

VMWare NSX-T Advanced Load Balancer (ALB)

Transforming application delivery



Contents

1. Introduction.....	3
2. Application delivery challenges	3
3. NSX ALB architecture	4
4. Benefits of NSX Advance Load Balancer	5
5. Key features of NSX-T ALB	6
6. Licensing feature comparison.....	7
7. Customer use case for migration from Netscaler LB to NSX Advanced LB	8
7.1 Introduction	8
7.2 Customer requirement	8
7.3 Process workflow:.....	9
7.4 Challenges	9
7.5 Benefits	10
8. Conclusion	10
9. About the Author	11

1. Introduction

VMware NSX ALB, also known as AVI, is one of the critical components in network infrastructure. Its software-defined architecture, coupled with multi-cloud support, empowers organizations to seamlessly deploy and manage applications across diverse environments, including data centers, public clouds and containerized platforms. The platform focuses on application-centric features, such as performance monitoring, real-time analytics and advanced security capabilities, enhances application delivery and safeguards against evolving cyber threats.

Furthermore, the Avi Load Balancer's integration with popular automation and orchestration tools streamline operations, reduces manual intervention and accelerates time-to-market for new applications.

This document includes challenges with the legacy ADC, NSX Advance Load balancer architecture along with the benefits.

2. Application delivery challenges

Modern data centers use web scale technologies to optimize and automate compute and networking infrastructure. These environments use standard x86 servers for computing, centrally manage infrastructure as a fluid collection of resources and

enable seamless scaling by adding compute resources dynamically. However, load balancing and application services have been a different story. Enterprises have had little choice but to use inflexible hardware ADCs (application

delivery controller) or low performance, clumsy virtual appliances. These appliances are often overprovisioned and cause businesses to overspend to gain the necessary performance and availability.

They present several challenges:

- No central management - inefficient operations with each device managed separately
- Legacy ADCs often require manual configuration, which can be time-consuming and error prone.
- Limited API and automation capabilities can hinder operational efficiency and integration with other systems.
- Integration with modern infrastructure becomes difficult due to proprietary platform of legacy ADC.
- Not architected for cloud-native applications with lots of east-west traffic
- Proprietary hardware leads to expensive overprovisioning without elastic scalability; scaling vertically by adding more hardware can be costly and time-consuming.
- Unable to address per-application or per-service load balancing needs.
- Do not offer any visibility to the application or network to help resolve issues
- Cannot scale up or down in response to traffic and without manual intervention
- Lack of consistent architecture for multi-cloud and hybrid-cloud use cases



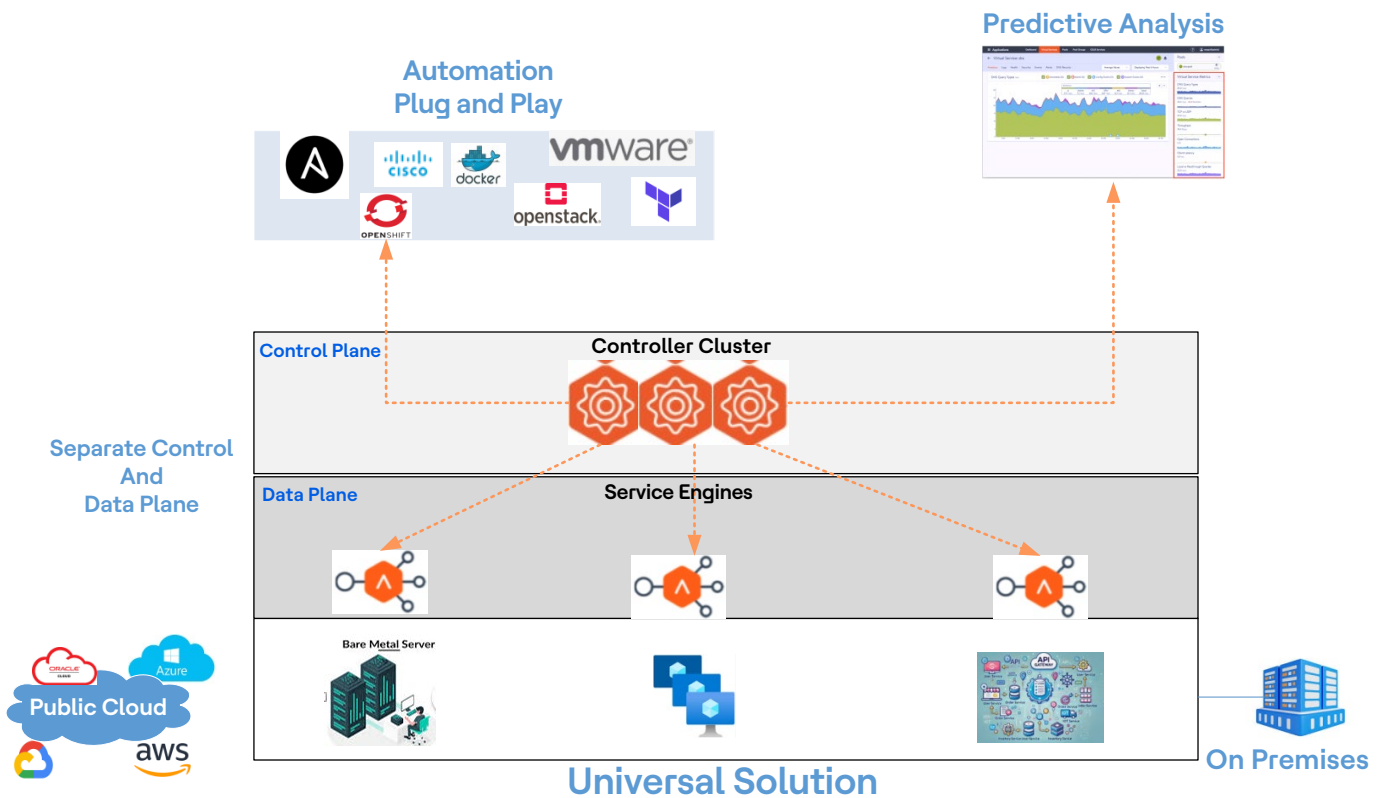
3. NSX ALB architecture

NSX Advanced Load Balancer is a software-defined Application Delivery Controller (ADC), providing local load balancing, global server load balancing and application security features such as Web Application Firewall (WAF), bot detection and management and DDoS (Distributed Denial of Service) mitigation.

NSX Advanced Load Balancer can be deployed in various environments including private cloud (on-premises in vCenter, OpenStack SDDCs (Software-Defined Data Centers) or x86-based Linux servers), public clouds (Amazon Web Services, Microsoft Azure, Google Cloud Platform and many others) as well as container platforms like

Kubernetes/OpenShift.

The solution includes two major components – the Controller, which is the point of configuration and management and the service engines, which provide the actual load-balancing capabilities. Architecturally, the solution provides separation between the management (control plane) and the end-user (data plane) traffic.



NSX ALB controller

The NSX ALB controller is the single point of management and control that serves as the “brain” of the system. The controller is a virtual appliance form factor (e.g.: OVA (Open Virtual Appliance) file for a vCenter-based deployment). Typically, three controllers are deployed as a cluster for high availability and redundancy.

The controller, based on configured options and requirements, deploys the data

path engines (the service engines) and pushes the configuration to these service engines.

In cases where full automation and deployment of the service engines by the controller is not needed, the service engines can be deployed manually (e.g.: deploying the service engine OVA for a vCenter environment). In this scenario, the service engine connects to the controller based on the configuration and the

controller then pushes the configuration to the SEs (Service Engines).

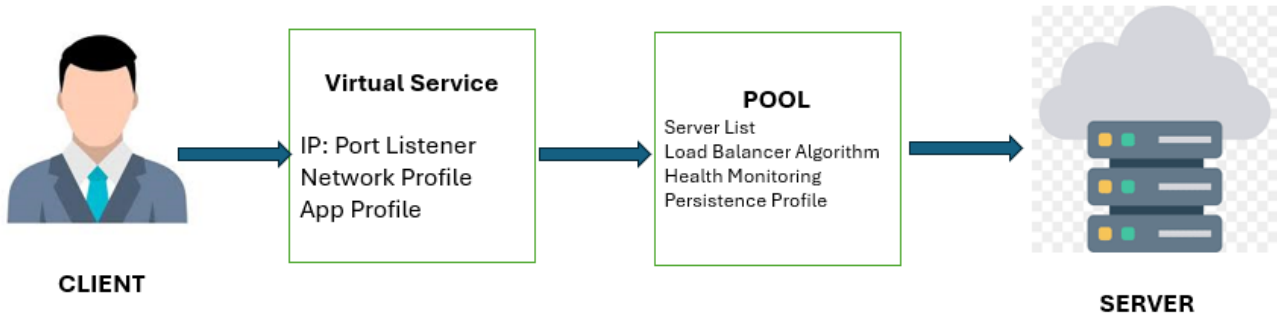


Service engines

NSX ALB Service Engines (SEs) handle all data plane operations within NSX ALB by receiving and executing instructions from the

controller. The SEs perform load balancing and all client- and server-facing network interactions. It collects real-time

application telemetry from application traffic flows. High availability is supported.



In a typical load balancing scenario, a client will communicate with a virtual service, which is an IP address and port hosted in NSX ALB by an SE. The virtual service internally passes the connection through several profiles. For HTTP traffic,

the SE may terminate and proxy the client TCP connection, terminate SSL/TLS, and proxy the HTTP request. Once the request is validated, it is forwarded internally to a pool, which will choose an available back-end server. A new TCP connection then originates

from the SE, using an IP address of the SE on the internal network as the request's source IP address. Return traffic takes the same path back. The client communicates exclusively with the virtual service IP address, not the back-end server IP.

4. Benefits of NSX Advance Load balancer



Operational efficiency

NSX Advanced Load Balancer software replaces hardware appliances, automates manual processes and delivers consistent load balancing features across multiple clouds. Network ops teams save time and raise their overall productivity.



Low capex

The NSX Advanced Load Balancer is software. Configurations are automated and updates are easier. The platform is a clean escape from costly regular hardware replacement.



Orchestration and automation

Central orchestration with the Avi Controller in the NSX Advanced Load Balancer platform is a key differentiator when compared to legacy load balancers. The Avi Controller goes well beyond a mere management interface that is typical of the central control claimed by legacy load balancer vendors.



Self-healing

The NSX Advanced Load Balancer is a resilient, self-healing fabric that fixes failures without manual intervention.



Enhanced scalability

Easily scale applications to meet fluctuating demand.



Easy troubleshooting

The NSX Advanced Load Balancer has a user-friendly interface that enables you to fix problems and leverage actionable analytics.



Enhanced security

Protect applications from threats with integrated security capabilities.



Simplified management

Centralized management and automation reduce operational overheads.



Improved application performance

Optimize application response times and user experiences.

5. Key features of NSX-T ALB



Application-aware load balancing

NSX-T Advanced LB intelligently distributes traffic based on application characteristics, ensuring optimal performance and resource utilization.



Advanced traffic management

Features like SSL offloading, compression and caching enhance application responsiveness and reduce latency.



High availability and resiliency

Built-in redundancy and failover mechanisms guarantee uninterrupted application availability.



Security and compliance

Integrated security features, such as WAF, DDoS protection and TLS encryption, safeguard applications from threats.



Integration with NSX

Seamless integration with the NSX-T network virtualization platform provides unified management experience.



Hybrid cloud support

NSX-T ALB can be deployed in both on-premises and cloud environments, enabling consistent application delivery across hybrid and multi-cloud architectures.



No vendor locking

Seamless integration with all the leading vendors to guarantee uninterrupted application availability.



6. Licensing feature comparison

		License type	
Categories	Feature	Essentials for Tanzu	Enterprise / Enterprise with cloud service edition
Local traffic management	L4 LB	TCP & UDP Fast Path No SSL/TLS	TCP, UDP, DNS, SIP, RADIUS DSR, TLS support, PROXY protocol support
	L7 LB	X	HTTP/2, content rewrite, compression, caching
	L7 policies	X	Match on: IP reputation DB, string groups, etc.
Global traffic manager	Global server load balancing	X	Enterprise grade GSLB
Application security	SSL/TLS	X	Dynamic CRLs, OCSP stapling, TLSv1.3, HSM and cert management
	Application rate limiting	X	Rate limiters can be applied for L4, L7, DNS, and WAF
	DDoS protection	X	L3, L4, and L7 DDoS protection
	Intelligent WAF	X	CRS, learning/PSM, IPReputation, application signatures, Bot detection on cloud service edition
Container ingress	Service type LB	Yes Full ingress DNS and GSLB integration Multi K8s cluster and multi-AZ support	Yes
Platform	Administration	Basic LB administration	Fully multi-tenant and granular RBAC Rich alerts and events Various 3rd party integrations Integrations with various IDPs
	Scale and HA	Active/Standby only	Active/Active deployments BGP and ECMP support Auto scale of load balancers
	Flexible upgrades	X	Flexible LCM across tenants/clouds/se-groups
	Integration	No access cloud vCenter	Native integrations with all major public and private clouds and container orchestration platforms
Advanced analytics	Application visibility/analytics	X	Advanced application telemetry

7. Customer use case for migration from Netscaler LB to NSX Advanced LB

7.1 Introduction

The customer was planning Datacenter exit for metro-cluster DC where NetScaler Load Balancer (LB) was running in active-standby mode. The migration for workloads and their NetScaler LB configurations to Azure VMware Solutions (AVS) or VMware Cloud Foundation (VCF) NSX Advanced Load balancer was planned depending on the feasibility like regulatory compliance, higher communication with other

on-prem applications. Each landing zone (AVS / VCF) had an active Disaster Recovery (DR) site. The workload migration was in a phased manner where it started with lower environment and moved into Prod environment (Dev -> Int -> Prod). Also, any application which was leveraging load balancer features were to be migrated to AVS / VCF NSX ALB with multiple changes to the configuration.

7.2 Customer requirement

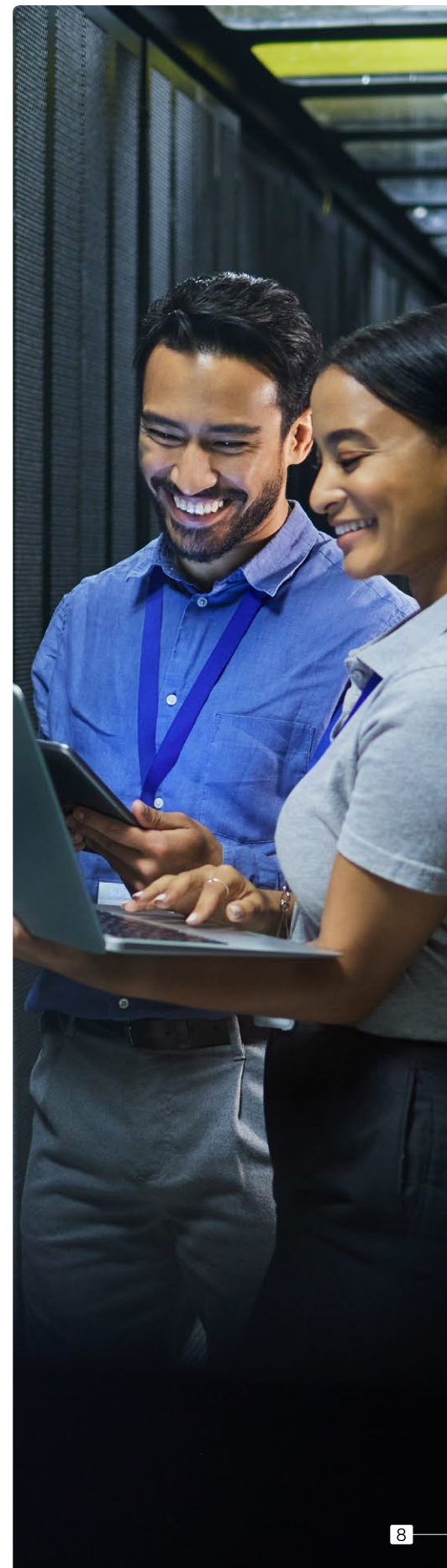
In the legacy datacenter, customer was not using any standard naming conventions for their load balancer configs and wanted to standardize the overall migration to AVS/VCF cloud. They had to go for Re-IP (Internet Protocol) of VIP (Virtual IP) as they used new subnets in the target cloud infrastructure. To minimize the operational work, they demanded using dynamic pool

members addition / deletion. As per the security standards, only strong ciphers and Transport Layer Security (TLS) were allowed and were added to Secure Socket Layers (SSL) profiles.

Unnecessary port redirections were used in source environment which we helped modify and used them in the same port for frontend and backend communications.

Moreover, the customer asked for below modifications in the existing configurations:

- Naming convention for VIP, pool, profiles, etc.
- IP address
- Move SSL Offload from LB to backend server.
- Dynamic addition of pool members based on tagging.
- No Port redirection from VIP to pool member except http to https redirection.
- Specific SSL profile to be added for https VIP.
- Modify complex policies in NetScaler to policies in AVI.

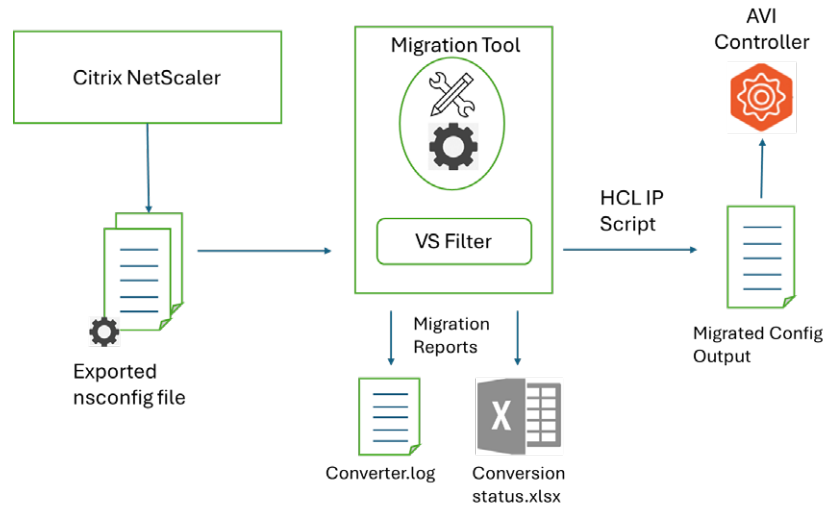


7.3 Process workflow

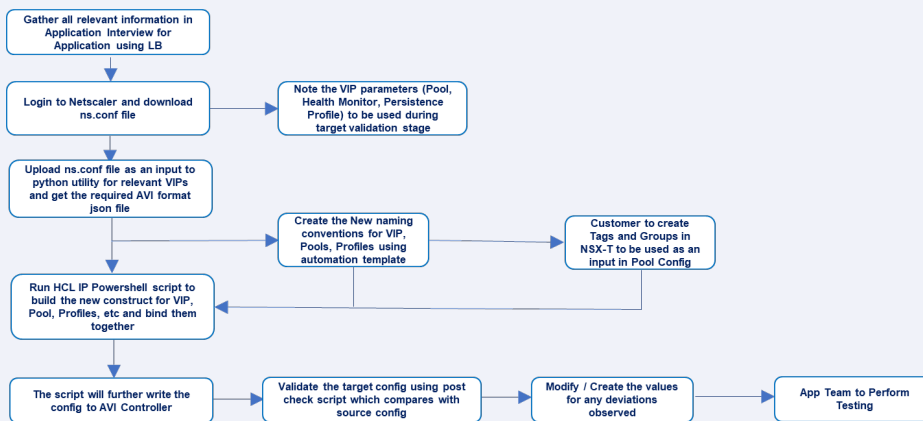
The workflow involves exporting the nsconf file from NetScaler load balancers, which is then passed to the migration tool. The tool generates two files: the first file contains the AVI-compatible JSON configuration, converted from the original NetScaler setup.

The second file will provide the conversion status as all configs are not converted using the script. The converted json construct will then pass via HCL IP script to update the naming conventions of VIP, pool, IP address, profile names, modify configs relevant to

port redirection and add correct SSL profile for HTTPS VIPs to get the final config which will eventually be pushed to the AVI controller. Subsequently, AVI controllers will push the config to AVI service engines for actual Data Plane traffic.



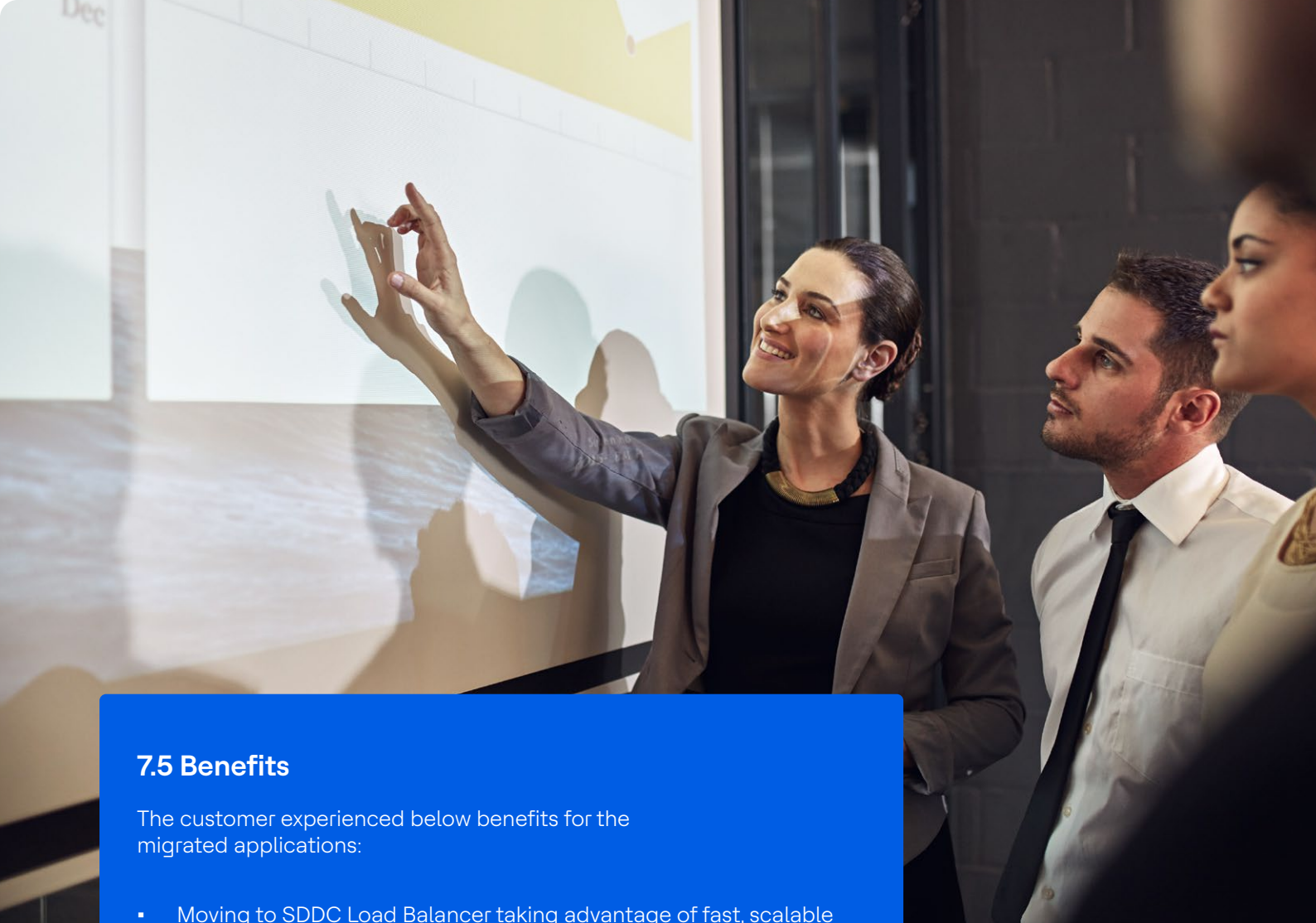
Flowchart for end-to-end flow



7.4 Challenges

Below are the major challenges faced by the customer during the migration process:

- The configuration conversion from one vendor HCL to another was overly complex.
- The manual configuration was time-consuming.
- DC exit timelines were very strict
- Customer had metro-cluster setup which supported Load balancer pair across different DC (Active in DC1 while Standby in DC2) and like to like migration was not supported in AVS. They wanted to implement the best solution with minimum downtime.



7.5 Benefits

The customer experienced below benefits for the migrated applications:

- Moving to SDDC Load Balancer taking advantage of fast, scalable and secure application experience
- Better visibility and easy troubleshooting
- Ease of migration
- Auto addition / deletion of pool members based on tags leading to lower operational expenses.
- Around 450+ VIPs along with all its components (pool, pool members, health checks, persistence profiles, Secure Socket Layers (SSL) profiles) were migrated using this approach across 150 applications.

8. Conclusion

In today's dynamic and demanding IT landscape, businesses require a robust and agile load balancing solution to ensure optimal application performance, security and scalability. The Avi Load Balancer emerges as a powerful and versatile platform that addresses

these critical needs. By embracing the Avi Load Balancer, HCLTech agrees that businesses can achieve improved application performance, enhanced security, increased agility, reduced costs and enhanced visibility and control over their application delivery

infrastructure. In conclusion, the Avi Load Balancer stands as a cornerstone for modern application delivery, empowering businesses to navigate the complexities of today's digital world with confidence and efficiency.



Anandit Gupta

Senior Consultant

About the Author

- Network SME with 15 years of experience in designing, build and support for large-scale, mission-critical software define network.(VCF,VMC, AVS).
- Hands on experience on migrations from legacy network to Software Define Network.



Nisheeth Khemka

Senior Consultant

About the Co Author

- Network/NSX SME with around 14 years of experience in design, build and migrate large scale Datacenters.
- Experience in design and build Private Cloud with Arista in underlay and NSX in overlay.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to more than 220,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending December 2024 totaled \$13.8 billion. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

