Docker clusters on AWS with Amazon ECS and Kubernetes

Julien Simon, Principal Technical Evangelist
@julsimon

aws

The problem

Given a certain amount of processing power and memory,

how can we best manage an arbitrary number of apps running in Docker containers?

http://tidalseven.com

aws

Docker on Amazon Web Services

Amazon EC2 Container Service (ECS)

- https://aws.amazon.com/ecs/
- Launched in 04/2015
- No additional charge

Amazon EC2 Container Registry (ECR)

- https://aws.amazon.com/ecr/
- Launched in 12/2015
- Free tier: 500MB / month for a year
- $0.10 / GB / month + outgoing traffic

ECS & ECR are available in 13 regions (US, EU, APAC, China)

aws

What's new?

October '17: per-second billing for EC2 and EBS

Oct 11	Introducing Lifecycle Policies for Amazon EC2 Container Registry
Oct 10	Amazon ECR Now Available in Asia Pacific (Seoul) Region
Oct 04	Amazon ECS Now Available in Asia Pacific (Seoul) Region
Sep 22	Amazon ECS Adds Support for Adding or Dropping Linux Capabilities to Containers
Sep 07	Amazon EC2 Container Service Now Integrated with Network Load Balancer to Support High-Throughput and Direct TCP Connections with Containers
Aug 10	Amazon ECS is now HIPAA Eligible
Jun 27	Amazon ECS RunTask and StartTask APIs now support additional override parameters
Jun 07	Amazon ECS Now Supports Time and Event-Based Task Scheduling
Jun 06	Amazon ECS Adds Console Support for Spot Fleet Creation

https://aws.amazon.com/ecs/new/

aws

Container Partners

https://aws.amazon.com/containers/partners/

aws

Selected ECS customers

Case studies and re:Invent videos: https://aws.amazon.com/ecs/

Case study: Coursera

https://www.youtube.com/watch?v=a45J6xAGUvA

Coursera deliver Massive Open Online Courses (14 million students, 1000+ courses). Their platform runs a large number of batch jobs, notably to grade programming assignments. Grading jobs need to run in near-real time while preventing execution of untrusted code inside the Coursera platform.

After trying out some other Docker solutions, Coursera have picked Amazon ECS and have even written their own scheduler.

"*Amazon ECS enabled Coursera to focus on releasing new software rather than spending time managing clusters*" - Frank Chen, Software Engineer

Case study: Segment

Segment.io

https://aws.amazon.com/fr/solutions/case-studies/segment/

Segment provides a service used by businesses to collect customer data for later use in analytics and marketing.

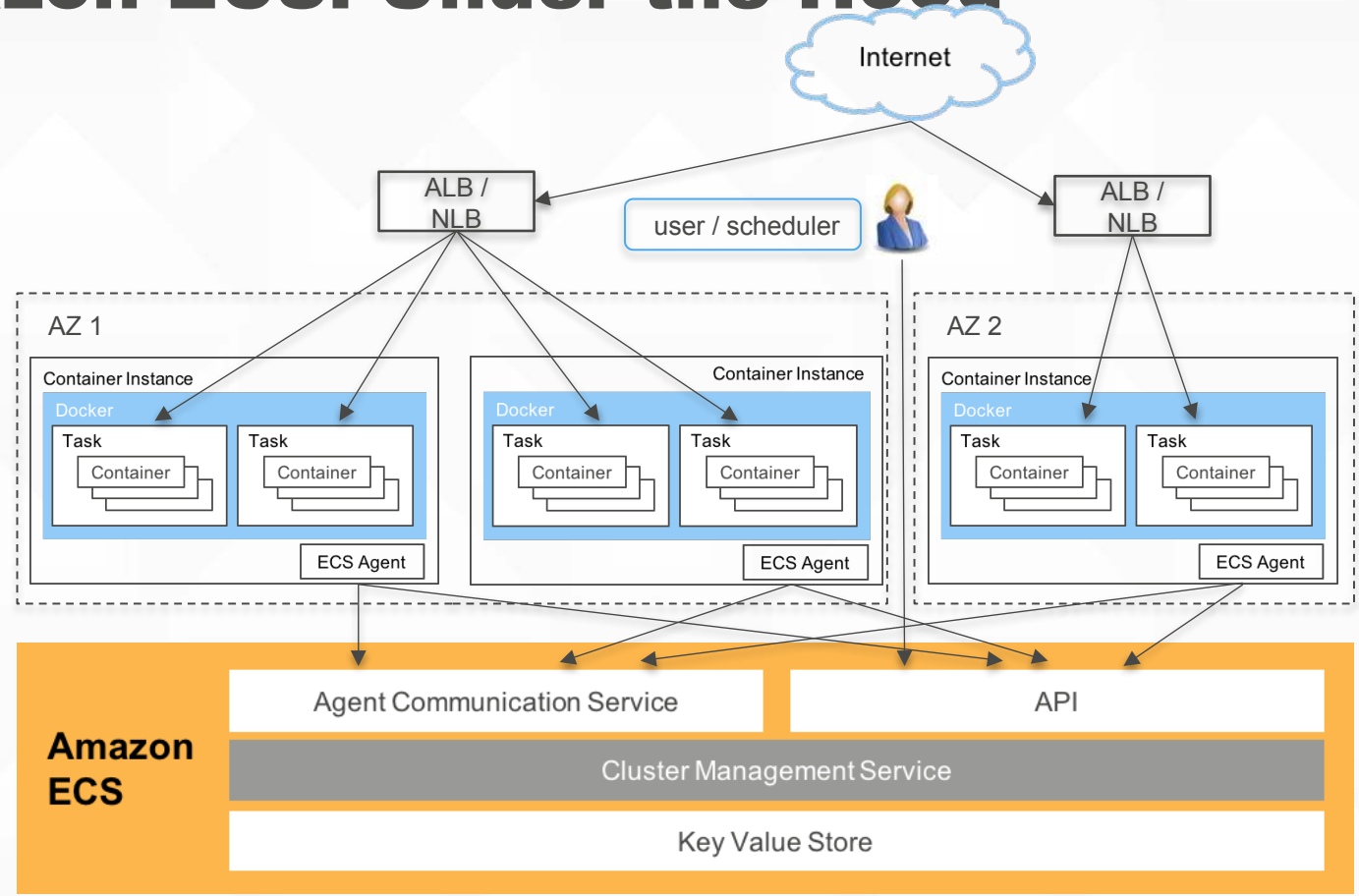
Segment moved to Docker for a better configuration management and needed a way to manage and schedule containers at scale.

Different services such as API, CDN, and App are deployed on different Amazon ECS clusters. Each service registers to an ELB and Amazon Route 53 points a local entry at each ELB. Services can communicate with each other through DNS.

"*Switching to Amazon ECS has greatly simplified running a service without needing to worry about provisioning or availability*"
Calvin French-Owen, Cofounder and CTO

aws

Amazon ECS: Under the Hood



https://github.com/aws/amazon-ecs-agent

aws

The Amazon ECS CLI in one slide

https://github.com/aws/amazon-ecs-cli

```
ecs-cli configure --cluster myCluster --region eu-west-1
ecs-cli up --keypair myKey --capability-iam –size 3
ecs-cli down myCluster --force

ecs-cli compose service up
ecs-cli compose service ps
ecs-cli compose service scale 8
ecs-cli compose service stop
ecs-cli compose service delete

aws ecs list-clusters
aws ecs describe-clusters --cluster myCluster
aws ecs list-container-instances --cluster myCluster
```

Resources

Tech articles by Werner Vogels, CTO, Amazon.com

http://www.allthingsdistributed.com/2014/11/amazon-ec2-container-service.html

http://www.allthingsdistributed.com/2015/04/state-management-and-scheduling-with-ecs.html

http://www.allthingsdistributed.com/2015/07/under-the-hood-of-the-amazon-ec2-container-service.html

Amazon ECS videos @ AWS re:Invent 2016

https://aws.amazon.com/blogs/compute/amazon-ec2-container-service-at-aws-reinvent-2016-wrap-up/

Staying in touch

https://aws.amazon.com/ecs/new/

https://aws.amazon.com/blogs/compute/category/amazon-ecs/

Follow the ECS evangelists @abbyfuller @nathanpeck @tiffanyfayj

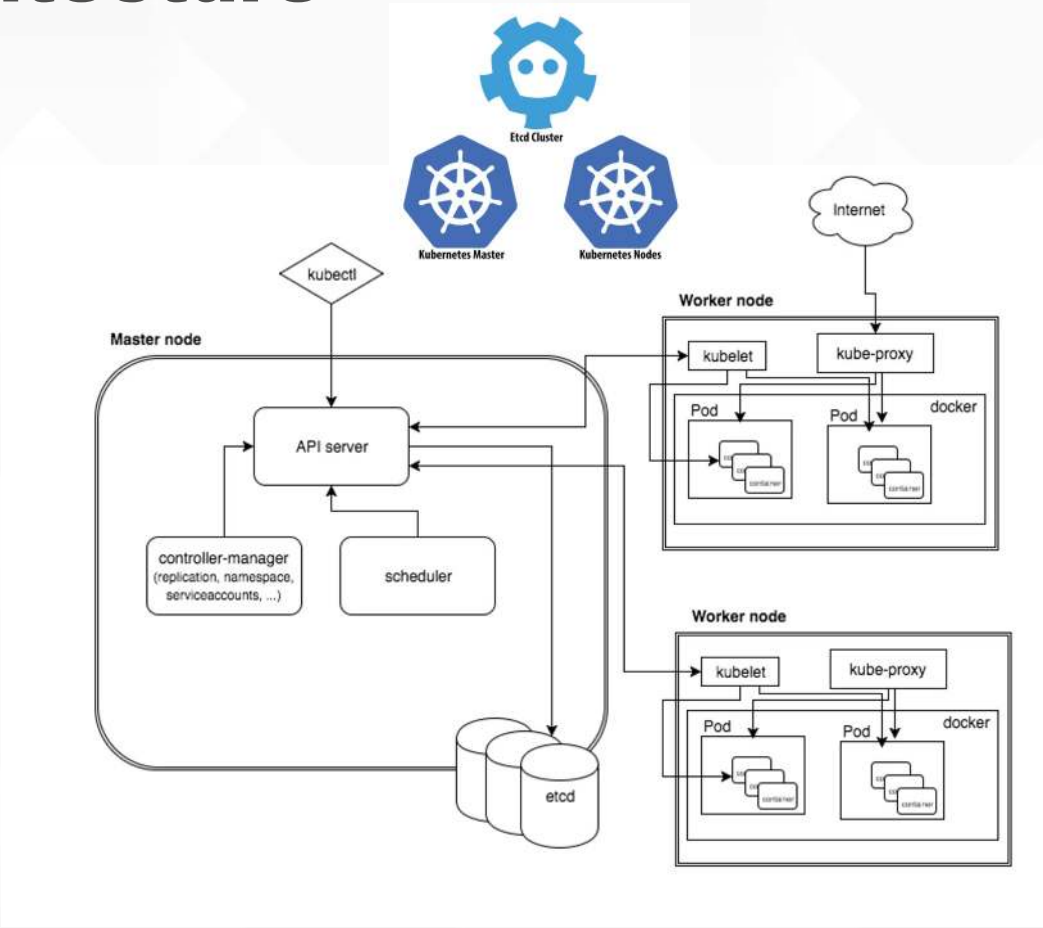
aws

Kubernetes

What is Kubernetes?

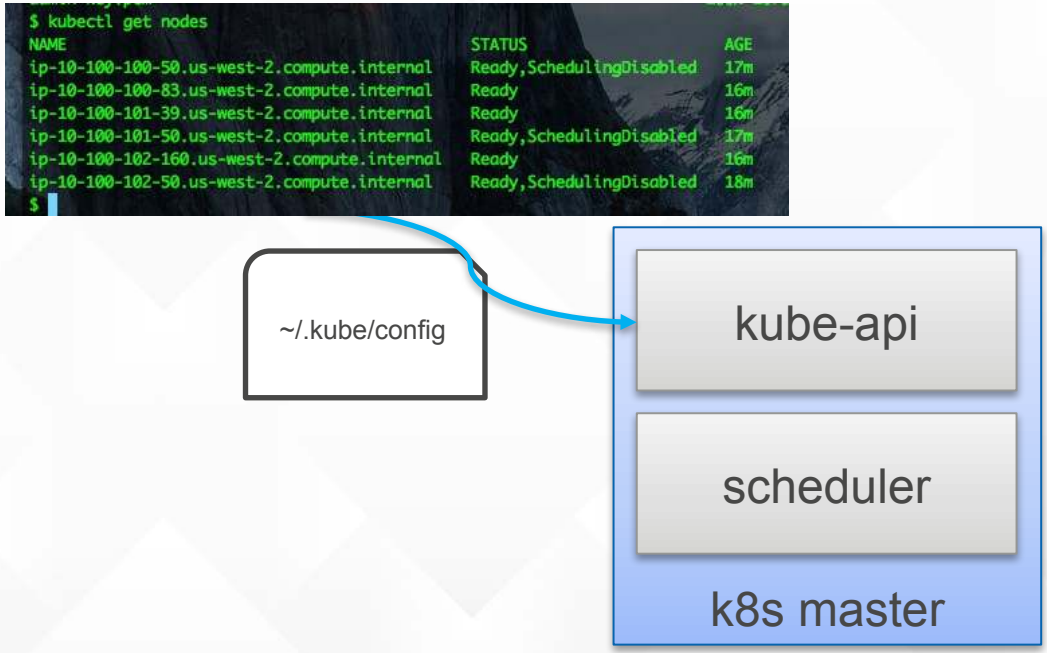
- Open sourced container cluster manager for automating the deployment, scaling and operations of application containers
- Originally developed by Google, influenced by internal project “Borg” https://research.google.com/pubs/pub43438.html
- Version 1.0 was released in Summer 2015

Architecture



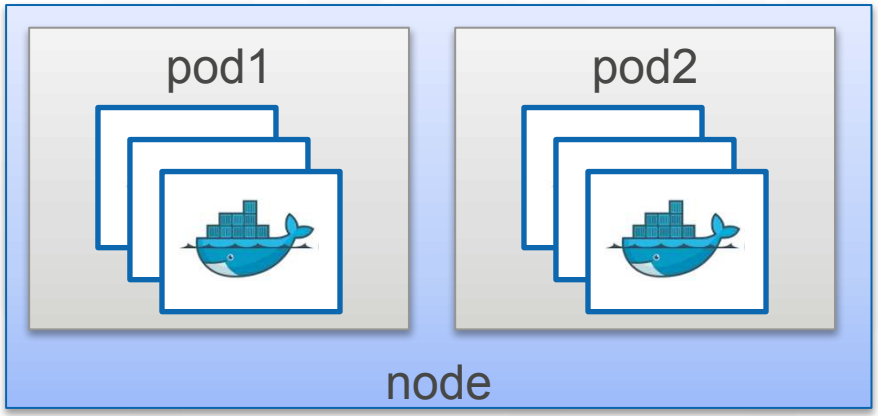
kubectl

- Command line interface for running commands against the Kubernetes API
- Intuitive familiar commands (get, create, describe, delete, etc.) that are simple to learn and easy to use



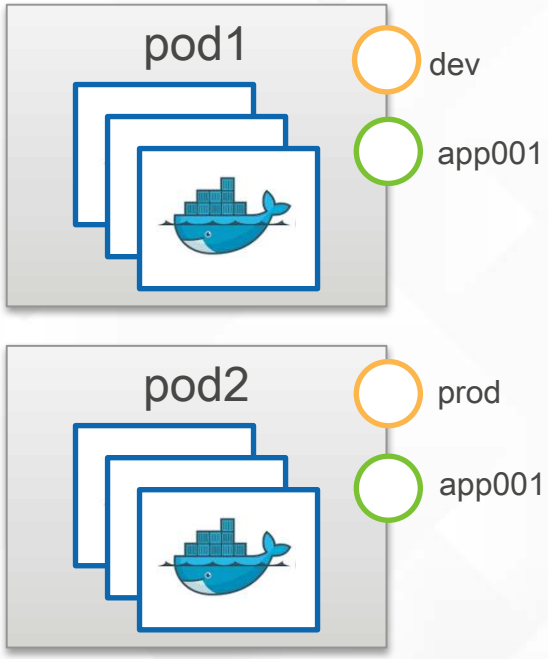
Pods

- A group of one or more containers
- Shared:
  - Data volumes
  - cgroup
  - Network, IPC, etc.



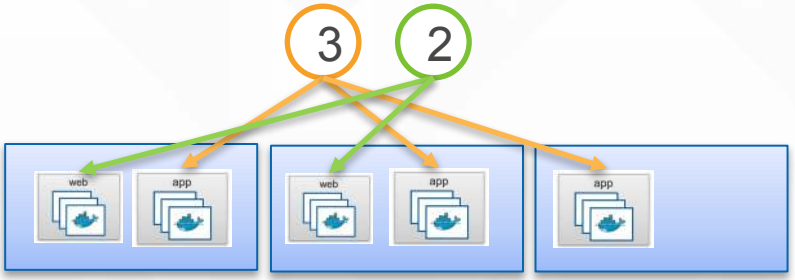
Labels

- Key/Value Pairs
- Used to query specific resources within your cluster



Replica Sets

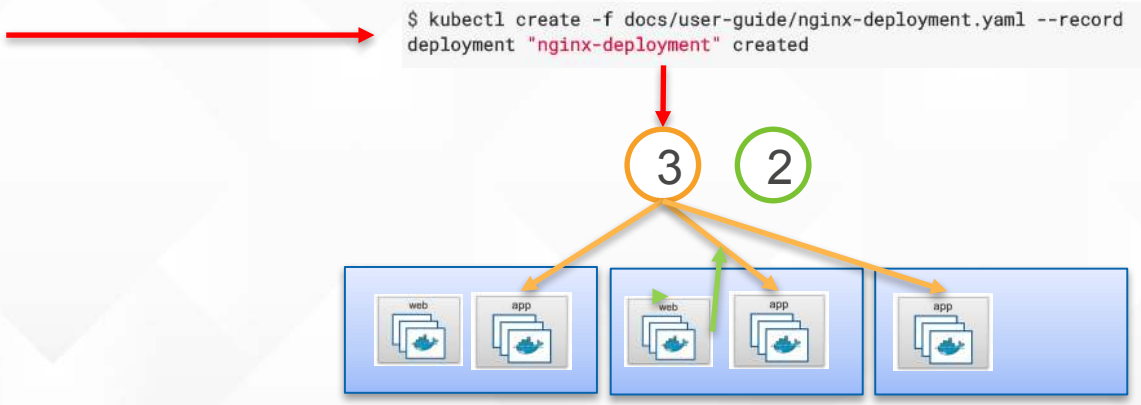
Ensure that a specified number of pod “replicas” exist in the cluster



Deployments

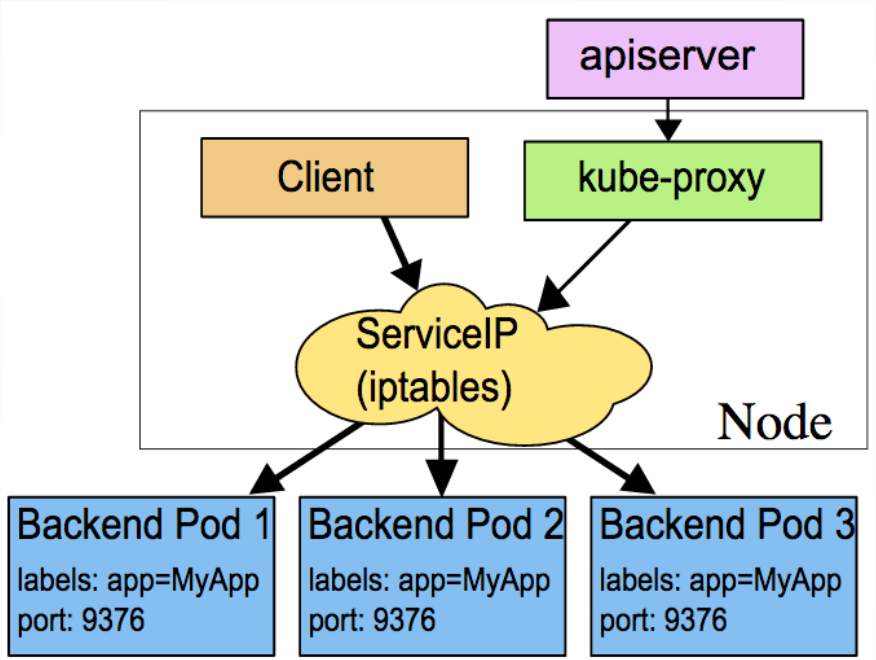
Declarative updates for Pods and ReplicaSets

```yaml
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  replicas: 3
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.7.9
        ports:
        - containerPort: 80
```



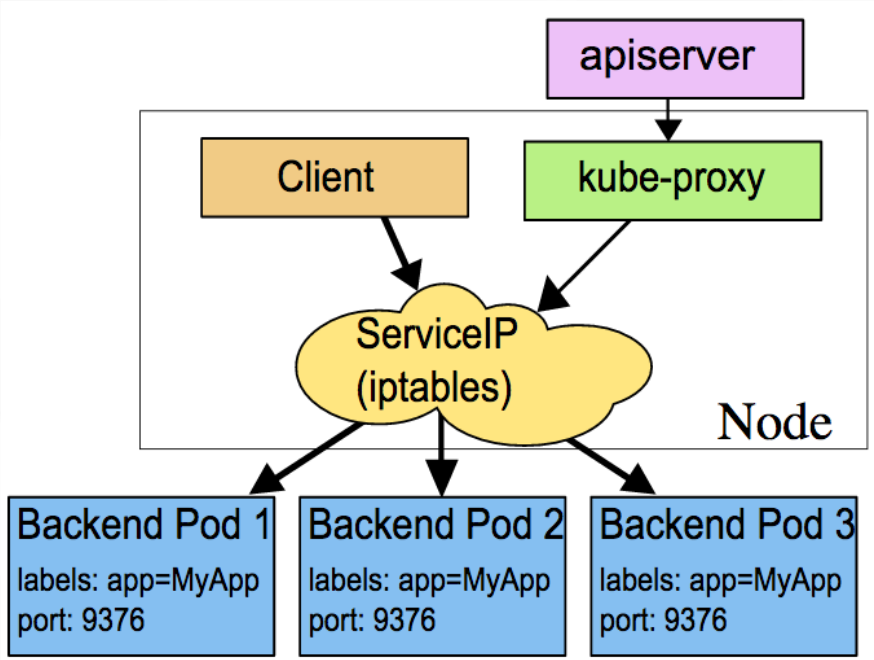
Services

Abstraction which defines a logical set of pods and policy by which to access them



Services

- Service Discovery
  - Environment variables
  - DNS
- Publishing Services
  - LoadBalancer (ELB)
  - ClusterIP, NodePort, External Name (DNS)



KOPS (Kubernetes Ops)

- Owned by Kubernetes https://github.com/kubernetes/kops
- CLI tool for launching and managing clusters
- Can provision simple single-AZ clusters or multi-AZ production ready clusters
- Provides choice of networking configuration
- Manages DNS configuration
- Can generate Terraform and CloudFormation configuration
- Stores cluster state in S3

KOPS (Kubernetes Ops)

`kops create cluster`

`kops create cluster <clustername>` creates a cloud specification in the registry. It will not create the cloud resources unless you specify `--yes`, so that you have the chance to `kops edit` them. (You will likely `kops update cluster` after creating it).

`kops update cluster`

`kops update cluster <clustername>` creates or updates the cloud resources to match the cluster spec.

It is recommended that you run it first in 'preview' mode with `kops update cluster --name <name>`, and then when you are happy that it is making the right changes you run `kops update cluster --name <name> --yes`.

`kops get clusters`

`kops get clusters` lists all clusters in the registry.

`kops delete cluster`

`kops delete cluster` deletes the cloud resources (instances, DNS entries, volumes, ELBs, VPCs etc) for a particular cluster. It also removes the cluster from the registry.

It is recommended that you run it first in 'preview' mode with `kops delete cluster --name <name>`, and then when you are happy that it is deleting the right things you run `kops delete cluster --name <name> --yes`.

KOPS (Kubernetes Ops)

Advanced Example

Example Create Cluster Command for HA / Private Topology

```
kops create cluster \
    --node-count 3 \
    --zones us-west-2a,us-west-2b,us-west-2c \
    --master-zones us-west-2a,us-west-2b,us-west-2c \
    --dns-zone example.com \
    --node-size t2.medium \
    --master-size t2.medium \
    --node-security-groups sg-12345678 \
    --master-security-groups sg-12345678,i-abcd1234 \
    --topology private \
    --networking weave \
    --cloud-labels "Team=Dev,Owner=John Doe" \
    --image 293135079892/k8s-1.4-debian-jessie-amd64-hvm-ebs-2016-11-16 \
    ${NAME}
```

Resources

Kubernetes tutorials

https://kubernetes.io/docs/tutorials/

https://kubernetes.io/docs/getting-started-guides/aws/

re:Invent 2016 - Introduction to Container Management on AWS

https://www.youtube.com/watch?v=nkguMBVsRbE

Kubernetes on AWS workshop (@arungupta)

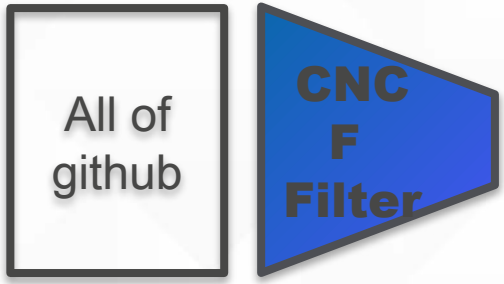
https://aws.amazon.com/blogs/compute/kubernetes-clusters-aws-kops/

https://github.com/arun-gupta/kubernetes-aws-workshop

CNCF

Cloud Native Computing Foundation

A curated collection of interesting open source projects that have broad support



Kubernetes
Orchestration

Prometheus
Monitoring

CoreDNS
Service Discover

OpenTracing
Tracing

Fluentd
Logging

Containerd
Container Runtime

linkerd
Service Mesh

gRPC
Remote Procedure Call

rkt
Container Runtime

CNI
Networking

Envoy
Service Mesh

Jeager
Distributed Tracing

aws

AWS (and everyone else) joined CNCF

Promote Cloud Native to enterprise customers

Integrate CNCF components into AWS ECS – CNI, containered, etc.

Integrate Kubernetes with AWS – installers, IAM, security, etc.

CNCF serverless working group

aws

Kubernetes

Managed by customers

Single tenant install

Control plane overhead

Version upgrade management

Networking: CNI

IAM integration fixes needed

vs

AWS ECS

Managed for you by AWS

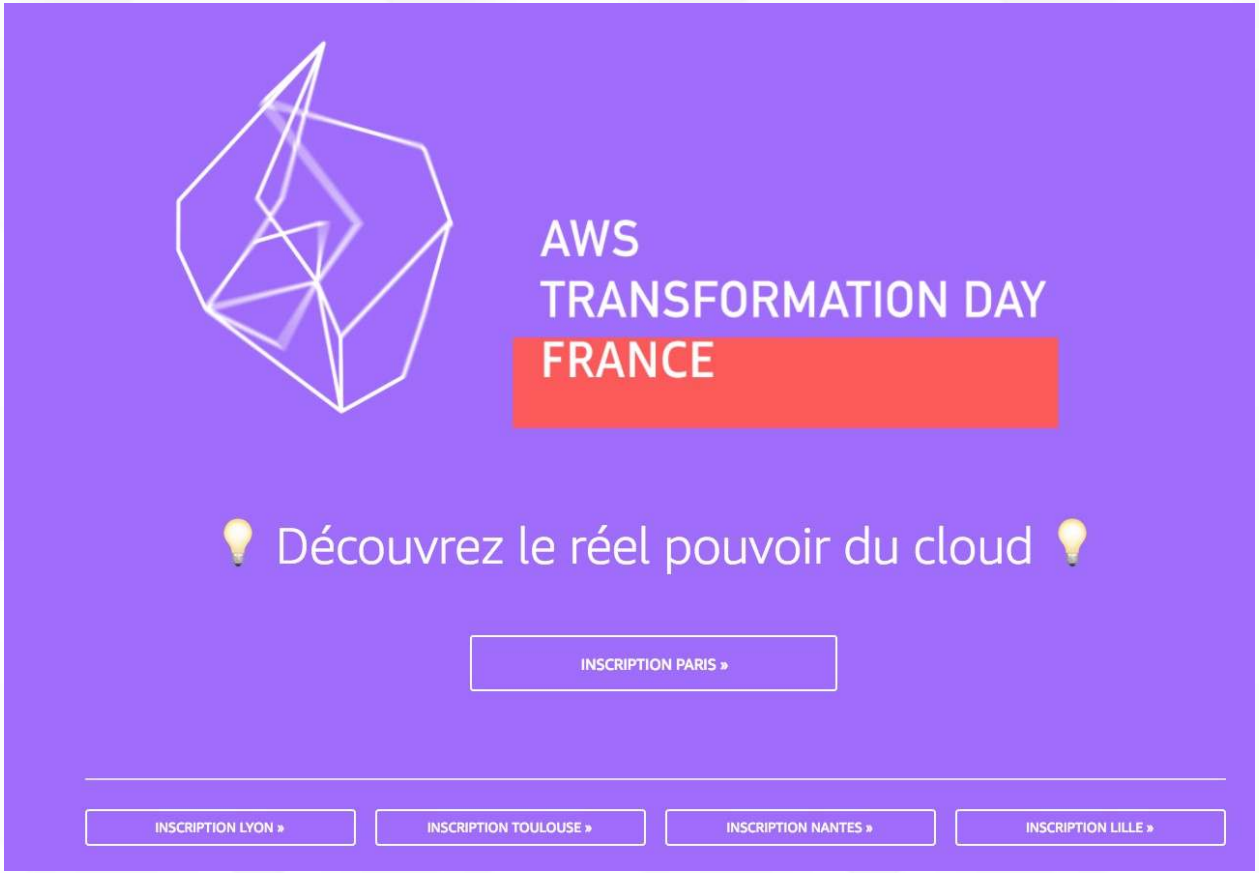
Multi tenant service

Just EC2 instances by the second

Doesn’t apply

Moving to CNI

IAM Integrated



https://aws.amazon.com/fr/events/transformation-day-france/

aws

Thank you!

Julien Simon, Principal Technical Evangelist
@julsimon

aws