Service Mesh on AWS

Jakarta Kubernetes — 20 June 2019

Donnie Prakoso

Technical Evangelist, AWS

About me

Donnie Prakoso, MSc

Technical Evangelist, ASEAN

- 13 years of devops, design patterns, and software engineering
- Self-proclaimed barista, café racer enthusiast
- Speak in Go and Python
- I talk about microservices a lot — design patterns, containers and serverless

Twitter: @donnieprakoso

LinkedIn: donnieprakoso

aws

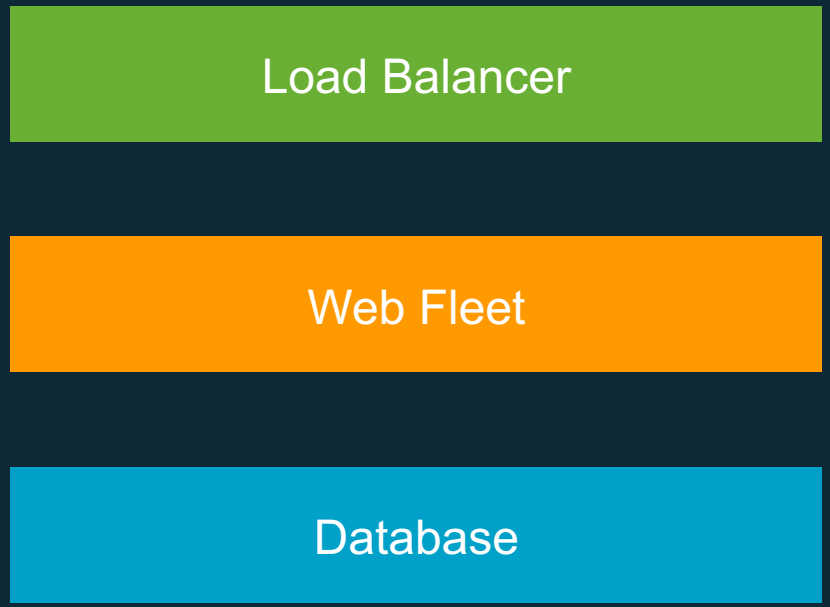
Once upon a time...

Life used to be easier

The three tier monolithic app

- Complexity in the codebase
- Harder to scale/deploy

- …but easy to observe
- Include an observability library/sdk in our application

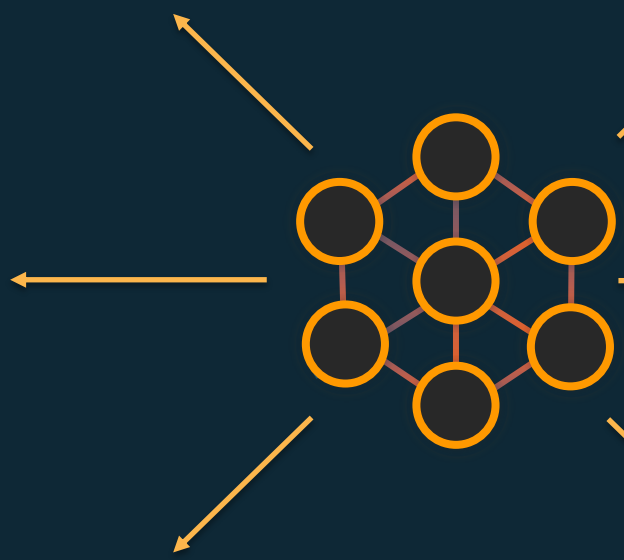


aws

Characteristics of Microservices

Decentralized

Polyglot



Independent

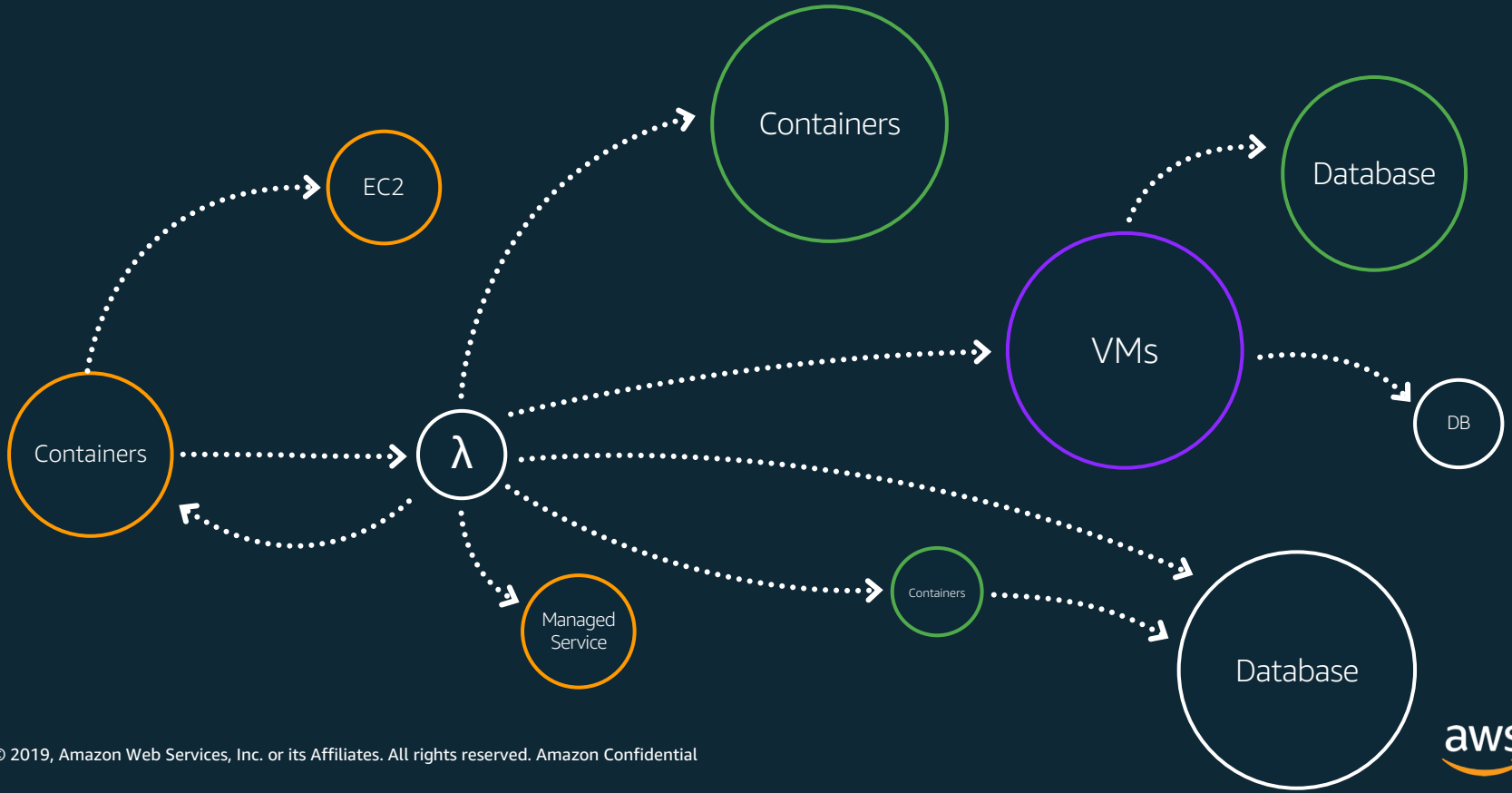
Do one thing well

Black box

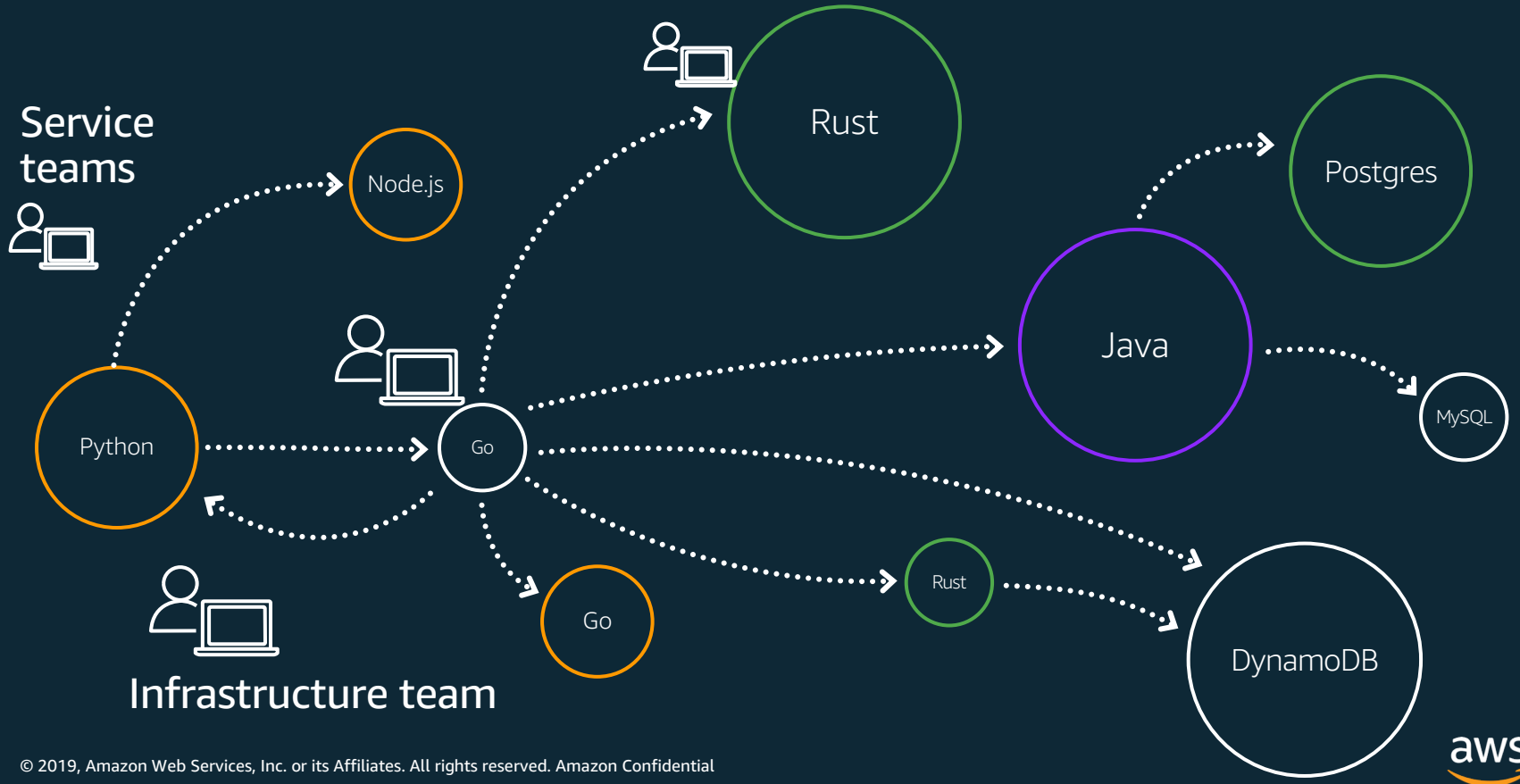
You build it, you run it

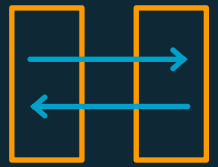
aws

Polyglot of Technologies



Polyglot of Languages





Consistent communications management

Complete visibility

Failure isolation and protection

Fine-grained deployment controls

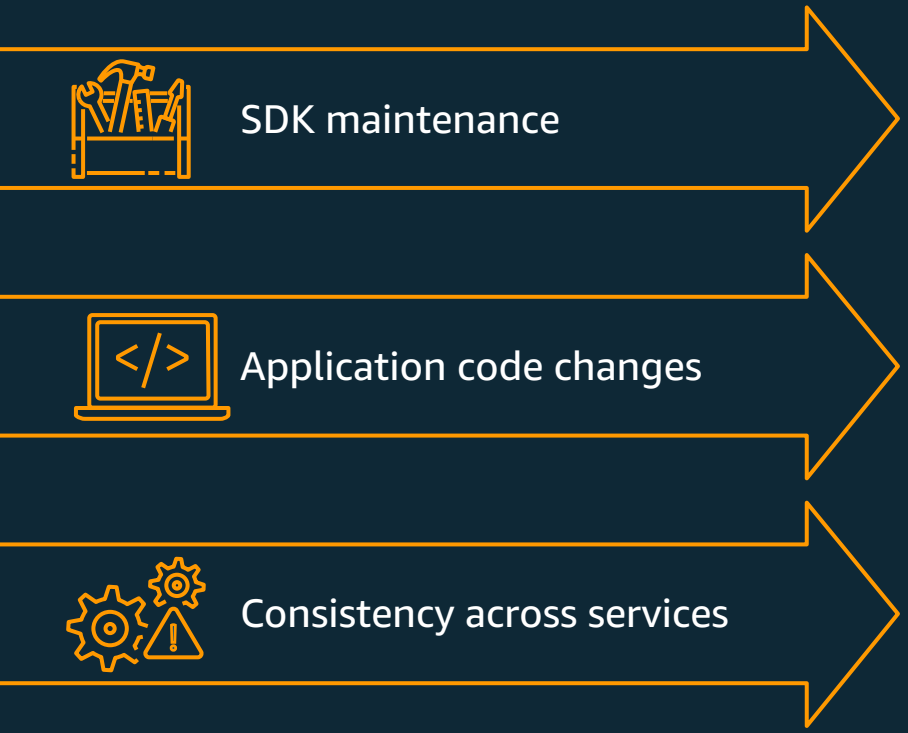
aws

… ok, so now what?

Let's talk observability

aws

Option 1: Library / SDK



Languages

Java
Scala
Node.js
Python
C++
Django
.NET
GO
…

Sidecar to the rescue!

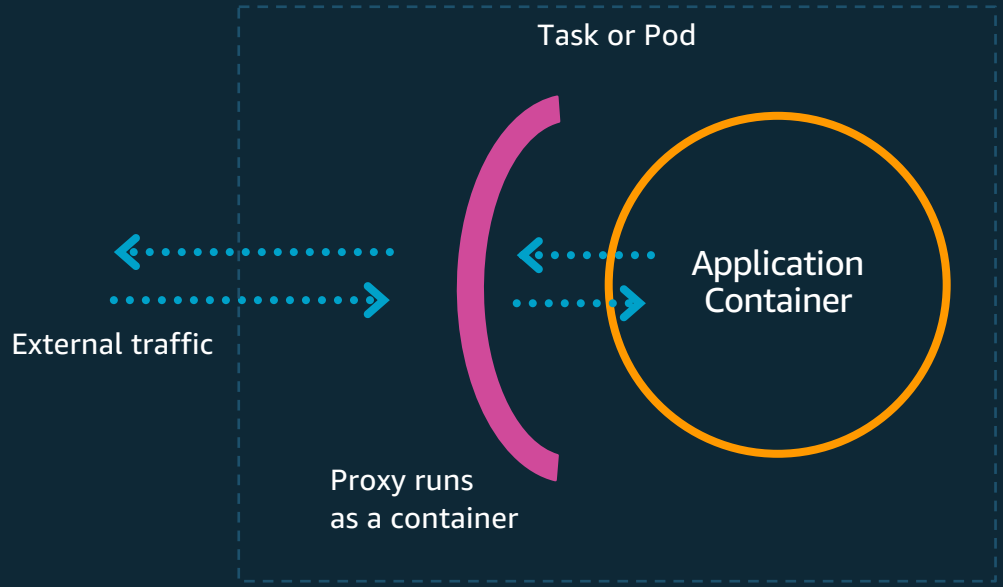
Photo credits: hiconsumption.com

aws

Option 2: side-car proxy

Proxy

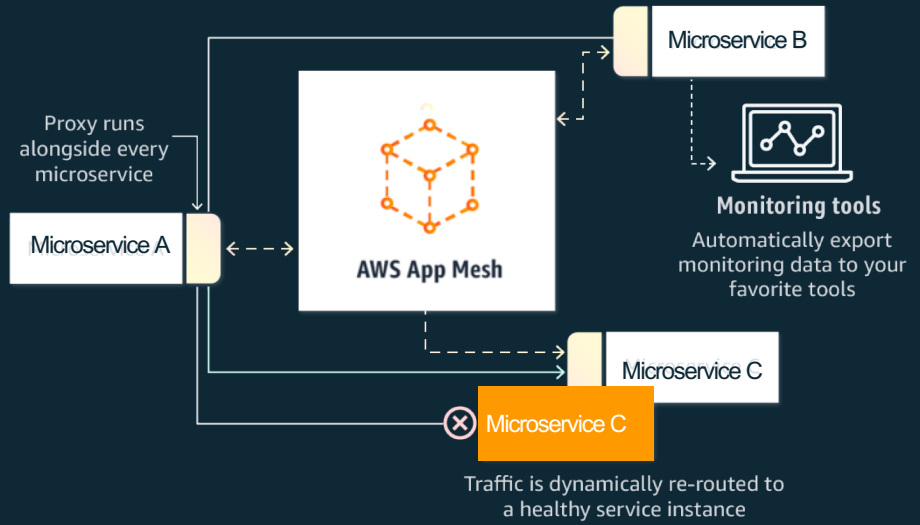
Monitoring
Routing
Discovery
Deployment



AWS App Mesh

Application-level networking for all your services

Easily monitor and control microservices App Mesh with Amazon ECS and Amazon EKS to better run containerized microservices at scale



Amazon EC2

aws

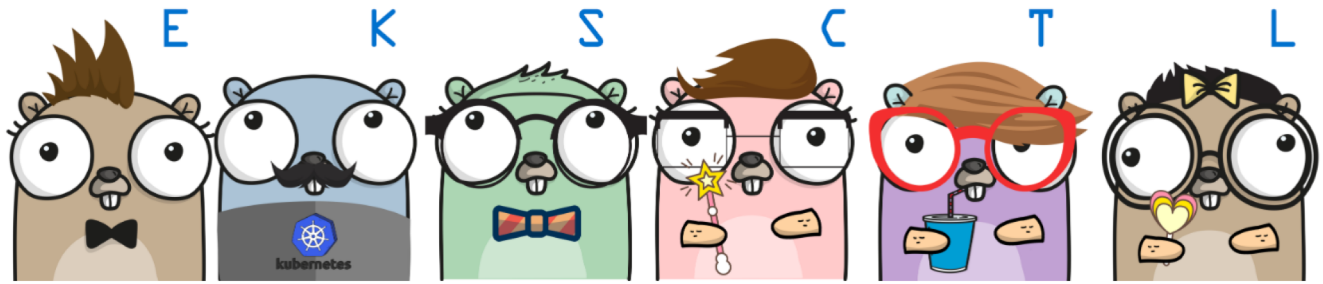
Amazon EKS… getting started

`eksctl` - a CLI for Amazon EKS

circleci passing | coverage 38% | go report A+

`eksctl` is a simple CLI tool for creating clusters on EKS - Amazon's new managed Kubernetes service for EC2. It is written in Go, and uses CloudFormation.

You can create a cluster in minutes with just one command – **`eksctl create cluster`**!



aws

Deploying K8s with Amazon EKS

$ brew install weaveworks/tap/eksctl

$ eksctl create cluster

Additional flags for node groups, IAM permissions, subnets, VPC, SSH access, etc.

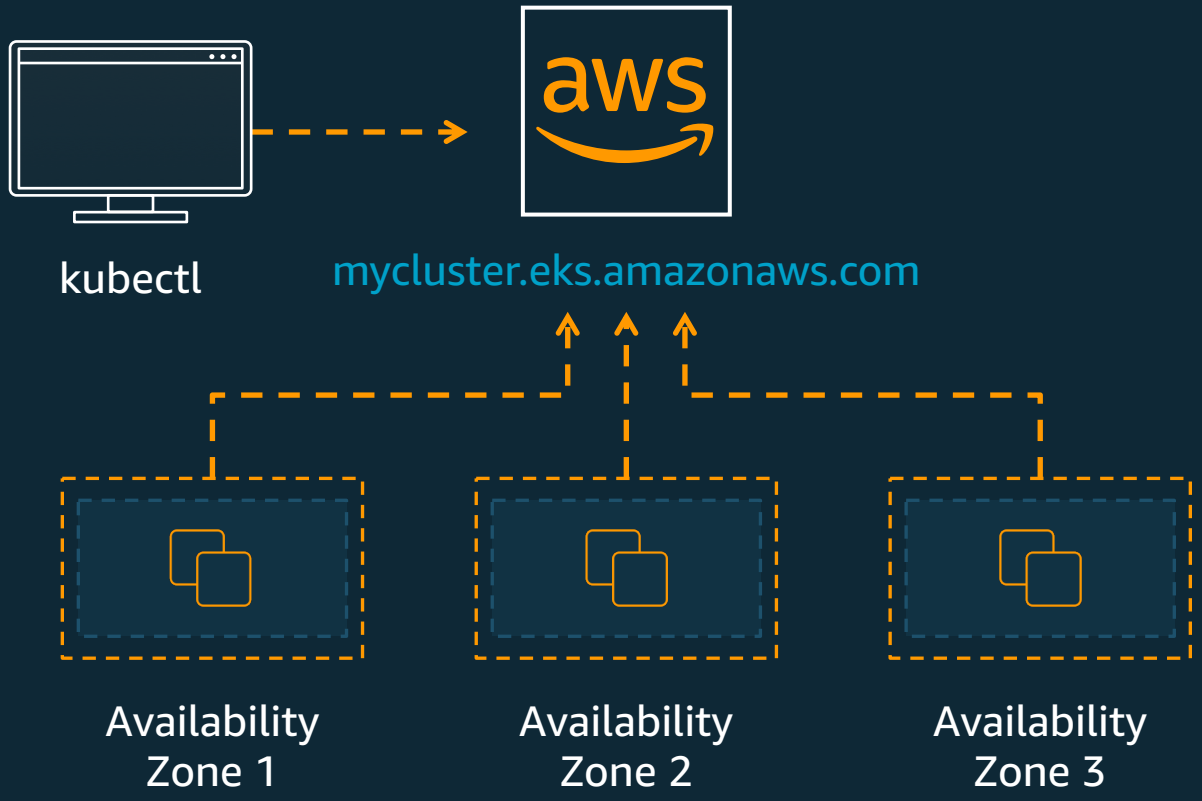
aws

eksctl, the declarative way

```yaml
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: cluster-in-existing-vpc
  region: eu-north-1

vpc:
  subnets:
    private:
      eu-north-1a: {id: subnet-0ff156e0c4a6d300c}
      eu-north-1b: {id: subnet-0549cdab573695c03}
      eu-north-1c: {id: subnet-0426fb4a607393184}

nodeGroups:
  - name: ng-1-workers
    labels: {role: workers}
    instanceType: m5.xlarge
    desiredCapacity: 10
    privateNetworking: true
  - name: ng-2-builders
    labels: {role: builders}
    instanceType: m5.2xlarge
    desiredCapacity: 2
    privateNetworking: true
    iam:
      withAddonPolicies:
        imageBuilder: true
```

```
$ eksctl apply --cluster-config cluster.yaml
```


aws



Demo

App Mesh uses Envoy proxy

OSS project

Wide community support, numerous integrations

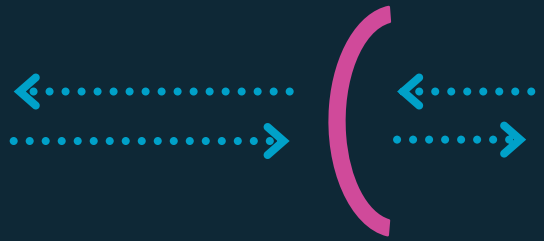
Stable and production-proven

“Graduated Project” in Cloud Native Computing Foundation

Started at Lyft in 2016

aws

Protocol level observability (Layer 7)



Logging
generates access logs

Prometheus Exporter
Listens on tcp/9090

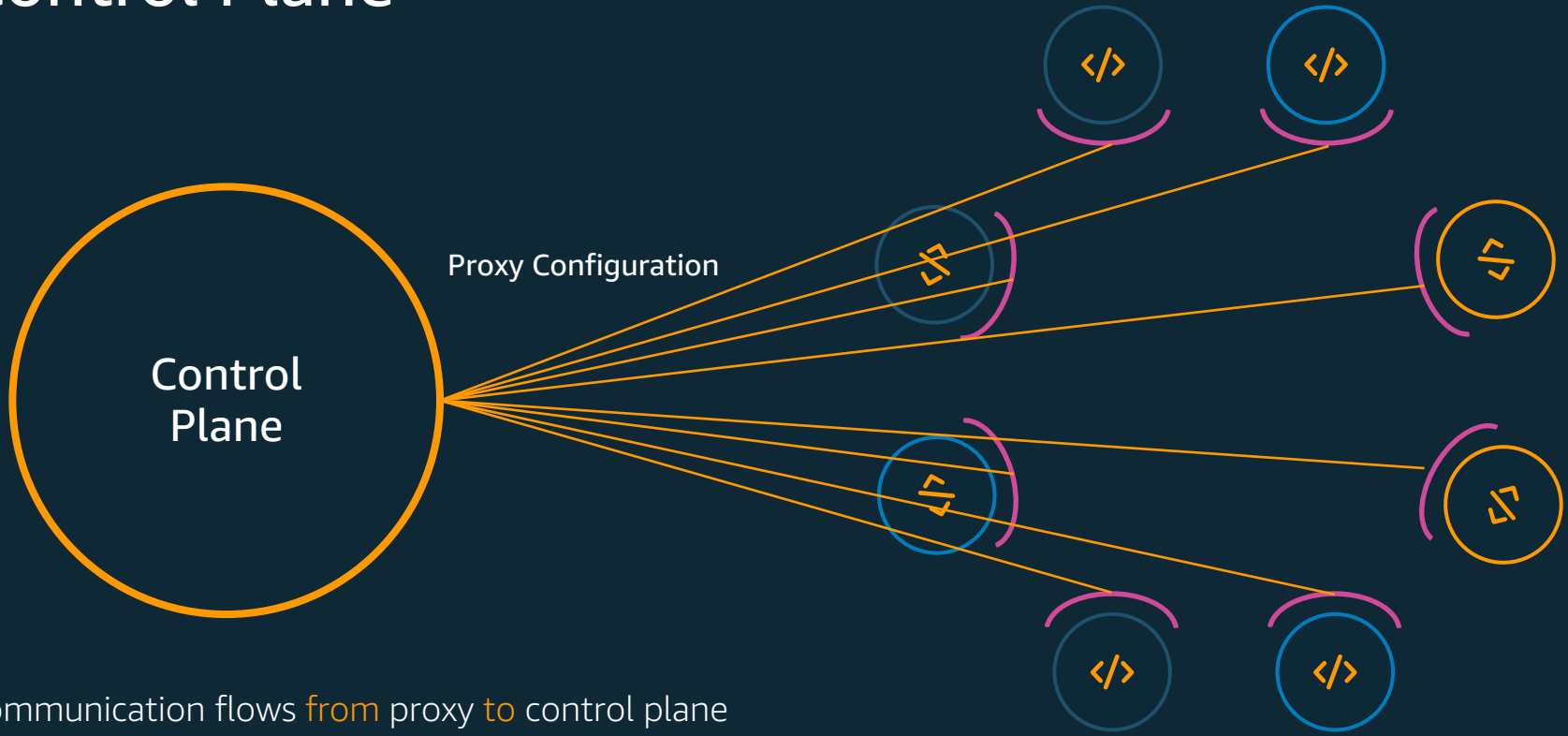
StatsD
Sends metrics to a StatsD server

Amazon X-Ray
forwards traces to AWS

Integrations with
Datadog, Alcide, HashiCorp, Sysdig, Signalfx, Spotinst, Tetrate, Neuvector, Weaveworks, Twistlock, Wavefront by VMware, Aqua.

aws

Control Plane

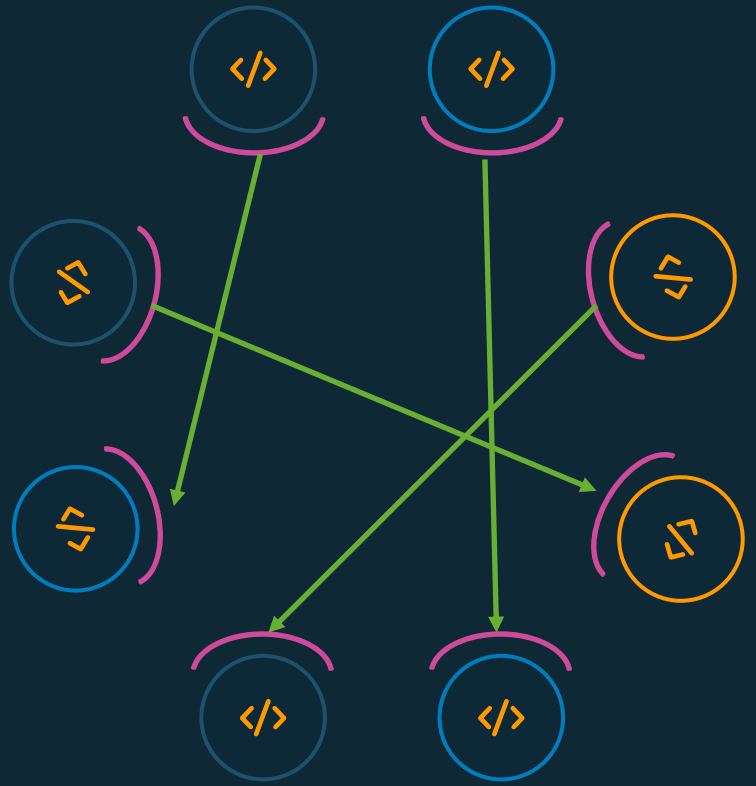


Communication flows from proxy to control plane
Uses Envoy xDS protocol over GRPC
https://github.com/envoyproxy/data-plane-api/blob/master/xds_protocol.rst

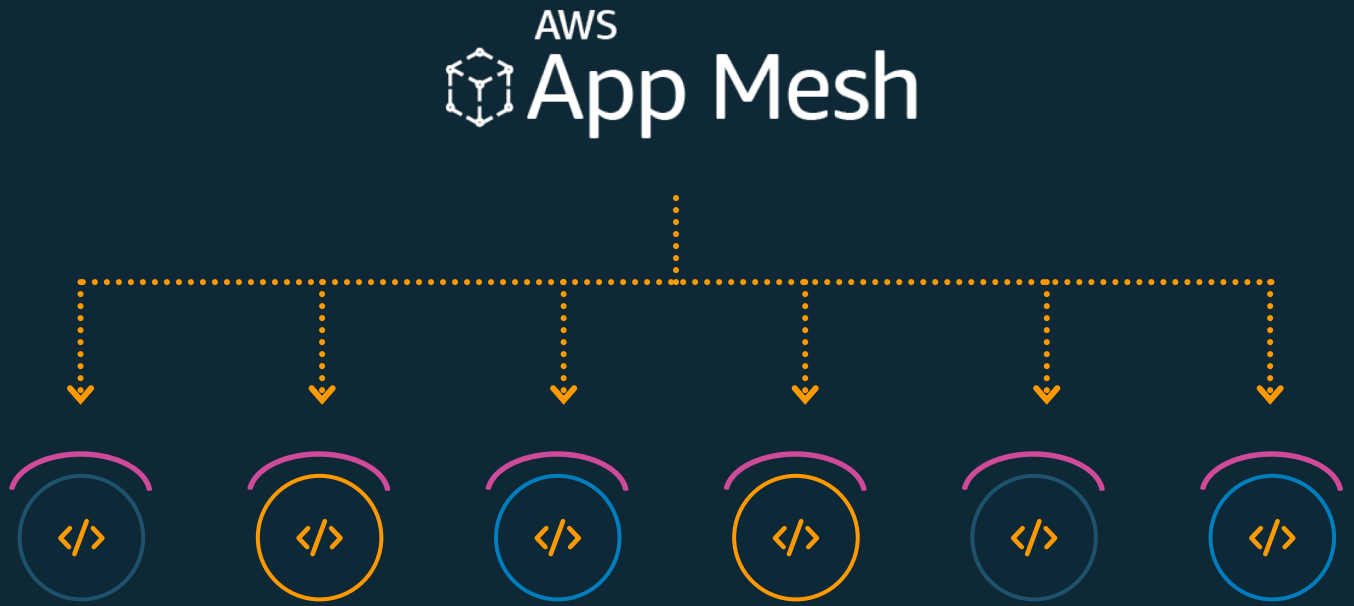
aws

Data Plane

Control Plane



AWS App Mesh uses a managed control plane



Why service mesh control plane

vs. static config or self-built control plane

Don’t need to spend dev to build and ops to maintain

Not tied to application deployment system
(e.g., container orchestration)

Works across different compute systems

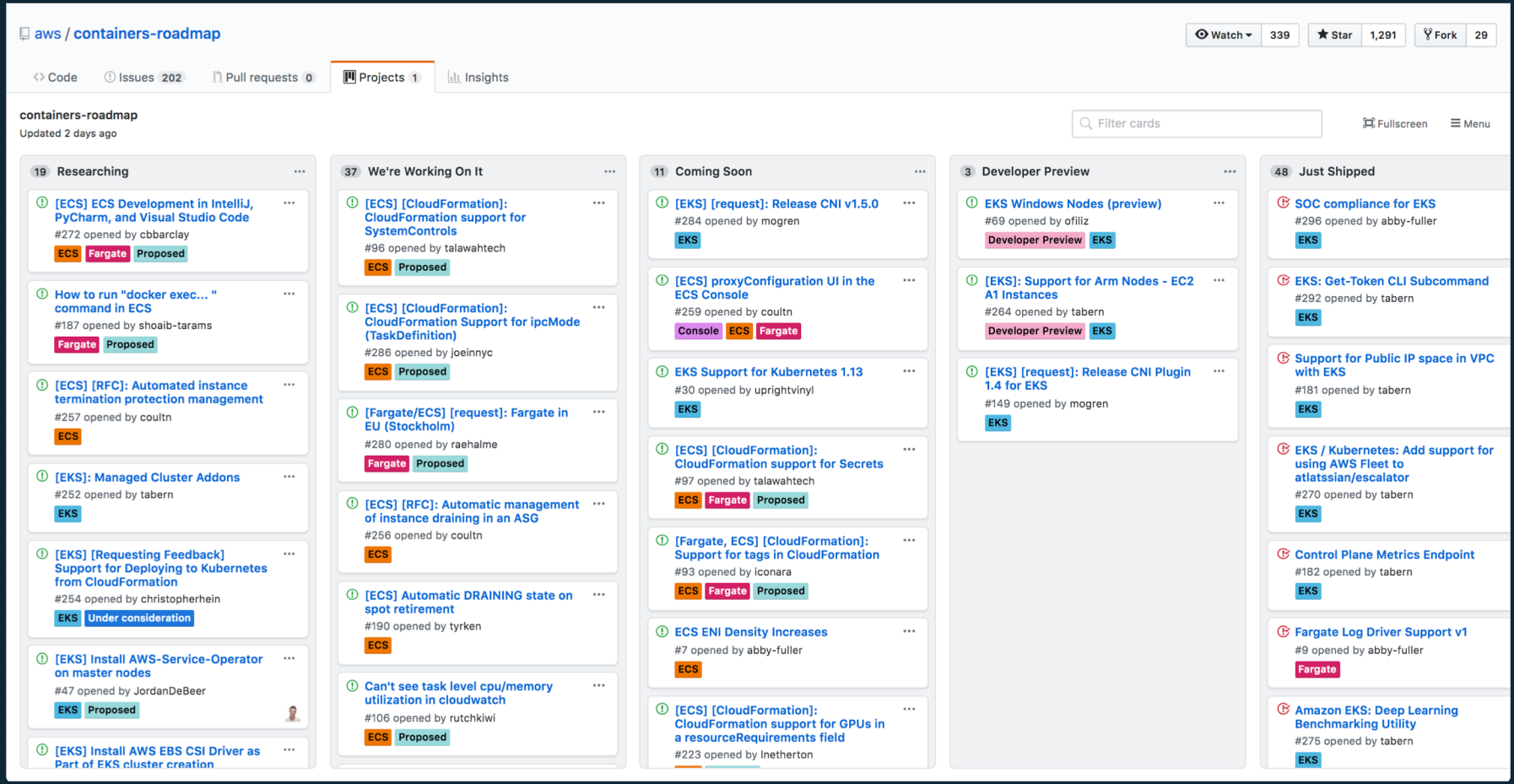
Reliably store and distribute configuration

aws

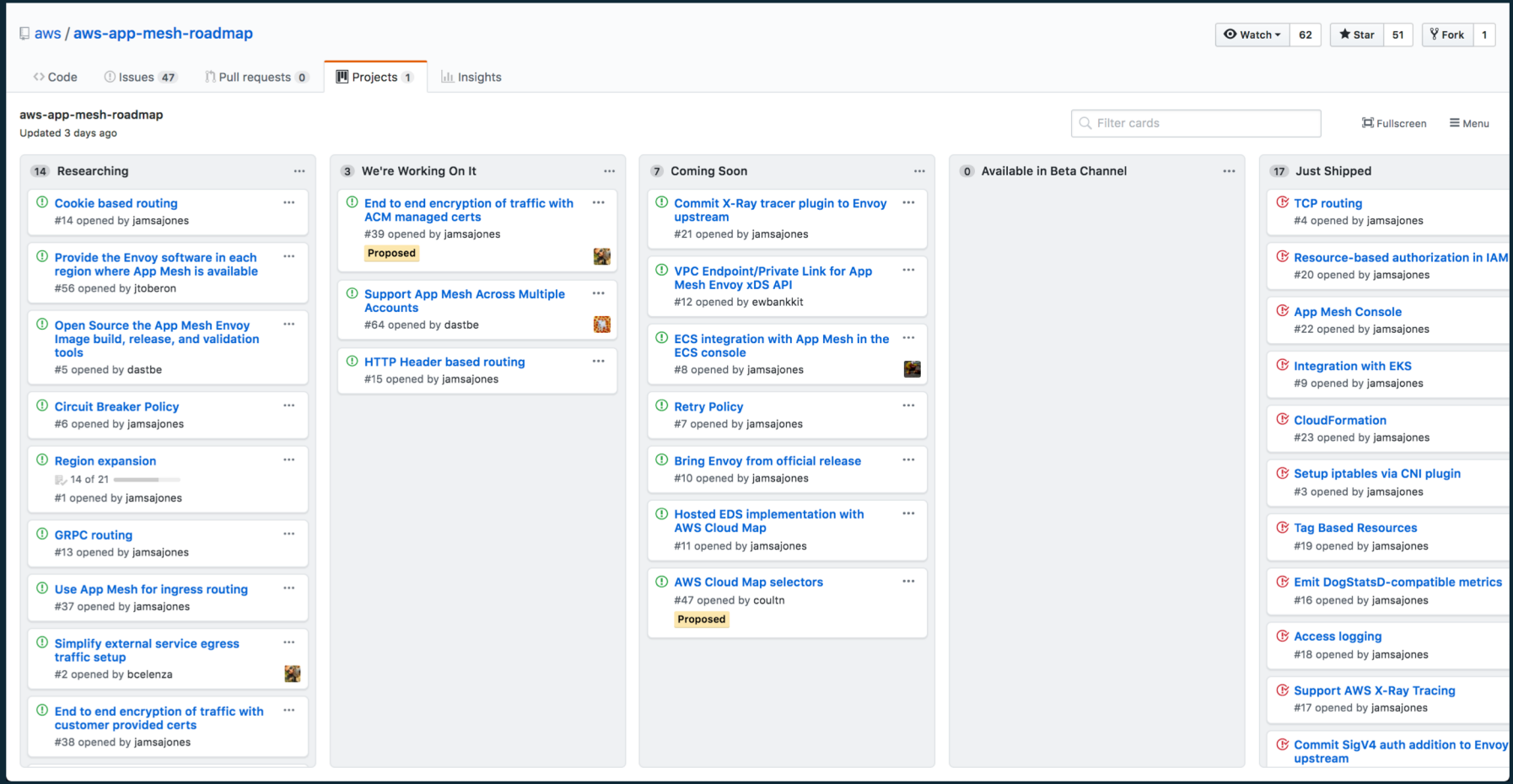
$0

Roadmap

github.com/aws/containers-roadmap



github.com/aws/aws-app-mesh-roadmap



aws / aws-app-mesh-roadmap

Watch 62 | Star 51 | Fork 1

Code | Issues 47 | Pull requests 0 | Projects 1 | Insights

aws-app-mesh-roadmap
Updated 3 days ago

Filter cards | Fullscreen | Menu

14 Researching

- Cookie based routing
  #14 opened by jamsajones
- Provide the Envoy software in each region where App Mesh is available
  #56 opened by jtoberon
- Open Source the App Mesh Envoy Image build, release, and validation tools
  #5 opened by dastbe
- Circuit Breaker Policy
  #6 opened by jamsajones
- Region expansion
  14 of 21
  #1 opened by jamsajones
- GRPC routing
  #13 opened by jamsajones
- Use App Mesh for ingress routing
  #37 opened by jamsajones
- Simplify external service egress traffic setup
  #2 opened by bcelenza
- End to end encryption of traffic with customer provided certs
  #38 opened by jamsajones

3 We're Working On It

- End to end encryption of traffic with ACM managed certs
  #39 opened by jamsajones
  Proposed
- Support App Mesh Across Multiple Accounts
  #64 opened by dastbe
- HTTP Header based routing
  #15 opened by jamsajones

7 Coming Soon

- Commit X-Ray tracer plugin to Envoy upstream
  #21 opened by jamsajones
- VPC Endpoint/Private Link for App Mesh Envoy xDS API
  #12 opened by ewbankkit
- ECS integration with App Mesh in the ECS console
  #8 opened by jamsajones
- Retry Policy
  #7 opened by jamsajones
- Bring Envoy from official release
  #10 opened by jamsajones
- Hosted EDS implementation with AWS Cloud Map
  #11 opened by jamsajones
- AWS Cloud Map selectors
  #47 opened by coultn
  Proposed

0 Available in Beta Channel

17 Just Shipped

- TCP routing
  #4 opened by jamsajones
- Resource-based authorization in IAM
  #20 opened by jamsajones
- App Mesh Console
  #22 opened by jamsajones
- Integration with EKS
  #9 opened by jamsajones
- CloudFormation
  #23 opened by jamsajones
- Setup iptables via CNI plugin
  #3 opened by jamsajones
- Tag Based Resources
  #19 opened by jamsajones
- Emit DogStatsD-compatible metrics
  #16 opened by jamsajones
- Access logging
  #18 opened by jamsajones
- Support AWS X-Ray Tracing
  #17 opened by jamsajones
- Commit SigV4 auth addition to Envoy upstream

THANK YOU

https://github.com/weaveworks/eksctl

https://github.com/aws/containers-roadmap

Twitter: @donnieprakoso
LinkedIn: donnieprakoso

aws