PagerDuty

Service Messy

Pagerduty's Service Mesh Journey

Liz Frost, SRE IV
PagerDuty Core Infrastructure

Liz Frost, SRE IV
PagerDuty Core Infrastructure

On pronunciation

/kubɜɹˈnɛtiz/ or /kubɜːˈnɛtiz

vs

kəˈbɜɹnɛtiz

PagerDuty

- What to know before you go
- How we migrated
- Random Gotchas

What We Have

- Consul
- Kubernetes (from Nomad)
- Lots of Elixir
- Lots of *other* languages
- An “Opinionated Wrapper Library”
- A lot of small rocks and some *really big ones*

Eventual Consistency

App Types	Total per-app Type to migrate
Elixir	100
Shell	10
Python	23
Envoy	0
Nginx	4
Ruby	6
Scala	7
Go	1
Java	5
TypeScript	4
JavaScript	2
C#	3
N/A	0

Problems:

- Too many languages
- Too many implementations
- Compliance issues

PagerDuty

Mesh Time

(know before you go)

Pros

- Increased Visibility
- Security
- Traffic Features

Cons

- Complexity
- Latency
- Resource Intensive
- Learning Curve

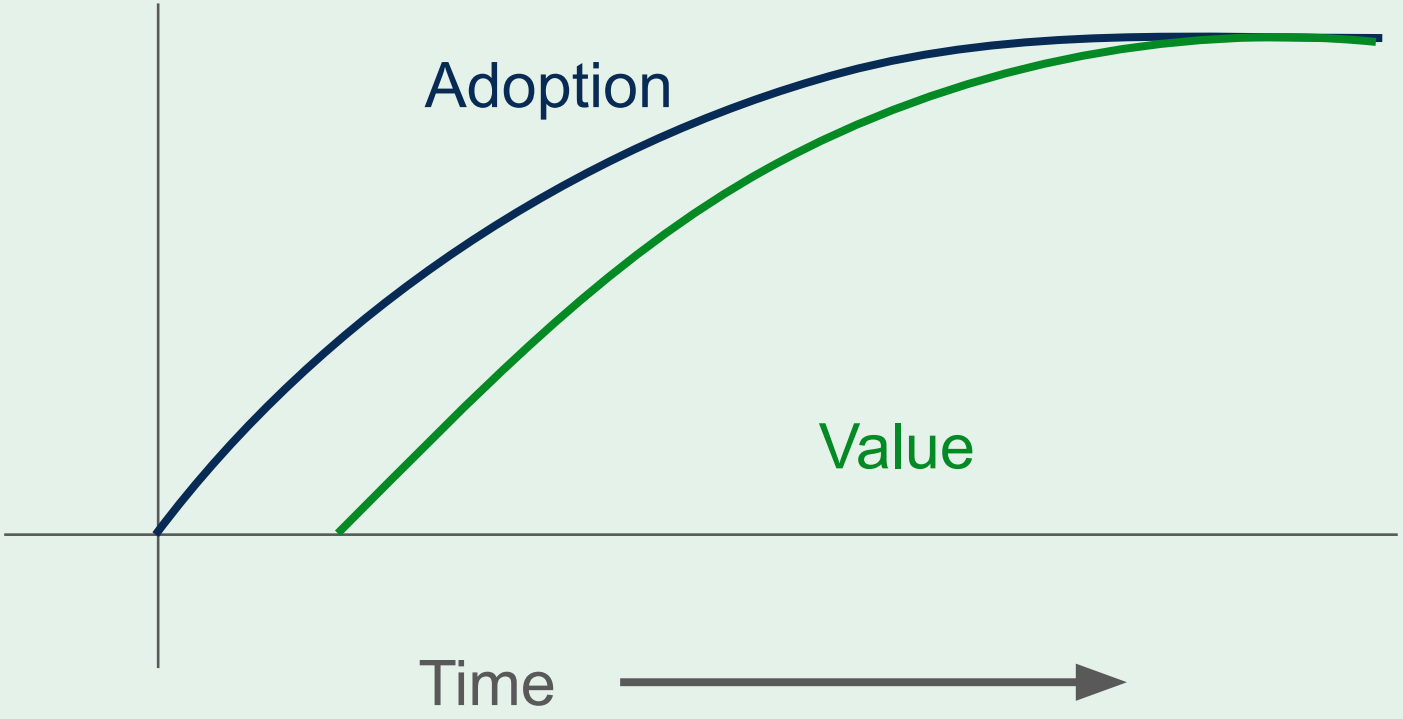
Pros

- Increased Visibility
- Security
- Traffic Features
  - Retries, Canaries, Circuit breakers…

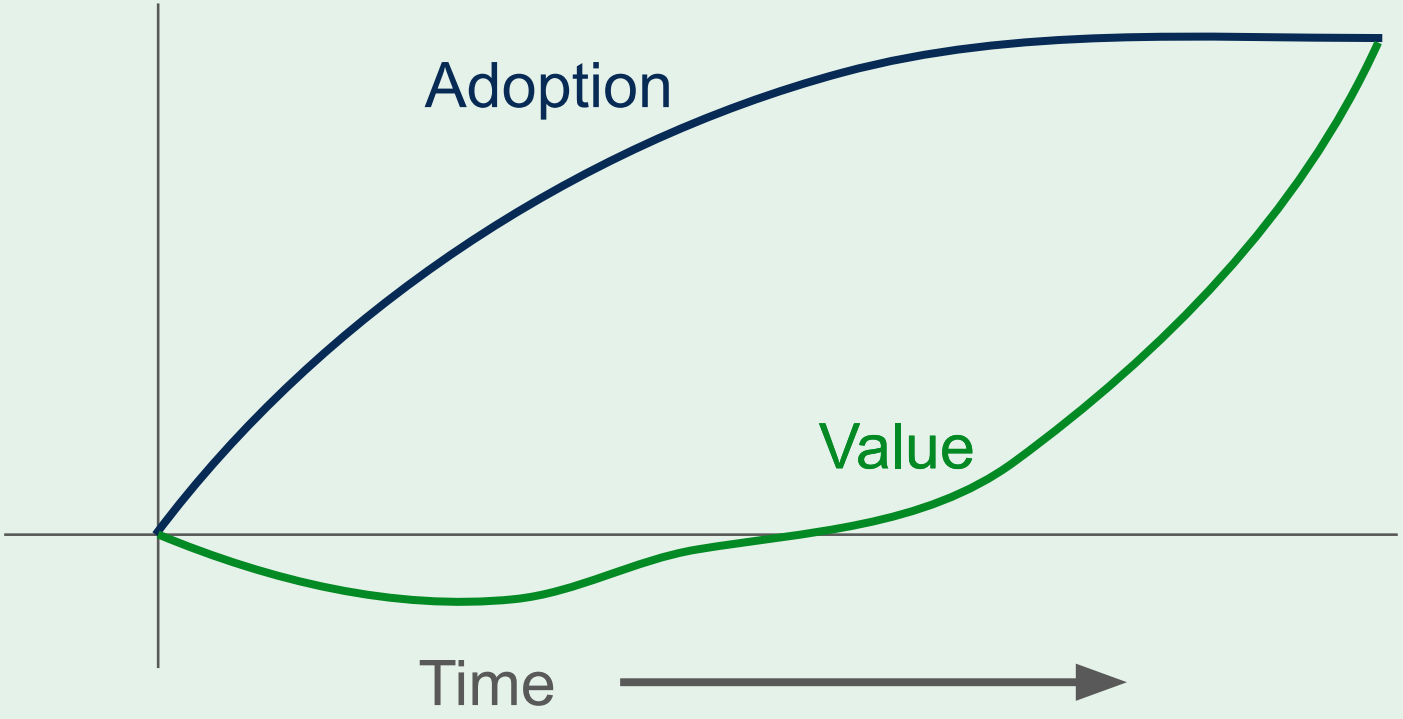
Cons

- Complexity
- Latency
- Resource Intensive
- Learning Curve

Network Effect :)



Network Effect :(



Day 1

Pros

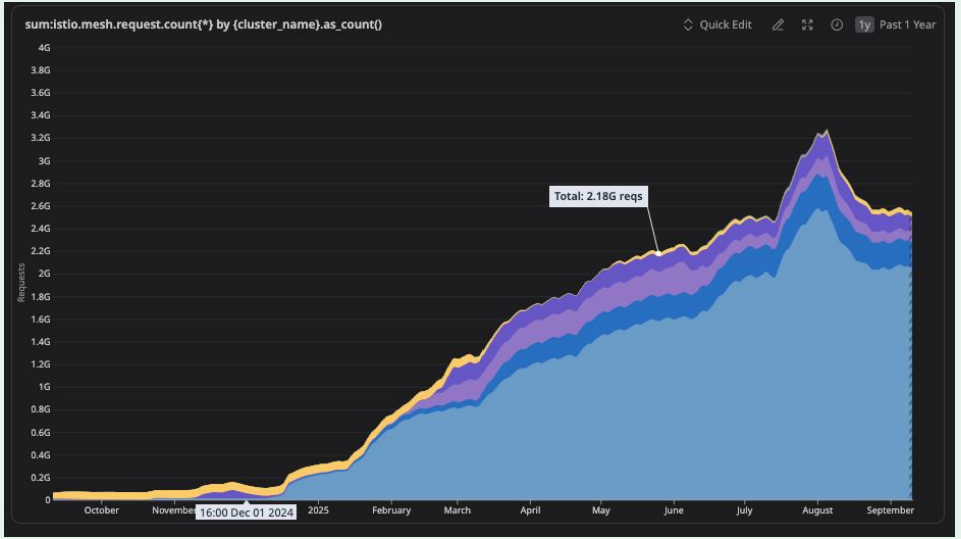
- Increased Visibility
- ~~Security~~
- ~~Traffic Features~~

Cons

- Complexity
- Latency
- Resource Intensive
- Learning Curve

Metrics work 🎉

- Source **or** destination
- Normalised across every app
  - No guessing metric names!
- Graph go up



Security

- No Enforcement
- Partial Encryption?
  more like no encryption :(
- No Validation

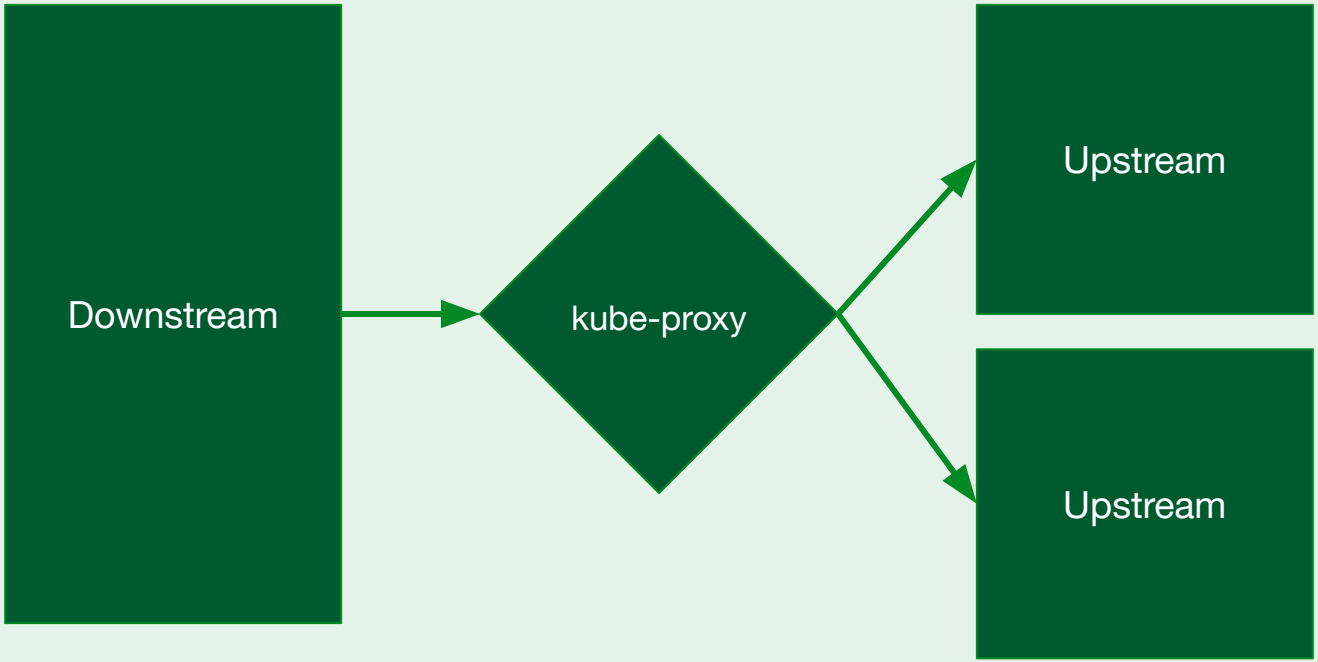
ssl added and removed
everywhere :(

Traffic Features?

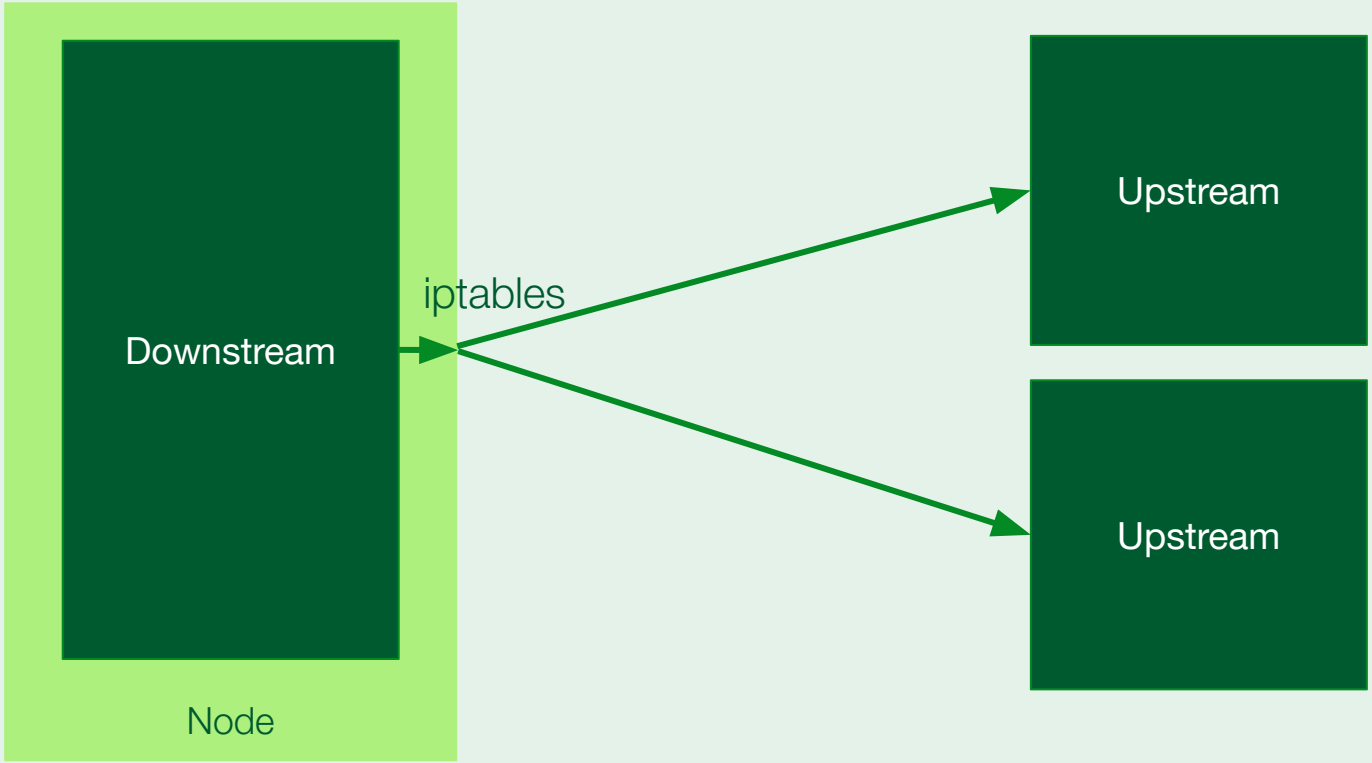
A Brief Detour...

```yaml
apiVersion: v1
kind: Service
metadata:
  name: pony-api
  namespace: pony-api
spec:
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 8080
  selector:
    app: pony-api
  type: ClusterIP
```

How you think about it



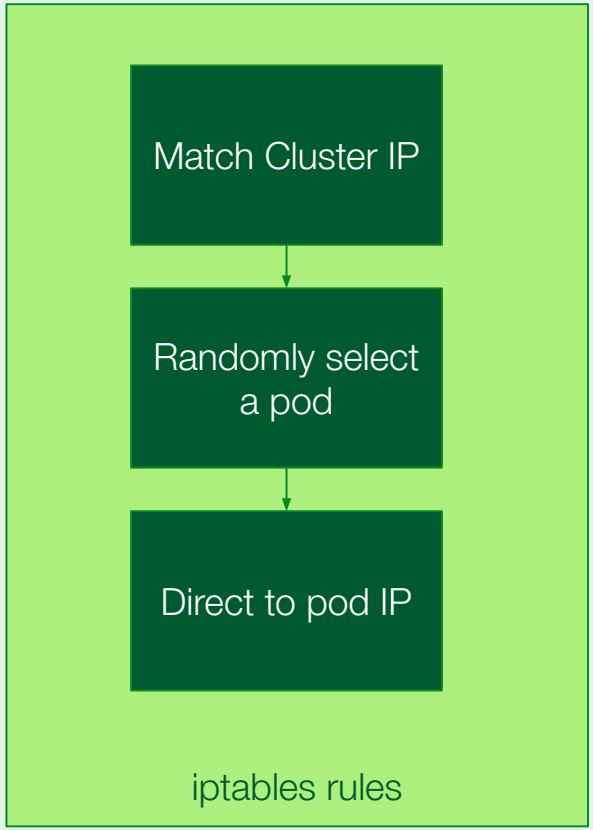
How you think about it



the cluster IP does not exist!

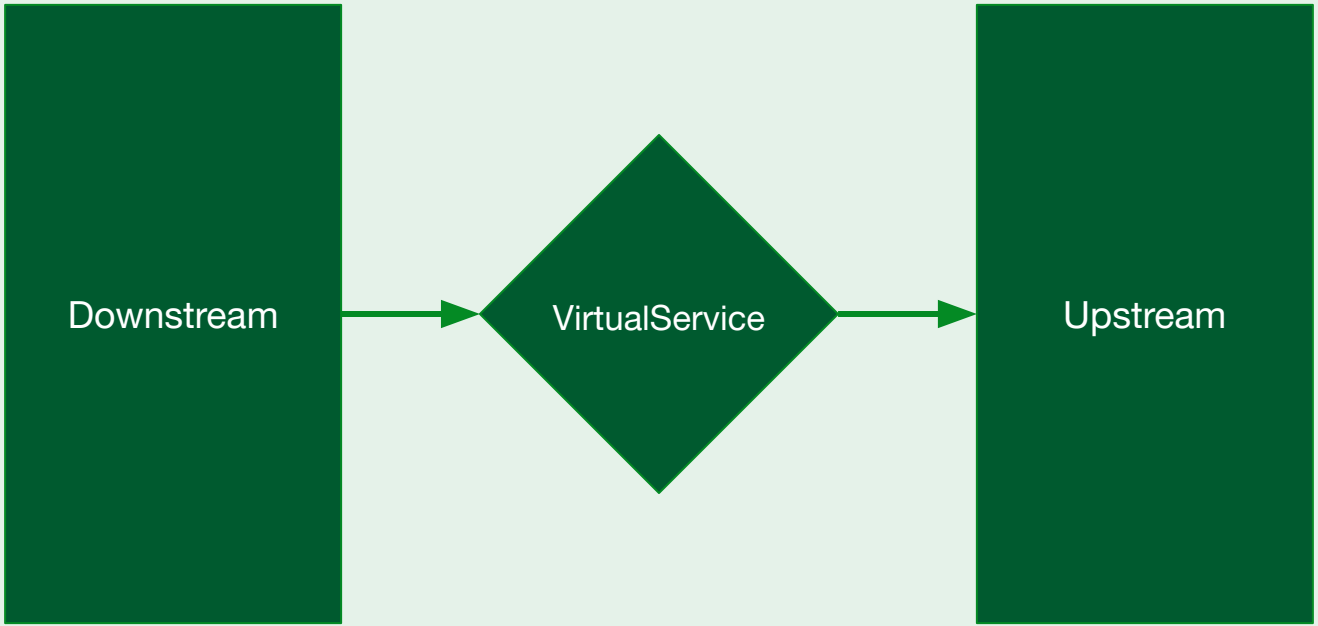
kube-“proxy”

it’s all iptables

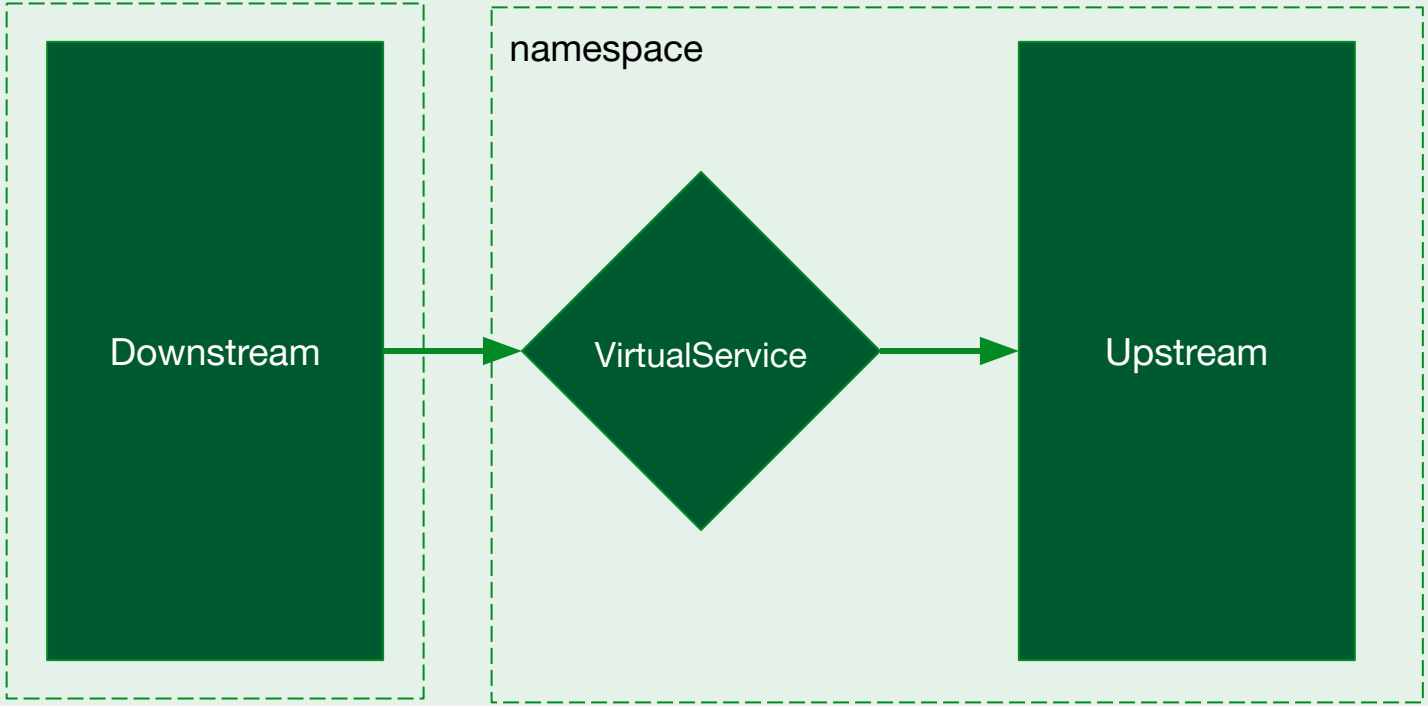


```yaml
apiVersion: networking.istio.io/v1
kind: VirtualService
metadata:
  name: pony-api
spec:
  hosts:
  - pony-api.pony-api.svc.cluster.local
  http:
  - route:
    - destination:
        host: pony-api.pony-api.svc.cluster.local
        port:
          number: 80
    retries:
      attempts: 3
```

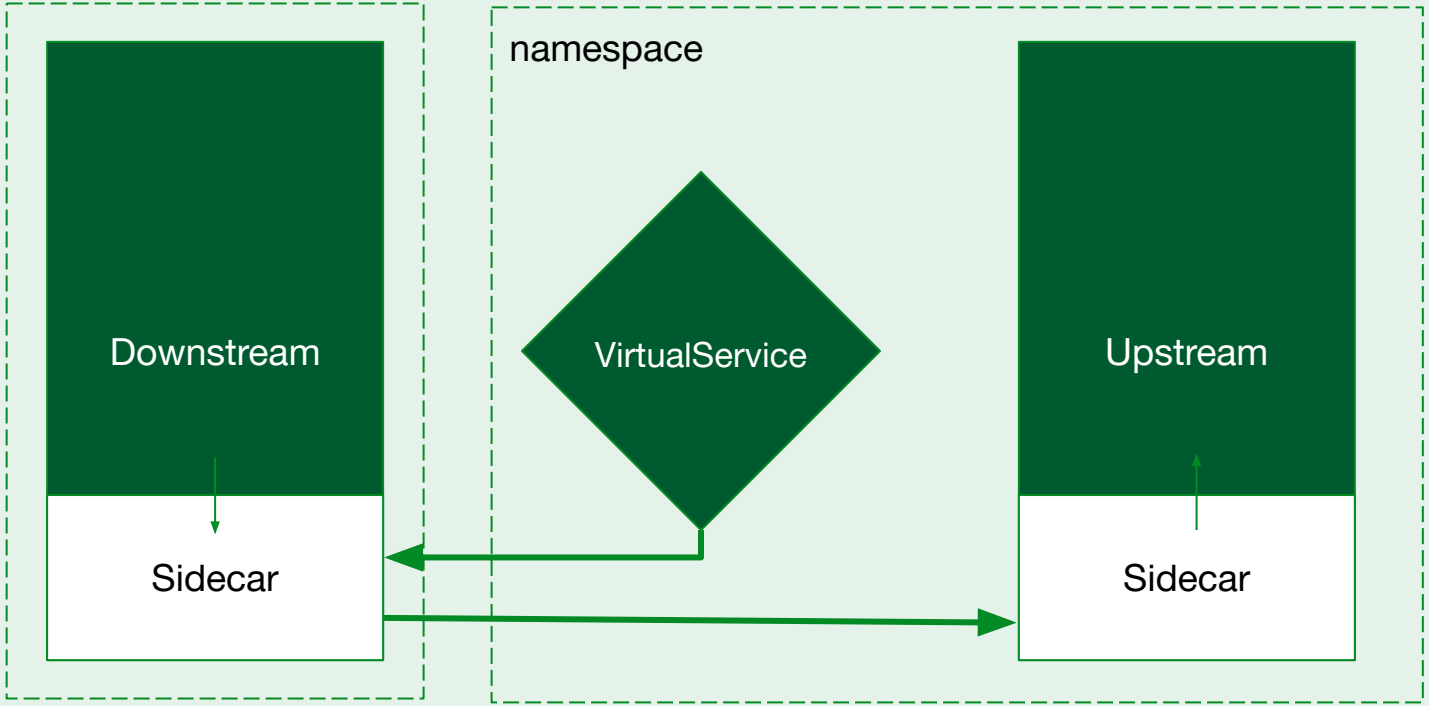
How you think about it



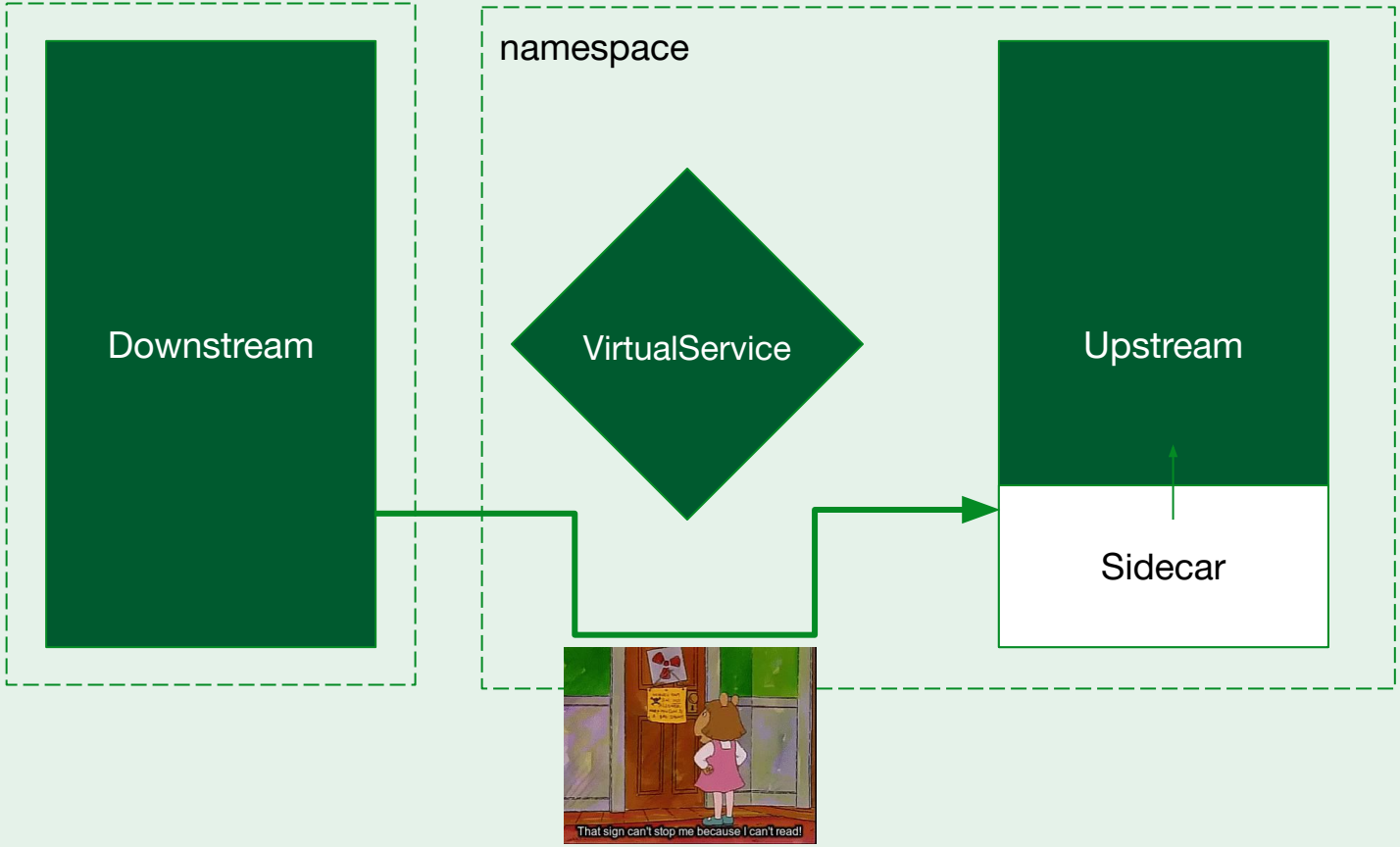
How you think about it



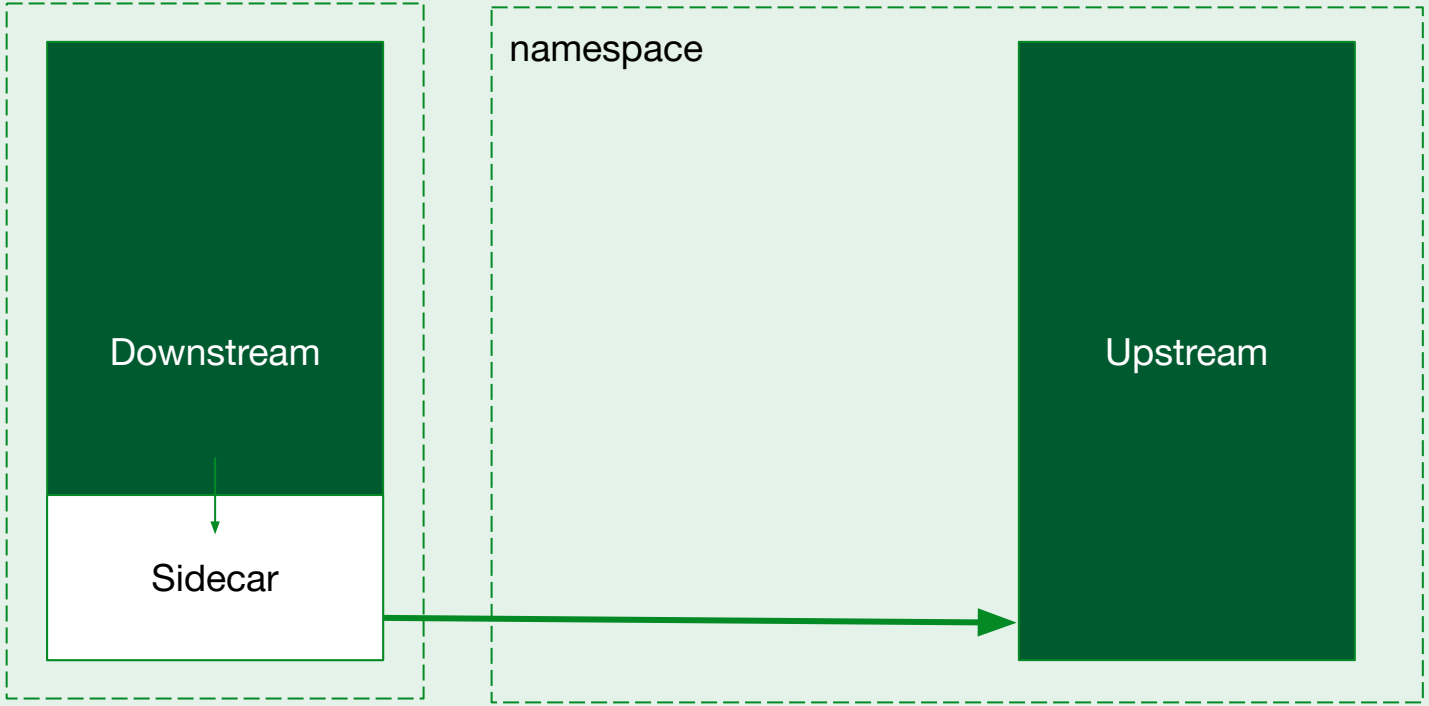
How It’s Implemented



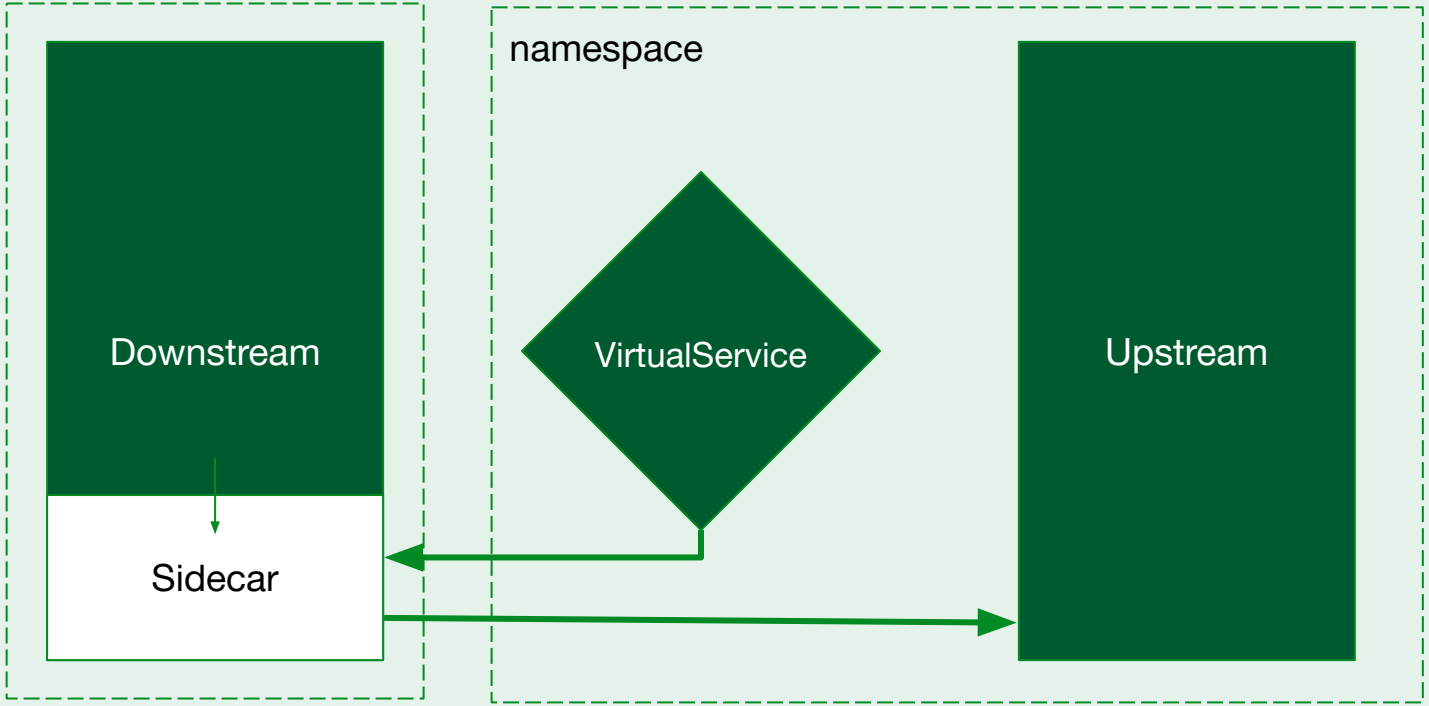
How It’s Implemented



Downstream Only



Who knows!



It’s All Happening Downstream

Retries

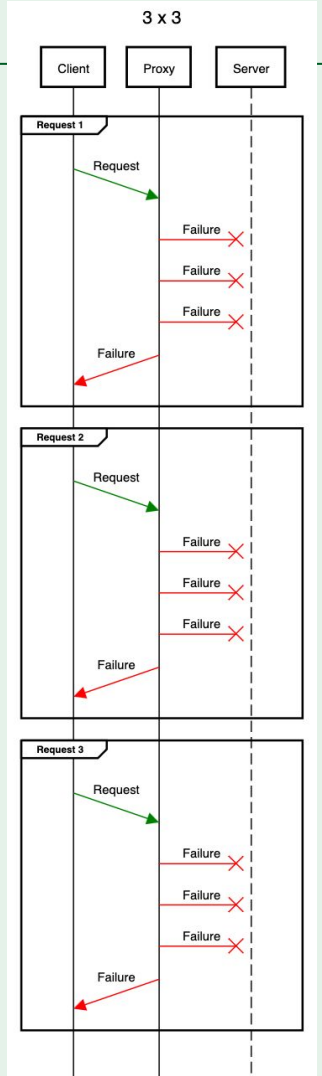
Before: Configured in Client (Downstream)

```
config :service_mesh_http_owl,
  retry_count: 3,
  retry_start: 250
```

Now: Configured in VirtualService (Upstream)

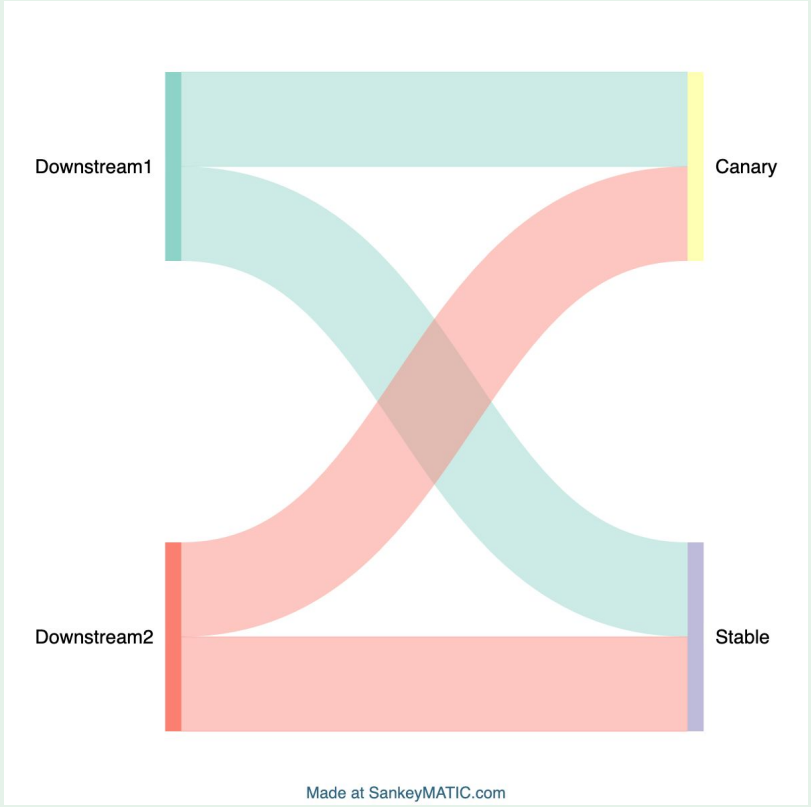
```
retries:
  attempts: 3
  retryOn: >-
    5xx,
    connect-failure,
    retriable-4xx,
   perTryTimeout: 2s
   backoff: 3s
```

Don’t Nest Retries!



Canaries

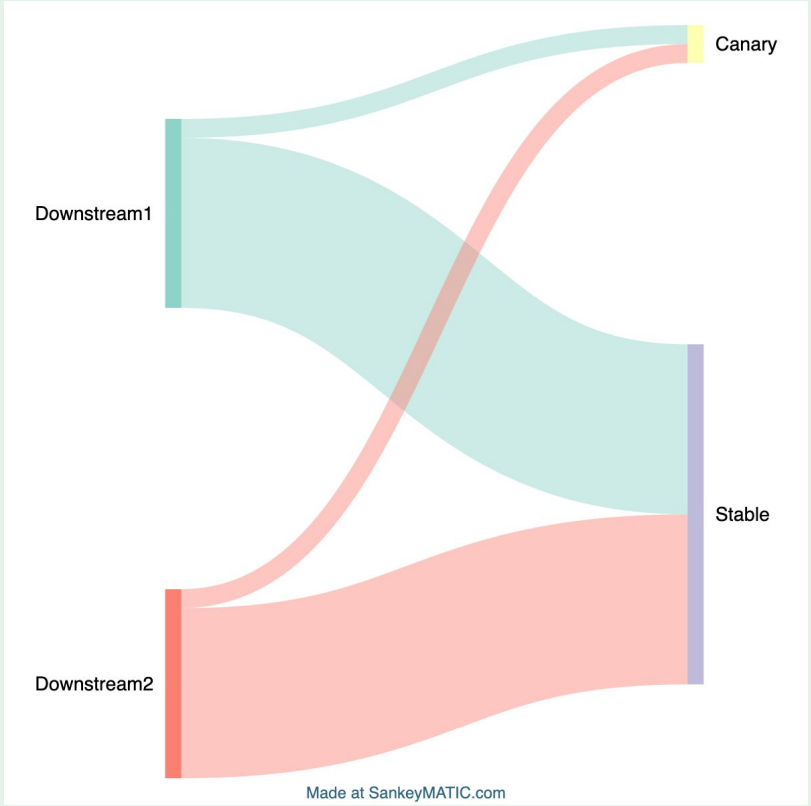
Canaries



50%

50%

Canaries

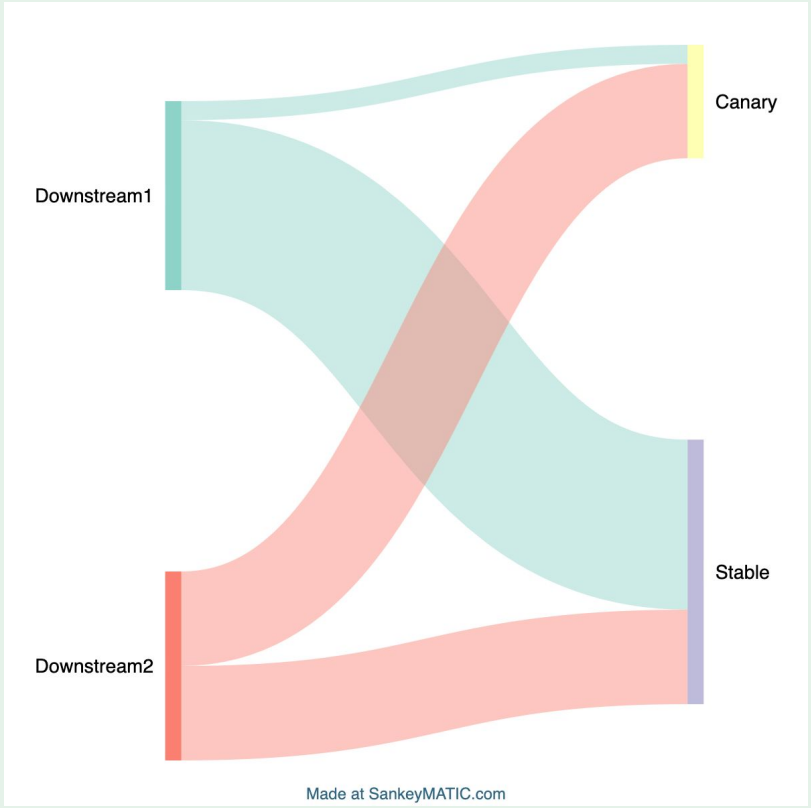


10%

90%

Canaries

mesh



30%

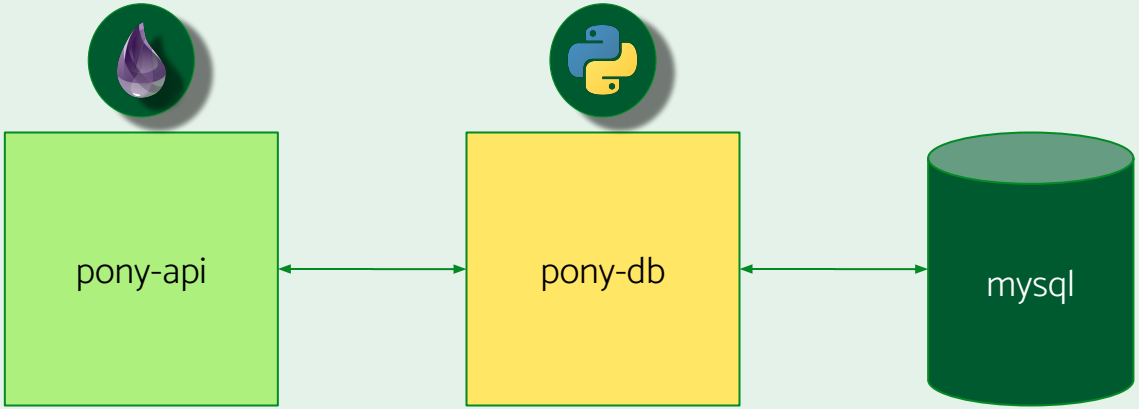
70%

no mesh

PagerDuty

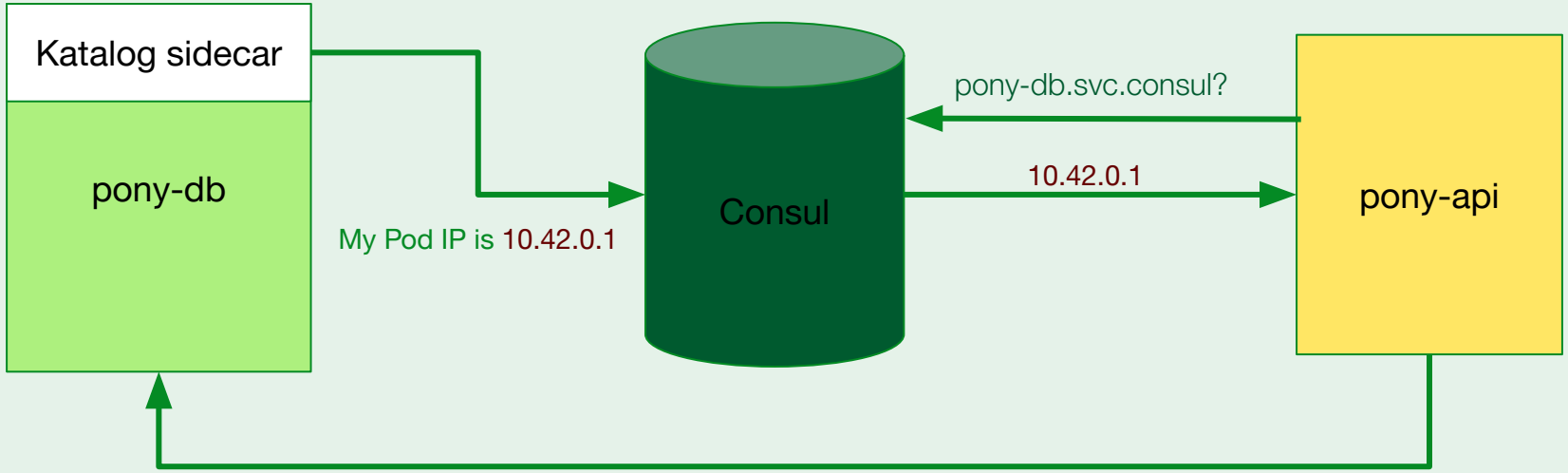
How we migrated

(how do you eat an elephant?)



PD’s most critical service

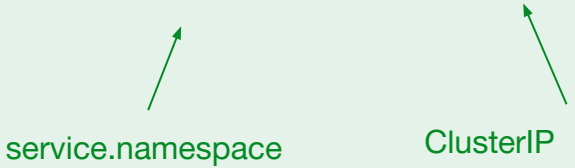
Consul Discovery



How does Istio route traffic?

```
VHOST NAME
pony-db.pony-db.svc.cluster.local:80
```

```
DOMAINS
pony-db.pony-db, 10.43.223.228
```



- ✓ `http://pony-db.pony-db`
- ✓ `http://pony-db.svc.cluster.local`
- ✓ `http://10.43.223.228`

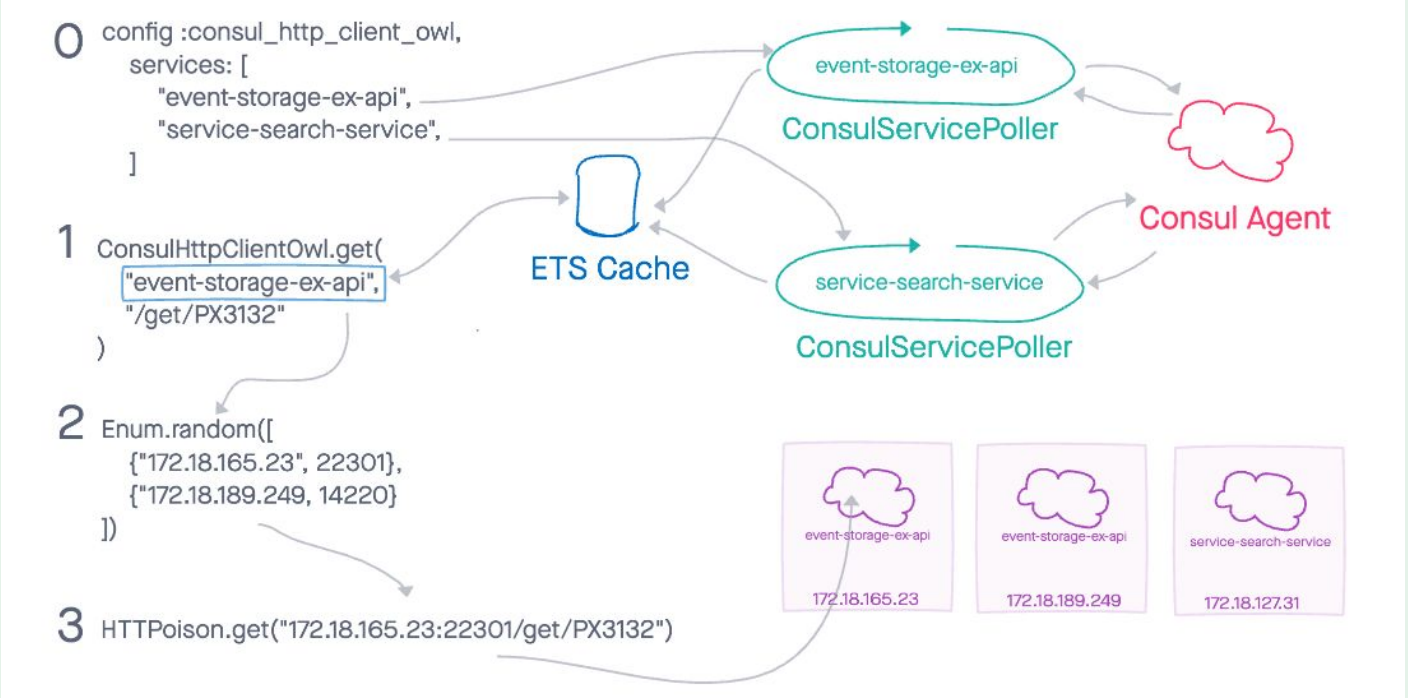
Can we just match the domain?

```
apiVersion: networking.istio.io/v1
kind: VirtualService
metadata:
  name: pony-db
spec:
  hosts:
  - pony-db.service.consul
```

How does Istio route traffic?

- ✓ `http://pony-db.pony-db`
- ✓ `http://pony-db.svc.cluster.local`
- ✓ `http://10.43.223.228`
- ✓ `http://pony-db.service.consul`

Not just DNS


0
config :consul_http_client_owl,
services: [
"event-storage-ex-api",
"service-search-service",
]
1
ConsulHttpClientOwl.get(
"event-storage-ex-api",
"/get/PX3132"
)
2
Enum.random([
{"172.18.165.23", 22301},
{"172.18.189.249, 14220}
])
3
HTTPoison.get("172.18.165.23:22301/get/PX3132")
event-storage-ex-api
ConsulServicePoller
Consul Agent
ETS Cache
service-search-service
ConsulServicePoller
event-storage-ex-api
172.18.165.23
event-storage-ex-api
172.18.189.249
service-search-service
172.18.127.31

How does Istio route traffic?

✓ `http://pony-db.pony-db`

✓ `http://pony-db.svc.cluster.local`

✓ `http://10.43.223.228`

✓ `http://pony-db.service.consul`

✗ `http://10.42.0.1`

Two Phase Migration

Step 1: Kubedns

Two Phase Migration

Step 1: Kubedns

Also update dependencies, change wrapper libraries, add a new package repository, replace names…

AI?

sed: the original AI

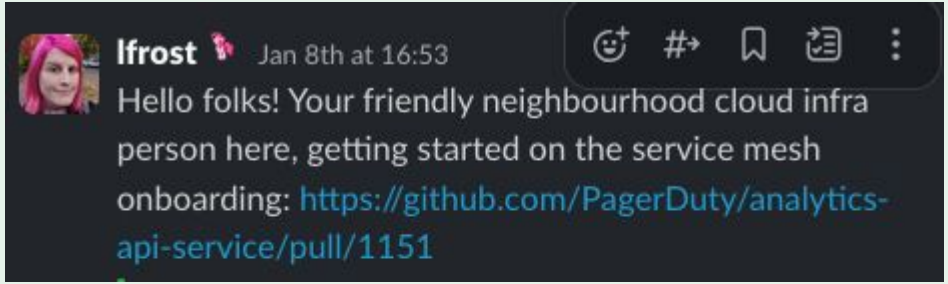
```
('ConsulHttpClientOwl', 'ServiceMeshHttpOwl'),
('ConsulServiceLookupOwl', 'ServiceMeshHttpOwl'),
('consul_http_client_owl_mod', 'http_client_mod'),
('consul_http_client_owl', 'service_mesh_http_owl'),
('consul_service_lookup_owl', 'service_mesh_http_owl'),
('consul_name', 'service_name'),
('PdClientMock', 'PdWebClientMock'),
('PdClient.Mock', 'PdWebClientMock'),
('PdClient.Behaviour', 'ServiceMeshHttpOwl.PdWebClientBehaviour'),
('PdClient', 'ServiceMeshHttpOwl.PdWebClient')
```

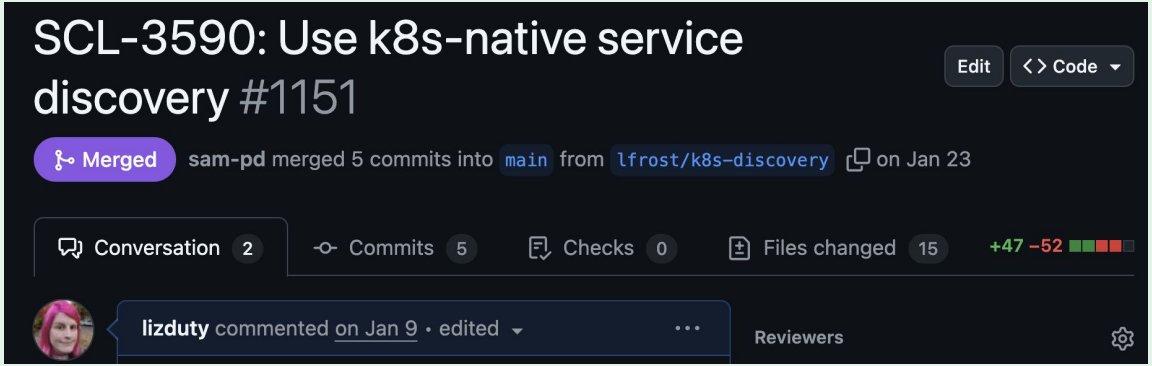
Away Team Model

aka “white glove” or “we code so you don’t have to”

Away Team Model

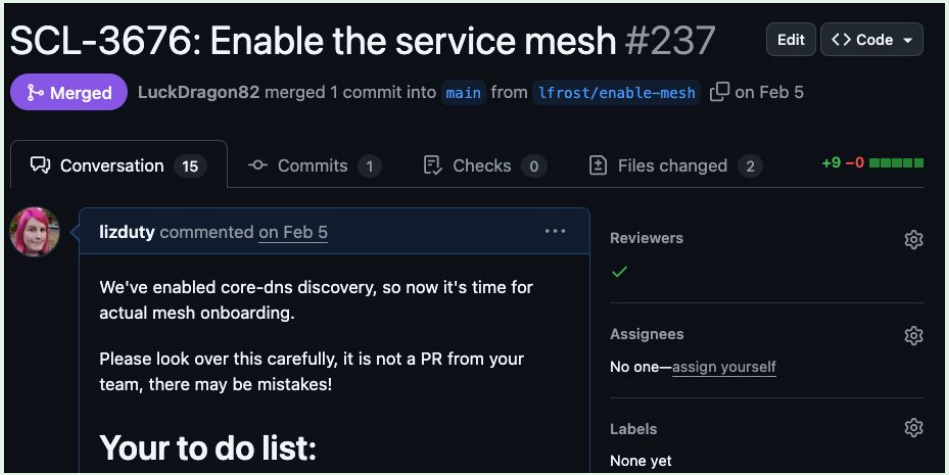
- Divided up by language
- Concentrates experience
- Many hands make light(er) work
- Preserves social capital





Two Phase Migration

```
+  mesh:
+     enabled: true
```



Helm Chart

```yaml
mesh:
  enabled: false
  access_logs:
    enabled: false
  envoy_dns_cache:
    disable: false
  settings:
    max_request_headers_kb: 120
```

Access Logs

```
spec:
  accessLogging:
    - disabled: false
      providers:
        - name: full
  selector:
    matchLabels:
      app.kubernetes.io/instance: pony-api
      app.kubernetes.io/name: pony-api
      app.pagerduty.com/env: production
      app.pagerduty.com/service-region: prod
      app.pagerduty.com/short-env: prod
```

max_header_size?

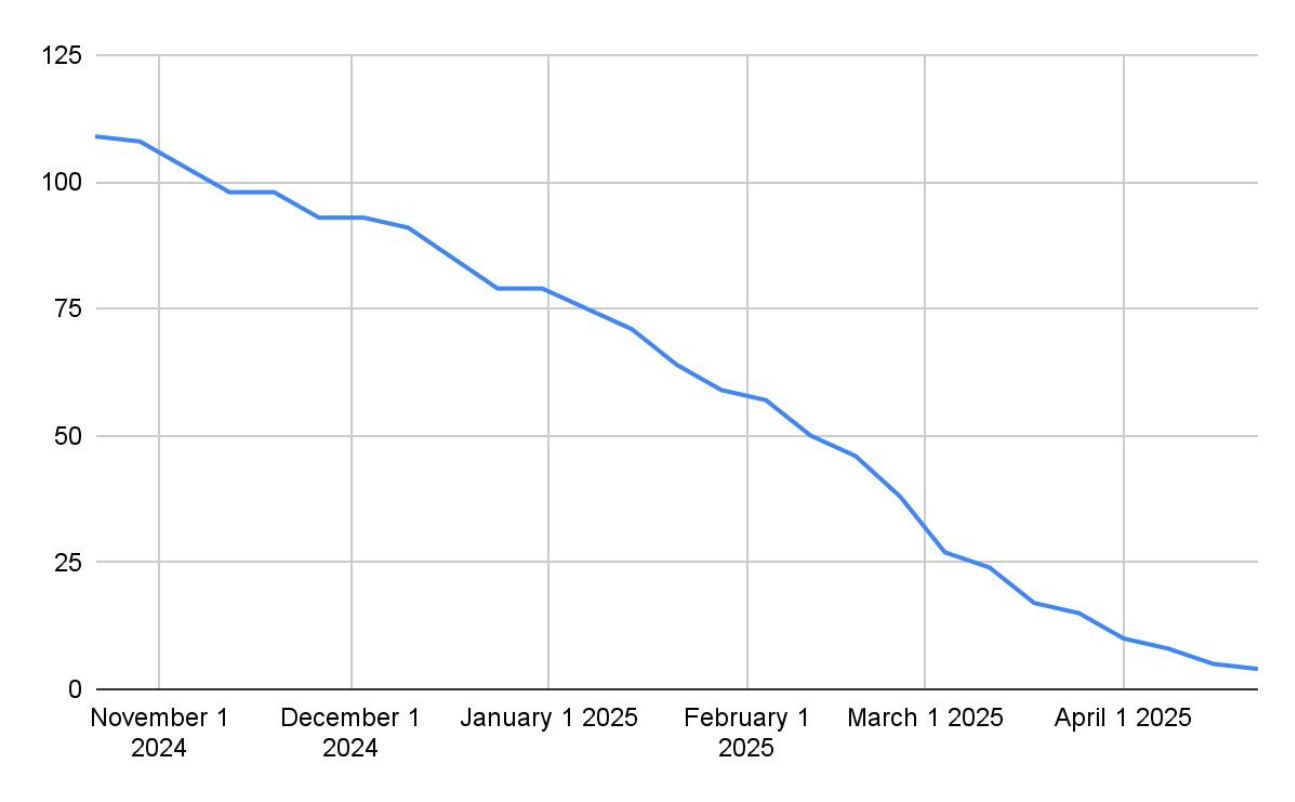
```
spec:
  configPatches:
    - applyTo: NETWORK_FILTER
      match:
        context: SIDECAR_INBOUND
        listener:
          filterChain:
            filter:
              name: envoy.filters.network.http_connection_manager
      patch:
        operation: MERGE
        value:
          typed_config:
            '@type': >-

type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.v3.HttpConnectionMa
nager
            max_request_headers_kb: 128
  workloadSelector:
    labels:
      app.kubernetes.io/name: advance-configuration-service
```

Tracking Progress

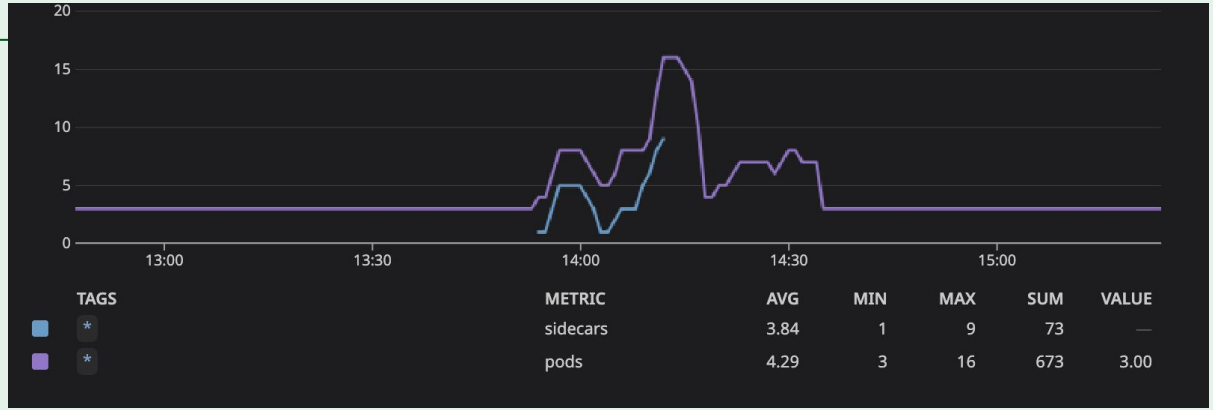
Planned Migration Timeline	App type	COUNT of NAM
13 - January Total		31
08 - August Total		10
09 - September Total		5
10 - October Total		51
11 - November Total		38
12 - December Total		30
Grand Total		**165**

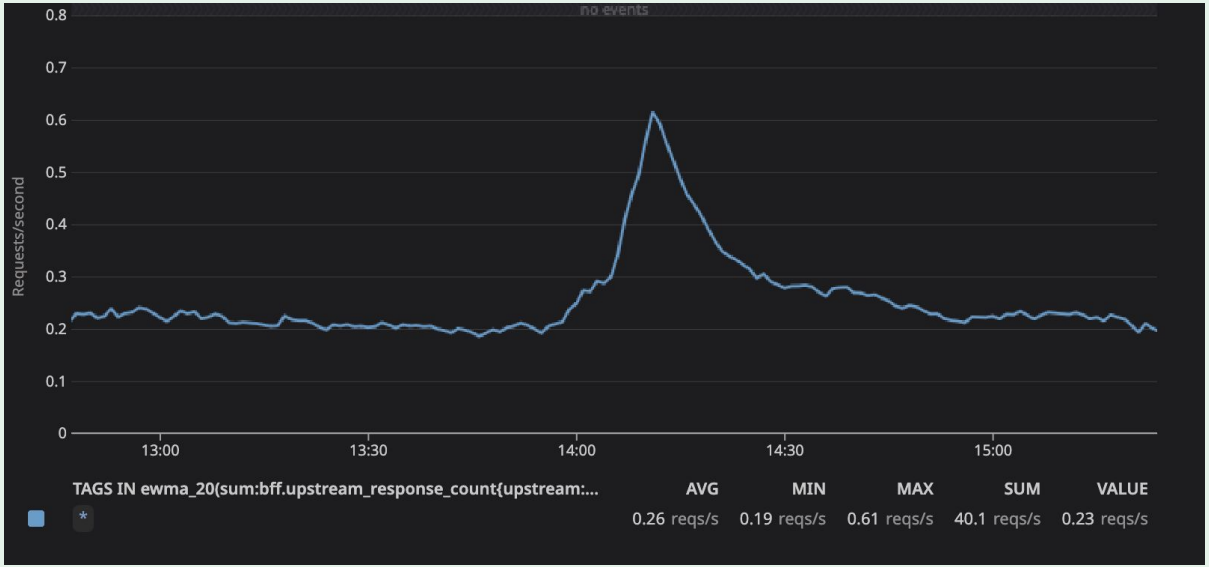
slow and steady



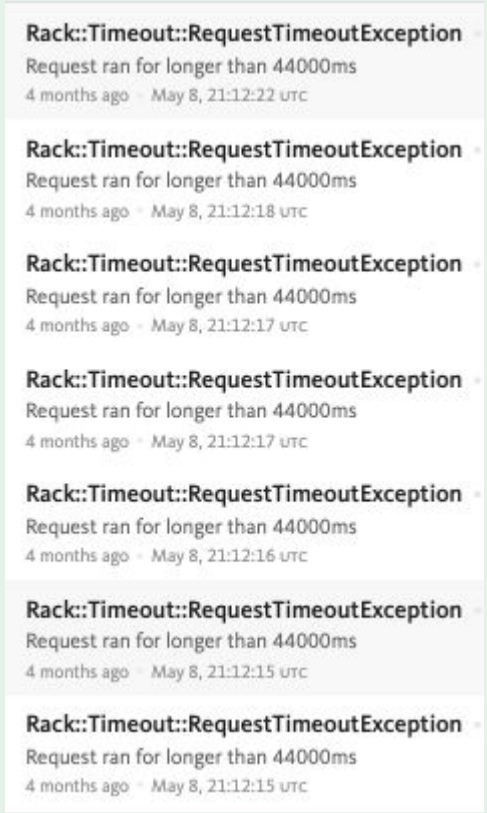
The Big Rock

The Symptom


20
15
10
5
0
13:00
13:30
14:00
14:30
15:00
TAGS
METRIC
AVG
MIN
MAX
SUM
VALUE
*
sidecars
3.84
1
9
73
—
*
pods
4.29
3
16
673
3.00


no events
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Requests/second
13:00
13:30
14:00
14:30
15:00
TAGS IN ewma_20(sum:bff.upstream_response_count{upstream:...
AVG
MIN
MAX
SUM
VALUE
*
0.26 reqs/s
0.19 reqs/s
0.61 reqs/s
40.1 reqs/s
0.23 reqs/s

They’re all timeouts



What didn’t work

- Both client and server on mesh
- Isolated Kubernetes node
- More memory/CPU
- conntrack allowances
- Any sort of reproduction in staging

YOU!

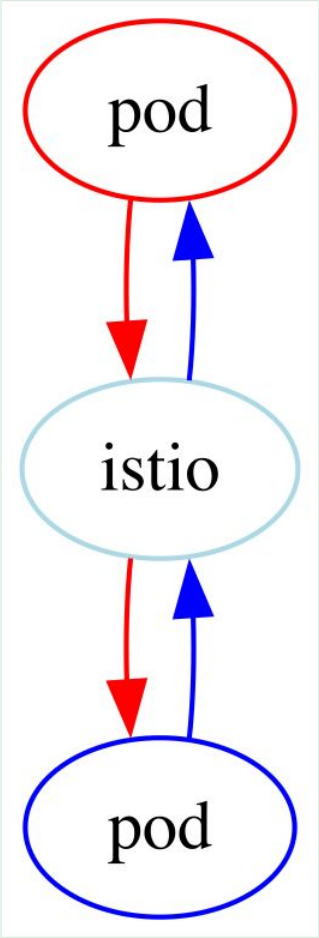
Ongoing work!

- TProxy?
- Nftables / conntrack
- Combinatorics

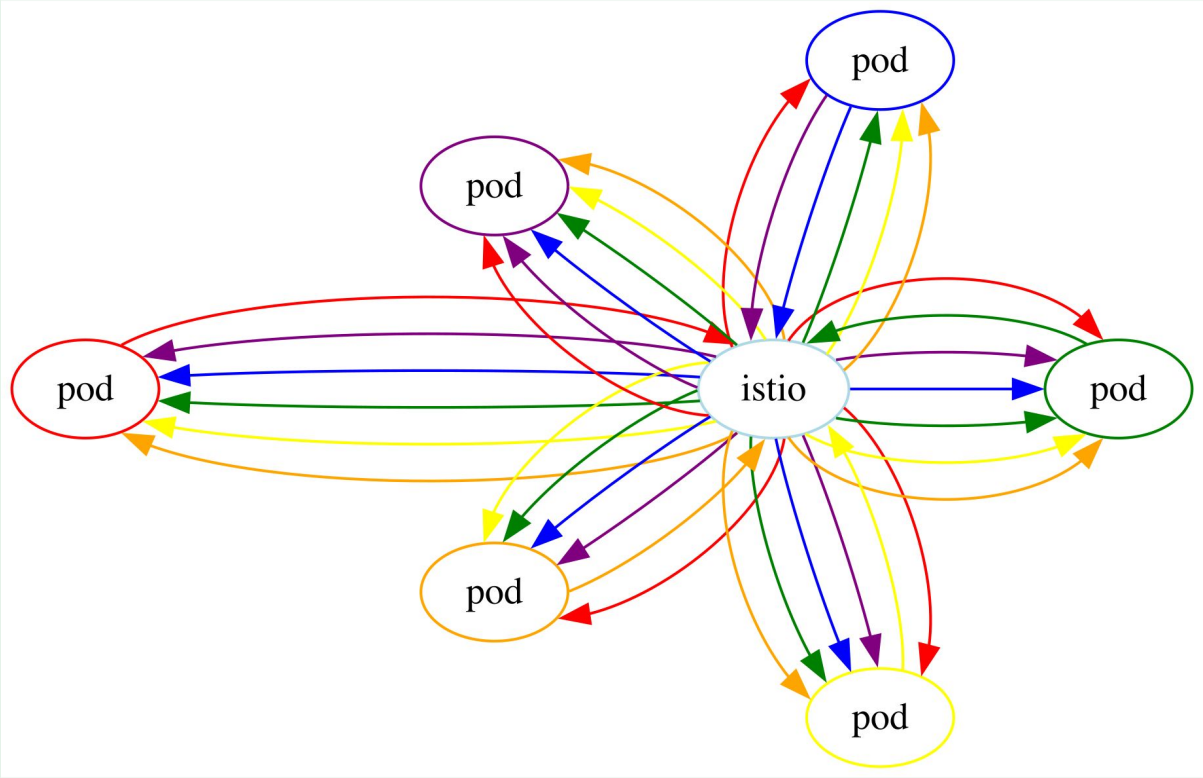
Ongoing work!

- TProxy?
- Nftables / conntrack
- **Combinatorics**

Two pods

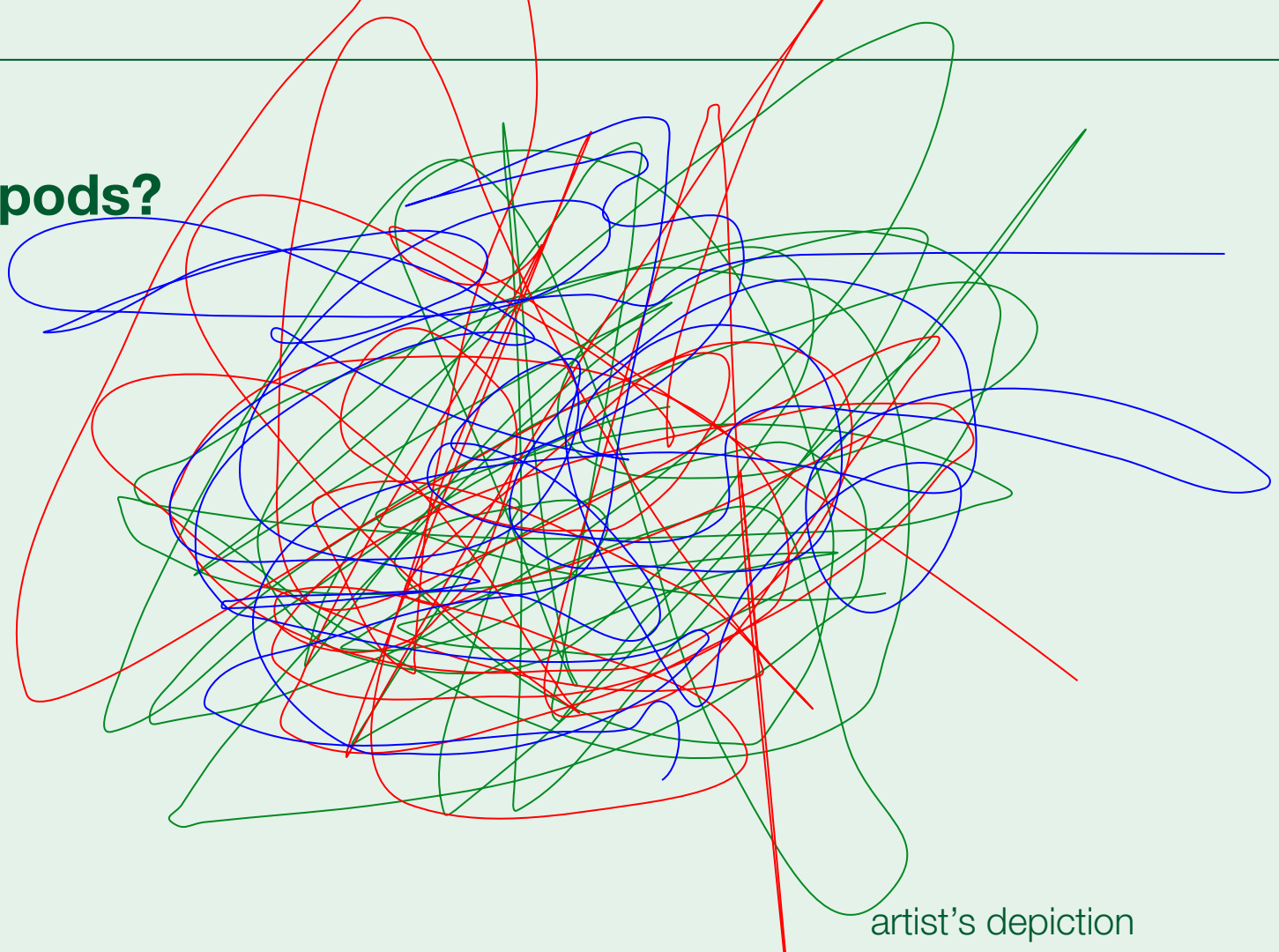


Six pods



4000+ pods?

4000+ pods?



artist’s depiction

PagerDuty

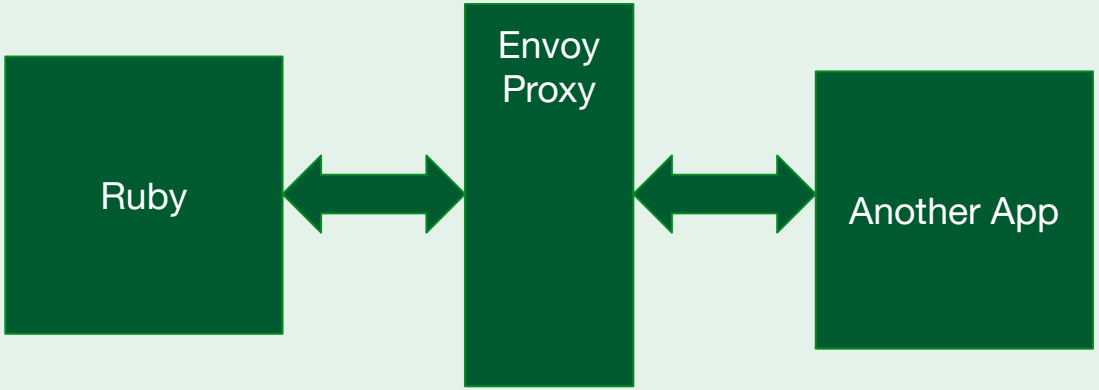
Random Gotchas

legos on the floor

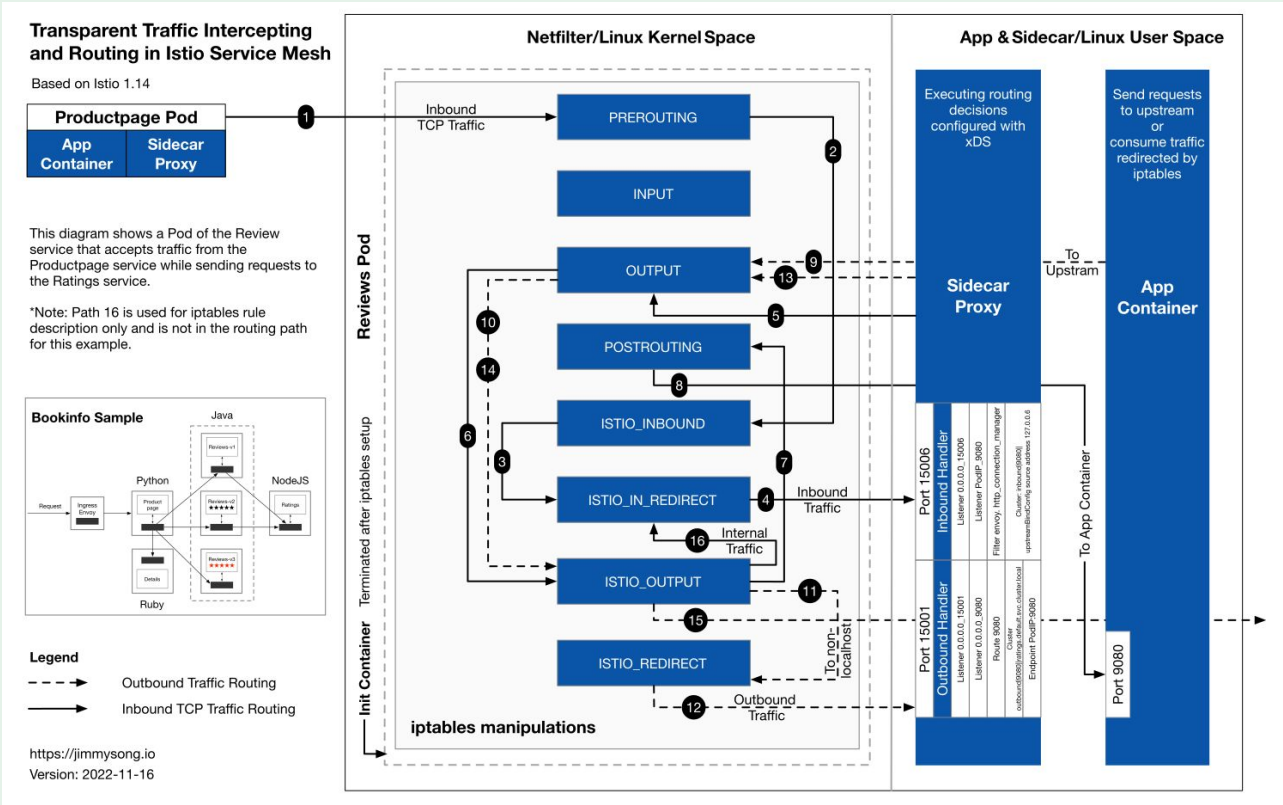
Not everything is http

```yaml
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: disable-mtls-for-smtp
  namespace: postfix-email-ingestion
spec:
  selector:
    matchLabels:
      app.kubernetes.io/name:
postfix-email-ingestion
  mtls:
    mode: UNSET
  portLevelMtls:
    25:
      mode: DISABLE
```

Normal Envoy flow



“Transparent Proxy” isn’t perfect

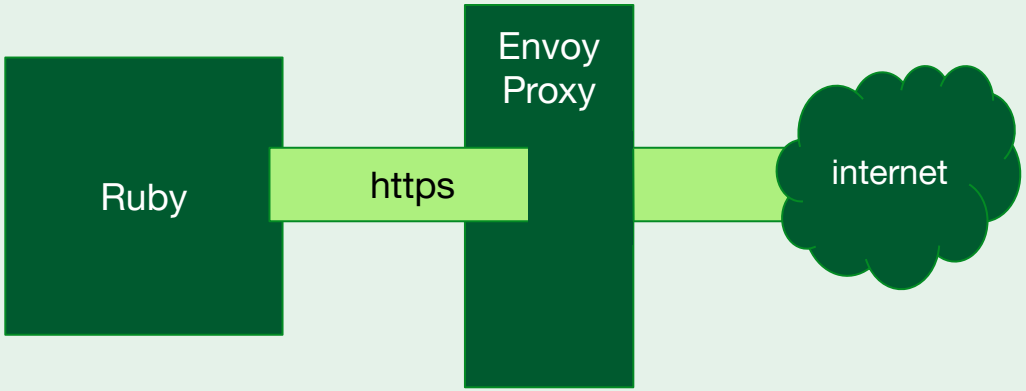


https://jimmysong.io/en/blog/sidecar-injection-iptables-and-traffic-routing/

Proxied TLS issues

```
SSL_write() error: error:1409E10F:SSL routines:ssl3_write_bytes:bad length
```

Typhoeus (libcurl) to Faraday(net/http)



No native rate limiting :(

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: filter-ratelimit
  namespace: istio-system
spec:
  workloadSelector:
    # select by label in the same namespace
    labels:
      istio: ingressgateway
  configPatches:
    # The Envoy config you want to modify
    - applyTo: HTTP_FILTER
      match:
        context: GATEWAY
        listener:
          filterChain:
            filter:
              name: "envoy.filters.network.http_connection_manager"
```

Max header Size

Envoy Filters

```
spec:
  configPatches:
    - applyTo: NETWORK_FILTER
      match:
        context: SIDECAR_INBOUND
        listener:
          filterChain:
            filter:
              name: envoy.filters.network.http_connection_manager
      patch:
        operation: MERGE
        value:
          typed_config:
            '@type': >-

type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.
v3.HttpConnectionManager
            max_request_headers_kb: 128
  workloadSelector:
    labels:
      app.kubernetes.io/name: advance-configuration-service
```

Where do they go?

- Just read istio github issues until someone solves it

```
$ istioctl proxy-config clusters $POD -o json | wc -l
4655
```

jq?

```
.configs[] |
select( ."@type" |
contains("Listeners") ) |
.dynamic_listeners[] |
select (.name ==
"virtualInbound").active_state.listener.filter_chains[].filters[] |
select (.name == "envoy.filters.network.http_connection_manager")
```

what could possibly go wrong –

```
panic: runtime error: slice bounds out of range [-2:]

goroutine 19414 [running]:
github.com/envoyproxy/go-control-plane/envoy/config/core/v3.(*SocketAddress).MarshalToSizedBufferVTStrict(0xc0070b7730
, {0xc0013f0000, 0x8, 0x15be})
      github.com/envoyproxy/go-control-plane@v0.12.1-0.20240415211714-57c85e1829e6/envoy/config/core/v3/address_vtprot
o.pb.go:191 +0x415
github.com/envoyproxy/go-control-plane/envoy/config/core/v3.(*Address_SocketAddress).MarshalToSizedBufferVTStrict(0xa4
7?, {0xc0013f0000, 0x8, 0x0?})
      github.com/envoyproxy/go-control-plane@v0.12.1-0.20240415211714-57c85e1829e6/envoy/config/core/v3/address_vtprot
o.pb.go:507 +0x94
github.com/envoyproxy/go-control-plane/envoy/config/core/v3.(*Address).MarshalToSizedBufferVTStrict(0xc00608cc80,
{0xc0013f0000, 0x8, 0x15be})
      github.com/envoyproxy/go-control-plane@v0.12.1-0.20240415211714-57c85e1829e6/envoy/config/core/v3/address_vtprot
o.pb.go:490 +0x19a
github.com/envoyproxy/go-control-plane/envoy/config/listener/v3.(*Listener).MarshalToSizedBufferVTStrict(0xc00304ad00,
{0xc0013f0000, 0x15be, 0x15be})
      github.com/envoyproxy/go-control-plane@v0.12.1-0.20240415211714-57c85e1829e6/envoy/config/listener/v3/listener_v
tproto.pb.go:782 +0x12e6
github.com/envoyproxy/go-control-plane/envoy/config/listener/v3.(*Listener).MarshalVTStrict(0xc00304ad00)
```

Resource Utilisation

Can’t autoscale sidecars :(

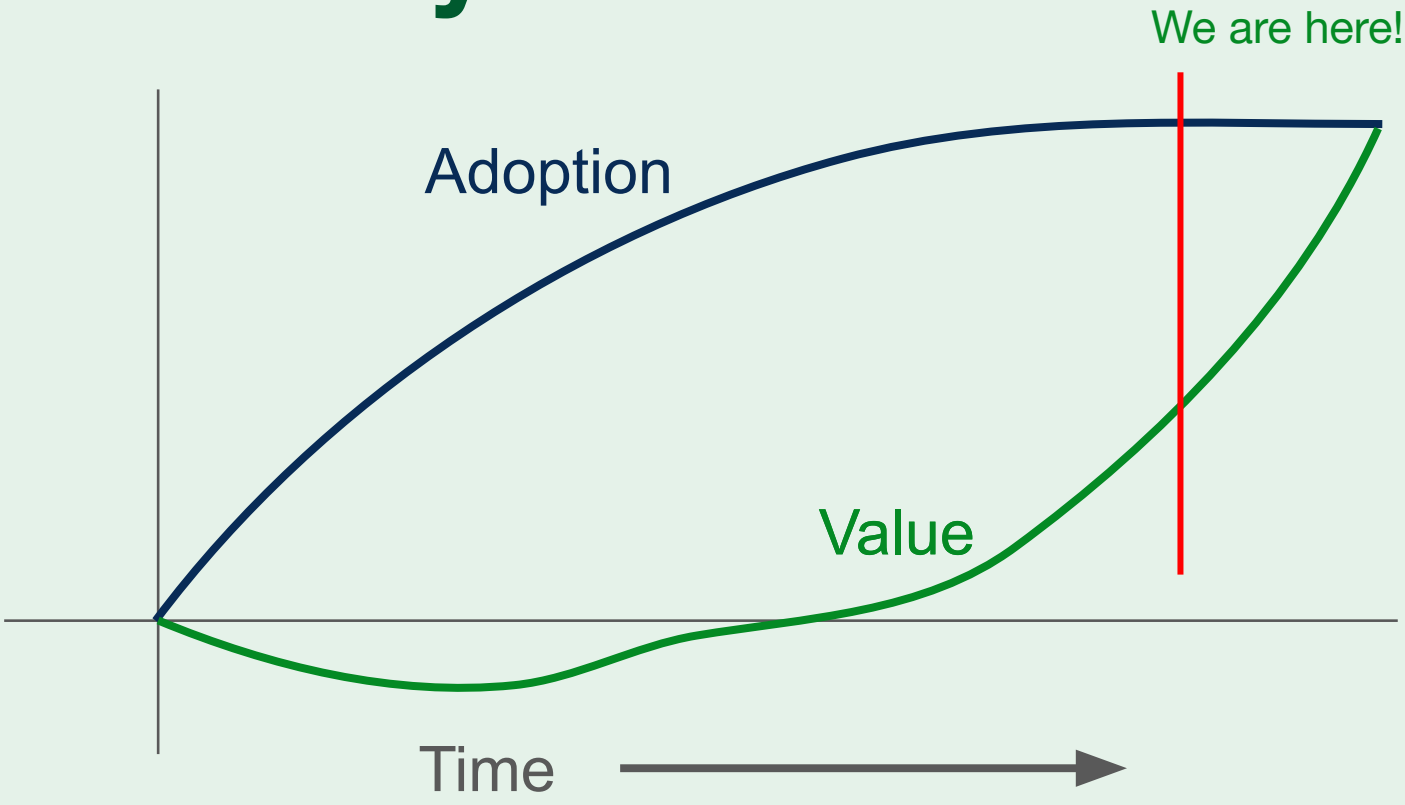
What is the problem?

The service mesh sidecar (Envoy proxy) is exhibiting high resource usage, which can lead to instability. You may be here because the service mesh sidecar monitoring module service_mesh of terraform-pd-service has referred you to this runbook.

CronJob support required a Kubernetes Upgrade

- Native Sidecar supported added in k8s 1.29
- Stable now!
- Default in Istio!
- Don’t worry about it!!

The Reality



Thank you

Liz Frost
lfrost@pagerduty.com

Booth 26
Shifts: Weds / Thurs morning