Start Next session at 15:00

Feel free to break or play lab 1 - 4

aws

Part 2

AWS Workshop Series

Day 3: Container for Beginner

Taking Enterprise Beyond the Cloud by TrueIDC

Mr. Athiwat Itthiwatana

Cloud & Solution Consultant

Presented by

- Athiwat Itthiwatana (HAM)
- Cloud & Solution Consultant, TrueIDC
- AWS Specialist
- SAP Basis Specialist
- athiwat.itt@ascendcorp.com

trueIDC

Agenda

- Kubernetes
- Container Best Practice
- Lab: AWS Container Immersion Day Part EKS

Source: AWS Immersion day

What is Kubernetes ?

- Open-source Container Orchestration tool
- Developed by Google
- Help you manage containerized application in different deployment environments.

aws

trueIDC

Need for a container orchestration tool

- Trend from Monolith to **Microservices**
- Increased usage of **containers**
- Demand for a **proper way** of **managing** hundreds of containers

Orchestration tools Feature

- High Availability
- Scalability and High performance
- Disaster recovery

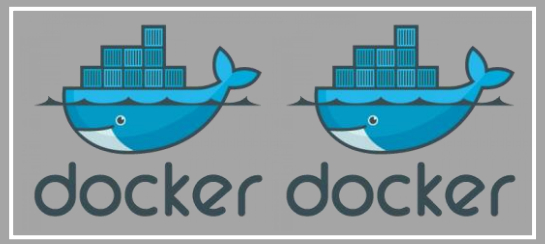
Kubernetes High level

Pod is smallest unit in K8S

Worker node can have
Many Pod nodes

Worker Node

Pod Node

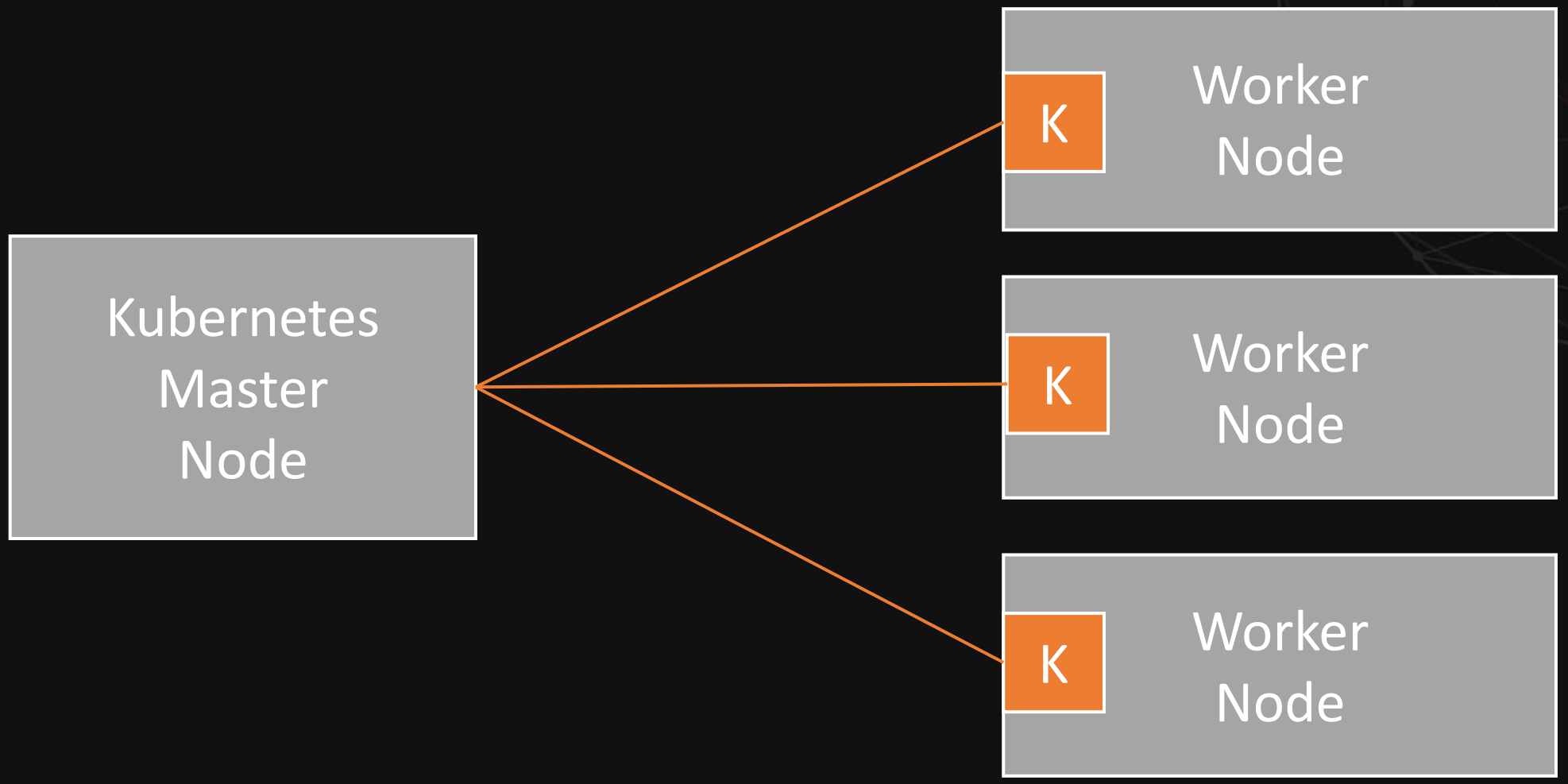


Kubernetes
Master
Node

Master node give instruction
To Worker node

One Pod can store one
or more container

Kubelet

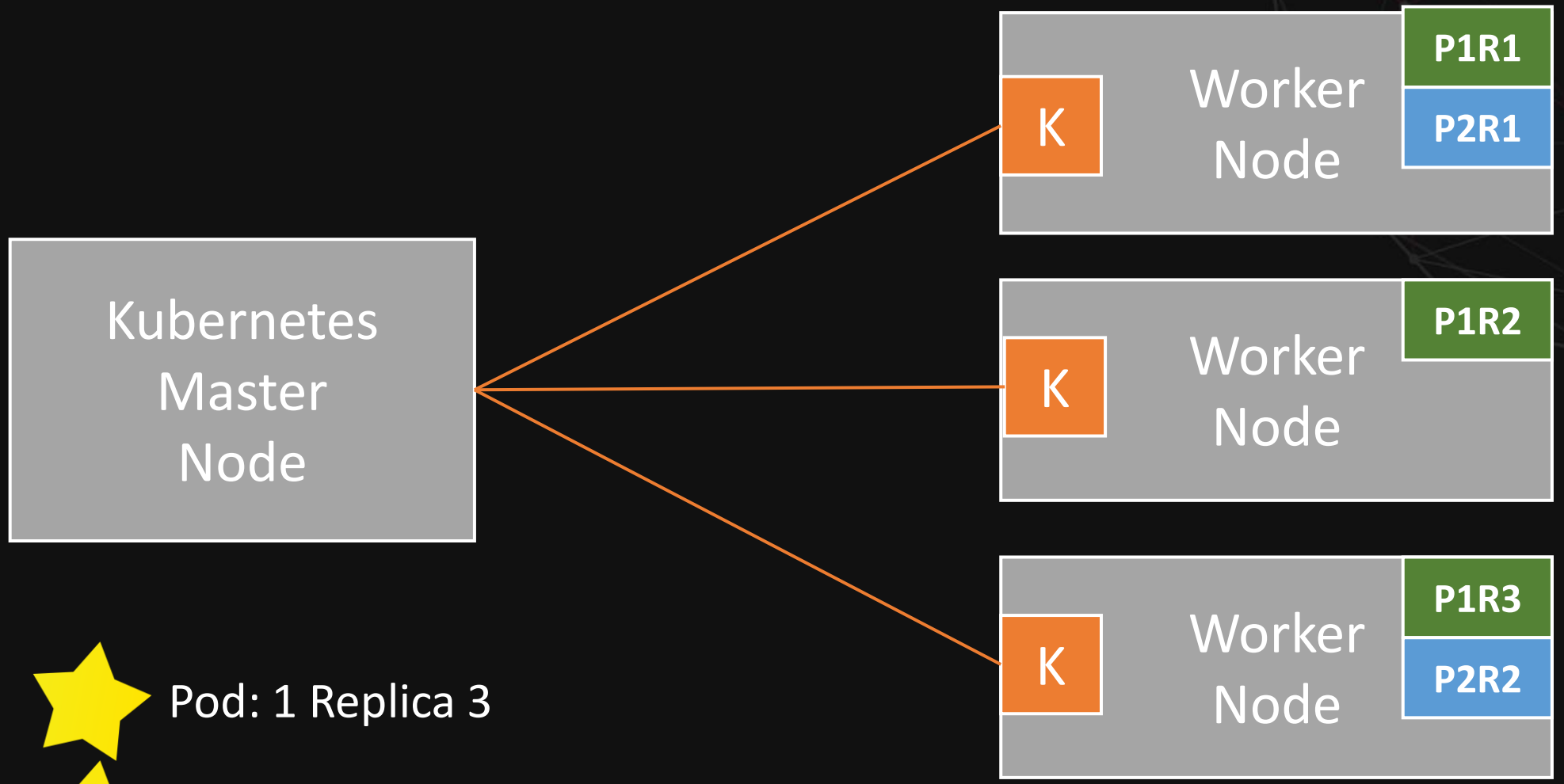

Kubernetes Master Node
K
Worker Node
K
Worker Node
K
Worker Node

Manage K8S with YAML

Kubernetes
Master
Node

```yaml
cat << EOF > monolith-app.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: mythical-mysfits-eks
  namespace: default
  labels:
    app: mythical-mysfits-eks
spec:
  replicas: 2
  selector:
    matchLabels:
      app: mythical-mysfits-eks
  template:
    metadata:
      labels:
        app: mythical-mysfits-eks
    spec:
      serviceAccount: mythical-misfit
      containers:
        - name: mythical-mysfits-eks
          image: $MONO_ECR_REPOSITORY_URI:latest
          imagePullPolicy: Always
```

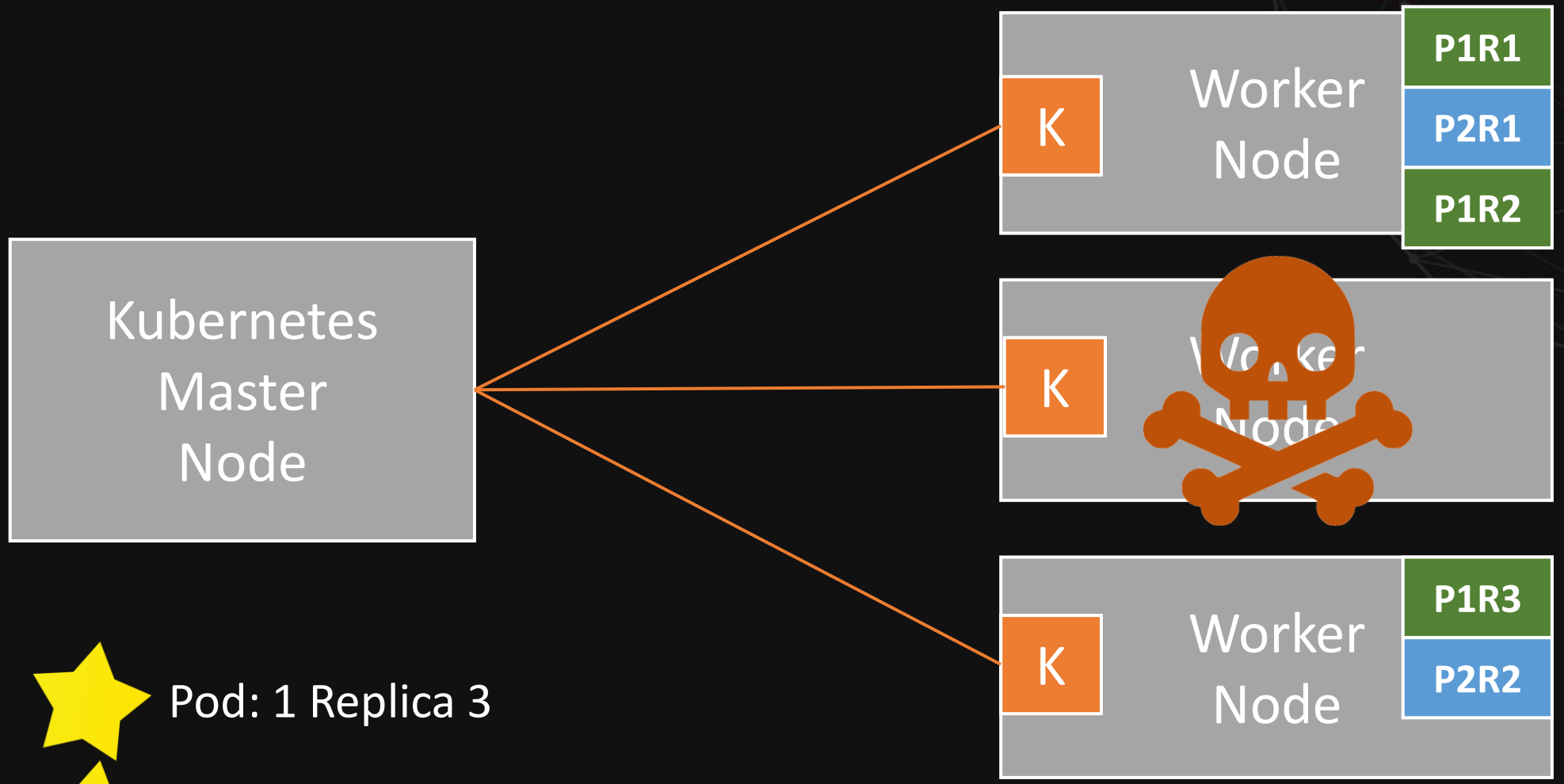
Example: Deployment



- Pod: 1 Replica 3
- Pod: 2 Replica 2

trueIDC

Example: Lose a Worker



Pod: 1 Replica 3

Pod: 2 Replica 2

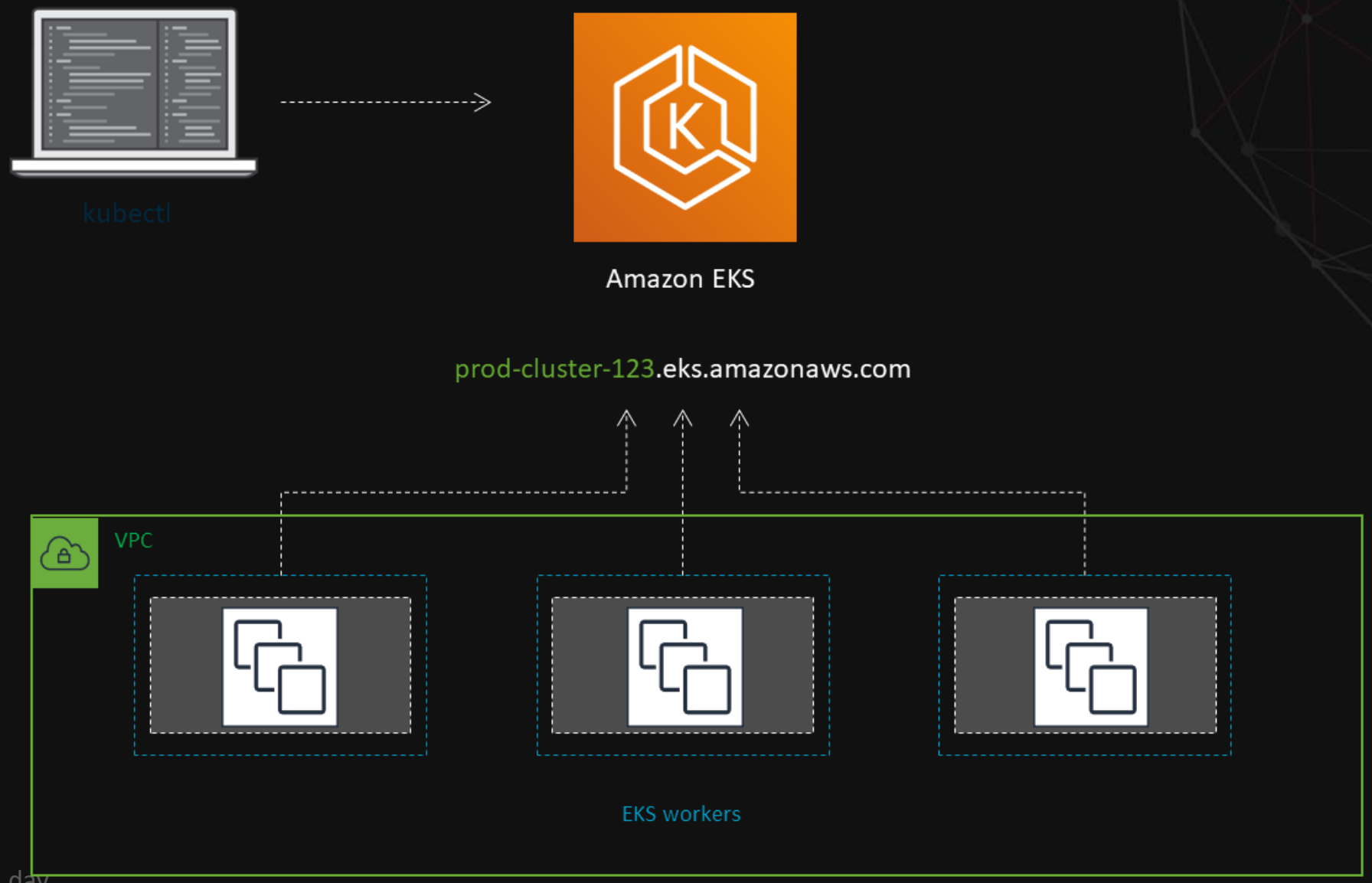
trueIDC

Kubernetes on AWS

Amazon Elastic Kubernetes Service (EKS) is a fully **managed** Kubernetes service. EKS runs upstream Kubernetes and is **certified** Kubernetes conformant.

Source: AWS Immersion day

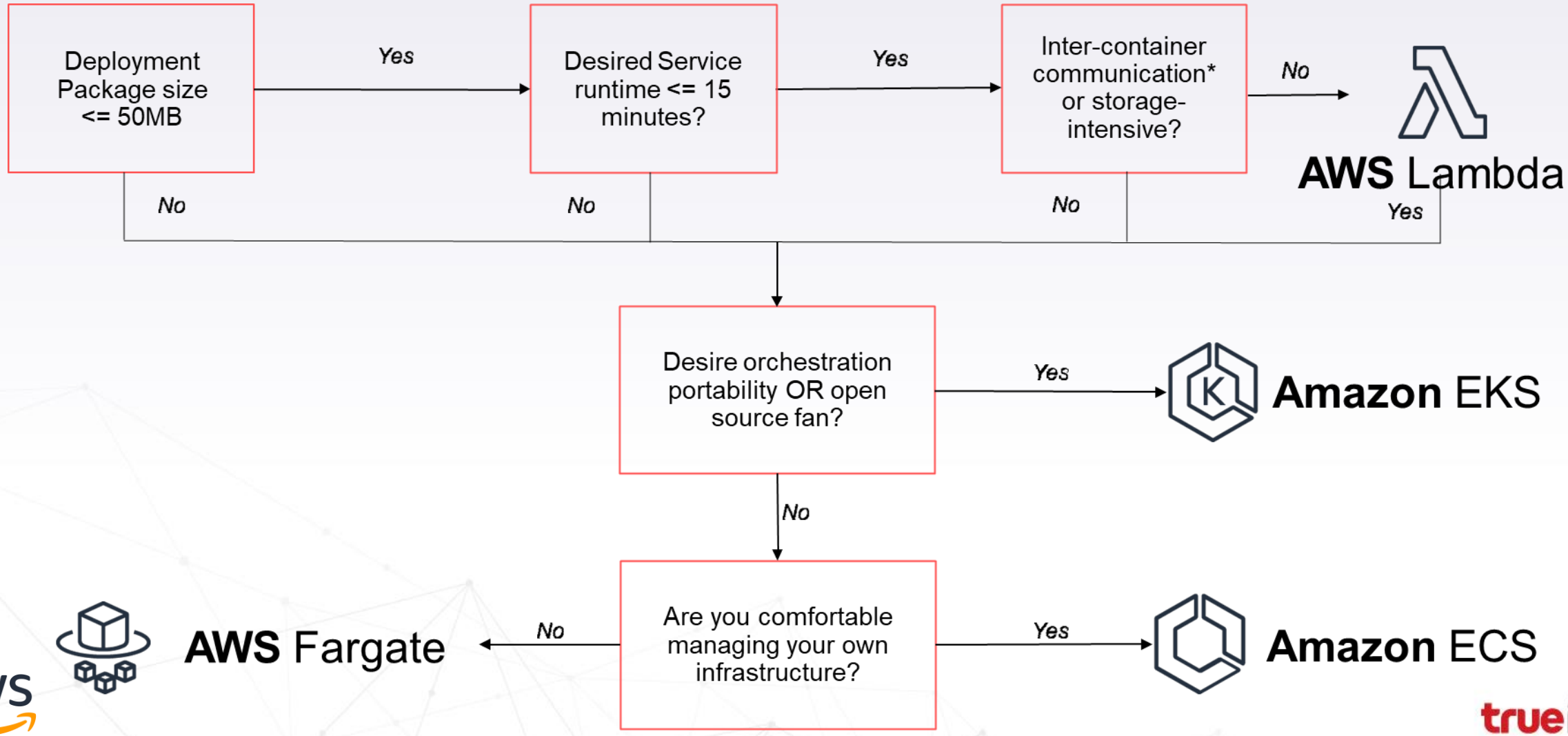
Amazon EKS Architecture



Source: AWS Immersion day

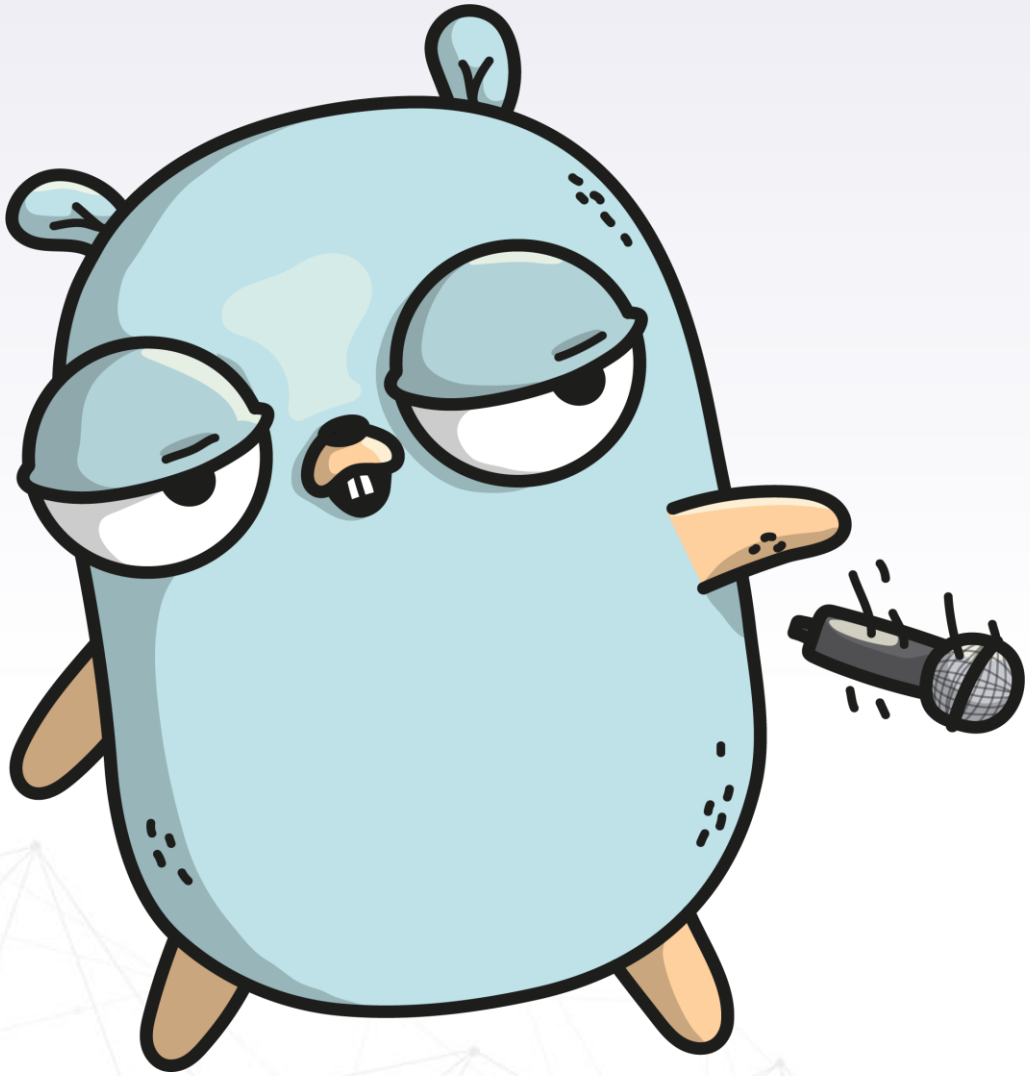
Container Best Practice

Decision Tree – Microservice



Source: AWS Summit berlin 2019

Think about your applications‘ needs



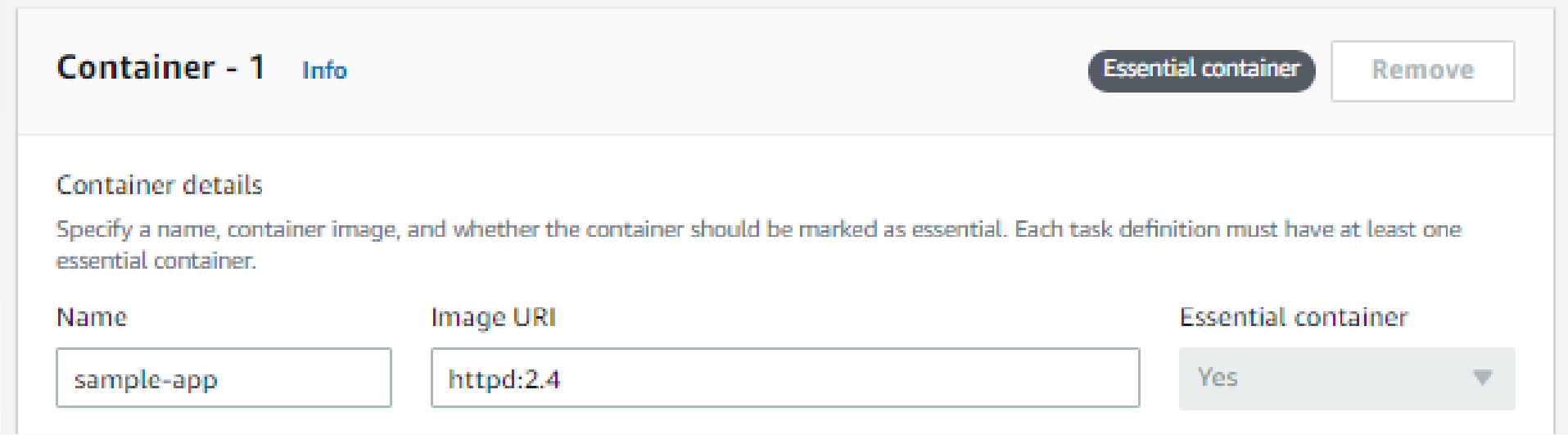
Source: AWS Summit berlin 2019

Optimizing your Container & K8S

- Use specific Image Versions
- Optimize pods replacement
- Small image
- Security is job Zero

Source: AWS Summit berlin 2019

Use specific Image Versions



DO NOT use a latest tag

Fixate the version

The more specific, better

Source: AWS Summit berlin 2019

Optimize pod placement

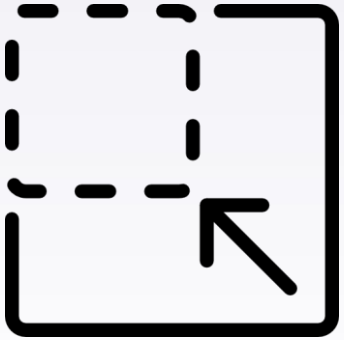
```yaml
apiVersion: v1
kind: Pod
metadata:
  name: app
spec:
  containers:
  - name: app
    image: nathanpeck/app
    resources:
      requests:
        memory: "256Mi"
        cpu: "250m"
      limits:
        memory: "512Mi"
        cpu: "500m"
```

Make sure you use resource constraints:

- Request the baseline average resource needs of the app
- Put a limit on the max resources of a pod

Source: AWS Summit berlin 2019

Small images



Less storage space

Provision faster

Source: AWS Summit berlin 2019

Shared Responsibility Model

CUSTOMER

Responsible for
Security "**in**" the cloud

- Customer Data
- Applications
- Platform
- Identity & Access Management
- Operating System
- Network and Firewall Configuration

AWS

Responsible for
Security "**of**" the cloud

- Compute
- Storage
- Database
- Networking
- Regions
- Availability Zones
- Edge Locations

aws

trueIDC

Source: AWS Summit berlin 2019

IAM = Who can do what in the platform and/or cluster?

People

Code / Pipelines

Source: AWS Summit berlin 2019

Shared Responsibility Model

CUSTOMER

Responsible for
Security "**in**" the cloud

- Customer Data
- Applications
- Platform
- Identity & Access Management
- Operating System
- Network and Firewall Configuration

AWS

Responsible for
Security "**of**" the cloud

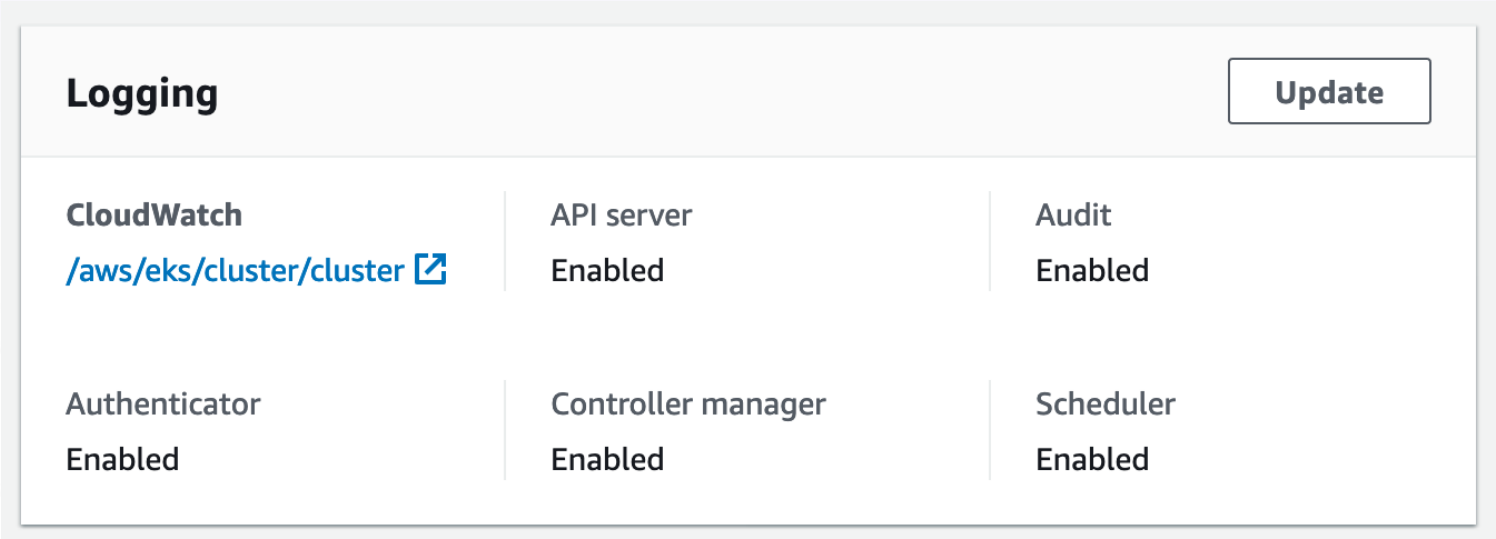
- Compute
- Storage
- Database
- Networking
- Regions
- Availability Zones
- Edge Locations

Source: AWS Summit berlin 2019

Logging and Auditing the Control Plane

Logging of the control plane, especially around an audit trail of API actions, is an important aspect of security and being able to work out who did what.

When using EKS you can (and should) enable such logging to CloudWatch Logs.



Source: AWS Summit berlin 2019

Shared Responsibility Model

CUSTOMER

Responsible for
Security "**in**" the cloud

- Customer Data
- Applications
- Platform
- Identity & Access Management
- Operating System
- Network and Firewall Configuration

AWS

Responsible for
Security "**of**" the cloud

- Compute
- Storage
- Database
- Networking
- Regions
- Availability Zones
- Edge Locations

Source: AWS Summit berlin 2019

Installing a Network Policy Provider on Kubernetes

Firewalling within Kubernetes is controlled by Network Policies. You first need to add a Network Policy Provider to EKS / Kubernetes in order to use Network Policies. A popular one covered in our documentation is Calico.

https://docs.aws.amazon.com/eks/latest/userguide/calico.html

Source: AWS Summit berlin 2019

Shared Responsibility Model

CUSTOMER

Responsible for
Security "**in**" the cloud

- Customer Data
- Applications
- Platform
- Identity & Access Management
- Operating System
- Network and Firewall Configuration

AWS

Responsible for
Security "**of**" the cloud

- Compute
- Storage
- Database
- Networking
- Regions
- Availability Zones
- Edge Locations

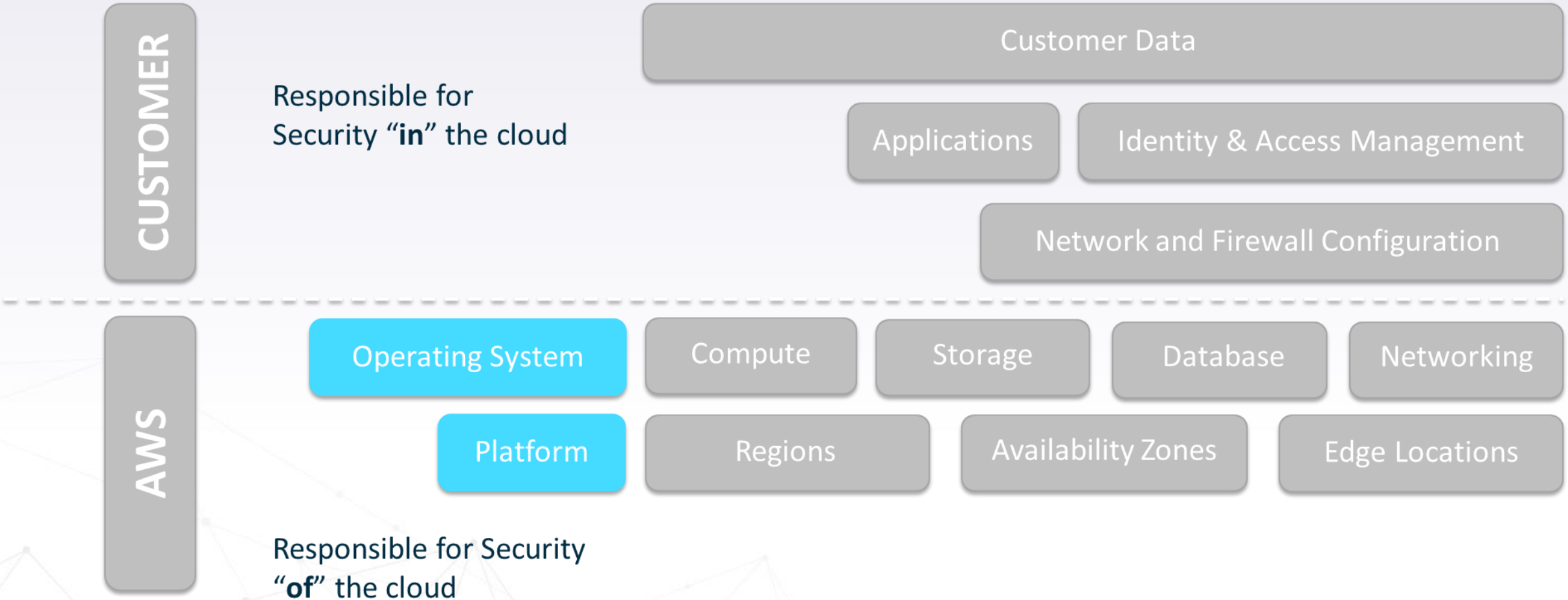
Source: AWS Summit berlin 2019

EC2 Mode – Customer Responsibilities

- Instance type and quantity to choose?
  - What is the CPU to RAM ratio?
  - Excess capacity for scaling and availability?
- Which OS to choose?
  - If Amazon Linux we provide AMIs
- Hardening the OS (e.g. against CIS benchmark)
- The patching of the OS, Docker, ECS Agent or kubelet etc.

Source: AWS Summit berlin 2019

Shared Responsibility Model - Fargate



Source: AWS Summit berlin 2019

Lab: AWS Container Immersion Day Part EKS

https://github.com/TIDC-PS-Inter/AWS-Workshop

Source: AWS Immersion day

trueIDC

REGIONAL
DATA CENTER & CLOUD SERVICE PROVIDER