



Istio

Your K8S cluster best friend ❤️

@davinkevin



Istio

Le meilleur ami de votre cluster K8S ❤️

@davinkevin



Our world is changing

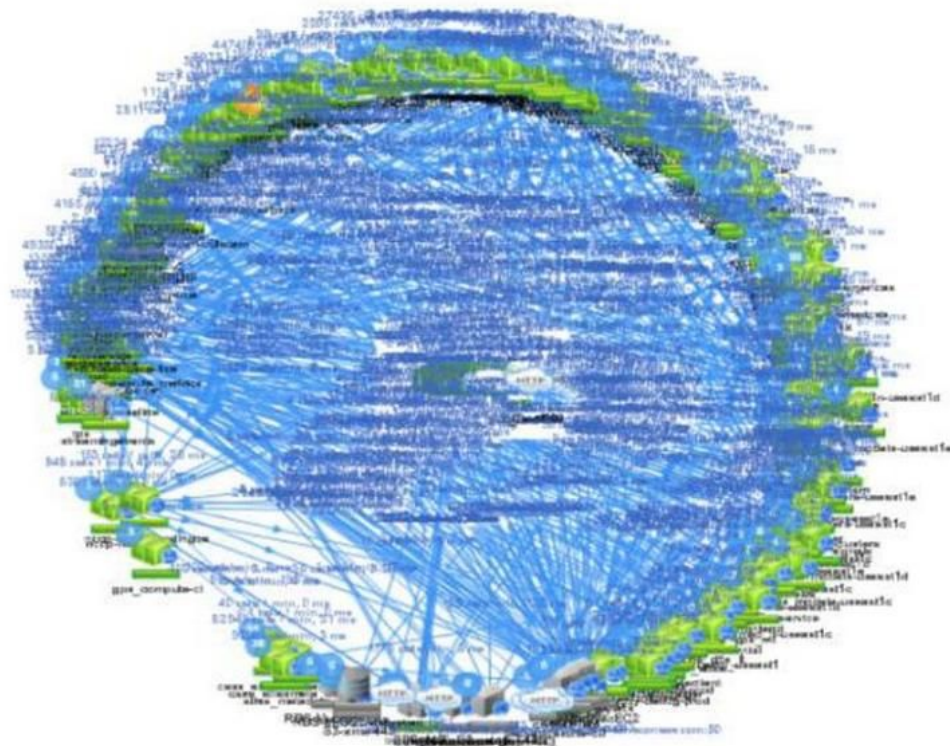
"do-everything"
app



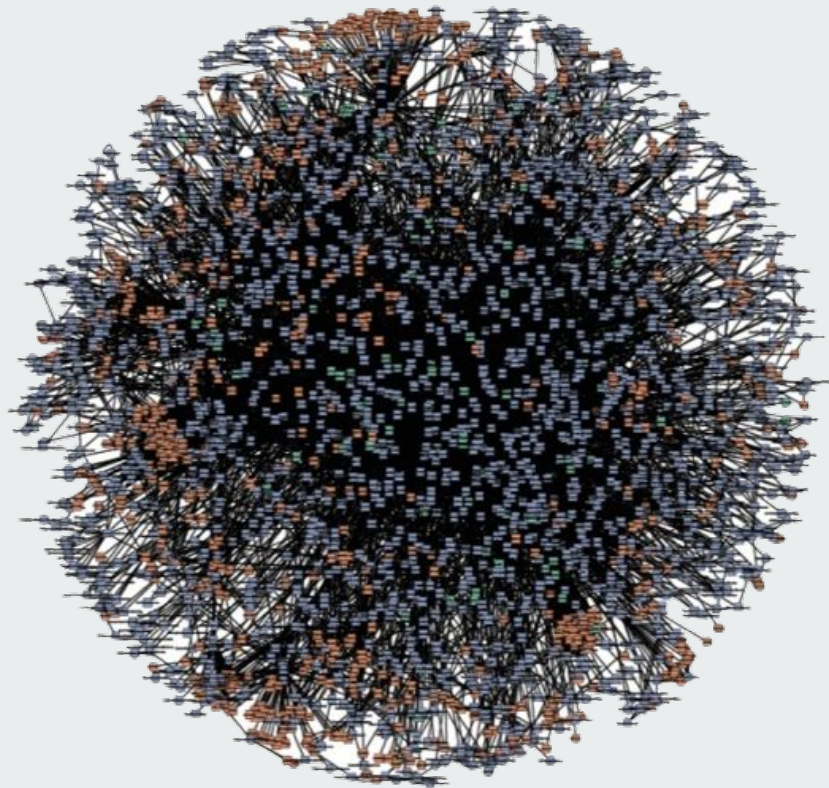




NETFLIX



amazon





Handling this in production is hard



which solves many problems...
but not all of them !





Kevin DAVIN

@davinkevin



Google Developer
Expert



Gitlab Heroes

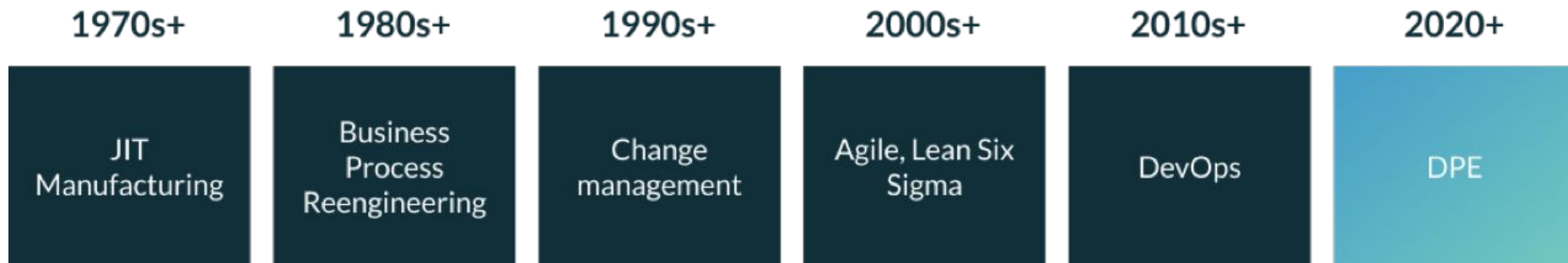




Our mission at **Gradle** is to **accelerate developer productivity** and
make developers happier



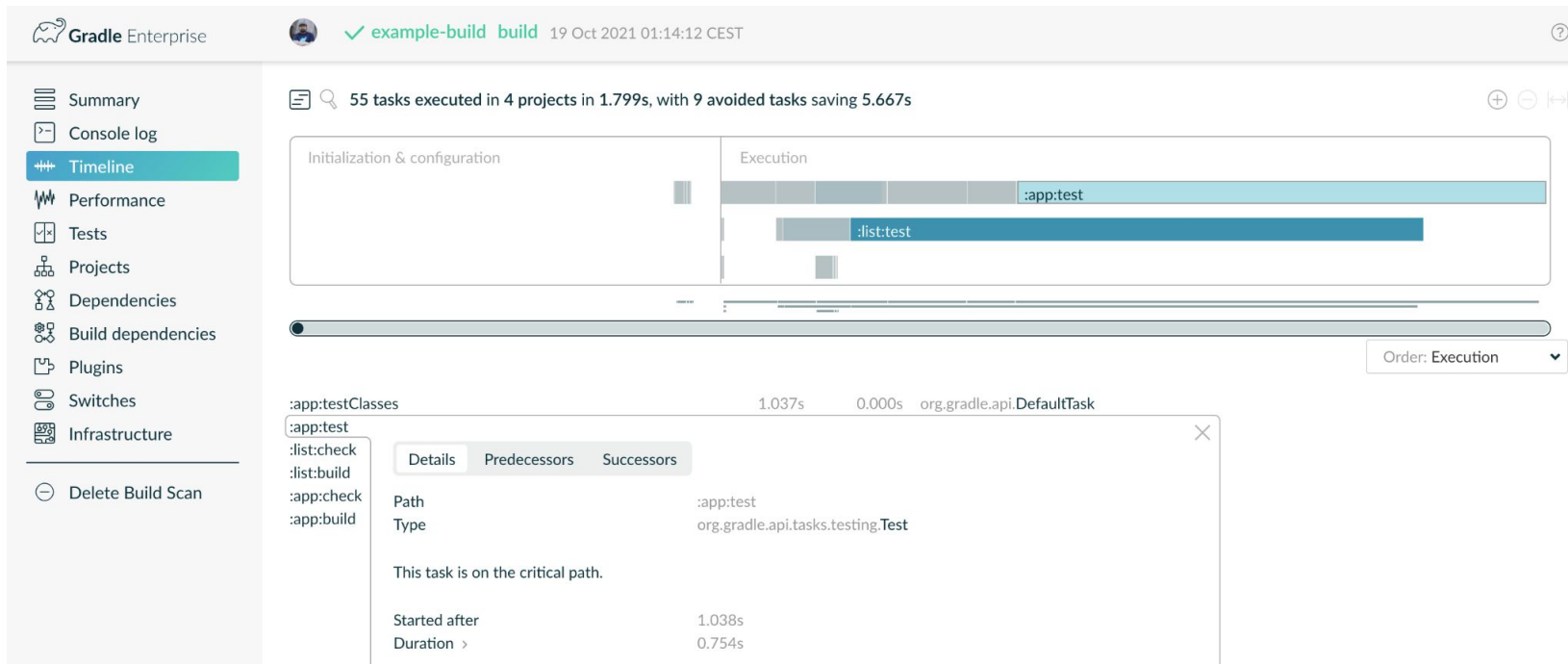
What comes after DevOps?



Developer Productivity Engineering

“If you can’t measure it, you can’t improve it!”

by Peter Drucker



Container



Docker

Kubernetes





Cloud

Istio







Istio



lyft

Google

IBM

Release v0.1.0



Istio

@IstioMesh



Introducing Istio: An open community project to help connect, manage, monitor and secure microservices everywhere.

istio.io/blog/istio-ser...



319 16:03 - 24 mai 2017



258 personnes parlent à ce sujet



> Blog announcement

Release v1.0



> Blog announcement

Release v1.1



Istio
@IstioMesh



Another big day for [#Istio](#) contributors and community!
Istio is now version 1.1 and enterprise-ready. Details on the
blog -

[Traduire le Tweet](#)

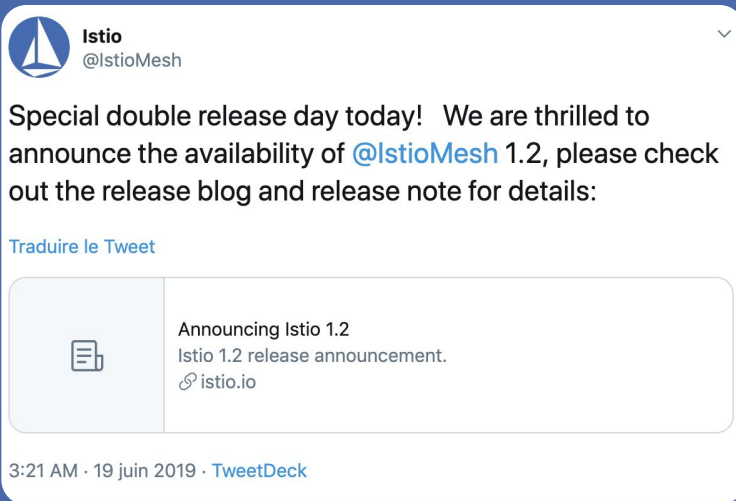


Announcing Istio 1.1
Istio 1.1 release announcement.
[istio.io](#)

9:05 PM · 19 mars 2019 · [TweetDeck](#)

> Blog announcement

Release v1.2.0



> Blog announcement

Release v1.3.0



Istio
@IstioMesh



Super excited to announce our 1.3 release today. The theme of Istio 1.3 is user experience! Please check out release blog and release note for details:

[Traduire le Tweet](#)



Announcing Istio 1.3

Istio 1.3 release announcement.

istio.io

9:12 PM · 12 sept. 2019 · [TweetDeck](#)

76 Retweets **160** J'aime

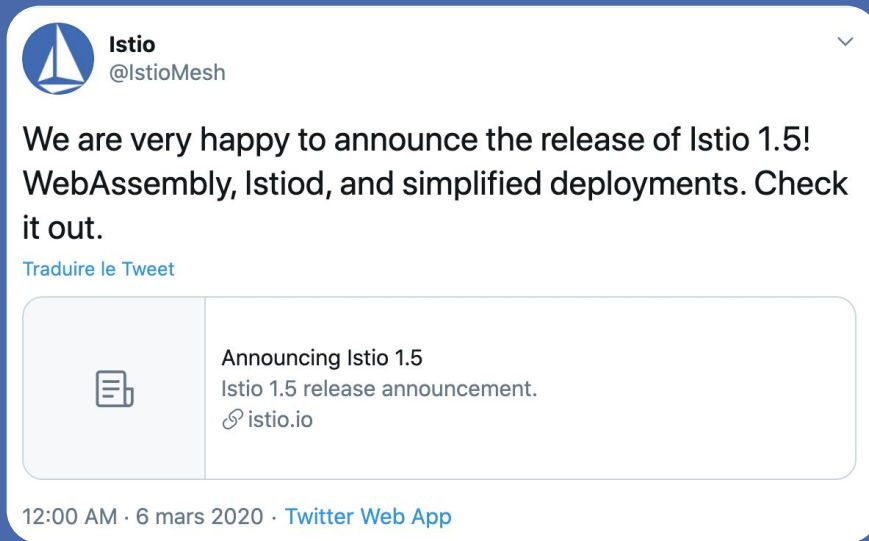
> Blog announcement

Release v1.4.0



> Blog announcement

Release v1.5.0



> Blog announcement

Release v1.6.0



Istio
@IstioMesh



We are happy to announce the availability of Istio 1.6.

With this release, we continue the path toward more simplicity, a better installation experience, and we have added other goodies as well.

Find the details here:

[Traduire le Tweet](#)

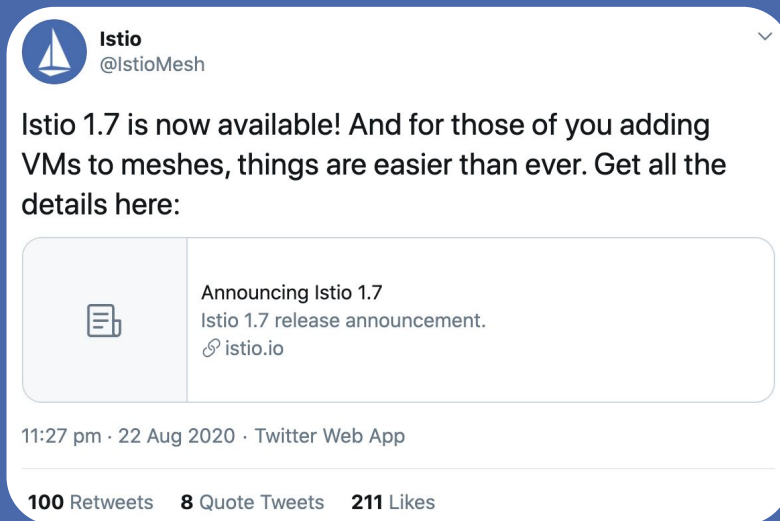


Announcing Istio 1.6
Istio 1.6 release announcement.
istio.io

9:40 PM · 21 mai 2020 · [Twitter Web App](#)

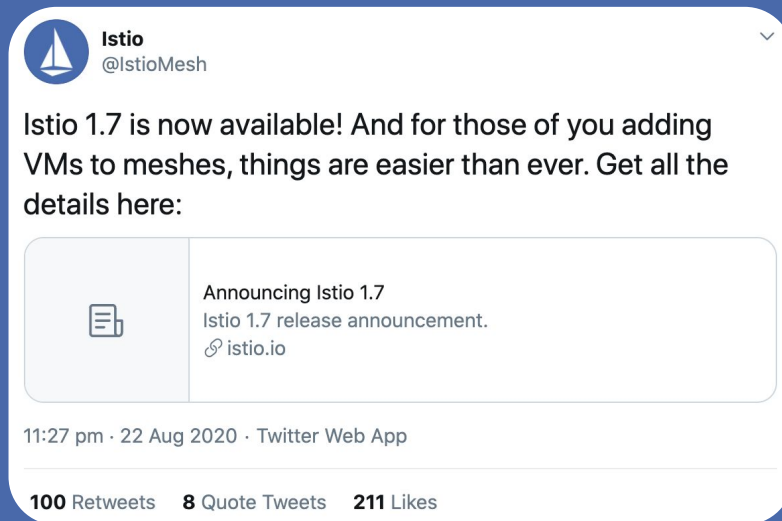
> Blog announcement

Release v1.7.0



> Blog announcement

Release v1.7



> Blog announcement

Release v1.11



> [Blog announcement](#)

Release v1.13



Istio
@IstioMesh

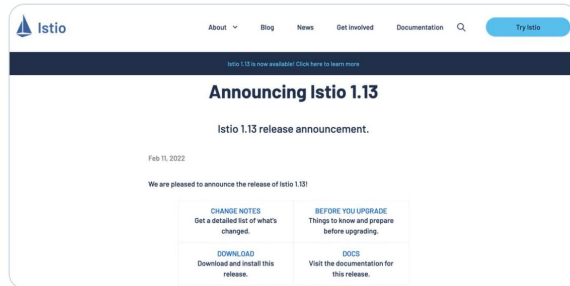
...

Istio 1.13 is out!

Read our news post and release notes to learn about the new features and enhancements.

istio.io/latest/news/re...

[Traduire le Tweet](#)



2:18 AM · 16 févr. 2022 · Tweetbot for Mac

25 Retweets · 2 Tweets cités · 61 J'aime


Young project

(almost) 5 years old





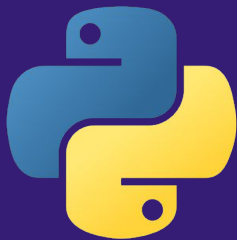
Main goal of Istio ?



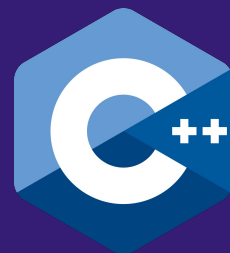
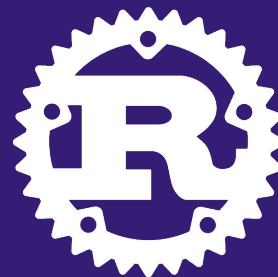
**Writing reliable, loosely coupled,
production-grade applications based
on micro-services**

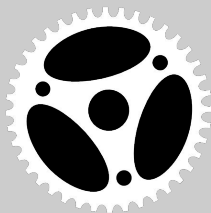


Technology Agnostic 🎉

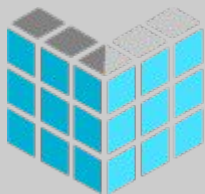
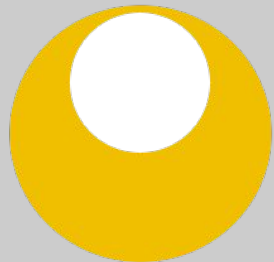


Language

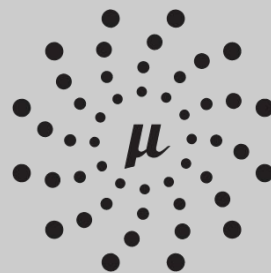




Framework



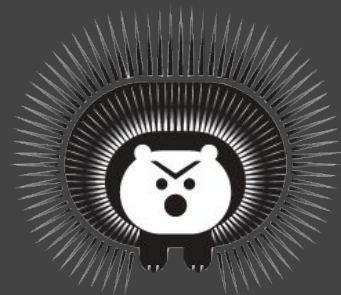
VERT.x

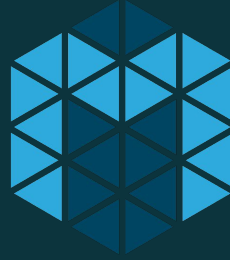
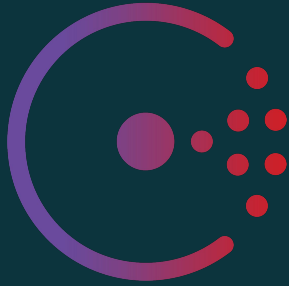
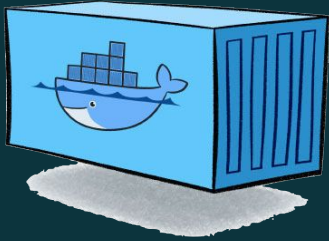


Not only them...

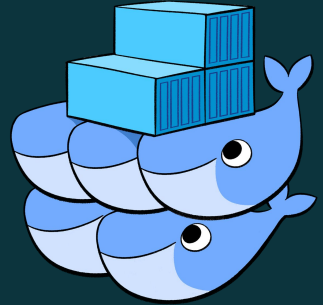


NETFLIX
EUREKA





Infrastructure

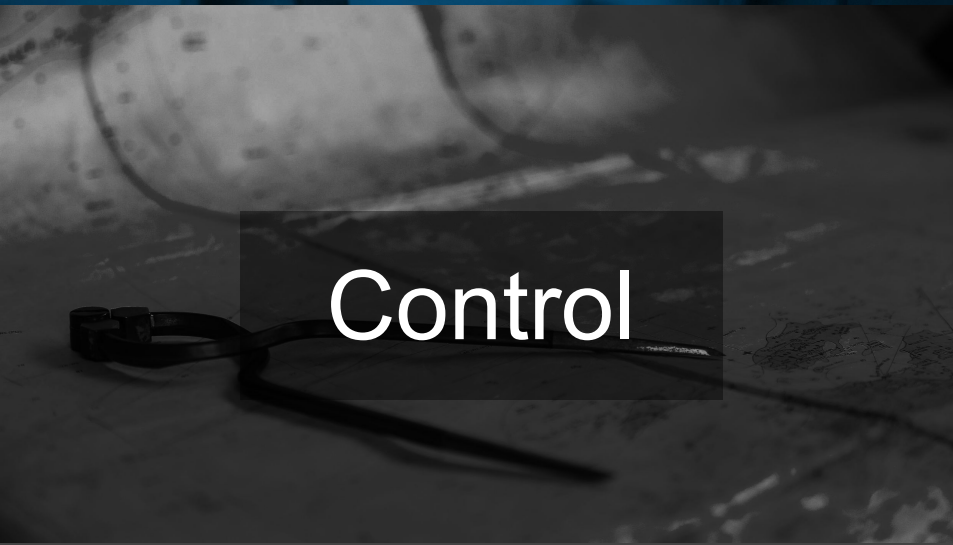




Observability



Connect



Control



Security

**Distributed tools
for distributed
software**



Istio Architecture





Application
concerns

Application

Content transformation, service call orchestration, splitting, aggregating, content routing



Service Mesh

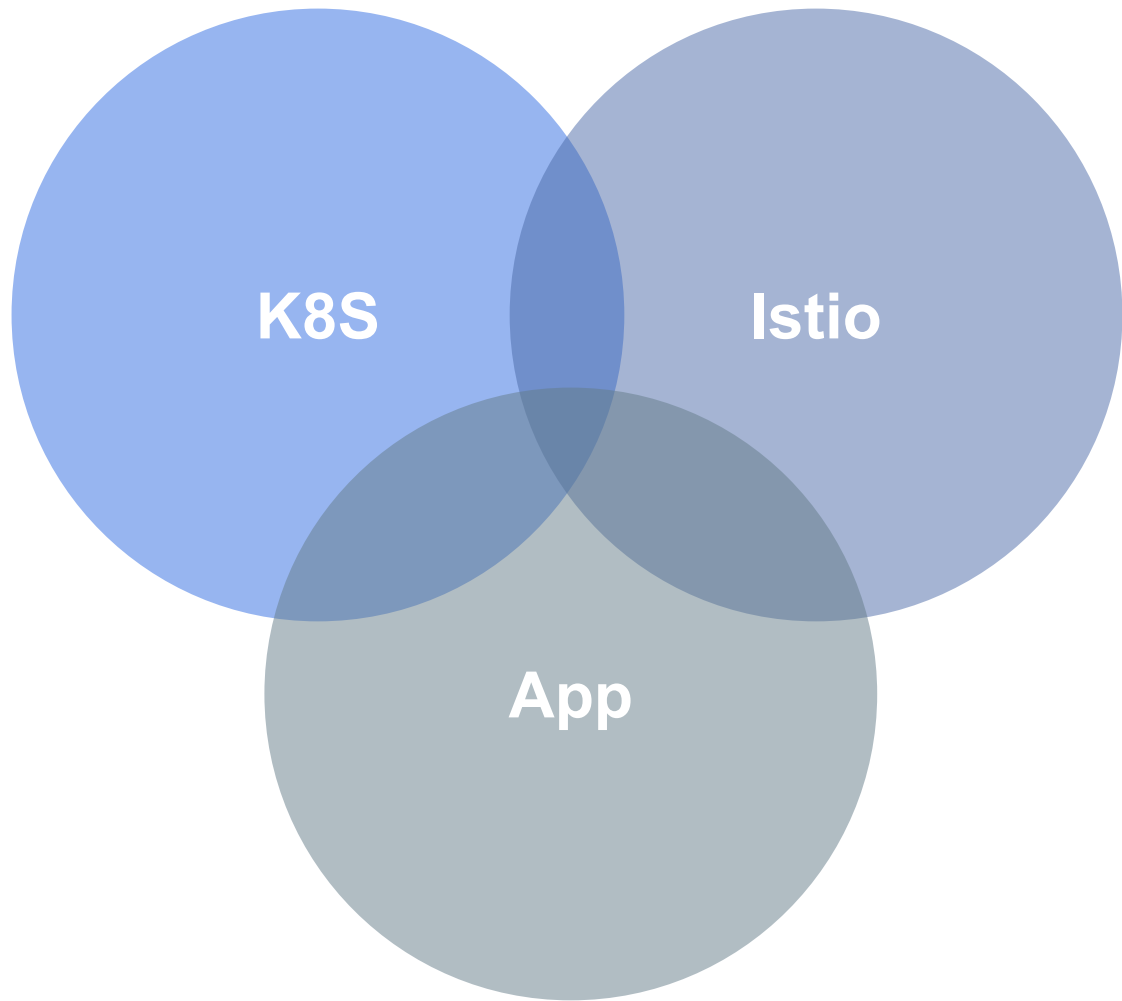
Network resilience, security, policy enforcement, metric collector, load balancing...



Infrastructure
concerns

Deployment Platform

Instance placement, scaling/auto Scaling, resource usage, job scheduling



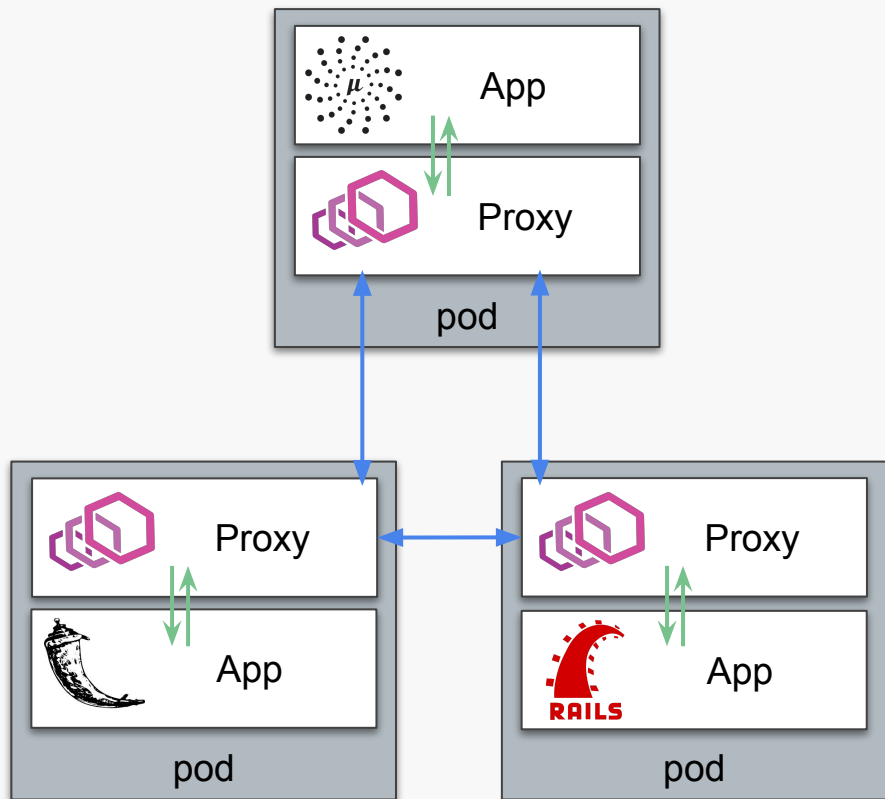
Data Plane



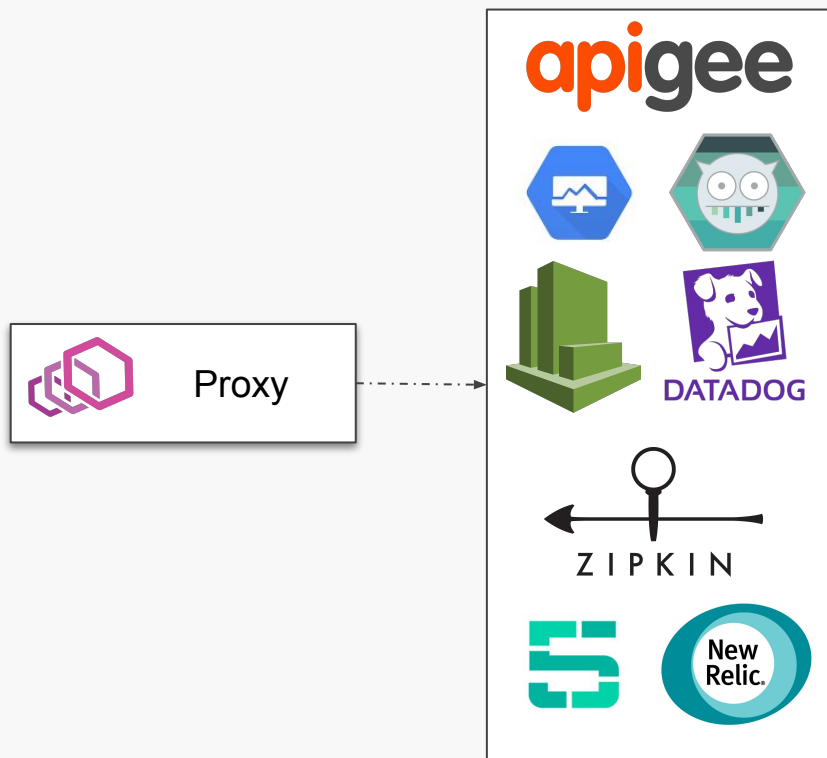
Control Plane



Istio Data Plane



Istio Data Plane



Istio Control Plane

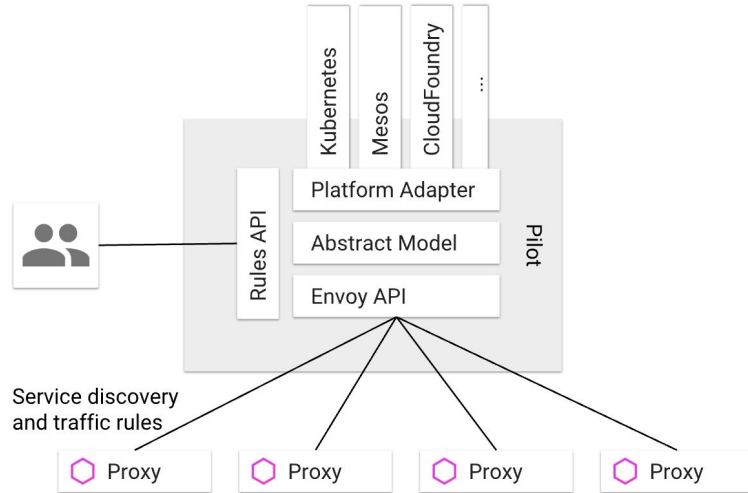


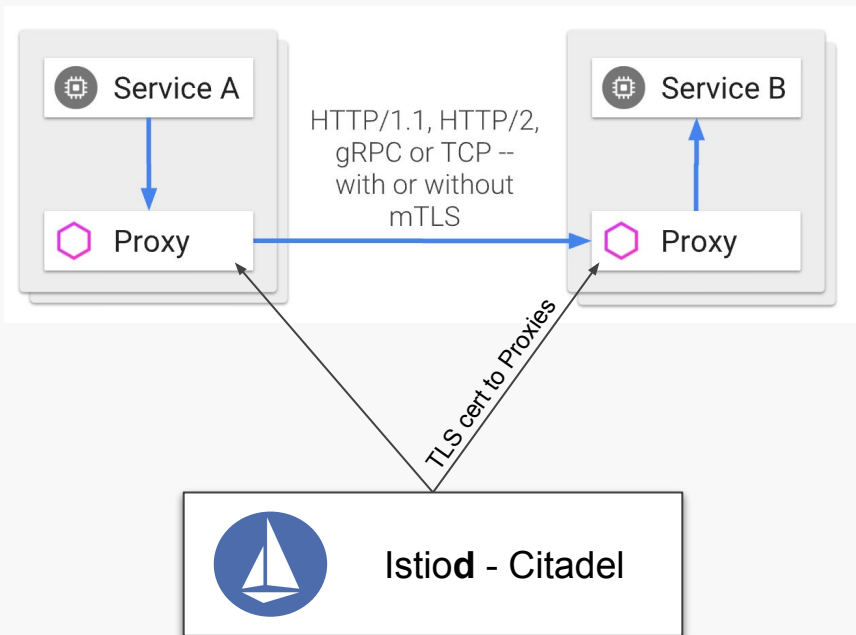
Istiod

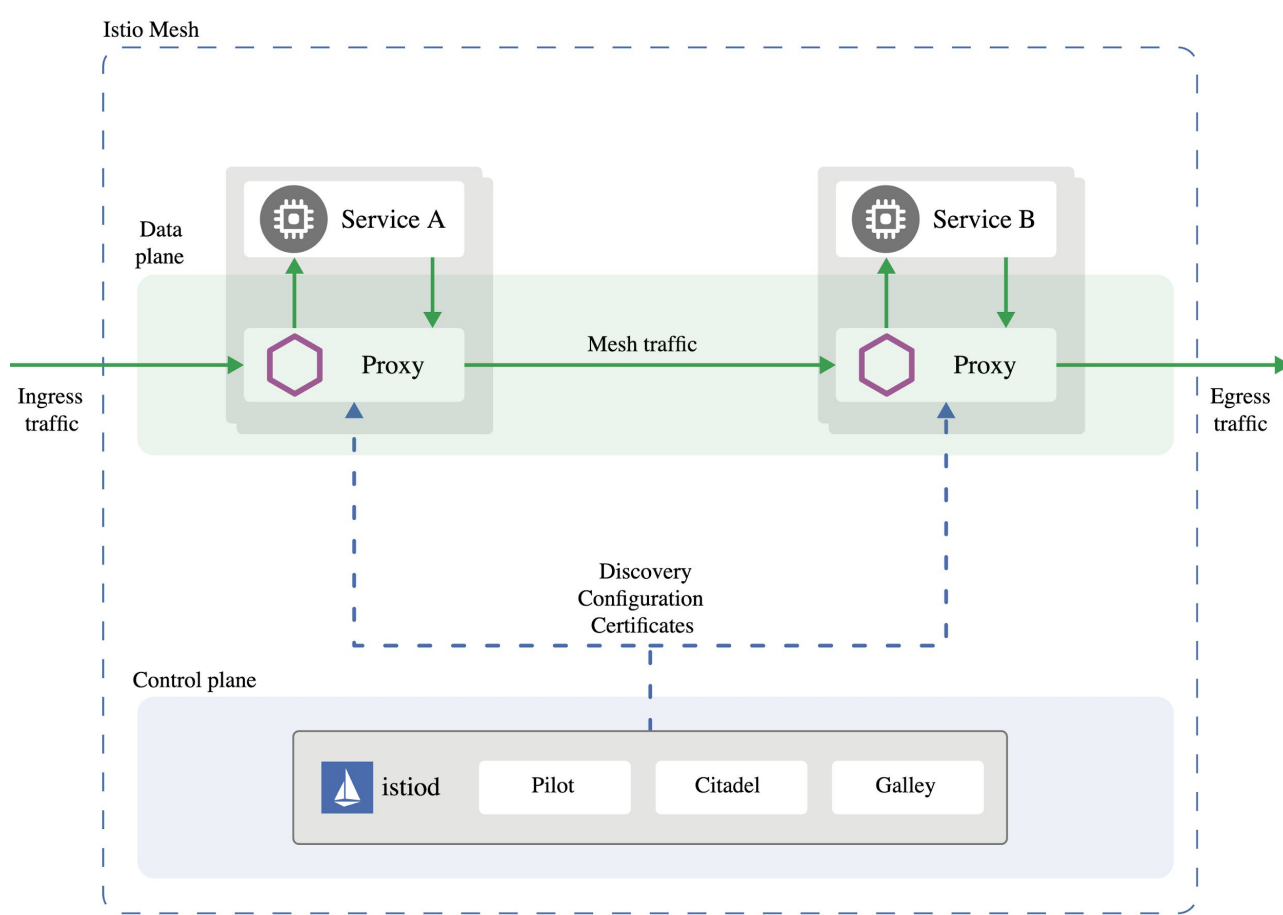




Istiod - Pilot





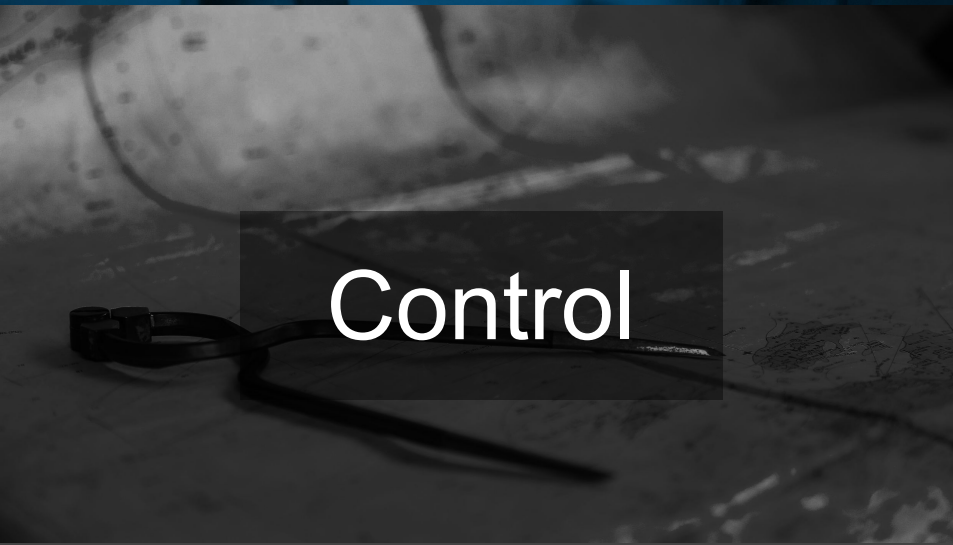




Observability



Connect



Control



Security

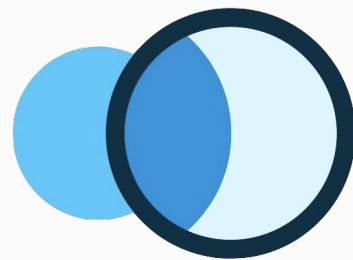
Observability



Observability



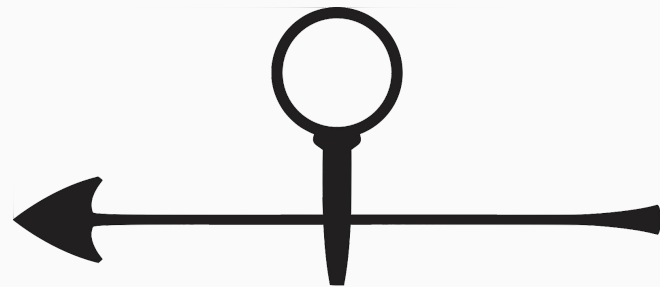
JAEGER



kiali



Grafana



ZIPKIN

Observability

```
class MainHandler(val foo: FooService, val bar: BarService) {  
  
    fun para(request: ServerRequest) = foo  
        .fetch()  
        .zipWith(bar.fetch())  
        .flatMap { ok().syncBody(HelloMessage("Vxd Bucharest 22", "parallel")) }  
  
    fun seq(request: ServerRequest) = foo  
        .fetch()  
        .flatMap { bar.fetch() }  
        .flatMap { ok().syncBody(HelloMessage("Vxd Bucharest 22", "sequential")) }  
  
}
```

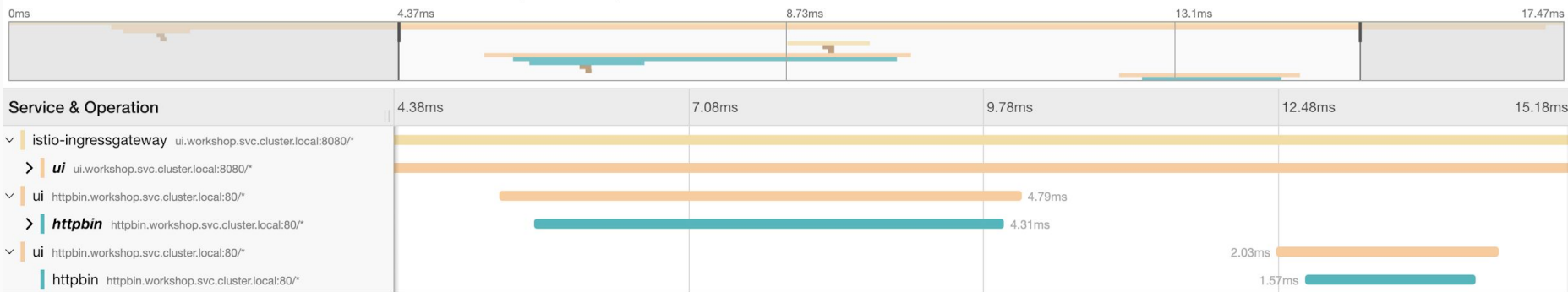

Observability



▼ istio-ingressgateway: ui.workshop.svc.cluster.local:8080/*

[View Options](#) ▼

Trace Start: December 30, 2018 7:18 AM | Duration: 17.47ms | Services: 4 | Depth: 5 | Total Spans: 15



Observability



▼ istio-ingressgateway: ui.workshop.svc.cluster.local:8080/*

[View Options](#) ▼

Trace Start: December 30, 2018 7:18 AM | Duration: 12.34ms | Services: 4 | Depth: 5 | Total Spans: 12



Service & Operation

▼ istio-ingressgateway ui.workshop.svc.cluster.local:8080/*

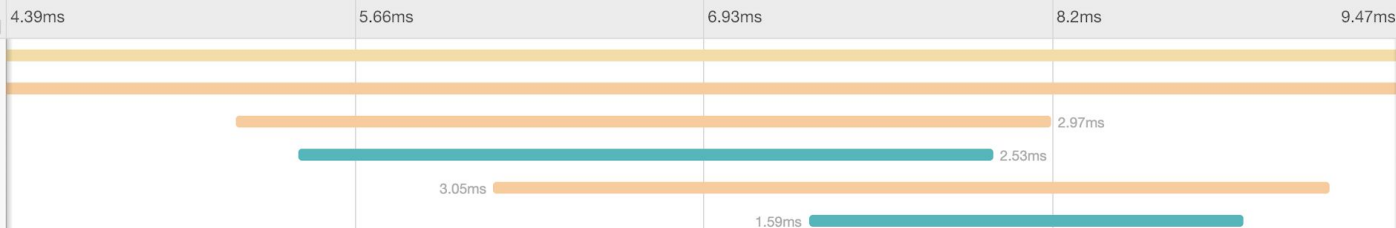
> ui ui.workshop.svc.cluster.local:8080/*

▼ ui httpbin.workshop.svc.cluster.local:80/*

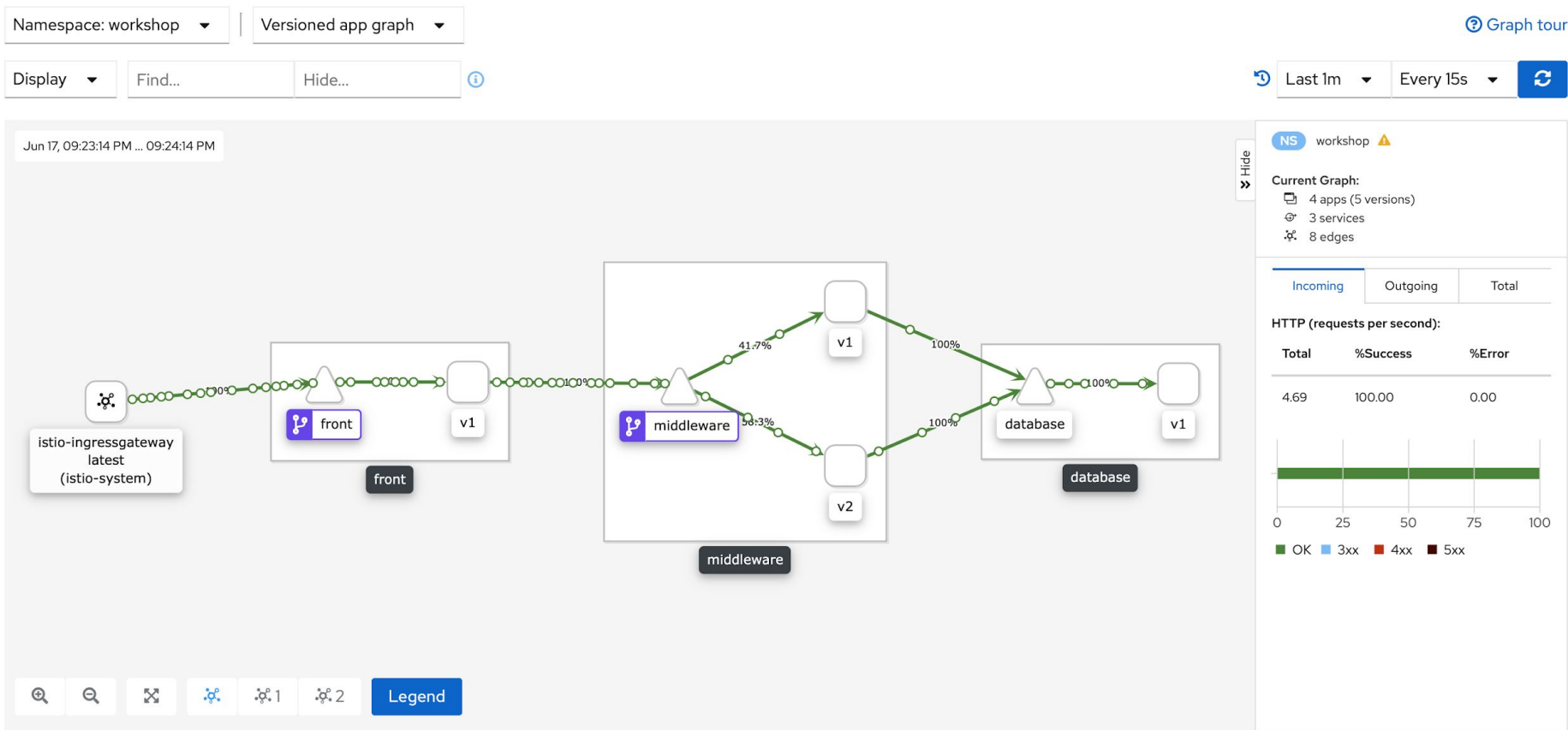
httpbin httpbin.workshop.svc.cluster.local:80/*

▼ ui httpbin.workshop.svc.cluster.local:80/*

httpbin httpbin.workshop.svc.cluster.local:80/*



Observability



Observability



kiali



admin ▾

Overview

Graph

Applications

Workloads

Services

Istio Config

Namespace: workshop ▾

Workloads

Workload Name ▾

Filter by Workload Na...

Last 1m ▾

Every 15s ▾



Name ↑	Namespace ↑	Type ↑	Labels	Health ↑	Details ↑
W database-v1	NS workshop	Deployment	app: database version: v1	✓	
W front-v1	NS workshop	Deployment	app: front version: v1	✓	
W middleware-v1	NS workshop	Deployment	app: middleware version: v1	✓	
W middleware-v2	NS workshop	Deployment	app: middleware version: v2	✓	

Observability

Workloads > Namespace: workshop > middleware-v1

Overview Traffic Logs Inbound Metrics Outbound Metrics

Last 1m



Workload Properties

Name

middleware-v1

Template Labels

app middleware version v1

Type

Deployment

Created at

Jun 7, 09:39 PM

Resource Version

34671

Graph Overview



Health Overview

Overall Health



Healthy

Pod Status



middleware-v1: 1 / 1

Error Rate over 1m



Inbound: 0.00%

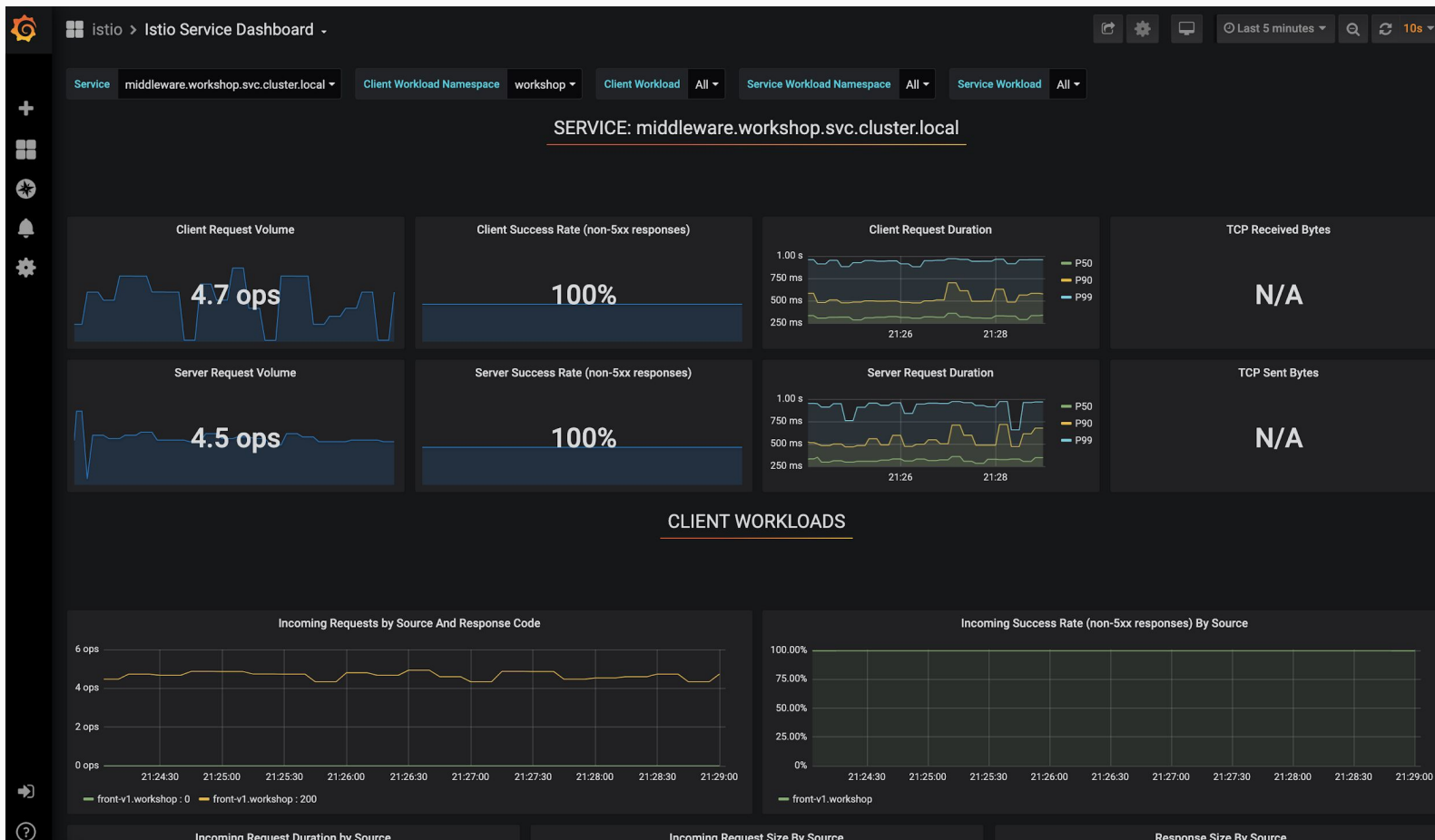


Outbound: 0.00%

Pods (1) Services (1)

Status	Name	Created at	Created by	Labels	Istio Init Containers	Istio Containers	Phase
✓	middleware-v1-76b7c79f66-scq5t	Jun 7, 09:39 PM	middleware-v1-76b7c79f66 (ReplicaSet)	app middleware istio.io/rev default More labels...	docker.io/istio/proxy v2:1.6.0	docker.io/istio/p roxyv2:1.6.0	Running

Observability



Observability



Client Request Volume

155 ops

Client Success Rate (non-5xx responses)

97.2%

Client Request Duration



Server Request Volume

154 ops

Server Success Rate (non-5xx responses)

97.3%

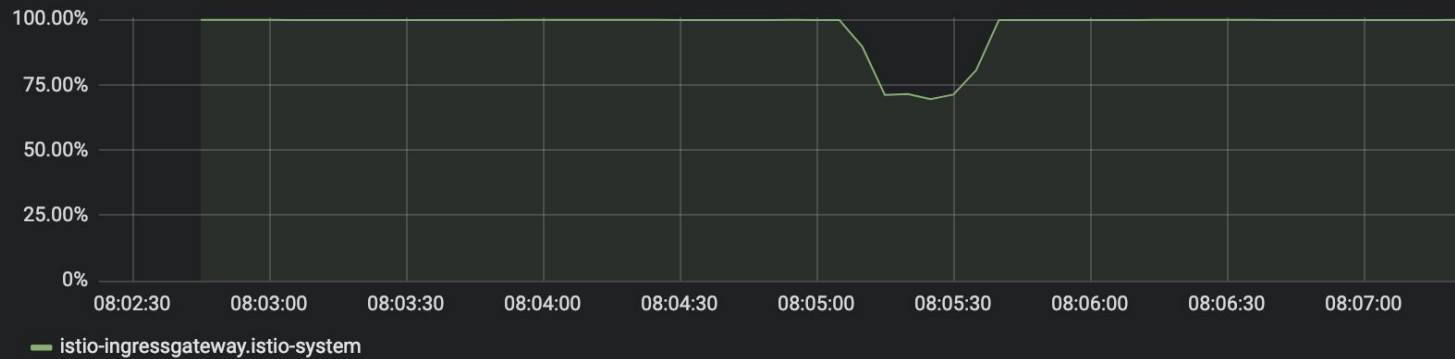
Server Request Duration



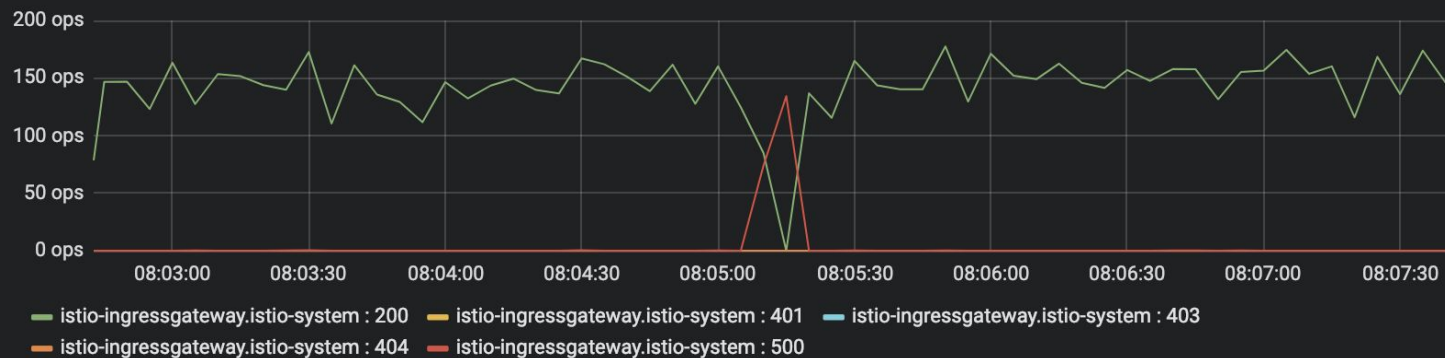
Observability



Incoming Success Rate (non-5xx responses) By Source



Incoming Requests by Source And Response Code



Observability



Connect



more YAML



Virtual Service

VirtualService defines the rules that control **how requests** for a service **are routed** within an Istio service mesh

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - route:
        - destination:
            host: ui
            subset: v1
```


Destination Rule

DestinationRule configures the set of **policies** to be **applied to a request** after VirtualService routing has occurred

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
```

Service Entry

ServiceEntry is commonly used to **enable requests** to services **outside** of an Istio service mesh

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: github-https
spec:
  hosts:
    - api.github.com
  location: MESH_EXTERNAL
  ports:
    - number: 443
      name: https
      protocol: HTTPS
  resolution: DNS
```

Gateway

Gateway configures a load balancer for HTTP/TCP traffic, most commonly operating at the **edge of the mesh** to enable **ingress/egress traffic** for an application

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: ui-gateway
spec:
  selector:
    istio: ingressgateway
  servers:
    - port:
        number: 443
        name: https
        protocol: HTTPS
      hosts:
        - "ui.example.com"
```

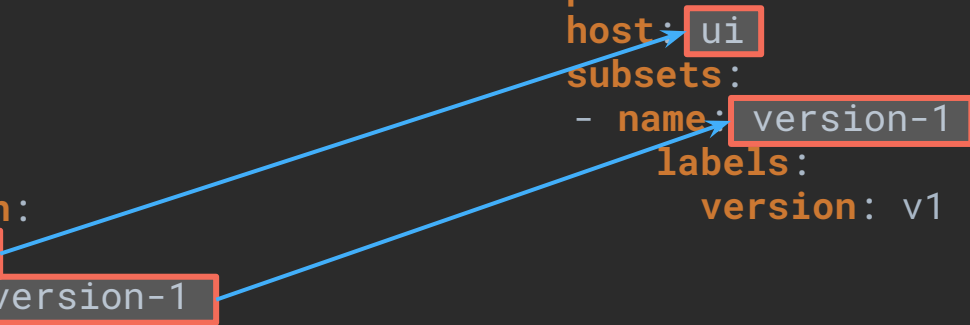

Connect

Virtual Service

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - route:
        - destination:
            host: ui
            subset: version-1
```

Destination Rule

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
  labels:
    version: v1
```



Control





Virtual Service

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - route:
        - destination:
            host: ui
            subset: version-1
```

Destination Rule

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
```

Virtual Service

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - match: {}
      route:
        - destination:
            host: ui
            subset: version-1
```

Destination Rule

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
```

An aerial photograph of a river with a complex, meandering path through a dry, brownish landscape. The river is dark blue, contrasting with the surrounding terrain. The meanders are sharp and frequent, creating a series of loops and curves. The landscape is textured with patches of different shades of brown and tan, suggesting varying vegetation or soil types. A semi-transparent white box is overlaid on the top left of the image, containing the text "Go to Production" flow.

“Go to Production” flow

Traffic Mirroring





Testing in Production

Virtual Service

apiVersion: networking.istio.io/v1alpha3

kind: VirtualService

metadata:

name: ui

spec:

hosts:

 - ui

http:

 - **route:**

 - **destination:**

host: ui

subset: version-1

mirror:

host: ui

subset: version-2-beta

Destination Rule

apiVersion: networking.istio.io/v1alpha3

kind: DestinationRule

metadata:

name: ui

spec:

host: ui

subsets:

 - **name:** version-1

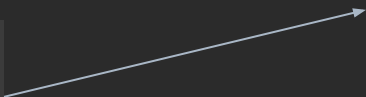
labels:

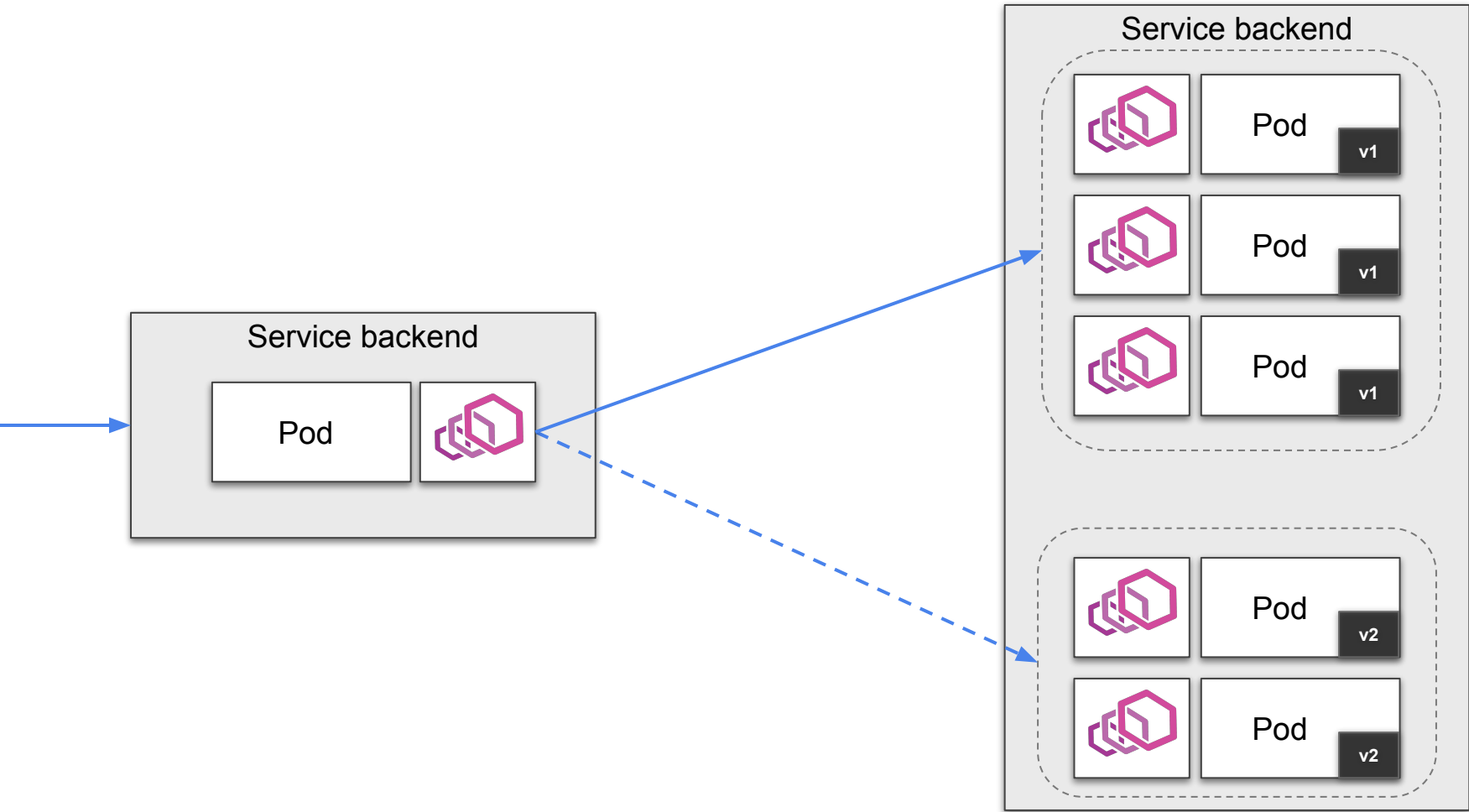
version: v1

 - **name:** version-2-beta

labels:

version: v2



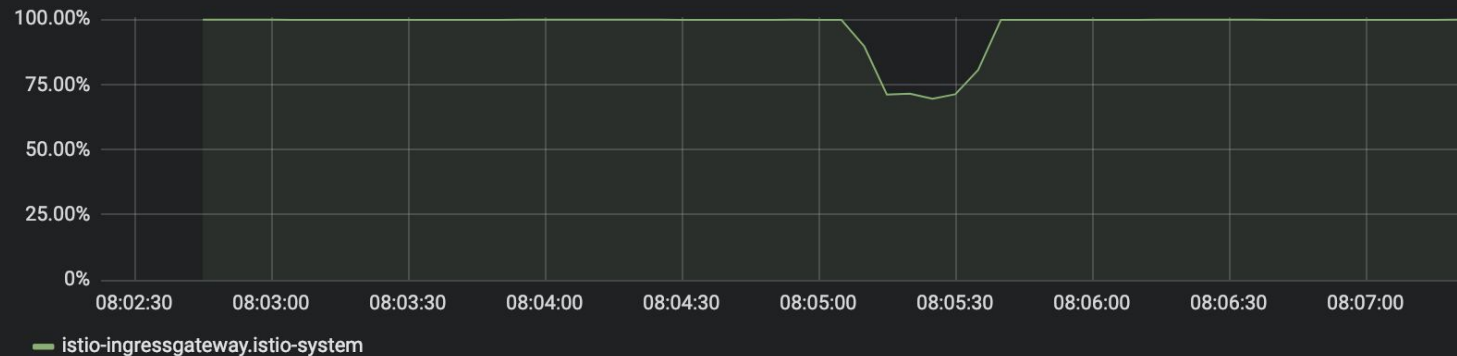




Pod

v2

Incoming Success Rate (non-5xx responses) By Source



Canary Deployment



```
# Virtual Service
```

```
apiVersion: networking.istio.io/v1alpha3
```

```
kind: VirtualService
```

```
metadata:
```

```
  name: backend
```

```
spec:
```

```
  hosts:
```

```
    - ui
```

```
  http:
```

```
    - route:
```

```
      - destination:
```

```
        host: ui
```

```
        subset: version-1
```

```
    - match:
```

```
      headers:
```

```
        version:
```

```
          exact: beta
```

```
      route:
```

```
    - destination:
```

```
      host: ui
```

```
      subset: version-2-beta
```

```
# Destination Rule
```

```
apiVersion: networking.istio.io/v1alpha3
```

```
kind: DestinationRule
```

```
metadata:
```

```
  name: ui
```

```
spec:
```

```
  host: ui
```

```
  subsets:
```

```
    - name: version-1
```

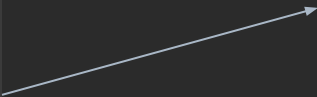
```
      labels:
```

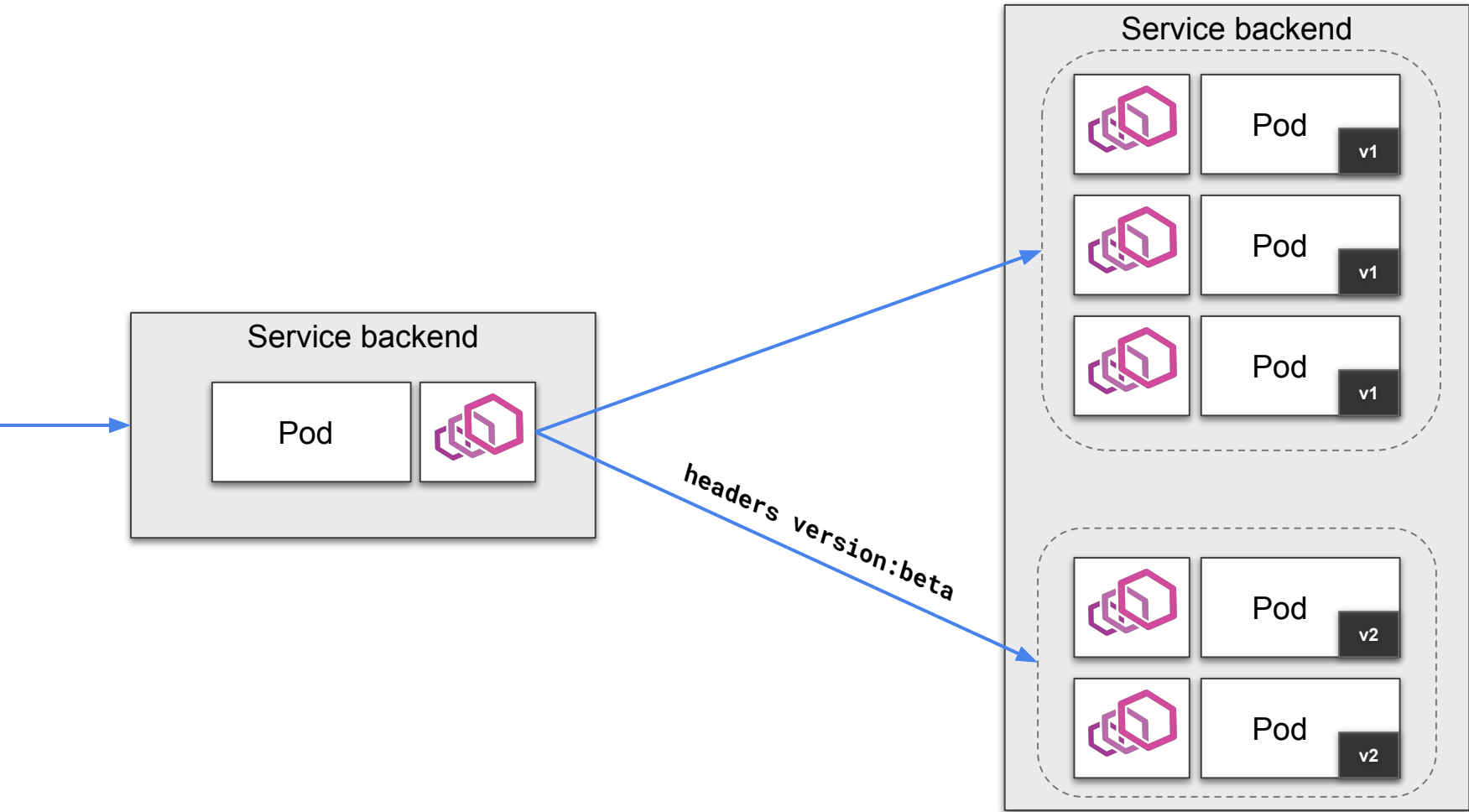
```
        version: v1
```

```
    - name: version-2-beta
```

```
      labels:
```

```
        version: v2
```





Virtual Service

apiVersion: networking.istio.io/v1alpha3

kind: VirtualService

metadata:

name: backend

spec:

hosts:

- ui

http:

- **route:**

- **destination:**

host: ui

subset: version-1

- **match:**

headers:

version:

exact: beta

route:

- **destination:**

host: ui

subset: version-2-beta

Destination Rule

apiVersion: networking.istio.io/v1alpha3

kind: DestinationRule

metadata:

name: ui

spec:

host: ui

subsets:

- **name:** version-1

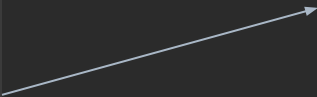
labels:

version: v1

- **name:** version-2-beta

labels:

version: v2



HTTPMatchRequest

URI | Scheme | Method | Authority

Headers | Ports | SourceLabels

Gateways

```
# Virtual Service
...
http:
  - match:
      headers:
        version:
          exact: beta
      uri:
        prefix: /foo/bar
      scheme:
        prefix: http.*
      method:
        regex: (GET|POST)
    route:
...

```




Canary for 1 client



141.0.205.122

```
# Virtual Service
```

```
...
```

```
  http:
```

```
    - match:
```

```
      headers:
```

```
        x-forwarded-for:
```

```
          exact: 141.0.205.122
```

```
      route:
```

```
...
```



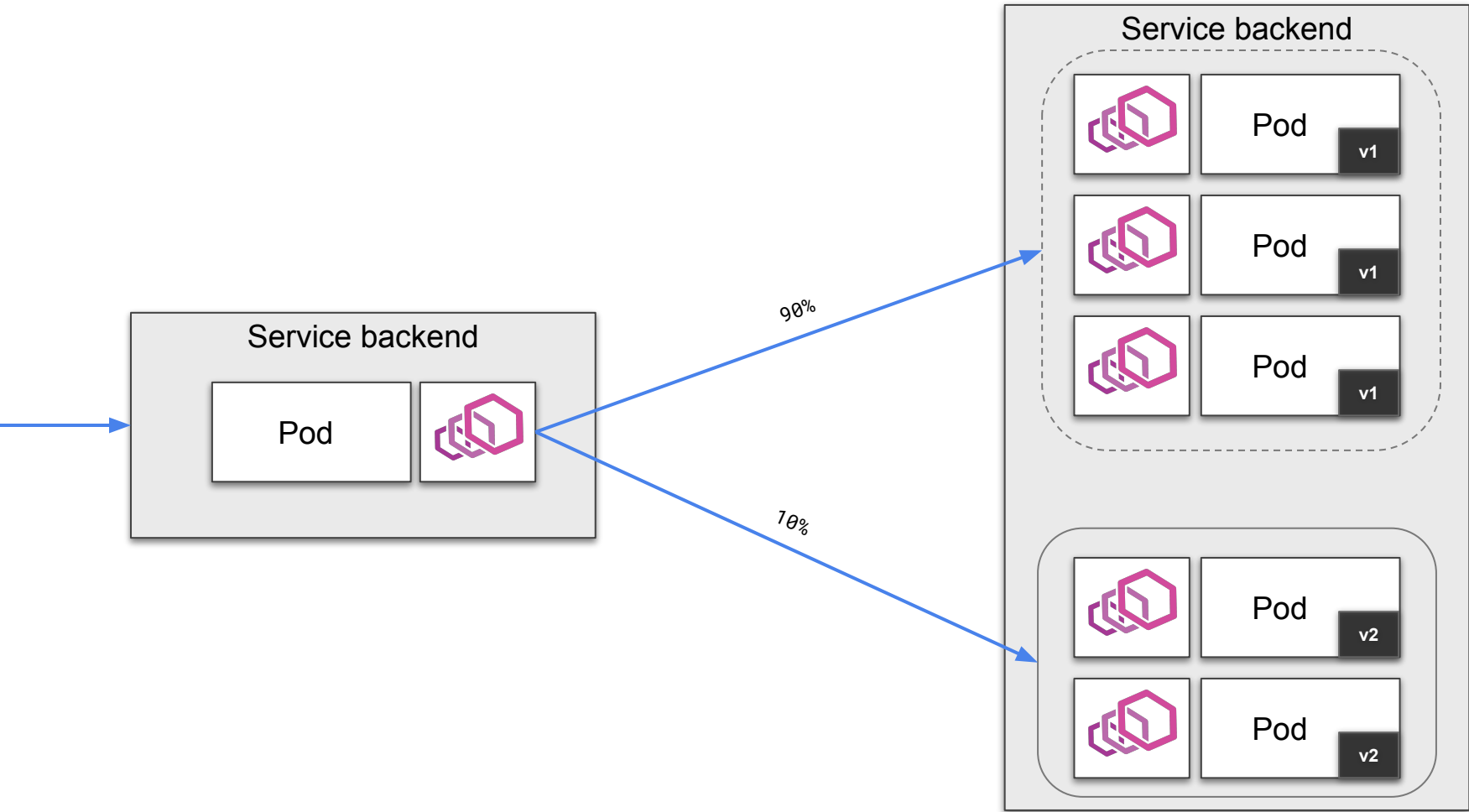

Traffic Splitting

Virtual Service

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - route:
        - destination:
            host: ui
            subset: version-1
            weight: 90
        - destination:
            host: ui
            subset: version-2-beta
            weight: 10
```

Destination Rule

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
    - name: version-2-beta
      labels:
        version: v2
```

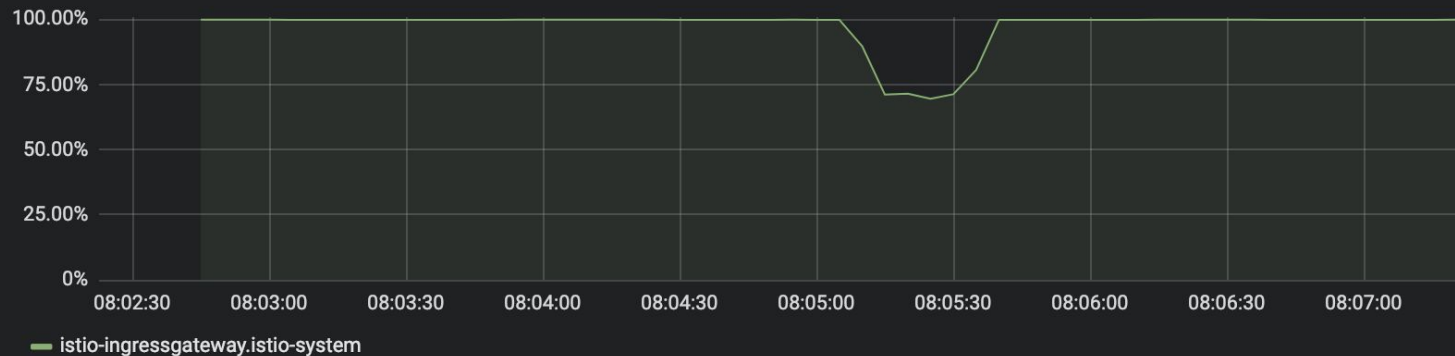


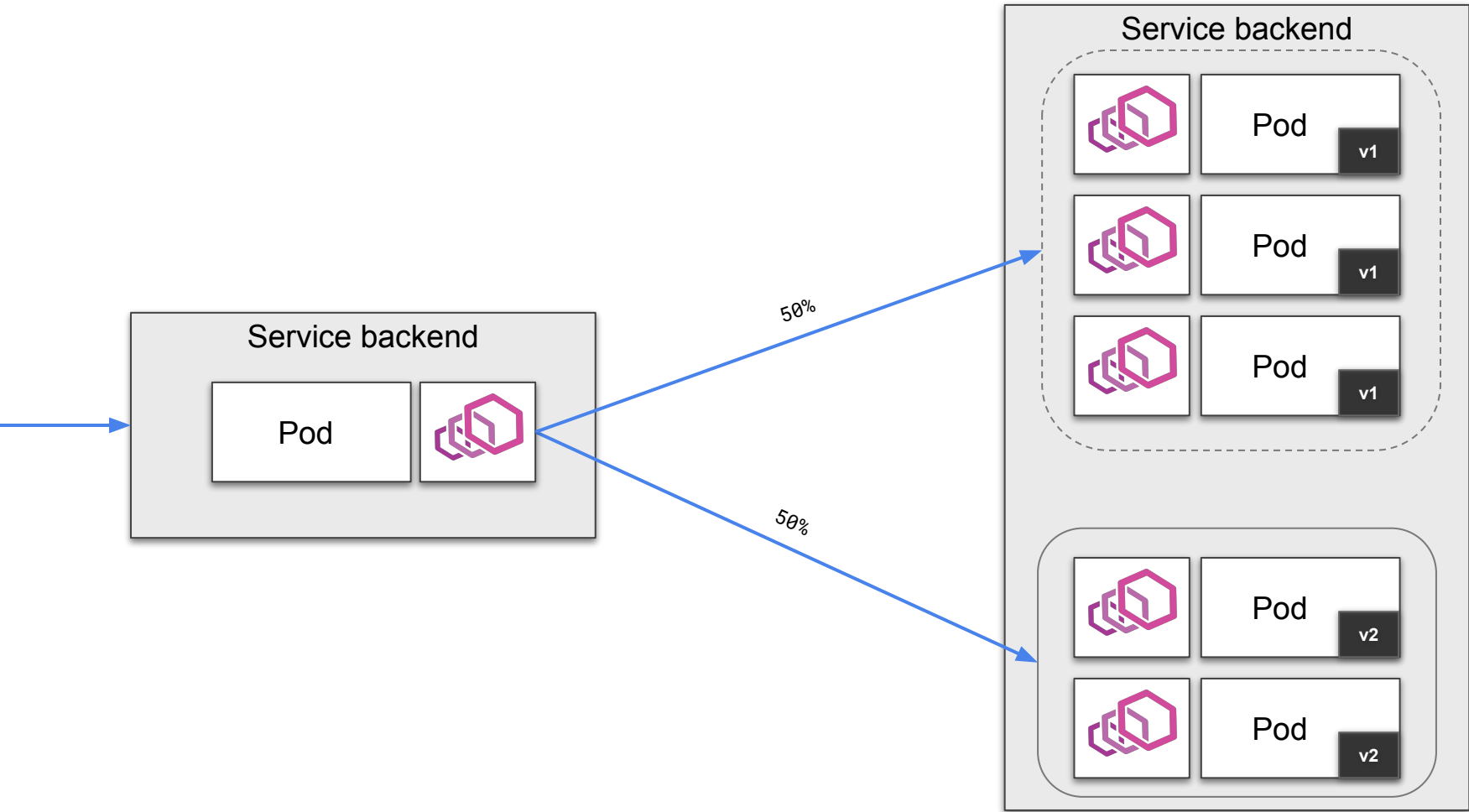


Pod

v2

Incoming Success Rate (non-5xx responses) By Source





Virtual Service

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - route:
        - destination:
            host: ui
            subset: version-1
            weight: 0
        - destination:
            host: ui
            subset: version-2-beta
            weight: 100
```

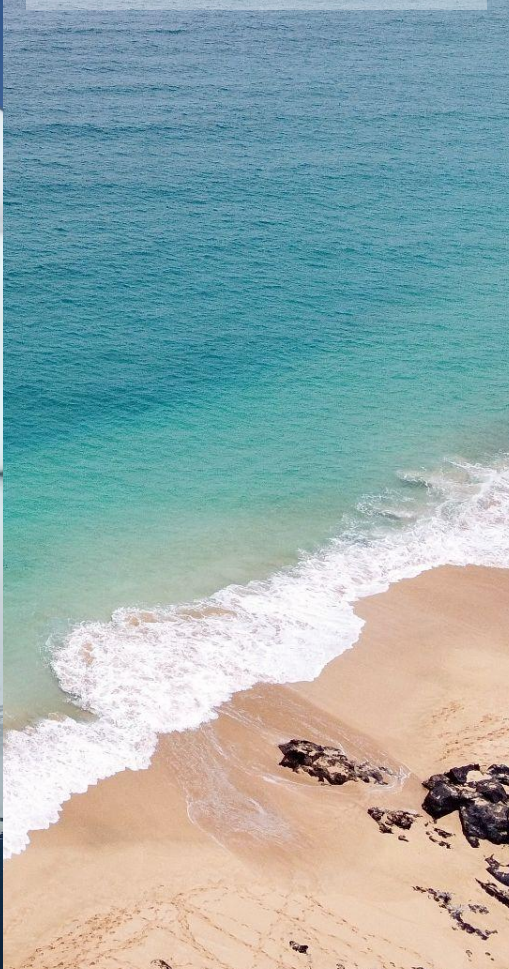
Destination Rule

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
    - name: version-2-beta
      labels:
        version: v2
```

Mirroring



Canary



Splitting



Release



Release without any downtime



Be resilient, any time !

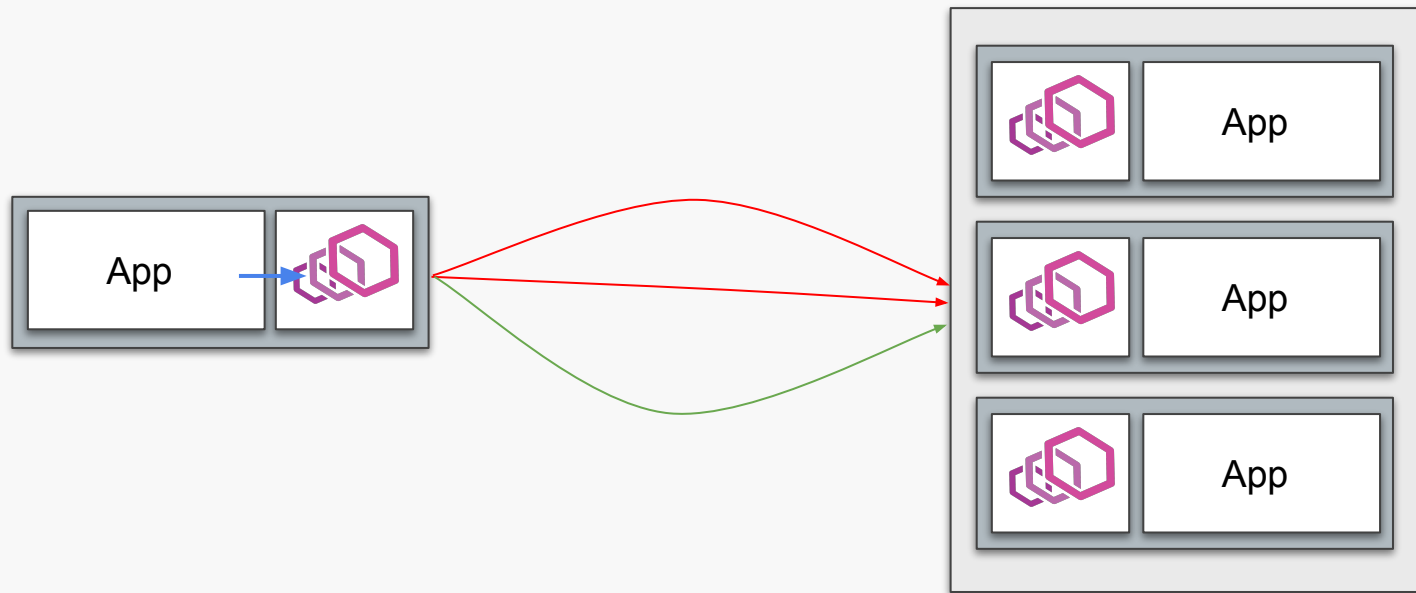


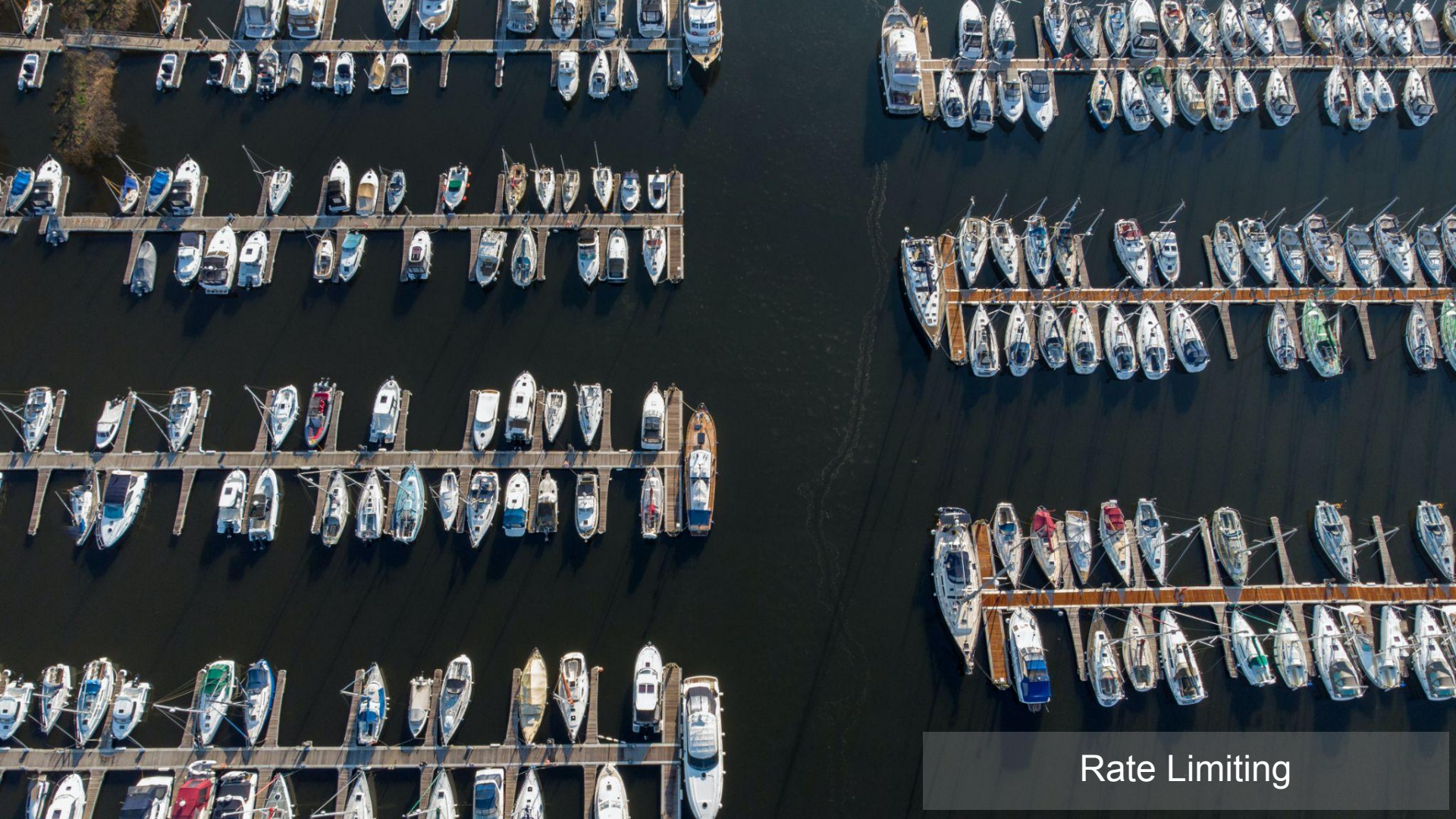


Prevent fault

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ui
spec:
  hosts:
    - ui
  http:
    - retries:
        attempts: 3
        perTryTimeout: 2s
      route:
        - destination:
            host: backend
            subset: v1
```

Retry

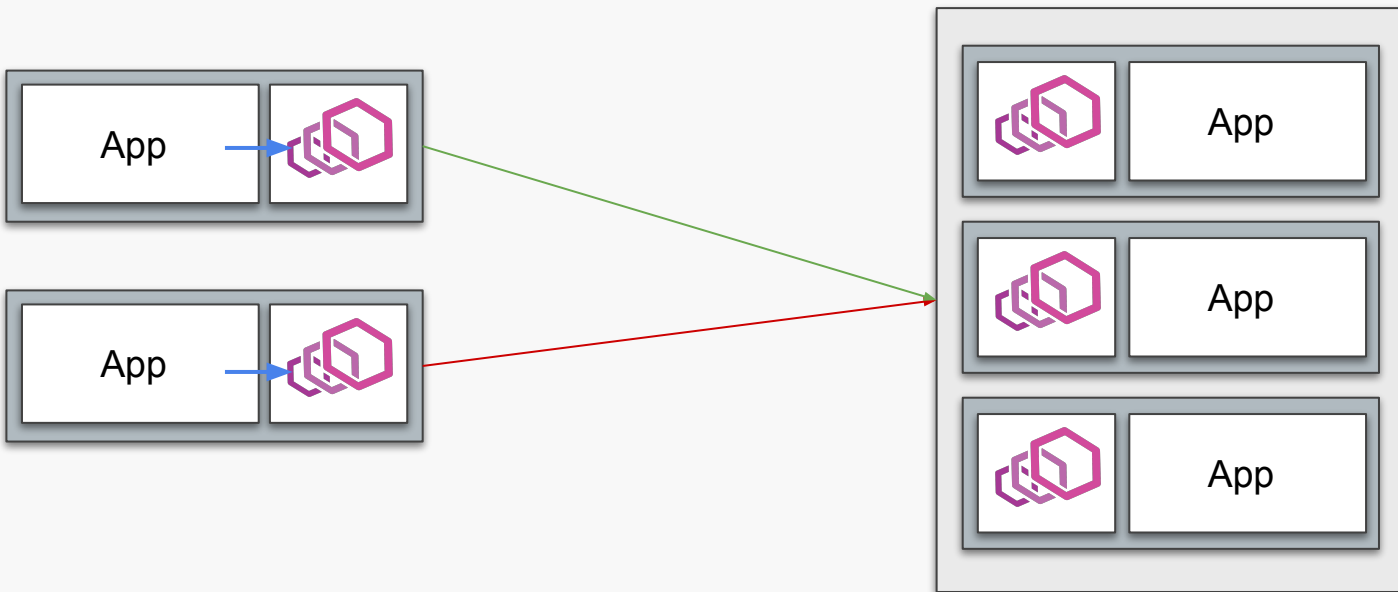




Rate Limiting

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
spec:
  host: ui
  subsets:
    - name: version-1
      labels:
        version: v1
    - name: version-2-beta
      labels:
        version: v2
  trafficPolicy:
    connectionPool:
      http:
        http1MaxPendingRequests: 1
        maxRequestsPerConnection: 1
      tcp:
        maxConnections: 1
```

Rate Limiting

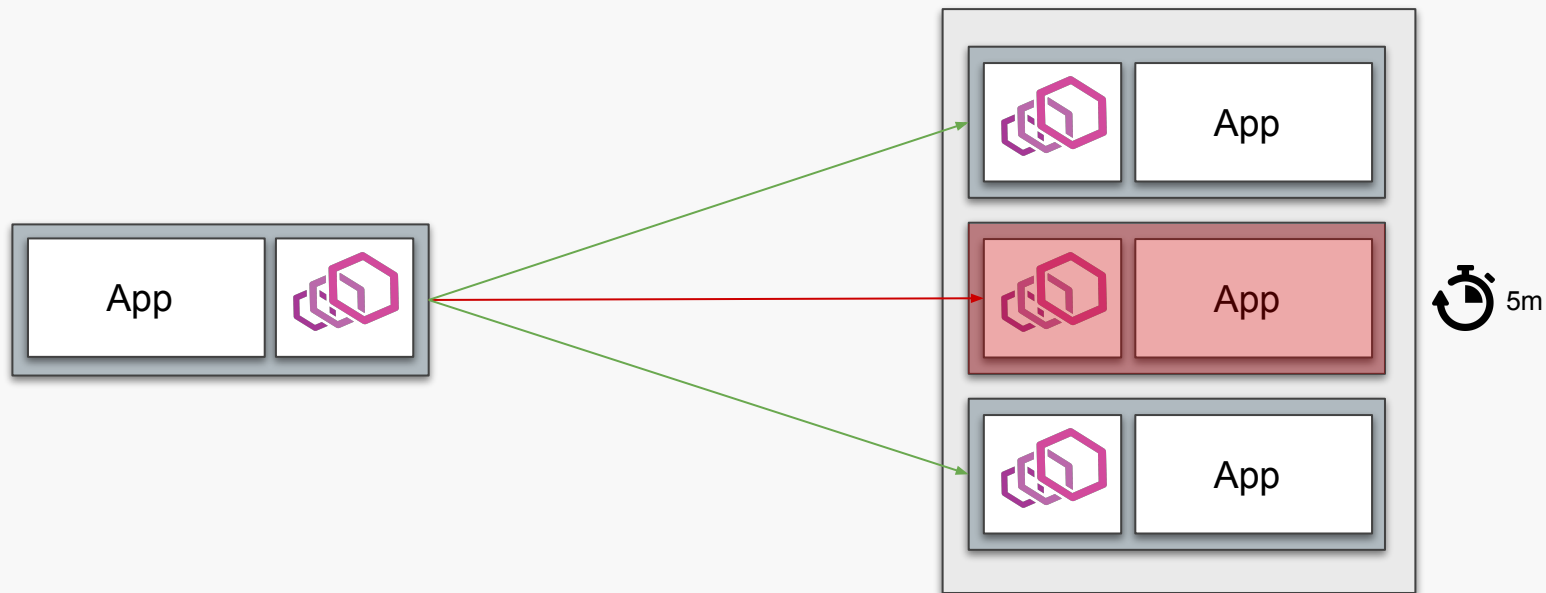


Pool Ejection



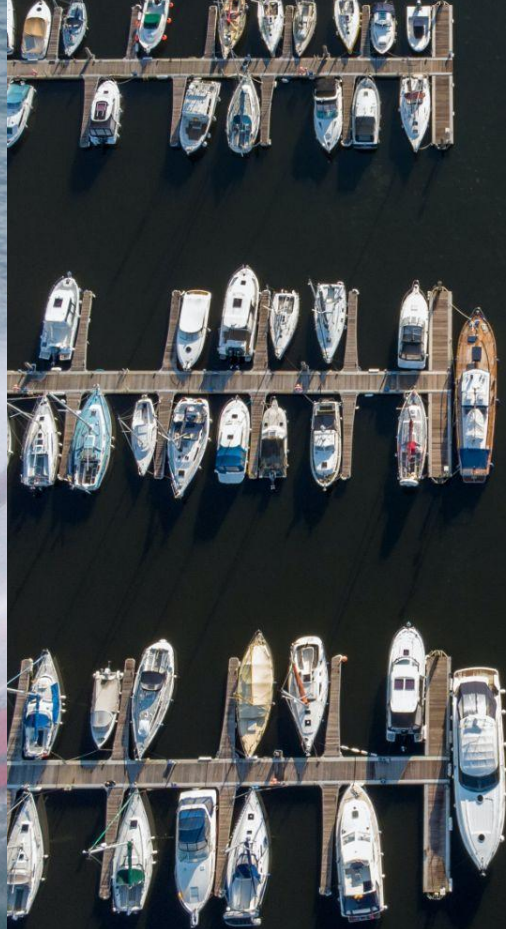

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: ui
...
- name: version-2-beta
  labels:
    version: v2
  trafficPolicy:
    connectionPool:
      http: {}
      tcp: {}
    outlierDetection:
      baseEjectionTime: 5m
      consecutiveErrors: 1
      interval: 5s
      maxEjectionPercent: 100
```

Pool Ejection





Retry



Rate Limiting



Pool Ejection



Global Resiliency



Having Control with Fun !



Fault Injection



```
@Component
class AwesomeHandler(val cache: Cache, val db: Database) {

    fun fetch(id: String) = cache
        .findById(id)
        .onErrorResume { Mono.empty() }
        .switchIfEmpty { db.findById(id) }
}
```

Testing your **resiliency**



Fault

Abort | Delay

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: search
spec:
  hosts:
    - search
  http:
    - fault:
        abort:
          percent: 10
          httpStatus: 400
      route:
        - destination:
            host: search
            subset: v1
```

Fault

Restricted to route...
... | URI | Scheme | ...

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: backend
spec:
  hosts:
    - backend
  http:
    - fault:
        abort:
          percent: 10
          httpStatus: 400
        route:
          - destination:
              host: backend
              subset: v1
```

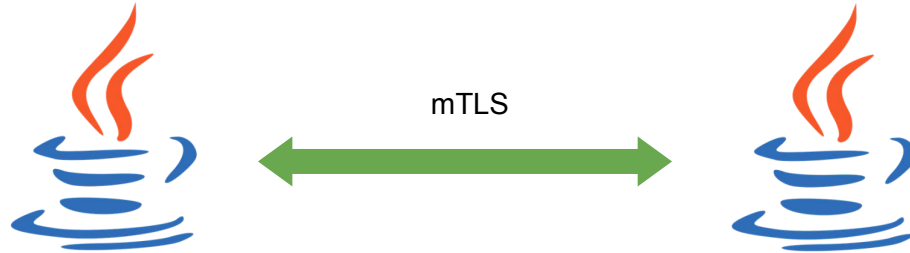
Security



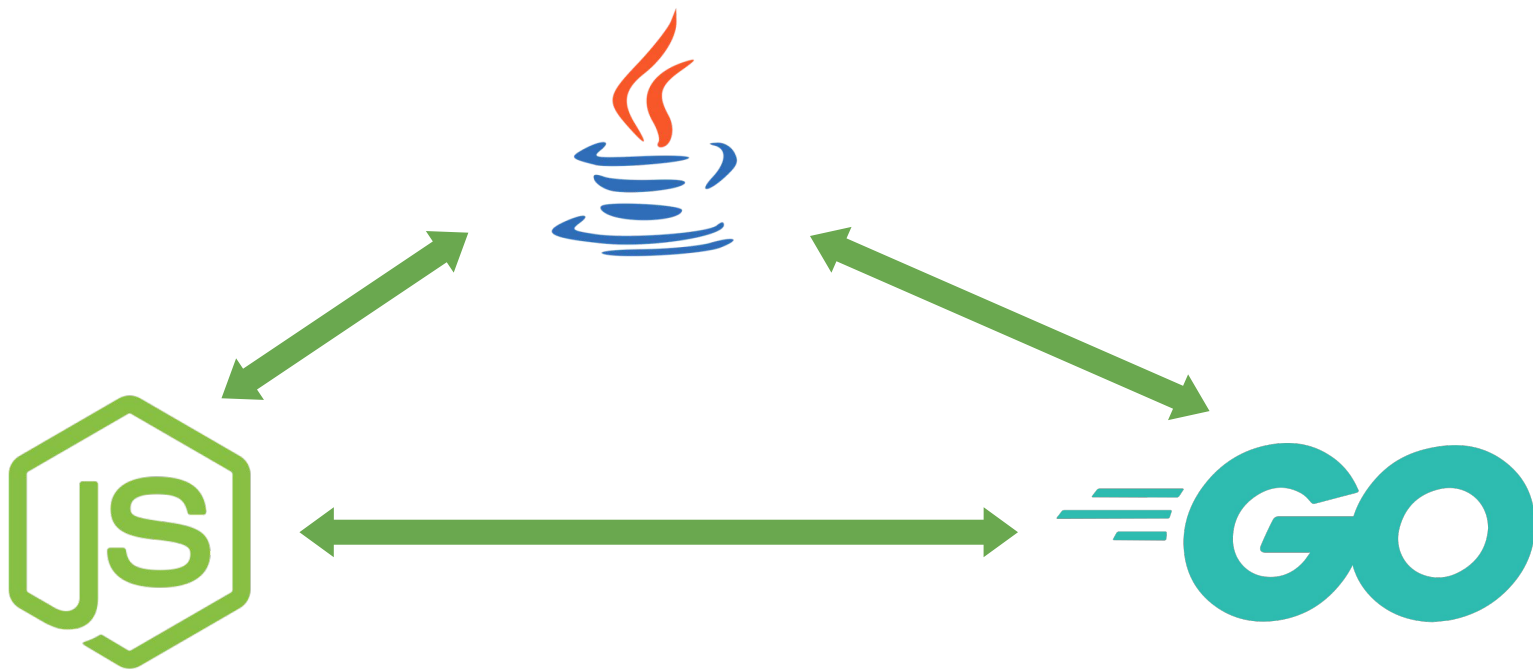
Mutual TLS



Have you ever tried ?



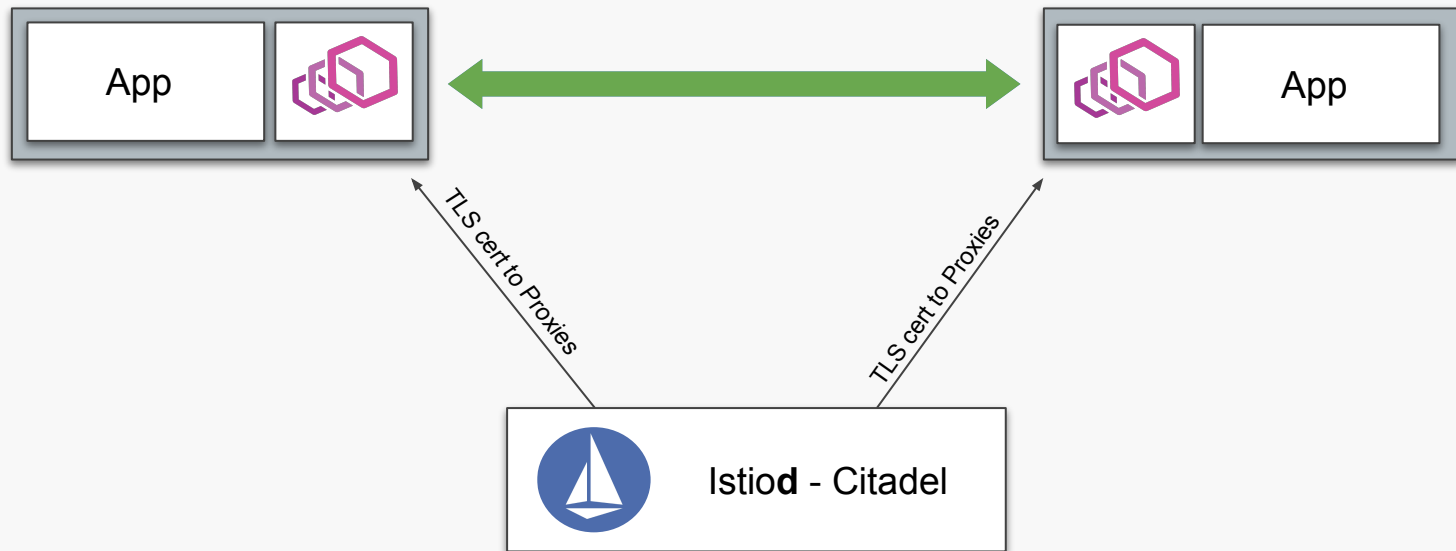
Have you ever tried ?




```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
  namespace: custom-ns
spec:
  mtls:
    mode: STRICT
```

```
kind: DestinationRule
metadata:
  name: default
  namespace: custom-ns
spec:
  host: "*.custom-ns.svc.cluster.local"
  trafficPolicy:
    tls:
      mode: ISTIO_MUTUAL
```

Mutual Authentication TLS (mTLS)



Authentication as a Service



apiVersion: security.istio.io/v1beta1

kind: RequestAuthentication

metadata:

name: jwt-auth

spec:

selector:

matchLabels:

app: ui

jwtRules:

- issuer: "jwt@foo.bar.com"
- jwksUri: "https://foo.bar.com/.../jwks.json"

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
  name: is-customer
spec:
  selector:
    matchLabels:
      app: ui
  action: ALLOW
  rules:
    - to:
        - operation:
            methods: ["GET"]
            paths: ["/orders*"]
      when:
        - key: request.auth.claims[groups]
          values: ["customer"]
```

JWT Authentication



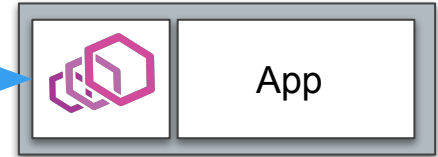
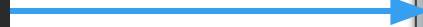
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0IjEyZ291c2NyaGV0e3RvbmVyeS51b250e3ZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.xVlgv05bE5WEkFAWU6SVuqpr1YddK92M1jgSPUNCyLM



JWT Authentication



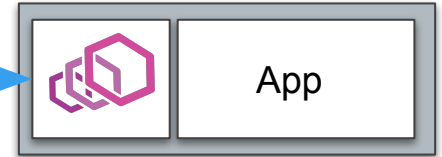
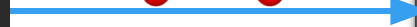
```
{  
  "sub": "1234567890",  
  "goup": "customer",  
  "name": "John Doe",  
  "iat": 1516239022  
}
```



JWT Authentication



```
{  
  "sub": "1234567890",  
  "goup": "anonymous",  
  "name": "John Doe",  
  "iat": 1516239022  
}
```

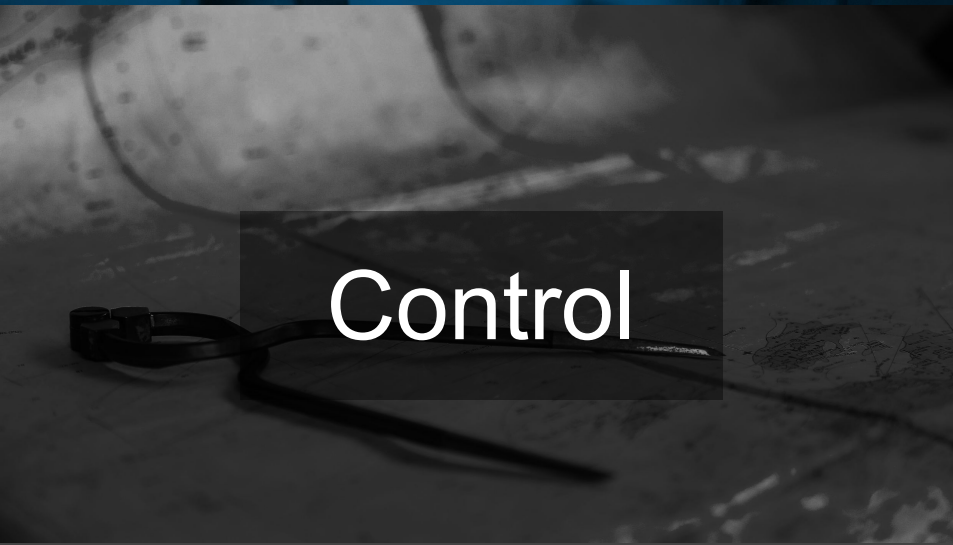




Observability



Connect



Control



Security

Go beyond...





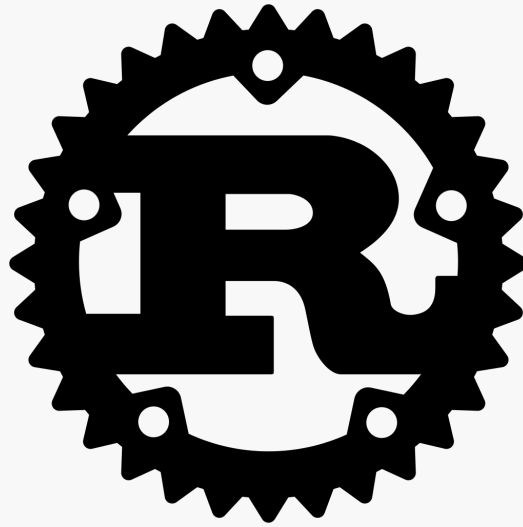
```
apiVersion:
networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: foo-lua
spec:
  workloadLabels:
    app: ui
  filters:
    - listenerMatch:
        portNumber: 8080
        listenerType: SIDECAR_INBOUND
      filterName: envoy.lua
      filterType: HTTP
      filterConfig:
        inlineCode: |
          ...
```



```
filterType: HTTP
filterConfig:
  inlineCode: |
    function envoy_on_request(request_handle)
      request_handle:headers():add("foo", "bar")
    end
    function envoy_on_response(response_handle)
      body_size = response_handle:body():length()
      response_handle:headers():add("response-body-size", tostring(body_size))
    end
```



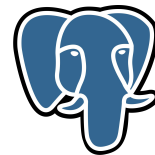
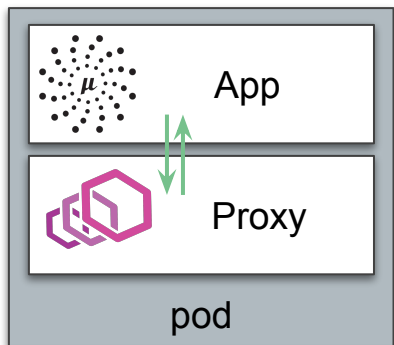

WEBASSEMBLY





WEB
AssemblyHub

Mesh Expansion



Virtual Machine




```
$ istioctl install
```



KUBERNETES
OPERATORS



More than **400** parameters

or with 4 profiles



End of Life



Google Kubernetes Engine



Istio is one click away

- ☐ Enable Cloud TPU (beta) ?
- ☐ Enable Kubernetes alpha features in this cluster ?
- ☐ Enable Kubernetes Dashboard ?
- ☒ Enable Istio (beta) ?
 - Enable mTLS (beta) ?

Strict ▼
- ☐ Enable node auto-provisioning (beta) ?

⌵ [Less](#)

Create

Reset

Equivalent [REST](#) or [command line](#)



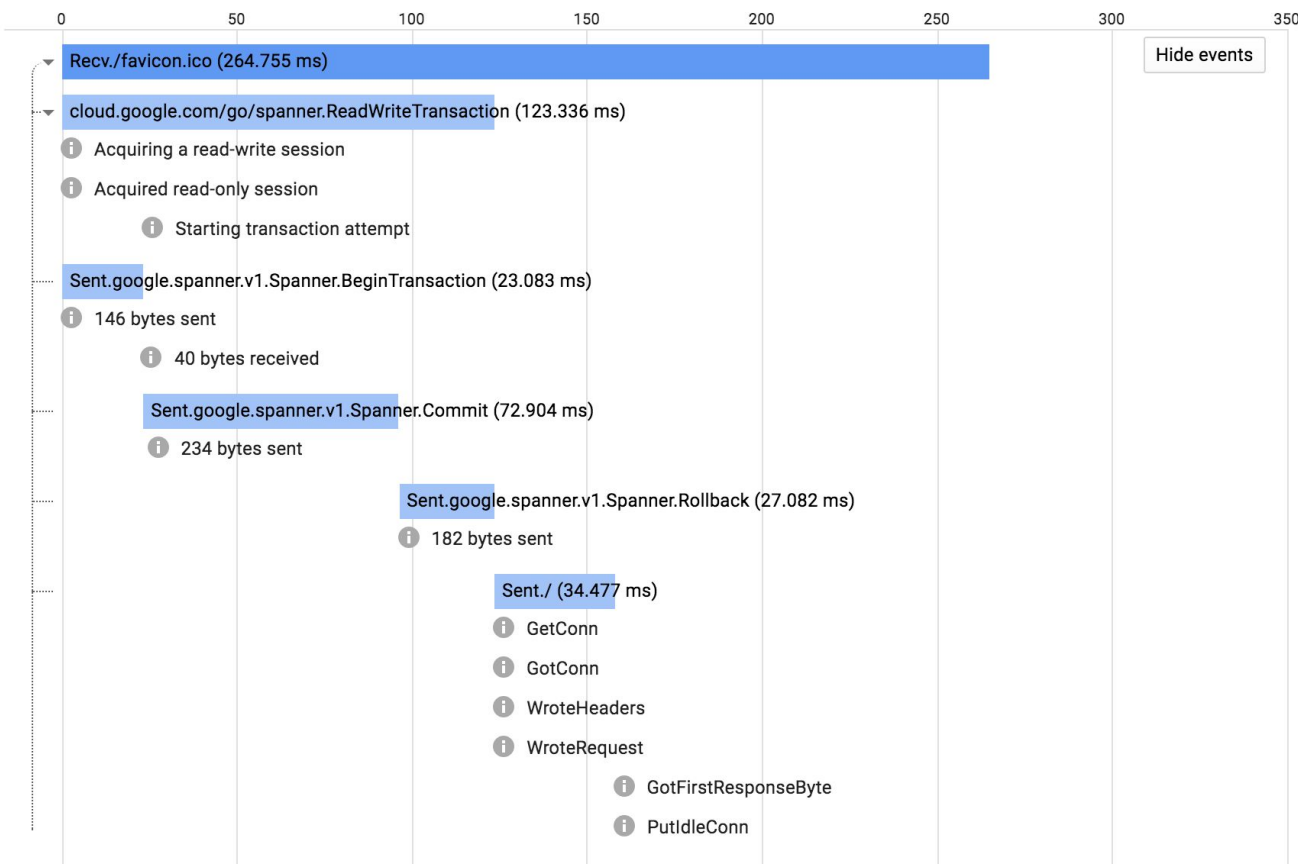
Cloud Monitoring



Cloud Monitoring



Cloud Monitoring



Cloud Monitoring



Cloud Monitoring





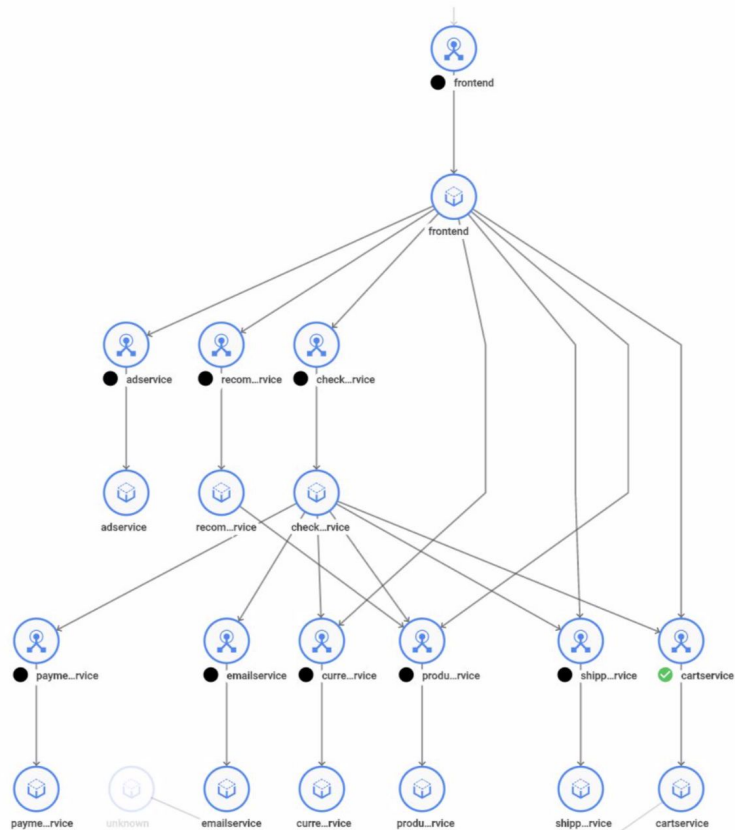


Legend

 Workload

 Service

Displaying data from:
Apr 7, 2:37 PM
to 3:37 PM



2:40 PM

2:50 PM

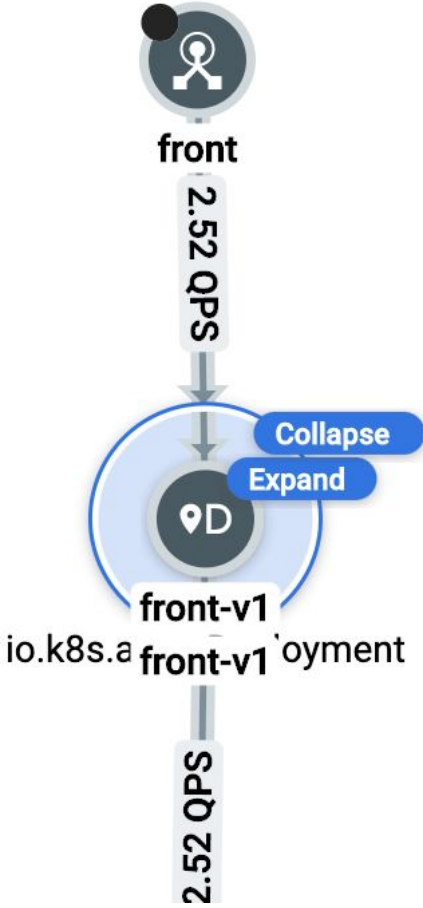
3:00 PM

3:10 PM

3:20 PM

3:30 PM

3:37 PM





middleware

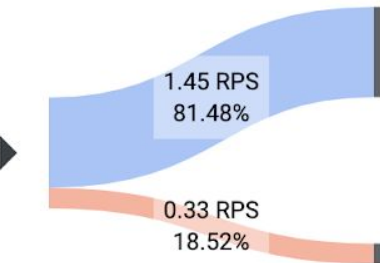


Alerts timeline No service alerts. Time selection is 4:59 AM to 5:59 AM.

Service traffic displays network traffic metrics and service routing details.



Incoming traffic



middleware
Kubernetes Service



middleware-v1
Workload

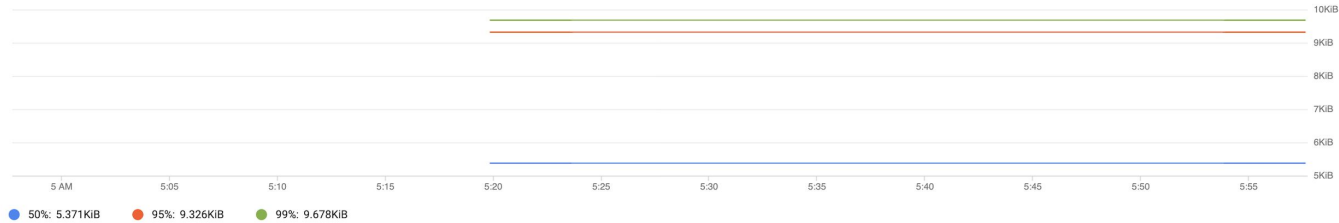


middleware-v2
Workload



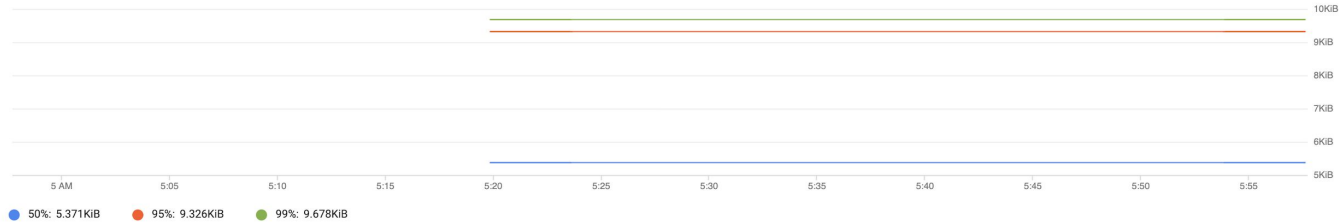
Request size ?

Breakdown By



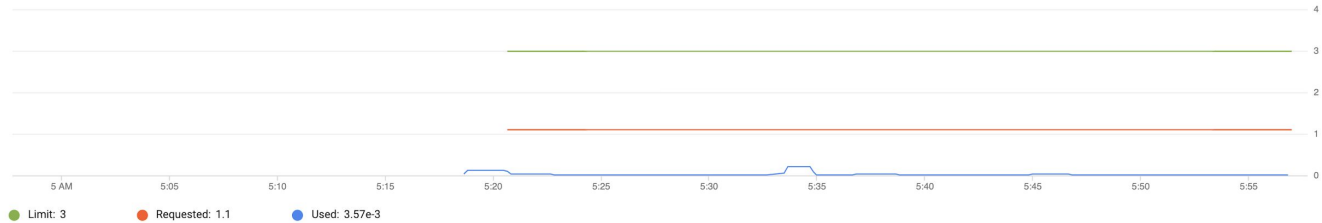
Response size ?

Breakdown By



CPU ?

Breakdown By





Google Cloud Platform

service-mesh-demo1 ▾



Service: weather-frontend

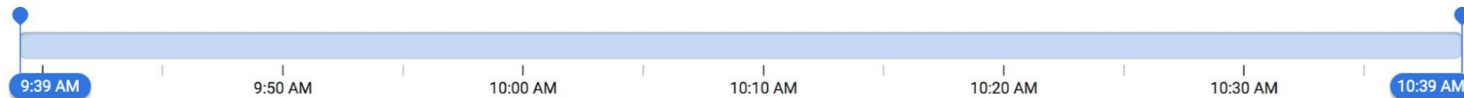
Alerts timeline No service alerts. Time selection is 9:39 AM to 10:39 AM.

RESET

Time Span

1 hour ▾

HIDE TIMELINE



OVERVIEW

HEALTH

METRICS

DIAGNOSTICS

INFRASTRUCTURE

CONNECTED SERVICES

Service status: none

There are no SLOs set for this service.

CREATE SLO

Requests ?

0.0/sec

0.0/sec (25%) previous 1 hr

Error rate ?

0.0%

0% (0%) previous 1 hr

Latency 50th percentile ?

154ms

+10ms (7%) previous 1 hr

Details

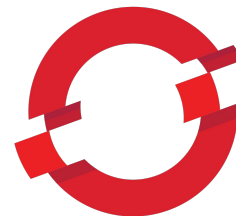
Namespace	weatherinfo
Mesh	service-mesh-demo1-mesh
Description	Automatically generated by SyncAgent
Clusters	service-mesh-demo1



Open Source



Google Cloud



OPENSIFT



Google Cloud Anthos



BANZAI CLOUD

Thank you...

@davinkevin

Questions ?

