Kubernetes as a Foundational Layer of Infrastructure
HELLO, I'M Vicki
Lyft was founded in 2012
375.5M rides in 2017, more than double that in 2018
1B rides total as of Sept 2018
Available to 95 percent of the US population
- 300+ microservices
- 40,000+ EC2 instances
- All on Envoy mesh network
Infrastructure’s goal is to enable and empower
Enabling

● Microservices
● Batch jobs
● ML model training
● R&D / prototyping
Empowering

When does infrastructure get in the way?
When the surface area is too large!
Think cloud API to provision, then configure, then run and healthcheck
So you build some abstractions
But when the surface area is too small, it’s a black box
Kubernetes provides a set of reasonable abstractions for your infrastructure
Going for 100% migration at enterprise scale...
The ecosystem surrounding Kubernetes is young and rapidly evolving.
Challenge

**ark**
Heptio Ark is a utility for managing disaster recovery, specifically for your Kubernetes cluster resources and persistent volumes. Brought to you by Heptio.

- Go  
- 1.8k
- 226

**autoscaler**
Autoscaling components for Kubernetes

- Go  
- 1,180
- 484
- 2k Apache-2.0

**contour**
Contour is a Kubernetes ingress controller for Lyft’s Envoy proxy.

- Go  
- 1.1k
- 128

**k8s-device-plugin**
NVIDIA device plugin for Kubernetes

- Go  
- 282
- 74
- Updated on Aug 22

**kiam**
Integrate AWS IAM with Kubernetes

- Go  
- 276
- 43

**ingress-nginx**
NGINX Ingress Controller for Kubernetes

- Go  
- 3,069
- 1,546
- 1 Apache-2.0

**node-problem-detector**
This is a place for various problem detectors running on the Kubernetes nodes.

- Go  
- 409
- 113
- 2k Apache-2.0
- Updated 18 hours ago

**prometheus**
The Prometheus monitoring system and time series database.

- Go  
- 19.7k
- 2.6k
Internal “Lyft cluster” release process to verify community releases
Work with the community to address rough edges
Challenge

Providing **incremental improvements** instead of pulling the rug from under engineers
Make sure old tooling works with Kubernetes so it’s not a foreign UI
How much Kubernetes do you expose to your users?
What We’re Doing

Have tooling, but also allow access directly to Kubernetes so it’s not a black box
Migrating production traffic safely and confidently
Challenge

- Single request can go through 20-30 services
- Have over 200+ RPC calls in one request
What We’re Doing

Seamless routing between pods and EC2 instances at the networking layer
What We’re Doing

**cni-ipvlan-vpc-k8s**

AWS VPC Kubernetes CNI driver using IPvlan

- cats
- kubernetes
- cni-plugin
- mudkip

- Go
- ⭐ 202
- 🔐 30
- Apache-2.0
- 1 issue needs help
Our pods across all clusters join the same Envoy mesh network as our old stack
What We’re Doing

EC2 Service A

VPC IP: 10.0.0.2

Envoy

K8s Pod

VPC IP: 10.1.0.2

Envoy

Service B

VPC IP: 10.0.0.2
What We’re Doing

Distributed tracing with Envoy

Service A

Envoy

Forward the ot-span-context header.
This is just an id.

Span information.
Big payloads

Trace Collectors

K8s Pod

Envoy

Service B

Distributed tracing with Envoy
At Lyft, we now run our machine learning training and batch jobs on Kubernetes.
Our production traffic is going through both legacy and Kubernetes