AWS re:Invent

CON211-S

Set up Kubernetes clusters on premises & on AWS with Cisco Container Platform

John Day
Technical Marketing Engineer
Cisco Systems Inc.

AWS re:Invent

aws

Agenda

- A bit of context
- Demo of hybrid microservices application on Amazon Elastic Kubernetes Service (Amazon EKS) and on premises
- Deployment of the clusters on premises and in Amazon EKS
- Mapping Amazon EKS components to on premises
- Additional features
- Demo of redeployment of microservices application to new clusters
- Product details

Kubernetes (k8s) is the new platform of choice

Applications

On-premises environments

Speed

Portability

Scalability

Cloud

Developers want k8s to be…

On-premises environment

Campus

Branch

DC/Co-lo

IoT/edge

- Delivered fast
- Consistent on premises and in the cloud
- Open – 100% upstream
- Configured with storage, networking, monitoring
- Secure, highly available
- Optimized for AI/ML development

aws

But it can be difficult to deliver

On-premises environment

Campus

Branch

DC/Colo

IoT/Edge

- Download and install Kubernetes
- Set up clusters
- Configure storage and networking
- Configure security: identities, secrets, and RBAC
- Install logging, monitoring, set up registries, load balancing
- Manage upgrades and patches
- AI/ML lifecycle management
- …repeat public cloud to match on-premises configuration?
- Support it (?)

aws

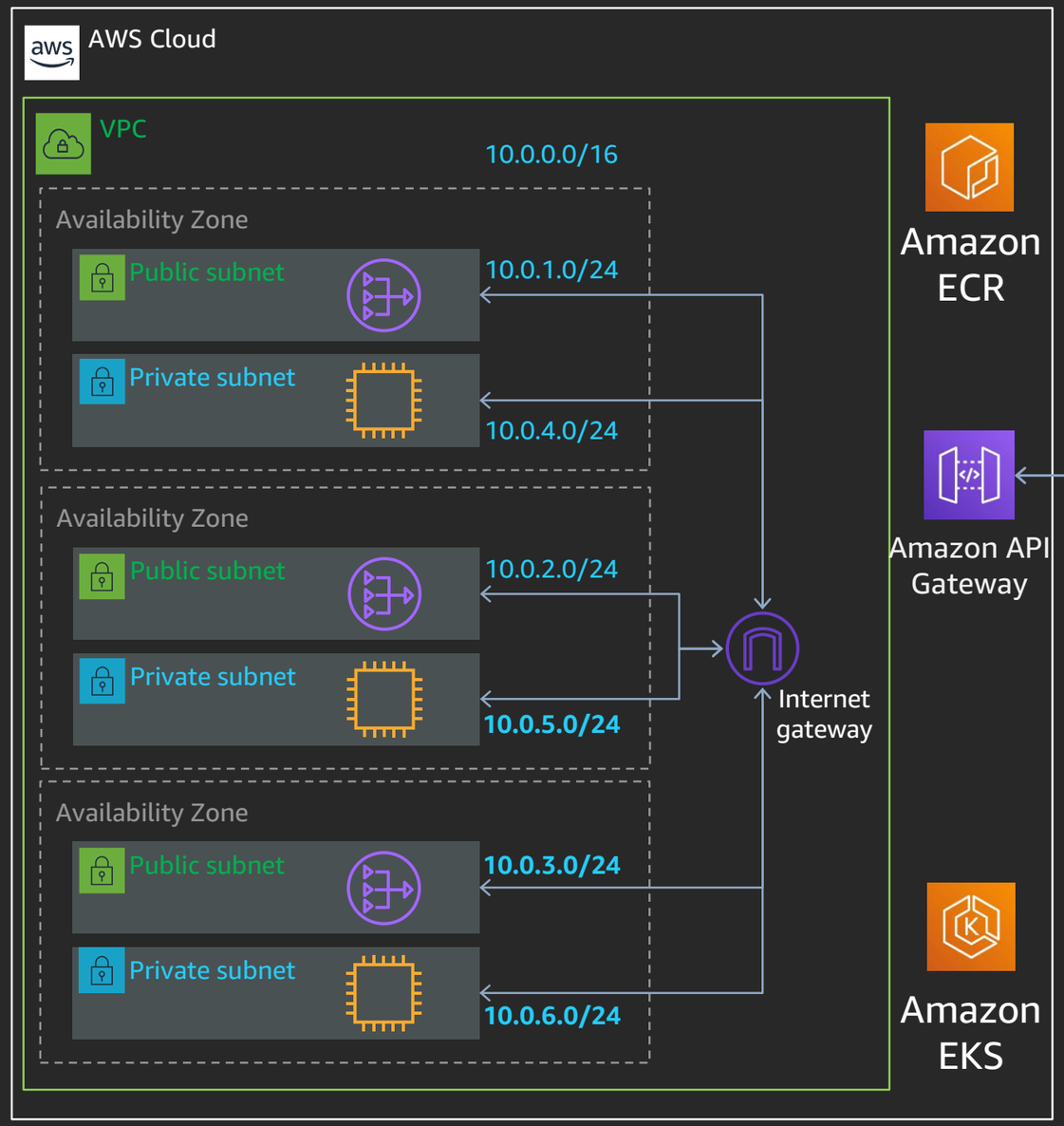
Which can result in…

Complexity and cost

With lack of common tools to manage and deploy Kubernetes

Bottlenecks

With lack of common experience slowing down development

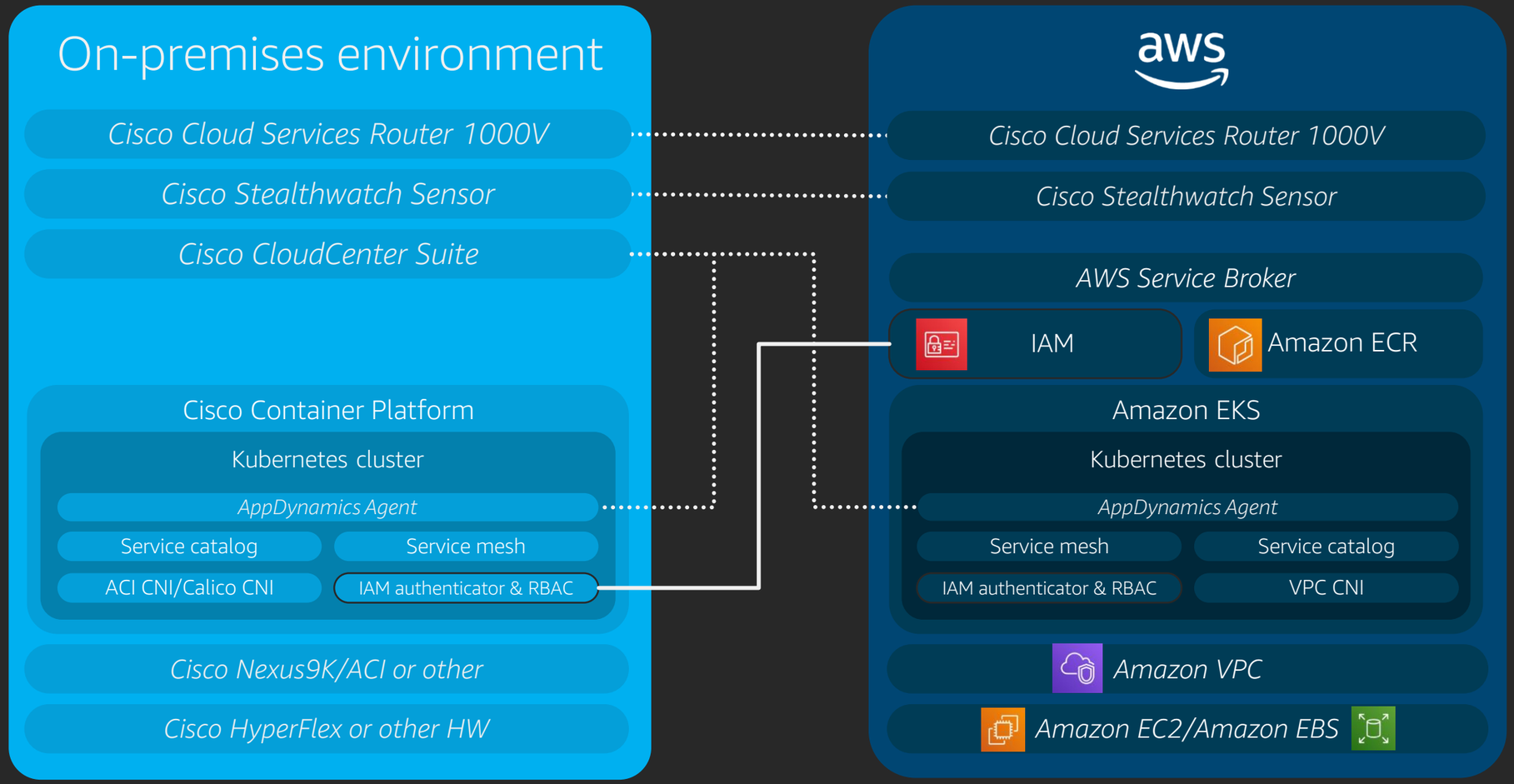


Cisco Container Platform

Turnkey container management software for consistent production-grade hybrid Kubernetes

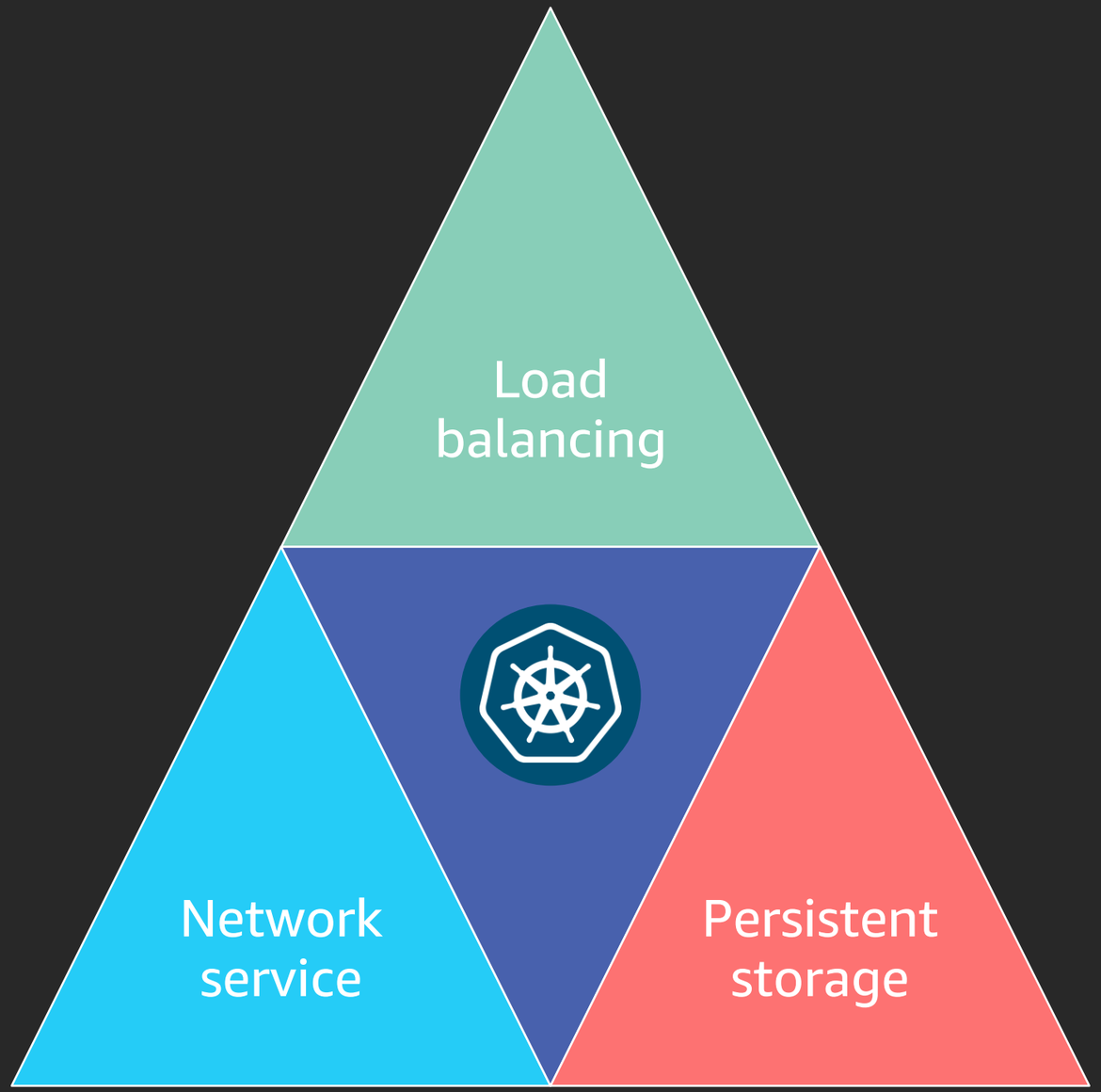
Demo

Common authentication for both sides!



Demo

Mapping Amazon EKS components to on premises


Load
balancing
Network
service
Persistent
storage

Cluster external IP load balancing (service LoadBalancer)

Amazon EKS

By default, classic load balancers are used for LoadBalancer-type services

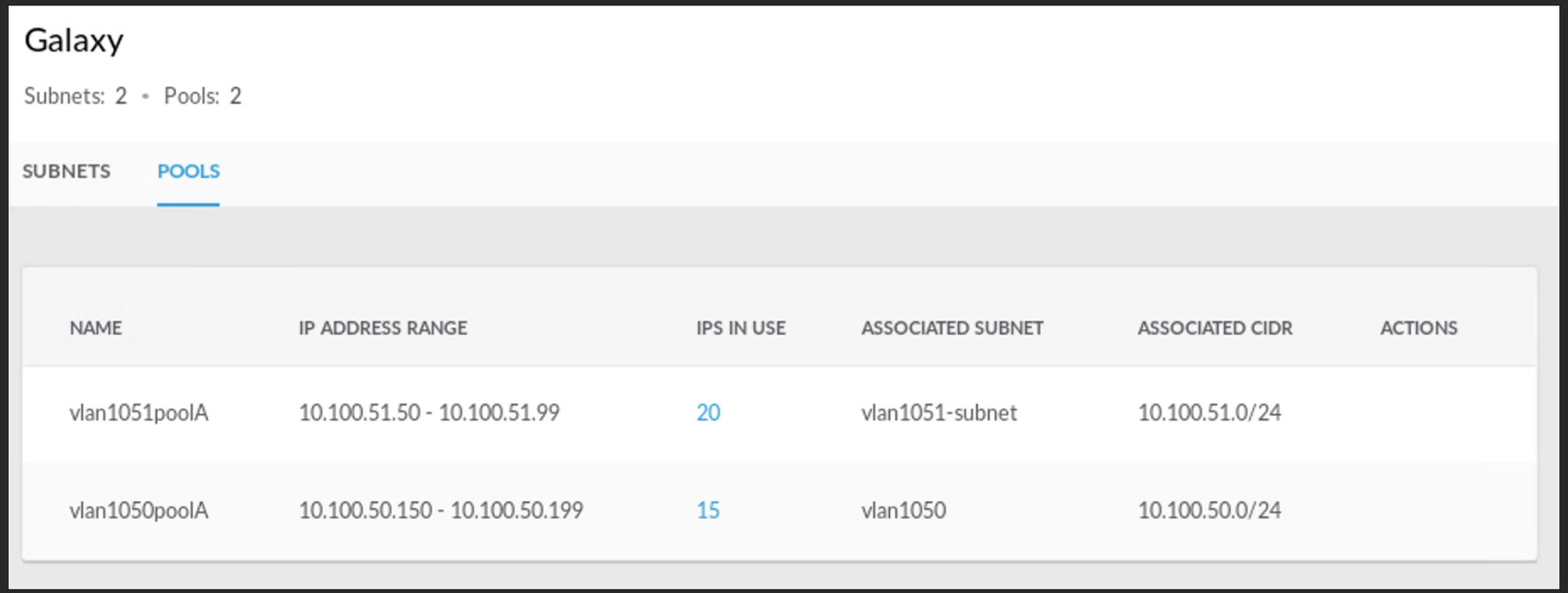
On premises

By default, static IPs are assigned to a MetalLB service running on the cluster

IP ranges are managed from the CCP Control Plane

```
apiVersion: v1
kind: Service
metadata:
  name: frontend-external
spec:
  type: LoadBalancer
  selector:
    app: frontend
  ports:
  - name: http
    port: 80
    targetPort: 8080
```

Cluster external IP load balancing (service LoadBalancer)



Kubernetes Container Network Interface (CNI) plugin

Amazon EKS

By default, Amazon uses its own open-source plugin, amazon-vpc-cni-k8s, for pod networking in Kubernetes using elastic network interfaces on AWS

Using this CNI plugin allows Kubernetes pods to have the same IP address inside the pod as they do on the Amazon Virtual Private Cloud (Amazon VPC) network; this CNI plugin is an open-source project that is maintained on GitHub

Kubernetes Container Network Interface (CNI) plugin

CCP

You can select 2 supported CNI plugins from CCP

Calico – CCP uses the ipipMode set to Always, and Calico routes traffic using IP-in-IP for all traffic originating from a Calico enabled–host to all Calico networked containers in the IP pool

Cisco ACI-CNI – CCP also enables customers running Cisco's ACI network fabric to automatically create tenants within a fabric and enables Kubernetes pods full representation as endpoints that can be seen and have policies applied to them from a network and/or security group using policies; this also replaces the standard MetalLB deployment with the use of the inherent load balancer capabilities of ACI

Kubernetes persistent storage: Storage classes

Amazon EKS

In the current deployments of Amazon EKS clusters from the CCP dashboard, use the in-tree Amazon Elastic Block Store (Amazon EBS) storage provisioner (kubernetes.io/aws-ebs) using gp2 storage

An awsElasticBlockStore volume mounts an Amazon EBS volume into your pod

Note: Amazon EKS clusters from 1.14+ can also use the Amazon Elastic File System (Amazon EFS) CSI Driver or the Amazon EBS CSI Driver

Amazon EBS

Amazon EFS

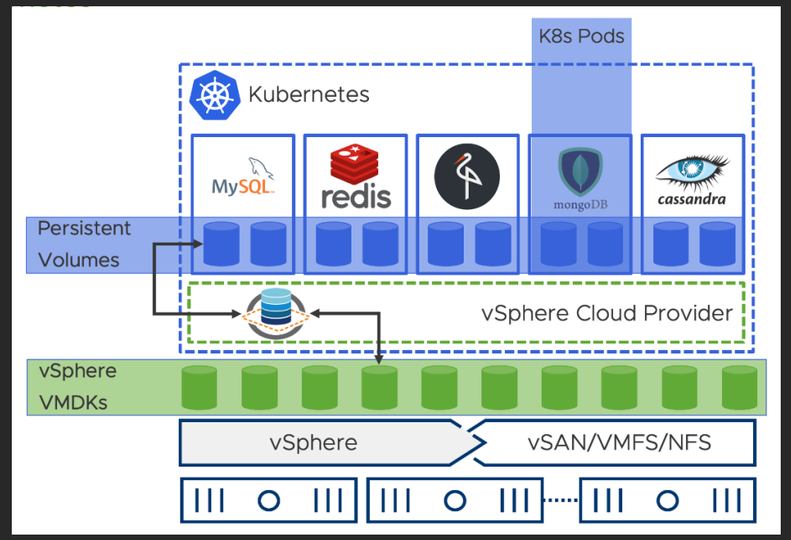
Kubernetes persistent storage: Storage classes

CCP

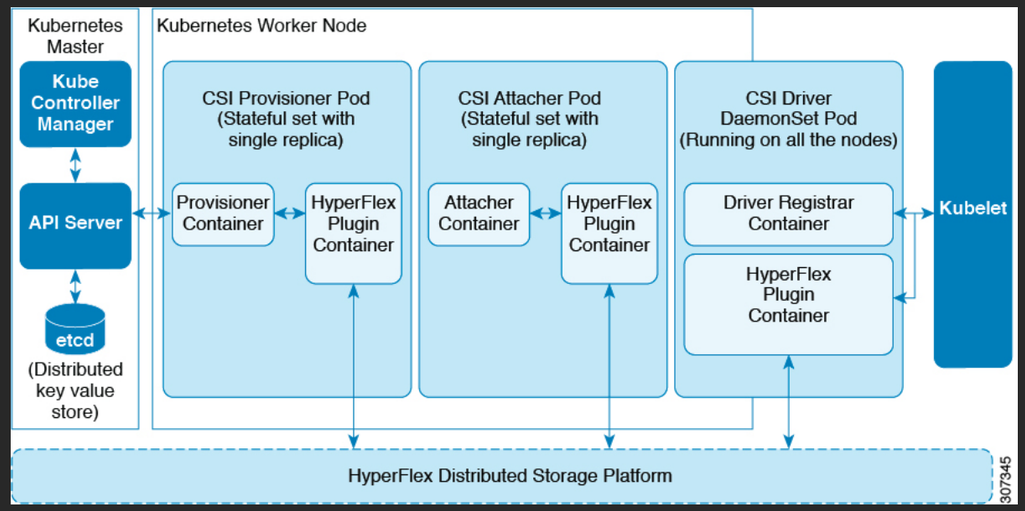
You can select 2 supported plugins from CCP

vSphere Volume – the default class uses the in-tree vSphere Volume storage provisioner (kubernetes.io/vsphere-volume)

A vSphere Volume creates a VMDK (Virtual Machine Disk) and mounts the volume into your pod

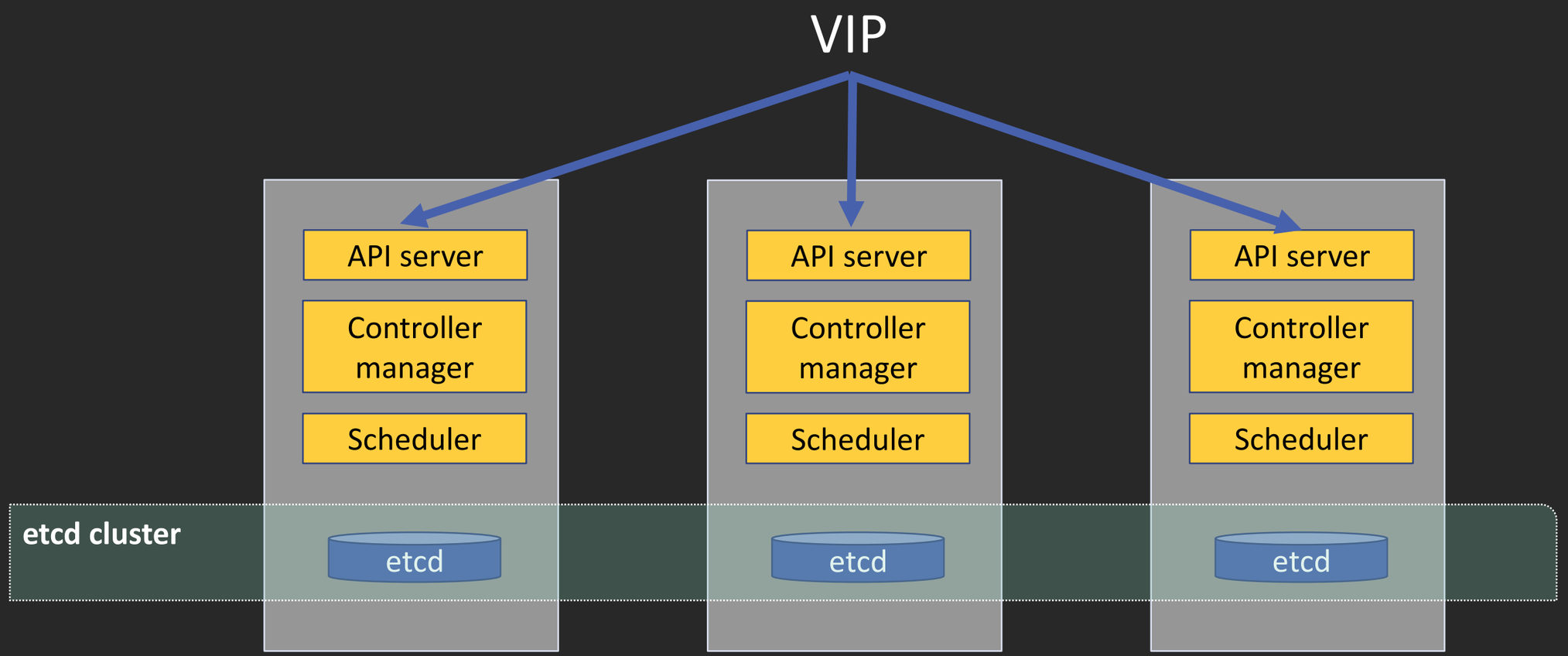


Cisco HyperFlex Container Storage Interface (CSI) is an out-of-tree container-based Kubernetes storage integration, which is deployed and consumed through standard Kubernetes primitives such as Persistent Volume Claims and Storage Classes



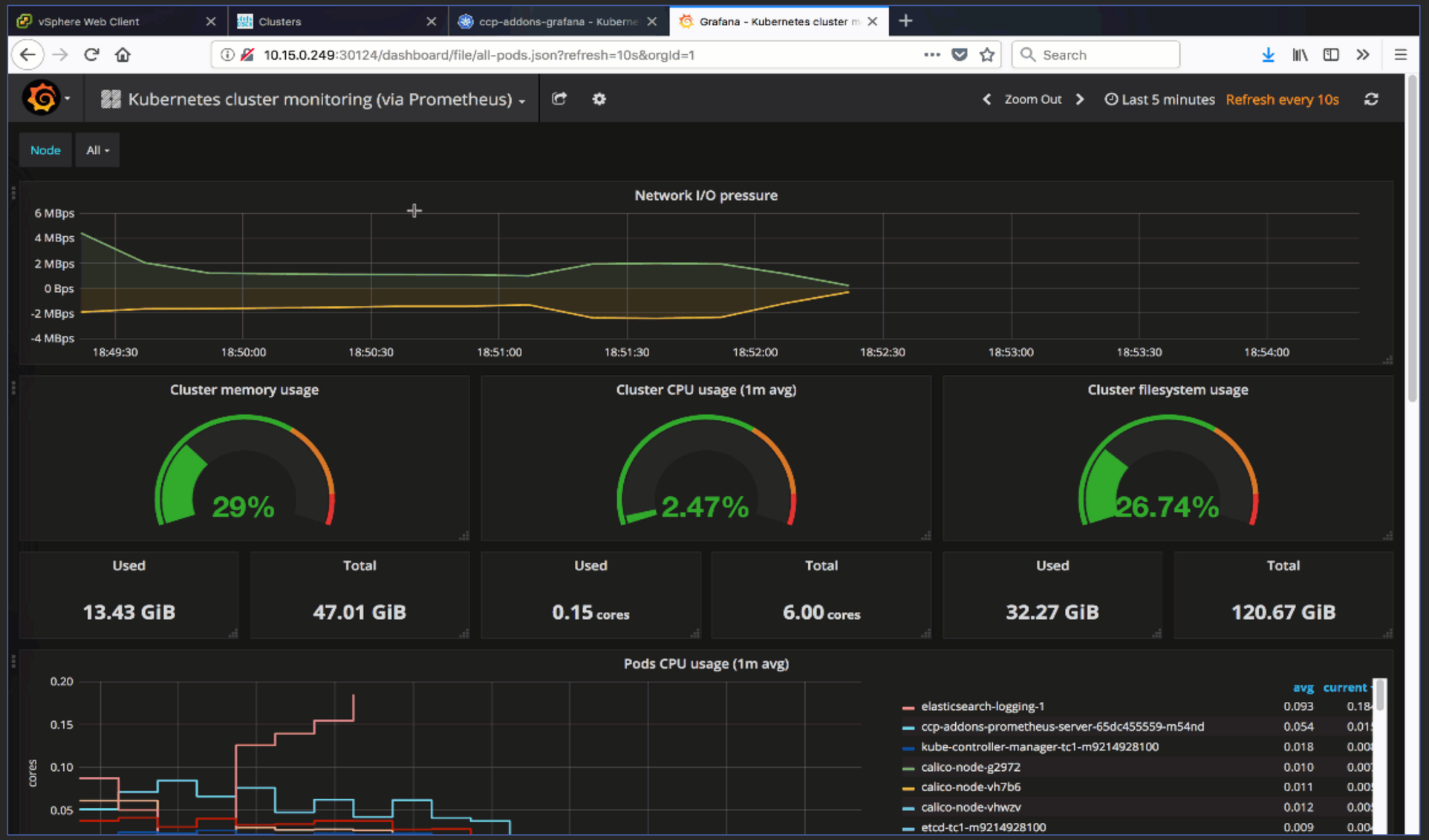
Additional features

High availability multi-master clusters

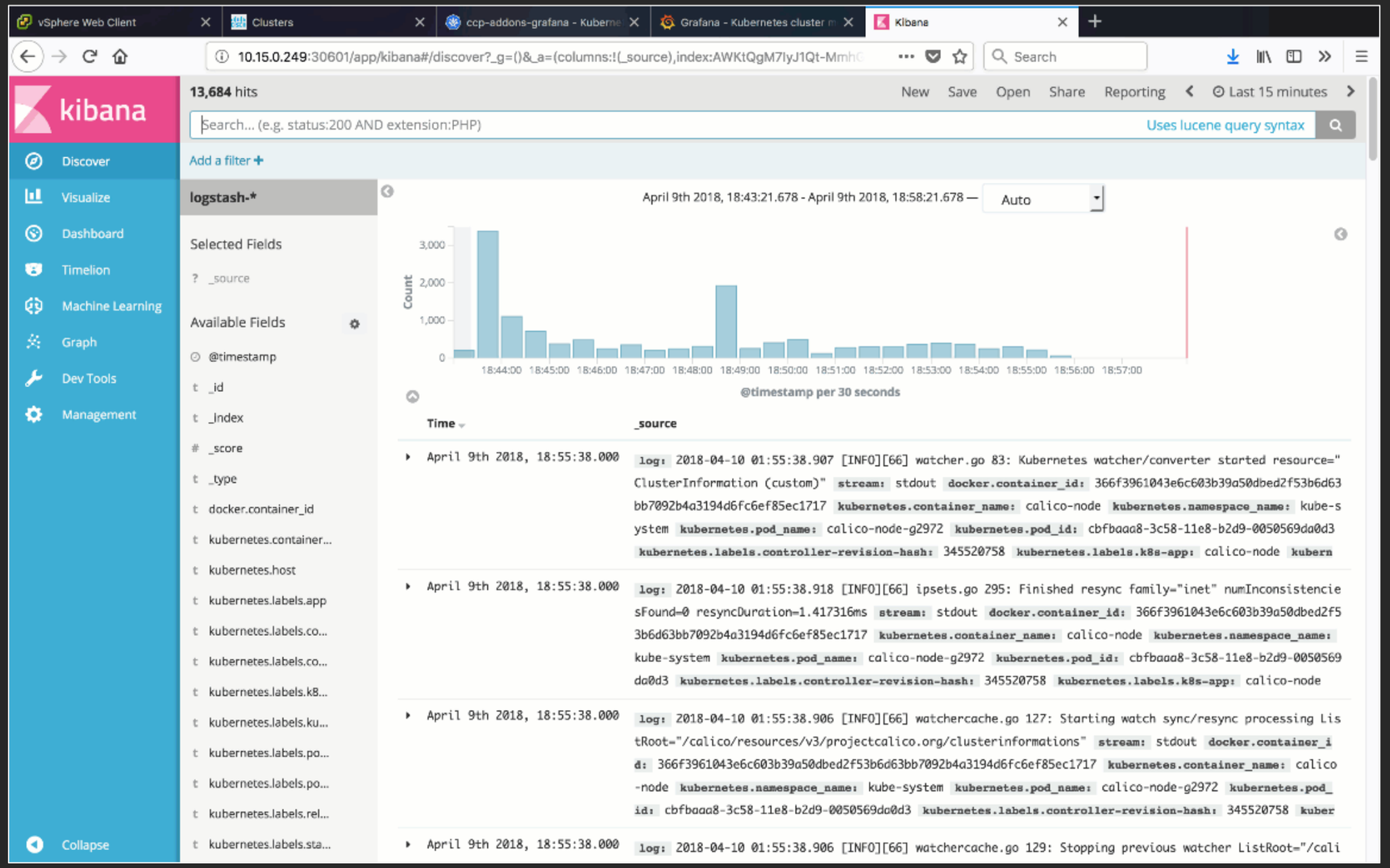


- Can select 1 or 3 masters
- Sustain failure of single master node/etcd
- Upgrade of master nodes does not result in any downtime

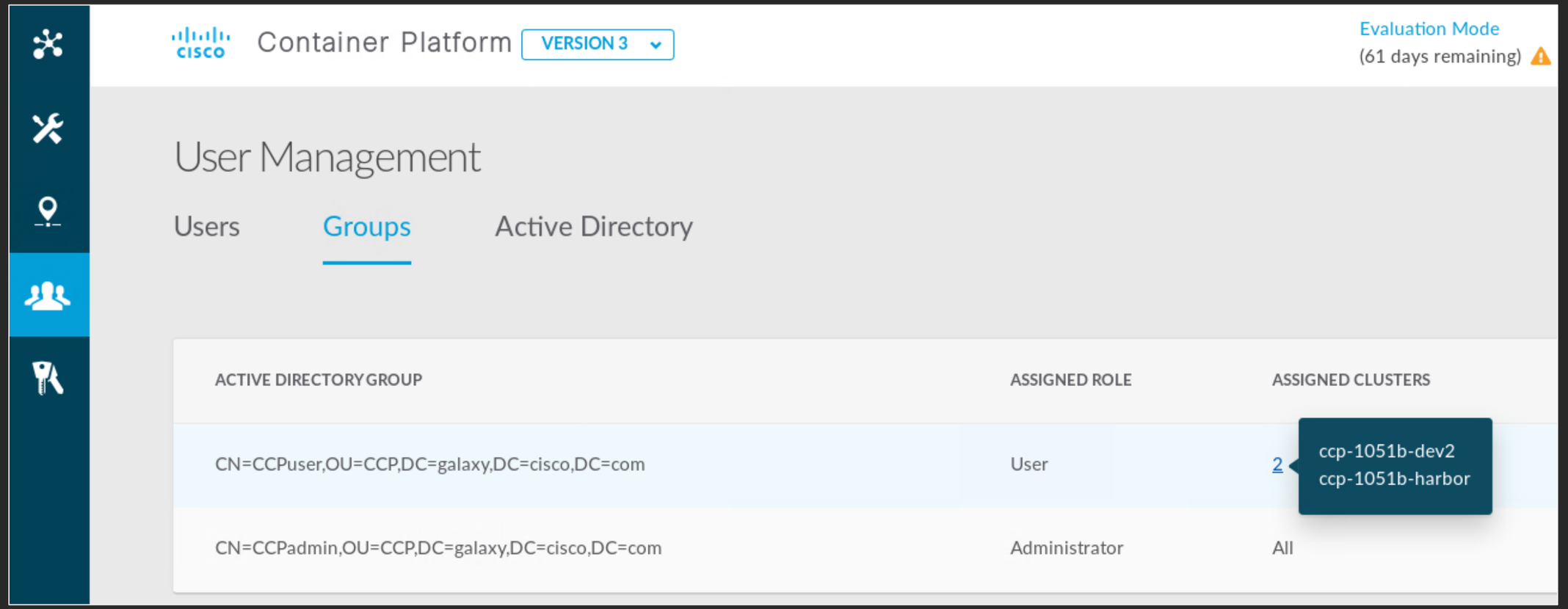
Monitoring with Prometheus and Grafana



Logging with EFK (Amazon Elasticsearch Service, Fluentd, and Kibana)



Role-based access control



Demo

Cisco Container Platform

Turnkey container management software for consistent production-grade Kubernetes

certified kubernetes

- Runs on ANY infrastructure* as a lightweight self-hosted software (optimized for Cisco HX and UCS)
- Automates the installation and deployment of self-service, 100% upstream k8s clusters
- Includes all the necessary networking, storage, logging/ monitoring, load balancing, and registry tooling
- Integrates natively with Amazon EKS
- Built for the enterprise with hardened security and enhanced availability features like multi-master and self-healing
- Optimized for AI/ML workloads with multi-GPU support
- Supported end-to-end by Cisco

**Deployed on top of VMware vSphere, OpenStack/CVIM, bare metal (coming soon)*

Benefits

CXO

Accelerate innovation and reduced time-to-market with consistent k8s

Security

Reduce risk with enterprise-class security, availability, and control

DevOps

Benefit from multiple accepted open-source projects built into an enterprise-supported product

Product details

- Software subscription (1,3, or 5 years)
- Software-only or integrated with hardware
- Sold by Cisco and partners
- Supported end-to-end by Cisco

Come visit us at booth 2220

Don’t miss our other sessions

MGT205-S
Monday, December 2, 4:00 p.m.
Aria, Level 1 East, Joshua 9

Finding the signal in the noise when running cloud-native applications

Speakers:
Aaron Newcomb, Director of Cloud Strategy, AppDynamics (now a part of Cisco)
Marius Dornean, Director of R&D, Mitchell International

NET214-S
Thursday, December 5, 1:45 p.m.
Bellagio, Monet 3

What everyone should know about hybrid cloud networking

Speakers:
Azeem Suleman, Principal Engineer, Data Center Business Group, Cisco
Mayuri Kulkarni, Senior Product Manager, Cisco

Thank you!

Demos are available in booth 2220

AWS re:Invent

aws

Please complete the session survey in the mobile app.