

INTRODUCTION

EXPLORING EKS

DEVELOPING FOR
EKS

EKS IN
PRODUCTION

APPLYING BEST
PRACTICES

APPENDIX

THE WEEKS MANIFEST

INTERACTIVE SUPPLEMENT
FOR THE
AMAZON EKS DEEP DIVE
COURSE

MARK RICHMAN, TRAINING ARCHITECT

Course Introduction

This Amazon EKS Deep Dive course has been developed to provide you with the requisite knowledge to not only understand the concepts behind the EKS architecture and operations, but also gain the hands-on experience required to become confident and competent working in a real-world environment.

From the Author

Dear Students and Fellow Cloud Professionals,

It is my pleasure to bring you this course for the Amazon Elastic Container Service for Kubernetes, or EKS! I want you to know I have had a lot of fun putting this course together. Preparing for this course and hands-on learning activities were exciting for me because the content is based on real-world scenarios. We are not just throwing a lot of theory and terminology around. This course covers significant concepts around daily EKS usage and should provide you plenty to think about regarding your own organizations and applications.

I am happy and excited you have decided to take this journey in learning with us! As always, feel free to post in the community on Linux Academy if you need any help or have any concerns, and we will be there to help. Also, there are rating features on all the content in this course. I would appreciate it if you would help me by providing feedback.

So if you are ready to go...Let's get started!

Regards,
Mark Richman



INTRODUCTION

EXPLORING EKS

DEVELOPING FOR EKS

EKS IN PRODUCTION

APPLYING BEST PRACTICES

APPENDIX



Linux Academy

Exploring EKS

This topic will provide a high-level explanation over the fundamentals of how Amazon EKS works.

Concepts covered in this topic include:

- What is EKS?
- Managed Control Plane
- Kubernetes & VPC Networking
- AWS CNI Network Plugin
- EKS-optimized AMI
- Spot Instances

[Continue to Lesson 1...](#)

1 2 3 4



What is EKS?

- Managed Kubernetes service
- Runs upstream K8s - not an AWS fork
- Use kubectl and friends
- ECS is cheaper than EKS for small/simple deployments
- EKS is loosely integrated with other AWS services, but this is changing rapidly
- K8s is more popular than ECS or Elastic Beanstalk
- K8s runs on all major cloud providers, and on-premises
- ~60% of K8s deployments run on AWS!
- EKS is secure by default

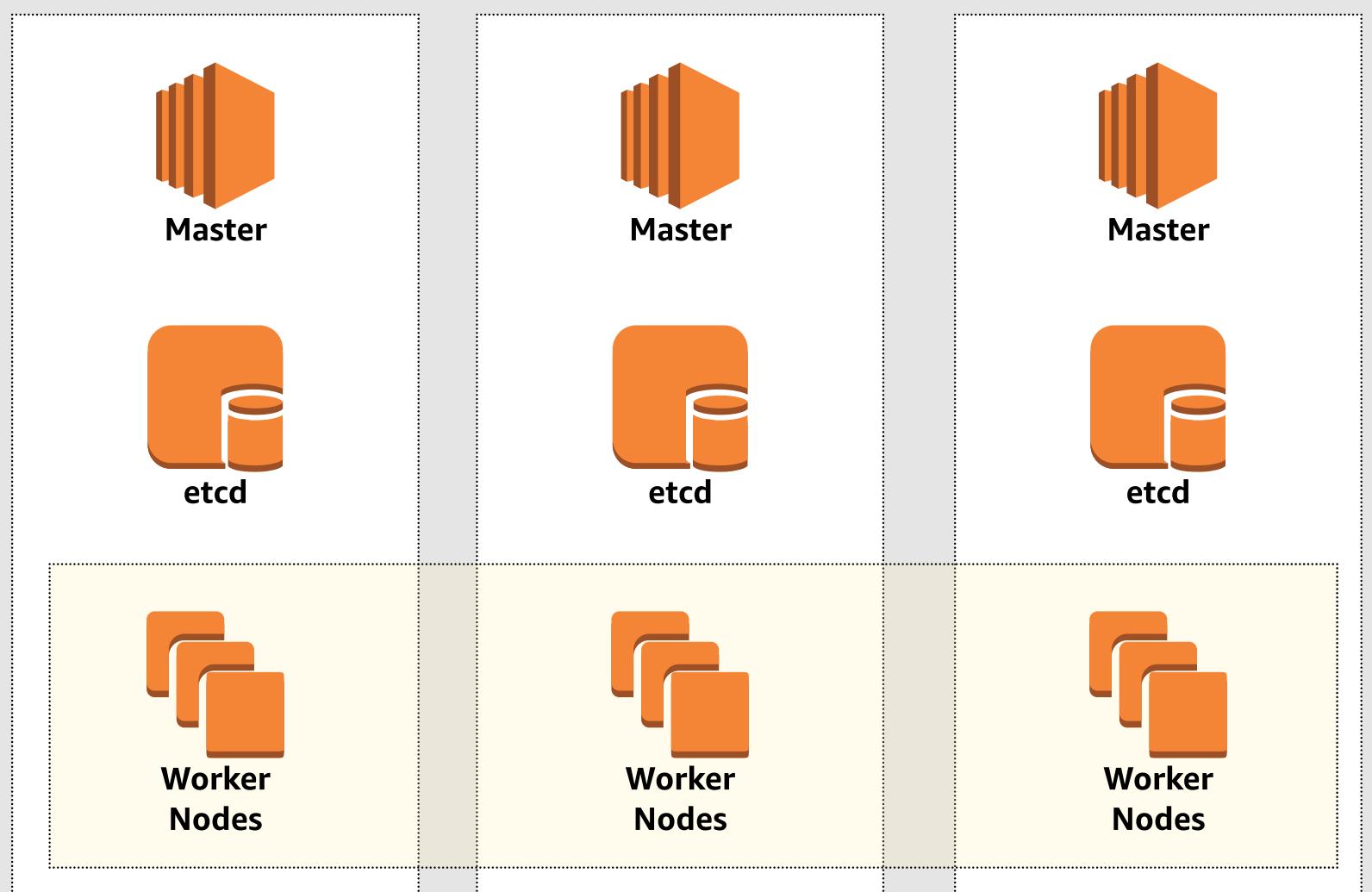


Amazon EKS

1 2 3 4



Managed Control Plane



Availability Zone 1

Availability Zone 2

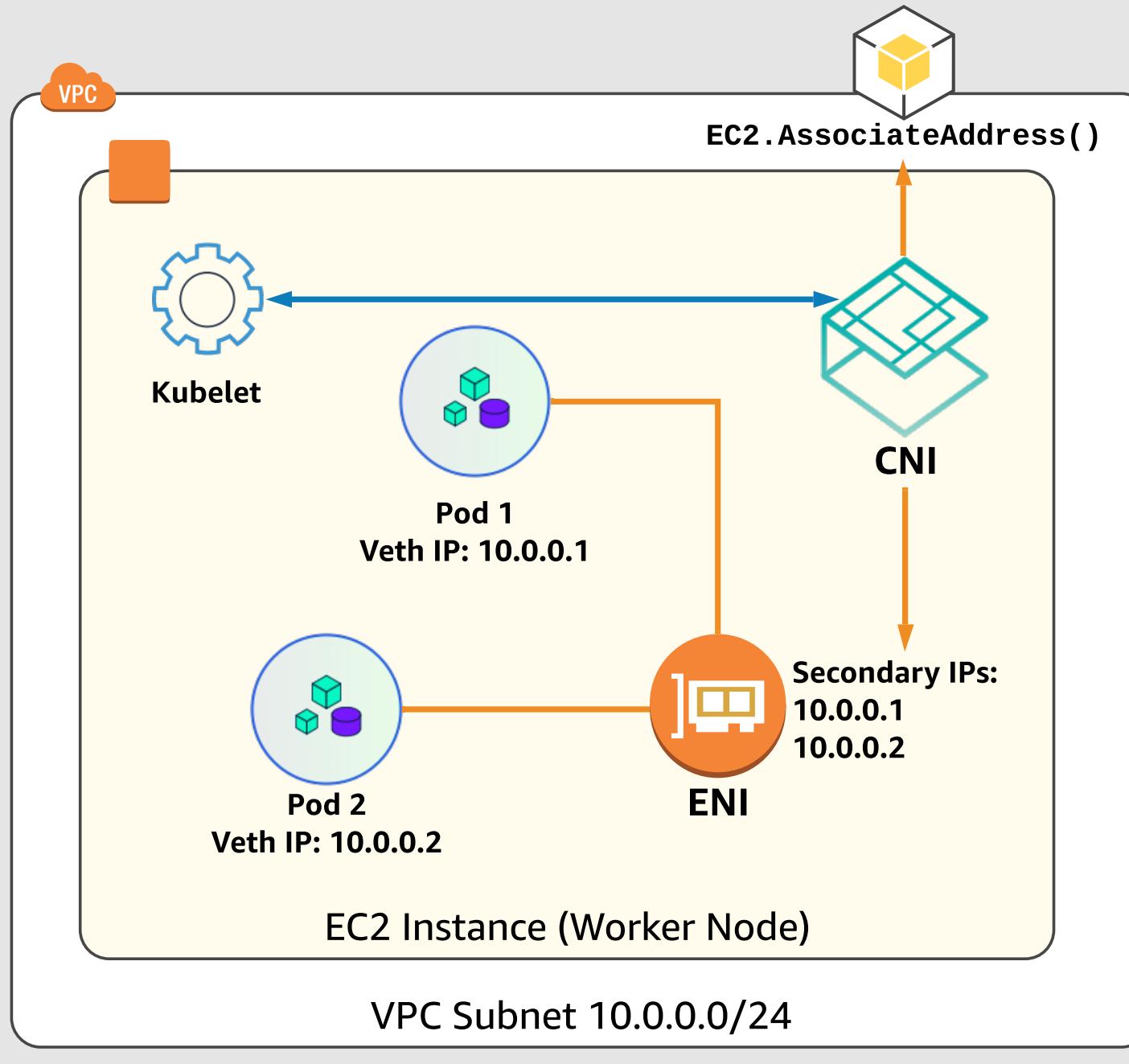
Availability Zone 3

- EKS provides K8s master nodes, API servers, etcd layer
- 3 master and 3 etcd nodes by default
- Backups, etcd snapshots, autoscaling included
- You provision and manage the EC2 worker nodes
- Unlike kops, you don't roll your own master (<https://github.com/kubernetes/kops>)
- Masters and etcd are Multi-AZ
- EKS scales master nodes for you

1 2 3 4



Kubernetes and VPC Networking



1 2 3 4



EKS-Optimized AMI

- AWS-supplied AMI based on Amazon Linux 2
- Preconfigured with Docker, kubelet, AWS IAM Authenticator
- EC2 User Data bootstrap script
- Allows automatic joining to EKS cluster
- Built using Packer

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

Region	Amazon EKS-optimized AMI	with GPU support
US West (Oregon) (us-west-2)	ami-0f54a2f7d2e9c88b3	ami-08156e8fd65879a13
US East (N. Virginia) (us-east-1)	ami-0a0b913ef3249b655	ami-0c974dde3f6d691a1
US East (Ohio) (us-east-2)	ami-0958a76db2d150238	ami-089849e811ace242f
EU (Ireland) (eu-west-1)	ami-00c3b2d35bdd4f5c	ami-0c3479bcd739094f0

AWS Marketplace
Subscription Required



1 2 3 4



Spot Instances

- Use AWS's unused capacity at up to 90% discount
- Less expensive than on-demand or reserved instances
- Spot price is determined by supply and demand
- Spot instances can be terminated with little notice
- Use as EKS worker nodes for a cheap boost in capacity
- Develop applications to be flexible and fault-tolerant
- Spot Fleet can help diversify instances

```
1 NodeLaunchConfig:
2   Type: AWS :: AutoScaling :: LaunchConfiguration
3   Properties:
4     SpotPrice: "1.50" ← Bid Price
5     Foo: Bar
6     UserData:
7       Fn :: Base64:
8         !Sub |
9           #!/bin/bash
10          set -o xtrace
11          /etc/eks/bootstrap.sh ${ClusterName} ${BootstrapArguments}
12          /opt/aws/bin/cfn-signal --exit-code $? \
13            --stack ${AWS :: StackName} \
14            --resource NodeGroup \
15            --region ${AWS :: Region}
```



Linux Academy

Exploring EKS - Lesson 2

Creating the EKS Cluster

Concepts covered in this topic include:

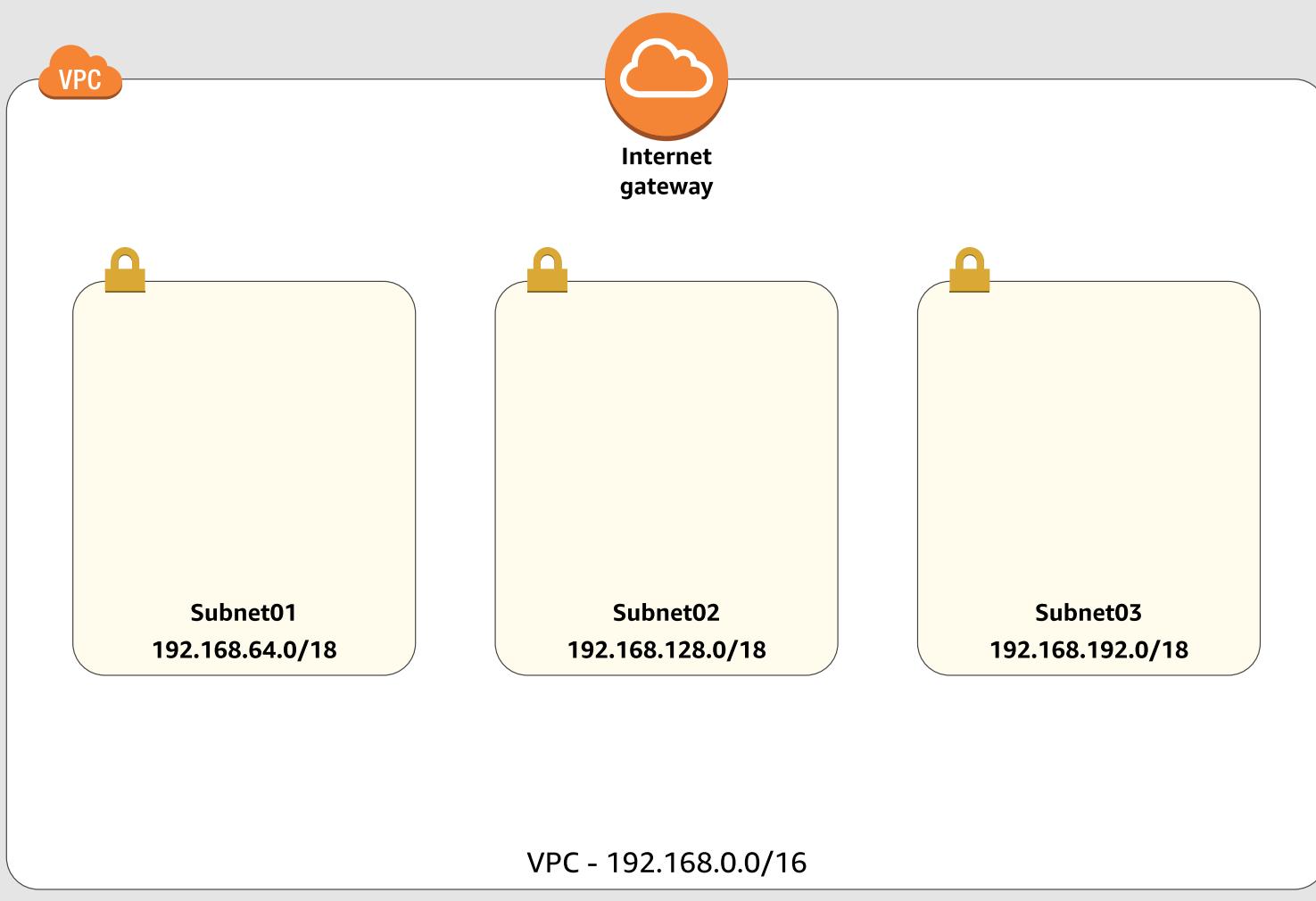
- Creating the EKS service role
- Creating the VPC infrastructure using CloudFormation
- Creating a cluster in the AWS Management Console
- Configuring kubectl for EKS
- Configuring aws-iam-authenticator

[Continue to Lesson 2...](#)

1 2 3 4



EKS Cluster VPC Configuration



CloudFormation Template:

<https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2018-11-07/amazon-eks-vpc-sample.yaml>

Note the following outputs:

VpcId, SubnetIds, SecurityGroups

Amazon-vended kubectl:

<https://amazon-eks.s3-us-west-2.amazonaws.com/1.10.3/2018-07-26/bin/linux/amd64/kubectl>

1 2 3 4



Install kubectl:

```
mkdir $HOME/bin  
  
curl -o kubectl  
https://amazon-eks.s3-us-west-2.amazonaws.com/\  
1.10.3/2018-07-26/bin/linux/amd64/kubectl  
  
chmod +x ./kubectl  
  
cp ./kubectl $HOME/bin/kubectl  
  
export PATH=$HOME/bin:$PATH  
  
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc  
  
kubectl version --client
```

1 2 3 4



Install aws-iam-authenticator:

```
mkdir $HOME/bin

curl -o aws-iam-authenticator
https://amazon-eks.s3-us-west-2.amazonaws.com/\
1.10.3/2018-07-26/bin/linux/amd64/\
aws-iam-authenticator
aws-iam-authenticator or darwin or windows
chmod +x ./aws-iam-authenticator
cp ./aws-iam-authenticator $HOME/bin
export PATH=$HOME/bin:$PATH
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc
aws-iam-authenticator help
```

Configure kubectl for EKS:

```
curl -O https://bootstrap.pypa.io/get-pip.py
python get-pip.py --user
pip install awscli --upgrade --user
export PATH=$HOME/.local/bin:$PATH
echo 'export PATH=$HOME/.local/bin:$PATH' >>
~/.bashrc

aws eks update-kubeconfig --name <cluster name>
kubectl config view
kubectl get svc
```



Linux Academy

Exploring EKS - Lesson 3

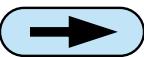
Provisioning Worker Nodes

Concepts covered in this topic include:

- Launching EKS worker nodes
- Deploying the Kubernetes dashboard

[Continue to Lesson 3...](#)

1 2 3 4



Launch Worker Nodes:

CloudFormation Template:

<https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2018-11-07/amazon-eks-nodegroup.yaml>

Region	Amazon EKS-optimized AMI
US West (Oregon) (us-west-2)	ami-0f54a2f7d2e9c88b3
US East (N. Virginia) (us-east-1)	ami-0a0b913ef3249b655
US East (Ohio) (us-east-2)	ami-0958a76db2d150238
EU (Ireland) (eu-west-1)	ami-00c3b2d35bdd4f5c

Latest AMI List:

<https://docs.aws.amazon.com/eks/latest/userguide/eks-optimized-ami.html>

```
curl -O  
https://amazon-eks.s3-us-west-2.amazonaws.com/\cloudformation/2018-11-07/aws-auth-cm.yaml
```

```
# Edit aws-auth-cm.yaml, set Node Instance Role ARN  
kubectl apply -f aws-auth-cm.yaml  
kubectl get nodes --watch
```

1 2 3 4



Deploy the Kubernetes Dashboard:

```
kubectl apply -f  
https://raw.githubusercontent.com/kubernetes/  
dashboard/v1.10.1/src/deploy/recommended/  
kubernetes-dashboard.yaml  
  
kubectl proxy &
```

Deploy Heapster and InfluxDB:

```
kubectl apply -f  
https://raw.githubusercontent.com/kubernetes/  
heapster/master/deploy/kube-config/influxdb/  
heapster.yaml  
  
kubectl apply -f  
https://raw.githubusercontent.com/kubernetes/  
heapster/master/deploy/kube-config/influxdb/  
influxdb.yaml  
  
kubectl apply -f  
https://raw.githubusercontent.com/kubernetes/  
heapster/master/deploy/kube-config/rbac/  
heapster-rbac.yaml
```

[https://github.com/linuxacademy/eks-deep-dive-2019/
tree/master/1-3-Provisioning-Worker-Nodes](https://github.com/linuxacademy/eks-deep-dive-2019/tree/master/1-3-Provisioning-Worker-Nodes)



Linux Academy

Exploring EKS - Lesson 4

IAM Authentication

Concepts covered in this topic include:

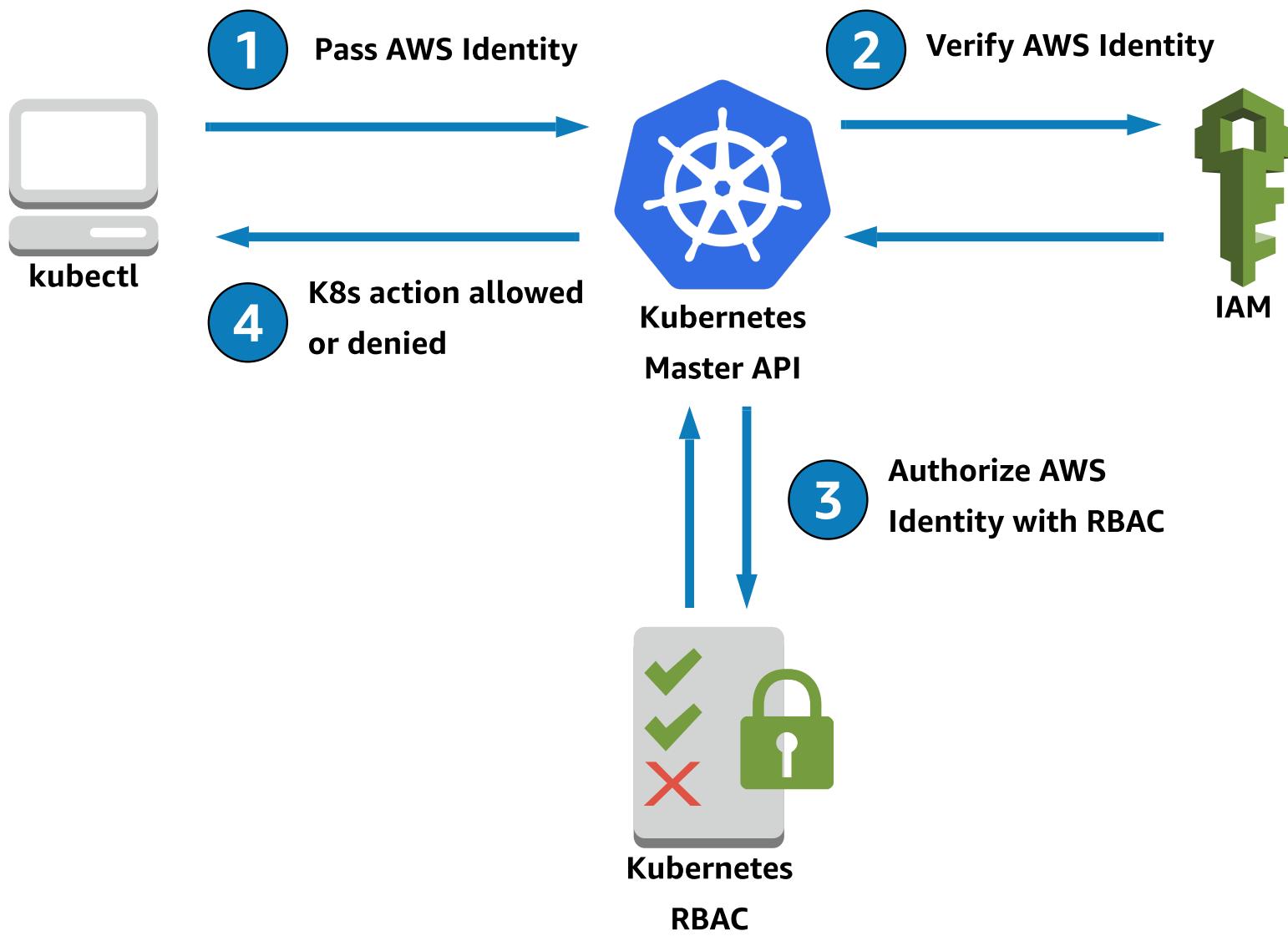
- How EKS authentication and authorization works
- Granting IAM users access to the EKS cluster

[Continue to Lesson 4...](#)

1 2 3 4



User Authentication and Authorization



AWS IAM Authenticator:

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

Granting an IAM User Access

Edit AWS Auth Config Map:

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

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: <node instance role ARN>
      username: system:node:{EC2PrivateDNSName}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam:123456789012:user/Alice
      username: alice
      groups:
        - system:masters
kind: ConfigMap
metadata: ...
```



Linux Academy

Understanding the Application Architecture

This lecture explains provides an overview of the sample application used in this section of the course.

Concepts Covered in this Topic include:

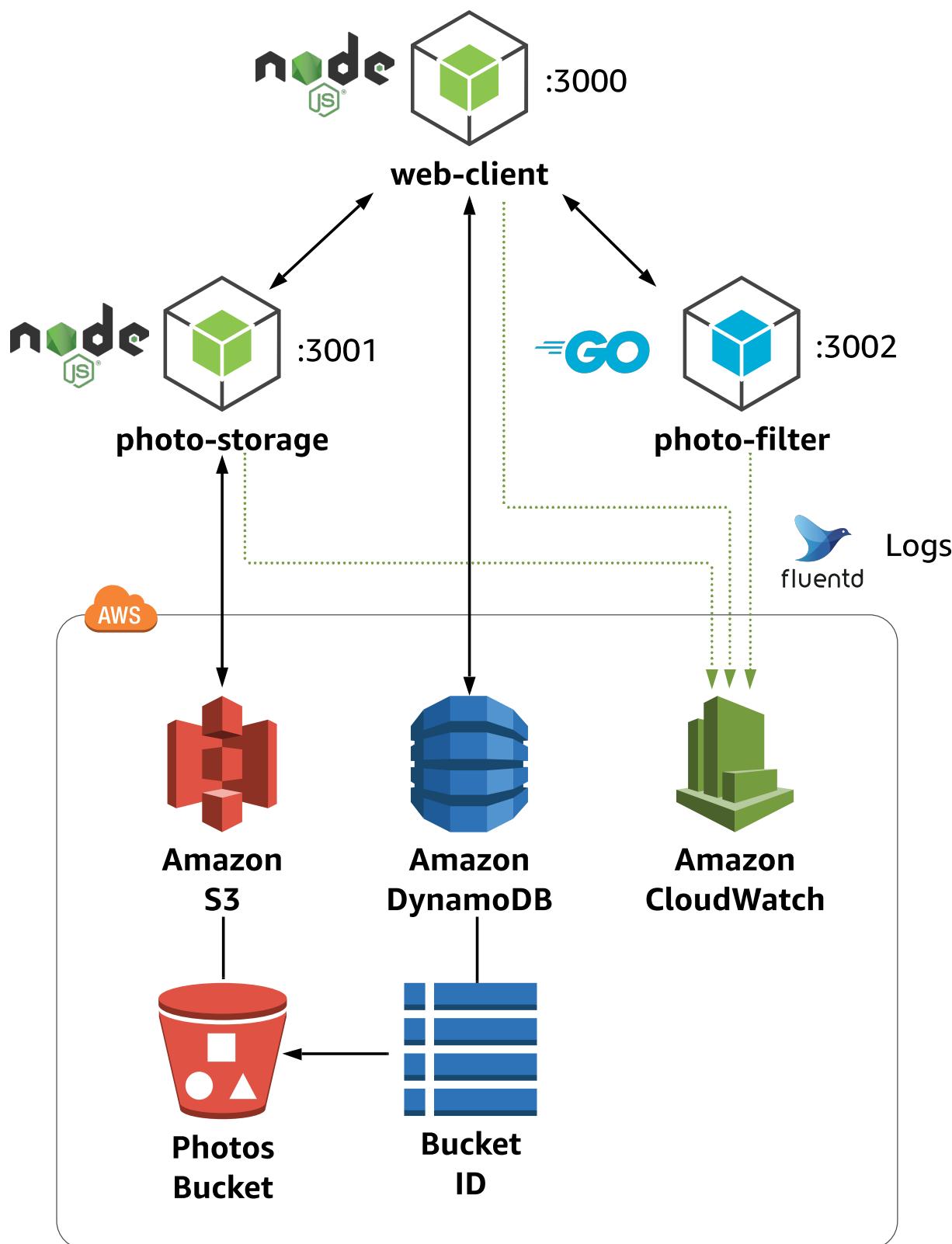
- 1) Sample application demo
- 2) Architecture
- 3) S3 and DynamoDB Integration

[Continue to Lesson 1...](#)

1 2 3 4

Sample Application: picture-upload

<https://github.com/linuxacademy/eks-deep-dive-2019/tree/master/picture-upload>





Linux Academy

Building from Source

This lecture walks through building the sample application from source code.

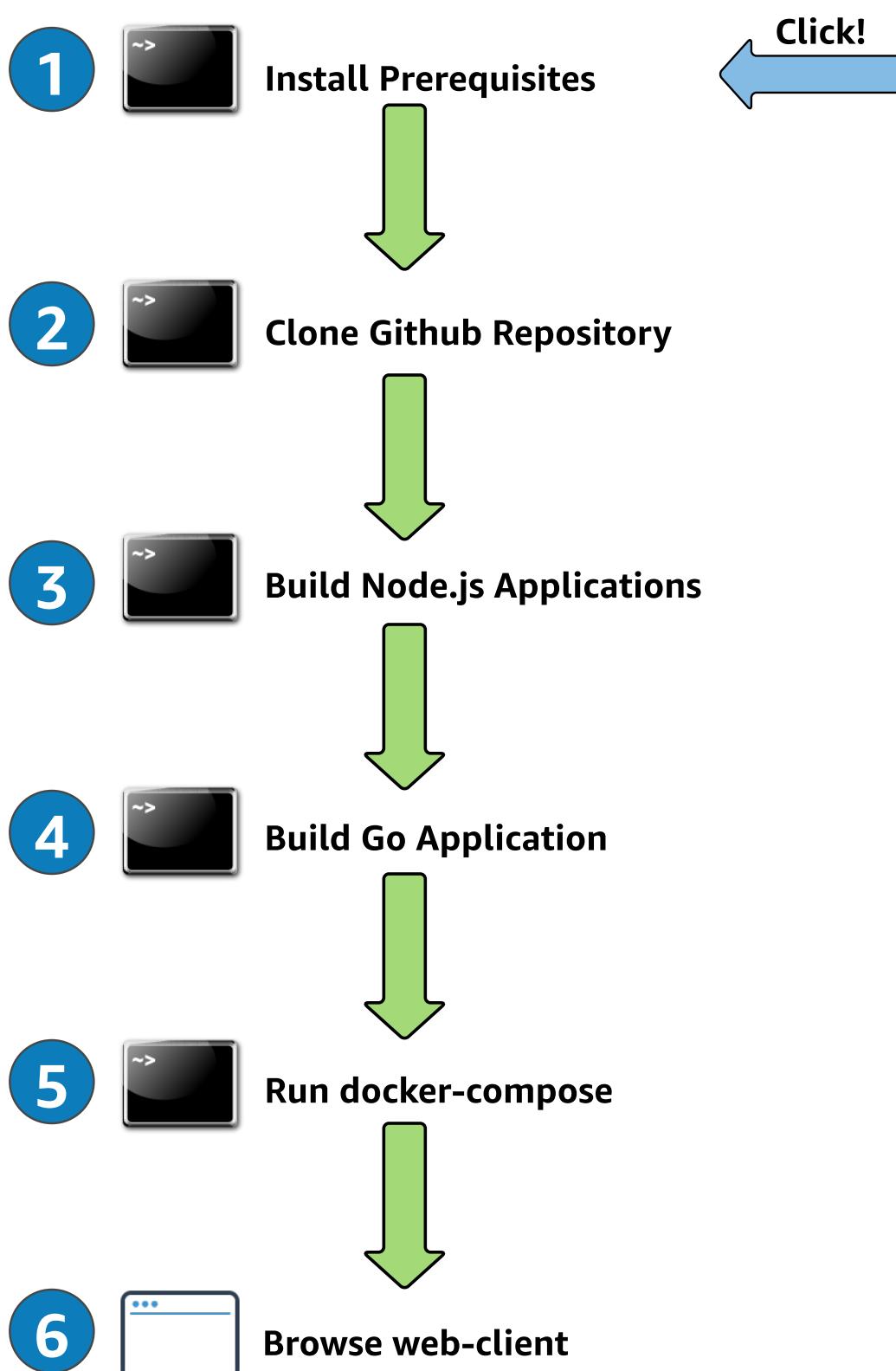
Concepts Covered in this Topic include:

- 1) Installing prerequisites
- 2) Cloning Github repository
- 3) Building the application

[Continue to Lesson 2...](#)

1 2 3 4

Building from Source



1 2 3 4

Install Prerequisites



1. Update all packages
2. Install Docker & Git
3. Install Developer Tools
4. Start Docker service
5. Install docker-compose
6. Install nvm and Node.js
7. Install Go
8. Add \$USER to docker group

THE EKS MANIFEST

1 2 3 4

Build Node.js Applications



1. cd picture-upload
2. make install

THE EKS MANIFEST

1 2 3 4

Build Go Application



1. cd picture-upload/apps/photo-filter
2. go build

1 2 3 4

Run docker-compose



1. Edit docker-compose.yml
2. For web-client and photo-storage:
 - a. Set AWS_ACCESS_KEY_ID
 - b. Set AWS_REGION
 - c. Set AWS_SECRET_ACCESS_KEY
3. Run docker-compose up

THE EKS MANIFEST

1 2 3 4

Browse web-client



1. Find Public IP of EC2 Instance
2. Browse <http://<public IP>:3000>



Linux Academy

Publishing to ECR

This lecture details how ECR is integrated with EKS, simplifying the development to production workflow.

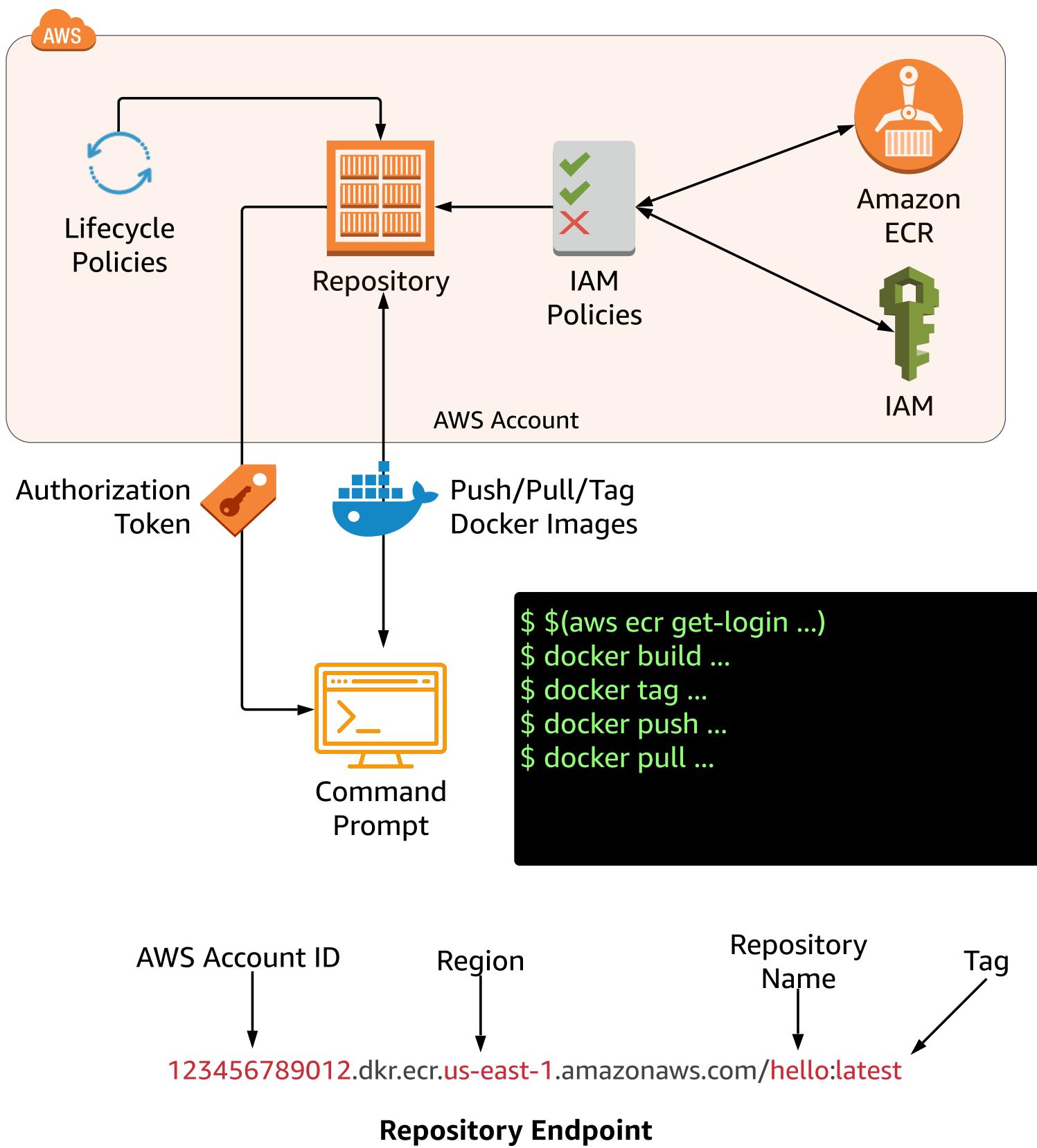
Concepts Covered in this Topic include:

- 1) ECR Components
- 2) Authenticating to ECR
- 3) Creating ECR Repositories
- 4) Tagging and Pushing Images to ECR

[Continue to Lesson 3...](#)

1 2 3 4

ECR Components





Linux Academy

Deploying to EKS

This lecture walks through deploying the sample application to an EKS cluster.

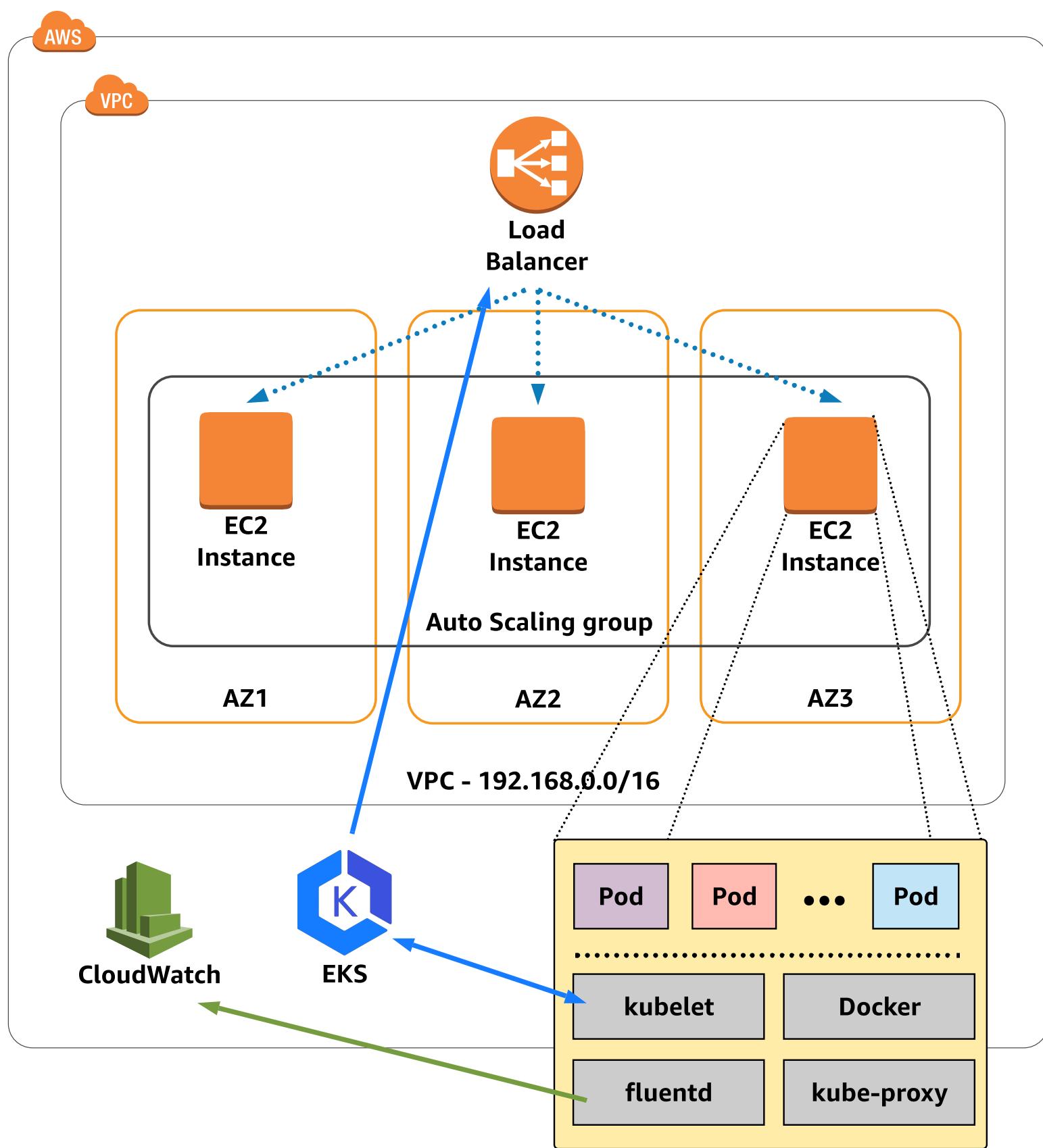
Concepts Covered in this Topic include:

- 1) Cluster Architecture
- 2) Deploying Services
- 3) ELB Integration
- 4) Scaling Up & Down
- 5) Undeploying Services

[Continue to Lesson 4...](#)

1 2 3 4

EKS Cluster Infrastructure





Linux Academy

Autoscaling an EKS Cluster

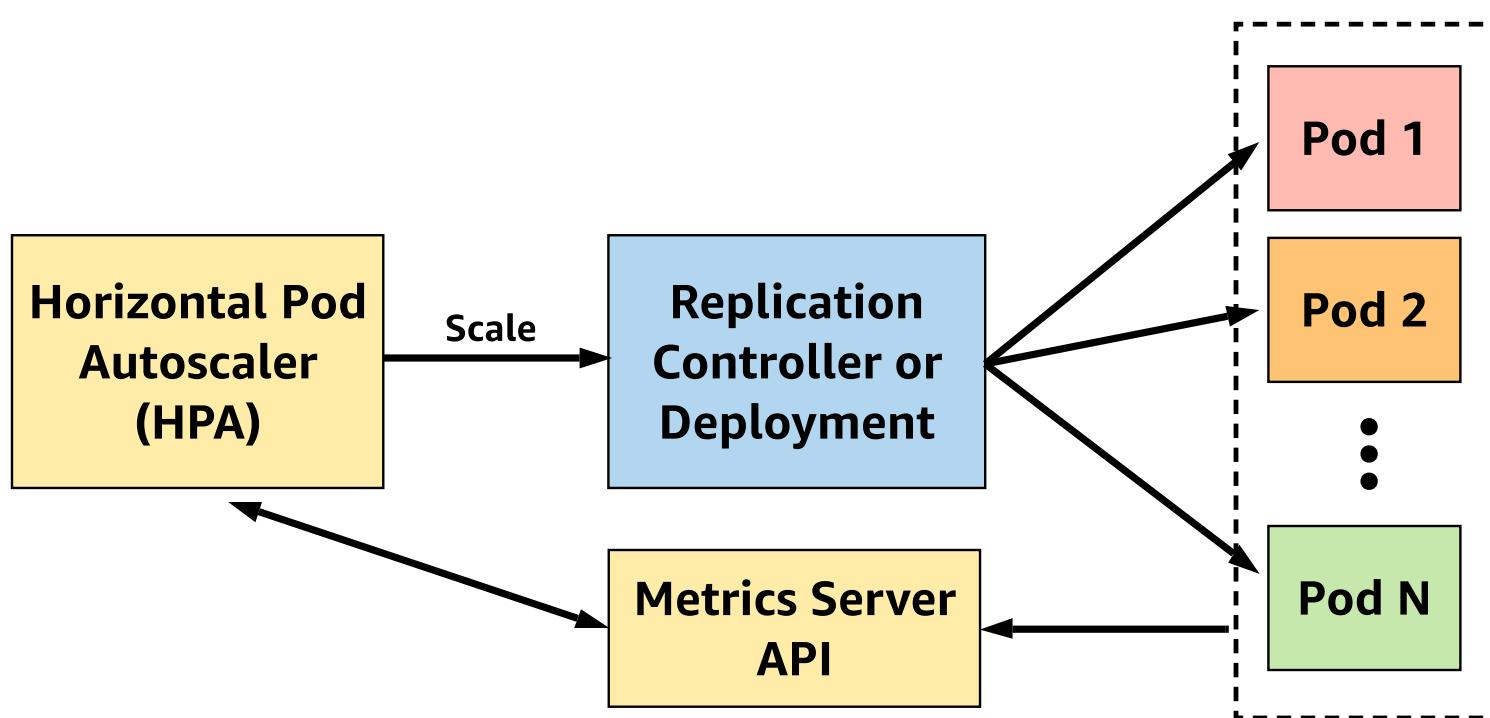
This lecture details two mechanisms for autoscaling in EKS.

Concepts Covered in this Topic include:

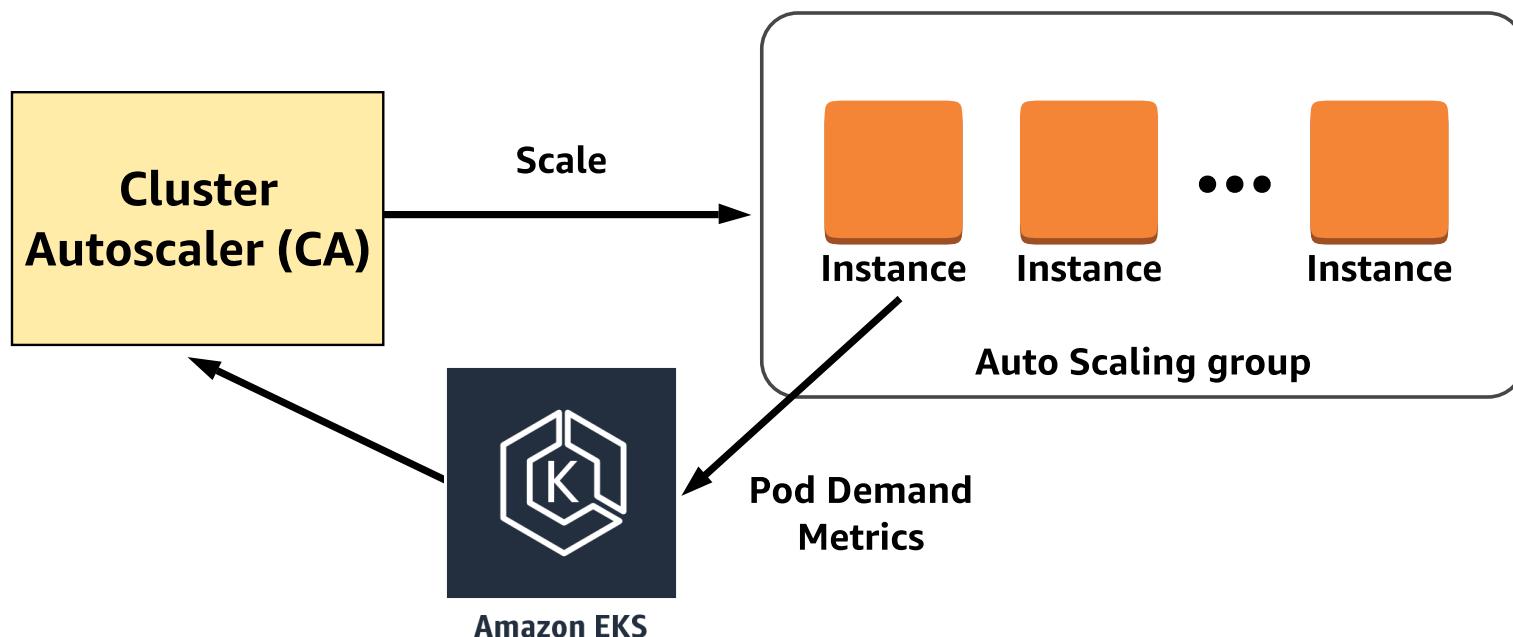
- 1) Horizontal Pod Autoscaler (HPA)
- 2) Cluster Autoscaler (CA)

[Continue to Lesson 1...](#)

Horizontal Pod Autoscaler (HPA)



Cluster Autoscaler (CA)





Linux Academy

Monitoring an EKS Cluster

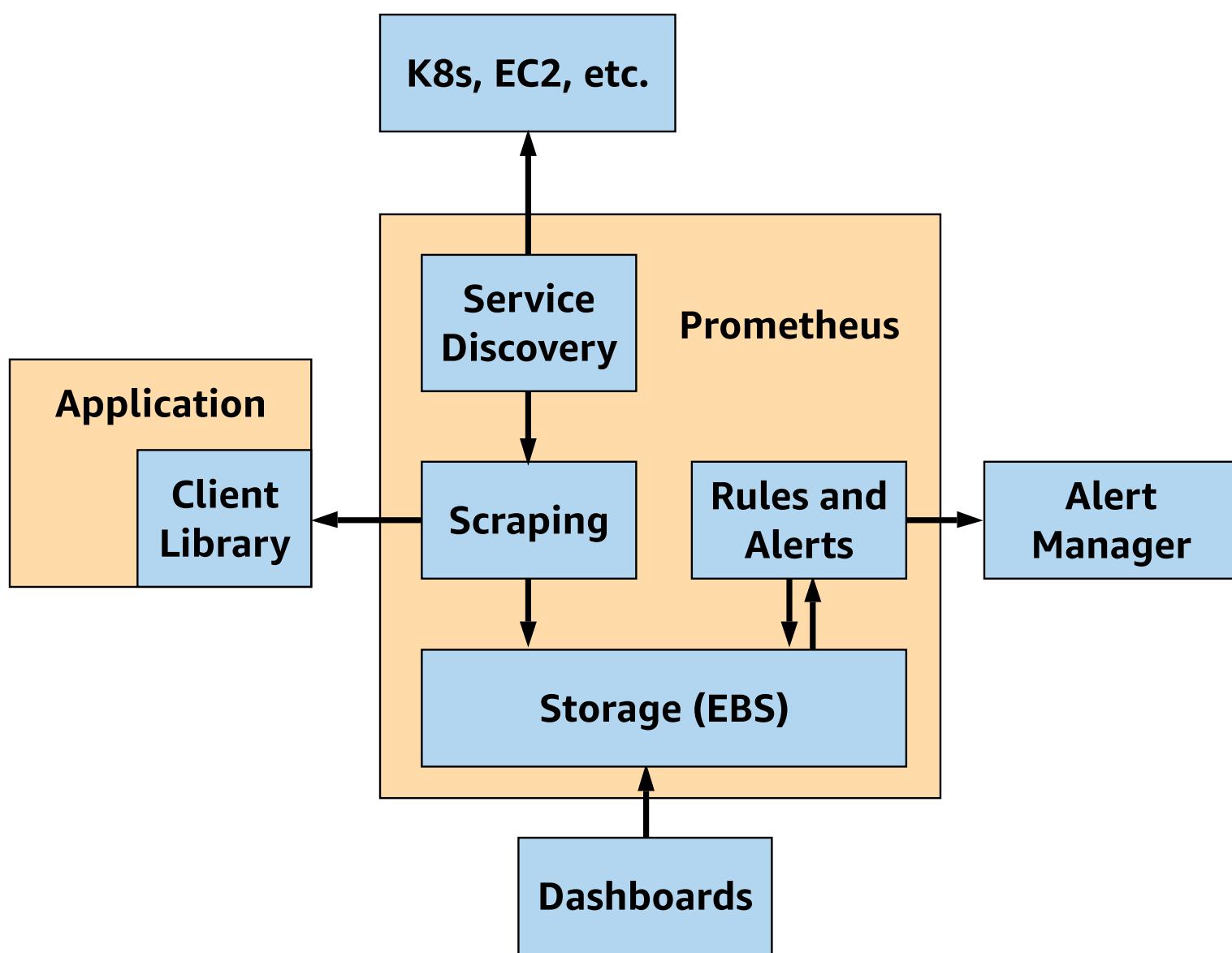
This lesson demonstrates how to monitor our EKS cluster using Prometheus and Grafana.

Concepts covered in this video:

- CloudWatch Limitations
- Gathering Metrics with Prometheus
- Visualizing Data with Grafana

[Continue to Lesson 2...](#)

Prometheus Architecture





Linux Academy

Updating EKS in Production

This lesson explains how to update your production EKS cluster.

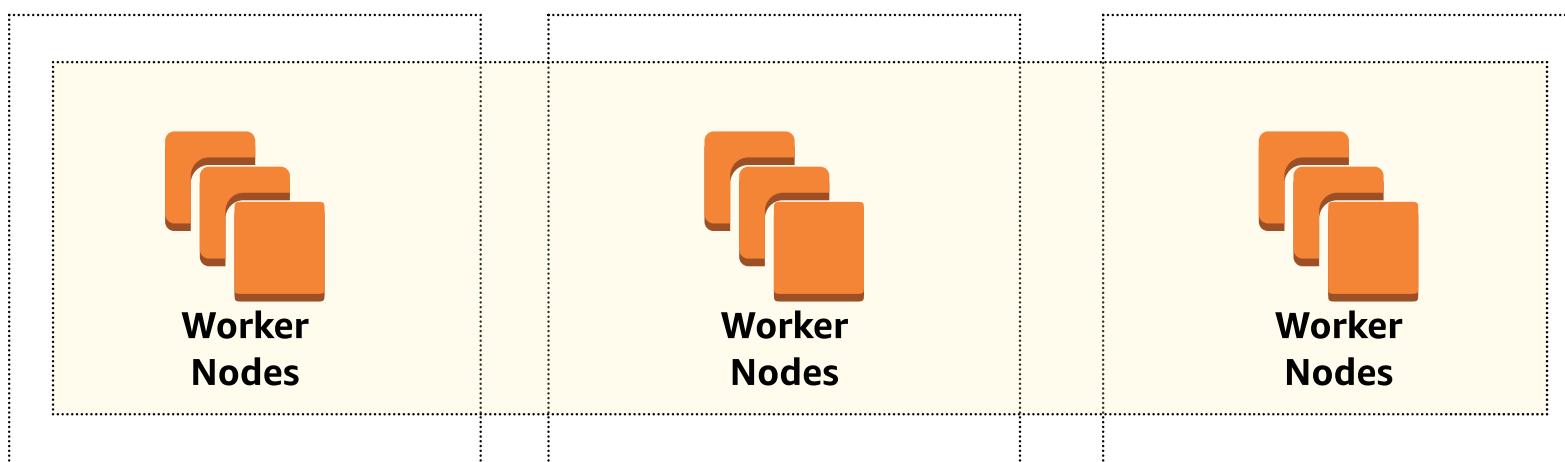
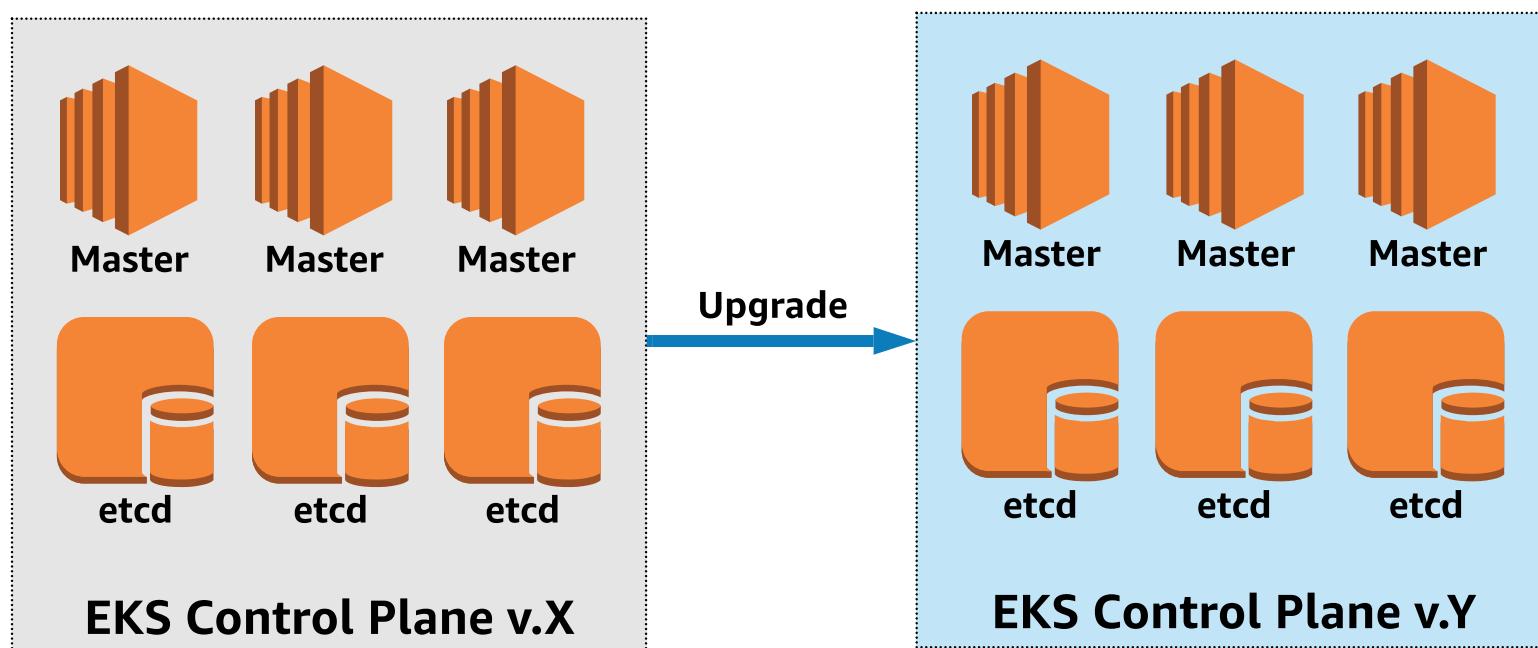
Concepts covered in this video:

- Updating the cluster version
- Switching from kube-dns to CoreDNS
- Updating the worker node group

[Continue to Lesson 3...](#)



Updating the Cluster Version



Availability Zone 1

Availability Zone 2

Availability Zone 3



Switching from kube-dns to CoreDNS



kube-dns

**Default
DNS in k8s
< 1.11**



CoreDNS

**Default
DNS in k8s
>= 1.11**

- 1 Patch kube-dns with new selector

```
spec:  
  selector:  
    matchLabels:  
      'eks.amazonaws.com/component': 'kube-dns'
```

- 2 Deploy CoreDNS

```
curl -o https://.../dns.yaml  
cat dns.yaml | sed ... | kubectl apply -f -
```

- 3 Scale kube-dns down to 0 replicas

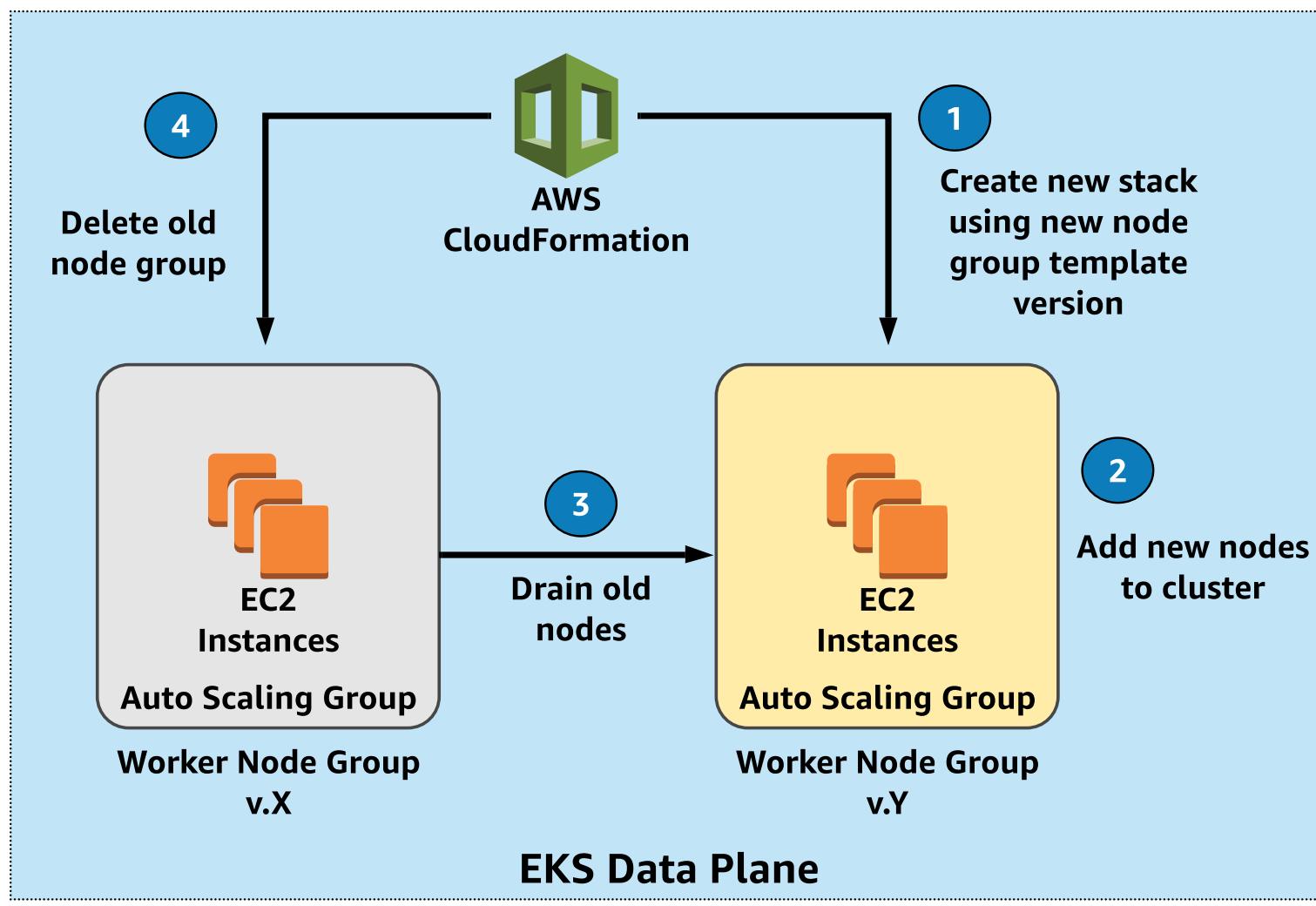
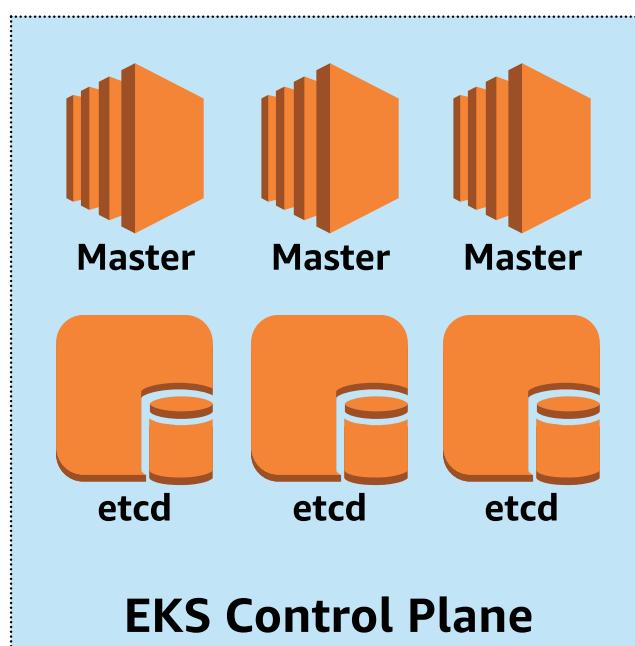
```
kubectl scale -n kube-system \  
  deployment/kube-dns --replicas=0
```

- 4 Delete kube-dns resources

```
kubectl delete -n kube-system \  
  deployment/kube-dns \  
  serviceaccount/kube-dns \  
  configmap/kube-dnsconfig
```



Updating the Worker Node Group





Linux Academy

Logging with CloudTrail

This lesson covers AWS CloudTrail and how to use it with EKS.

Concepts covered in this video:

- CloudTrail and its use cases
- Configuring CloudTrail
- Observing EKS events in CloudTrail logs

[Continue to Lesson 1...](#)



What is CloudTrail?

CloudTrail is the primary service we use for logging in AWS.

Important Features:

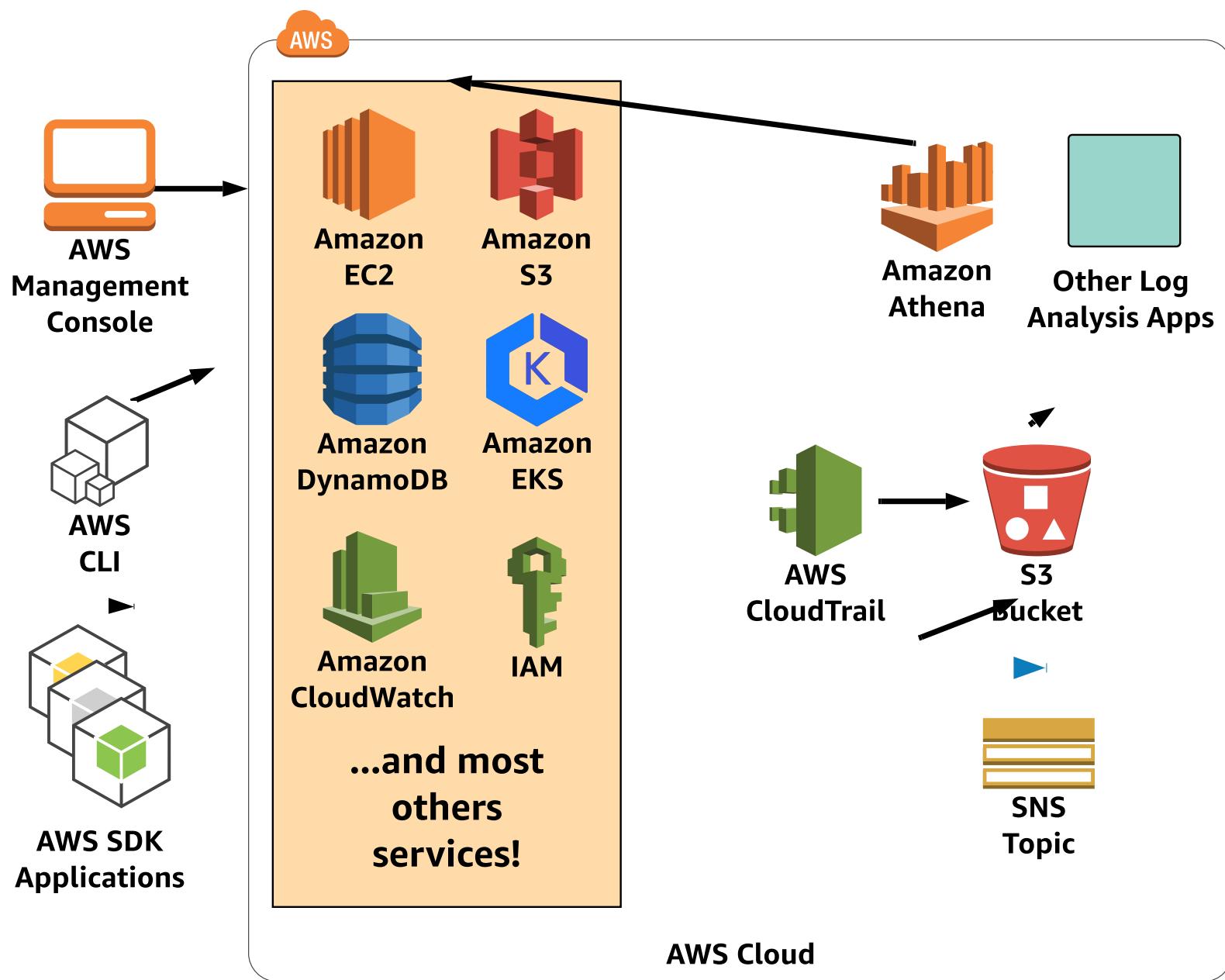
- It logs all the API calls in an AWS account (includes Console, CLI, API/SDK calls)
- Is enabled when your account is created
- Entries can be viewed using the **Event History** (past 90 days)
- **Trail**- a configuration allowing for logs to be sent to an S3 bucket:
 - Single region or multi-region trails can be configured
 - Trails can make multi-account logging possible, more on this later

Trails have several configuration options:

- **Management events**- enabling will log control plane events, such as:
 - User login events
 - Configuring Security
 - Setting up logging
- **Data Events**, which include:
 - Object-level events in S3
 - Function-level events in Lambda
- **Encryption** flexibility:
 - Encrypted in S3 server-side by default, can be changed to KMS
 - The logs can be sent to an **S3 bucket** of choice and even prefixed (folders)



CloudTrail Architecture





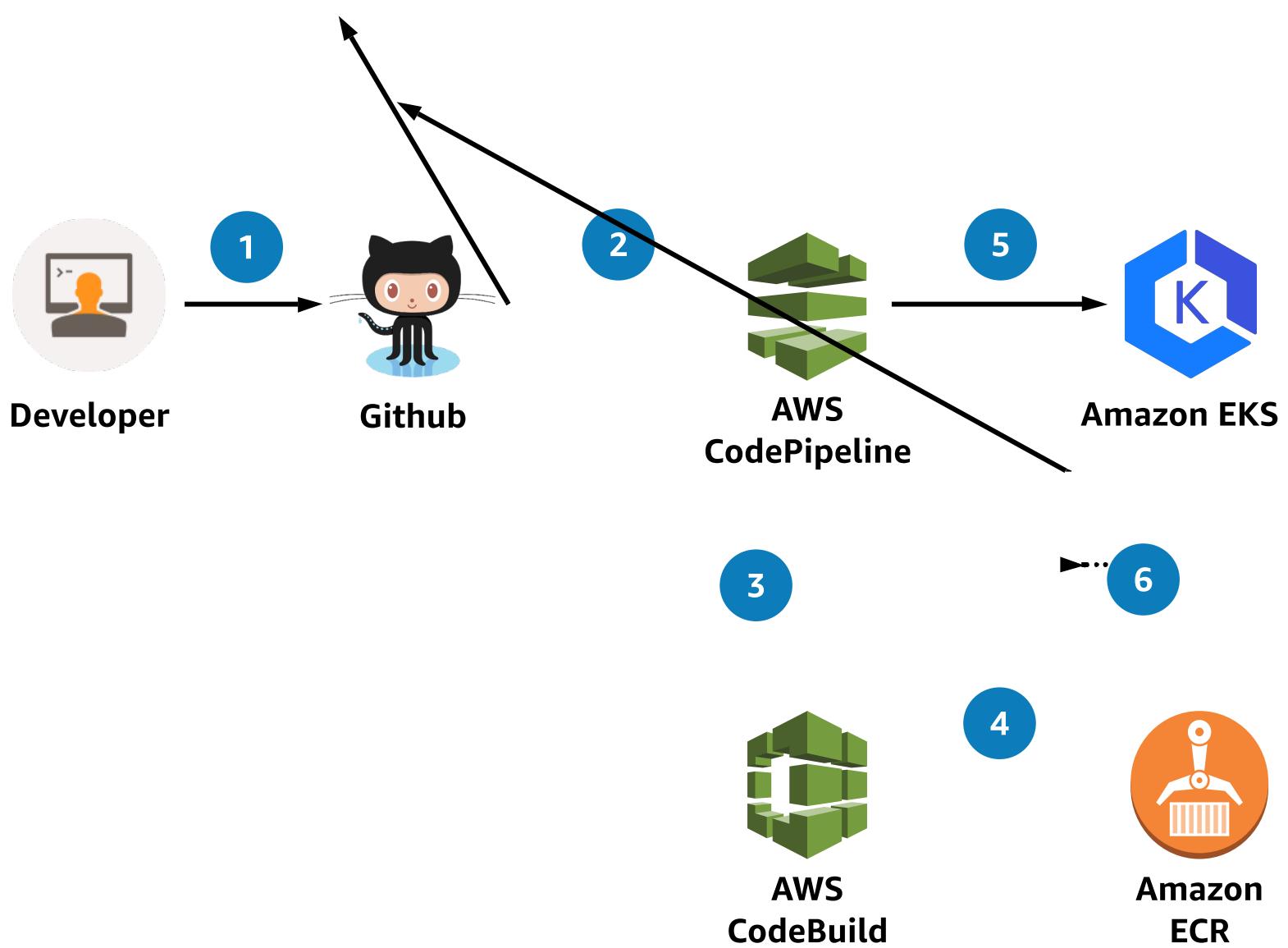
Linux Academy

Continuous Deployment with CodePipeline and EKS

This lesson demonstrates creating a Continuous Integration/Continuous Deployment (CI/CD) pipeline integrated with EKS.

[Continue to Lesson 2...](#)

CodePipeline





Linux Academy

Application Tracing with AWS X-Ray

- Deploy X-Ray agent in EKS
- Deploy sample microservices
- Examining Traces and Service Maps in X-Ray

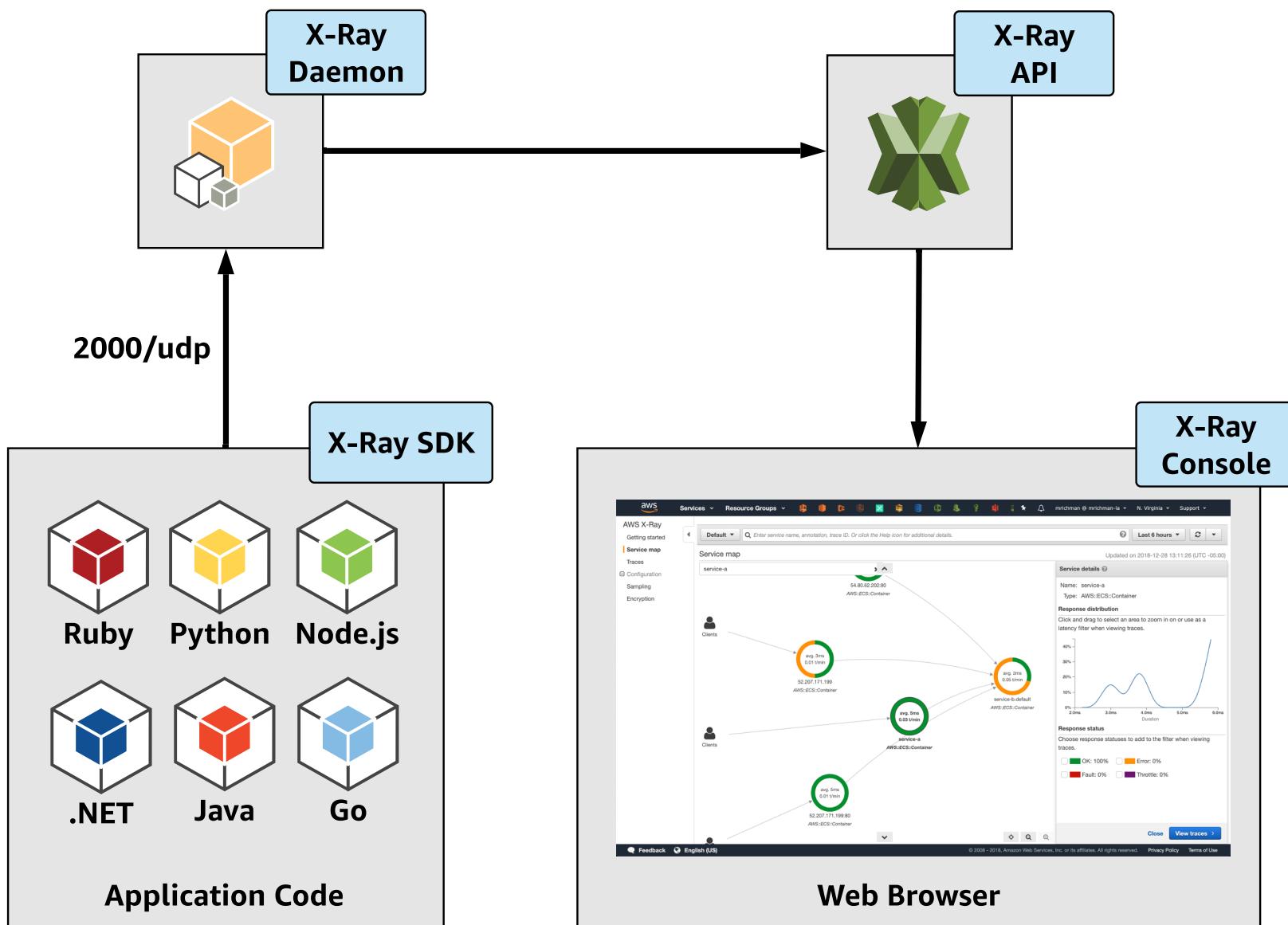
[Continue to Lesson 3...](#)

AWS X-Ray

X-Ray helps answer three critical questions about your application:



1. How is my application doing?
2. Why is my application performing the way it is?
3. Who is impacted by the issues?





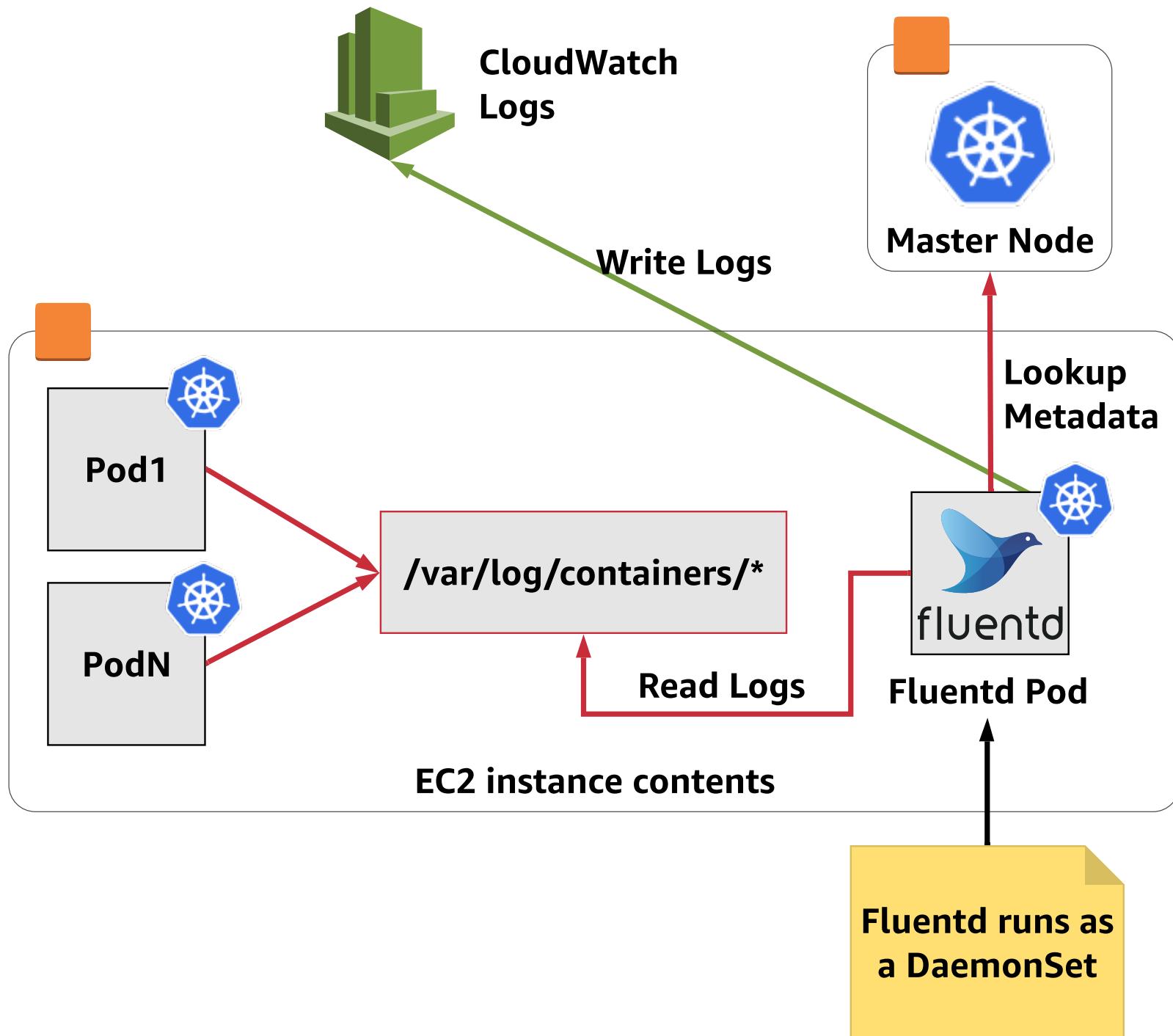
Linux Academy

Logging to CloudWatch with Fluentd

- Overview of Fluentd Architecture
- Deploying Fluentd to EKS

[Continue to Lesson 4...](#)

Fluentd Architecture



Appendix

This course's Github:

<https://github.com/linuxacademy/eks-deep-dive-2019>

eksctl (EKS CLI): <https://eksctl.io/>

Fluentd: <https://www.fluentd.org/>

Prometheus: <https://prometheus.io/>

Grafana: <https://grafana.com/>

Cluster Autoscaler:

<https://github.com/kubernetes/autoscaler/blob/master/cluster-autoscaler/cloudprovider/aws/README.md>



Mark Richman
mark@linuxacademy.com
[@mrichman](https://twitter.com/mrichman)