Webinar Containers – Part2

Amazon Elastic Container Service

For Kubernetes

Abass SAFOUATOU, AWS Solutions Architect
Patrick Madec, Partner Solutions Architect
Kun Song, AWS Solutions Architect
Roberto Migli, AWS Solutions Architect

Agenda

Time	Topic
9H00	Amazon Elastic Container Service for Kubernetes (EKS)
10H15	Break
10H30	EKS Workshop
12H00	Wrap-up

Why are enterprises adopting containers?

- Accelerate software development
- Build modern applications
- Automate operations at web scale

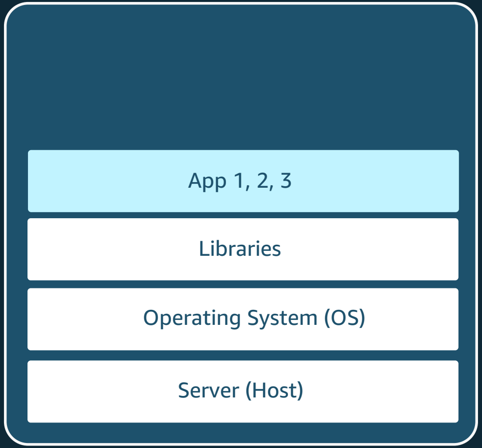
Early 2014

```
$ vi Dockerfile
$ docker build -t mykillerapp:0.0.1
$ docker run -it mykillerapp:0.0.1
```

Polyglot packaging

Portable runtime

Containers vs VMs



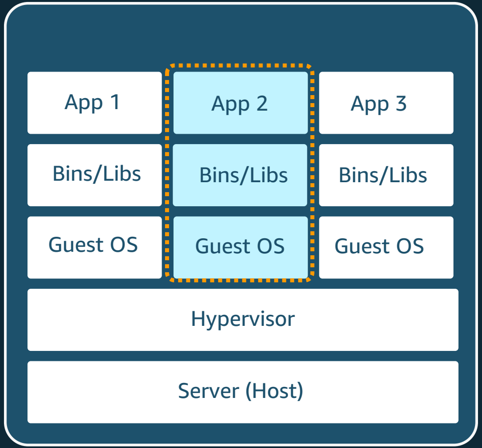
App 1, 2, 3

Libraries

Operating System (OS)

Server (Host)

Bare Metal



App 1 | App 2 | App 3

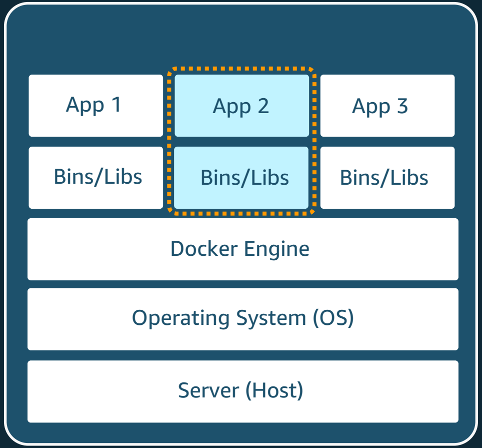
Bins/Libs | Bins/Libs | Bins/Libs

Guest OS | Guest OS | Guest OS

Hypervisor

Server (Host)

Virtual Machine



App 1 | App 2 | App 3

Bins/Libs | Bins/Libs | Bins/Libs

Docker Engine

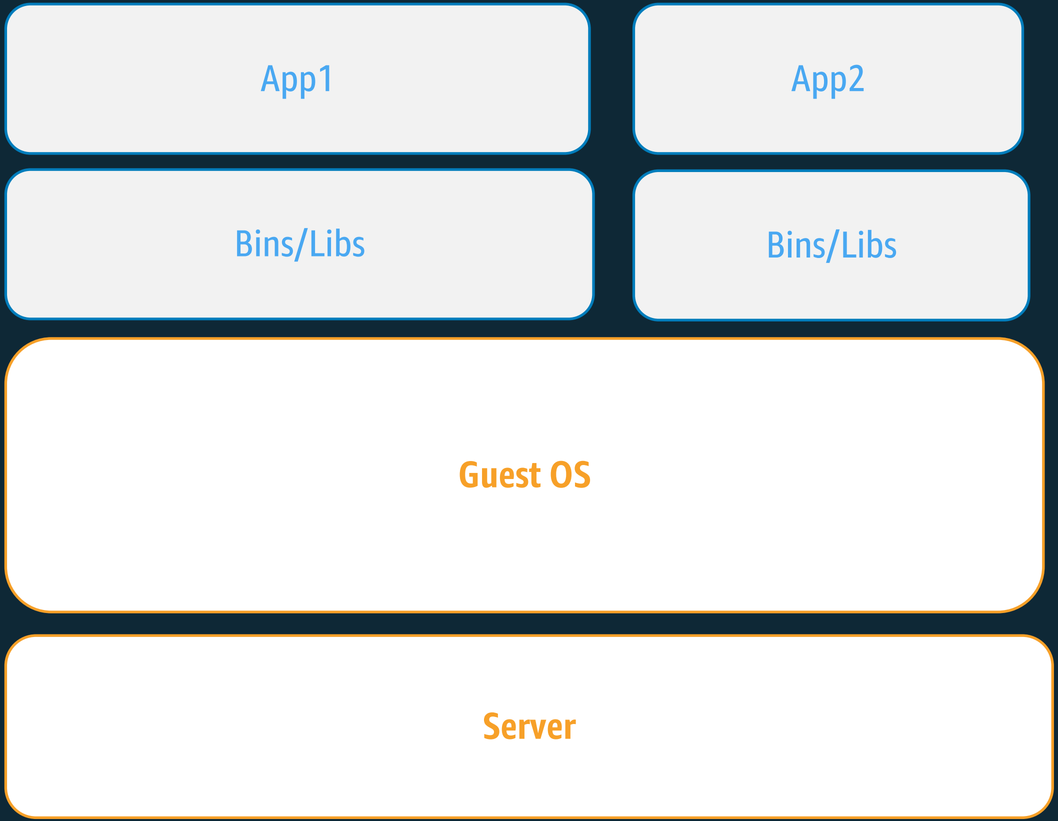
Operating System (OS)

Server (Host)

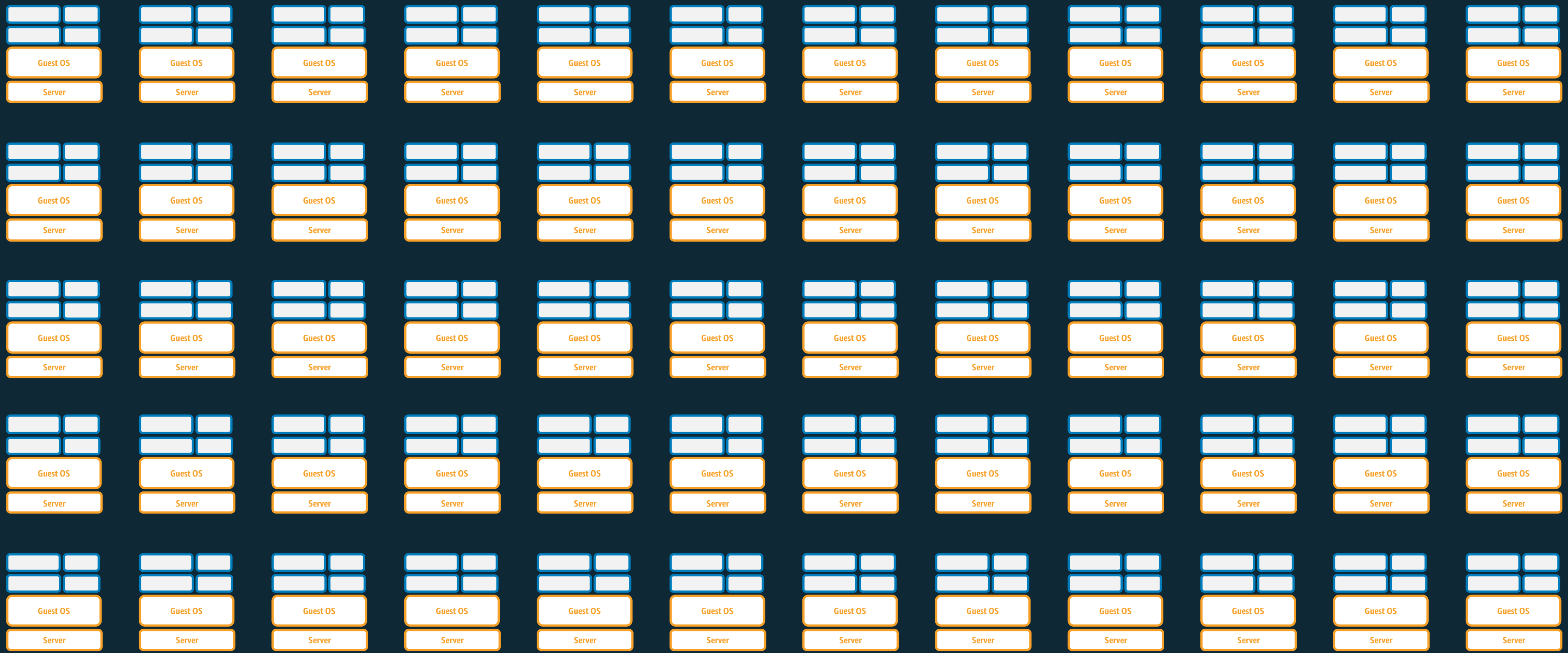
Containers

So what’s the catch?

Managing one container is easy…



…But managing many containers is difficult



docker SWARM

Amazon Elastic Container Service

kubernetes

Enter containers orchestration tools

HashiCorp Nomad

Apache MESOS™

Make AWS the **BEST PLACE** to run **ANY** containerized applications

AWS container services landscape

Management

Deployment, Scheduling, Scaling & Management of containerized applications

Amazon Elastic Container Service

Amazon Elastic Container Service for Kubernetes

Hosting

Where the containers run

Amazon EC2

AWS Fargate

Image Registry

Container Image Repository

Amazon Elastic Container Registry

Amazon EKS

What is Kubernetes?

What is Kubernetes?

Open source container management platform

Helps you run containers at scale

Gives you primitives for building modern applications

Why developers love Kubernetes

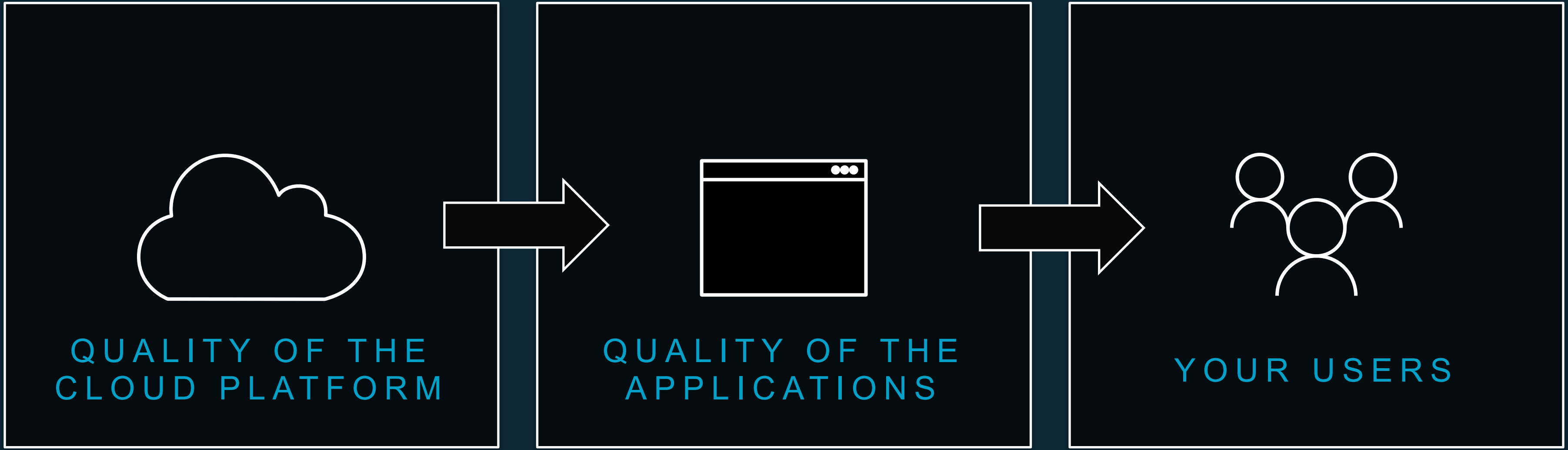
A single extensible API

SCALE

PERFORMANCE

BREADTH

Where you run K8s matters



QUALITY OF THE CLOUD PLATFORM

QUALITY OF THE APPLICATIONS

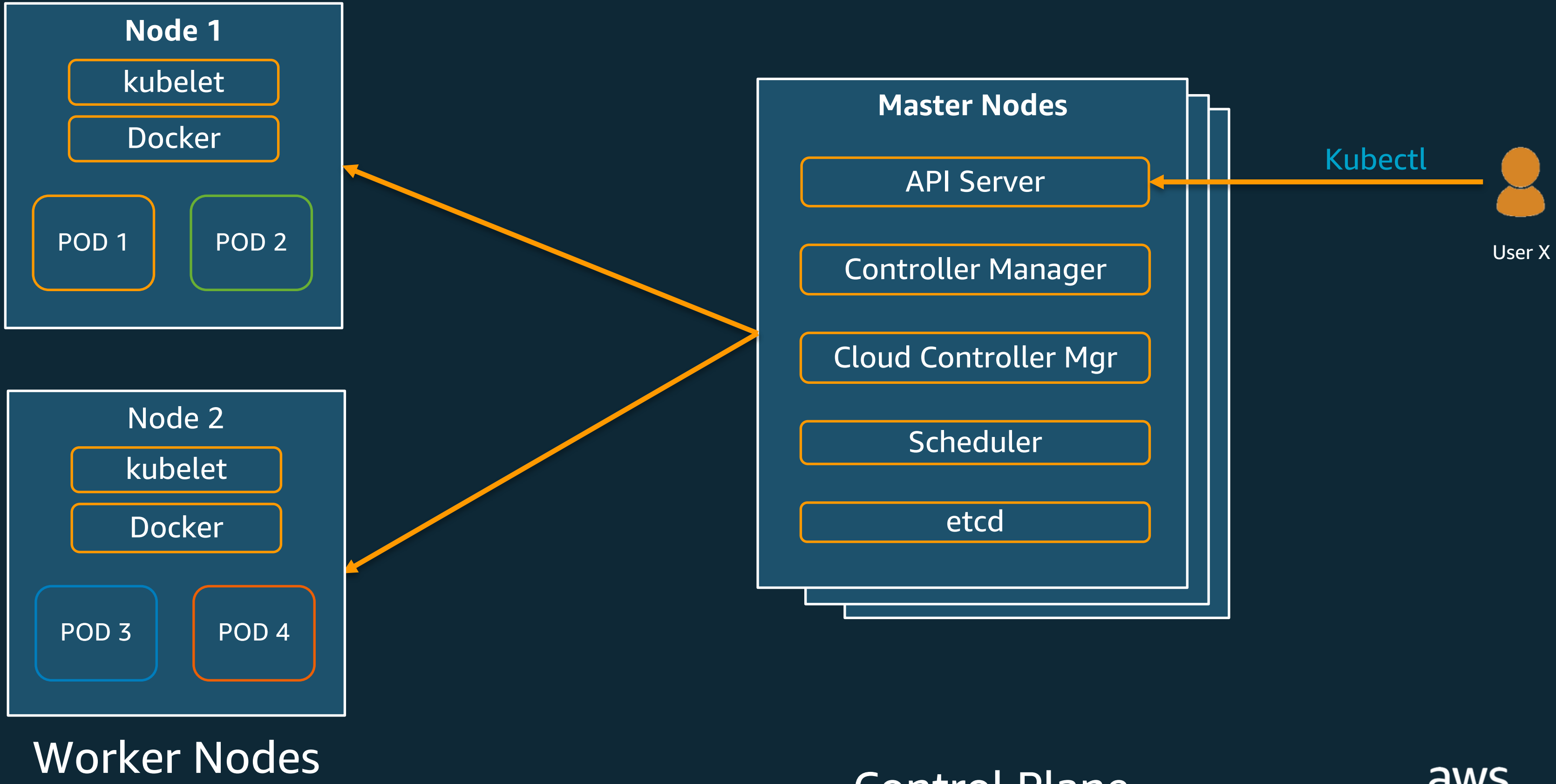
YOUR USERS

51% of Kubernetes workloads run on AWS today

—CNCF survey

https://www.cncf.io/blog/2018/08/29/cncf-survey-use-of-cloud-native-technologies-in-production-has-grown-over-200-percent/

Kubernetes Architecture



Control Plane

Kubernetes Core Concepts

Pod - Group of one or more containers with shred storage/network

Manifest File - YAML/JSON used to deploy Kubernetes objects

Deployment - Run specified # of Pods of your application

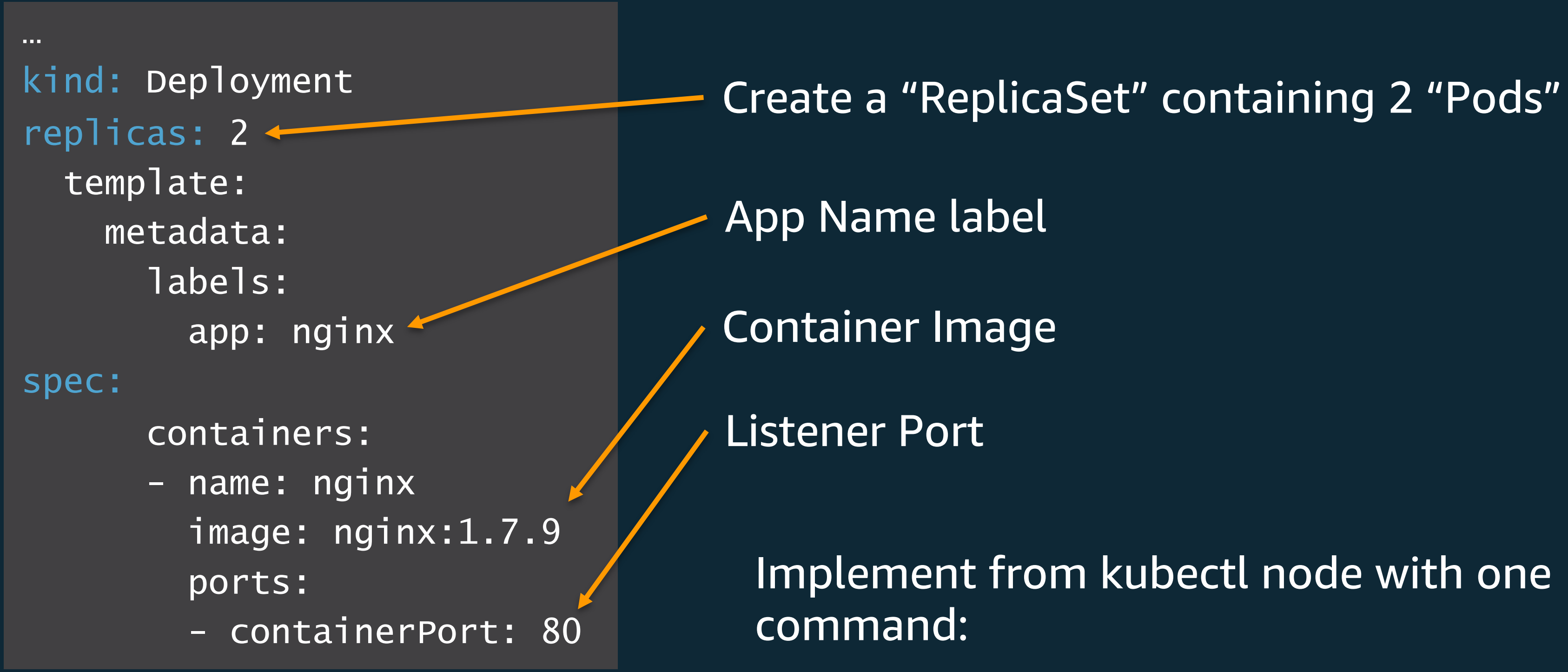
Service - Maps a fixed IP address to a logical group of pods

Annotation - Key/Value pairs to hold non-identifying information

Label - Key/Value pair used for association and filtering

DaemonSet - Implements a single instance of a pod on a worker node

Example nginx-pods.yaml



```yaml
…
kind: Deployment
replicas: 2
  template:
    metadata:
      labels:
        app: nginx
spec:
      containers:
      - name: nginx
        image: nginx:1.7.9
        ports:
        - containerPort: 80
```

Create a “ReplicaSet” containing 2 “Pods”

App Name label

Container Image

Listener Port

Implement from kubectl node with one command:

“`kubectl apply –f nginx-pods.yaml`”

Example nginx-svc.yaml (Classic Load Balancer)

```
…
kind: Service
spec:
 selector:
    app: nginx
  type: LoadBalancer
  ports:
  - name: http
    port: 80
    targetPort: 80
```

Route traffic to Apps named “nginx”

Deploy an AWS Load Balancer

Listener and Target Config

Implement from kubectl node with one command:

“`kubectl apply –f. nginx-svc.yaml`”

“Run Kubernetes for me.”

“Native AWS Integrations.”

"An Open Source Kubernetes Experience.”

Amazon Elastic Container Service for Kubernetes (EKS)

Managed Kubernetes on AWS

Master

Etcd

Managed Kubernetes Control Plane

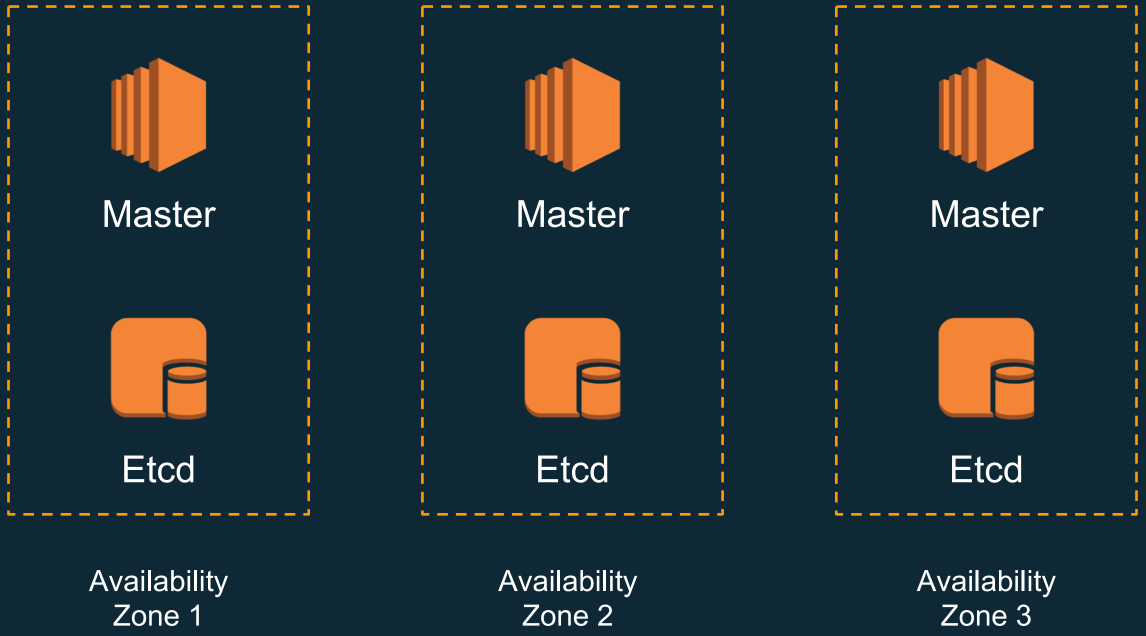
Highly Available

Automated Version Upgrades

Integration with Other AWS services

Kubernetes on AWS

3x Kubernetes masters for HA



Master

Etcd

Availability Zone 1

Master

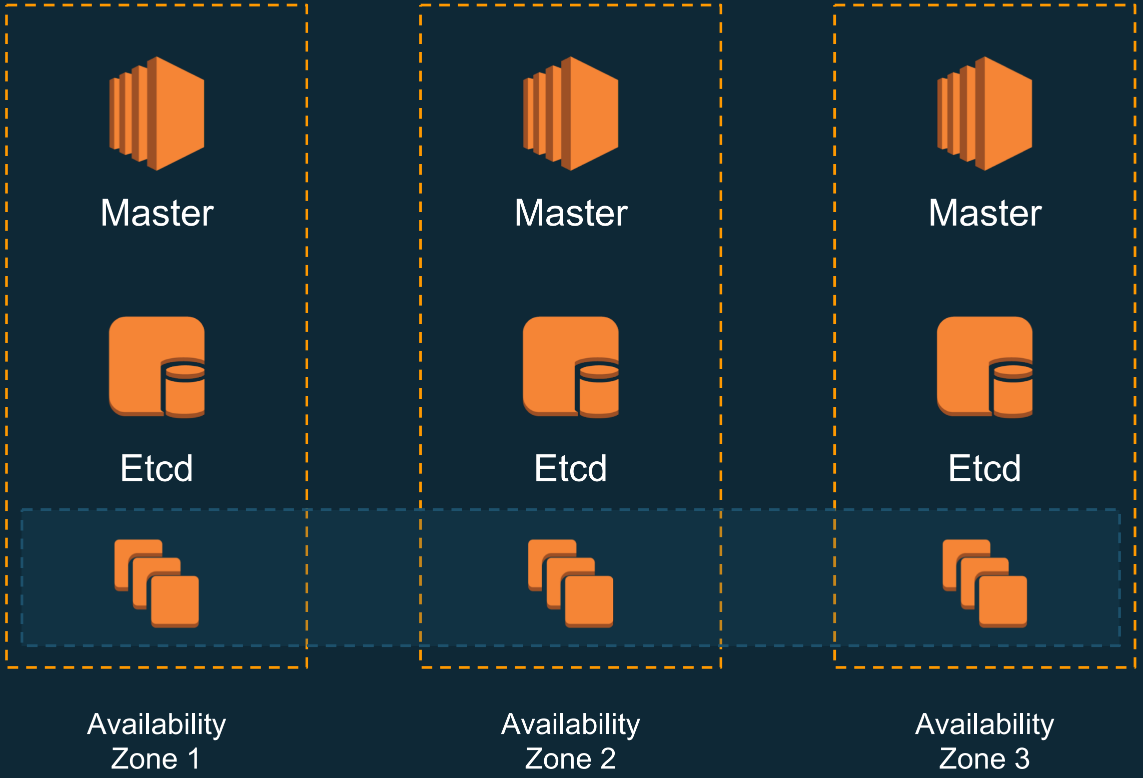
Etcd

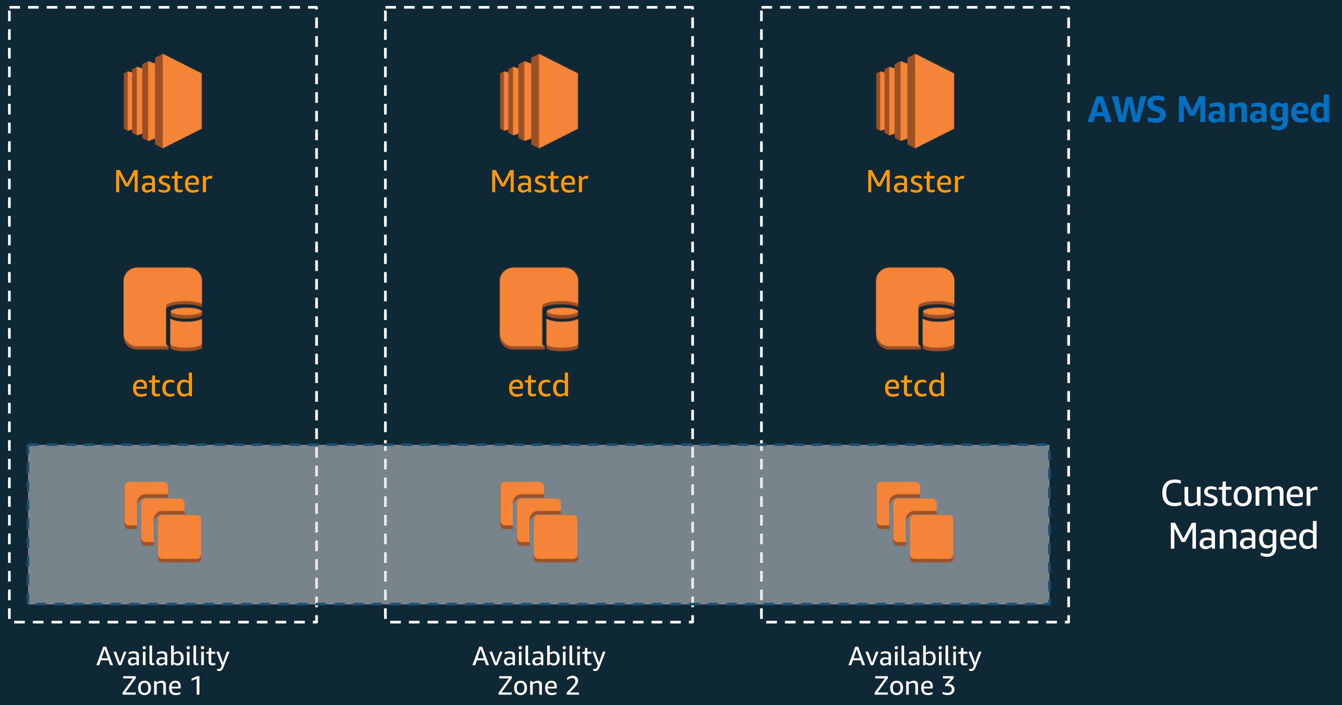
Availability Zone 2

Master

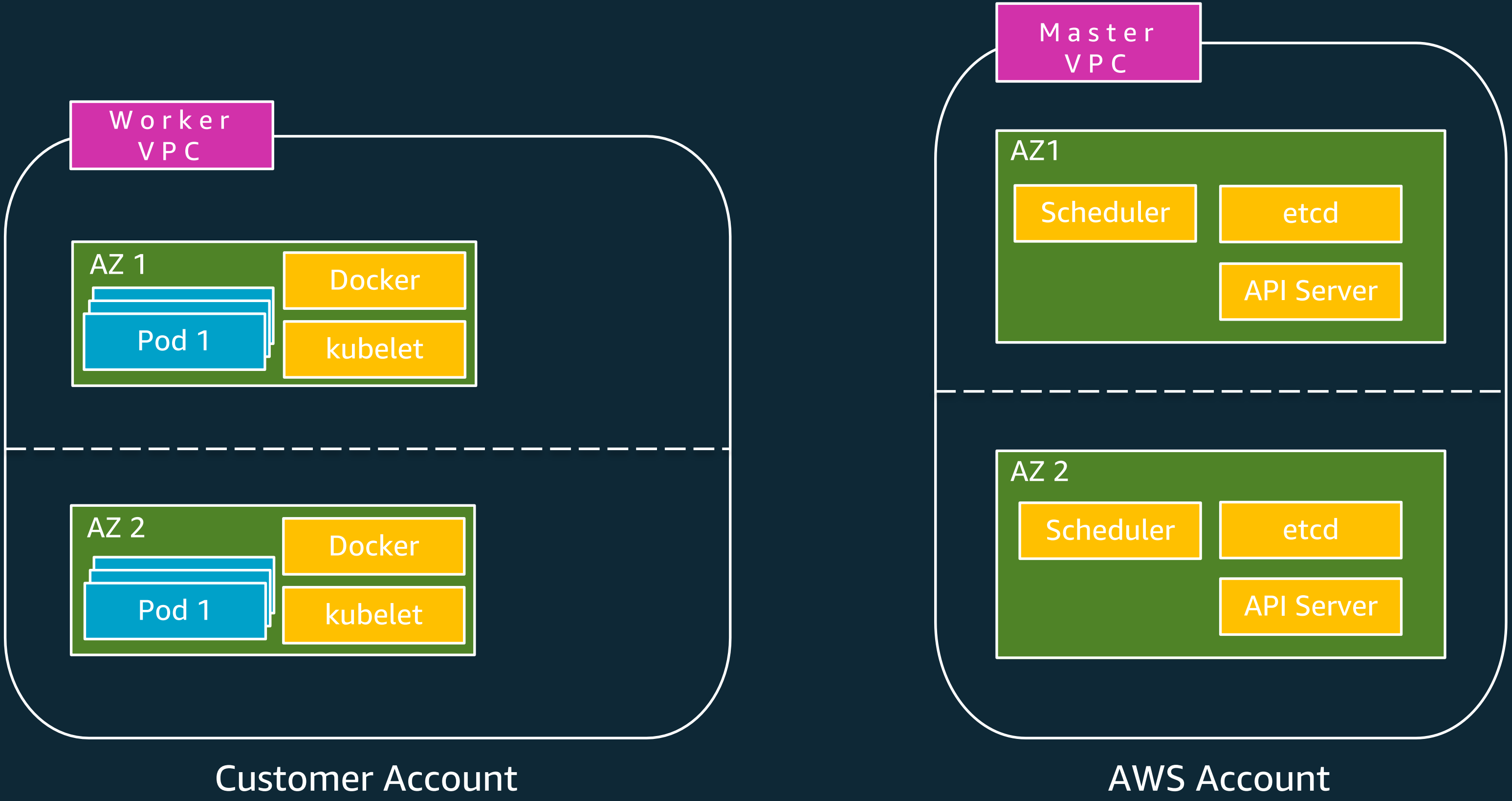
Etcd

Availability Zone 3

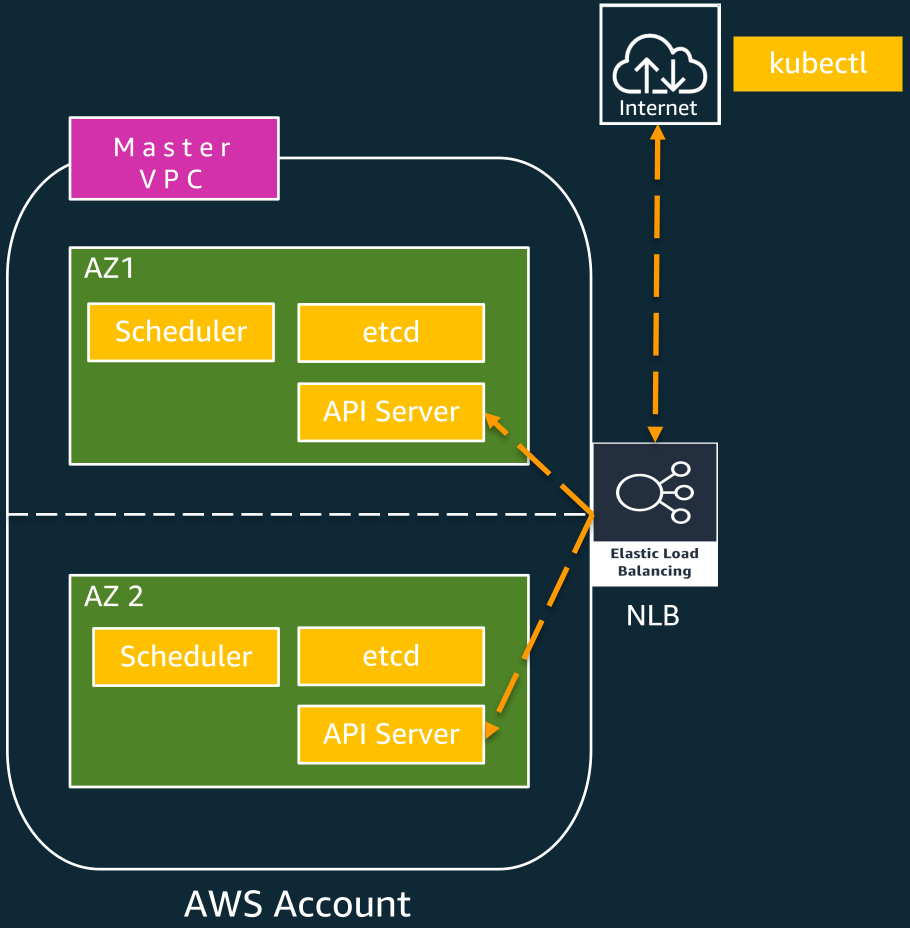

Master
Etcd
Master
Etcd
Master
Etcd
Availability Zone 1
Availability Zone 2
Availability Zone 3


Master
Master
Master
AWS Managed
etcd
etcd
etcd
Customer Managed
Availability Zone 1
Availability Zone 2
Availability Zone 3

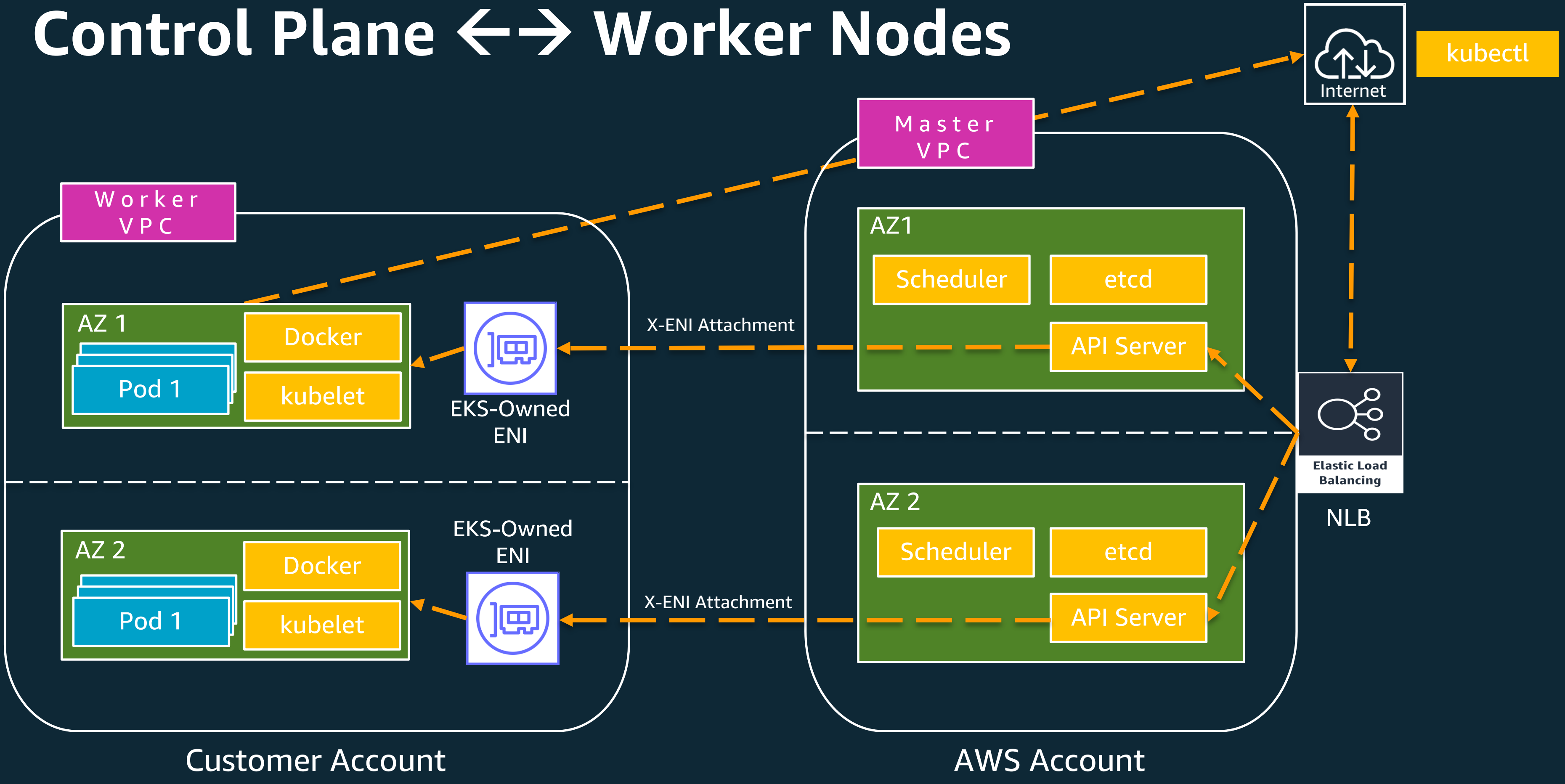
EKS Architecture



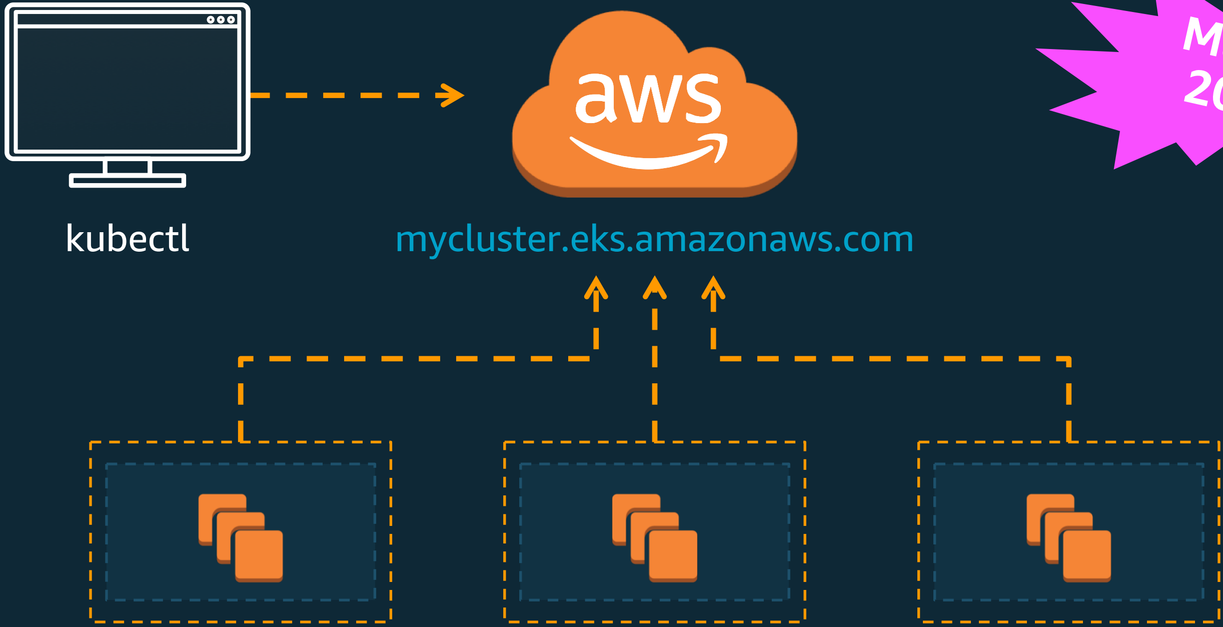
Control Plane Networking



Control Plane ←→ Worker Nodes



Kubernetes Endpoint Private Access



March 2019

EKS versions and upgrades

Versions

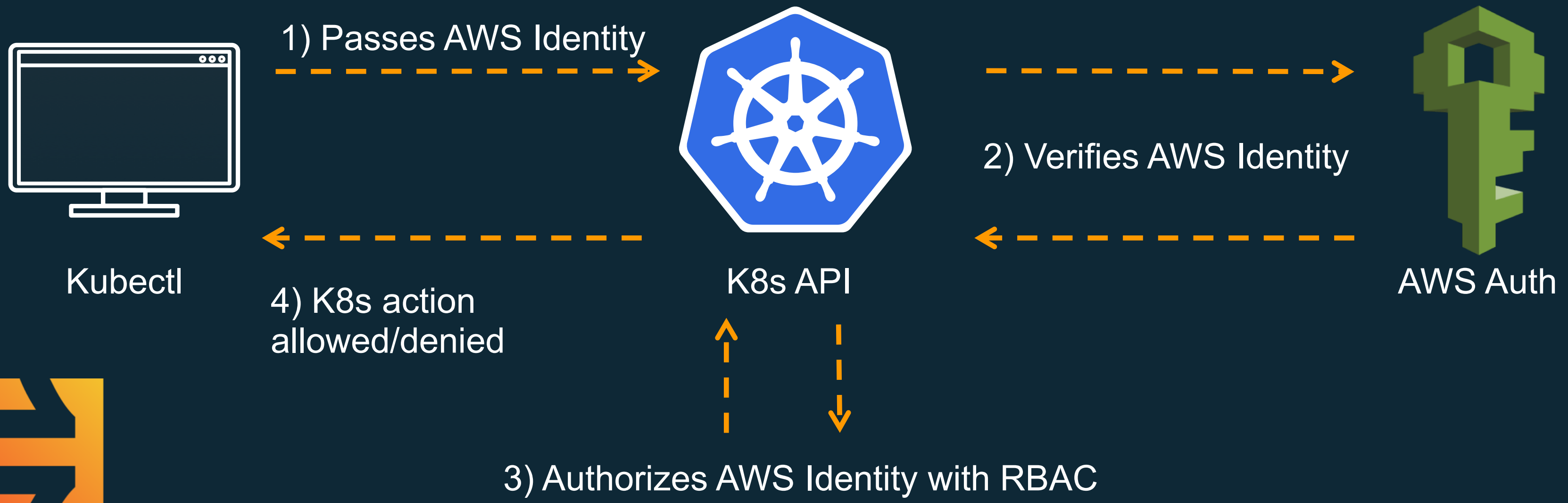
- Kubernetes version X.Y.Z
  X: major version
  Y: minor version
  Z: patch version
- Maintains last three minor releases
- Releases every 3 months (so branch maintened ~ 9 months)

- EKS version X.Y
  X: major version
  Y: minor version
- Platform version EKS.N:
  - Kubernetes patches
  - API server changes
  - Automatic apply
- Support 3 stable Kubernetes versions

1.10.x version has been deprecated since July 22th 2019

EKS Security

IAM Authentication + Kubectl



1) Passes AWS Identity

2) Verifies AWS Identity

3) Authorizes AWS Identity with RBAC

4) K8s action allowed/denied

heptio

aws

Pod Security Policy

Container is about to remove dependenci containers access resources that you don

- Ex: root user is not recommeded inside but…

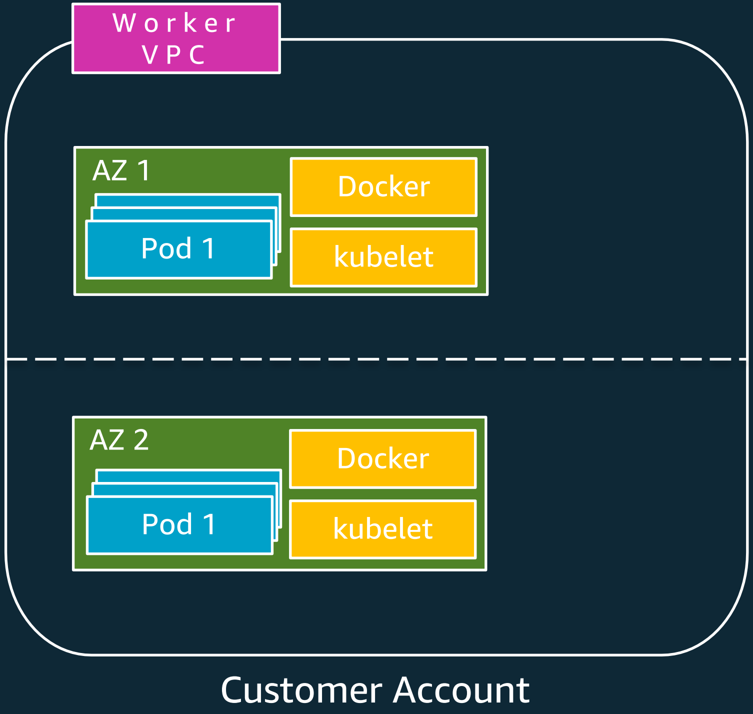
Feature: PodSecurityPolicy

- Defines what accesses your pod can have(root, syscall, R/W etc…)
- An EKS 1.13 cluster now has the PSP admission plugin enabled by default, you can use it directly
- The default policy is still permissive to keep backbward compatibility

Available K8s 1.13

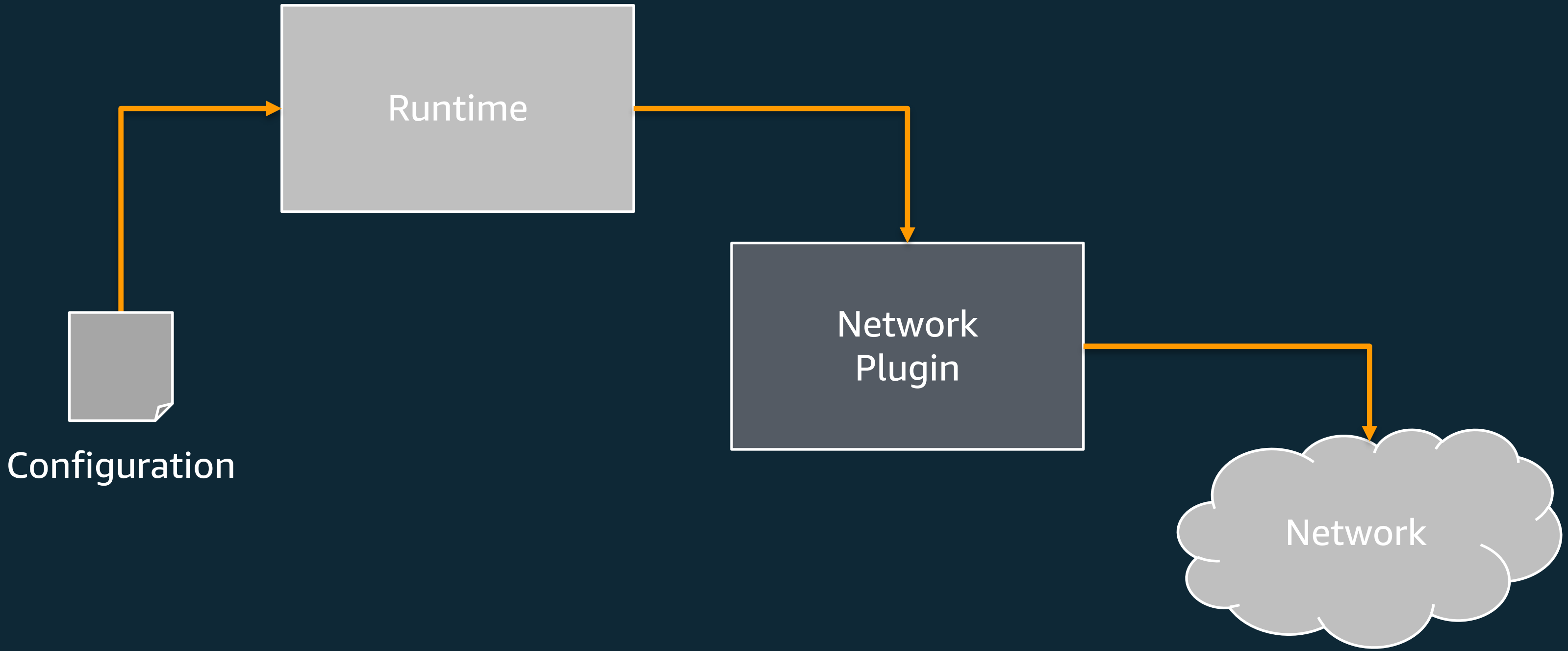
EKS Network

Kubernetes Network Requirements



- All containers can communicate with all other containers without NAT
- All nodes can communicate with all containers (and vice-versa) without NAT
- The IP address that a container sees itself as is the same IP address that others see it as

Container Network Interface (CNI)



Amazon VPC CNI Plugin Goals

1. Simplify networking options for customers

2. Support high throughput, high availability, low latency and minimal jitter

3. Allow customers to reuse AWS VPC networking and security best practices such as use of:
   - VPC flow logs for troubleshooting and compliance auditing
   - VPC routing polices for traffic engineering
   - Security groups for isolation and regulatory requirements

4. Setup Pod networking within seconds

5. Support cluster scale to a minimum of 5000+

Amazon VPC CNI Plugin

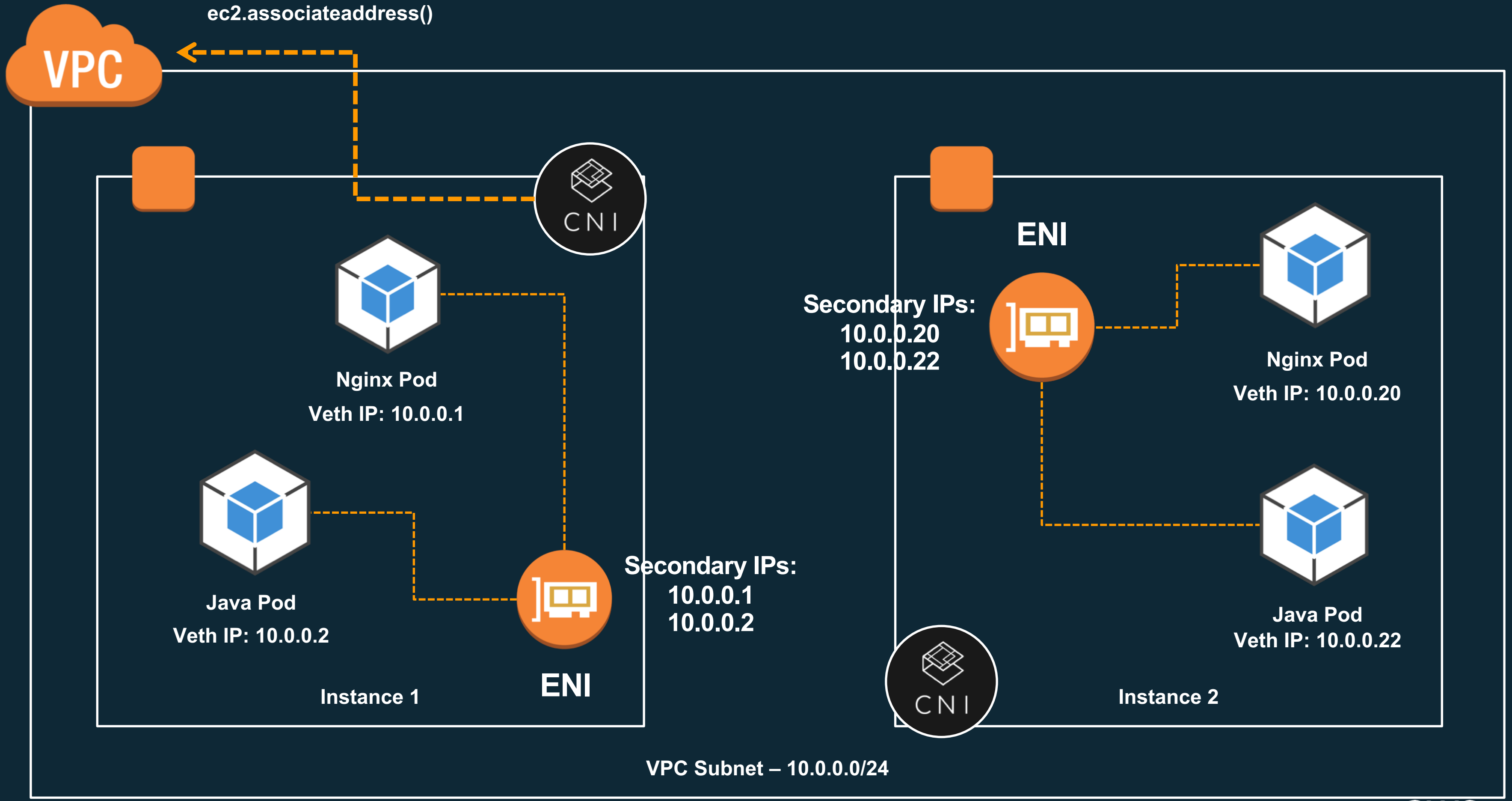
Native VPC networking with CNI plugin

Pods have the same VPC address inside the pod as on the VPC

Simple, secure networking

Open source and on Github

https://github.com/aws/amazon-vpc-cni-k8s


ec2.associateaddress()
VPC
CNI
Nginx Pod
Veth IP: 10.0.0.1
Java Pod
Veth IP: 10.0.0.2
Secondary IPs:
10.0.0.1
10.0.0.2
ENI
Instance 1
ENI
Secondary IPs:
10.0.0.20
10.0.0.22
Nginx Pod
Veth IP: 10.0.0.20
Java Pod
Veth IP: 10.0.0.22
CNI
Instance 2
VPC Subnet – 10.0.0.0/24

aws

Amazon VPC CNI plugin – Understanding IP Allocation

Primary CIDR range

RFC 1918 addresses ➔ 10/8, 172.16/12, 192.168/16

Publicly routable CIDR block (since May 2019)

Used in EKS for:

Pods

X-account ENIs for (masters → workers) communication (exec, logs, proxy etc.)

Internal Kubernetes services network (10.100/16 or 172.20/16)

Secondary CIDR ranges

non-RFC 1918 address blocks (100.64.0.0/10 and 198.19.0.0/16)

CNI 1.2.1+

Used in EKS for Pods only

How?

Amazon EKS custom network config ➔ enable ➔ create ENIConfig CRD ➔ annotate nodes

What’s new

What’s New?

Amazon EKS

September 18: EKS simplifies cluster setup with update-kubeconfig CLI command
October 18 : EKS adds support for Dynamic Admission Controllers (Istio)
November 18: EKS launches in Ohio
November 18: EKS Adds ALB Support with AWS ALB Ingress Controller
December 18: EKS Adds Managed Cluster Updates and Support for Kubernetes Version 1.11
December 18: EKS Available in Frankfurt, Singapore, Sydney, and Tokyo
February 19 : Amazon EKS Available in Mumbai, London, and Paris AWS Regions
March 19: Amazon EKS now supports Kubernetes version 1.12 and Cluster Version Updates Via CloudFormation
April 19: Amazon EKS Now Delivers Kubernetes Control Plane Logs to Amazon CloudWatch
April 19: Amazon EKS Supports EC2 A1 Instances as a Public Preview
May 19: Amazon EKS Releases Deep Learning Benchmarking Utility
May 19: Amazon EKS Adds Support for Public IP Addresses Within Cluster VPCs
May 19: Amazon EKS Simplifies Kubernetes Cluster Authentication
May 19: Introducing Amazon CloudWatch Container Insights for Amazon EKS and Kubernetes - Now in Preview
June 19: Amazon EKS now supports Kubernetes version 1.13, ECR PrivateLink, and Kubernetes Pod Security Policies
July 19: AWS VPC CNI Version 1.5.0 Now Default for Amazon EKS Clusters
July 19: Amazon EKS Available in Hong Kong Region

aws

ECS Workshop : Objectives

- Build a cluster
- Creation of 3 microservices
- Test the RBAC feature

https://eksworkshop.com

Faites nous vos retours

http://bit.ly/AWScontainerParis

Thank you