



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

Once upon a time...

Life used to be easier

The three tier monolithic app

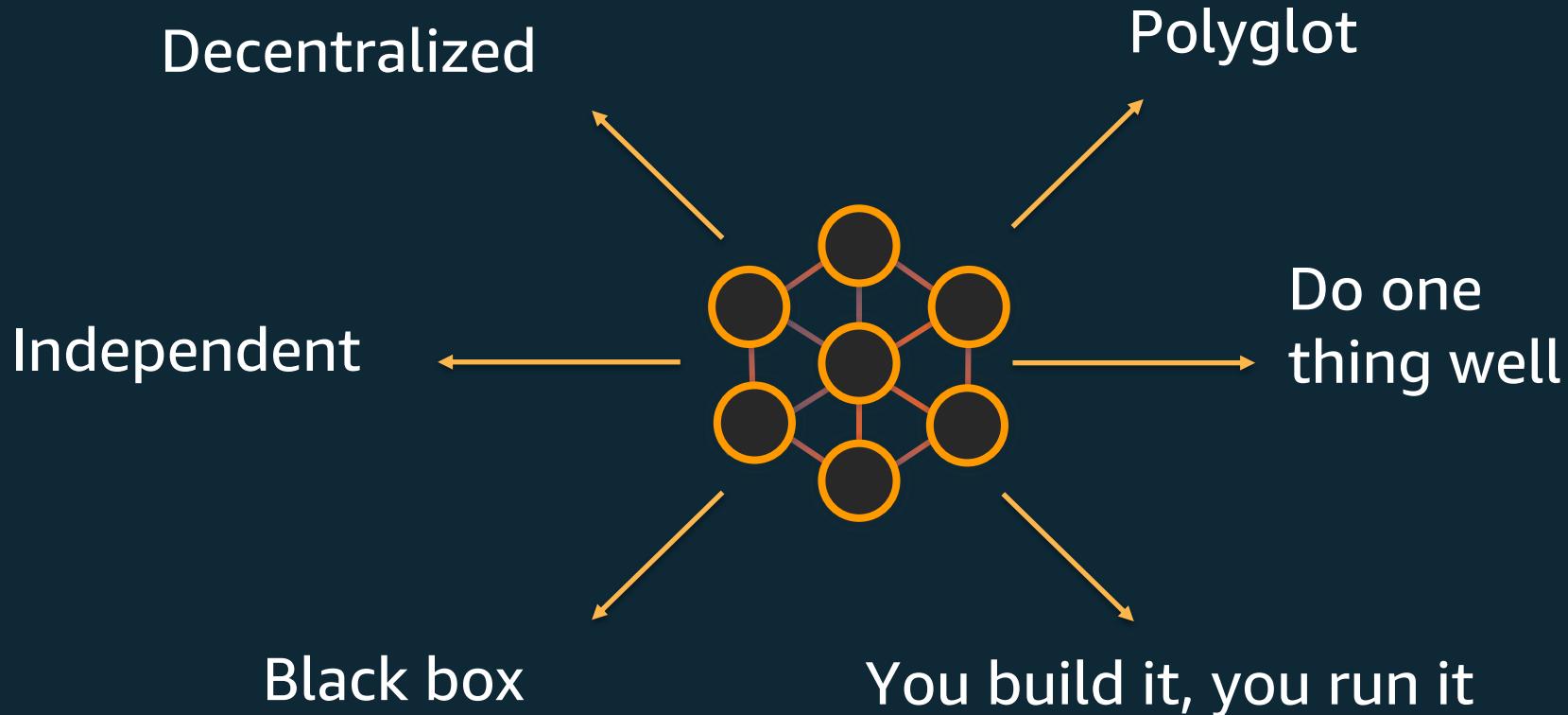
- Complexity in the codebase
- Harder to scale/deploy
- ...but easy to observe
- Include an observability library/sdk in our application

Load Balancer

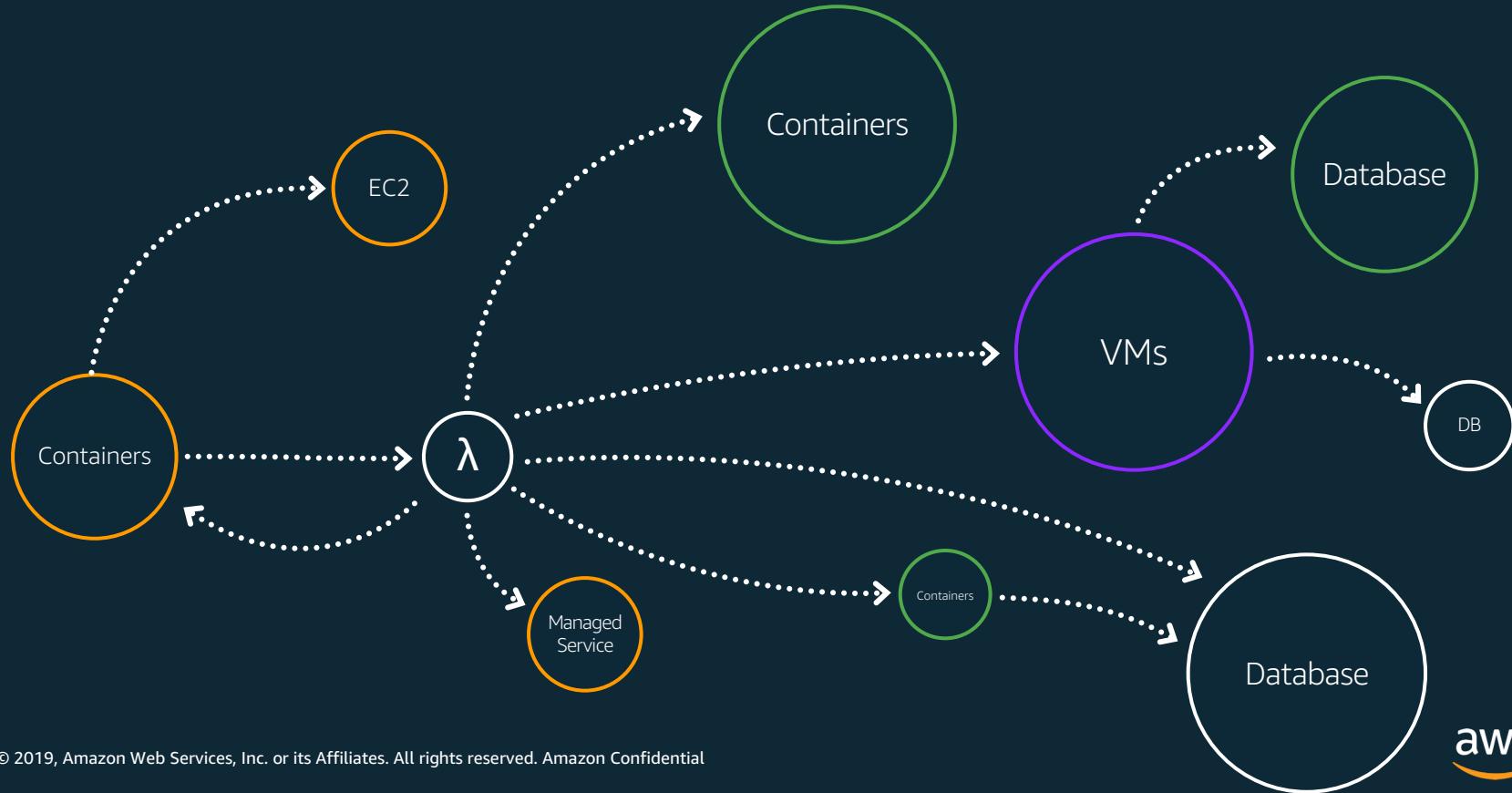
Web Fleet

Database

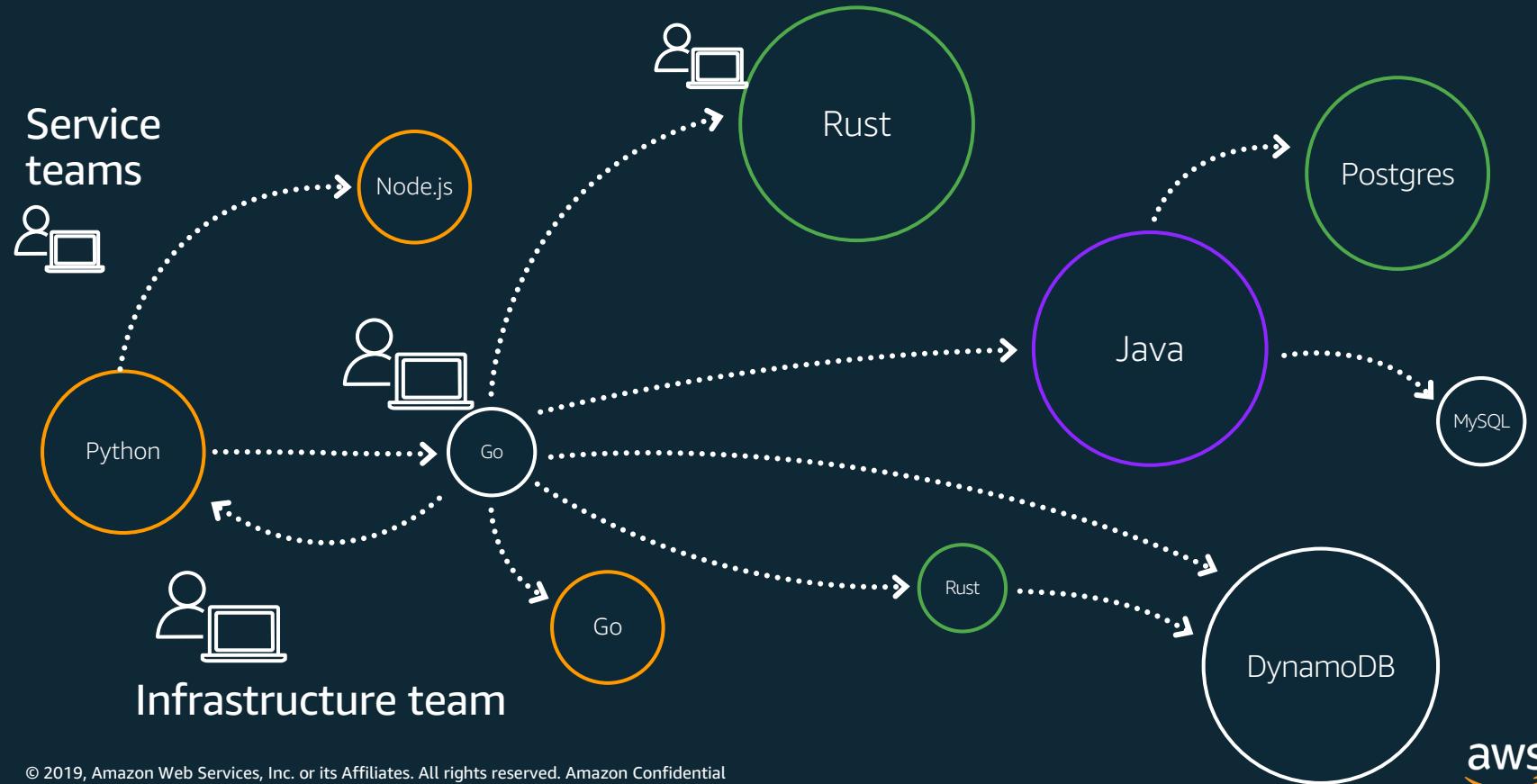
Characteristics of Microservices

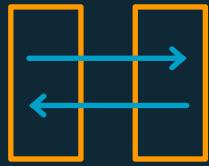


Polyglot of Technologies



Polyglot of Languages





Consistent
communications
management



Complete visibility



Failure isolation
and protection



Fine-grained
deployment controls

... ok, so now what?

Let's talk observability

Option 1: Library / SDK



SDK maintenance



Application code changes



Consistency across services



Languages

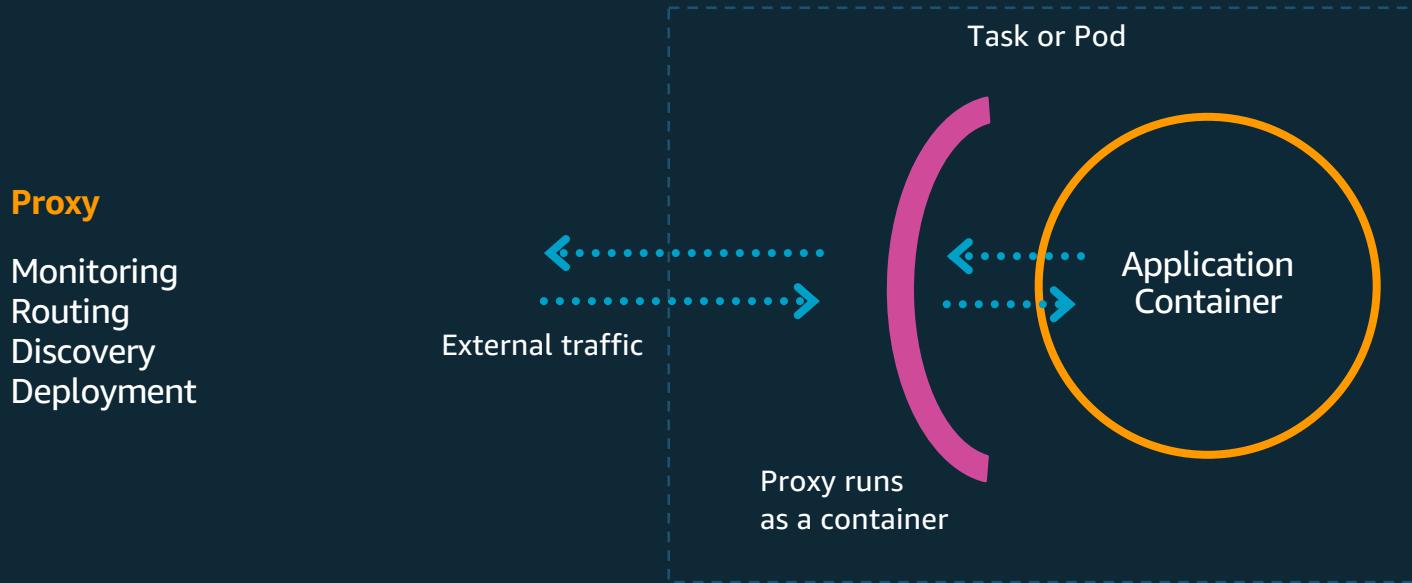
Java
Scala
Node.js
Python
C++
Django
.NET
GO
...

**Sidecar
to
the
rescue!**



Photo credits: hiconsumption.com

Option 2: side-car proxy

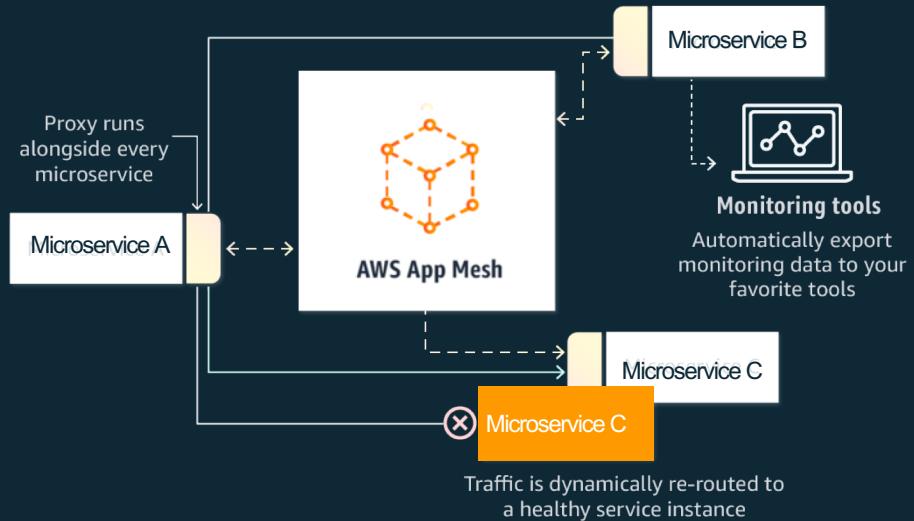




AWS App Mesh

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 EKS



Amazon ECS



AWS App Mesh



AWS Fargate

Amazon EC2

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` !

The image features six cartoon gophers arranged horizontally, each wearing glasses and holding a letter above their head. From left to right, the gophers are: E (brown fur, bow tie), K (blue fur, mustache, Kubernetes logo on chest), S (green fur, bow tie), C (pink fur, bow tie, star on chest), T (purple fur, red glasses, holding a drink), and L (brown fur, bow tie, heart on chest).

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.

eksctl, the declarative way

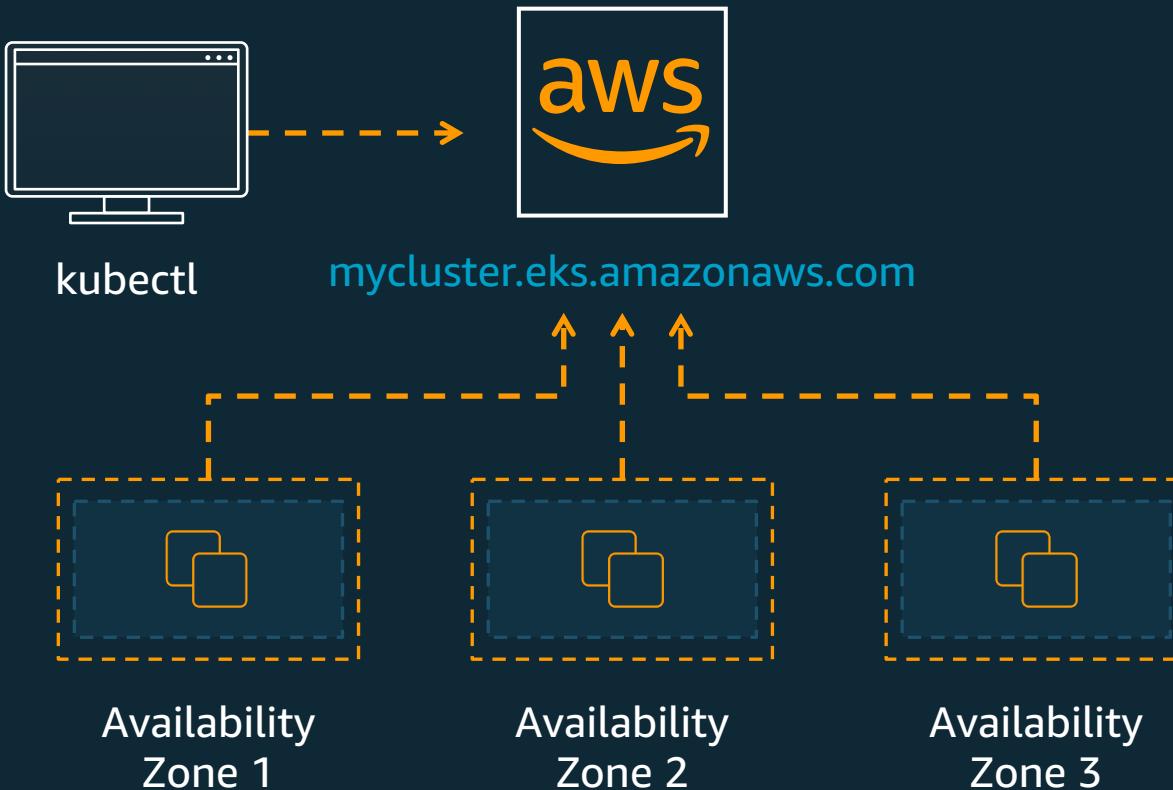
```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

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
```



Demo

App Mesh uses Envoy proxy



OSS project

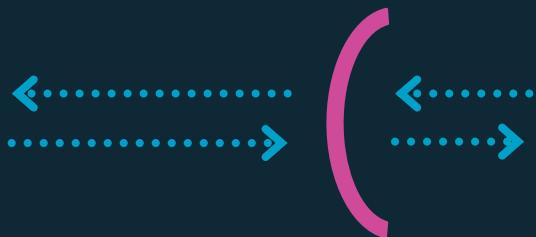
Wide community support, numerous integrations

Stable and production-proven

"Graduated Project" in Cloud Native Computing Foundation

Started at Lyft in 2016

Protocol level observability (Layer 7)



Logging
generates access logs

Prometheus Exporter
Listens on tcp/9090

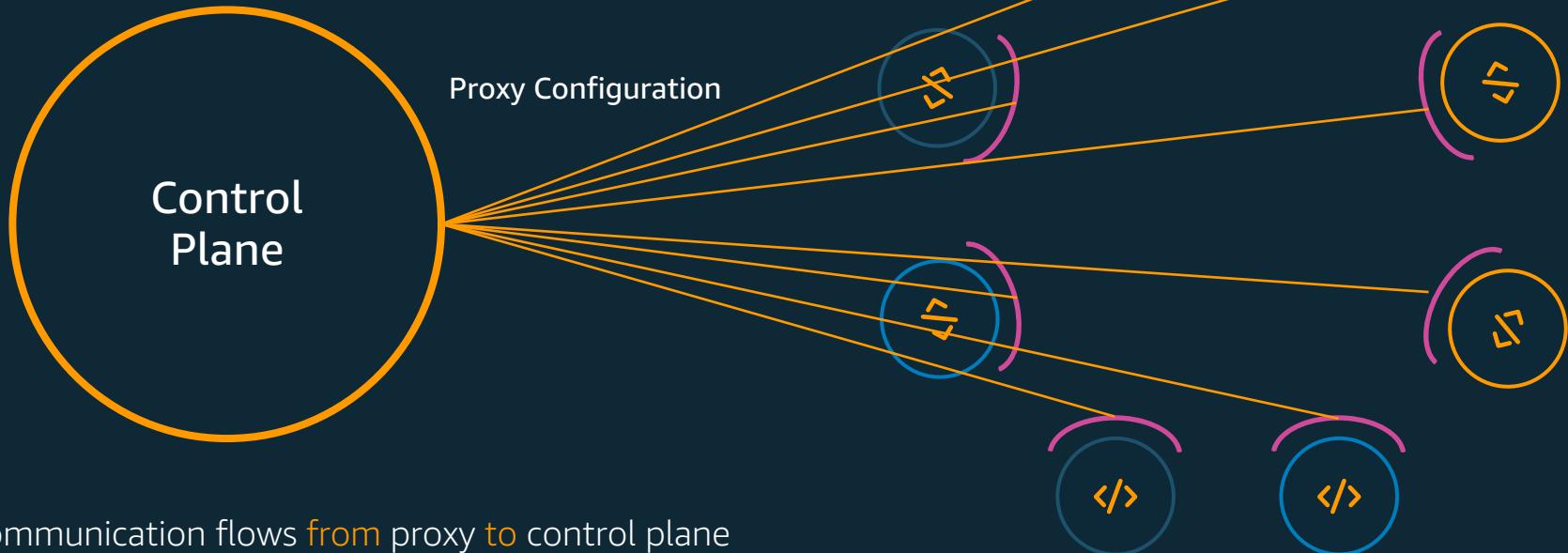
StatsD
Sends metrics to a StatsD server

Amazon X-Ray
forwards traces to AWS

Integrations with

Datadog, Alcide, HashiCorp, Sysdig, SignalFx, Spotinst, Tetrate, Neuvector, Weaveworks, Twistlock, Wavefront by VMware, Aqua.

Control Plane

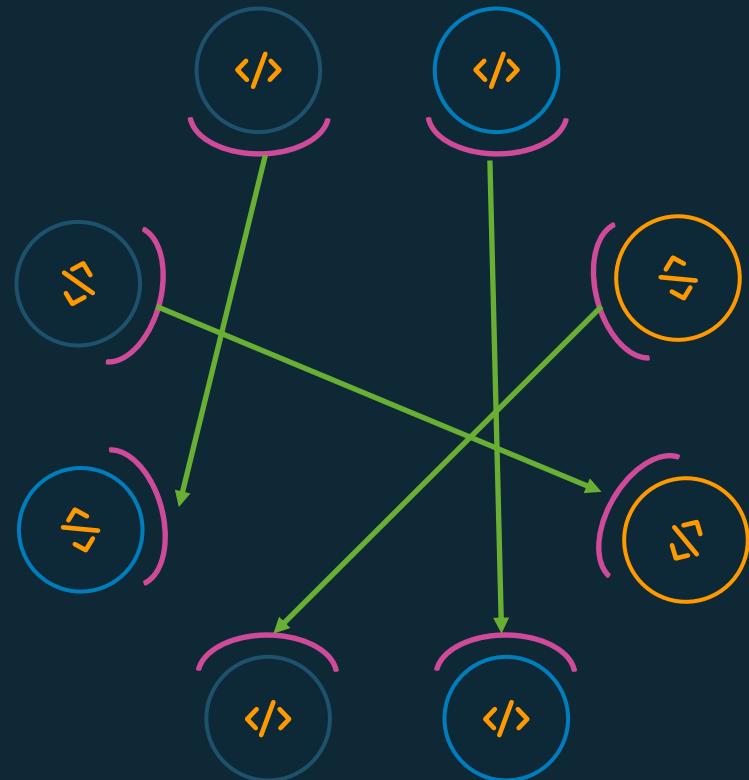


Communication flows from proxy to control plane

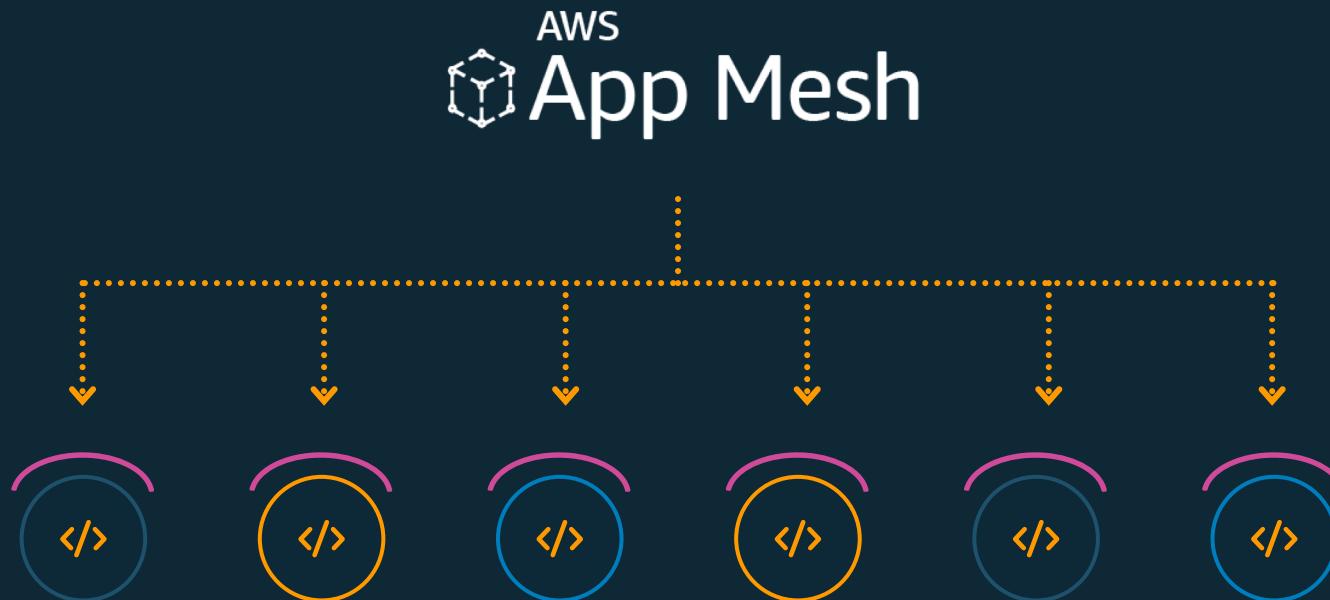
Uses Envoy xDS protocol over GRPC

https://github.com/envoyproxy/data-plane-api/blob/master/xds_protocol.rst

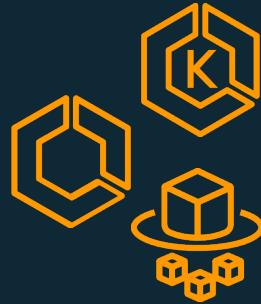
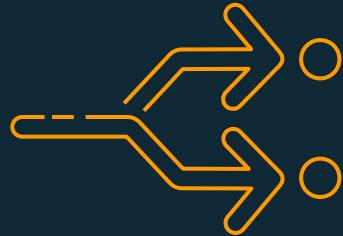
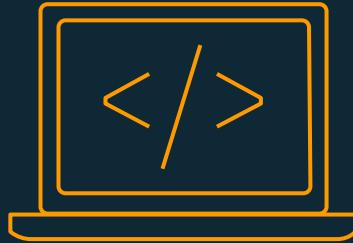
Data Plane



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

\$0

Roadmap

github.com/aws/containers-roadmap

aws / containers-roadmap

Watch 339 ⭐ Star 1,291 Fork 29

Code Issues 202 Pull requests 0 Projects 1 Insights

containers-roadmap Updated 2 days ago

Filter cards Fullscreen Menu

19 Researching

- [ECS] ECS Development in IntelliJ, PyCharm, and Visual Studio Code #272 opened by cbbarclay **ECS Fargate Proposed**
- How to run "docker exec..." command in ECS #187 opened by shaib-tarams **Fargate Proposed**
- [ECS] [RFC]: Automated instance termination protection management #257 opened by coultn **ECS**
- [EKS]: Managed Cluster Addons #252 opened by tabern **EKS**
- [EKS] [Requesting Feedback] Support for Deploying to Kubernetes from CloudFormation #254 opened by christopherhein **EKS Under consideration**
- [EKS] Install AWS-Service-Operator on master nodes #47 opened by JordanDeBeer **EKS Proposed**
- [EKS] Install AWS EBS CSI Driver as Part of EKS cluster creation

37 We're Working On It

- [ECS] [CloudFormation]: CloudFormation support for SystemControls #96 opened by talawahitech **ECS Proposed**
- [ECS] [CloudFormation]: CloudFormation Support for ipcMode (TaskDefinition) #286 opened by joeinnyc **ECS Proposed**
- [Fargate/ECS] [request]: Fargate in EU (Stockholm) #280 opened by raelahame **Fargate Proposed**
- [ECS] [RFC]: Automatic management of instance draining in an ASG #256 opened by coultn **ECS**
- [ECS] Automatic DRAINING state on spot retirement #190 opened by tyrken **ECS**
- Can't see task level cpu/memory utilization in cloudwatch #106 opened by rutchiwi **ECS Proposed**

11 Coming Soon

- [EKS] [request]: Release CNI v1.5.0 #284 opened by mogren **EKS**
- [ECS] proxyConfiguration UI in the ECS Console #259 opened by coultn **Console ECS Fargate**
- EKS Support for Kubernetes 1.13 #30 opened by uprightvinyl **EKS**
- [ECS] [CloudFormation]: CloudFormation support for Secrets #97 opened by talawahitech **ECS Fargate Proposed**
- [Fargate, ECS] [CloudFormation]: Support for tags in CloudFormation #93 opened by iconara **ECS Fargate Proposed**
- ECS ENI Density Increases #7 opened by abby-fuller **ECS**
- [ECS] [CloudFormation]: CloudFormation support for GPUs in a resourceRequirements field #223 opened by Inethertron **ECS**

3 Developer Preview

- EKS Windows Nodes (preview) #69 opened by ofiliz **Developer Preview EKS**
- [EKS]: Support for Arm Nodes - EC2 A1 Instances #264 opened by tabern **Developer Preview EKS**
- [EKS] [request]: Release CNI Plugin 1.4 for EKS #149 opened by mogren **EKS**

48 Just Shipped

- SOC compliance for EKS #296 opened by abby-fuller **EKS**
- EKS: Get-Token CLI Subcommand #292 opened by tabern **EKS**
- Support for Public IP space in VPC with EKS #181 opened by tabern **EKS**
- EKS / Kubernetes: Add support for using AWS Fleet to atlassian/escalator #270 opened by tabern **EKS**
- Control Plane Metrics Endpoint #182 opened by tabern **EKS**
- Fargate Log Driver Support v1 #9 opened by abby-fuller **Fargate**
- Amazon EKS: Deep Learning Benchmarking Utility #275 opened by tabern **EKS**

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

aws / aws-app-mesh-roadmap

Code Issues 47 Pull requests 0 Projects 1 Insights

Watch 62 Star 51 Fork 1

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 ewbankit
- 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 couln 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