Avi Vantage Platform: Universal Service Mesh for Container and Traditional Apps

MICROSERVICES AND THE EVOLUTION OF APPLICATIONS

Application-centric enterprises are choosing microservices architectures to enable continuous application delivery. Microservices architectures take advantage of the flexibility of container-based infrastructure models by breaking large monolithic applications into smaller services that can be deployed, developed and updated independently without causing major outages.

While application architectures have evolved, application services need a generational change. Traditional appliance-based load balancers are not equipped to support the east-west interactions between the services and offer no visibility into microservices. IT and app developers need application services such as service discovery, proxy services to manage service interactions, visibility, security, load balancing and application autoscaling.

AVI VANTAGE PLATFORM FOR MICROSERVICES

Avi Vantage separates the data plane (of distributed service proxies) and control plane (central management) to provide application services in an on-premises or cloud environment. Avi Vantage consists of a centralized Avi Controller cluster and distributed Avi Service Engines (distributed load balancers) running as containers. The Avi Controller integrates with the cluster management framework to automate the provisioning of service proxy instances. As applications are created, scaled out, and scaled in, and as cluster nodes are added and deleted, the Avi Controller automatically updates the proxy configuration in the cluster (See Figure 1).

CHALLENGES

- Traditional, appliance-based load balancers are infeasible for container apps dependent on service-to-service east-west traffic.
- Open source solutions are not feature complete.
- IT and DevOps lack visibility or application insights, which hampers troubleshooting.
- Microservices applications require dynamic provisioning for non-disruptive updates.

SOLUTION

- The Avi Vantage Platform delivers full-featured load balancing that supports north-south and east-west traffic, as well as automated configuration updates.
- Avi’s universal service mesh provides full stack L4 - L7 services that integrate with Kubernetes/OpenShift/Istio for fully automated, policy driven deployments.
- Application maps offer real-time observability into inter-service monitoring and analytics.
- An integrated IPAM/DNS server allows for automatic service discovery of microservices.

BENEFITS

- Avi provides enterprise-grade security, including micro-segmentation, firewalling, SSL offload, DDoS protection, and URL filtering.
- Avi elastically autoscales applications based on predictive load and real-time performance.
- Avi simplifies CI/CD operations by supporting blue-green deployments and canary upgrades.
Avi Vantage integrates with container orchestration platforms such as Kubernetes/OpenShift and open source Istio service mesh to deliver comprehensive container services for both traditional and cloud-native applications. Universal Service Mesh is optimized for North-South (ingress) and East-West traffic management, including local and global server load balancing (GSLB), web application firewall (WAF) and performance monitoring. It extends service mesh beyond containers to virtual machines and baremetal servers across multi-cluster, multi-region, and multi-cloud environments (See Figure 2).

**Figure 2: Universal Service Mesh for Microservices Applications**

**TRAFFIC ROUTING**
- Advanced ingress gateway with integrated IPAM/DNS, blacklist/whitelist policies and rate limiting
- Full-featured load balancer, including advanced L7 policy-based switching and, SSL/TLS offload
- East-west and north-south traffic management including content switching, redirection, caching and compression automated service discovery and application map based on 100% REST APIs

**ADVANCED SECURITY**
- Zero trust security model, encryption and URL filtering
- Single sign-on (SSO) integration for enterprise-grade authentication and authorization
- Distributed web application firewall (WAF) for DDoS protection against L4 or L7 attacks

**REAL-TIME OBSERVABILITY**
- Dynamic application map with latency, connections, and throughput information in a dashboard view (see Figure 3)
- Health monitoring on 100s of metrics per microservice instance with automatic synchronization
- Full HTTP log analytics with Google-like search to derive application insights
- Security insights including TLS/SSL versions, SSL security profiles and certificates for each microservice
- Client insights for north-south (external) traffic
PRODUCTION-READY SERVICE MESH

Enterprise-grade application services include service discovery to identify all services that make up an application: L4 – L7 security services including firewalls, micro-segmentation, URL filtering, SSL offload, and DDoS protection; service visibility and performance monitoring; and predictive autoscaling of services across thousands of nodes. The platform adapts application services to changes in dynamic container-based environments with services spinning up or down and applications being updated or migrated. Avi Vantage enables administrators to automate operations and empowers developers with programmable self-service for application services. With role-based access control (RBAC), developers can view a graphical map of services, their interactions, and application performance from a single dashboard.

PREDICTIVE AUTOSCALING OF SERVICES

- Autoscaling of load balancers and apps based on traffic patterns
- Ability to deploy a load balancer with different capacity in real time
- Auto workload management
- On-demand autoscaling triggered by traffic thresholds

BLUE-GREEN APP DEPLOYMENT

- Blue-Green app deployment of apps in test and production environments
- Non-disruptive and graceful migration to newer versions of apps
- Real-time visibility into app performance and end-user experience

UNIVERSAL SERVICE MESH USE CASES

INTEGRATION FOR OPENSHIFT-KUBERNETES CLUSTERS

Avi provides a centrally orchestrated, elastic proxy services fabric with load balancing, service discovery, security, and analytics for container applications running in Red Hat OpenShift and Kubernetes environments. (See Figure 4).

Figure 3: Application Map Shows Service Interactions

Figure 4: Integration with Red Hat OpenShift and Kubernetes
ISTIO INTEGRATED INGRESS GATEWAY

Avi’s Istio Integrated Ingress Gateway for containers fills the need of Istio service mesh to provide secure and reliable access from external users to the Kubernetes and Red Hat OpenShift clusters, regardless of deployments in on-premises data centers or public clouds such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. (See Figure 5).

Figure 5: Ingress Gateway with Istio Integration

ISTIO INTEGRATED SERVICE MESH

Avi’s Universal Service Mesh integrates with Istio Service Mesh to provide comprehensive application services from traffic management and security to observability and performance management (see Figure 6) in a single platform. The integration with Istio extends the Istio service mesh beyond containers in Kubernetes or OpenShift to bare metal servers and virtual machines, across on-premises data centers and multi-cluster, multi-cloud, and multi-region environments.

Figure 6: Universal Service Mesh with Istio Integration