Plug-and-Play Load Balancing for VMware Cloud Foundation with VMware® Avi™ Load Balancer

vmware®
by **Broadcom**

Table of contents

VMware Cloud Foundation

VCF simplifies self-service private cloud with a consistent operating, governance, and consumption model. It provides quick time to value by enabling self-service consumption and delivery of private cloud resources, providing users and developers with a unified and consistent self-service layer. VCF customers can take advantage of the self-service private cloud with solutions to enable use cases and help drive increased business and IT agility, productivity, and efficiency.

VMware Avi Load Balancer

For those who have realized the value of VCF, why not extend the same principles you have come to believe into application delivery? With its genesis in the software-defined principles and backed by VMware's validated designs, guided by simplified operations, self-service automation, holistic visibility, and overarching security that complements the network security, VMware Avi Load Balancer offers a superior load balancing solution like none other.

Executive Summary

Plug-and-Play Load Balancing with a Cloud Operating Model

As organizations have started selectively embracing the public cloud for a portion of their business needs, they increasingly realize the advantages of cloud infrastructure and operations. They now require a public cloud-like self-service experience for on-premises environments, too.

While public cloud has its place in app development and digital initiatives, it is not a fit for everything. Due to compliance, integration, and cost considerations, certain apps and workloads may need to reside in on-premises environments. Self-service delivery models enable IT organizations to abstract services and provide users with what they need. At the same time, IT retains the flexibility to move resources on the back end with control and compliance, optimizing the use of strategic corporate infrastructure resources simultaneously.

IT needs to transform its operational model as the legacy models of running IT are insufficient to accommodate the business's needs. These needs include but are not limited to:

- Self-service through API or portal
- On-demand, anytime, anywhere
- Scalable and expandable when needed
- Pay for what you consume

To support this digital transformation, it's essential to change how people, processes, and technology align with this goal. For individuals, this requires a shift in mindset in how services are provided. The focus should be on becoming a customer-centric organization. This shift means that people need to adopt multi-disciplinary skills and work cross-functionally.

A future-ready IT organization must have clear objectives and well-thought-out strategies to support them. Its app, data, and cloud strategies must align with higher-level business strategies, initiatives, and outcomes. This is often referred to as the Cloud Operating model.

All of this requires the adoption of a mindset focused on delivering resources to the business's IT consumers. As a result, processes will need to be re-aligned to accommodate the transition towards a Cloud Operating Model. The focus should be on automating or brokering the delivery of IT resources as much as possible and making them accessible through a self-service portal or API.

vmware®
by **Broadcom**

Why Load Balancing is Critical for VCF

Every Application Needs Load Balancing

We live in an application-driven economy. Enterprises are facing an unprecedented need to provide infrastructure that matches the agility of applications. The network team is pressured to support remote employees, deliver container apps, and support a much higher velocity of changes and updates to meet time-to-market considerations. Delivering great application experience is synonymous with business growth, better customer satisfaction, and workforce productivity. Organizations are realizing the need for a modern, software-defined load-balancing solution to enable a better application experience. Load balancing is a fundamental computing, storage, and network building block. Without load balancing, one cannot realize the value of applications and digital transformation.

Avi Enables the Cloud Operating Model

VMware Avi Load Balancer is designed to provide flexible deployment and simplified operations through automation and centralized management and support the Cloud Operating Model strategy. Avi Load Balancer decouples the control plane from the data plane with a software-defined approach to application delivery infrastructure. It provides consistent application delivery services across clouds and heterogeneous infrastructure, including bare metal servers, virtual machines (VMs), and containers. Unlike legacy load balancers, which are highly overprovisioned and wasteful, Avi enables optimal capacity management and highly elastic fabric through automatic zero-touch autoscaling features. Yet another disadvantage of the legacy load balancers is the inability to troubleshoot issues in time, often resulting in friction between the application and the network teams. Avi makes it easy to troubleshoot complex problems through rich and contextual analytics and stops the blame game. By completely integrating with the VCF ecosystem, you can enjoy the benefits of unified automation workflows, validated designs, and visibility for complete peace of mind, knowing your applications will be delivered as intended.

Avi is Built to Work Together with VCF

Customers continue to extract tremendous value from the VCF solution, keeping in line with the principles of the cloud operating model. However, the last-mile challenges with application delivery remain. These are compounded by geographically disparate data centers with broader attack surfaces and reduced analytics and visibility. This is where Avi adds tremendous value to the existing VCF customers. In addition to excellent server load balancing capabilities, the Avi enables Global Server Load Balancing with Intelligent Traffic distribution across Data centers and easily addresses essential use cases such as Disaster Recovery. With the inbuilt WAF, Avi can even provide application protection before traffic reaches the network. Lastly, it helps you proactively analyze and optimize the end-to-end application experience while simplifying troubleshooting and automatically building a self-healing infrastructure.

Enterprise Scale and Resiliency

As the mandate for application modernization takes effect, it becomes increasingly necessary to load balance applications across geographies and clouds for high availability and address critical issues such as disaster recovery and application upkeep. Avi provides global server load balancing (GSLB) services, which provide load balancing of applications across multiple geographically dispersed locations while providing centralized GSLB configuration, application monitoring, and analytics. That includes centralized provisioning with automated discovery of applications across sites and centralized application monitoring, logs, and analytics. In addition, integration with VCF ensures load balancing as a service is available with VCF Cloud Management and identity services like LDAP, Radius, and DNS servers for better scale and resiliency.

Cloud Experience for DevOps

Infrastructure-induced high latency is one of the top reasons for a suboptimal application experience. Deploying legacy or traditional hardware-based load balancers often leads to high latency and sluggish application experience. Avi reduces latency by eliminating hair pining of traffic seen with such external load balancers. It also offloads resource-intensive services, including connection management and Access Control List lookups from routers or switches, further accelerating application response times. The Avi integration with VCF can also enable you to proactively optimize resources and troubleshoot with end-to-end visibility, which is impossible with the legacy load balancers deployed as point solutions.

vmware®
by **Broadcom**

Comprehensive Web App Security

In recent years, web application security has become increasingly important, especially as web application attacks are the most common reason for breaches. WAFs have become a critical component of web application security, guarding against web application vulnerabilities while allowing customization of the security rules for each application. As WAF is in line with traffic, some functions are conveniently implemented by a load balancer. This is an additional layer of protection at Layer 7 before the traffic reaches your network. The WAF can protect your applications from common threats, including Cross-site Scripting (XSS), SQL injection, cookie poisoning, Layer 7 DoS, and Web scraping. Knowing that time to deploy and operational efficiency are critical to a successful security strategy is essential. Avi continuously provides consistent security policies and holistic visibility while reducing complexity and cost, thanks to its unique integration with VCF Networking by NSX.

IDC Business Value Study of VMware Avi Load Balancer

IDC interviewed organizations using the VMware Avi Load Balancer to deploy application services to understand how they are using the platform to support their business operations. IDC's whitepaper results show that study participants are achieving significant business value. Learn how Avi helps enterprises achieve*:

- 27% higher application developer productivity

- 90% faster to scale capacity

- 54% fewer outages

- 43% lower cost of operations

KEY RESULTS

Top-Line Impact
$13.6 million average higher revenue per year
27% higher application developer productivity

Day 2 Operations
90% faster to scale capacity
54% fewer outages

Lower Cost of Operations
6-month payback
43% cost of operations savings

CUSTOMER QUOTE:
"The most significant benefits for us of using VMware Avi Load Balancer are the visibility, the reduction of the costs, and the scaling on demand. If we still had the legacy solution and we had to scale, we'd have to order the equipment and wait for up to six months."

Avi and VCF Use Cases

Avi's software-defined architecture makes it the perfect candidate for an infrastructure-agnostic platform for any application – VMs, bare metal, or containers. The abstraction allows the same APIs, workflows, and automation to offer consistent load-balancing services regardless of the underlying environments.

Integrated Experience with Full Visibility for VCF

Customers demand better application experience round the clock with complete end-to-end analytics and automation from Layer 2 through 7. This requires full-stack integration with VCF and the backing of rigorously tested, validated, and supported deployment designs. Avi provides real-time AI-assisted visibility into application health, traffic patterns, and performance metrics, and integrates with the software-defined data center (SDDC) Manager for automated Day 0-2 lifecycle management of load balancing and enables self-service through integrating with VCF Automation (formerly known as Aria Automation).

Disaster Recovery across Multiple Sites with GSLB

Enterprise workloads are often mission-critical, demanding rigorous business continuity plans and application resilience. However, DR plans can be quite expensive with a standby site that is always idle. This translates to double the licensing cost and complex testing required to ensure this high-availability and failover process works in times of emergency. Avi's software-defined architecture and on-demand auto-scaling of capacity dramatically simplify the DR solution. Avi Cloud Console monitors and manages a pool of active licenses deployed across multiple sites – on-prem or cloud. With GSLB set up,

activating a standby site is as easy as reassigning licenses from one Avi Controller to another, eliminating the need for idle capacity and unused licenses. Maintaining consistent policies in the Avi Controller and ensuring data plane traffic is not impacted during the switchover is much more simplified.

Web Application Security for VCF with WAF

Security is only as good as its weakest point. With VCF Networking by NSX offering complete network security from L2-L3, Avi WAF enhances the protection for your workloads by offering excellent L4-7 web app security built into the platform without separate licenses. Avi provides comprehensive protection for applications hosted in private cloud environments and ensures compliance with GDPR, HIPAA, and PCI-DSS. WAF significantly enhances security by defending against sophisticated web-based threats, such as SQL injection, cross-site scripting (XSS), and other vulnerabilities in the OWASP Top 10. Key advantages of WAF with VCF include:

• Advanced Threat Mitigation: WAF inspects HTTP/S traffic in real-time, blocking malicious requests while ensuring legitimate traffic is unaffected.

• Customizable Security Policies: Administrators can create tailored rules to meet specific application requirements, ensuring maximum protection and flexibility.

• Automated Deployment: WAF deployment can be automated through SDDC Manager, enabling rapid provisioning and consistent configuration across environments.

• Centralized Management: Security policies, monitoring, and updates are managed centrally, simplifying operations and reducing administrative overhead.

• Synergies with VMware vDefend: WAF compliments vDefend products, enhancing application security alongside existing lateral security like micro-segmentation and distributed firewalls.

Container Ingress with Integrated Security

Container security with Avi ensures robust protection for modern, containerized applications while delivering high-performance traffic management. Avi acts as a Kubernetes Ingress Controller, managing ingress and securing inter-cluster traffic via GSLB. It includes a WAF to protect against web-based threats like SQL injection and XSS, while API security safeguards microservices. Avi supports TLS/SSL offloading, automates certificate management, and enables secure communication. With centralized visibility, it offers actionable insights into application performance and security metrics. Avi integrates seamlessly with DevOps workflows, ensuring security within CI/CD pipelines. Avi provides a scalable and resilient solution for securing containerized workloads by uniting advanced security features with simplified operations. Avi offers a comprehensive and consolidated set of Layer 4 to Layer 7 services for any Kubernetes environment, including VMware Tanzu, Red Hat OpenShift, and native public cloud Kubernetes services.

Avi and VCF Integration Advantages

Unlike the legacy load balancers that are either hardware-based or derivatives of the hardware-based solutions, Avi's software-defined load balancer brings elastic scale, robust performance, and intelligent analytics to every data center and cloud. Customers get enterprise-grade L4-L7 features with self-service automation and rich analytics while solving the significant operational challenges of appliance-based hardware load balancers. Avi offers the following distinct advantages as compared to legacy load balancers:

Single Hybrid Cloud Platform vs. Disjointed Point Products

Reduces operational complexities and delivers hybrid cloud consistency for flexibility and application portability. This also eliminates the need to retrain staff on different products and point solutions.

Controller vs. Instance Manager

Avi's software-defined architecture separates the control and data planes and delivers load balancing and WAF as an elastic fabric that auto-scales based on real-time traffic.

Decision Automation vs. Task Scripting

Built-in automation coupled with an API-based approach makes intelligent decisions, scales, and simplifies hybrid cloud application deployments. This is supported by Closed-loop analytics that helps automate decisions with over 800 unique application metrics.

Optimal Resource Utilization vs. Over-provisioning

Elastic, fabric approach with active-active HA ensures minimal unutilized capacity.

In-built Analytics vs. Bolt-on Solutions

Compared to a bolt-on implementation by legacy load balancers, analytics-first architecture with built-in visibility ensures complete end-to-end L2-7 visibility with VCF integration. Finally, thanks to the VCF and Avi integration by mapping apps to hosts, networks, and flows, Avi breaks visibility silos with holistic L2 to L7 visibility and analytics. This provides contextual Insights for faster Root Cause Analysis, thus reducing MTTR and exceeding customer SLA and expectations.

While these advantages make the standalone Avi load-balancing solution a forerunner in the load-balancing space, the plug-and-play integration with VCF truly makes this solution shine. This integration affords the solution of automated deployment of virtual services and service engines. VCF Customers can enjoy enhanced agility consistently using enterprise-wide unified workflow automation with automated contextual bidirectional visibility from the network to the applications. Avi with VCF also ensures a complete L2-7 security posture while reducing vendor and security fragmentation.

Avi Integrations with VCF Components

In this section, let's examine each of the VCF solution's components and examine some of the capabilities that customers can leverage to accelerate the adoption of the Cloud Operating model.
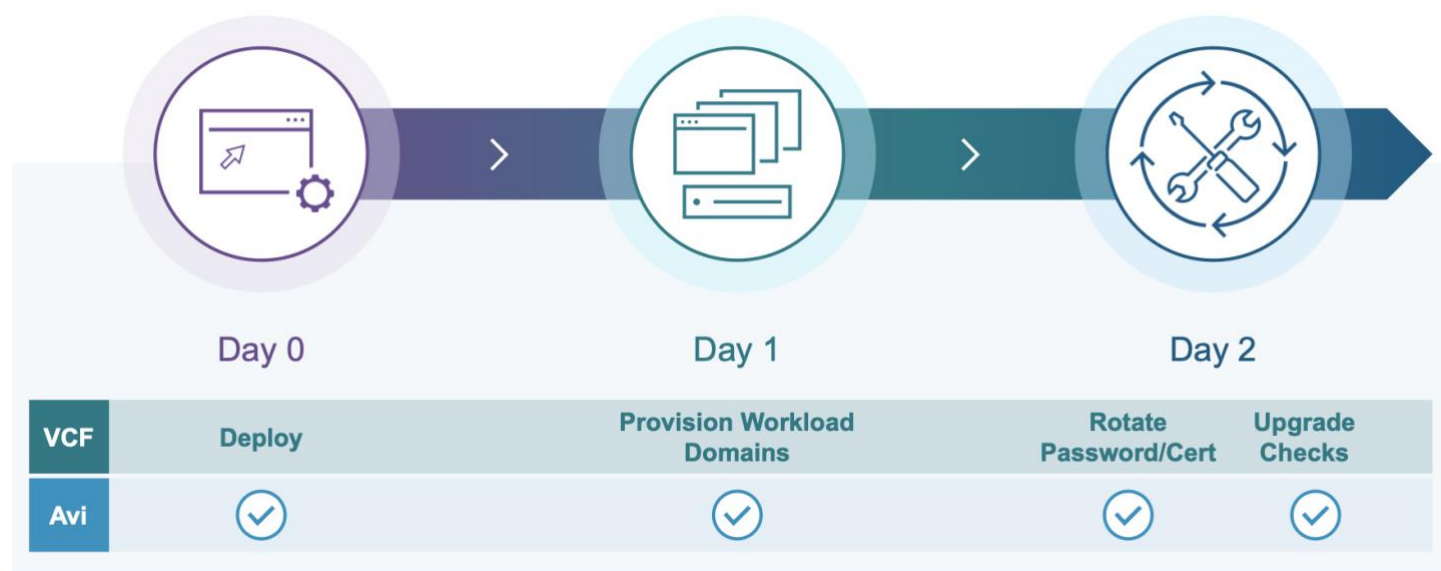
VCF SDDC Manager

The cloud operations design for the management domain must feature comprehensive virtual infrastructure provisioning and lifecycle management capabilities. SDDC Manager enhances daily operational efficiency by handling complete lifecycle management tasks, including deployment, configuration, patching, and upgrades, as well as streamlining and optimizing the management of the virtual infrastructure.

Avi is the only Load Balancer in the market that delivers true plug-and-play load balancing for VCF workloads through its integration with SDDC-M, which deploys Avi Controllers for each VCF workload. The Controllers deployed communicate directly with the VCF components, such as vCenter and NSX-T, integrating seamlessly with the management domain and easing the Day 0-2 operations process.

• Increased operational visibility

• Automated SE deployments in VCF workload domains.

• Efficient lifecycle management and Day 2 operations with automation tools suite.

• Convenient password rotation and certificate management through a simple GUI.

• Upgrade checks.

Figure 1 Avi Integration with VCF SDDC Manager Simplifies Operations across LB Lifecycle

To simplify operations and lifecycle management for large and complex systems, it's essential to be able to automate steps across initial deployment (day 0), automated configuration and provisioning (day 1), and automated lifecycle management (day 2 and beyond).

Relying on Avi's unique integration with SDDC-M, you can implement centralized load balancing (LB) for your application workloads within VCF and configure enterprise-grade load balancing, GSLB, application security, and container ingress services. With the joint solution, you can manage load balancers centrally across any environment and create new virtual services in minutes. This solution also helps you scale load balancing capacity dynamically based on traffic patterns and troubleshoot application issues without TCP dumps/log exports.

Day 0 automation through VCF provides automated deployment of private cloud infrastructure and management components to quickly stand up and deploy infrastructure. Day 1 automation provides configuration of these systems with provisioning of workload domains on demand—purpose-built and scalable for traditional and container apps. Day 2 and beyond is where most IT shops face difficulties in managing software updates and patching for large-scale software systems. VCF provides automation for full lifecycle management, including patching/upgrades, monitoring, scaling, and infrastructure management.

Plug-and-Play Load Balancing for VMware Cloud Foundation with VMware Avi Load Balancer

Avi is the only product in the market with a jointly created and validated solution that automates the deployment of the VCF management infrastructure, the lifecycle of the load balancers, which reside in the same space as the VCF workloads, and the required load balancing and security services to provide an unmatched experience for the application teams.

VCF Networking by NSX

Faster infrastructure provisioning is required to support the on-demand nature of container applications. While other vendors may provide solutions, managing these heterogeneous systems is a considerable threat to the simplicity and agility expected from that infrastructure. However, not with the NSX and Avi integration. In addition to Automated Network Configuration for Avi Lifecycle, the integration facilitates holistic, contextual visibility and a consistent, stronger security posture.

The combination of Avi and NSX enables Avi Controller to be the single management point. As developers and network admins configure app and load balancing instances, Avi Controller automatically spins up the distributed load balancers (Avi Service Engines), places the virtual IPs (VIPs) on the Service Engines, and places the network interfaces in the correct overlay or underlay network, without manual intervention. Avi also publishes rules and dynamically manages security for the load-balanced resources. Avi Controller scales out the resources as application traffic increases by creating additional Service Engines and scale-in when traffic recedes.

Below are the highlights of the NSX-T and Avi integration:

Enhanced Agility

- Automated discovery of NSX-T inventory & infrastructure objects by Avi
- Automated config of Virtual Service: virtual IP allocation, registration in DNS, NSX-T routing tables
- Automated Service Engine connection to logical network segment
- Eliminate inefficient hairpinning of E-W traffic for better performance & latency
  - o Automated Elasticity and Scale-out
  - o New SEs auto-configured with right network attributes
  - o Automated NSX-T IP route updates
  - o No config updates are needed when you add/remove app servers in a NSgroup

Faster Troubleshooting

- Discover and troubleshoot network connectivity issues faster with complete L2-L7 visibility and network, servers, and apps correlation by VCF Operations for Networks (formerly vRNI) integration
- Holistic contextual L1-L7 visibility with NSX-T (L2-L4) with Avi (L4-L7)
- Stop the blame game- Determine is it a network, server or application problem?
- Correlate Avi, NSX-T, and vCenter events, operational status and metrics with a single pane of glass
- Network mapped to flows and applications
- Visibility for virtual services, pools, service engines, controller nodes, paths, topology, traffic patterns, packet drops, retransmission count, RTT, latency & more

Stronger Security Posture

- Consistent security posture with your existing vDefend Distributed Firewall (DFW) policies
- Simplified and automated configuration
- User configured DFW rules using auto created NSgroups and service objects
- Better security posture with network security complemented by Application security (WAF, bot management, DDoS and API protection) with Avi

VCF Compute by vSphere

This integration enables the Avi Controller to interact with the vCenter Server and provide lifecycle management for the Service Engines. Avi enables the automated discovery of vSphere objects, and vCenter automated Service Engines are enhanced with automated object creation and deployment. Application elasticity and scale-out is also automated with Avi.

Below are the highlights of the vCenter and Avi integration:

Enhanced Agility
• Automated discovery of vSphere object

– Avi can discover ESXi hosts, Datastore, and networks

• Automated Service Engine life cycle with vCenter

– OVA creation and upload
– ESXi hosts placement with anti-affinity rules for higher resiliency
– Automated config of virtual NICs of SEs to connect to right networks

• Automated Elasticity and Scale-out with vCenter and NSX-T

– New SEs added or removed automatically without any manual configuration

Faster Troubleshooting
• Compute usage visibility in Avi with vCenter integration for faster troubleshooting

– Application Servers, Service Engines Instances and ESXi hosts performance statistics (e.g., CPU and memory usage)

VCF Cloud Management (formerly Aria or vRealize)

VCF Cloud Management is a platform that unifies applications, infrastructure, and services across private, hybrid, and public clouds in a single platform with a standard data model. With VCF Cloud Management, you can gain consistent operations of hybrid clouds with VMware's industry-leading products and services for cloud management. Organizations can embrace a cloud operating model to drive innovation and support digital transformation initiatives.

VCF Cloud Management integration means automated workflows for application deployment and changes. Operational support for application availability and optimization is automated through Avi and VCF Automation (formerly Aria Automation). Advanced analytics mean closed-loop automation can provide application resiliency and elasticity.

Avi enables developers to satisfy their load balancing needs at the click of a button thanks to integrating natively with VCF Automation to provide a seamless solution. Linking Avi objects inside VCF Automation using a simple drag-and-drop method makes it easier to satisfy end-user self-service goals and automate your load balancing as a service solution.

Below are the highlights of the VCF Cloud Management and Avi integration:

Enhanced Agility
• Automated workflow tasks with VCF Automation integration

– Avi, as a first-class native resource, can now be linked inside VCF Automation through simple drag-and-drop, reducing operational burden.

– Provide end users increased agility by automating Avi through VCF Automation.

– VCF Automation service broker forms are designed to use VCF Operations (formerly Aria Operations or vROps) to populate fields with external data, enhancing the self-service experience for deploying Avi through VCF Automation.

– Achieve greater flexibility with VCF Automation extensibility and VCF Operations actions.

Troubleshoot Faster
• End to end visibility and monitoring across geos, on-prem & clouds with VCF Operations integration for better operations

  – Continuous monitoring, object relationship visualization and unified alert reporting of all Avi resources, metrics, and properties for faster troubleshooting

  – One-stop view of health and availability with pre-built dashboards for virtual services, virtual services configs, Avi

• Discover and troubleshoot network connectivity issues faster with full L2-L7 visibility and network, servers and apps correlation by VCF Operations for Networks (formerly vRNI) integration

• Centralized Avi events, client request and server response log insights with VCF Operations for Logs (formerly Aria or vRealize Log Insight) integration

VMware Tanzu

Containerized applications are increasingly deployed in Kubernetes clusters and moved from test and dev labs to production environments. Providing reliable and secure application services is essential to application availability and responsiveness on-premises and across any cloud. Avi Load Balancer, together with VMware Tanzu Platform, brings the shortest path to production-ready Kubernetes clusters and consolidates L4-7 container networking services, including local and global traffic management, web application firewall (WAF), and container ingress on a single scalable platform.

When deployed together with Avi's container ingress capabilities, you enjoy the following benefits:

Integrated Solution
A comprehensive set of services, including load balancing, ingress controller, and application security capabilities such as WAF, GSLB, DNS, and IPAM, are offered on a single platform.

Operational Simplicity
A single solution with central orchestration of policy, lifecycle management, API endpoint, and ease of troubleshooting lowers operational costs by more than 50%.

Rich Observability
End-to-end visibility across multiple clusters and sets brings real-time telemetry and application insights across all components in a production Kubernetes deployment.

Cloud-native automation with elasticity
Elastic autoscaling, based on closed-loop analytics and decision automation, provides a resilient and secure backbone for scaling out containerized applications.

Below are the highlights of the VMware Tanzu and Avi integration:

Enhanced Agility
• Include AKO (Avi Kubernetes Operator) in your cluster's lifecycle

  – Create new clusters with automated AKO configurations

• Leverage Avi for Tanzu/K8s control plane API

• Leverage Avi for Kubernetes workloads

  – AKO configures Avi based on K8s API calls
  – Avi assigns IP automatically for your external Load Balancer
  – Register your FQDN automatically for your container applications

• Automated Elasticity and Scale-out

– New SEs auto configured with the right network attributes

– No config updates needed when you add/remove pods to your application

Stronger Security

• Comprehensive unified ingress app security for micro-services apps to reduce complexity, vendor, and security posture fragmentation

– WAF, bot management, DDoS protection, API protection

• Consistent security posture for your traditional and container apps by Avi

Summary

Avi Load Balancer is a key component of the VCF ecosystem, enabling the benefits businesses want to achieve from cloud architectures. Operational support of clouds is complicated, and Avi with VCF simplifies the operations and expertise required to manage the cloud and its applications. Application delivery in the cloud requires a change in how people, processes, and technology are aligned, and the tight integrations of Avi and VCF improve and simplify this alignment.

Through enhanced automation, improved security, and application visibility, Avi provides plug-and-play load balancing for VCF, helping adopt the mindset required to embrace the Cloud Operating model businesses are trying to achieve.