

# VMware NSX® Advanced Load Balancer™ (Avi Networks) together with VMware Tanzu

## KEY BENEFITS

- **Integrated solution**  
Consolidated services including load balancing, container ingress, application security, WAF, GSLB, DNS, and IPAM
- **Operational simplicity**  
A single solution with central control and ease of troubleshooting
- **Rich observability**  
Real-time telemetry with application insights, end-to-end across all components
- **Cloud-native automation**  
Elastic autoscaling based on closed-loop analytics and performance-based decision automation

## KEY FEATURES

- **Dynamic service discovery**, traffic management, and security, optimized for North-South traffic
- **Integration with Kubernetes** to automate deployment and management of container clusters
- **Multi-cluster, multi-site and multi-AZ** container cluster support across multiple geos and availability zones on a highly scalable platform

## WHAT'S INCLUDED

- Container ingress
- L4-L7 load balancing
- On-demand application scaling
- Web application firewall (WAF)
- Global server load balancing (GSLB)
- Real-time application analytics
- Integration with **VMware Tanzu**

## Simplify Operations for Production Ready Kubernetes

Modern containerized applications are increasingly deployed in Kubernetes clusters and moved from test and dev labs to production environments. Traditional appliance-based load balancers and open-source tools are not equipped to support modern application architectures based on microservices, which require robust security, elastic autoscaling, integrated container services and full-stack automation.

Using separate products from multiple vendors to provide load balancing, ingress controller, L4-L7 traffic management, DNS, IPAM and WAF services results in more complex operations. Managing and troubleshooting multiple independent components with disparate analytics and no end-to-end visibility prevents platform teams from delivering enterprise grade application services on production Kubernetes clusters.

Application services within a cluster and across clusters/regions, service discovery, traffic management, application security, network observability and simplified management are critical requirements of modern application infrastructure. They help ensure application availability, performance and responsiveness and bridge the gap from lab projects to production clusters. Enterprises require a scalable, consolidated, and resilient services fabric to deploy, manage and deliver containerized applications with a proven platform.

VMware is best suited to modernizing your applications and infrastructure together and bringing them ready for production enterprise environments. VMware Tanzu and VMware NSX® Advanced Load Balancer™ (by Avi Networks) offer full-stack networking and security capabilities, automate, deliver and manage applications centrally, securely, and at scale across multi-cloud environments while simplifying operations. (See Figure 1)

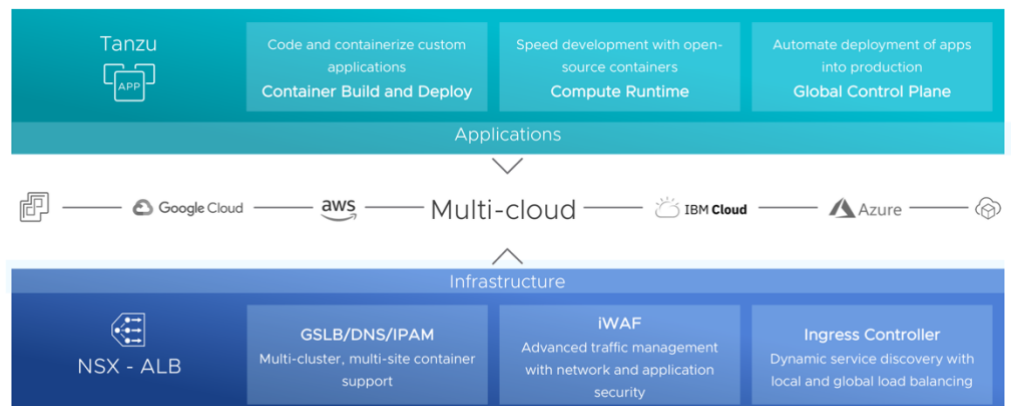


FIGURE 1: Tanzu and Avi for Multi-Cloud Environments

## Consolidated Application Services for Kubernetes

Avi helps enterprises embrace containers today and deliver application availability, security and responsiveness across on-premises and any cloud. Operations are simplified through consolidated L4-7 services including global load balancing, intelligent web application firewall (iWAF), and container ingress on a scalable platform for both traditional and modern applications. Tanzu and Avi provide a proven solution to deploy and manage container-based workloads in production environments using Kubernetes clusters.

Avi integrates with all leading container orchestration platforms including Tanzu and deploys on virtual machines and bare metal servers across on-prem, multi-cloud, multi-cluster, and multi-region environments. To deliver comprehensive container services for both traditional and cloud-native applications, *Avi Kubernetes Ingress Services* is optimized for North-South (ingress controller) traffic management including local and global server load balancing (GSLB), performance monitoring, dynamic service discovery, application security such as web application firewall (WAF), and DNS/IPAM management (see Figure 2). By consolidating application services in a single solution, Kubernetes Ingress Services provides operational consistency regardless of the underlying infrastructure the Kubernetes cluster is running on. It provides the following benefits:

- **Integrated solution**

Avi Kubernetes Ingress Services offers advanced L4-L7 services on a single platform. It helps reduce operational complexities with industry's only complete L2-L7 networking and security stack.

- **Operational simplicity**

Centralized policies and full lifecycle automation eliminate manual tasks and provide administrators with central control, self-service automation and operational consistency.

- **Rich observability**

Real-time telemetry with insights across all network, user and application through closed-loop analytics and deep machine learning provides holistic end-to-end observability, security, and real-time application performance monitoring.

- **Cloud-native automation with elasticity**

Elastic autoscaling based on closed-loop analytics and decision automation across on-premises data centers and public clouds, including VMware, OpenStack, AWS, Azure, and Google Cloud Platform.

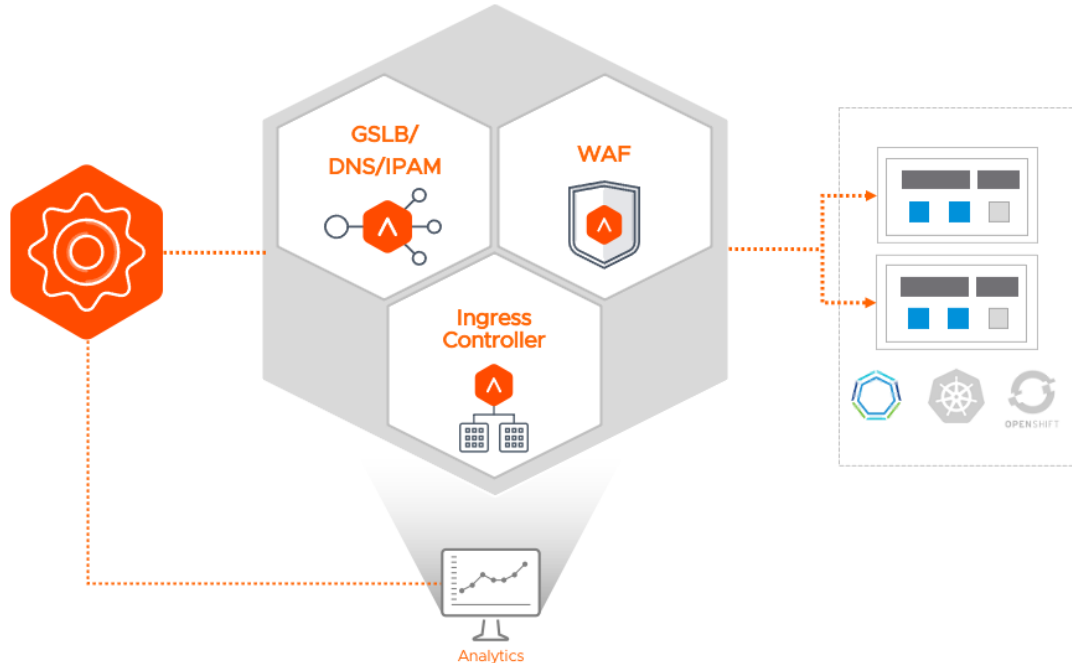


FIGURE 2: Consolidated Kubernetes Ingress Services

## Production Ready Kubernetes Clusters with Avi for Tanzu

VMware Tanzu is a portfolio of Kubernetes solutions that are tested and proven for enterprises in production environments. Avi integrates with various components in the networking layer and provides full capabilities in the Tanzu Advanced edition. It brings the shortest path to production-ready Kubernetes clusters and consolidates L4-7 services on a single scalable platform.

Together with Tanzu— the runtime environment to deploy and run Kubernetes clusters, Avi and Tanzu provide consolidated full-stack container services including networking, security and application services from a single vendor. At its core, Avi helps simplify the operations of a certified Kubernetes distribution at scale and with enterprise features.

Across the entire container lifecycle, Tanzu ensures resilient and secure connectivity of containers within and across clusters. The integration with Avi further bridges the support for both virtual machines and containers with a single solution. It also helps better secure, scale and observe microservices deployed in production Kubernetes clusters.

The joined solution also can be used with existing data center tools and workflows to give developers secure, self-serve access to conformant Kubernetes clusters in VMware private clouds. This enables running the same Kubernetes distribution across data centers, public cloud and edge for a consistent, secure experience for all development teams.

## Embracing DevSecOps with a Modern Approach to Applications and Infrastructure

Platform teams that support Kubernetes deployments are increasingly required to apply DevSecOps principles. Avi and Tanzu together make teams work better to bring modern applications to production.

### **Dev: Speed development and delivery of containerized workloads**

Tanzu includes the core elements a development team needs to build better apps, including Spring—a framework used by millions of developers to make best use of microservices, data pipelines and distributed systems, automatic packaging with dependencies, a curated catalog, and a stream of images to ignite a continuous delivery system.

Avi is based on 100% REST APIs and that means cloud-native automation is possible. Developers are able to self service provisioning services in minutes instead of waiting for an IT ticket that can take weeks. Avi's data plane is elastic and scalable, developers can easily scale out or scale in service engines to support the ephemeral container workloads. The application service fabric has resilience and high availability built-in to ensure minimal service exhaustion or disruption.

### **Sec: Secure the container lifecycle**

Tanzu makes security an integrated part of an end-to-end software supply chain – from a curated catalog of base runtimes, preset components, governance policies automatically applied through a declarative build process to all container images stored in a private registry, encrypted and continuously delivered to the Kubernetes clusters across clouds.

Avi provides application security that matches the granularity level and distributed nature of containers. Perimeter security such as traditional firewalls simply don't cut it. The consolidated networking and security services provide a central point of control at the ingress point before attacks ever reach or infiltrate the Kubernetes clusters. A comprehensive security stack includes DDoS protection, rate limiting, IP reputation, SSL/TLS offload and encryption, signature-based policies against common vulnerabilities, such as SQL Injection (SQLi) and Cross-site Scripting (XSS). The platform simplifies policy customization and autoscales on-demand across any environment.

### **Ops: Simplify operations of containers and clusters across clouds**

Tanzu streamlines management of Kubernetes at scale — all from one, central control plane – with consistent policies to Kubernetes clusters—including groups of clusters spanning clouds. With unified management, policy control, and visibility into service connectivity between containerized workloads and VMs, operators have visibility into the health and performance of clusters across clouds.

Avi drastically simplifies the operations to deliver, scale and secure applications. Instead of a wall of knobs from disparate products, it is built on a consolidated, centrally managed fabric to deploy multiple services in a single platform – spanning VMs and containers. Avi provides end-to-end observability into application and network, allowing DevOps teams to easily troubleshoot and identify issues. For continuous integration and delivery (CI/CD), Avi offers an out-of-the-box non disruptive, flexible upgrade capability. It provides graceful Blue-Green or canary deployment based on policy-based orchestration that automates the entire process.