Cisco Application Centric Infrastructure and Kubernetes Solution

Introduction

Cisco® Application Centric Infrastructure (Cisco ACI™) is designed to offer policy-based automation, security, mobility, and visibility for application workloads regardless of whether they run on bare-metal servers, hypervisors, or Linux containers. The Cisco ACI system-level approach extends the support for Linux containers by providing tight integration of Kubernetes, a popular container orchestration platform, and the Cisco ACI platform.

This integration allows Cisco ACI to provide a ready-to-use, secure networking environment for Kubernetes. The integration maintains the simplicity of the user experience in deploying, scaling, and managing containerized applications while still offering the controls, visibility, security, and isolation required by an enterprise.

Challenges

As IT teams expand their infrastructure to support microservice-based applications and Linux containers with Kubernetes, a number of new challenges emerge:

- Bare-metal servers, virtual machines, and containers: As adoption of containers grows, some core components for applications may exist outside the container environment in virtual machines or bare-metal servers.
- Policy and security: Security and policy may be applied at multiple points in the infrastructure environment. Although developers may use the Kubernetes network policy API, IT may want to define additional infrastructure policies that can be enforced in a seamless manner.
- Multitenancy: Kubernetes does not natively provide a means of isolating separate tenants or isolating Kubernetes from other infrastructure components.
- Visibility and telemetry: Kubernetes environments are frequently quite fluid, with containers starting and stopping across hosts in the environment. You must understand how containers interact with the physical networking environment to monitor and troubleshoot effectively.

The solution

Cisco ACI provides an integrated solution for Kubernetes environments (Figure 1). The solution architecture includes a Virtual Machine Manager (VMM) domain within the Cisco Application Policy Infrastructure Controller (APIC) specifically built for Kubernetes. This design allows the APIC to control and display contextual information from the Kubernetes environment directly in the APIC GUI. The solution also uses Cisco OpFlex®, an open southbound API for Cisco ACI, and Open vSwitch (OVS) to control, manage, and enhance each container host.

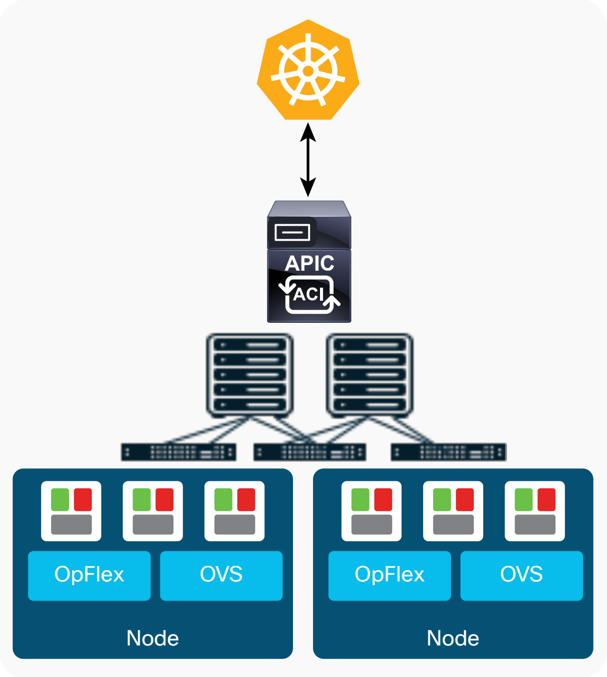
Conclusion

Cisco ACI provides tight integration with Kubernetes to accelerate and automate the deployment of container-based microservices. The solution offers a seamless developer experience intended to maintain the simplicity of Kubernetes while still enabling advanced capabilities within the Cisco ACI fabric and maintaining visibility across the infrastructure.

For more information

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_Kubernetes_Integration_with_ACI.html

Figure 1. Kubernetes and Cisco ACI architecture.



Solution benefits

The Cisco and Kubernetes solution offers the following benefits:

- Applications spread across containers, virtual machines, and bare-metal servers: Cisco ACI supports integration with multiple hypervisors and bare-metal servers in addition to containers. Applications can be designed to span all these components with Cisco ACI providing seamless connectivity and security.
- Flexible approach to policy: Cisco ACI offers the option of using native Kubernetes network policies as well Cisco ACI endpoint groups and contracts to isolate containers. This approach offers developers a cloud-native experience while additionally offering the option to use established APIC policy constructs.
- Automated, integrated load-balancing services: Load balancing plays a critical role in Kubernetes as a way of defining services. The solution automates load balancing through a combination of policy-based routing capabilities in the fabric and software-based approaches using Open vSwitch.
- Secure multitenancy: Although Kubernetes does not natively provide tenant isolation, Cisco ACI and APIC provide a naturally multitenant architecture. This design enables you to deploy multiple, isolated Kubernetes clusters on a fabric or to isolate Kubernetes name spaces in a seamless manner through Cisco ACI policies.
- Visibility and telemetry information: Through the Kubernetes VMM domain, the APIC provides contextual information from Kubernetes, including nodes, name spaces, deployments, services, and pods. It correlates this information with network telemetry information gathered by the fabric.