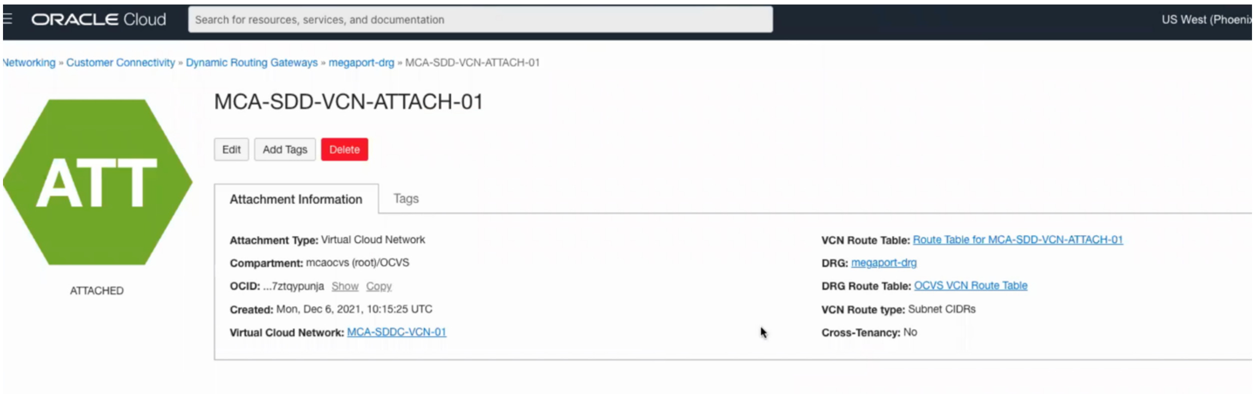
Gateway: Tier-0

View: NAT

NAT Rule AVI-SNAT-DNS added successfully

Name	Action	Match		Translated	Apply To	Enabled	Status
		Source	Destination				
AVI-DNAT-APP	DNAT	Any	10.24.0.28	10.124.8.12	1	Enabled	Success
AVI-DNAT-DNS	DNAT	Any	10.24.0.29	10.124.8.10	1	Enabled	Success
AVI-SNAT-APP	SNAT	10.124.8.12	Any	10.24.0.28	1	Enabled	Success
AVI-SNAT-DNS	SNAT	10.124.8.10	Any	10.24.0.29	1	Enabled	Uninitialized

Finally, there are couple more things we need to make sure are in place. Go to the hamburger menu, click on networking and Click on Dynamic Routing Gateway, click on your SDDC, then click on the attachment, then click on the VCN Route Table as per below image



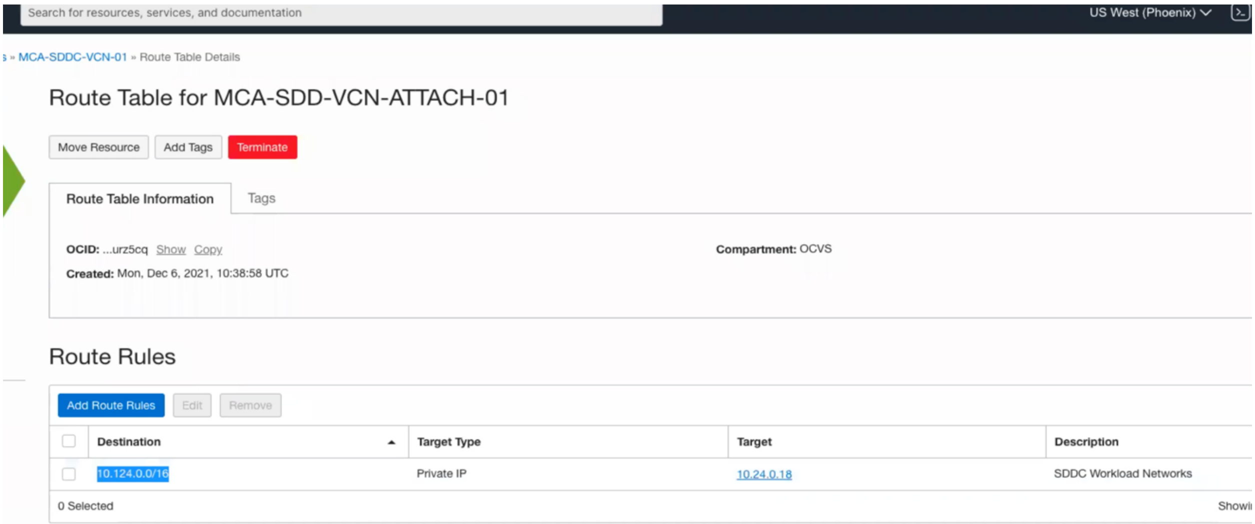
Networking » Customer Connectivity » Dynamic Routing Gateways » megaport-drg » MCA-SDD-VCN-ATTACH-01

MCA-SDD-VCN-ATTACH-01

Attachment Type: Virtual Cloud Network
Compartment: mcaocvs (root)/OCVS
OCID: ...7ztqypunja Show Copy
Created: Mon, Dec 6, 2021, 10:15:25 UTC
Virtual Cloud Network: MCA-SDDC-VCN-01

VCN Route Table: Route Table for MCA-SDD-VCN-ATTACH-01
DRG: megaport-drg
DRG Route Table: OCVS VCN Route Table
VCN Route type: Subnet CIDRs
Cross-Tenancy: No

Make sure you SDDC range (10.124.0.0/16 in my case) is forwarded to right target



s » MCA-SDDC-VCN-01 » Route Table Details

Route Table for MCA-SDD-VCN-ATTACH-01

OCID: ...urz5cq Show Copy
Created: Mon, Dec 6, 2021, 10:38:58 UTC
Compartment: OCVS

Route Rules

	Destination	Target Type	Target	Description
□	10.124.0.0/16	Private IP	10.24.0.18	SDDC Workload Networks

0 Selected

Showi

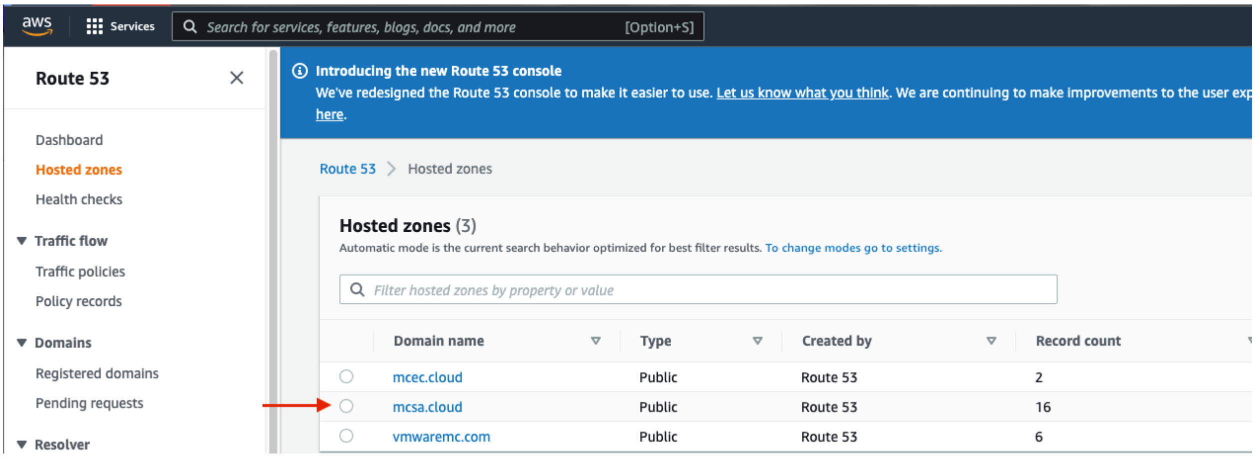
This completes all the required configuration on the OCI side, the next steps is to deploy AVI in OCVS, this is a vSphere deployment identical to the deployment we did early in this document found here. You can also follow the AVI configuration found here.

Global DNS Configuration using Route53

One of the real important things when it comes to AVI GSLB when you are using Route53 is domain delegation.

If you don't have a domain name setup in Route53, go the following link and follow the instructions: https://www.bogotobogo.com/DevOps/AWS/aws-Route53-DNS-Domain-Name-Server-Setup.php

In my case, I have a domain name already configured which I am going to use "mcsa.cloud". Next, I will configure a sub-domain for my AVI GSLB. More details in the table below.



ⓘ Introducing the new Route 53 console

We've redesigned the Route 53 console to make it easier to use. Let us know what you think. We are continuing to make improvements to the user exp here.

Hosted zones (3)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Filter hosted zones by property or value

	Domain name	Type	Created by	Record count
○	mcec.cloud	Public	Route 53	2
○	mcsa.cloud	Public	Route 53	16
○	vmwaremc.com	Public	Route 53	6

The next step is to create A and NS records for your AVI GSLB, you can apply similar configuration to what I create. Simply navigate to hosted zones > your domain > Create Record.

Then I have my NS record effectively saying, anything that has "demoavi.mcsa.cloud" in it, go ahead and send them to the associated name servers in the table below.

Once you apply this configuration, and you query the "demoavi.mcsa.cloud", Route53 will route traffic to these AVI authoritative servers based on your AVI GSLB configured algorithm (In my case Round Robin, for more information visit the configuration in here and go to step 4)

Record Name	Type	Routing	Value/Route Traffic	Notes
demoavi-ns1.mcsa.cloud	A	Simple	20.83.137.218	DNS-VS Public IP
demoavi-ns2.mcsa.cloud	A	Simple	34.102.29.94	DNS-VS Public IP
demoavi-ns3.mcsa.cloud	A	Simple	35.82.125.235	DNS-VS Public IP
demoavi-ns4.mcsa.cloud	A	Simple	158.101.45.54	DNS-VS Public IP
demoavi.mcsa.cloud	NS	Simple	demoavi-ns4.mcsa.cloud demoavi-ns3.mcsa.cloud demoavi-ns2.mcsa.cloud demoavi-ns1.mcsa.cloud	

Note, The IPs in the table are the DNS-VS IPs that you configured for each public cloud provider, for more information check the following:

- Azure - Link
- Google - Link
- VMC – Link
- Oracle – Link (This link is still WiP)

VMware AVI-GSLB multi-cloud Support Statement

VMware AVI supports deployment across private data centers and multiple public clouds for true hybridity.

Restrictions may apply depending on the versions running and licensing for VMware AVI and VMware infrastructure sites.

Future Work

Field AVI Demo Access

The Multi-Cloud team is working on a strategy to provide lab access to the field teams to demo AVI GSLB for multi-cloud SDDC deployments. For more information on this please reach out to @Amir Yanny or @John Marrone from the Multi-cloud architecture team

AVS Architecture future work

Public-IP for AVS

At the time of writing these lines, Azure has not yet developed the Public-IP feature for AVS. The only way to enable Public-IP for AVS is to configure vWAN as discussed elsewhere on this document.

vWAN hub + Azure Firewall adds additional costs that must be taken in consideration.

Azure will release Public-IP for AVS on April/May 2022, once this feature is added I will update the document to include this option.

GCVE Architecture future work

Google Cloud VMware Solution **– Internet Gateway**

When a GCvE is deployed in Google, a smaller version of an Internet Gateway is deployed for GCvE, this internet Gateway handles internet traffic for your GCvE deployment.

It is important to know that this Internet Gateway is not capable of handling large amount of traffic and might not be a good design consideration for production traffic.

It is recommended to route traffic from your GCvE Solution to a Google VPC Internet Gateway that is capable of expanding based on customer traffic demands.

I will discuss how to leverage a Google VPC Internet Gateway in later versions of this document.

OCVS Architecture

It is recommended to read the following two blog posts for more information about internet accessibility for OCVS.

https://notthe.blog/2021/11/ocvs-internet-access-1/

https://notthe.blog/2022/01/ocvs-internet-access-2/

Changelog

The following updates were made to this guide:

Date	Description of Changes
2022/05/18	

Author and Contributors

- Amir Yanny, Sr. Multi-Cloud Solutions Architect, VMware