
aws
INNOVATE
ONLINE CONFERENCE

aws INNOVATE
ONLINE CONFERENCE

分会场五：现代应用

基于 AWS 容器服务构建云原生应用

何归丽，AWS 解决方案架构师

议题

AWS 容器服务概览

Amazon EKS 与 AWS 其它服务的集成

新一代 IaC 部署 EKS 集群和应用

AWS 容器服务概览

aws INNOVATE
ONLINE CONFERENCE

为什么要采用容器技术?

- 敏捷开发，持续集成与发布
- 快速构建现代应用程序
- 实现任意规模的自动化

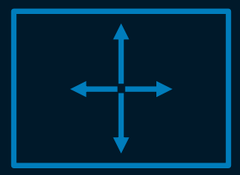
微服务是迈向现代应用的最佳选择
容器是微服务最常见的实现方式

Kubernetes 简介

CLOUD NATIVE COMPUTING FOUNDATION

kubernetes

开源的容器
管理/编排平台



协助大规模
运行容器

提供构建现代应用
的基本元素

AWS 容器技术全景图

管理

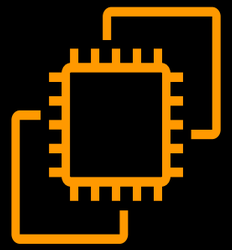
Deployment, Scheduling, Scaling & Management of containerized applications

Amazon Elastic Container Service (Amazon ECS)

Amazon Elastic Kubernetes Service (Amazon EKS)

集群

Where the containers run



Amazon EC2

AWS Fargate

镜像仓库

Container Image Repository

Amazon Elastic Container Registry

Amazon Elastic Kubernetes Service

80%

云中运行的所有容器化应用程序运行在 AWS 上的比例

84%

云中运行的所有 Kubernetes 应用运行在 AWS 上的比例

10x

EKS 使用量在一年内的增长

150%

AWS 容器服务的同比增长

1.6B+

通过 ECR 每周拉取的图像

参考链接: *https://nucleusresearch.com/research/single/guidebook-containers-and-kubernetes-on-aws/*

运行 Kubernetes 的平台至关重要

性能、稳定性、可扩展性以及与平台的良好集成

平台的品质及完整性

应用质量和良好运营

用户体验

AWS 丰富的产品服务系列

ANALYTICS 数据分析

ANALYTICS
- DATA EXCHANGE
- DATA LAKE
- DATA PIPELINES
- DATA WAREHOUSE
- ELASTICSEARCH

STREAMING
- ETL
- HADOOP/SPARK
- INTERACTIVE SQL QUERIES
- VISUALIZATIONS

AR + VR AR/VR

- AR/VR EXPERIENCES

AWS COST MANAGE 成本管理

- ANALYZE AWS COSTS
- COST & USAGE BUDGETS
- COST & USAGE REPORTS
- RESERVED INSTANCES REPORTING

APPLICATION INTEG 应用集成

- EMAIL
- MESSAGE BROKER
- QUEUEING & NOTIFICATIONS
- SEARCH
- TRANSCODING
- WORKFLOW

BUSINESS APPLICAT 企业应用

- EMAIL & CALENDARING
- ONLINE MEETINGS
- SHARING & COLLABORATION
- UNIFIED COMMUNICATIONS
- VOICE-ENABLED WORKPLACE

BLOCKCHAIN 区块链

- BLOCKCHAIN TEMPLATES
- LEDGER DATABASE
- MANAGED BLOCKCHAIN

CUSTOMER ENGAGE 客户关系

- CONTACT CENTER
- EMAIL TARGETING
- USER ENGAGEMENT ACROSS CHANNELS

COMPUTE 计算

COMPUTE
- AUTO SCALING
- BATCH JOBS
- EVENT-DRIVEN SERVERLESS COMPUTING
- INSTANCE TYPES
- MANAGED VIRTUAL PRIVATE SERVERS
- MANAGED REPOSITORY FOR SERVERLESS APPS
- RUN & MANAGE WEB APPS
- SERVERLESS COMPUTE
- VIRTUAL SERVERS

CONTAINTERS
- CONTAINER SERVICE
- MANAGED KUBERNETES
- STORE & RETRIEVE DOCKER IMAGES

DATABASE 数据库

REALTIONAL DATABASES
- HIGH-PERFORMANCE RELATIONAL DATABASE BUILT FOR THE CLOUD
- MANAGED MARIADB
- MANAGED MYSQL
- MANAGED ORACLE
- MANAGED POSTGRESQL
- MANAGED SQL SERVER

PURPOSE-BUILT DATABASES
- DOCUMENT DATABASE
- GRAPH DATABASE
- IN-MEMORY CACHING
- KEY-VALUE STORE DATABASE
- LEDGER DATABASE
- TIME SERIES DATABASE

DEVELOPER TOOLS 开发工具

- ANALYZE & DEBUG
- APPLICATION LIFECYCLE MANAGEMENT
- AUTHORING
- BUILD & TEST
- CONTAINERS
- DEVOPS RESOURCE MANAGEMENT
- ONE-CLICK APP DEVELOPMENT
- PATCHING
- PIPELINE ORCHESTRATION
- RESOURCE TEMPLATES
- TRIGGERS

END USER COMPUT 终端计算

- APP STREAMING
- DESKTOP COMPUTING
- MOBILE ACCESS
- STORAGE & COLLABORATION

HYBRID ARCHITECT 混合架构

- AWS SERVICES ON PREMISES
- DATA INTEGRATION
- INTEGRATED DEVICES & EDGE SYSTEMS
- INTEGRATED IDENTITY & ACCESS
- INTEGRATED NETWORKING
- INTEGRATED RESOURCE & DEPLOYMENT MANAGEMENT
- VMWARE CLOUD ON AWS

GAME TECH 游戏技术

- CROSS-PLATFORM 3D GAME ENGINE
- GAME SERVER HOSTING

INFRASTRUCTURE 基础设施

- AVAILABILITY ZONES
- CUSTOM HARDWARE
- DATA CENTER INFRASTRUCTURE
- GLOBAL NETWORK BACKBONE
- POINTS OF PRESENCE
- POWER INFRASTRUCTURE
- REGIONS

INTERNET OF THINGS 物联网

- RULES ENGINE
- DEVICE ANALYTICS
- DEVICE GATEWAY
- DEVICE SDK
- DEVICE SHADOWS
- EVENT DETECTION & RESPONSE
- LOCAL COMPUTE
- LOCAL DATA COLLECTION
- MANAGEMENT & SECURITY
- MICROCONTROLLER OPERATING SYSTEM
- REGISTRY
- VISUAL APPLICATIONS DEVELOPMENT

MACHINE LEARNING 机器学习

ML FRAMEWORKS
- DEEP LEARNING AMIs & CONTAINERS
- HARDWARE ACCELERATION
- ML AT THE EDGE
- TENSORFLOW, PYTORCH, MXNET

AI SERVICES
- CHATBOTS
- ENTITY EXTRACTION
- FACE ANALYTICS
- FACE SEARCH
- FORECASTING
- IMAGE LABELING
- NATURAL LANGUAGE PROCESSING
- PERSONALIZATION & RECOMMENDATION
- SENTIMENT ANALYSIS
- SPEECH TRANSCRIPTION
- TEXT & DATA EXTRACTION
- TEXT TO SPEECH
- TRANSLATION
- VIDEO & IMAGE ANALYSIS
- CONTENT MODERATION

SAGEMAKER
- AUTOMATIC MODEL TUNING
- DATA LABELING
- HOSTED NOTEBOOKS
- ML MARKETPLACE
- MODEL HOSTING
- MODEL OPTIMIZATION
- MODEL TRAINING
- PRE-BUILT ALGORITHMS
- TOPIC MODELING
- DEEP LEARNING MODELS
- REINFORCEMENT LEARNING
- SPOT INSTANCES
- BATCH PREDICTIONS
- REAL-TIME PREDICTIONS

MANAGEMENT & GOVERNANCE 管理/治理

- ACTIVITY & API USAGE TRACKING
- CHATBOT
- CONFIGURATION TRACKING
- GOVERNANCE
- INVENTORY TRACKING
- LICENSE MANAGER
- MANAGE POLICIES
- MANAGE RESOURCES
- MONITORING
- PROVISIONING
- RESOURCE TEMPLATES
- SECURITY RECOMMENDATIONS
- SERVER MANAGEMENT
- SERVICE CATALOG
- SYSTEMS MANAGER

MARKETPLACE 第三方服务市场

- ANALYTICS
- DATA PRODUCTS
- DATABASES
- DEVOPS
- IOT
- MACHINE LEARNING
- NETWORKING
- OPERATING SYSTEMS
- SECURITY
- STORAGE

MEDIA SERVICES 媒体服务

- LIVE VIDEO TRANSPORT
- MEDIA STORAGE
- TRANSCODING
- VIDEO ORIGINATION & PACKAGING
- VIDEO PERSONALIZATION & MONETIZATION
- VIDEO PROCESSING & DELIVERY
- VIDEO STREAMING ANALYSIS

MIGRATION & TRA 迁移与传送

- APPLICATION MIGRATION
- DATABASE MIGRATION
- EXABYTE-SCALE MIGRATION
- ONLINE DATA TRANSFER
- SCHEMA CONVERSION
- SERVER MIGRATION
- TRANSFER FOR SFTP

MOBILE 移动服务

- API GATEWAY
- DEVELOPMENT FRAMEWORK
- IDENTITY
- MOBILE ANALYTICS
- MOBILE APP TESTING
- SINGLE INTEGRATED CONSOLE
- SYNC
- TARGETED PUSH NOTIFICATIONS

NETWORKING & CONTENT DELIVERY 网络

- APPLICATION DELIVERY
- DEDICATED NETWORK CONNECTION
- DOMAIN NAME SYSTEM
- LOAD BALANCING
- MONITOR APIS
- MONITOR MICROSERVICES
- NETWORK TOPOLOGY
- NETWORKING HUB
- PRIVATE CONNECTION TO APPS
- SCALE VPC & ACCOUNT CONNECTIONS
- SERVICE DISCOVERY
- VIRTUAL PRIVATE CLOUD

ROBOTICS 机器人

- CLOUD ROBOTICS

SATELLITE 卫星

- SATELLITE OPERATIONS

SECURITY, IDE & COMPLIANC 安全, 认证, 合规

- ACCESS CONTROL
- ASSESSMENT & REPORTING
- CONFIGURATION COMPLIANCE
- DATA PROTECTION
- DDOS PROTECTION
- IDENTITY MANAGEMENT
- KEY MANAGEMENT & STORAGE
- MONITORING & LOGGING
- RESOURCE MANAGEMENT
- THREAT DETECTION
- WEB APPLICATION FIREWALL

STORAGE 存储

- ARCHIVE STORAGE
- BACKUP & RESTORE
- BLOCK STORAGE
- DATA TRANSFER
- EDGE PROCESSING & COMPUTING
- FILE STORAGE
- HIGH-PERFORMANCE FILE SYSTEM
- HYBRID CLOUD STORAGE
- OBJECT STORAGE
- WINDOWS FILE SYSTEM

CUSTOMER ENABLE 客户使能

- ACCOUNT MANAGEMENT
- DASHBOARD PERSONALIZATION
- ENTERPRISE SUPPORT
- EXPERTS MARKETPLACE
- OPTIMIZATION GUIDANCE
- PARTNER ECOSYSTEMS
- PROFESSIONAL SERVICES
- SECURITY & BILLING REPORTS
- SOLUTIONS MANAGEMENT
- TRAINING & CERTIFICATION

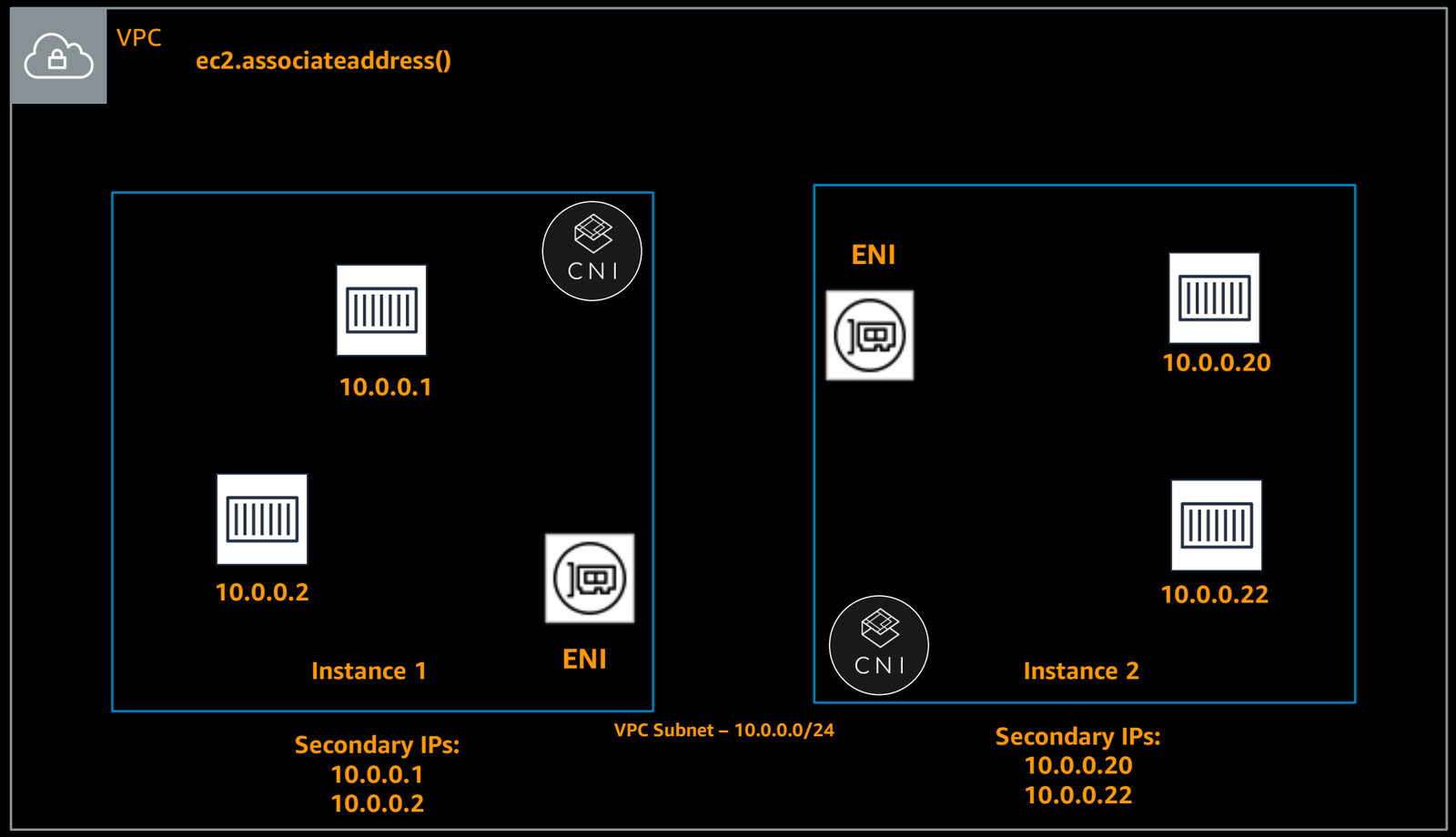
Amazon EKS 与 AWS 其它服务的集成

aws INNOVATE
ONLINE CONFERENCE

Amazon EKS 与 AWS 服务的集成

AWS VPC CNI 插件

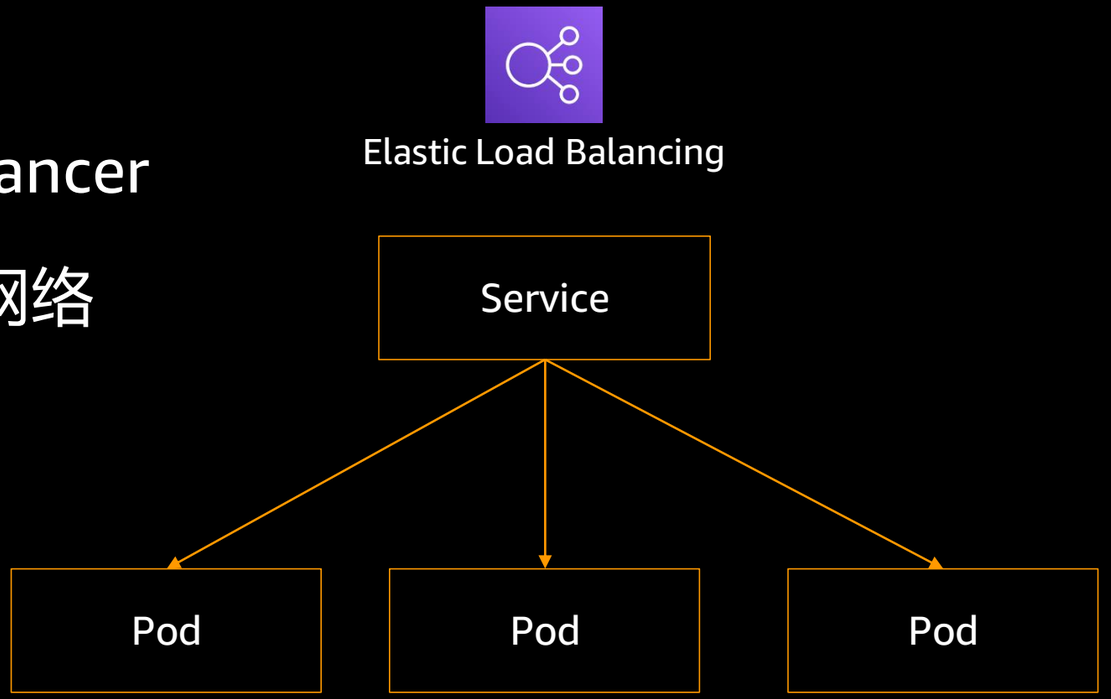
- 带有 CNI 插件的本地 VPC 网
- Pod 内部与 VPC 具有相同的 VPC 地址
- 简单，安全的网络
- 开源 / GitHub



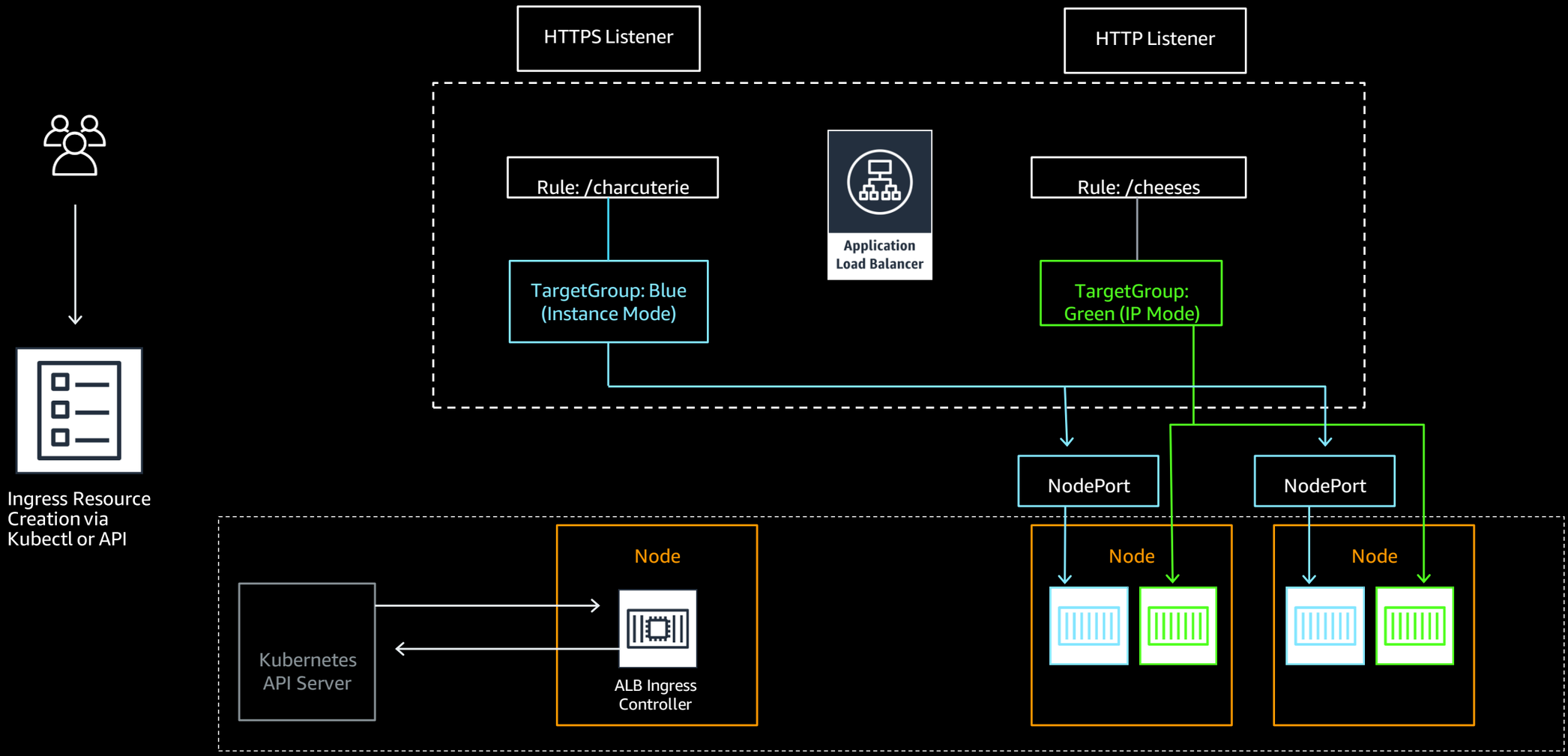
https://github.com/aws/amazon-vpc-cni-k8s

全面支持 AWS 各种负载均衡器

- Network Load Balancer , Classic Load Balancer
- 支持 L4 (TCP 等) or L7 (HTTP/HTTPS) 网络
- 通过 Annotation 支持 ELB 特性
- 自动创建

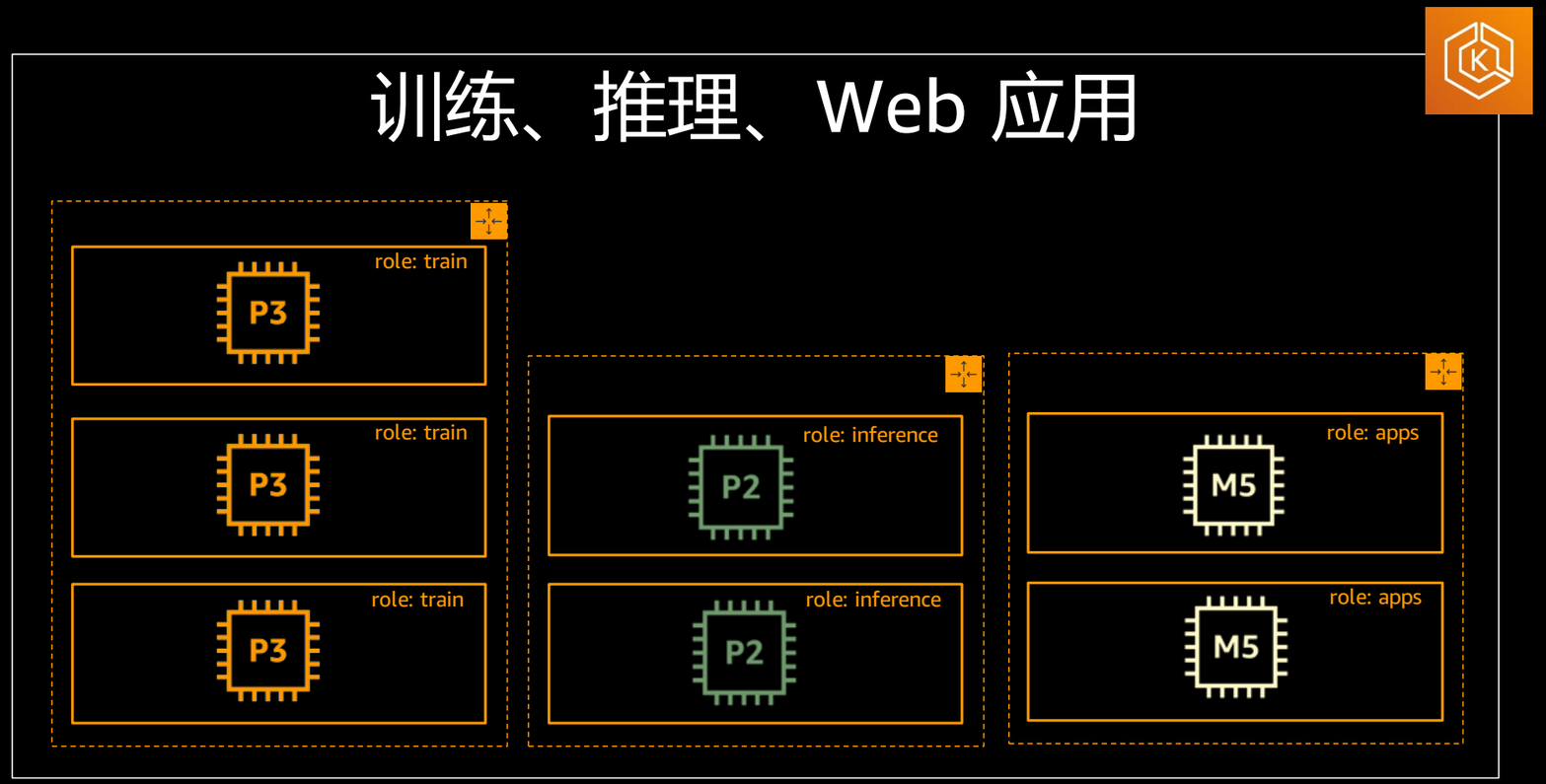


ALB Ingress Controller



https://github.com/kubernetes-sigs/aws-alb-ingress-controller

灵活使用多个节点组承载不同的负载

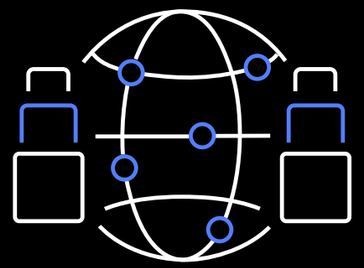


nodeSelector:
role: train

Amazon EKS 集群

可使用 Spot 实例大幅节省成本

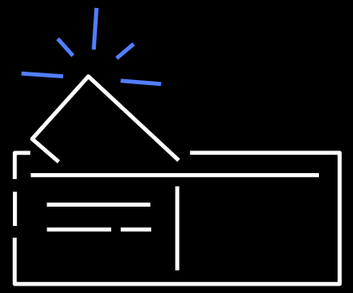
合理地使用将获得 70–90% 的成本节省



Spot 为富余容量

与按需实例

相同的基础架构



Spot 价格

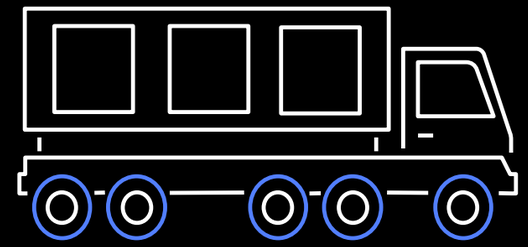
平滑、不频繁的变化

无峰值，可预测

中 断

仅在按需实例需求容量

时发生（非比价模式）



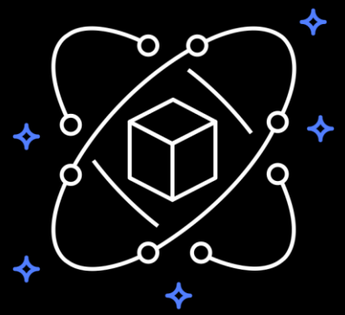
弹 性

可选择多种实例类型，

大小和可用区

https://github.com/aws/aws-node-termination-handler

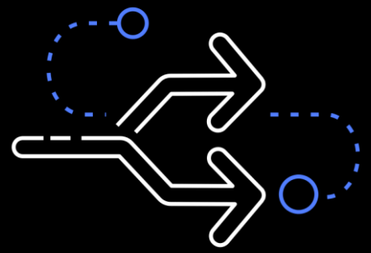
Amazon EKS 托管节点组



一条命令管理工作节点

使用 EKS Console, APIs, eksctl, Cloudformation 或者 Terraform.

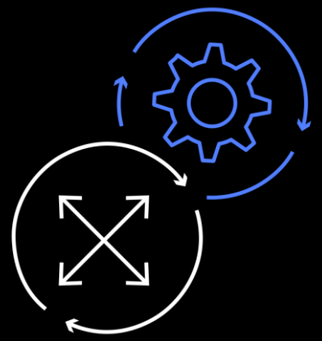
支持Kubernetes labels



持续更新

使用最新的 EKS-optimized AMIs.

轻松滚动更新



高可用特性

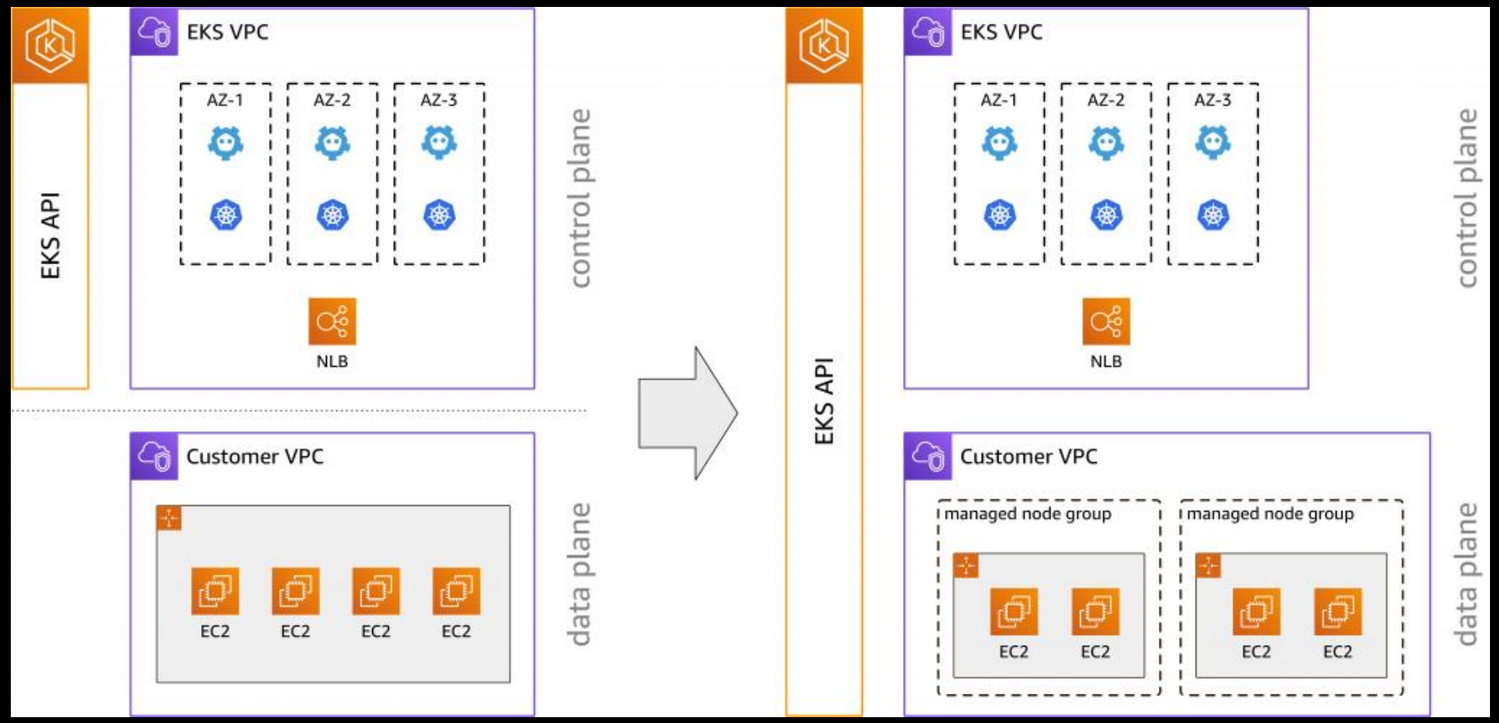
跨多可用区部署

自动配置检查，节点健康检查

删除节点前自动 cordon 和 drain

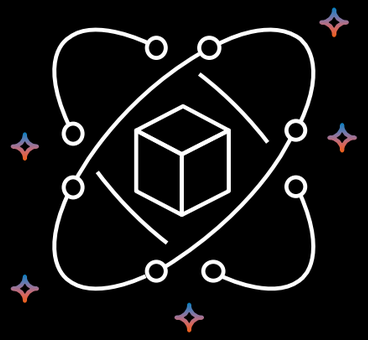
Amazon EKS 托管节点组

- 与 AWS Auto Scaling 集成自动完成跨可用区弹性伸缩节点
- 滚动更新节点组，安全撤出工作节点确保应用的高可用性
- 支持 Windows 和 Linux 节点
- 无额外成本



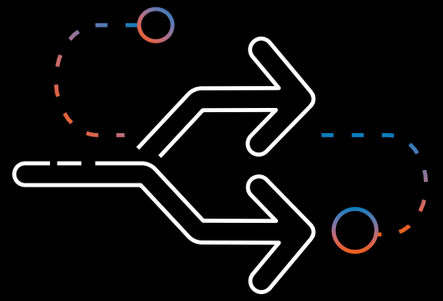
支持 Kubernetes 1.14 eks.3 以上
支持 EKS Console， eksctl， AWS CLI， AWS API， CDK，CloudFormation和Terraform

Amazon EKS on Fargate



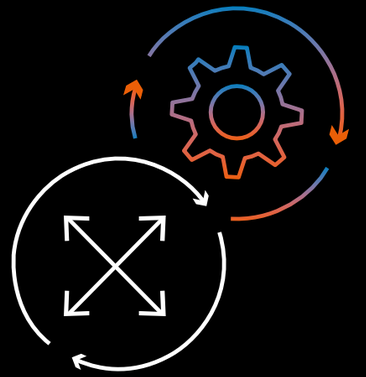
运行现有 Pod

无需更改现有 pod。Fargate 可以支持 Kubernetes 上现有的工作流程和服务。



适用于生产环境

快速启动 Pod。轻松跨多可用区运行 pod，获得高可用。每个 pod 都运行在隔离的计算环境中。

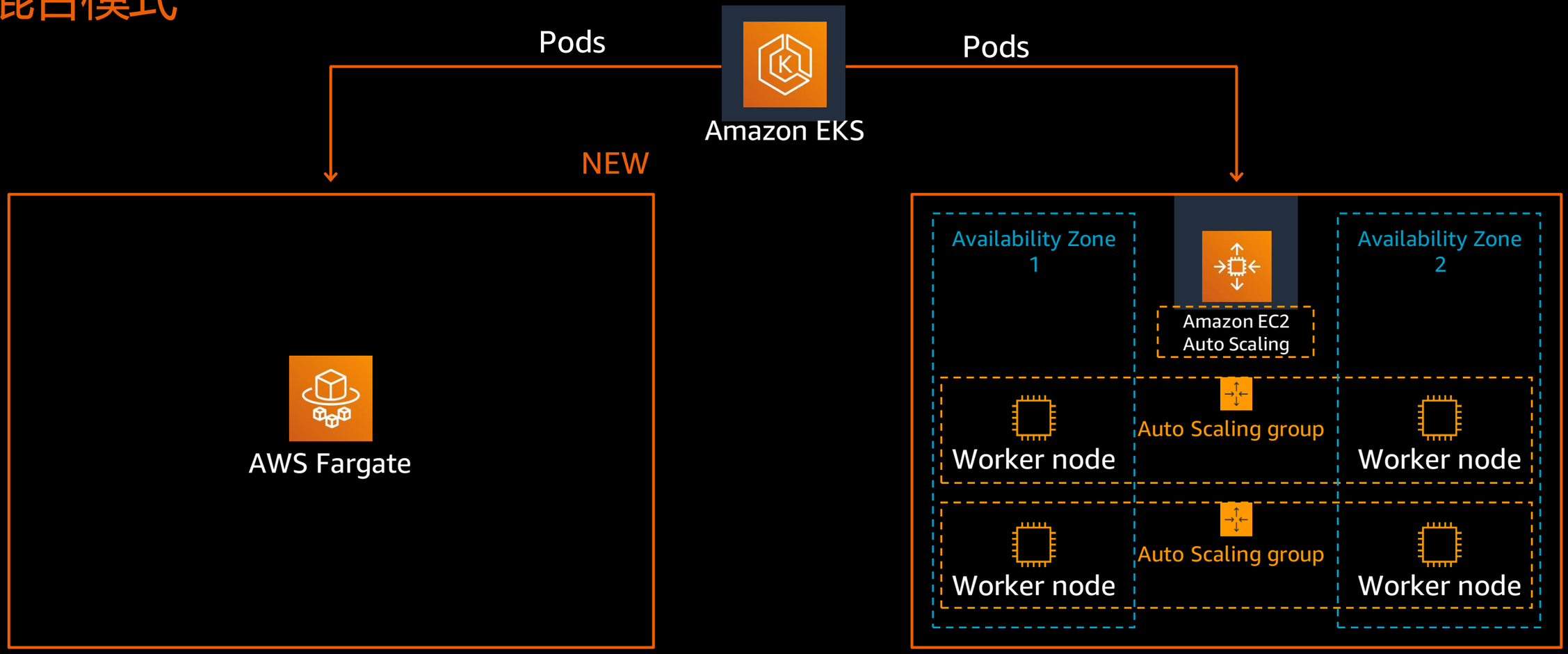


自动分配资源/原生集成

仅为运行 Pod 所需的资源付费。与 AWS 原生的网络和安全服务集成。

EKS 数据平面选项

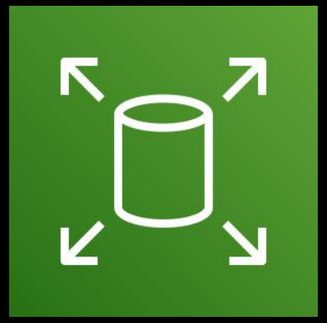
混合模式



Serverless container data plane

Traditional container data plane

与 AWS 存储服务全面集成



EBS CSI 驱动

https://github.com/kubernetes-sigs/aws-ebs-csi-driver

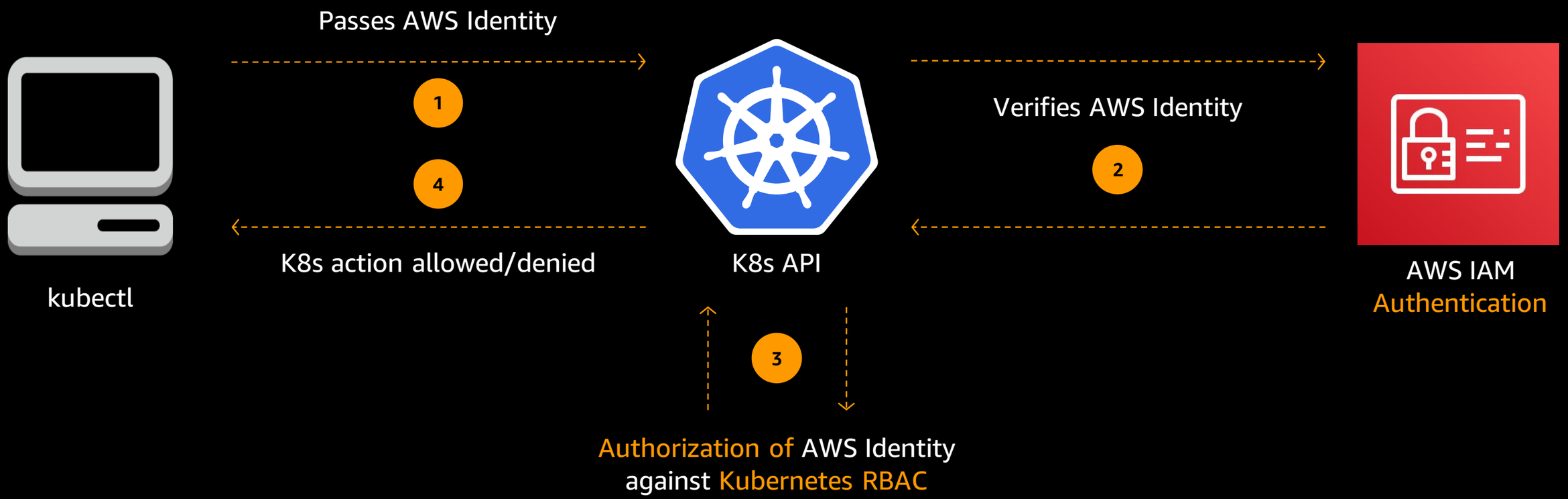
EFS CSI 驱动

https://github.com/kubernetes-sigs/aws-efs-csi-driver

FSx for Lustre CSI 驱动

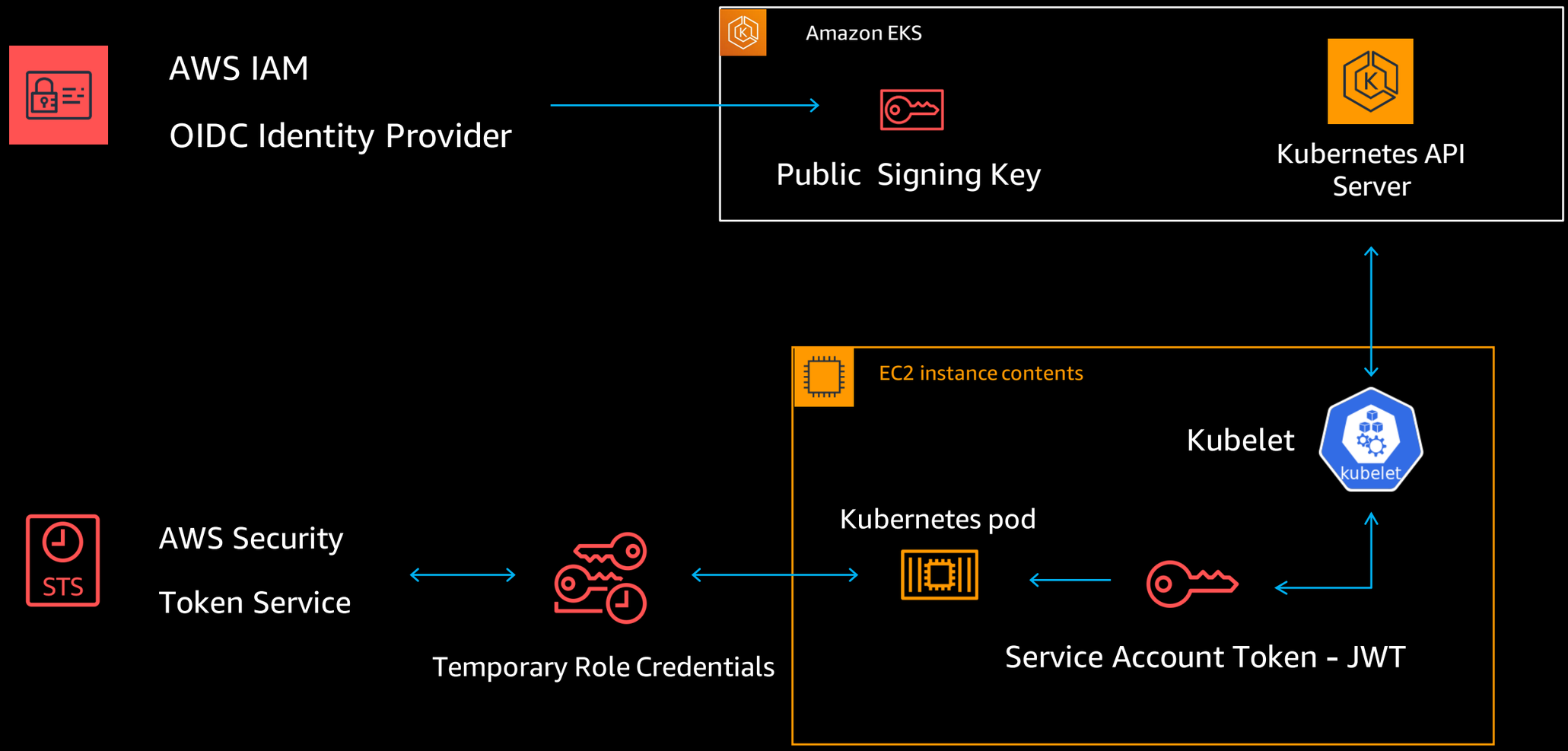
https://github.com/kubernetes-sigs/aws-fsx-csi-driver

与 IAM 的融合提供高安全性



https://github.com/kubernetes-sigs/aws-iam-authenticator

AWS IAM Roles for Service Accounts

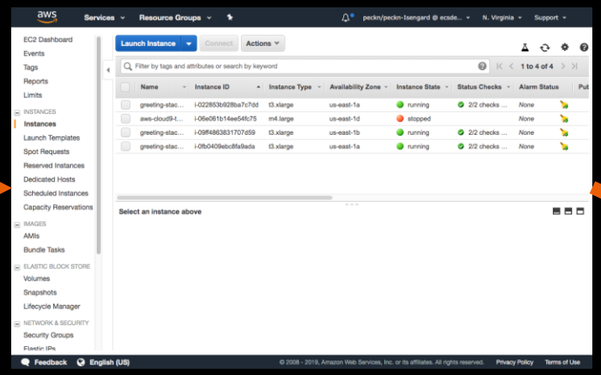


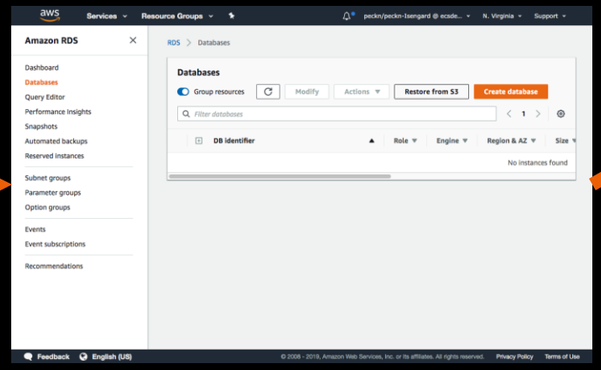
https://github.com/aws/amazon-eks-pod-identity-webhook/

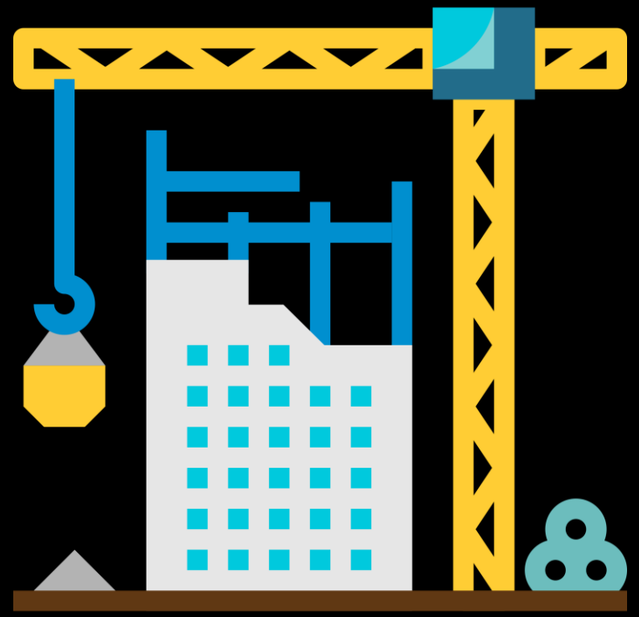
使用新一代 IaC 部署 EKS 集群和应用

aws INNOVATE
ONLINE CONFERENCE

Level 0: 手动创建基础架构

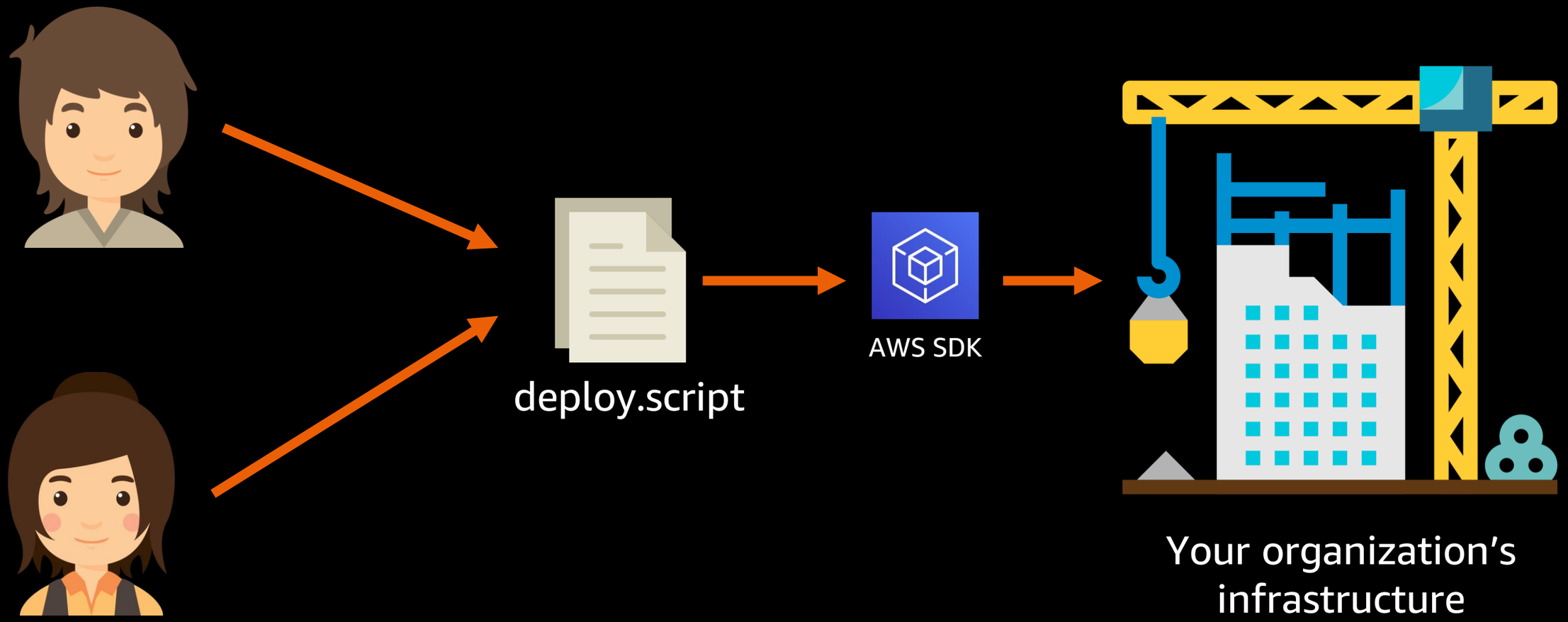




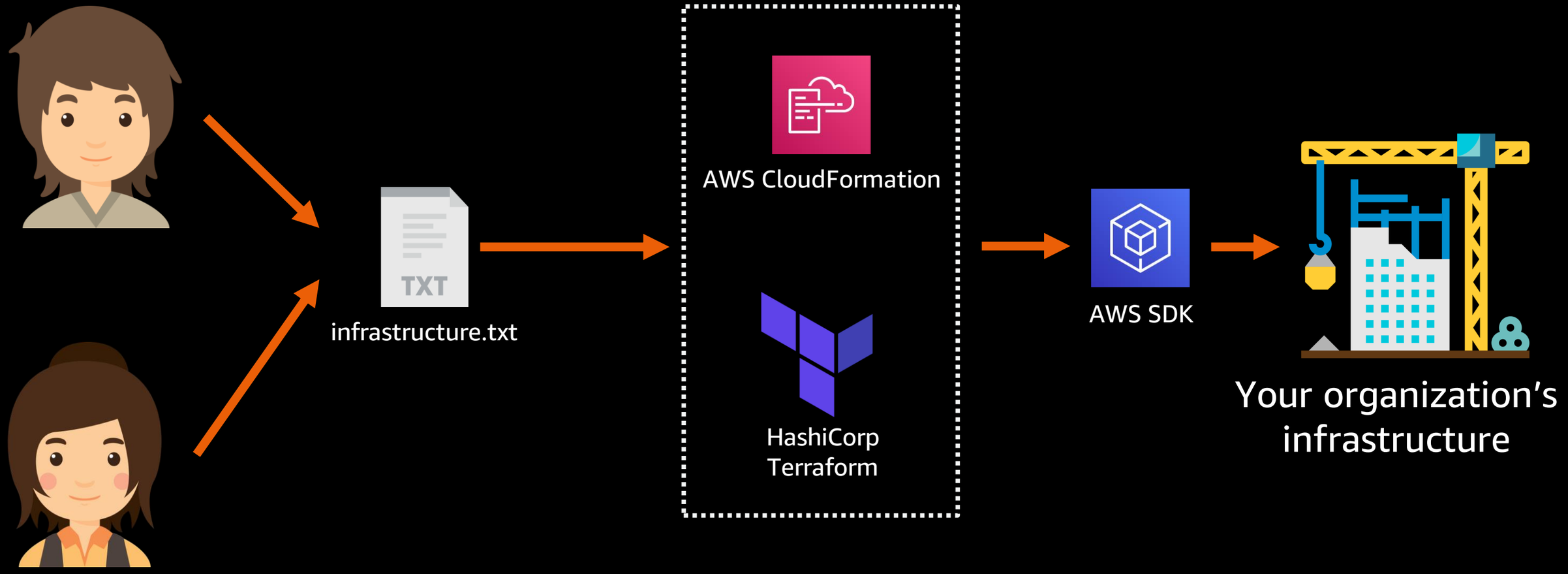


Your organization's infrastructure

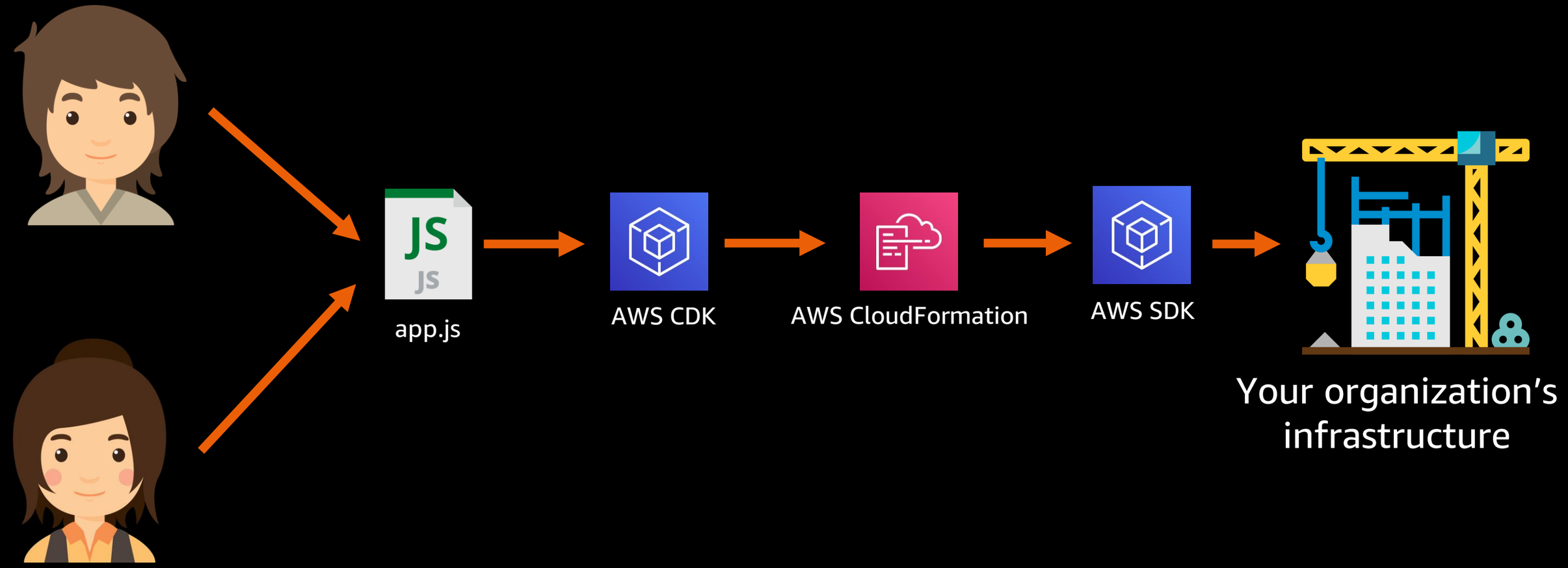
Level 1: 指令式 基础架构即代码



Level 2: 申明式基础架构即代码



Level 3: AWS Cloud Development Kit (AWS CDK)



AWS CDK 构建 EKS 集群并部署应用程序

```
// Create EKS cluster with 2 m5.large workers nodes
const cluster = new eks.Cluster(this, ‘eks1’);



// Add Fargate profile
cluster.addFargateProfile('MyProfile', {
  selectors: [ { namespace: 'default' } ]
});



// Add Spot instance node group
cluster.addCapacity('spot', {
  spotPrice: '0.1094’,
  instanceType: new ec2.InstanceType('t3.large’),
  maxCapacity: 10
});
```

```
// Add k8s Pod
cluster.addResource('mypod', {
  apiVersion: 'v1’,
  kind: 'Pod’,
  metadata: { name: 'mypod' },
  spec: {
    containers: [{
      name: 'hello’,
      image: 'paulbouwer/hello-kubernetes:1.5’,
      ports: [ { containerPort: 8080 } ]
    }]
  }
});

// Add Helm Chart
cluster.addChart('NginxIngress', {
  chart: 'nginx-ingress’,
  repository: 'https://helm.nginx.com/stable’,
  namespace: 'kube-system'
});
```

感谢参加 AWS INNOVATE 2020 在线技术大会

我们希望您在这里找到感兴趣的内容！

也请帮助我们完成**投票打分**和**反馈问卷**。

欲获取关于 AWS 的更多信息和技术内容，可以通过以下方式找到我们：

微信订阅号：AWS 云计算（awschina）

微信服务号：AWS Builder 俱乐部（amazonaws）

新浪微博：https://www.weibo.com/amazonaws/

抖音：亚马逊云计算（抖音号：266052872）

视频中心：http://aws.amazon.bokecc.com/

博客：https://aws.amazon.com/cn/blogs/china/

更多线上活动 ： https://aws.amazon.com/cn/about-aws/events/webinar/

AWS 中国账户注册

AWS 全球账户注册

aws INNOVATE
ONLINE CONFERENCE