Deploying NSX Advanced Load Balancer with VMware Cloud Director
# Table of contents

- Introduction .......................................................... 3
- Architecture ......................................................... 3
- VCD Support .......................................................... 4
- Design ........................................................................ 4
  - Dedicated Service Engines per VCD tenant ..................... 4
  - Shared Service Engines for VCD tenants ......................... 5
  - Management connectivity ........................................... 6
- Provider and tenant responsibilities ................................ 6
  - Provider responsibilities ............................................ 6
  - Tenant responsibilities ............................................. 6
- Installation .................................................................. 7
  - Deploying Avi Controller .......................................... 7
  - Performing the Avi Controller Initial setup ...................... 7
  - Mapping VCD tenants to NSX Advanced Load Balancer (Avi) tenants ........................................................... 10
- Configure networking for management traffic .................. 11
  - Create management Tier-1 ......................................... 11
  - Create management Logical Segment .......................... 12
- Configure networking for VIP traffic ............................... 12
  - Create VIP Logical Segment for each tenant .................. 12
- Deploy Service Engines .............................................. 13
- Generating Authentication Token ................................... 14
- NSX security configuration .......................................... 15
  - Exclusion List .......................................................... 15
  - Distributed Firewall ................................................ 15
- North-South VIP ...................................................... 16
- Virtual Service Configuration ........................................ 16
- Conclusion .................................................................. 17
Deploying NSX Advanced Load Balancer with VMware Cloud Director

Introduction
This whitepaper is intended for VCPP Cloud Providers who are interested in deploying VMware NSX Advanced Load Balancer (by Avi Networks) in their multi-tenant environments managed by VMware Cloud Director (VCD). The content below describes the design and installation procedures and also clearly delineates the cloud provider actions from the actions of the tenant, addressing both managed service and self-service offerings that are possible.

VMware NSX Advanced Load Balancer (Avi) provides multi-cloud load balancing, web application firewall and application analytics across on-premises data centers and any cloud. The software-defined platform delivers applications consistently across bare metal servers, virtual machines and containers to ensure a fast, scalable, and secure application experience.

The platform addresses the application delivery requirements of a wide range of customer organizations, including (but not limited to) those in the retail, financial services, technology sectors, and service providers. The NSX Advanced Load Balancer is particularly suited to organizations that need an automated and orchestrated approach to application delivery, with the ability to elastically scale application services up or down dynamically based on demand. As such, the platform enables customers to obtain optimal load-balancing capacity and other application services when needed, and then scale back down as application traffic decreases. The platform also features REST API–driven automation and provides application performance visibility that can aid reactive troubleshooting as well as proactive capacity planning.

The platform also supports advanced features like Global Server Load Balancing (GSLB) and Intelligent Web Application Firewall (iWAF). The GSLB feature allows enterprises to scale application across multiple regions or clouds and lets them manage client access based on their geographic location. WAFs prevent attacks that try to take advantage of the vulnerabilities in web-based applications. Vulnerabilities can be common in legacy applications or applications with poor coding or designs. iWAF handle the code deficiencies with custom rules or policies and generate application specific rules which helps reduce false positives.

Architecture
The NSX Advanced Load Balancer Platform (Avi) is architected on software-defined principles, decoupling the data and control planes. As a result, it centrally manages and dynamically provisions pools of application services, including load balancing, across multi cloud environments. Architecturally, the Platform comprises three core elements: the Avi Service Engines, the Avi Controller, and the Avi Console.

Avi Service Engines (SEs) take the form of distributed software that runs on bare metal servers, virtual machines, and containers. They implement application services across on-premises datacenters, colocation datacenters, and public clouds. They also collect data relating to application performance, security, and clients. As distributed software, Avi Service Engines are capable of horizontal auto-scaling within minutes while functioning as service proxies for micro services.
The Avi Controller provides central control and management of the Avi Service Engines. It orchestrates policy-driven application services, monitors real-time application performance (leveraging data provided by the Avi Service Engines), and provides for predictive auto-scaling of load balancing and other application services. Furthermore, it is capable of delivering per-tenant or per-application load balancing — increasingly in demand in multi cloud contexts — and also facilitates troubleshooting with traffic analytics.

Finally, the Avi Console provides web-based administration and monitoring. It is a web server running on the controller and offers a UI for configuration of application services, delivers visualization of network configurations and virtual IPs (VIPs), and displays application health scores and transaction round-trip times. It’s also where customers can view performance, security, and client insights, as well as where they can view service interactions.

VCD Support
The NSX Advanced Load Balancer supports VCD environments (9.7 and above) with NSX-T (2.5 and above) provided networking. NSX-V environments are not discussed in this document but are also supported. The current implementation supports NSX Advanced Load Balancer (Avi) only in No Orchestrator mode, where the components are deployed manually and managed using Avi console. This is aimed at helping VCCP Cloud Providers deploying the Advanced Load Balancer features in multi-tenant environment. Deeper integration with VCD and NSX-T is under development and will provide complete automation and lifecycle management of the NSX Advanced Load Balancer platform.

Design
Below are the recommended deployment modes for the NSX Advanced Load Balancer (Avi) in a VCD environment with NSX-T provided networking. Please note that the Service Engines should always be deployed in the provider VDC resource group. The deployment and network configurations are done directly on vSphere Client and NSX-T manager and not using the VCD.

Dedicated Service Engines per VCD tenant
A typical NSX Advanced Load Balancer (Avi) deployment on a simple NSX-T environment, with all server segments connected to a single tier-1 router, looks like below.
The VIP/Data segment must be created manually. The network adapter 1 of the service engine VM is reserved for management connectivity. Only one of the remaining nine data interfaces (network adapter 2-10) of the service engine VM is connected to the VIP/Data Segment. Rest of the interfaces must be left disconnected. The service engines are deployed in one arm mode, i.e. same interface is used for client and backend server traffic. The SE routes to backend server traffic through the tier-1 router.

The VIPs can be allocated form the same subnet as that of the VIP/Data interface of the Service engine. A range of static IP addresses must be reserved in the subnet assigned to VIP/Data segment, to be used as VIPs.

**Shared Service Engines for VCD tenants**

In NSX-T environments where web servers of different applications are connected to their individual tier-1 routers, create a VIP/Data segment on each tier-1.

The network adapter 1 of the service engine VM is reserved for management connectivity. One data interface (network adapter 2) is connected to VIP/Data segment-1 and one date interface (network adapter 3) is connected to VIP/Data segment-2. The rest of the interfaces are kept disconnected.

The VIPs can be allocated form the same subnet as that of the VIP/Data interface of the Service engine. A range of static IP addresses must be reserved in the subnet assigned to each VIP/Data segment, to be used as VIPs.

It is necessary to configure a separate Virtual Routing Framework (VRF) per tenant, and the data interfaces must be added to the VRF corresponding to the tier-1 segment of the VCD tenant it is connected to. For e.g., in the above diagram VRF-A and VRF-B must be configured on Avi Controller for Tenant-A and Tenant-B respectively. The SE interface connected to VIP/Data segment-1 must be added to VRF-A and the interface connected to VIP/Data segment-2 must be added to VRF-B.

This is required because the SE can maintain separate routing table for each VRF as the logical segments belonging to different VCD Tenants can have overlapping subnet.
Management connectivity

Avi Controller cluster VMs should be deployed adjacent to the NSX-T Manager, connected to the management port group. The deployment and network configurations are done directly on vSphere Client and NSX-T manager and not using the VCD. A separate tier-1 and connected management segment must be created for Avi service engine management connectivity.

![Diagram of management connectivity]

The network interface 1 of all SE VMs are connected to the management segment. The management tier-1 must be configured to redistribute the connected subnet routes to the tier-0. Tier-0 must advertise the VIP to external peer using BGP.

Provider and tenant responsibilities

Provider responsibilities
• Deploy Avi Controller Cluster
• Complete initial Avi Controller system configurations
• Creates tenants in Avi Controller for the organization
• Creates one or more SE groups for the tenant depending on his HA/scale out requirements
• Create management and VIP network on NSX-T
• Deploy SEs and connect to the controller
• Connect SE to the logical segments

Tenant responsibilities
• Create Virtual Service and the required policy/profiles/pool objects
• Monitor Virtual Service and pools via Avi Console
Installation
The Avi Controller OVA can be downloaded from the Avi customer portal. The service engine OVA can be downloaded from the controller console, after it is deployed.

Deploying Avi Controller
Log into the vCenter server through a vSphere Web Client. Use the client to deploy Avi Controller OVA file by following the steps mentioned below:

1. Click on File in the top menu and choose Deploy OVF Template.
2. Follow the Deploy OVA Template wizard instructions:
   o Choose Thick Provision Lazy Zeroed for disk format.
   o Choose a port group for Destination Networks in Network Mapping. This port group will be used by the Avi Controller to communicate with vCenter.
   o Specify the management IP address and default gateway. In the case of DHCP, leave this field empty (Only static IP addresses should be used in production environment).
   o Leave the Sysadmin login authentication key field blank
3. Power on the VM.

Performing the Avi Controller Initial setup
You can change or customize settings following initial deployment using the Avi Controller’s web interface.

Navigate to the Avi Controller IP on your 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.

• Configure the administrator account

Create Administrator Account

Username
admin

Password

Confirm Password

Email Address (optional)
john@doe.com

Create Account

Version: 18.2.8

Note: Email address is required for admin password reset in case of lockout
• Configure DNS and NTP server information

System Settings
Let's get started with some basic setup questions.

DNS Resolver:
8.8.8.8

DNS Search Domain:
vmware.com

NTP Authentication Keys
+ Add NTP Authentication Key

NTP Servers
Key Number | Server
--- | ---
Key Number | 0.us.pool.ntp.org

• Configure Email or SMTP information

Email/SMTP
SMTP Source:
None | Local Host | SMTP Server | Anonymous Server

From Address:
admin@avicontroller.net

• Select No Orchestrator

Orchestrator Integration
Save time by integrating with an orchestrator

- VMware
- openstack
- Amazon
- Linux

No Orchestrator
• Select **Yes** for multiple tenants

- Configure tenant settings as either of the below options, based on how you want to share the SE resources.
  - For per tenant Service Engines
    - Configure tenant settings as follows:
      - **IP Route Domain**
        - **Per tenant IP route domain.**
        - **Share IP route domain across tenants.**
      - **Service Engines Context**
        - **Service Engines are managed within the tenant context, not shared across tenants.**
        - **Service Engines are managed within the provider context, shared across tenants.**
    - Click **Complete** to save the configuration and exit the wizard.
  - For Service Engines shared across tenants
    - Configure tenant settings as follows:
      - **IP Route Domain**
        - **Per tenant IP route domain.**
        - **Share IP route domain across tenants.**
      - **Service Engines Context**
        - **Service Engines are managed within the tenant context, not shared across tenants.**
        - **Service Engines are managed within the provider context, shared across tenants.**
        - **Tenant has Read Access to Service Engines**
        - **Tenant has No Access to Service Engines**
    - Click **Complete** to save the configuration and exit the wizard.
Mapping VCD tenants to NSX Advanced Load Balancer (Avi) tenants
The VCD provider tenant maps to the admin tenant on NSX Advanced Load Balancer which is always available by default. Log in to Avi console and create Avi tenants with same name as the VCD tenants.

- Navigate to Administration > Accounts > Tenants and click Create

![Administration Account Tenants](image)

- Configure new tenant:

![New Tenant Tenant-A](image)

1. Specify the name
2. **Tenant Access to Provider Service Engine:**
   - Checked for SE shared across tenants
   - Unchecked for per-tenant SE
3. Check **Tenant VRF**

- Check and switch tenant using the dropdown on top right

![Dropdown Tenants](image)
Deploying NSX Advanced Load Balancer with VMware Cloud Director

Configure networking for management traffic
Provider should configure a tier-1 router and a management logical segment to allow management connectivity form Avi SE to Avi controller. All SEs connect to same management logical segment (even in case of per-tenant SE mode).

Create management Tier-1
Login to NSX-T manager UI and create VIP logical subnet

- Navigate to Networking > Tier-1 Gateways
- Click on ADD TIER-1 GATEWAY
- Configure Avi-Management Tier-1 gateway

1. Name the gateway
2. Select the tier-0 gateway
3. Select appropriate edge cluster
4. Expand the Route Advertisement option
5. Enable advertisement for “All Connected Segments”
6. Save the configuration

- Click YES to continue configuration on this tier-1 gateway
- Set DHCP server by clicking the No IP Allocation Set link

Note: Above steps 4 and 5 are optional. SEs can be allocated static management IP addresses.
Create management Logical Segment
Login to NSX-T manager UI and create VIP logical subnet

- Navigate to Networking > Segments
- Click on ADD SEGMENT

1. Name the management segment
2. Select the Avi management tier-1 router
3. Set the subnet. Set the range if DHCP is required

- Save the segment configuration

Configure networking for VIP traffic
Create VIP Logical Segment for each tenant
Login to NSX-T manager UI and create VIP logical subnet. DHCP must be enabled on the tier-1 router.

- Navigate to Networking > Segments
- Click on ADD SEGMENT

1. Name the VIP segment
2. Select the tier-1 router corresponding to the VCD tenant
3. Set the subnet. Make sure there are enough static IPs to be used as VIPs

![Set Subnets](image)

- E.g. 192.168.10.101-192.168.10.254 is kept static in above figure

- Save the segment configuration

Repeat the above steps for each VCD tenant. You can also configure multiple VIP segments for a tenant if required. All VIP segment segments belonging to a tenant should connect to the same tier-1 router.

Deploy Service Engines

The Service Engines should always be deployed in the provider VDC (PVDC) resource group. The OVA can be downloaded from the Avi console.

- Log in to Avi controller UI
- Navigate to Infrastructure > Clouds
- Click the download icon on Default Cloud and choose the Ova option

![Dashboard showing Ova option](image)

- The SE image will be generated and downloaded to your local disk

Log in to the vCenter server and upload the SE image to content library to be used to deploy the SE VMs.

- In Menu dropdown, select Content Libraries
- Create new content library named Avi-SE
- Import SE OVA from your local folder to the library

Deploy the service engine VMs using the image from content library.

- Select the SE image
- Click on Actions and select New VM from This Template
- Follow the Deploy OVA Template wizard instructions
- Select Folder (If deploying in per-tenant SE mode it is recommended to create a separate folder for each tenant’s SEs)
- Select cluster resource
- Select storage
Deploying NSX Advanced Load Balancer with VMware Cloud Director

- Select networks

**SE - New Virtual Machine from Content Library**

1. Connect the Management to Avi management segment
2. Connect Data Network 1 – 9 to tenant VIP segments

*Note: For per-tenant SE mode connect the Data Network only to VIP segment of the Tenant to which the SE belongs*

- Customize the template
  1. Provide the Avi Controller IP address
  2. Provide Authentication token (see Generate Authentication Token)
  3. Provide management interface IP address and gateway information if DHCP is not enabled on management segment
  4. Leave rest of the fields blank

- Review and click Finish
- Power on the SE VM once it is deployed

**Generating Authentication Token**

Avi Service Engine requires an authentication token to connect to the Avi Controller over secure channel. Follow below steps to generate the token.

1. Name
2. Default-Cloud
3. Token
4. Generate

*Cluster UUID: cluster-7d3e310d-efc7-4e48-8146-82b9e422e549
b6046722-3f6f-47e8-a41-d6619b4c26c6*
Deploying NSX Advanced Load Balancer with VMware Cloud Director

- If deploying in per-tenant SE mode, select the tenant from the dropdown. For shared SE mode switch to admin tenant.
- Navigate to Infrastructure > Clouds
- Click on the key icon
- Copy the generated token and use it Customize template step of SE VM deployment

**Note:**
A token is valid only for 1 hour after it is generated
A token cannot be reused for more than one SE

### NSX security configuration

#### Exclusion List
Avi SE redirects traffic from the primary SE to secondary SEs when using L2 scale out mode. This leads to asymmetric traffic which can get blocked by the Distributed Firewall because of its stateful nature. Hence to ensure that the traffic is not dropped when a virtual service scales out, the SE interfaces connected to the VIP/Data segment should be added to Exclusion List.

This can be done by creating an NSX Security Group (NSGroup) on NSX-T and adding the VIP/Data segment as member. This NSGroup can then be added to the Exclusion List. This way if a new SE is deployed its VIP/Data interface will dynamically get added to Exclusion List.

In case the SEs are connected to server segment, adding the segment to Exclude List is not an option as that will put all servers in the list too. Here the user must add individual SE VMs as members to the NSGroup.

#### Distributed Firewall
Avi Controller and the SEs require certain protocols/ports to be allowed for management traffic as listed in this knowledge base article: [https://avinetworks.com/docs/18.2/protocol-ports-used-by-avi-vantage-for-management-communication/](https://avinetworks.com/docs/18.2/protocol-ports-used-by-avi-vantage-for-management-communication/). If the distributed firewall is enabled with default rule as block/reject all, create the following allow rules on DFW:

- **Controller UI Access:**
  - Source: Any (Can be changed to restrict the UI access)
  - Destination: Avi Controller management IPs and Cluster IP
  - Service: TCP (80, 443)
  - Action: Allow

  **Note:** This rule is required only if Avi controller is connected to NSX-T managed segment

- **Controller Cluster Communication:**
  - Source: Avi Controller management IPs
  - Destination: Avi Controller management IPs
  - Service: TCP (22, 8443)
  - Action: Allow

  **Note:** This rule is required only if Avi controller is connected to NSX-T managed segment

- **SE to Controller Secure Channel:**
  - Source: Avi SE management IPs
  - Destination: Avi Controller management IPs
  - Service: TCP (22, 8443), UDP (123)
  - Action: Allow

  **Note:** SE initiates TCP connection for the secure channel to the controller IP

- **SE to Backend:**
  - Source: Avi SE data IPs
  - Destination: Backend server IPs
  - Service: Any (can be restricted to service port e.g. TCP 80)
  - Action: Allow

  **Note:** Client to VIP traffic does not require a DFW rule as the VIP interface is in Exclusion list. The front-end security can be enforced for each VIP using network security policies on the virtual service.
North-South VIP
If a tenant requires a VIP to be reachable for external clients, additional configuration needs to be done on NSX-T manager.

- The tenant Tier-1 must be configured to redistribute the VIP subnet to tier-0.
- Tier-0 must advertise the VIP to external peer using BGP.

Virtual Service Configuration
The tenants are responsible for creating the virtual service for their applications. Log in to Avi Controller console and follow the steps to create a basic HTTP virtual service.

- Navigate to Application > Virtual Services
- Click on Create Virtual Service and select Basic Setup
- Configure the virtual service parameters

1. Name the virtual service
2. Select virtual service type
3. Configure service port
4. Configure VIP from the static IP range for the tenant
5. Add the pool server IP addresses
6. Click on Add Server
7. Save the configuration

- Verify the VS status on the Dashboard tab
Conclusion

NSX Advanced Load balancer is a unified application delivery solution that provides load balancing, security, and application insights and analytics in multi-tenant environments managed by VMware Cloud Director (VCD). It provides actionable insights to application administrators on a modern web-based user interface that provides role-based access and analytics in a dashboard. It allows administrators to secure their applications using iWAF which covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, and signature-based detection. NSX Advanced Load Balancer is 100% REST API based, making it fully automatable and seamless with the CI/CD pipeline for application delivery.

Please refer to the NSX Advanced Load balancer (Avi) documentation website [https://avinetworks.com/docs/] for more details about the various features.