



INNOVATE CHINA 2018

在线技术大会



带你开启 Kubernetes 的云端之旅

周琦, AWS 解决方案架构师

演讲日程



- AWS 容器平台发展历程
- AWS 上运行 Kubernetes 集群的选择
- 什么是 Amazon EKS?
- Amazon EKS 架构介绍
- 通过 Amazon EKS 创建你的第一个托管 Kubernetes 集群

AWS 容器管理平台的前世今生



Amazon ECS (Elastic Container Service)

AWS 2015 年推出的第一款云中托管的容器集群管理服务



aws vpc 网络模式



全球部署



进阶的任务置放策略



强力的编排引擎



深度集成 AWS 相关服务



自动扩展组

...



ECS CLI



Amazon CloudWatch 监控
指标



负载均衡器



AWS Fargate 让客户专注于开发应用



AWS Fargate



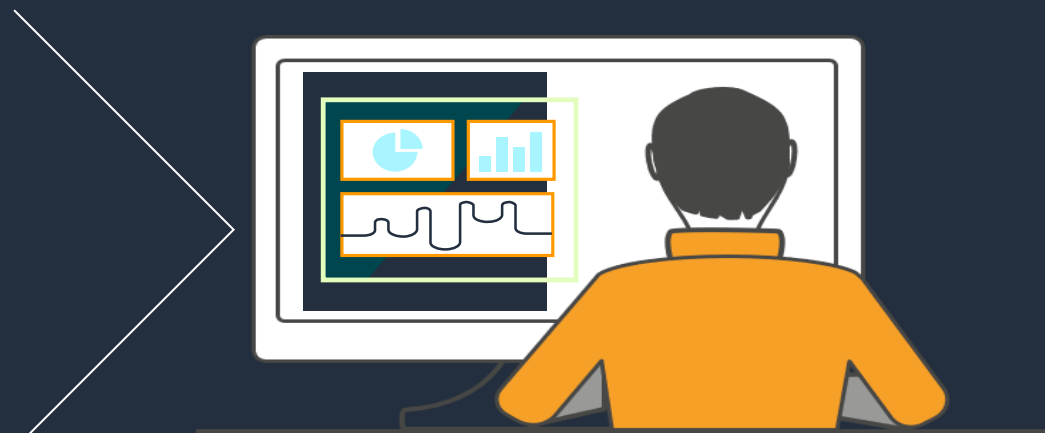
无需管理基
础设施



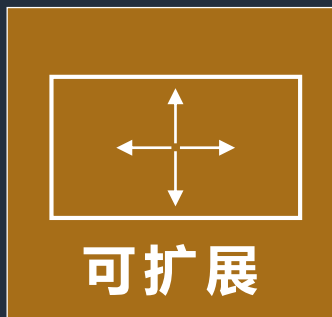
围绕任务为中
心的原生 API



基于实际的任
务资源计费



开发者青睐 Kubernetes



AWS 是众多客户首选的容器应用技术平台



57%

of Kubernetes workloads
run on AWS today
—CNCF survey

<https://www.cncf.io/blog/2017/12/06/cloud-native-technologies-scaling-production-applications/>

Kubernetes Cluster 搭建的选择

开发测试环境—Minikube

开源社区—Kops

- List: kubernetes-aws.io

 [kubernetes / kops](#)

企业级

- Rancher
- CoreOS Tectonic
- Red Hat OpenShift



自定义

- CloudFormation
- Terraform

APN 合作伙伴: Docker, Heptio, Mesosphere

通过 Kops 管理 Kubernetes 集群

github.com/kubernetes/kops

```
export AWS_AVAILABILITY_ZONES=${ZONES:-"us-east-1b,us-east-1c,us-east-1d"}
export KOPS_STATE_STORE="s3://kubernetes-aws-io"
kops create cluster cluster.k8s.local \
  --master-count 3 \
  --master-size m4.large \
  --node-count 5 \
  --node-size m4.large \
  --zones $AWS_AVAILABILITY_ZONES \
  --networking calico \
  --yes
```

AWS 上自建 Kubernetes 集群典型架构



Amazon EKS (Elastic Container Service for Kubernetes)



Amazon EKS



和开源 Kubernetes
一致体验



Upstream
保持和上游同步



支持企业生产级别的
容器应用



按需和 AWS 服务无
缝集成

Amazon EKS 集群典型架构



如何访问 Amazon EKS 集群

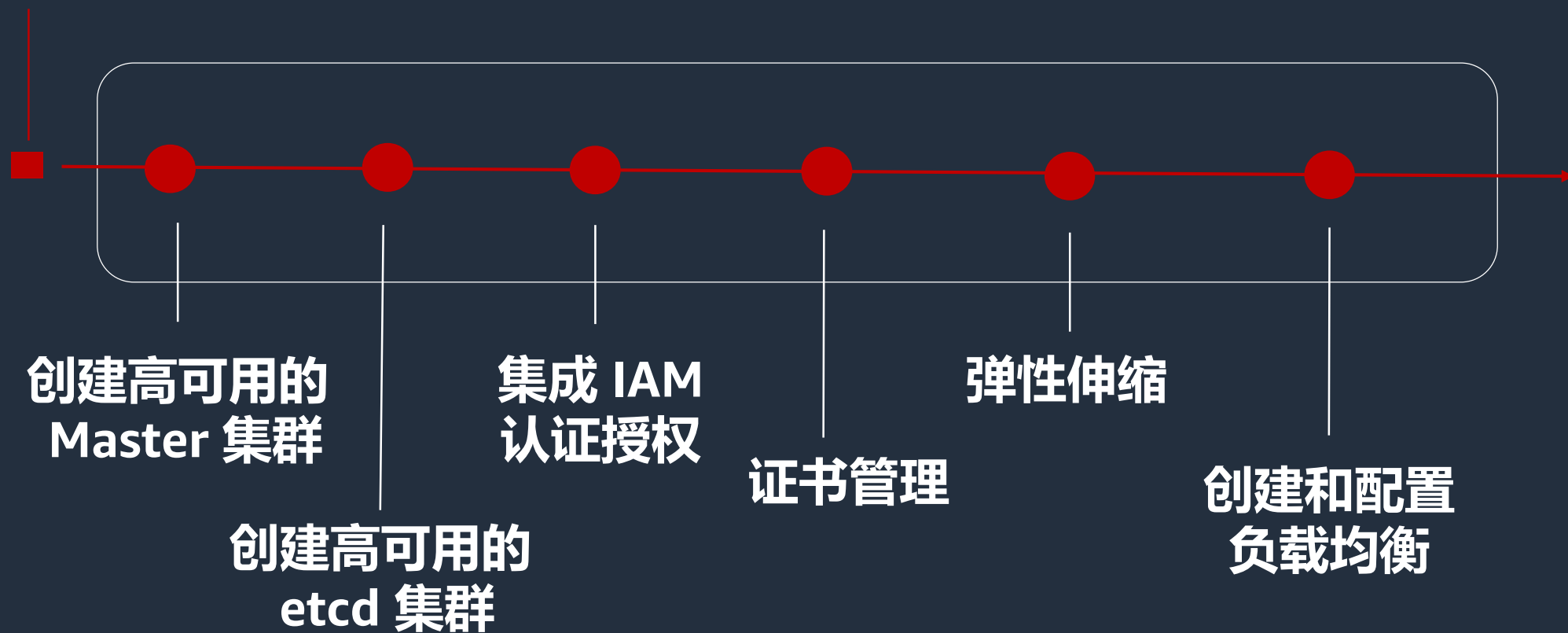


Amazon EKS 用户体验

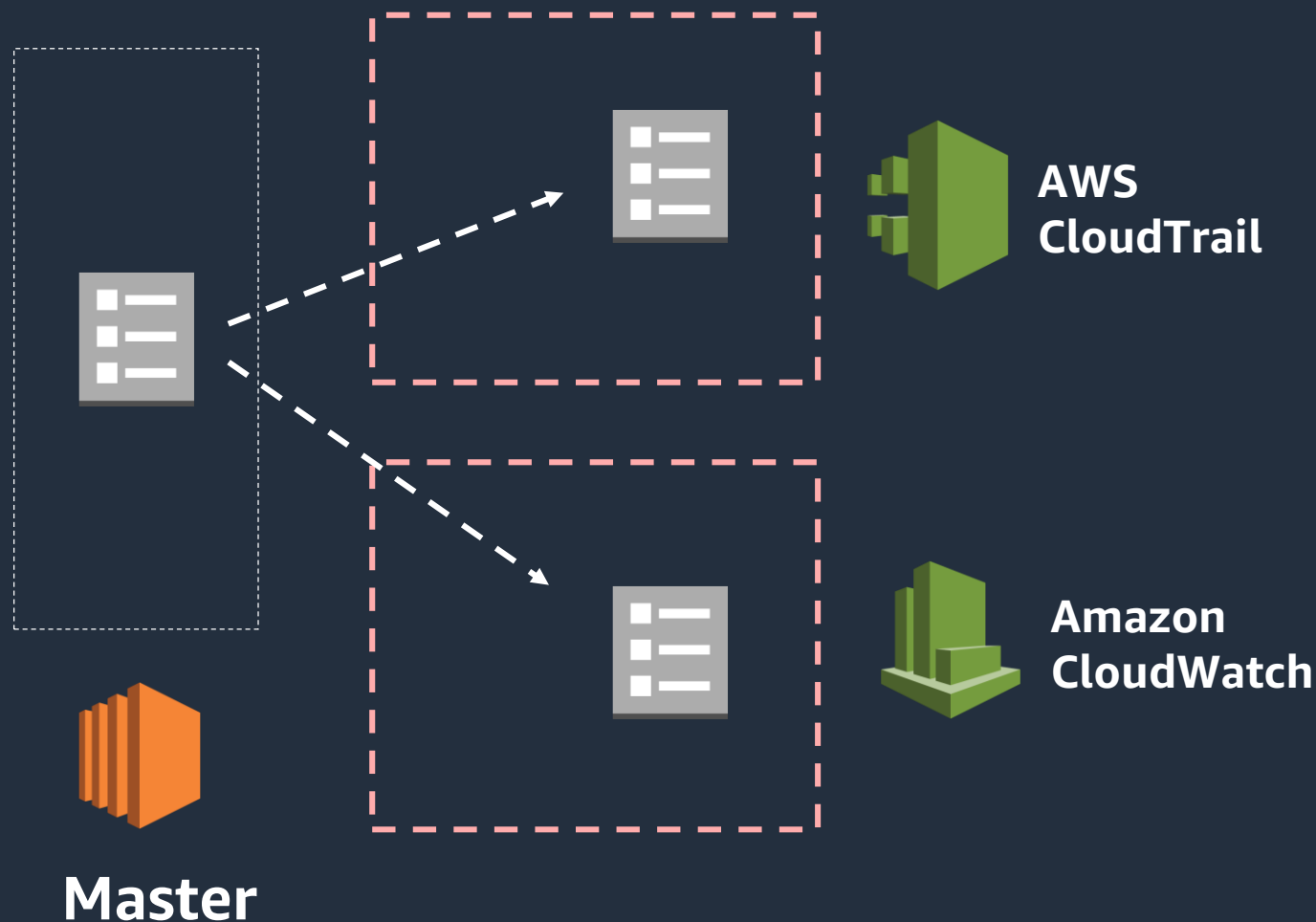


Amazon EKS Master 节点 创建过程

创建 Master



Amazon EKS Master 节点弹性伸缩

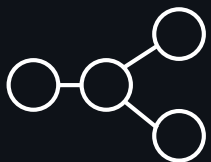


Amazon EKS 监控 Master 节点的性能指标，并在必要时进行扩展，保证 Kubernetes 集群控制平面的高可用性

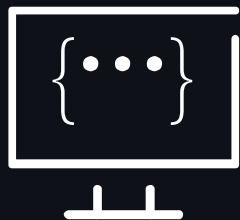
通过 Amazon CloudTrail 记录 EKS API 调用，Kubernetes Master 节点日志可以通过 CloudWatch 获得



支持 Kubernetes 集群的 Amazon VPC CNI 网络插件



原生的网络模型通过
CNI 插件支持 K8S



Pods 拥有和 VPC 中
节点 (Nodes) 一样的
VPC 网络地址



简单、安全、高效的
网络模型



Github 开源

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

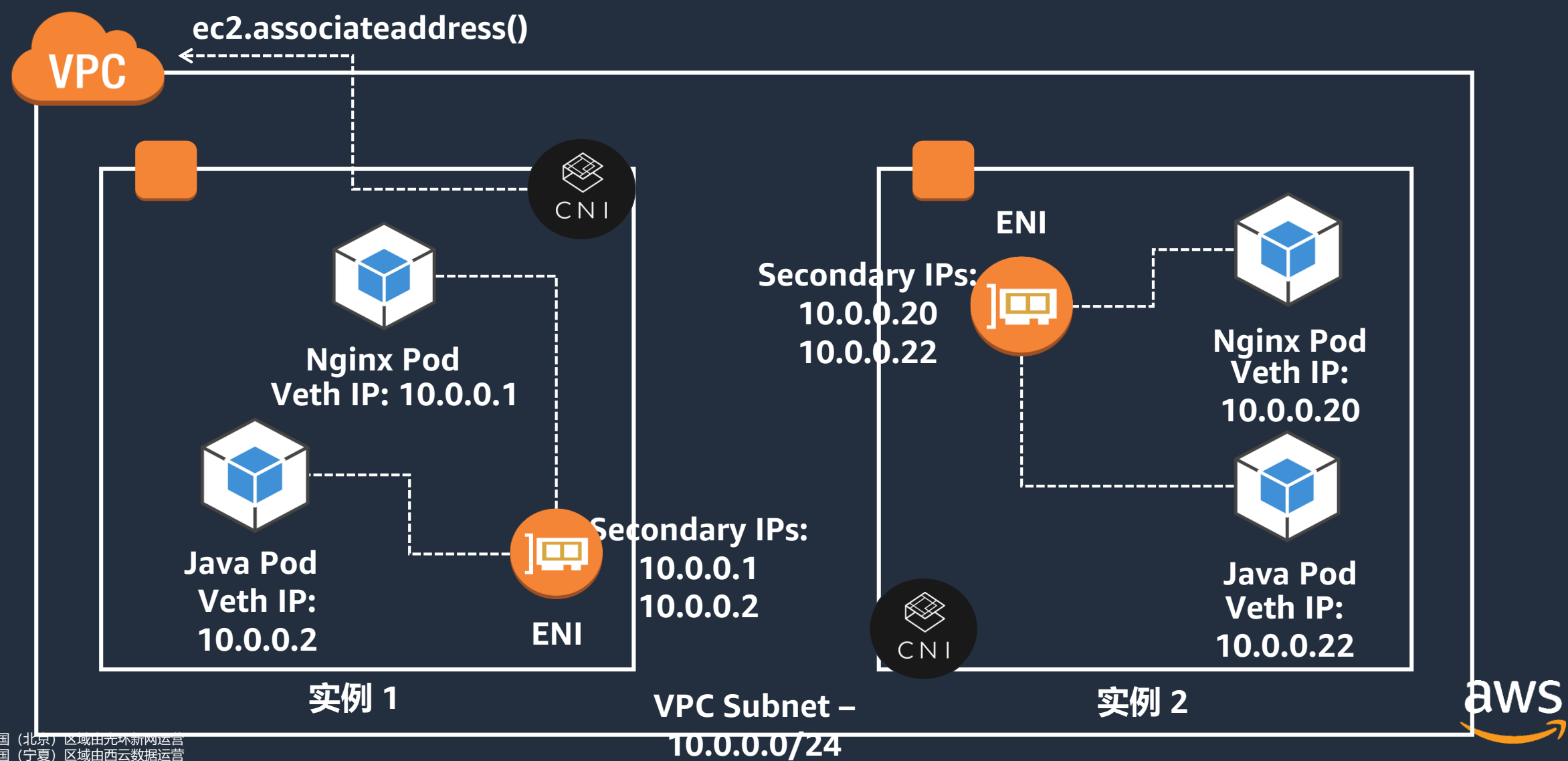


可以用在哪些 Kubernetes 场景?

- 任何运行在 AWS 上的 Kubernetes 集群:
 - Amazon EKS
 - BYO Kubernetes
- Daemonset 方式部署

```
kubectl create -f eks-cni.yaml
```

基于 Amazon VPC CNI 网络插件连接过程



Amazon EKS 如何保障网络安全?



**Kubernetes 网络策略
定义基于网络安全规
则的访问控制**



**Calico 是目前领先的
网络策略 API 接口的
实现方案**



**开源, 活跃的社区
(>100 贡献者)**



**Tigera 可提供商业支
持**

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

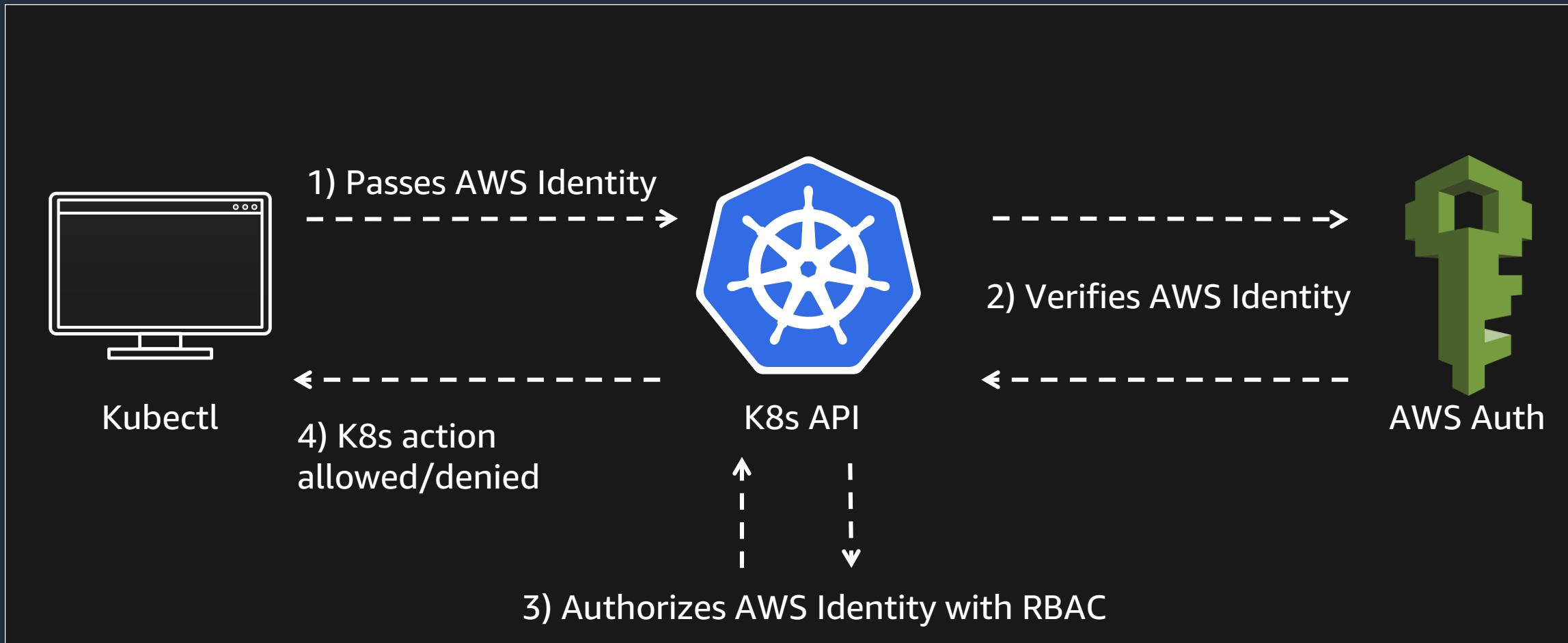


Kubernetes 集成 AWS IAM 认证授权

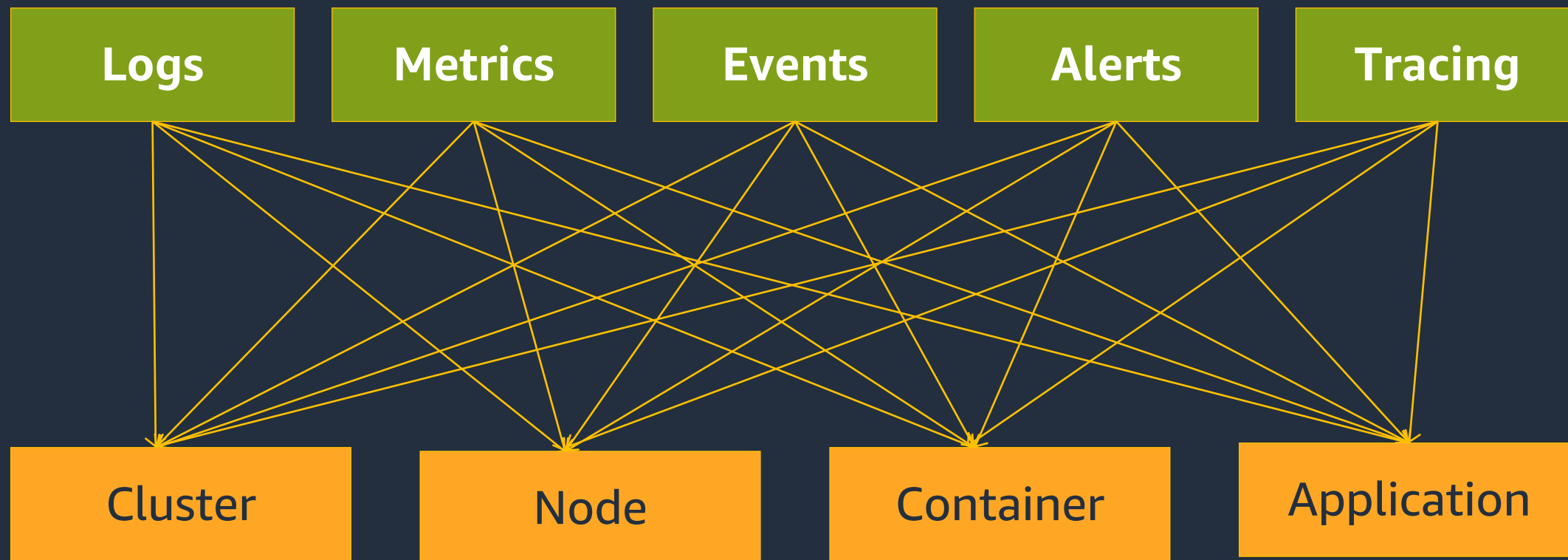
- AWS 原生的访问控制
- 和 Heptio 合作开发
- 支持 Kubectl 和 Worker 节点的认证授权
- 兼容 Kubernetes RBAC



用户认证和授权过程



Kubernetes 集群的可视化

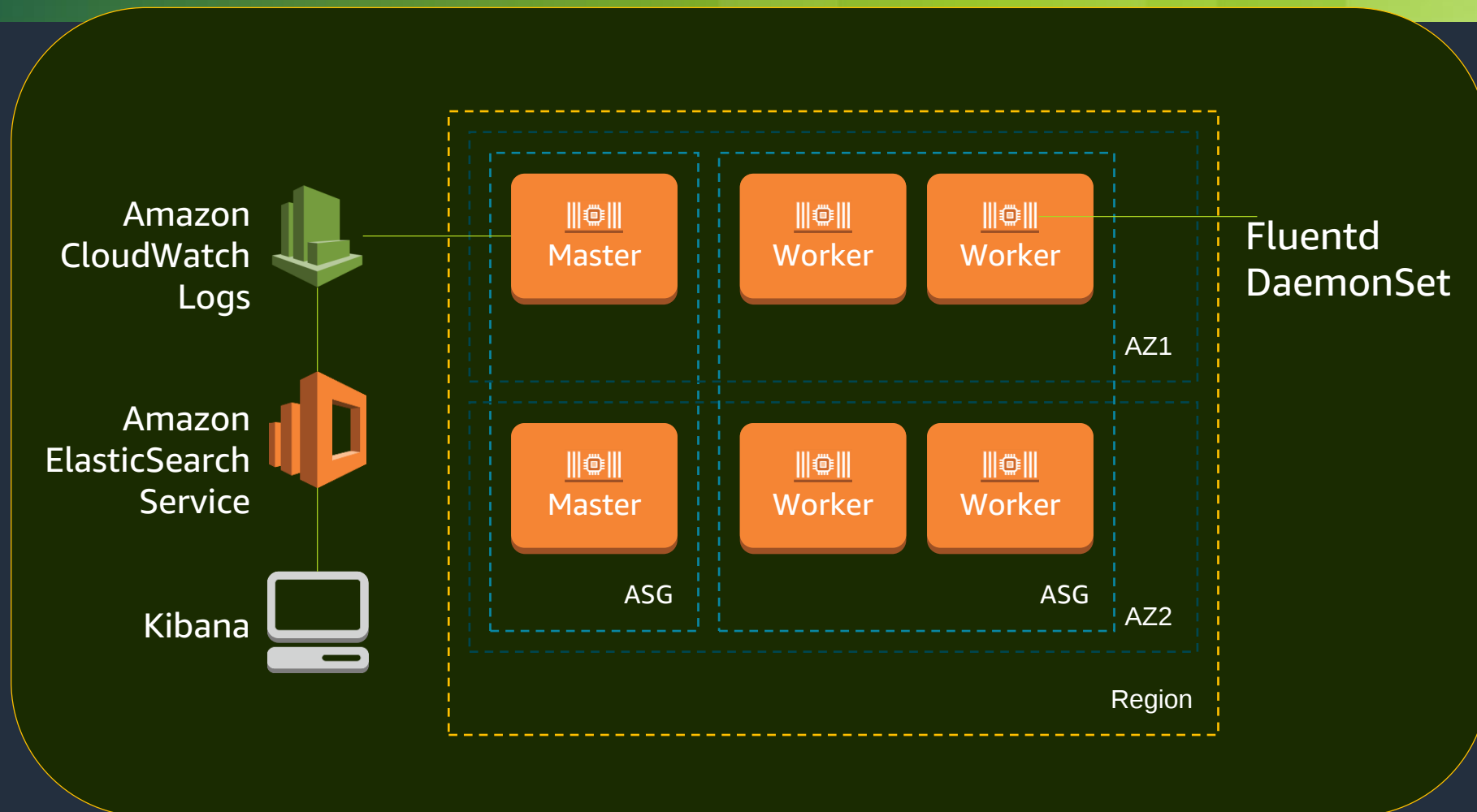


Amazon EKS 日志管理

日志

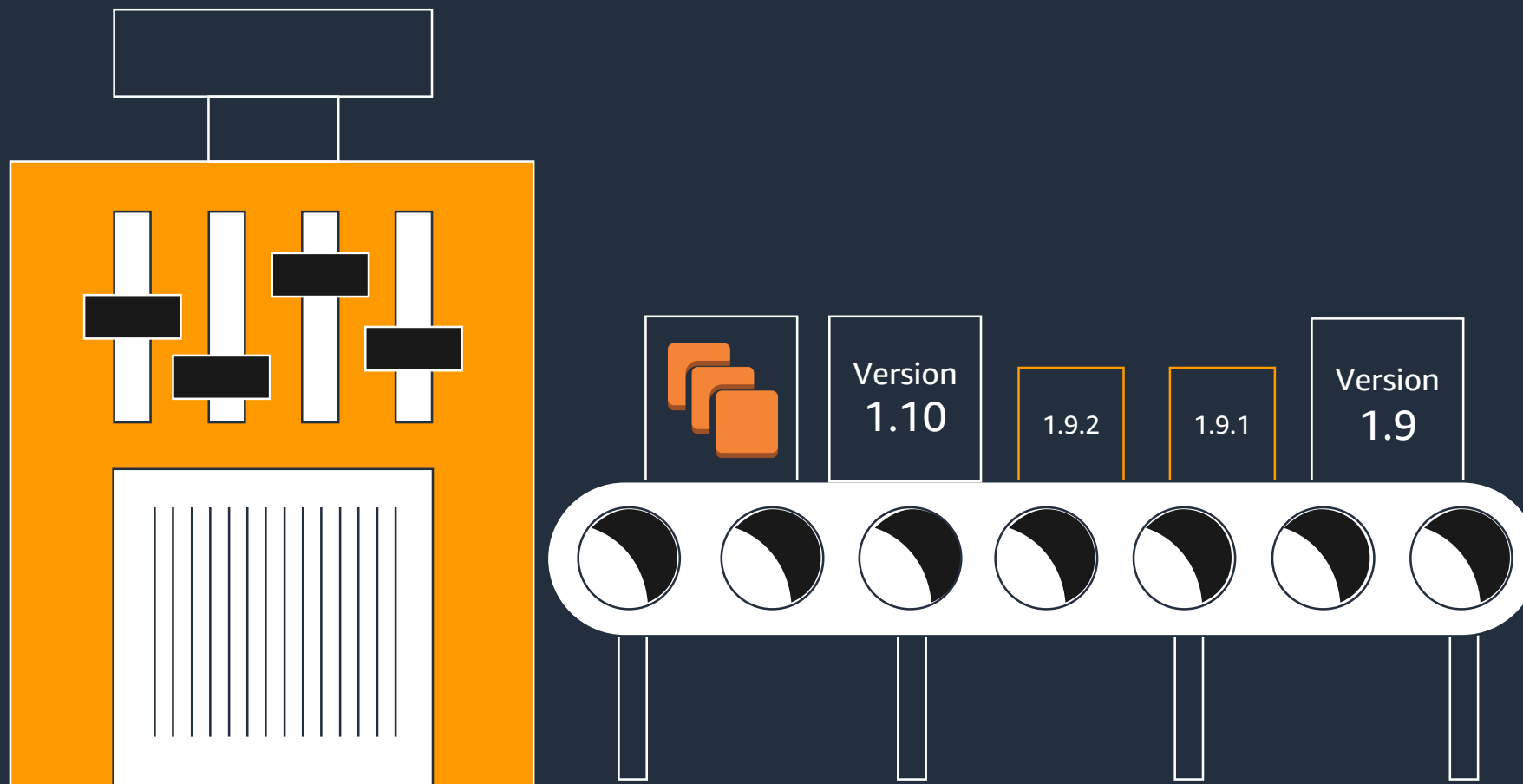
Kubectl logs

Elasticsearch (索引),
Fluentd (存储), 以及
Kibana (可视化)

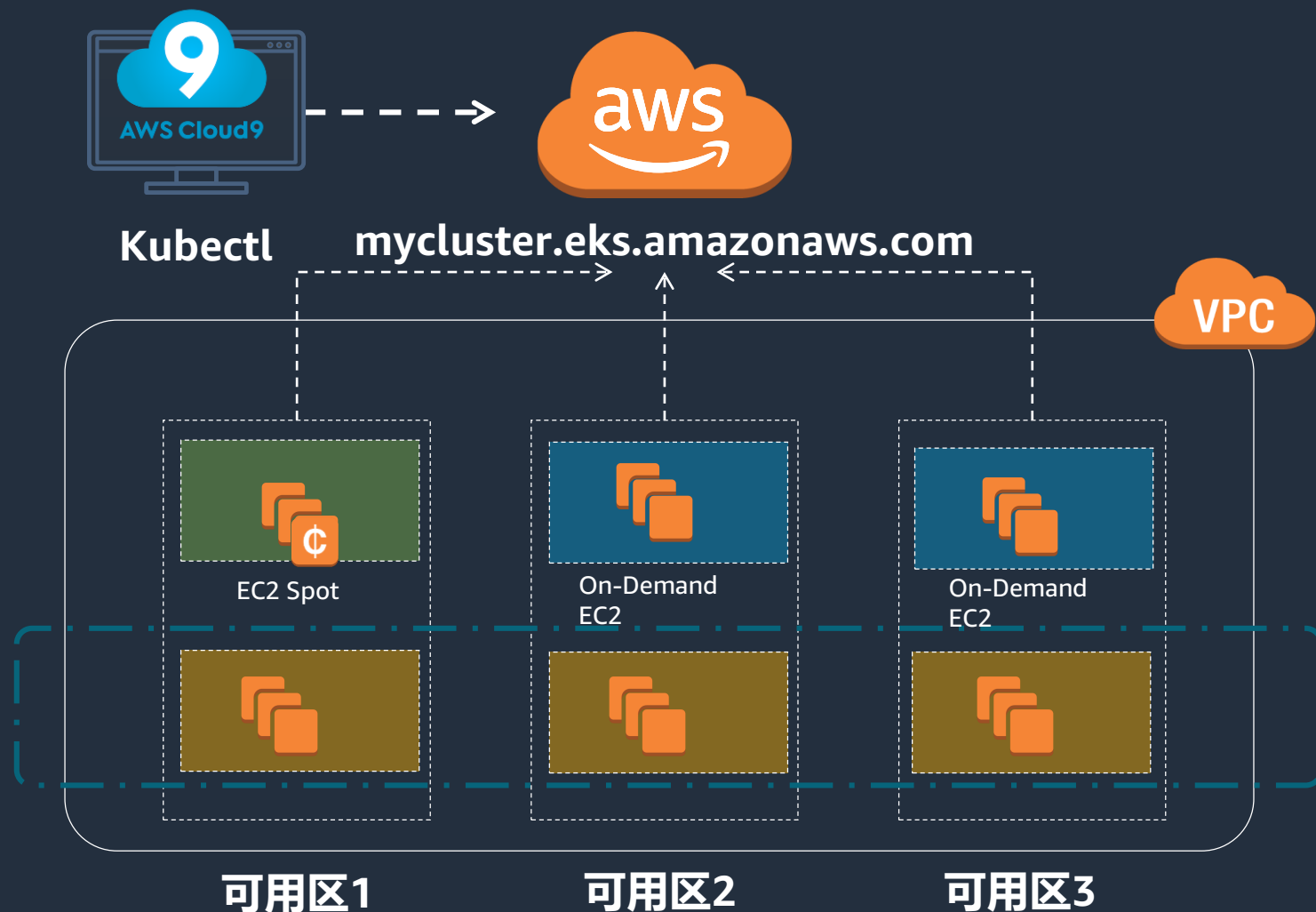


<https://github.com/aws-samples/aws-workshop-for-kubernetes/tree/master/02-path-working-with-clusters/204-cluster-logging-with-EFK>

可选择的自动升级配置



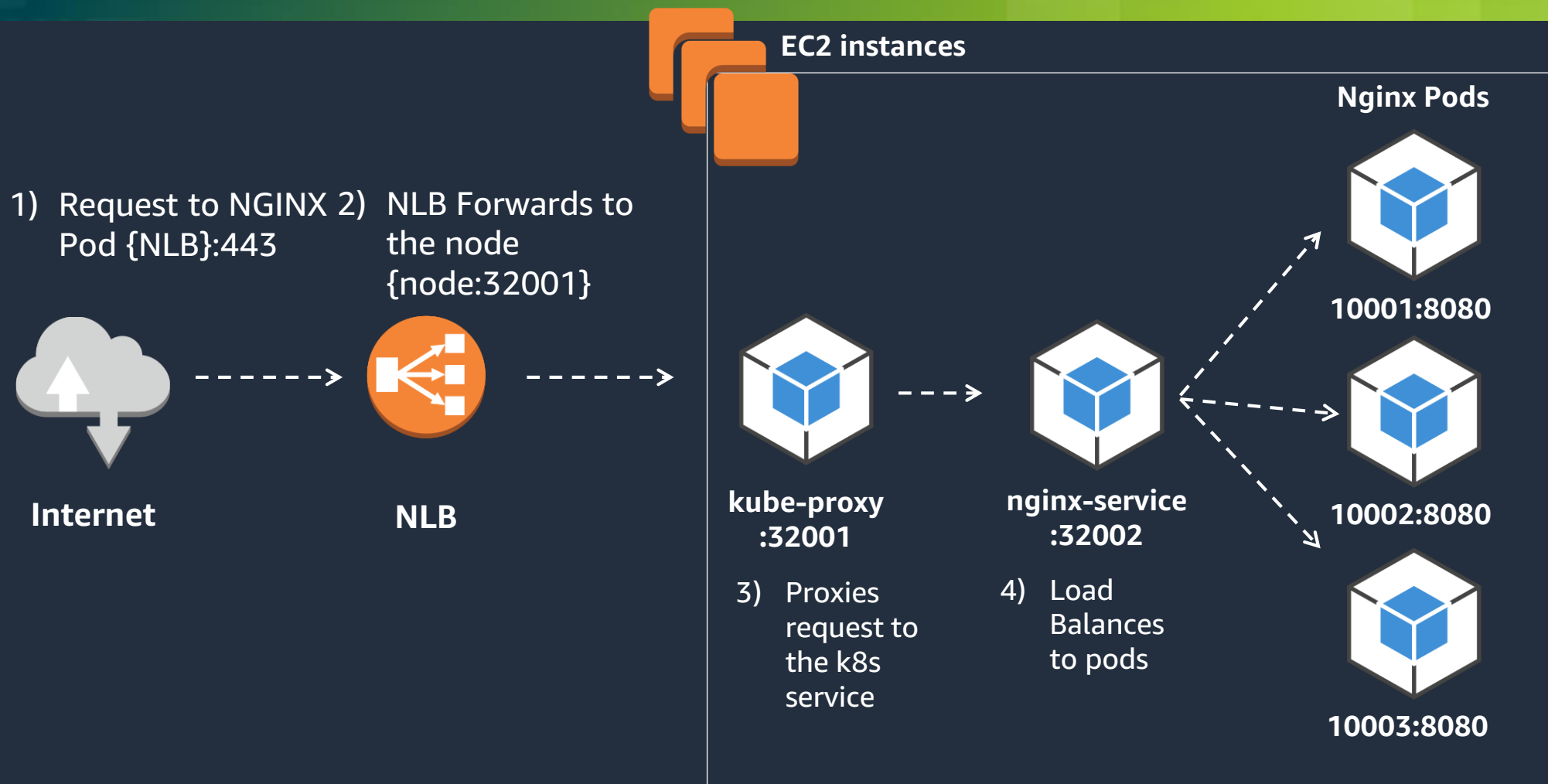
Amazon EKS 节点弹性伸缩(Cluster-Autoscaler)



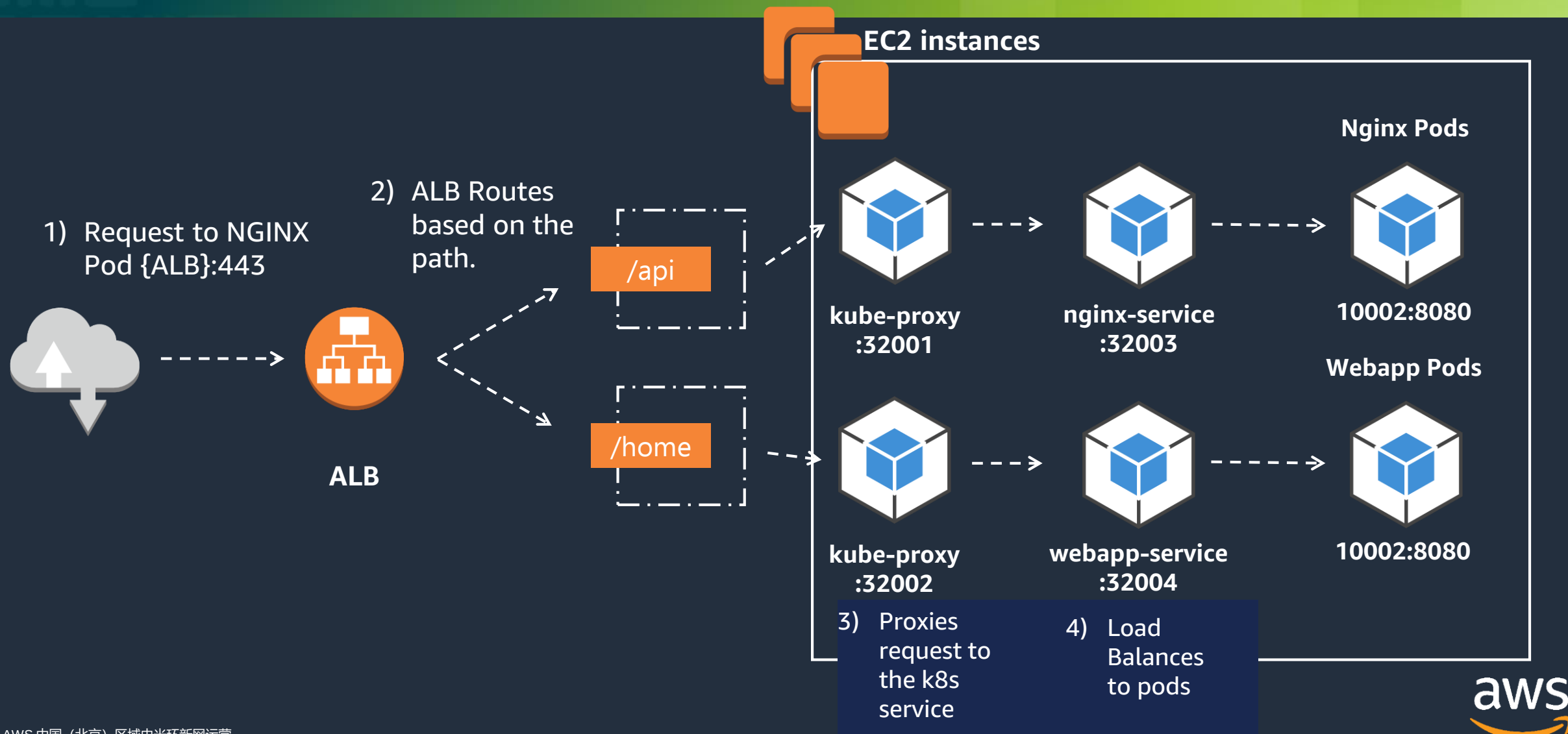
Cluster-autoscaler add-on 与 ASG 结合实现 worker nodes 节点扩展

Worker nodes 可以选择 On-Demand 或者 Amazon EC2 Spot 节点注册在 Amazon EKS 集群中

Amazon EKS Ingress 选择 (ELB/NLB)



Amazon EKS Ingress 选择 (ALB)



Amazon EKS 的 APN 合作伙伴生态体系



codefresh



heptio



weaveworks



TIGERA



DATADOG



sumologic®



GitLab



RANCHER®



Couchbase

cloudera®

signal fx

mongoDB

solarwinds
The Power to Manage IT



TREND
MICRO™



alcide



HASURA



New
Relic®



SUSE®



CISCO

APPDYNAMICS



Amazon EKS 客户案例



未来由你选择

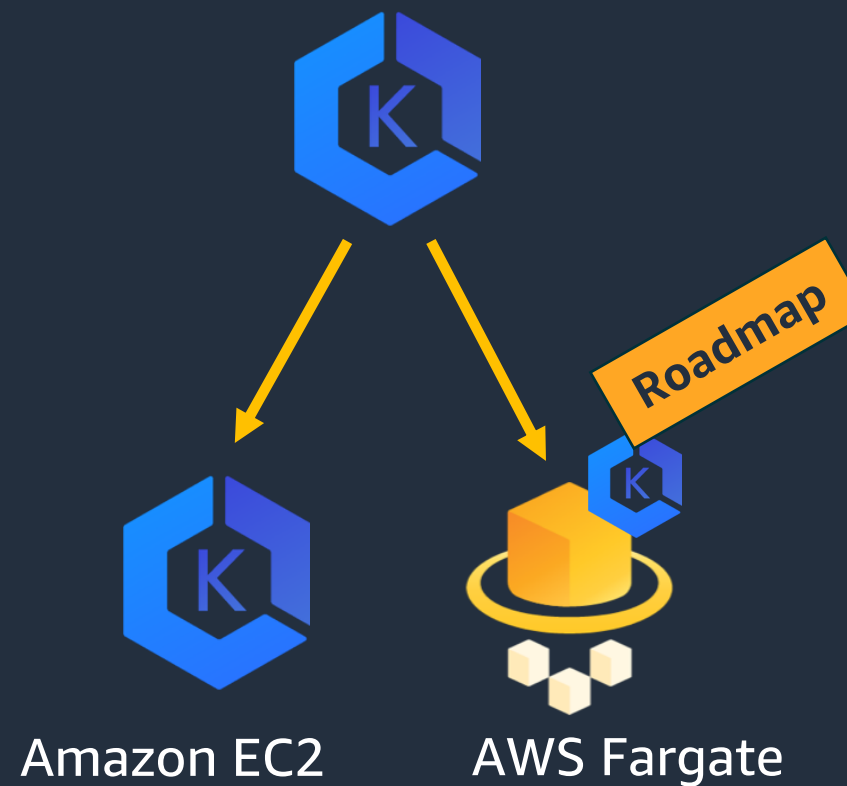
1. 选择需要的编排工具.

2. 选择需要的运行模式.

Amazon ECS



Amazon EKS



创建第一个 Amazon EKS 集群

创建集群环境的先决条件

- 创建您的 Amazon EKS 服务角色
- 创建您的 Amazon EKS 集群 VPC 及 Security Group
- 为 Amazon EKS 安装 kubectl
 - 为 Amazon EKS 安装 heptio-authenticator-aws
- 安装最新版本的 AWS CLI
 - Amazon EKS 至少需要版本 1.15.32 的 AWS CLI
 - 系统的 Python 版本必须为 Python 3 或 Python 2.7.9 或更高版本。

请参考：

https://docs.aws.amazon.com/zh_cn/eks/latest/userguide/getting-started.html

创建第一个 Amazon EKS 集群

```
aws eks create-cluster --cluster-name innovate2018 --desired-master-version  
1.10 --role-arn arn:aws:iam::account-id:role/role-name  
subnetIds=subnetid,securityGroupIds=security-group-id
```

```
186590d978e3:kubernetes zhouqiz$ aws eks create-cluster --name innovate2018 --role-arn arn:aws:iam::442073319574:role/eksServiceRole --resources-vpc-config subnetIds=subnet-02b3e  
c0b0707bc72d,subnet-068b7e05f051c7a81,subnet-036b4441d7d84bedd,subnet-0041a973268162bf8,securityGroupIds=sg-02bf871985a56d108  
{  
  "cluster": {  
    "status": "CREATING",  
    "name": "innovate2018",  
    "certificateAuthority": {},  
    "roleArn": "arn:aws:iam::442073319574:role/eksServiceRole",  
    "resourcesVpcConfig": {  
      "subnetIds": [  
        "subnet-02b3ec0b0707bc72d",  
        "subnet-068b7e05f051c7a81",  
        "subnet-036b4441d7d84bedd",  
        "subnet-0041a973268162bf8"  
      ],  
      "vpcId": "vpc-0757dcedf8b23f268",  
      "securityGroupIds": [  
        "sg-02bf871985a56d108"  
      ]  
    },  
    "version": "1.10",  
    "arn": "arn:aws:eks:us-east-1:442073319574:cluster/innovate2018",  
    "createdAt": 1534489272.188  
  }  
}
```

获取 endpoint 及 certificateAuthority 信息

```
aws eks describe-cluster --name innovate2018
```

```
186590d978e3:kubernetes zhouqiz$ aws eks describe-cluster --name innovate2018
```

```
{
  "cluster": {
    "status": "ACTIVE",
    "endpoint": "https://224CD333884F870CDCC7FF0A90AA95FA.yl4.us-east-1.eks.amazonaws.com",
    "name": "innovate2018",
    "certificateAuthority": {
      "data": "LS0tLS1lbnRlcjEwLWVudC0ubG9zaXZlLnN5RENDQWJDZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVFERXdwc
mRXSmwKY201bGRHVnpNQjRYFRFNE1EZ3h0eKEzTURrek4xb1hEVEk0TURneE5EQTNNGT6TjFvd0ZURVRNqkVHQTTFVRQpBeE1LYTNWaVpYSnVaWFJsY3pDQ0FTSXdEUVlKS29aSWh
2Y05BUUVCQlFBRGdnRVB BRENDQVFvQ2dnRUJBT TVrCkd tVE5pMWZoU25kdGlUOS9xYkd pRjE2Vm g zZW5IRG14Z3FFcTU4M3NtWVZXSmxkYjh hQzI1REtGYnd0c2hXR00KWDVtTVRvZ
FRPN3ZFRmtJd0t5OG9TVzhkRkJscDJZtVFp2RkRSOApYUUFUR0tzTk5KZTR3RlNsT29qanBudUZBWVU5UjhaWDDSV1UzZDJy bU4zMGI
mSlRzU2x4dFR2Y2c5QjdIRy9OCjN JjeEZHTz1VUit0MHF4TKnpRWNaDU1XZ08wK29ZeFdYK3NYMGQKZVo1ZGs zMVArAHJMcnB40DZLN
UVCL2x FZXVjWG01M2dPRkttMEN1V0tqZUNPwUN6bUo2bj10N2ZGMnF4N2t1Lwp6bTFIK01FcDR5RVE2bTBKK1NNQ0F3RUFBYU1qTUNFd0RnWURWUjBQQVFILOjBUURBZ0trTUE4R0E
xVWRFd0VCCi93UUZNQU1CQWY4d0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dFRkFLVTdBc2IyY1lRNngwNSs1Zk xJAFhqNnRVRjQKQXdyNFJWSXROaGJIbUNiM2hiTk t3bWRiMno5b292b
zg1VEgrOWs1V052Y2w0UDhuMXlxVlVHU21VUG1VZTV2SQpGNi8rQVB BbEhvSEl LOXQzV1FBc0NAel l iVmVkSuPNSXRrVXhtRX d1dmNLNFPUM2tLOGJPMWUwZEVXWlFDa010CmExUXF
OMmFZaVJhc zBBN2xzVlc4RmFvY3ZpamhlM282TzQrY25LR1p4ZVhmWjlxa1dZTjZoZEPOU3BJbUVtemMKS2d3Zkd1QW5QNjd LZG5acGFKOG5UaXE3NEkyZFk1T1c1eHp3V21LUWUXY
zk4UjdLRWF5eVZsbks1cGJpcEtQdQpXclJmd1FSVGIXZ09ETGN6M050TnBJN0ZMNXdVs lp0V2QzNU1VRFM1Mlpqe lNoN2ZMY281Tud3SE1ZMD0KLS0tLS1FTkQgQ0VSVElGSUNBVEU
tLS0tLQo="
    },
    "roleArn": "arn:aws:iam::442073319574:role/eksServiceRole",
    "resourcesVpcConfig": {
      "subnetIds": [
        "subnet-02b3ec0b0707bc72d",
        "subnet-068b7e05f051c7a81",
        "subnet-036b4441d7d84bedd",
        "subnet-0041a973268162bf8"
      ],
      "vpcId": "vpc-0757dcdf8b23f268",
      "securityGroupIds": [
        "sg-02bf871985a56d108"
      ]
    }
  },
  "version": "1.10",
  "arn": "arn:aws:eks:us-east-1:442073319574:cluster/innovate2018",
  "createdAt": 1534489272.188
}
```

为新创建的 Amazon EKS 集群配置 Kubectl

- 创建 Kubeconfig 文件
- 将该文件保存到 `~/.kube/config-<cluster-name>`
- 将该文件路径添加到 KUBECONFIG 环境变量
 - `export KUBECONFIG=$KUBECONFIG:~/.kube/config-<cluster-name>`
 - `echo 'export KUBECONFIG=$KUBECONFIG:~/.kube/config-<cluster-name>' >> ~/.bash_profile`

启动和配置 Amazon EKS 的 Worker Nodes

通过 Amazon CloudFormation 模板创建 Worker Nodes

<https://amazon-eks.s3-us-west-2.amazonaws.com/1.10.3/2018-06-05/amazon-eks-nodegroup.yaml>

Create stack

Select Template

Specify Details

Options

Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name innovate2018-worker-nodes

Parameters

EKS Cluster

ClusterName innovate2018

The cluster name provided when the cluster was created. If it is incorrect, nodes will not be able to join the cluster.

ClusterControlPlaneSecurityGroup ekscluster-control-plane (sg-02bf87198...)

The security group of the cluster control plane.

Worker Node Configuration

NodeGroupName innovate2018-worker-nodes

Unique identifier for the Node Group.

NodeAutoScalingGroupMinimumSize 1

Minimum size of Node Group ASG.

NodeAutoScalingGroupMaximumSize 3

Maximum size of Node Group ASG.

NodeInstanceType t2.medium

EC2 instance type for the node instances

NodeImageId ami-dea4d5a1

AMI id for the node instances.

KeyName kops_demo

The EC2 Key Pair to allow SSH access to the instances

```
kubectl get nodes
```

```
[186590d978e3:EKS zhouqiz$ kubectl get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
ip-10-0-0-116.ec2.internal	Ready	<none>	42s	v1.10.3
ip-10-0-3-203.ec2.internal	Ready	<none>	42s	v1.10.3
ip-10-0-3-85.ec2.internal	Ready	<none>	44s	v1.10.3

```
aws eks delete-cluster --name innovate2018
```

相关链接

快速开始使用 **Amazon EKS**

官网链接: <http://aws.amazon.com/eks>

Kubernetes Workshop

<https://github.com/aws-samples/aws-workshop-for-kubernetes>



INNOVATE CHINA 2018

在线技术大会



感谢参加 AWS INNOVATE 2018 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：



微信公众号：AWSChina



新浪微博：<https://www.weibo.com/amazonaws/>



领英：<https://www.linkedin.com/company/aws-china/>



知乎：<https://www.zhihu.com/org/aws-54/activities/>



视频中心：<http://aws.amazon.bokecc.com/>



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