Deep Dive into Elastic Kubernetes Service

Bryan Landes, Solutions Architect
April 22, 2020

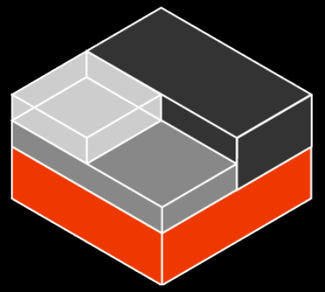
aws SUMMIT

We’re making AWS the best place to run containers and Kubernetes

aws SUMMIT

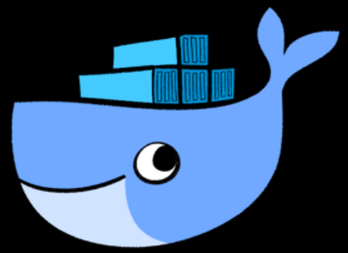
What is a container?

- A lightweight, stand-alone, executable package of software that includes all dependencies: code, runtime, system tools, system libraries, settings.
- Containers isolate software from its surroundings
  - development and staging environments
  - help reduce conflicts between teams running different software on the same infrastructure.
- Long history: chroot, FreeBSD Jails, Solaris Containers, OpenVZ, LXC
- Docker simplified creation/management/operation of containers



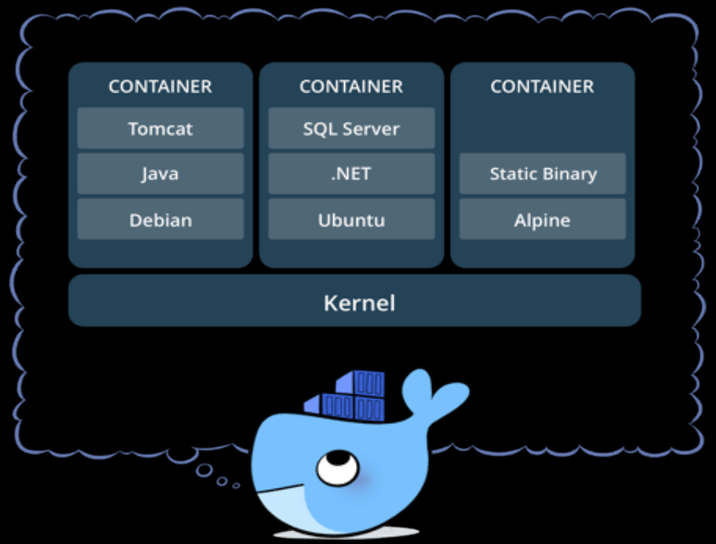
Rocket

containerd



What is a container?

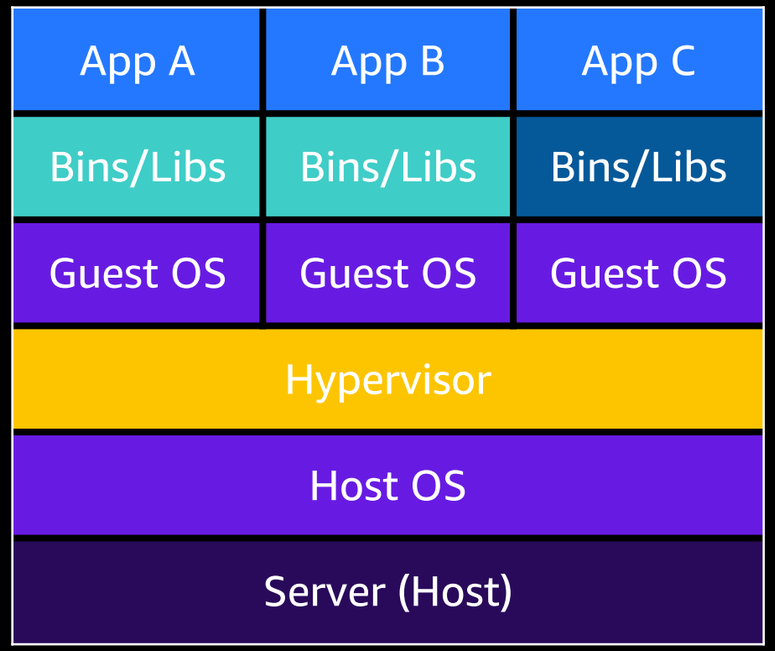
- Containers share a machine's OS kernel.
- They start instantly and use less compute and RAM.
- Images are constructed from filesystem layers and share common files. This minimizes disk usage and image downloads are much faster.



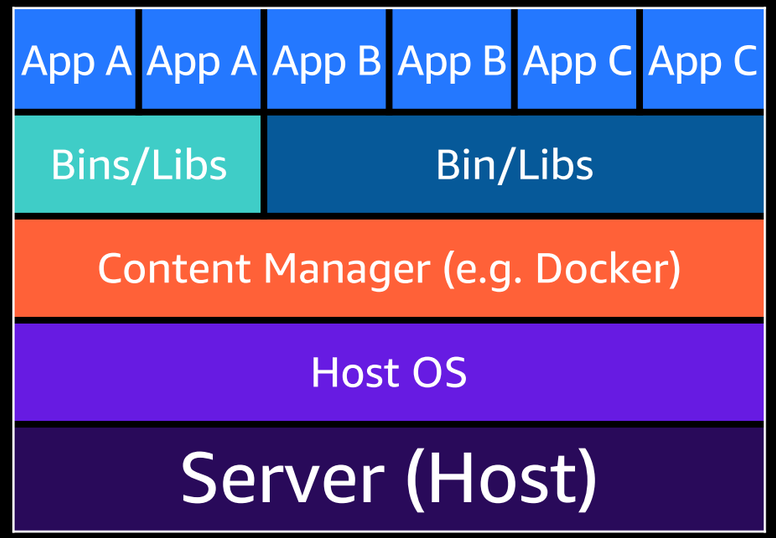
Why are they so popular?

- Portable runtime application environment
- Package application and dependencies in a single artifact
- Run different application versions (different dependencies) simultaneously
- Faster development & deployment cycles
- Better resource utilization

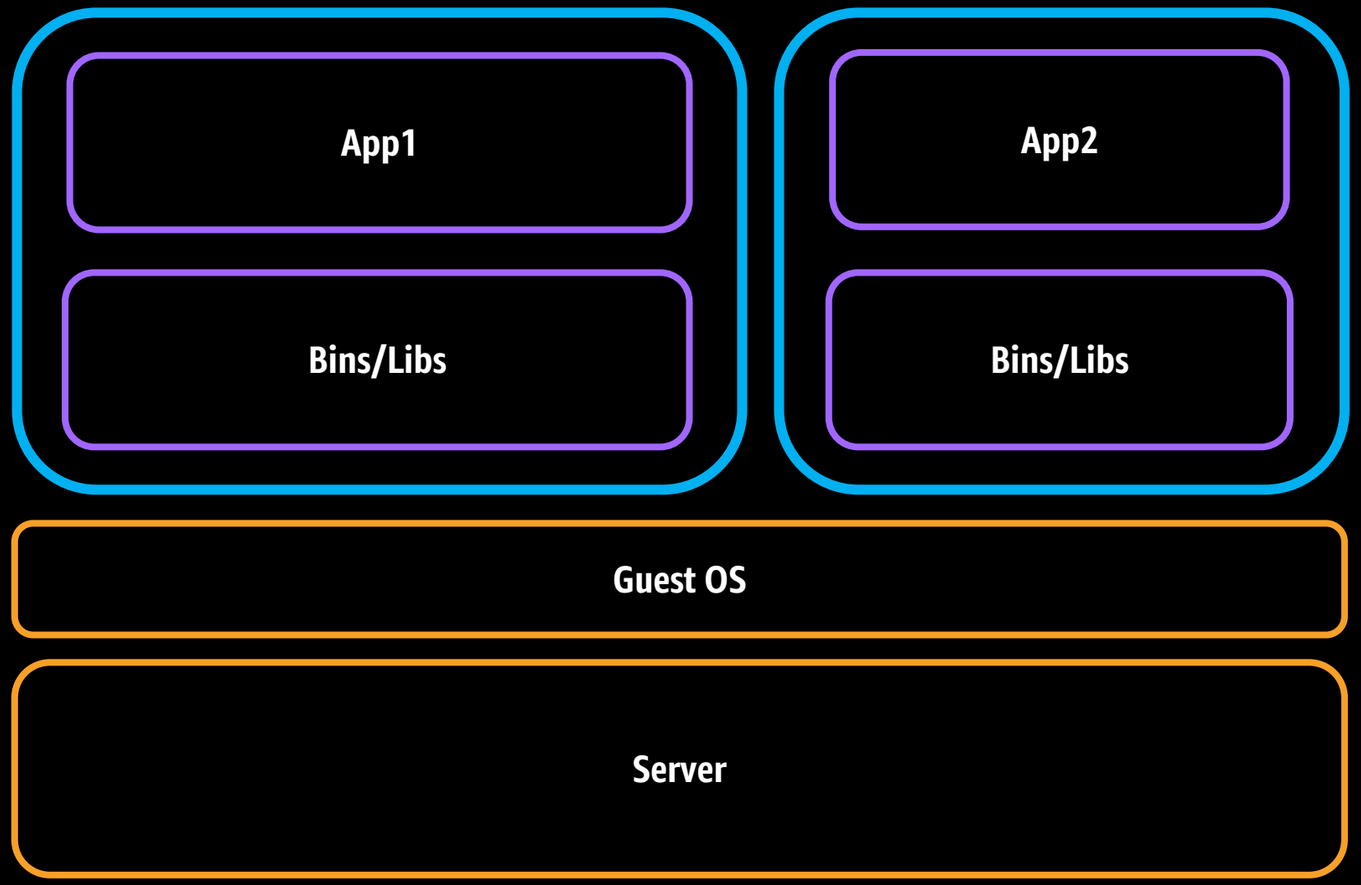
VMs VS. Containers

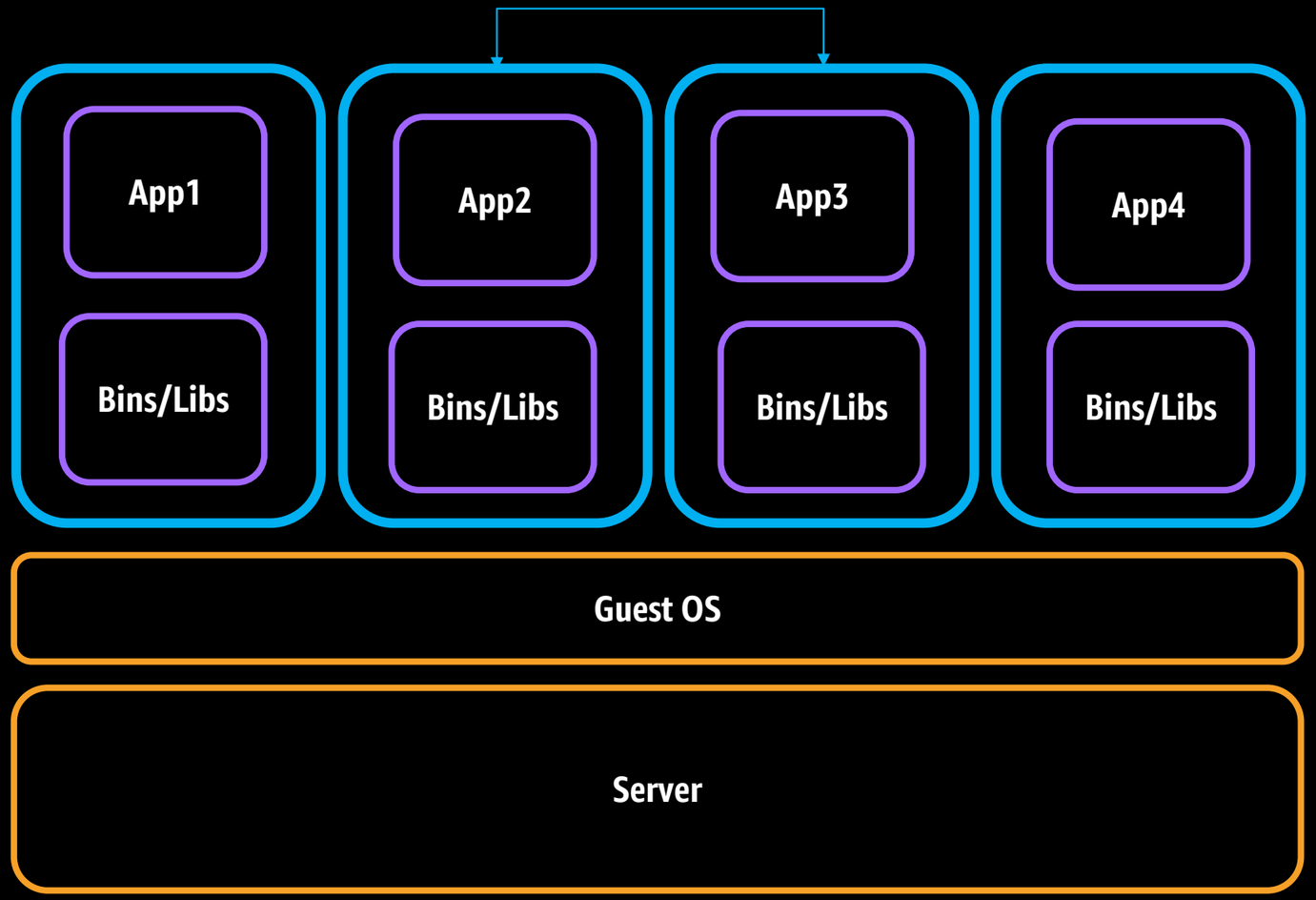


VMs

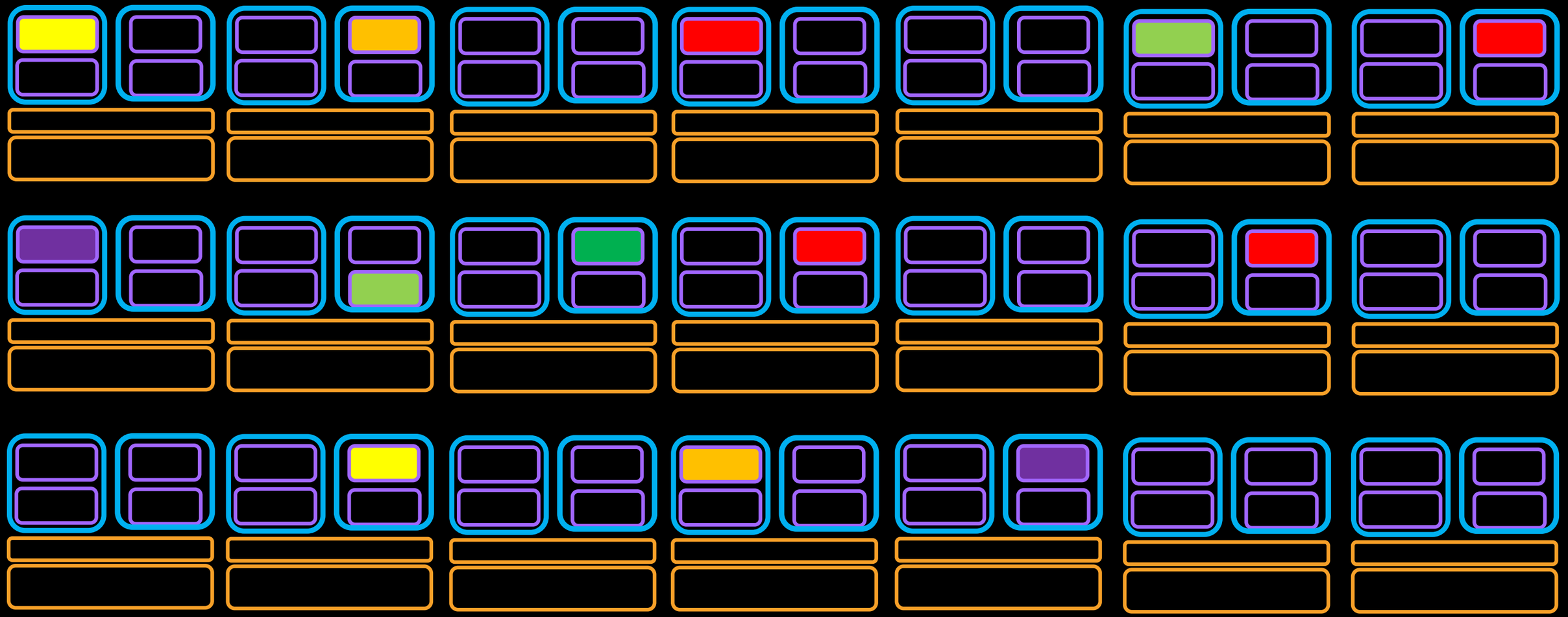


Containers





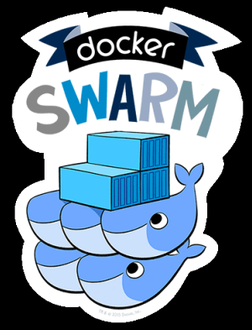
Managing many containers is hard



aws SUMMIT

What are container orchestration tools?

Framework for managing, scaling, deploying containers.



Containers on AWS

aws SUMMIT

AWS container services landscape

Management

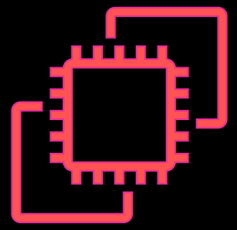
Deployment, scheduling, scaling & management of containerized applications

Amazon Elastic Container Service (Amazon ECS)

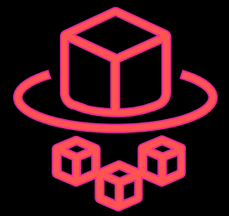
Amazon Elastic Kubernetes Service (Amazon EKS)

Hosting

Where the containers run



Amazon Elastic Compute Cloud (Amazon EC2)



AWS Fargate

Image Registry

Container image repository

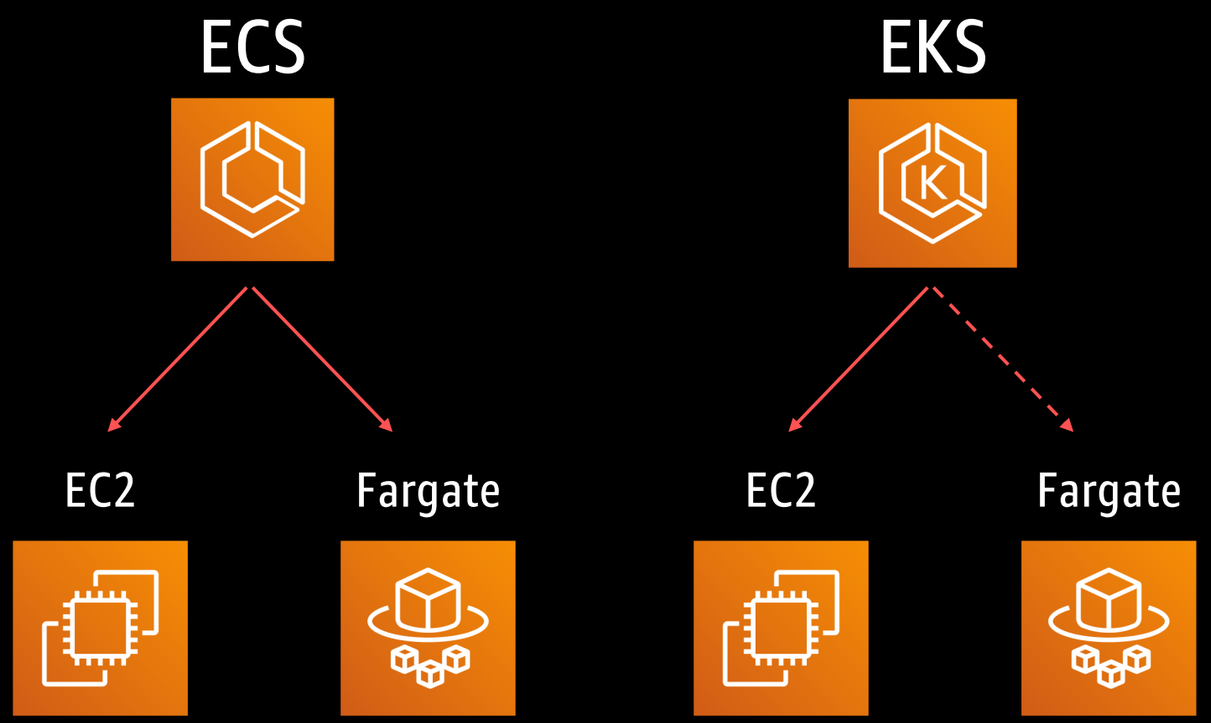
Amazon Elastic Container Registry (Amazon ECR)

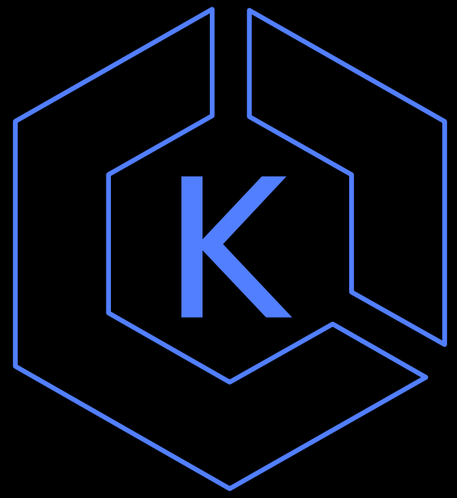
So you want to run a (managed) container on AWS?

AMAZON CONTAINER SERVICES

1 Choose your orchestration tool

2 Choose your launch type

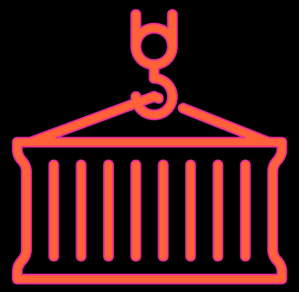




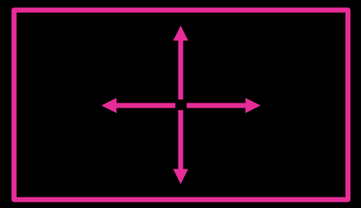
Amazon EKS

aws SUMMIT

What is Kubernetes?



Open-source container-management platform



Helps you run containers at scale

Gives you primitives for building modern applications

Community, contribution, choice

kubernetes

But where you run Kubernetes matters

Quality of the cloud platform

Quality of the applications

Your users

+

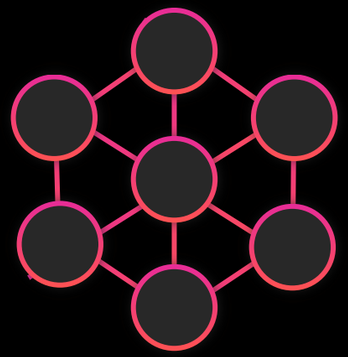
aws

51%

of Kubernetes workloads run on AWS today

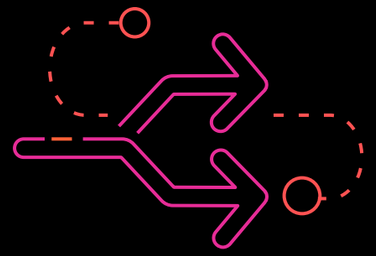
—**CNCF**

How are customers using Amazon EKS?

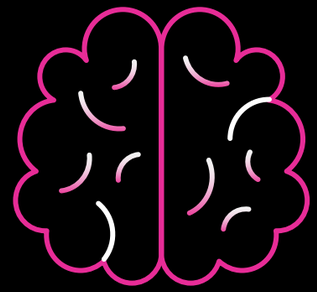


Microservices

Platform as a service



Enterprise app migration



Machine learning

Customers adopting Kubernetes on AWS

Customer example: Snap

"Undifferentiated heavy lifting is work that we have to do that doesn't directly benefit our customers. It's just work. Amazon EKS frees us up to worry about delivering customer value and allows developers without operational experience to innovate without having to know where their code runs."

More detailed talk: AWS New York Summit 2018 - Run Kubernetes with Amazon EKS (SRV318)

Who is using Amazon EKS?

"We built the next generation of our PaaS using Amazon EKS for large enterprise workloads. We manage thousands of applications and have hundreds of DevOps teams."

Rich partner ecosystem

Foundation

CANONICAL

RANCHER

DevOps

pulumi

ATLASSIAN

Monitoring & logging

Security

Networking

aws SUMMIT

Our tenets

1. Amazon EKS is a platform to run **production-grade workloads**. Security and reliability are our first priority. After that we focus on doing the heavy lifting for you in the control plane, including lifecycle-related things like version upgrades.

2. Amazon EKS provides a **native and upstream Kubernetes** experience. Amazon EKS provides vanilla, un-forked Kubernetes. In keeping with our first tenet, we ensure the Kubernetes versions we run have security-related patches—even for older, supported versions—as quickly as possible. But there's no special sauce and no lock-in.

3. If you want to use additional AWS services, **integrations** are as **seamless** as possible.

4. The Amazon EKS **team** at AWS **actively contributes** to the **upstream Kubernetes** project and the wider CNCF activities, both on the technical level as well as community, from communicating good practices to participation in SIGs and working groups.

Amazon EKS, a year in review

June – December 2018:

Amazon EKS achieves K8s conformance, HIPAA-eligibility, generally available
Amazon EKS AMI build scripts and AWS CloudFormation templates available in GitHub
Support for GPU-enabled EC2 instances, support for HPA with custom metrics
Amazon EKS launches in Dublin, Ireland
Amazon EKS simplifies cluster setup with `update-kubeconfig` CLI command
Amazon EKS adds support for Dynamic Admission Controllers (Istio), ALB Support with the AWS ALB ingress controller
Amazon EKS launches in Ohio, Frankfurt, Singapore, Sydney, and Tokyo
Amazon EKS adds Managed Cluster Updates and Support for Kubernetes Version 1.11, CSI Driver for Amazon Elastic Block Store (Amazon EBS)

2019:

Amazon EKS launches in Seoul, Mumbai, London, and Paris
Amazon EKS achieves ISO and PCI compliance, announces 99.9% SLA, cluster creation limit raised to 50
API server endpoint access control, AWS App Mesh controller
Windows support (preview), Kubernetes version 1.12
CSI drivers for Amazon Elastic File System (Amazon EFS), Amazon FSx for Lustre, control plane logs, A1 (ARM) instance support (preview)
Deep Learning Benchmark Utility, public IP address support
Simplified cluster authentication, SOC compliance, Kubernetes 1.13, PodSecurityPolicies
Container Insights, CNI 1.5.0, Amazon ECR, AWS PrivateLink support

Pre-re:Invent - 2019

AWS App Mesh controllers for Kubernetes are now available as Helm Charts

Amazon EKS Increases Limits to 100 Clusters per Region

Amazon EKS now available in the Canada (Central) Region

Amazon EKS adds support for provisioning and managing Kubernetes worker nodes

AWS supports Automated Draining for Spot Instance Nodes on Kubernetes

Amazon EKS Generally Available in São Paulo Region

Amazon ECS Service Events Now Available as CloudWatch Events

ECS container monitoring now available in Amazon CloudWatch Container Insights

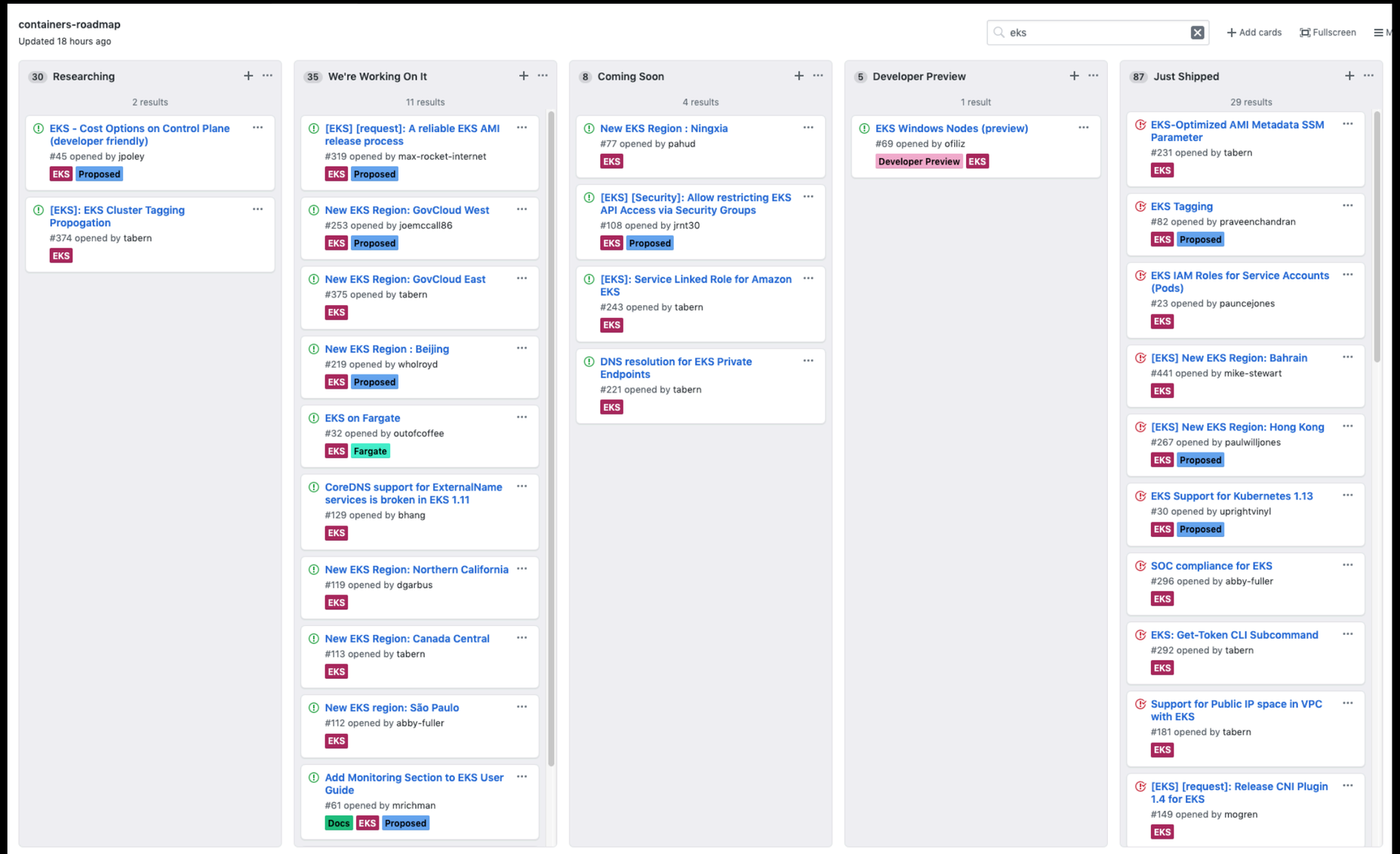
AWS launches FireLens, a log router for Amazon ECS and AWS Fargate

Amazon Elastic Container Service publishes multiple GitHub Actions

ECR events now published to EventBridge

Open-source roadmap

https://github.com/aws/containers-roadmap/



Amazon EKS services roadmap: Highlights

Shipped

- Amazon EKS control plane logs
- Support for public IP space in VPC
- SOC compliance
- Amazon EKS: Deep Learning Benchmarking Utility
- New Amazon EKS Regions: Paris, London, Mumbai
- CNI v1.5.0

Shipped

- Amazon EKS support for K8s version 1.15 + ECR AWS PrivateLink
- Amazon EKS and KMS integration
- New Amazon EKS Regions: Beijing, Hong Kong, Sao Paulo, Canada Central
- Managed Worker Nodes / Fargate
- DNS resolution of Amazon EKS private endpoints

Working on it

- Managed add-ons
- New Amazon EKS Regions: Ningxia
- Next-generation CNI plugin

Amazon EKS deep dive

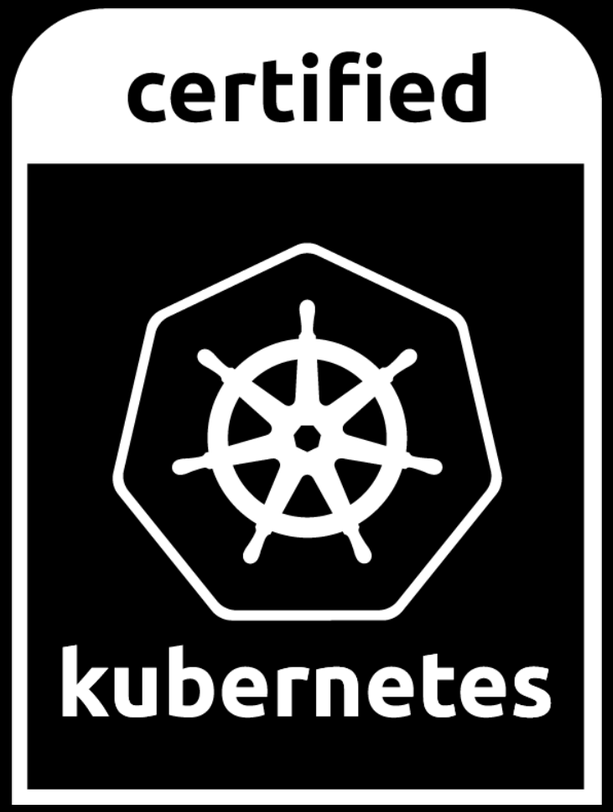
- Configuration & setup
- Availability
- Storage
- Operations
- Security
- Networking
- Logging
- Monitoring
- Application communication

aws SUMMIT

Configuration & setup

aws SUMMIT

Amazon EKS is Kubernetes-certified



Kubernetes conformance

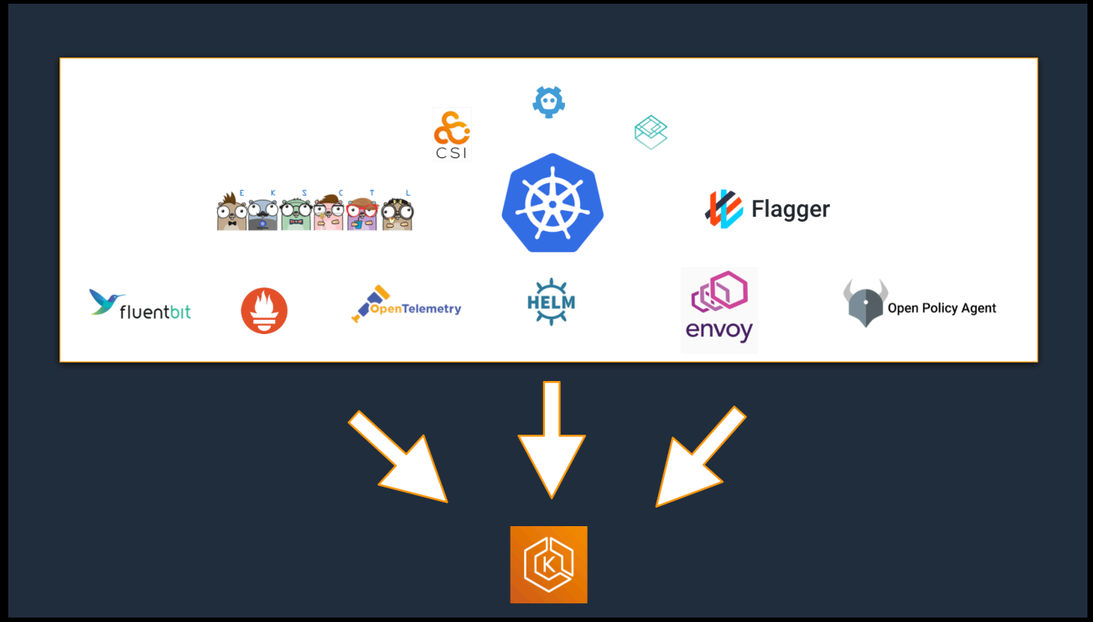
- Guaranteed portability and interoperability
- Timely updates
- Confirmability

Open-source and Amazon EKS

Amazon EKS runs 100% upstream Kubernetes

Key components of Amazon EKS are open source

- Amazon VPC CNI plugin
- AWS Identity and Access Management (IAM) authenticator
- Amazon EKS AMI



Team contributes to or manages 20+ OSS projects

- /kubernetes
- /kubernetes/autoscaler
- /aws-labs/aws-service-operator
- /weaveworks/eksctl
- Amazon EBS, Amazon EFS, Amazon FSx CSI drivers

Kubernetes versions

Latest: 1.15
Amazon EKS will support up to three versions of Kubernetes at once

Deprecation in line with the community stopping support for older versions

eksctl—a CLI for Amazon EKS

- Single command cluster creation

```
eksctl create cluster --nodes=4
```

- Open source and on GitHub
- Built by Weave and AWS
- Official Amazon EKS CLI

Bring your own instances
Instance flexibility

Standard EC2 compute instance types

P2 and P3 accelerated instances

i3 bare metal

Spot Instances

Bring your own OS
Amazon EKS AMI build scripts

https://github.com/awslabs/amazon-eks-ami

Source of truth for Amazon EKS Optimized AMI

Easily build your own Amazon EKS AMI with Packer

Build assets for Amazon EKS AMI for each supported Kubernetes version

Amazon EKS-optimized GPU AMI

Includes NVIDIA packages to support Amazon P2 and P3 instances

Easily run TensorFlow on Amazon EKS

Now supporting P3dn.24xlarge instances

CUDA 10 with NVIDIA v410 coming soon!

Windows containers

Run Windows containers and Windows Server nodes with Amazon EKS

Supports heterogeneous (mixed) clusters

Kubernetes version 1.11+

Available in all Amazon EKS Regions

Developer preview:
https://github.com/aws/containers-roadmap

Bottlerocket OS

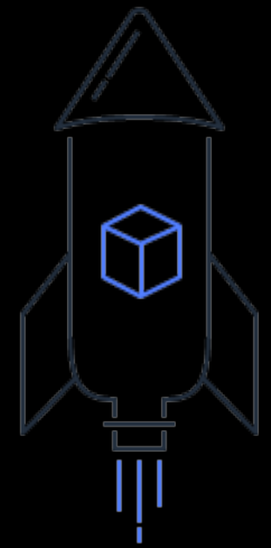
Free and open-source Linux-based operating system meant for hosting containers.

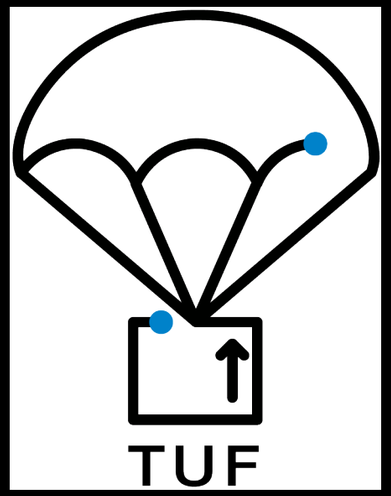
API access for configuring your system, with secure out-of-band access methods when you need them.

Updates based on partition flips, for fast and reliable system updates.

Modeled configuration that's automatically migrated through updates.

Security as a top priority.





Provisioning worker nodes

AWS CloudFormation

eksctl

eksctl

Terraform
Pulumi
Rancher

. . . and more

Partners

Availability

aws SUMMIT

Global availability

Americas

Virginia, Ohio, Oregon

EMEA

Ireland, Frankfurt, London, Paris, Stockholm

Asia Pacific

Bahrain, Hong Kong, Singapore, Tokyo, Sydney, Seoul, Mumbai

Service level agreement

99.95%

Service commitment

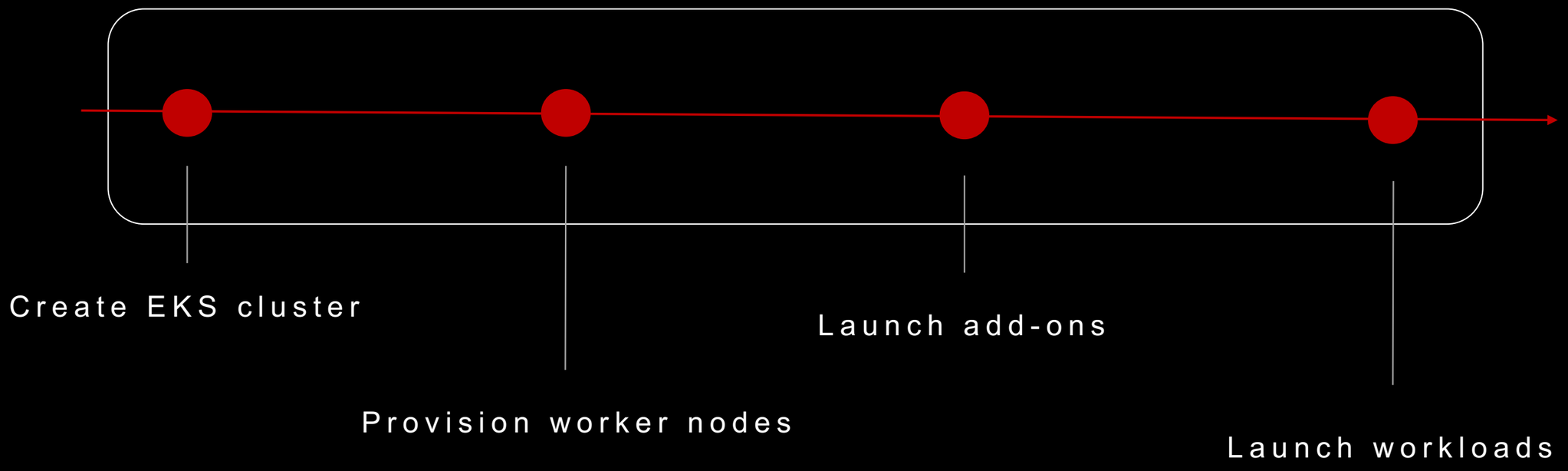
AWS will use commercially reasonable efforts to make the endpoint for an Amazon EKS cluster available with a monthly uptime percentage of at least 99.95% during any monthly billing cycle.

In the event Amazon EKS does not meet the monthly uptime percentage commitment, you will be eligible to receive a Service Credit.

Architecture

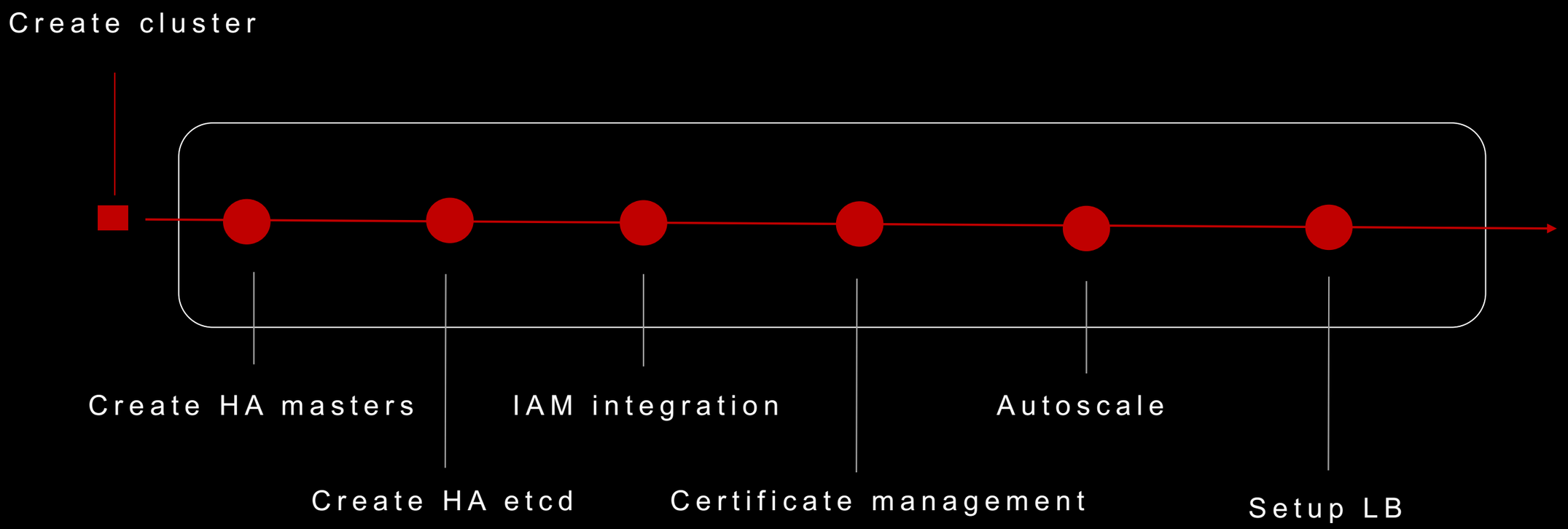
aws SUMMIT

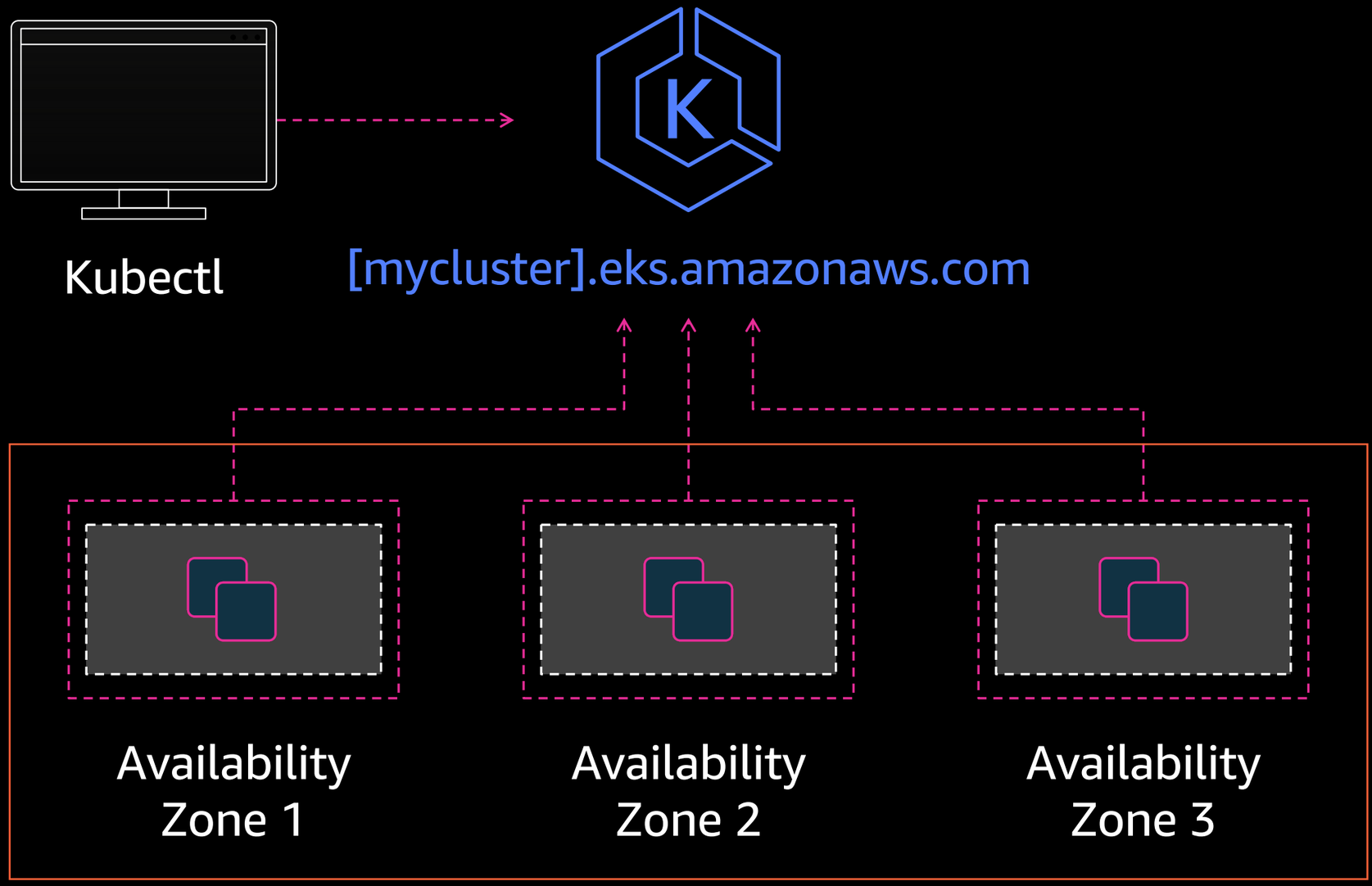
EKS Customers



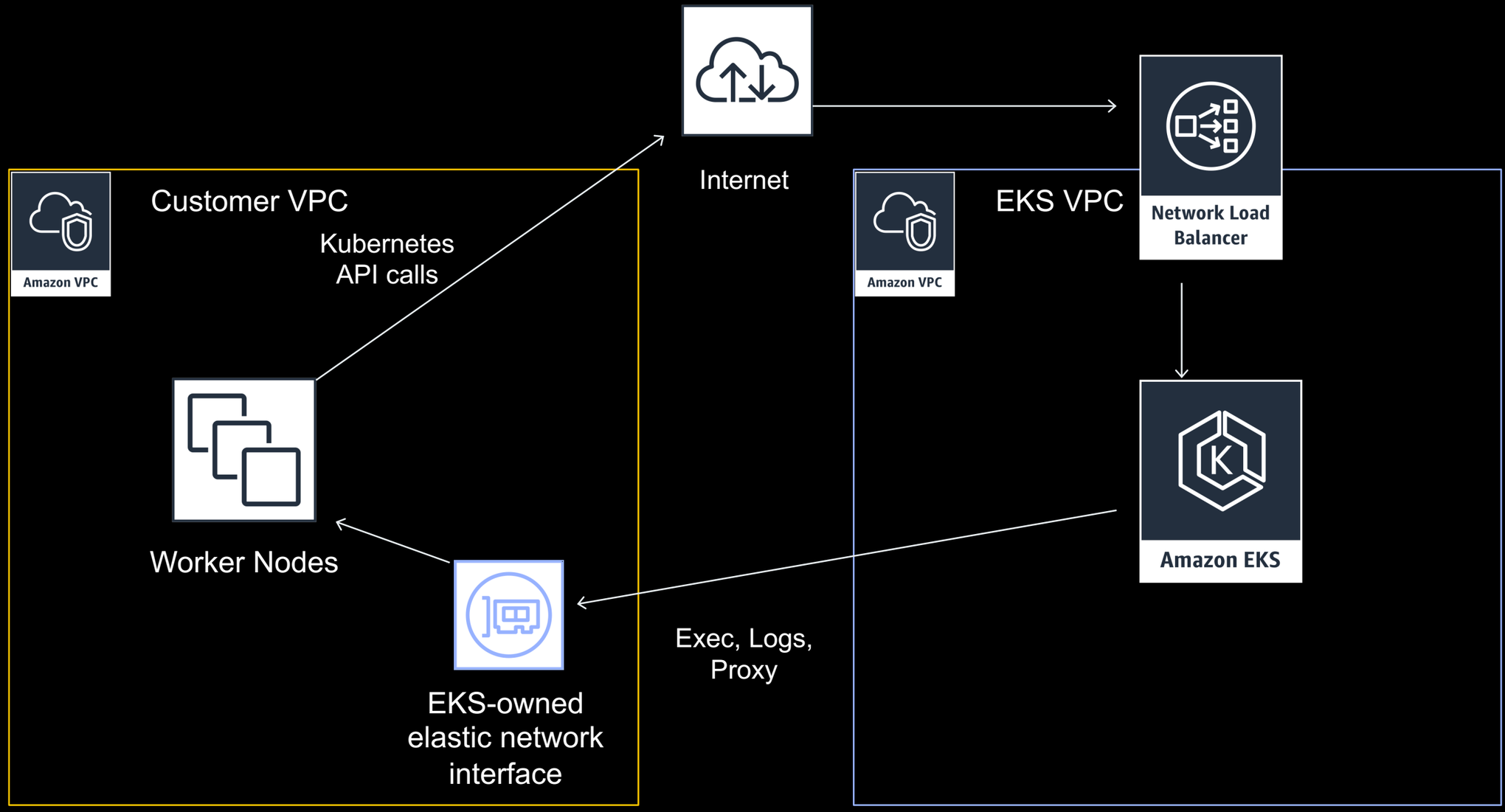
aws SUMMIT

EKS – Kubernetes masters



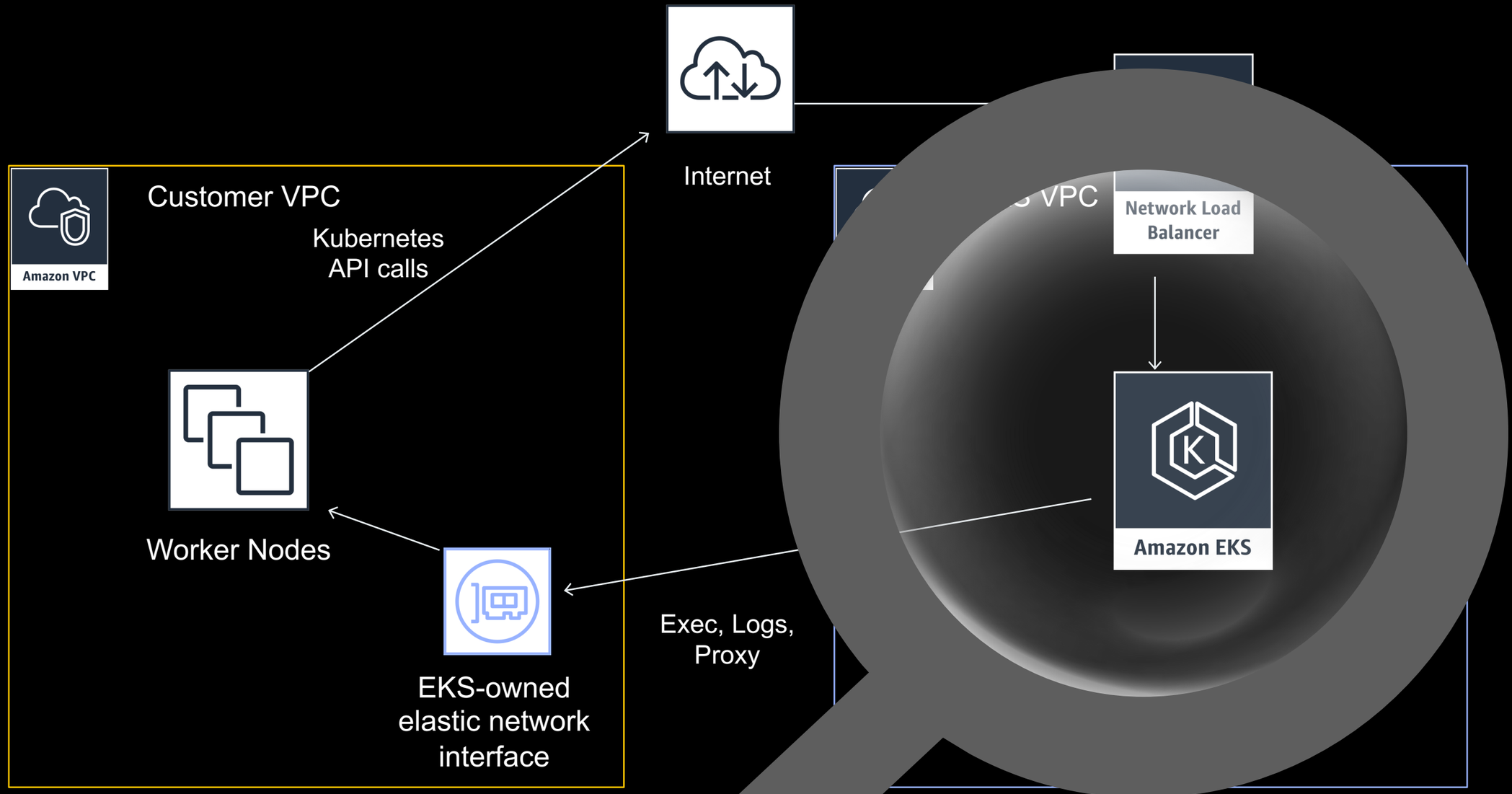


Amazon EKS Architecture



aws SUMMIT

Amazon EKS Architecture

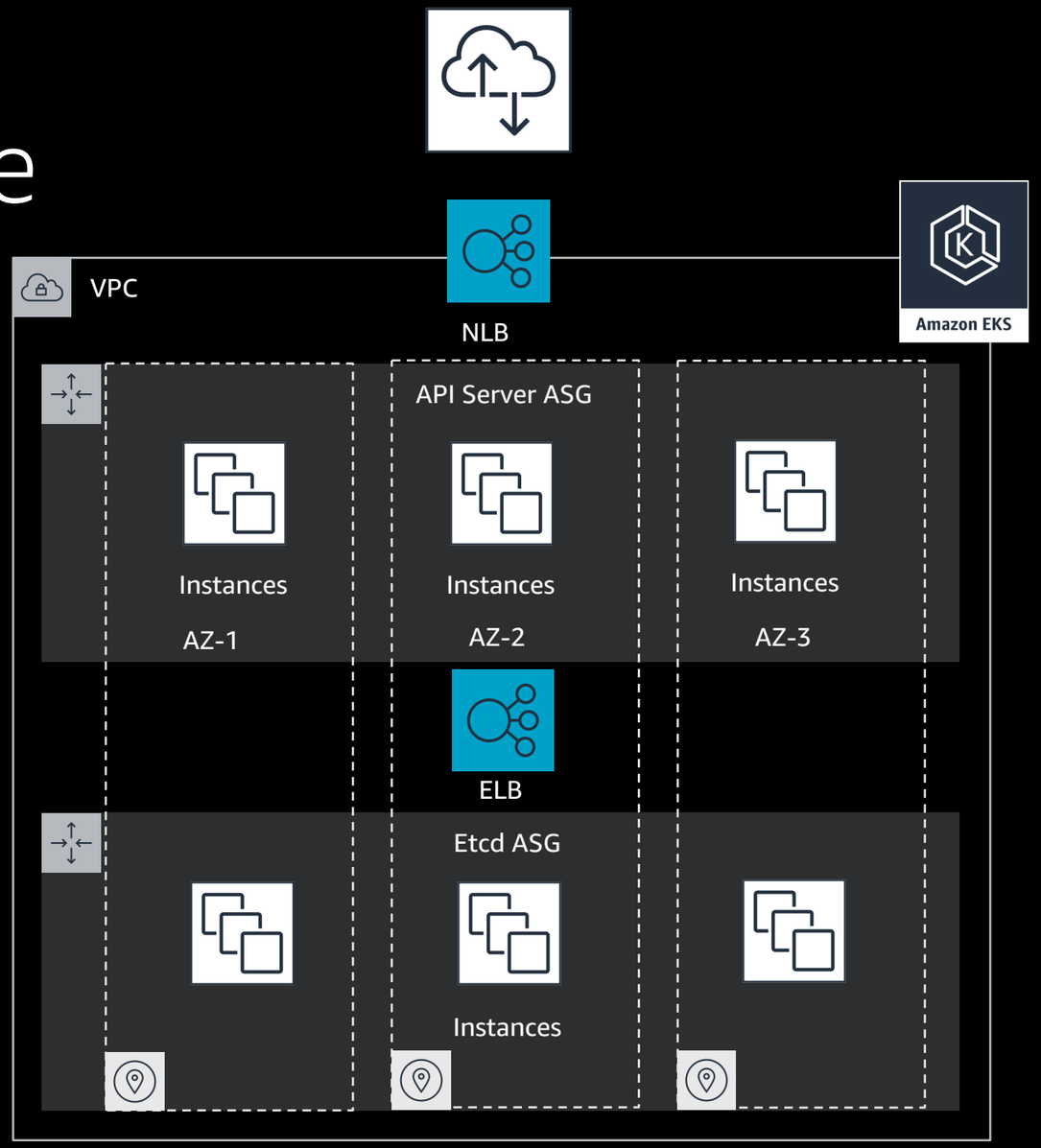


Kubernetes Control Plane

Highly available and single tenant infrastructure

All “native AWS” components

Fronted by an NLB

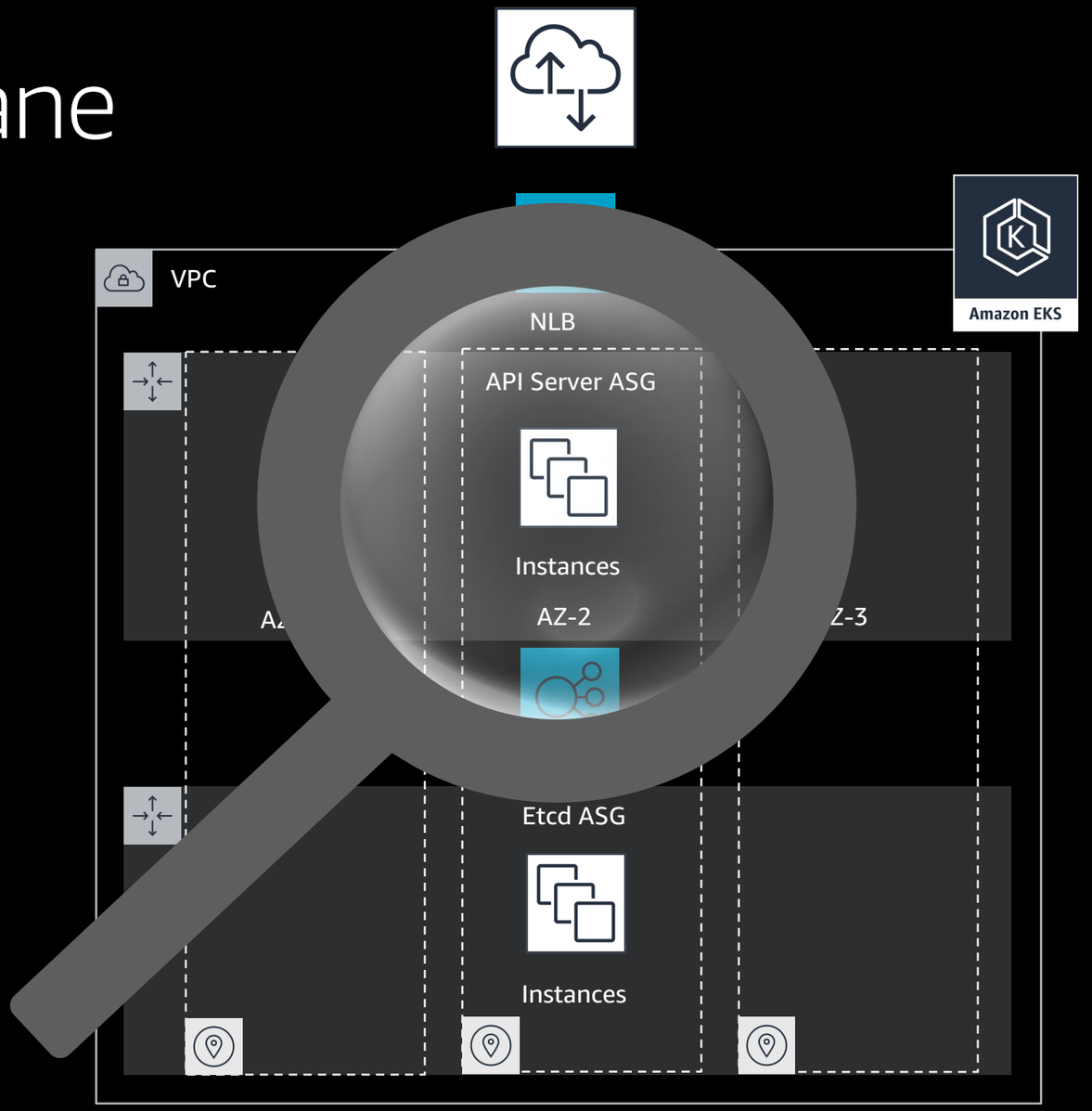


Kubernetes Control Plane

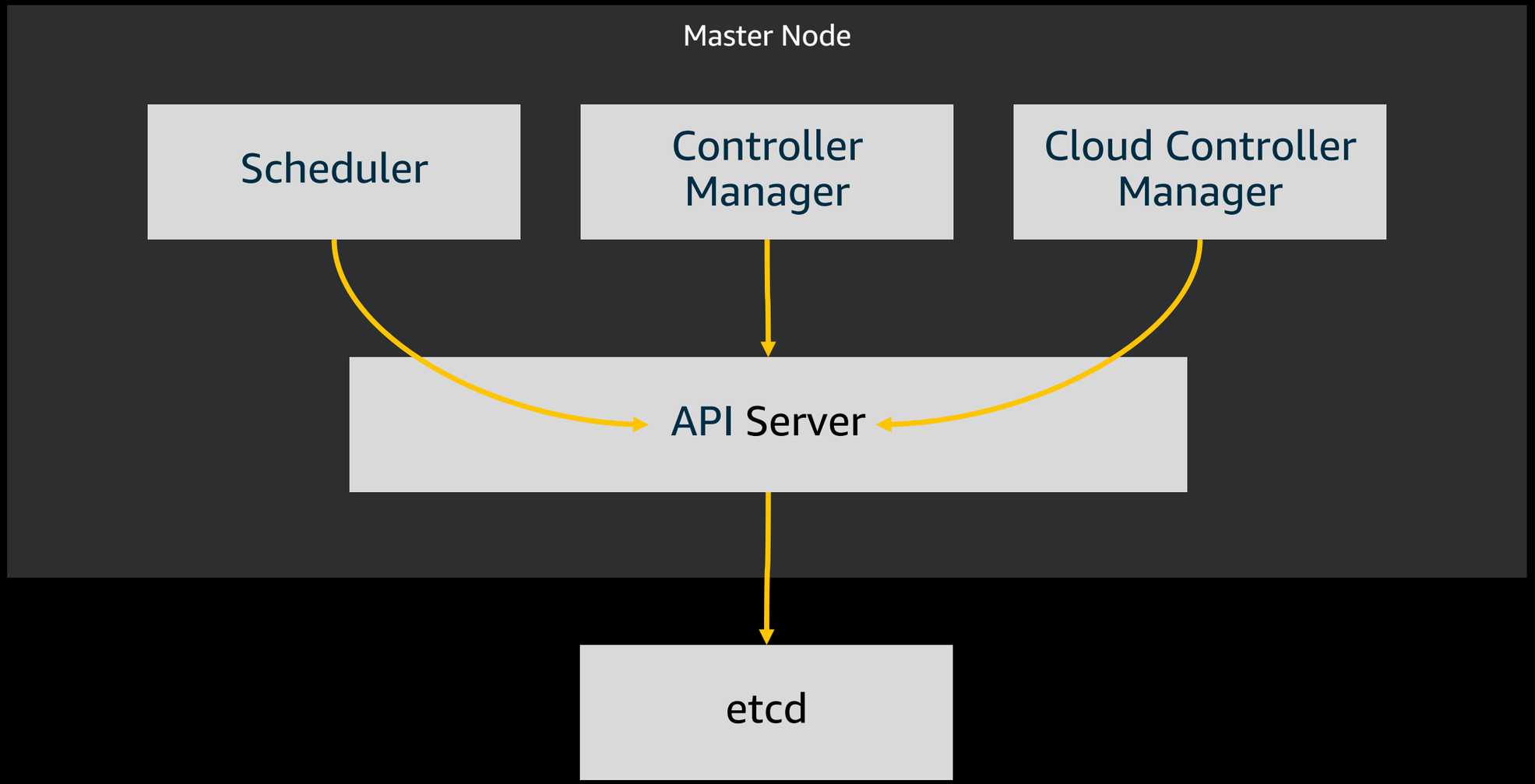
Highly available and single tenant infrastructure

All “native AWS” components

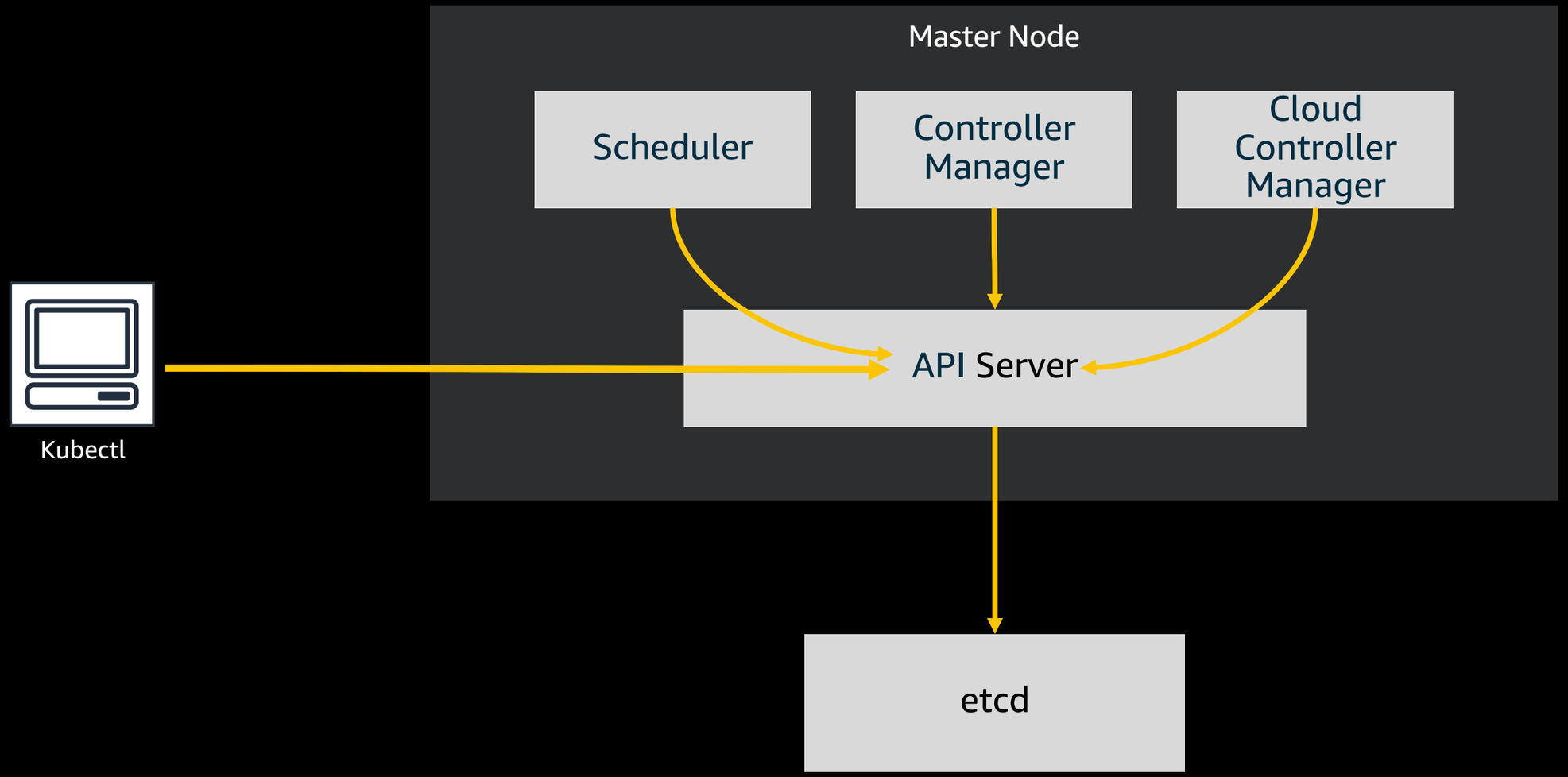
Fronted by an NLB



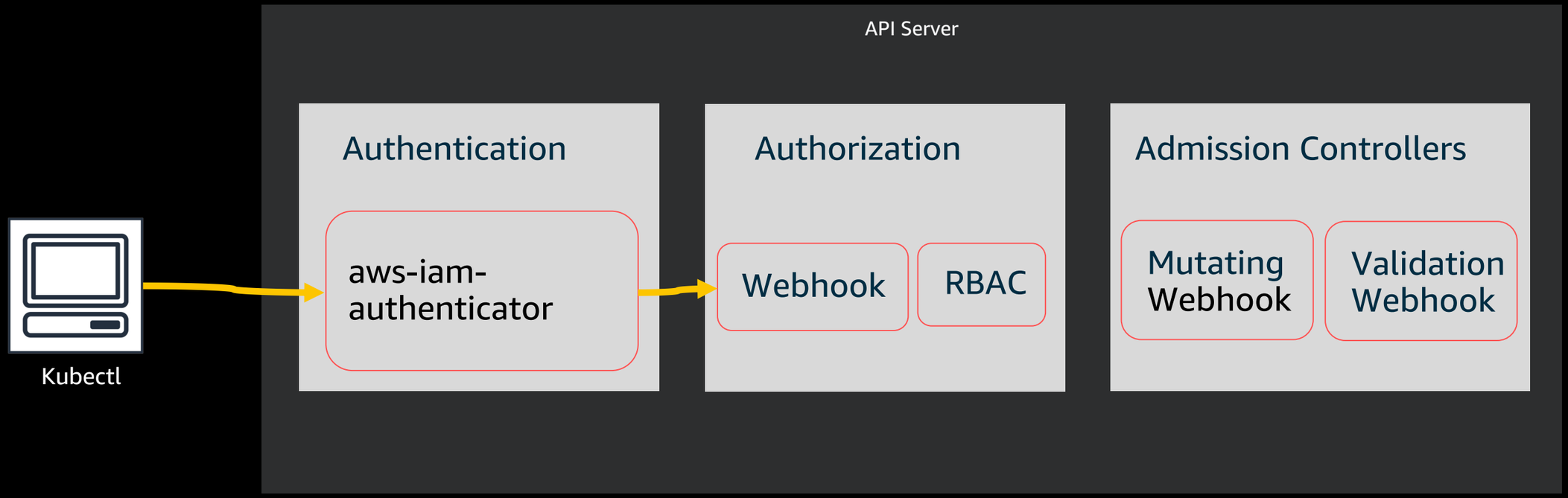
Kubernetes Control Plane



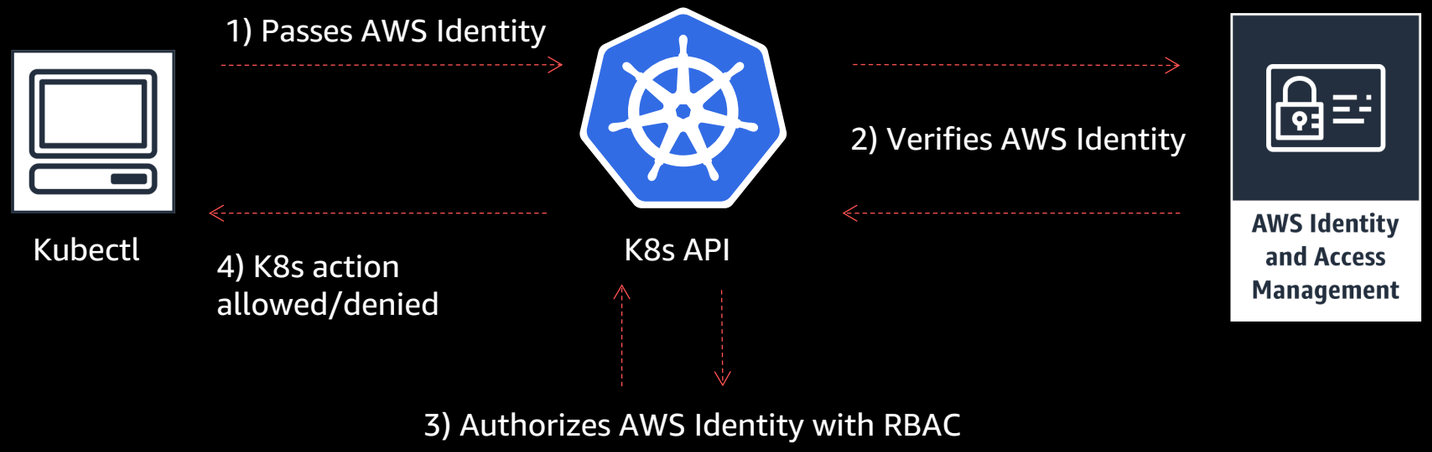
Kubernetes Control Plane



Kubernetes API Server



IAM Authentication

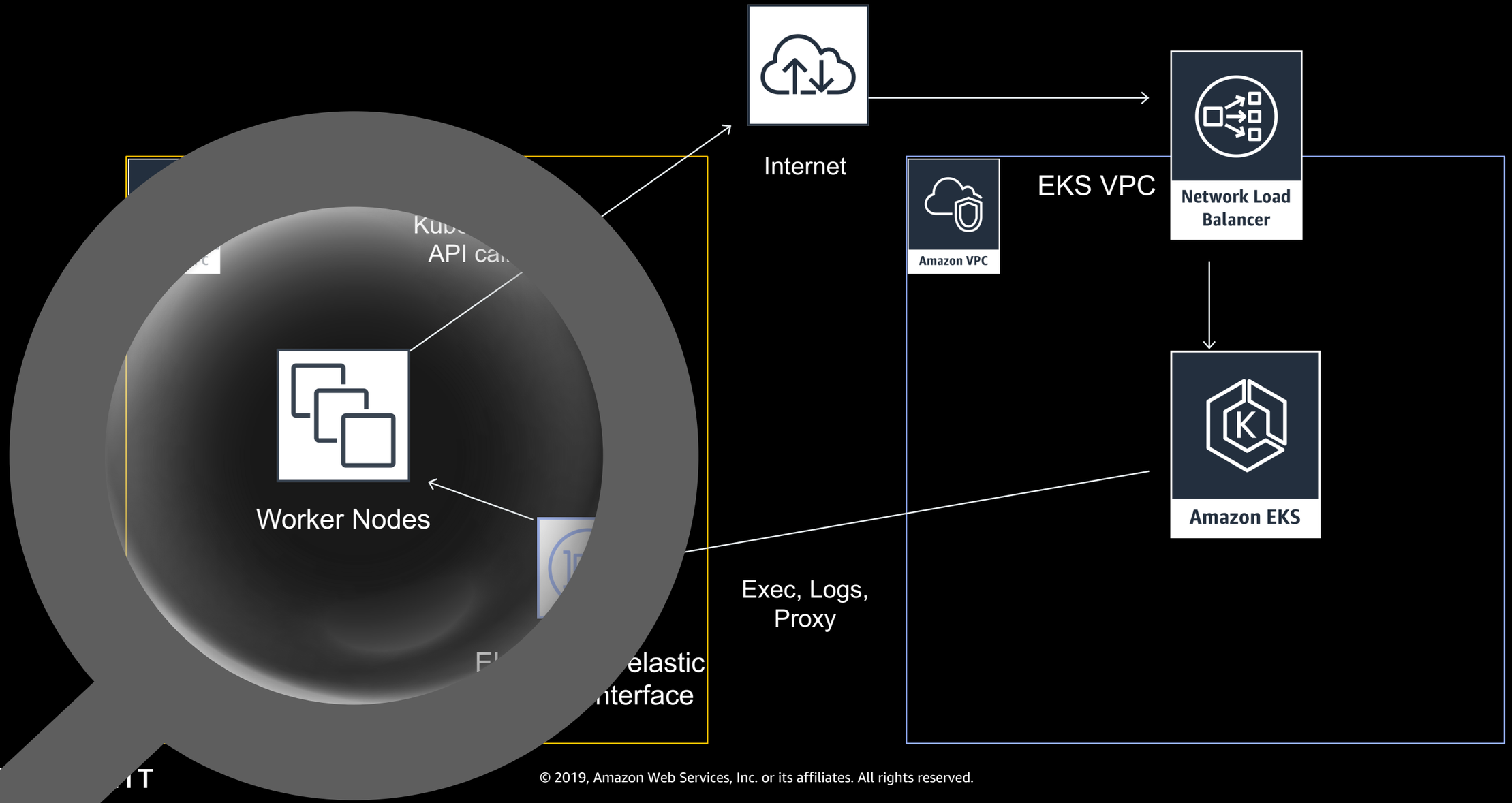


Cluster Authentication and Authorization

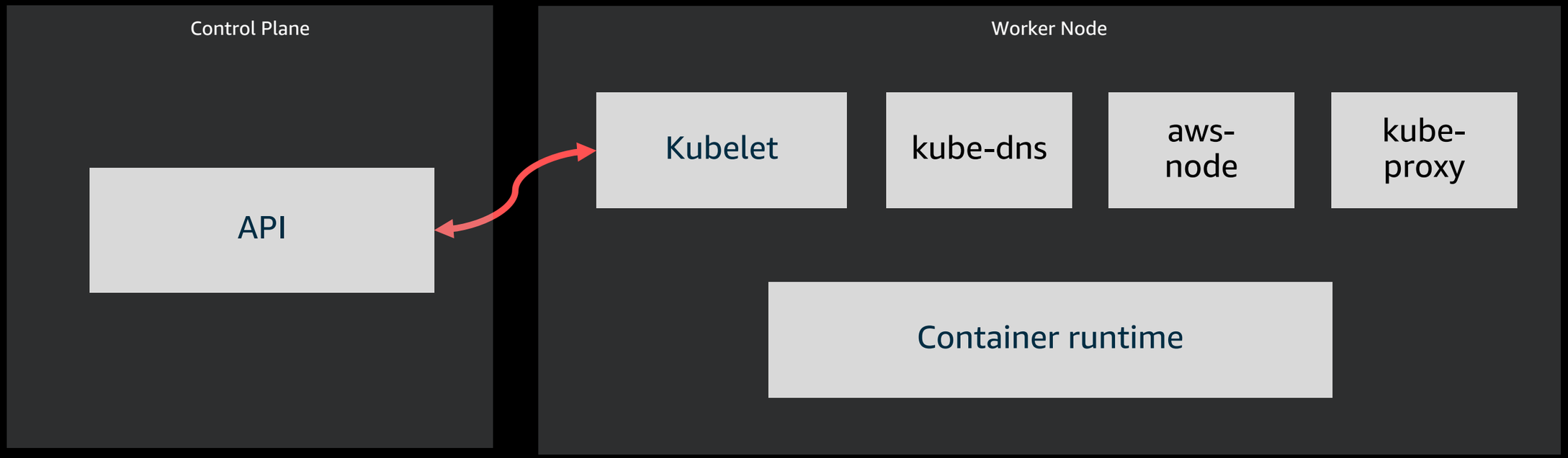
- User or IAM role who **creates** Amazon EKS cluster gains Admin privileges
- This {“super”} user/role can then add additional users or IAM roles and configure RBAC permissions
- To add, configure aws-auth Configmap

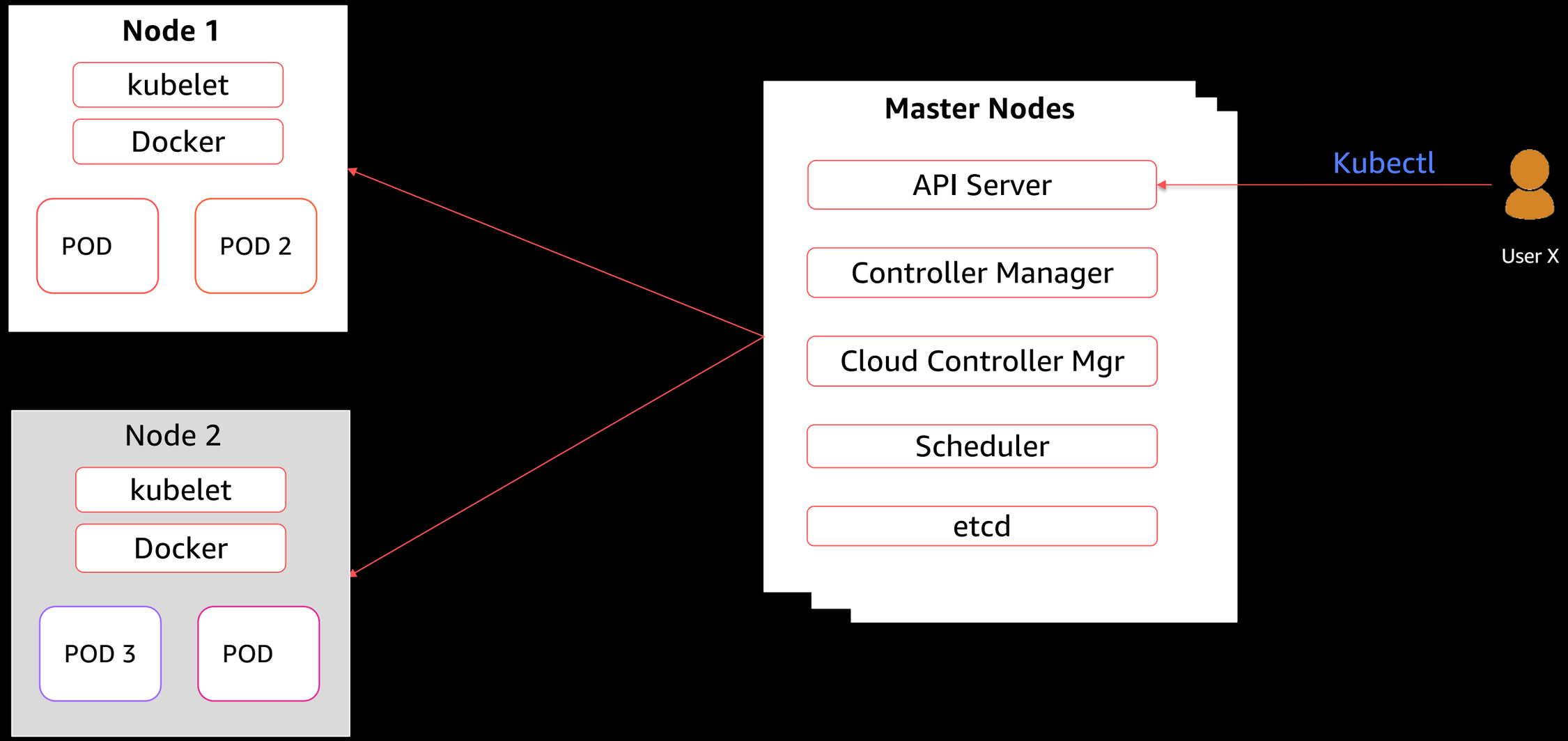
```
kubectl edit -n kube-system configmap/aws-auth
```

Kubernetes Data Plane



Kubernetes Data Plane





EKS and Fargate

aws SUMMIT

Containers

General Availability

Introducing

Amazon EKS for AWS Fargate

The only way to run serverless Kubernetes containers securely, reliably, and at scale

Simplified deployment, management, and scaling of Kubernetes on AWS

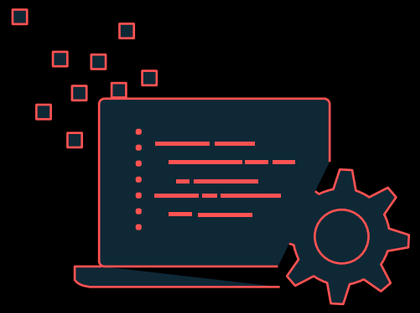
Strong security isolation for every pod by default

Focus on building applications

LEARN MORE	CON-326R - Running Kubernetes Applications on AWS Fargate

aws SUMMIT

Make Kubernetes apps serverless with Amazon EKS + Fargate



Bring existing pods

You don’t need to change your existing pods. Fargate works with existing workflows and services that run on Kubernetes.

Production ready

Launch ten or tens of thousands of pods in seconds. Easily run pods across multiple AZs for high-availability.

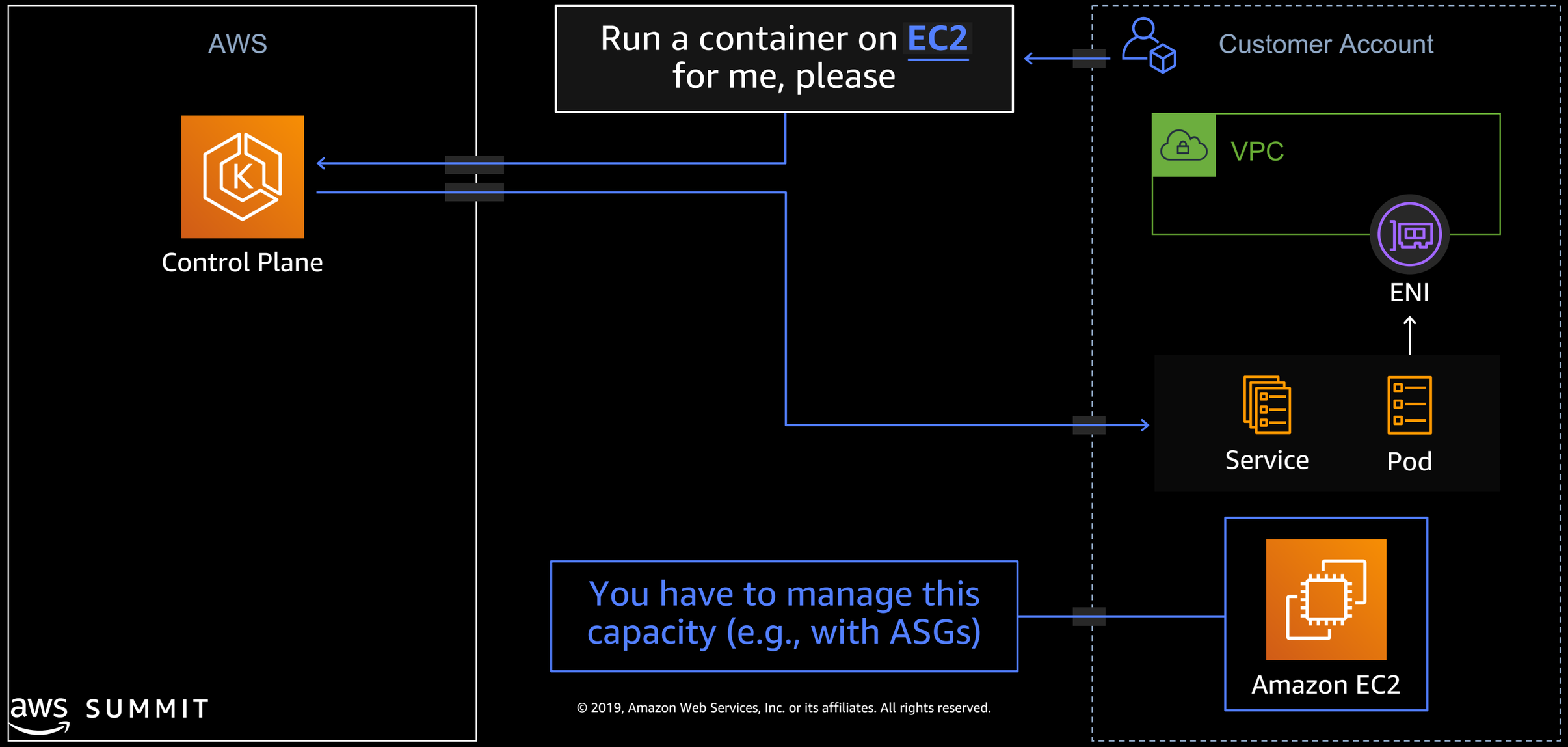
Right-Sized and Integrated

Only pay for the resources you need to run your pods. Includes native AWS integrations for networking, and security.

Fargate runs tens of millions of containers for AWS customers every week

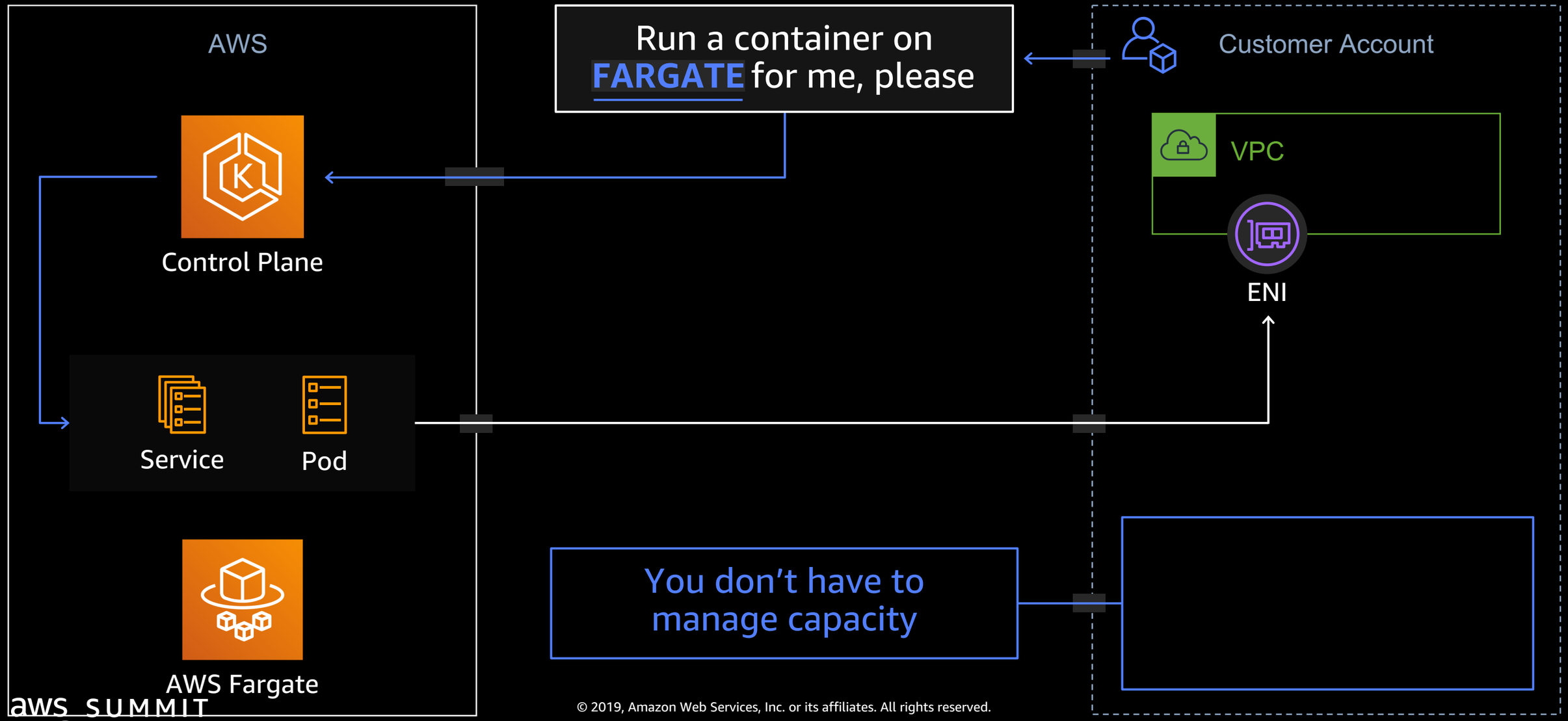
aws SUMMIT

The EC2 flow at 33,000 feet



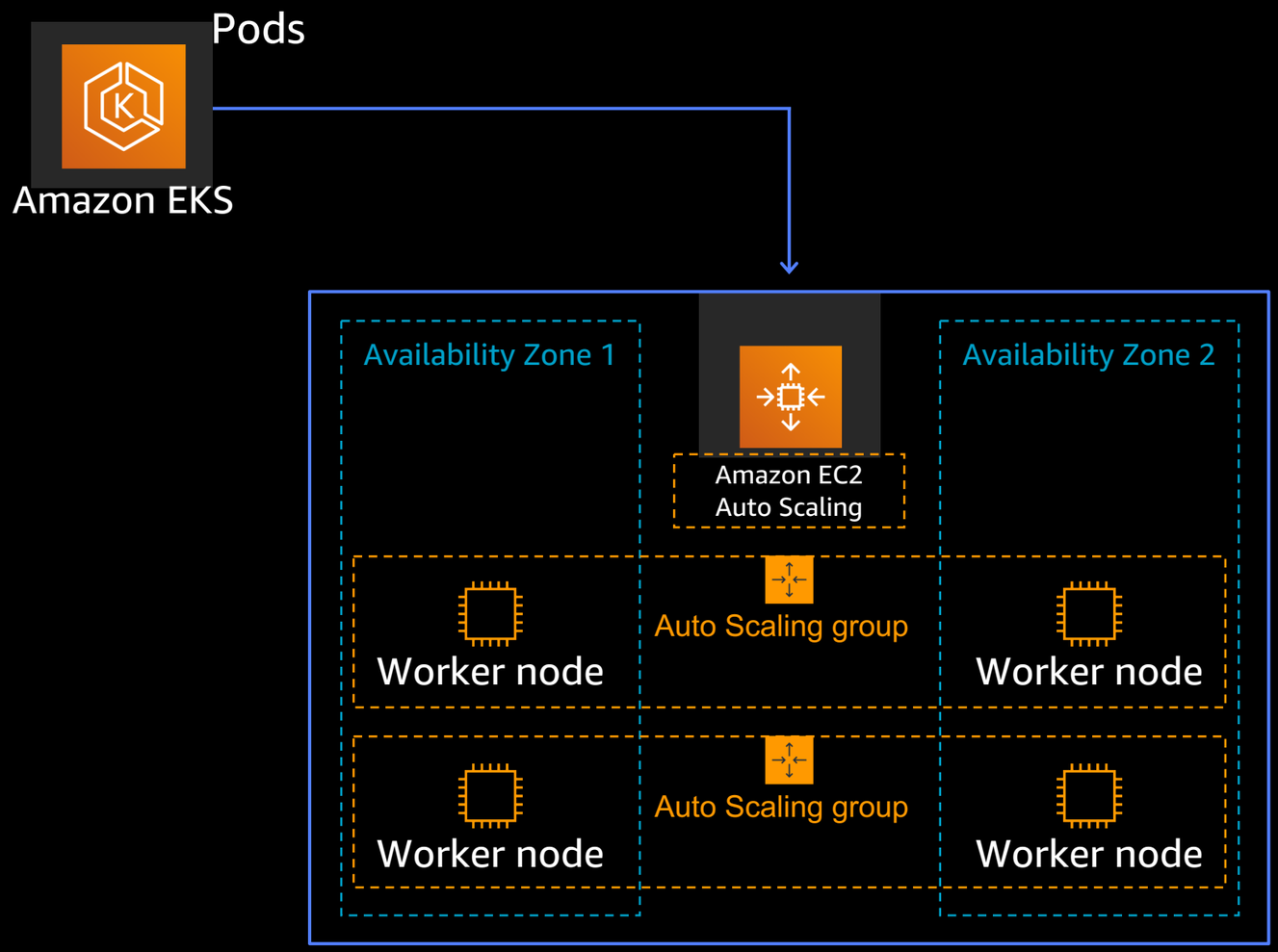
aws SUMMIT

The Fargate flow at 33,000 feet



EKS data plane options

Worker nodes only

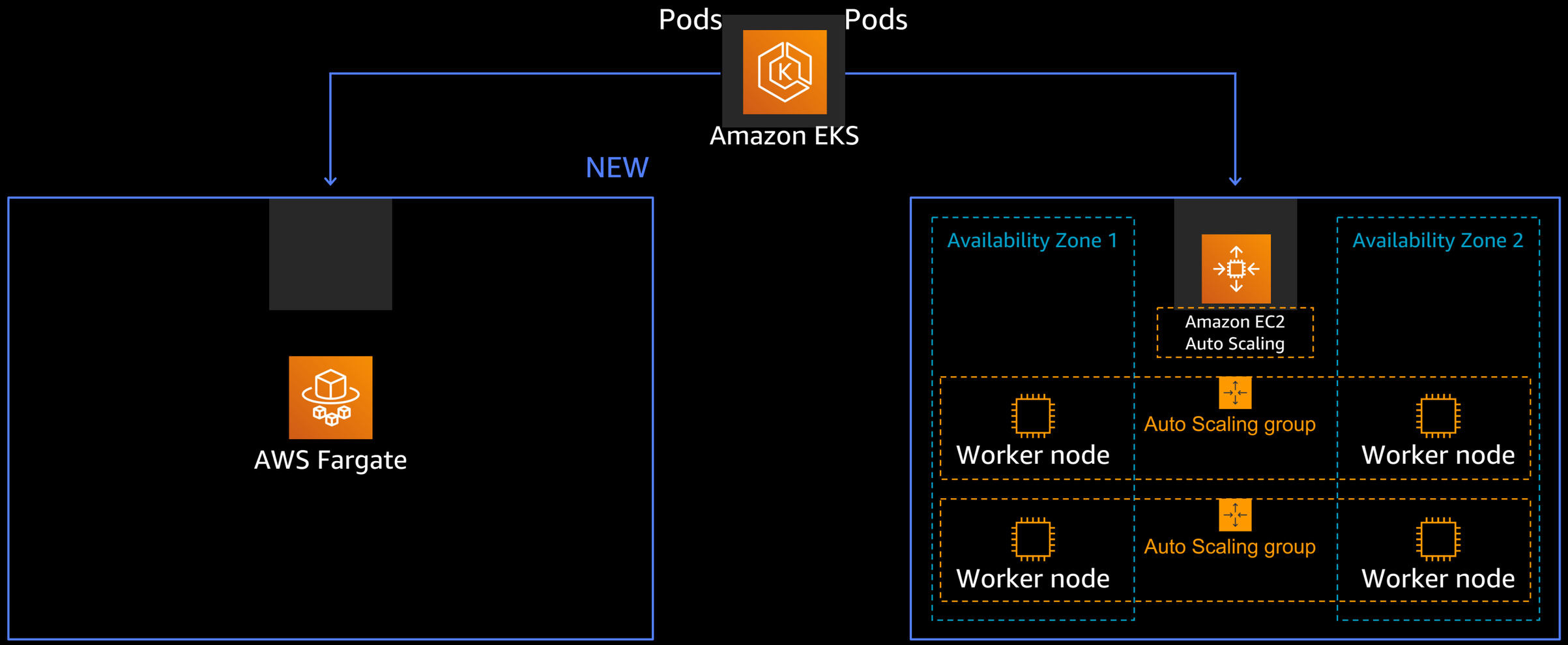


Traditional container data plane

aws SUMMIT

EKS data plane options

Mixed mode



Serverless container data plane

Traditional container data plane

aws SUMMIT

Availability

Available today for all new 1.14 clusters

- Create a new cluster
- Update a 1.13 cluster to 1.14
- We'll automatically update existing 1.14 clusters in the coming weeks

Use EKS with Fargate in

- Virginia (us-east-1)
- Ohio (us-east-2)
- Dublin (eu-west-1)
- Tokyo (ap-northeast-1)

Recap: EKS for Fargate introduces UX changes

Things you no longer need to do

- Manage Kubernetes worker nodes
- Pay for unused capacity
- Use K8s Cluster Autoscaler (CA)

Things you get out of the box

- VM isolation at pod level
- Pod level billing
- Easy chargeback in multi-tenant scenarios

Things you can't do (for now)

- Deploy Daemonsets
- Use service type LoadBalancer (CLB/NLB)
- Running privileged containers
- Run stateful workloads

Fargate Vs. (Un)Managed Nodes

	Fargate	Managed nodes	Unmanaged nodes
Units of work	Pod	Pod and EC2	Pod and EC2
Unit of charge	Pod	EC2	EC2

Fargate Vs. (Un)Managed Nodes

	Fargate	Managed nodes	Unmanaged nodes
Units of work	Pod	Pod and EC2	Pod and EC2
Unit of charge	Pod	EC2	EC2
Host lifecycle	There is no visible host	AWS (SSH is allowed)	Customer
Host AMI	There is no visible host	AWS vetted AMIs	Customer BYO

Fargate vs. (Un)Managed Nodes

	Fargate	Managed nodes	Unmanaged nodes
Units of work	Pod	Pod and EC2	Pod and EC2
Unit of charge	Pod	EC2	EC2
Host lifecycle	There is no visible host	AWS (SSH is allowed)	Customer
Host AMI	There is no visible host	AWS vetted AMIs	Customer BYO
Host : Pods	1 : 1	1 : many	1 : many

Questions

aws SUMMIT

Thank you!

Bryan Landes
landesb@amazon.com

aws SUMMIT