# Istio, do you need more Kubernetes networking headaches?

—

Richard Bakker
Technical Sales



IBM Cloud

# Agenda

**Kubernetes Networking**

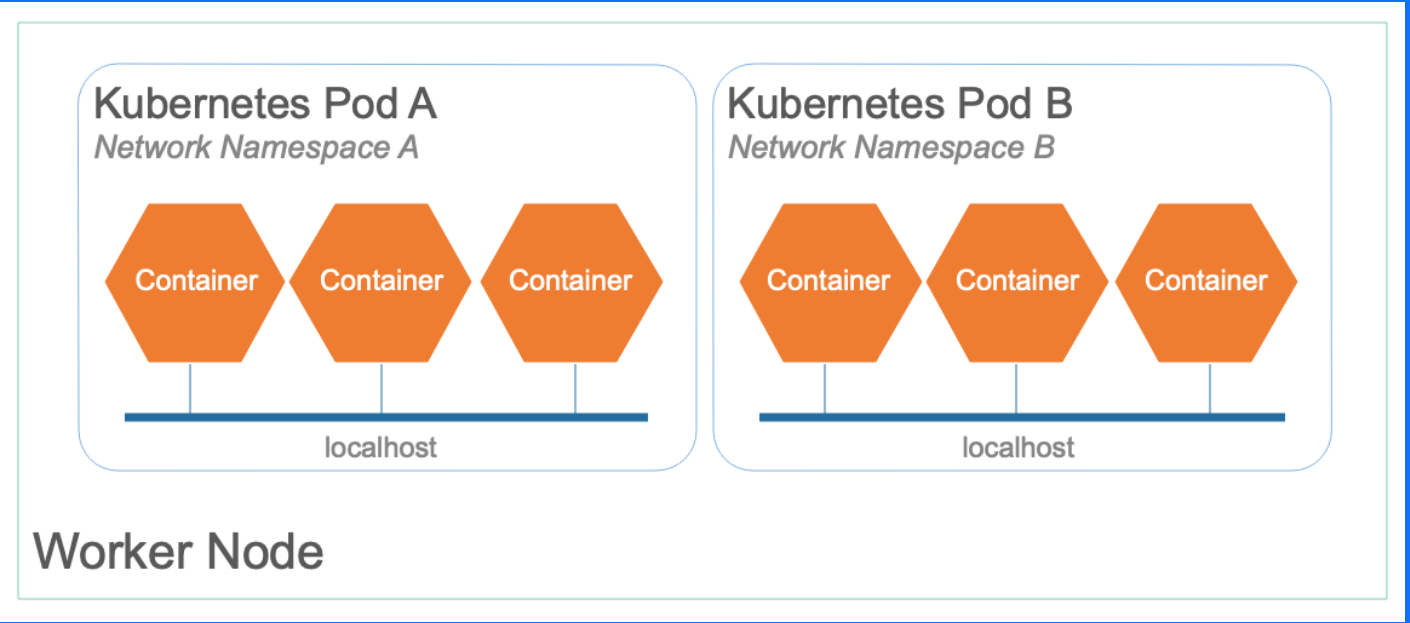
**Istio Use Cases**
Traffic Management
Policies and Security
Observability

**Istio Architecture**
Resources
Data Plane
Control Plane

**What's next**
Is it ready?
Getting started

# Pods

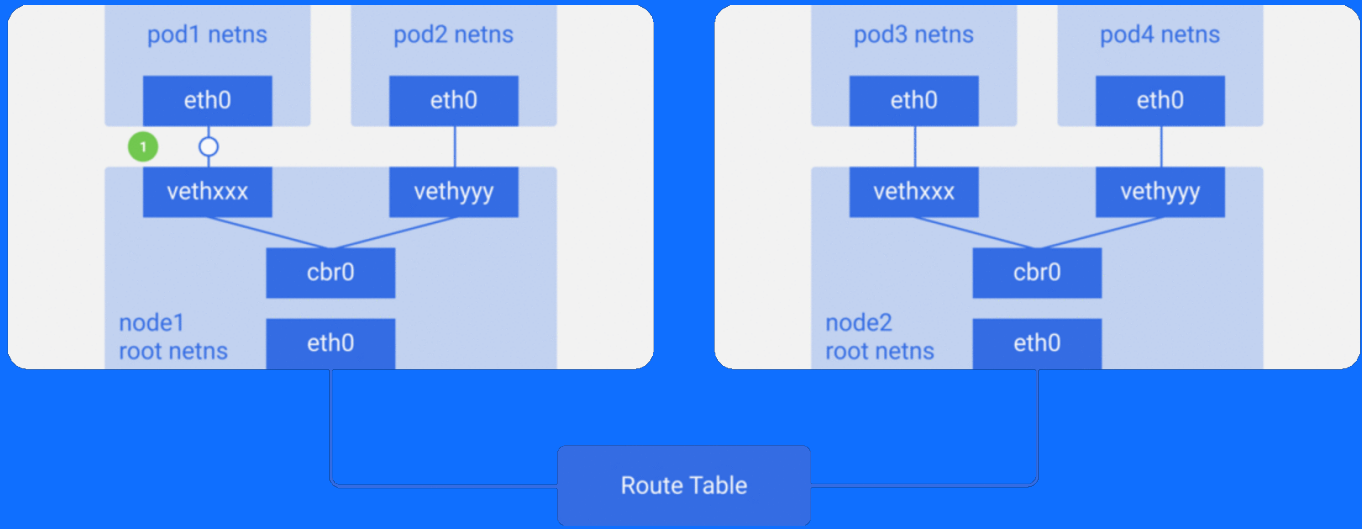
- Containers run in Pods
- Share a network namespace
- Can communicate using local host



# Pod network

Source: https://itnext.io/an-illustrated-guide-to-kubernetes-networking-part-1-d1ede3322727

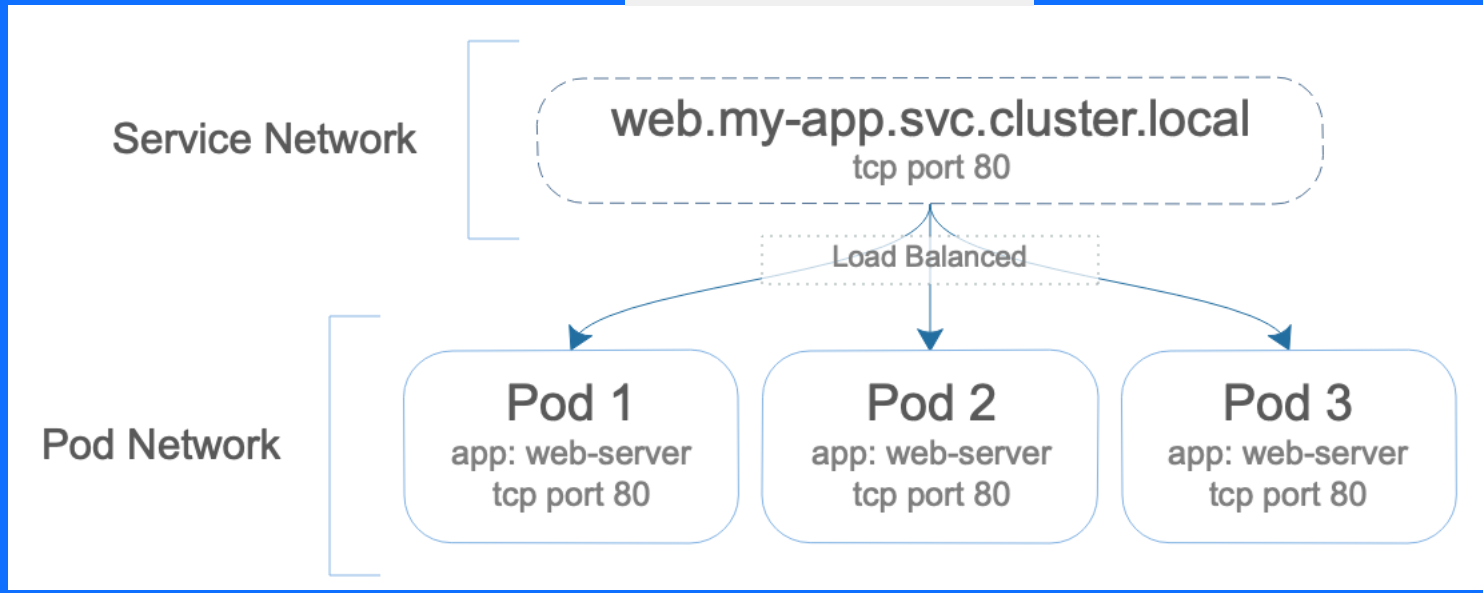
- Pods get IP address
- Containers bind ports
- Address block is Pod network
- Pod management can change IP addresses



# Service network

- Service defines a name
- Service IP address a bit more stable
- Service finds Pods

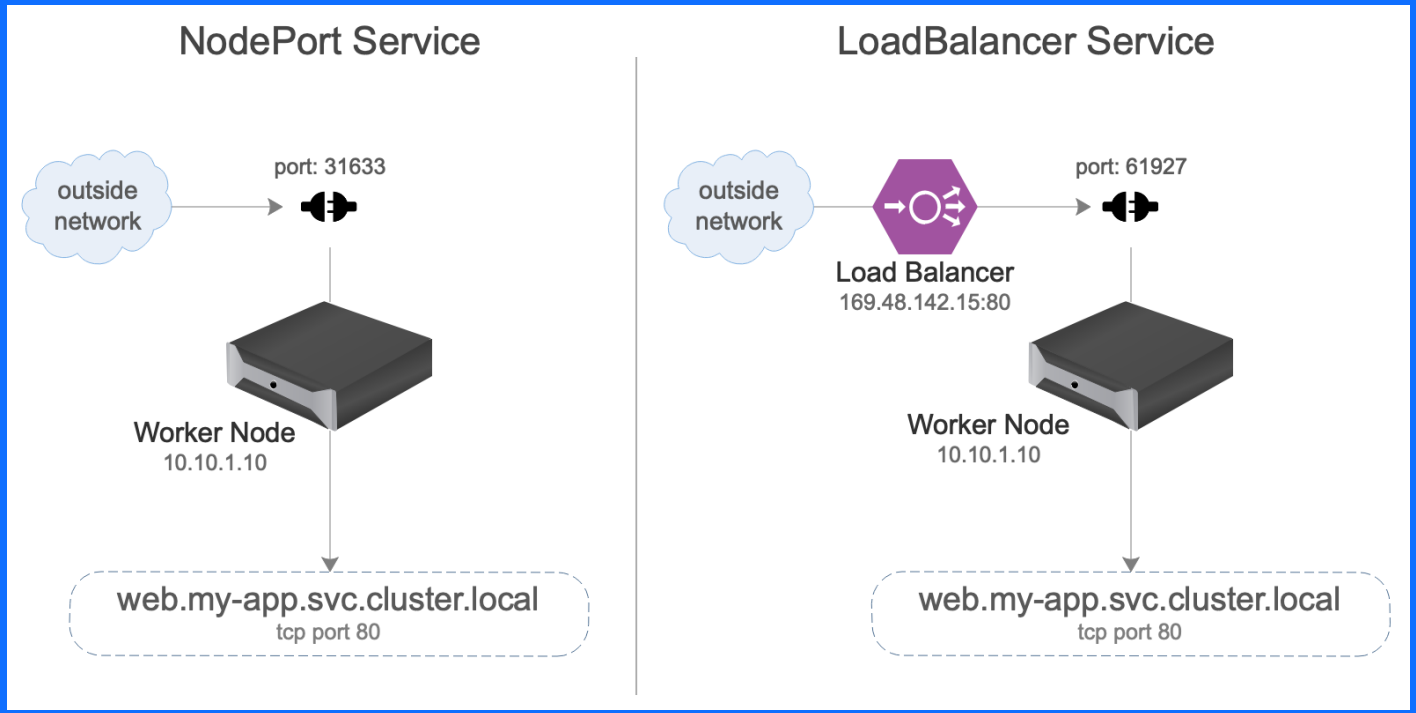
```
kind: Service
apiVersion: v1
metadata:
  name: web
  namespace: my-app
spec:
  selector:
    app: web-server
  ports:
  - name: web
    protocol: TCP
    port: 80
    targetPort: 80
```



# Service access

Source: If applicable, describe source origin

- ClusterIp: within cluster
- NodePort: direct access to worker node, random port
- LoadBalancer: external IP address



# Istio Use Cases

Traffic Management
- Request Routing
- Traffic Shifting
- Fault Injection
- Circuit Breaking

Policies and Security
- Secure communication
- Rate limiting

Observability
- Metrics
- Distributed Traces

# Traffic Management – Request Routing (A/B Testing)

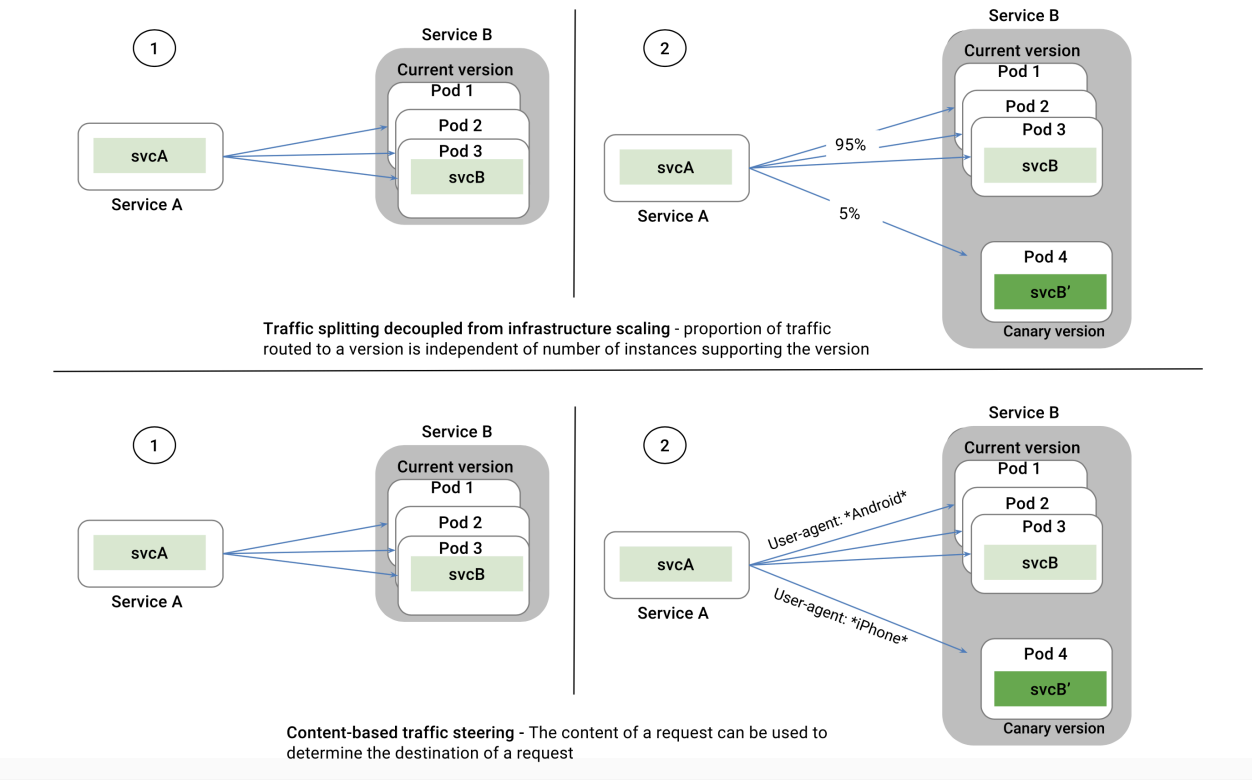
Source: https://www.invespcro.com/blog/multiple-testing-problem-how-adding-more-variations-to-your-ab-test-will-impact-your-results/

- Route request to multiple versions
- Based on URL
- Based on HTTP header

# Traffic Management – Traffic Shifting a.k.a. Canary Deployment

Source: If applicable, describe source origin

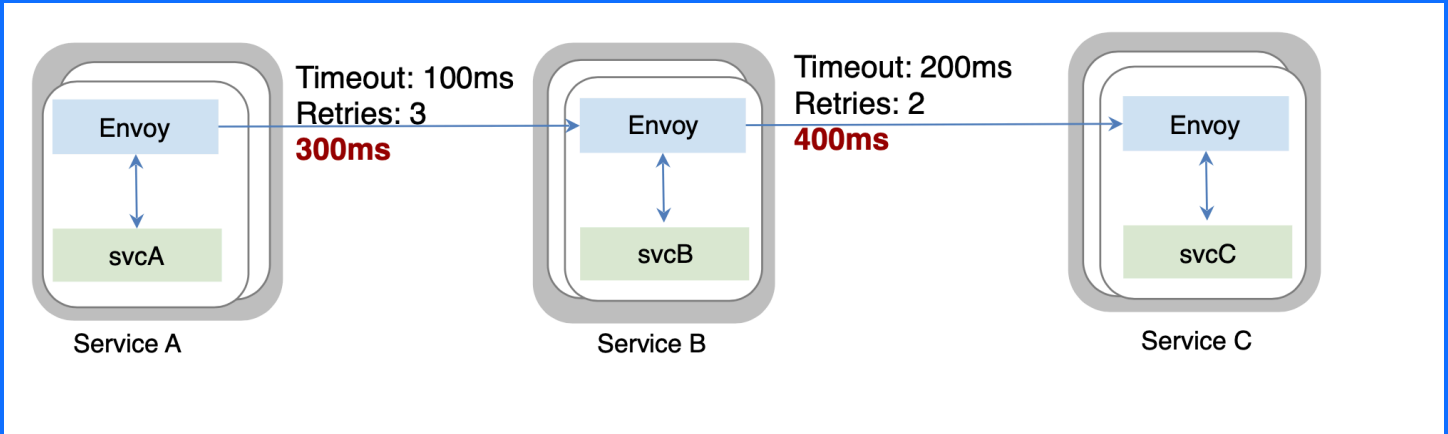
- Route request gradually to a newer version
- Applying weights
- Can also match on HTTP header
- Does not depend on scaling



# Traffic Management – Fault Injection

Source: aapc.com

- Test robustness of your system
- At the application layer
- Introduce delays
- Abort a service



# Traffic Management – Circuit Breaker

- Reduce the impact of network issues
- Trip on number of connections, requests
- Configure outlier detection

Source: If applicable, describe source origin

# Policies and Security – Secure Communication

Source: itsfoss.com

- Service-to-service authentication
- Strong Identity
- Secure communication
- Key Management system

# Policies and Security – Rate Limiting

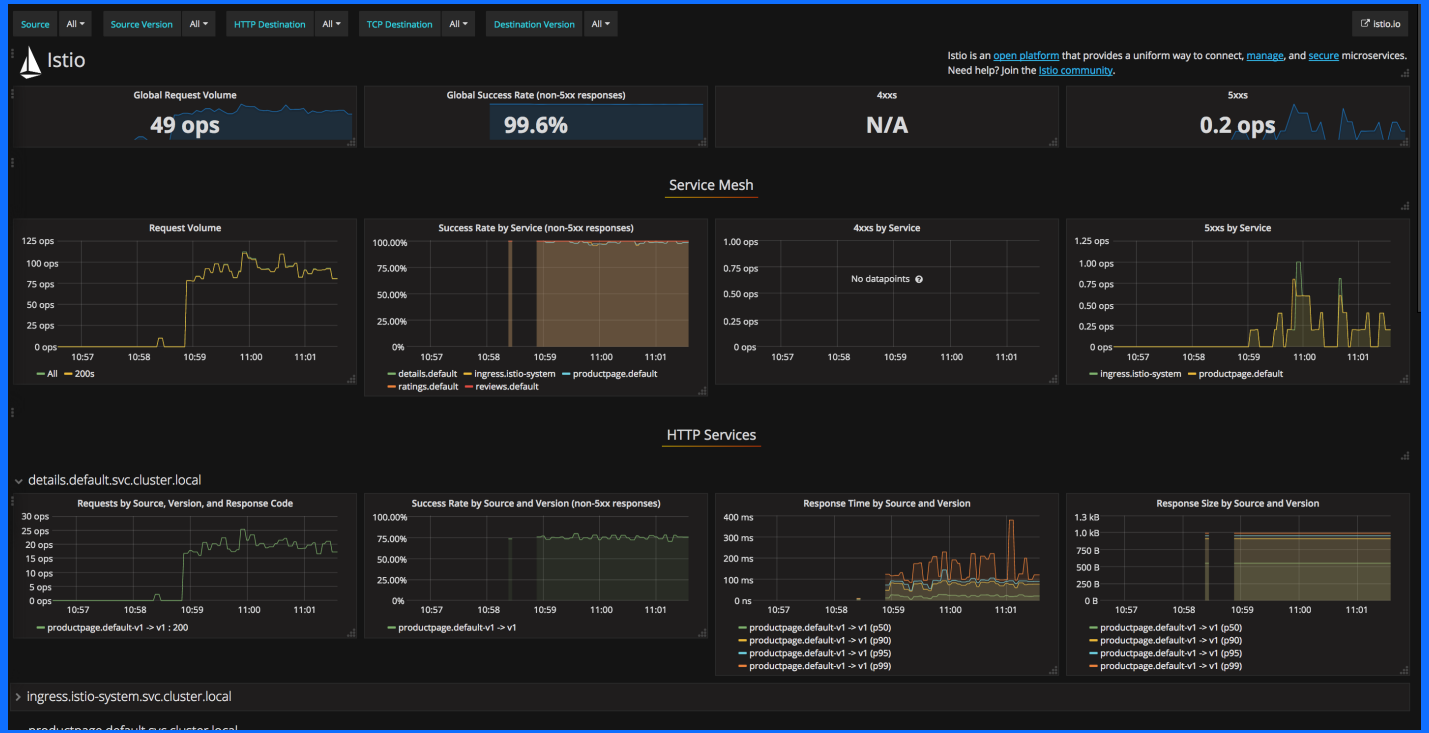
Source: If applicable, describe source origin

- Set Quota for Client Requests
- Can exempt certain clients
- No rate or all:
- Denials
- Blacklist
- Whitelist

# Observability - Metrics

Source: If applicable, describe source origin

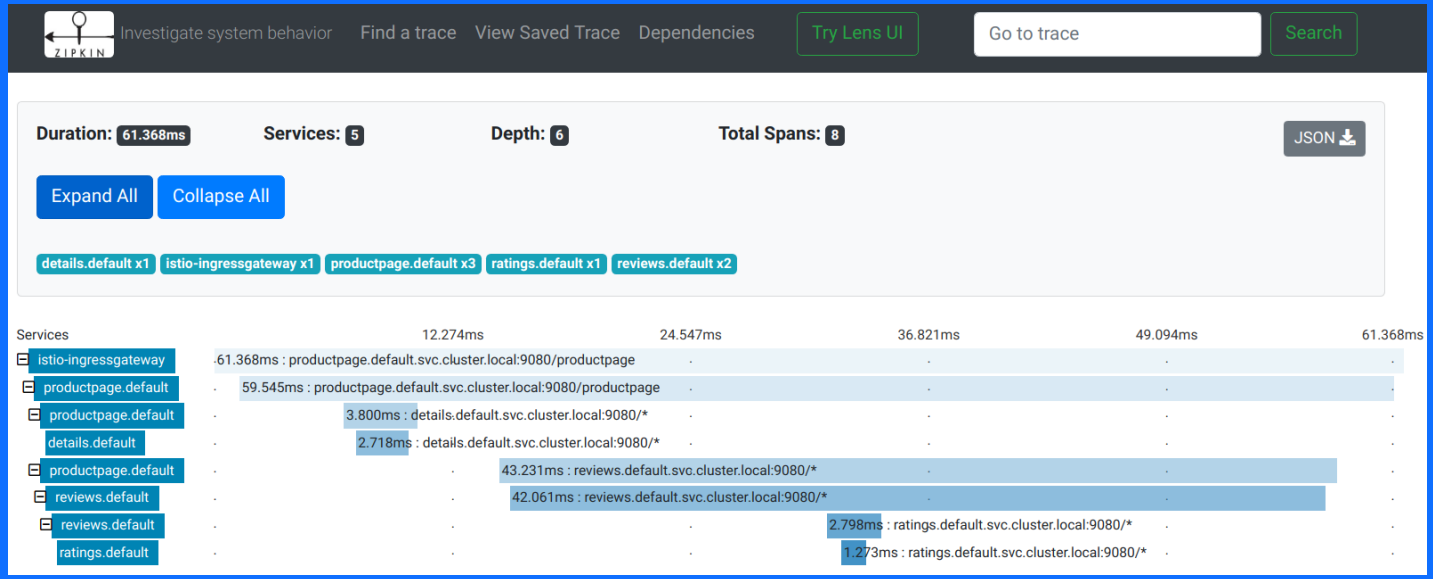
- Service traffic: in, out, within
- Volume, error rates, response times
- Proxy metrics
- Control Plane metrics



# Observability – Distributed Tracing

Source: If applicable, describe source origin

- Monitor individual requests
- Understand service dependencies
- Find the latencies

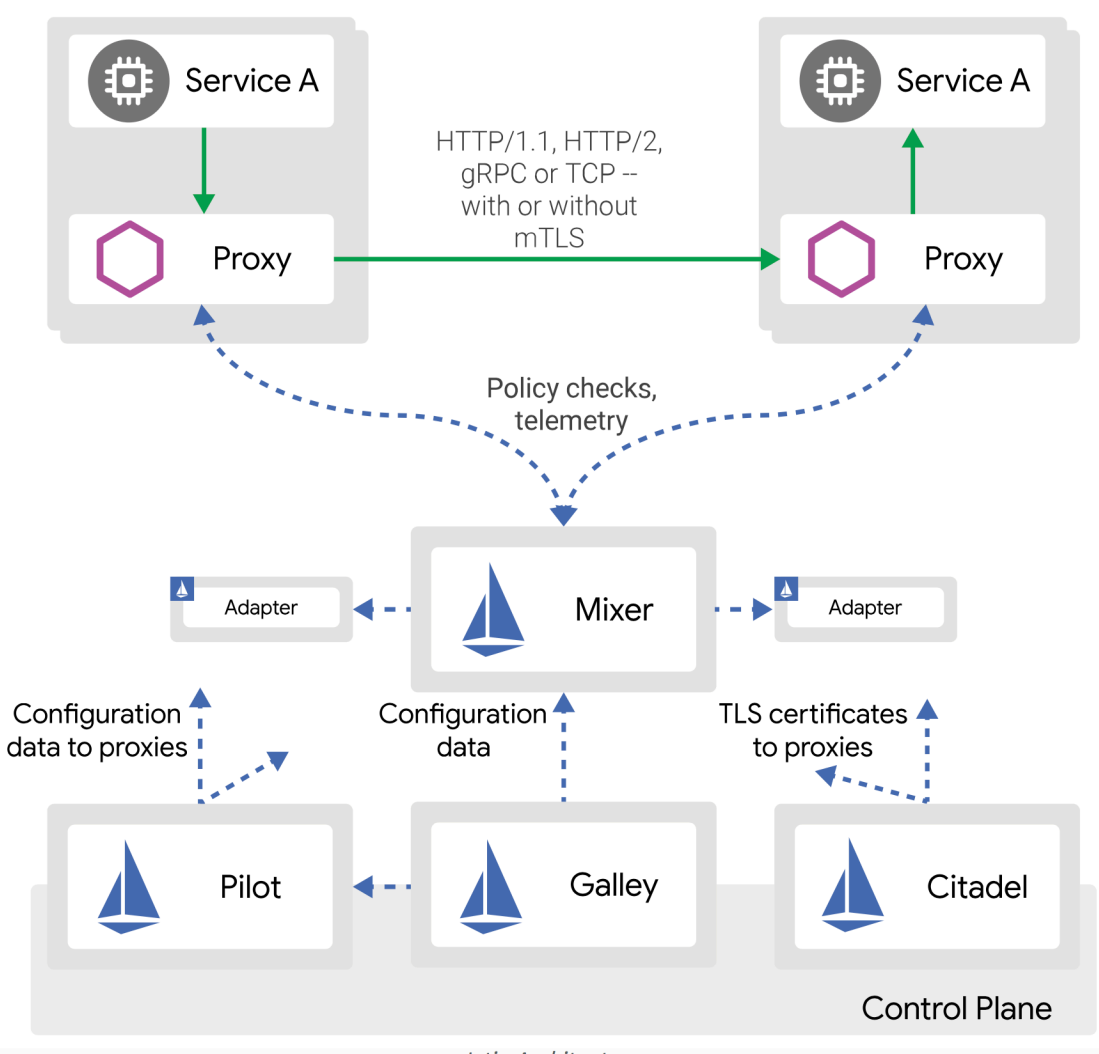


# Istio Architecture

Data Plane
- Envoy

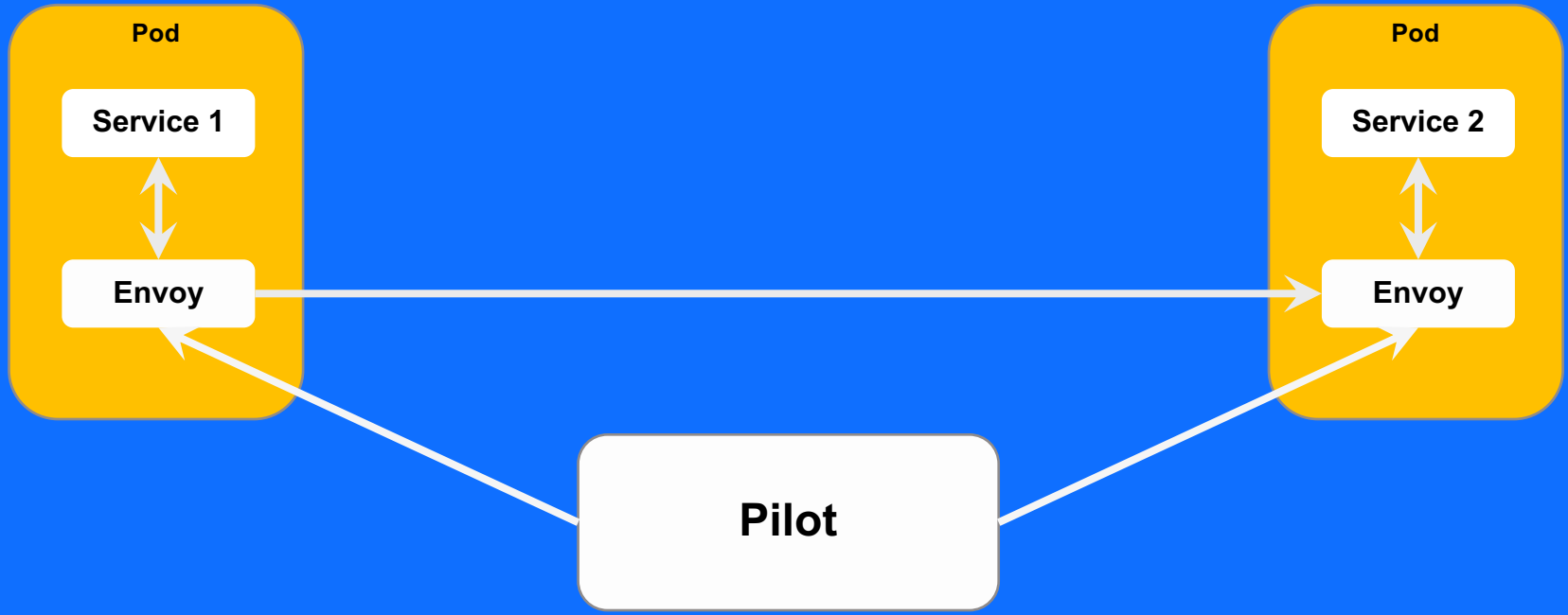
Resources
- Virtual Services
- Destination Rules
- Gateways

Control Plane
- Mixer
- Pilot
- Citadel
- Galley

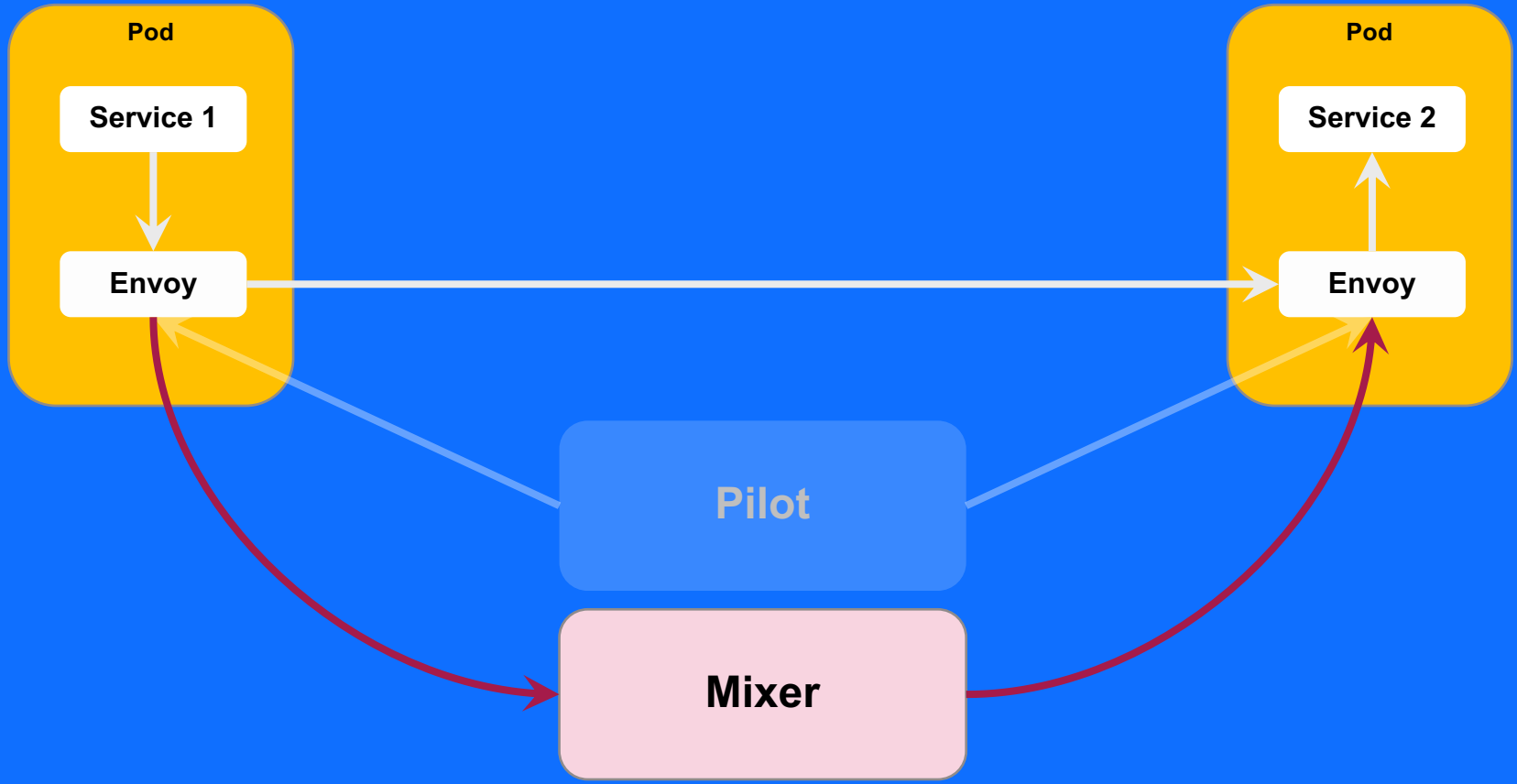



*Istio Architecture*

# Pilot: Instruct on routing



# Mixer: Access control, policies and telemetry collection



# Citadel: authentication, identity and credential management

Service 1

Service 2

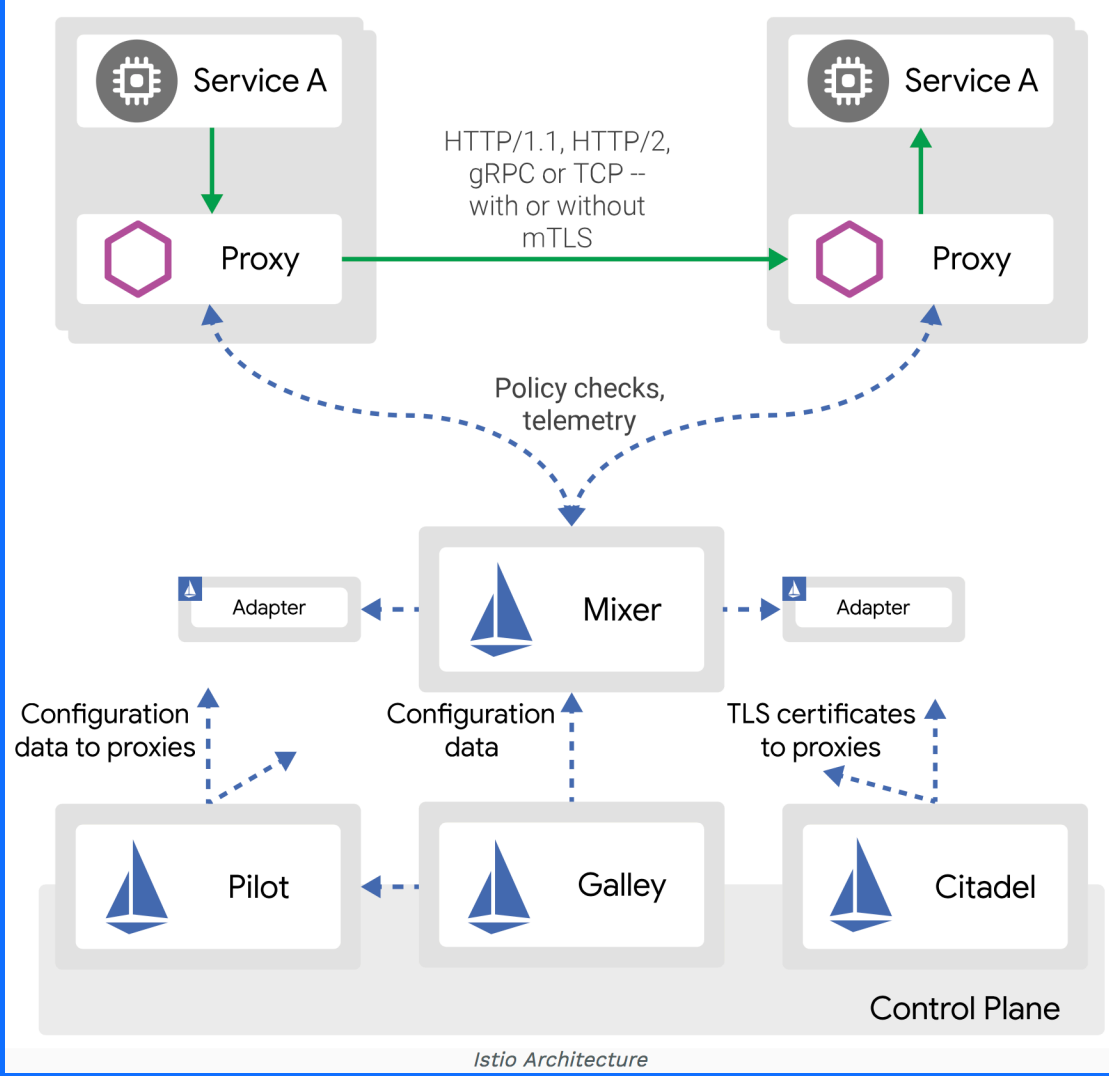
**Mutual TLS & Secure Naming**

```
SAN: "spiffe://myorg.com/ns/prod/sa/foo"
- Namespace: prod
- Service account: foo
```

```
SAN: "spiffe://myorg.com/ns/prod/sa/bar"
- Namespace: prod
- Service account: bar
```

**Istio Certificate Authority**

# Putting it all together




*Istio Architecture*

# Example for Creating Istio resources

```
NAME         TYPE           CLUSTER-IP      EXTERNAL-IP     PORT(S)        AGE
guestbook    LoadBalancer   172.21.36.181   169.61.37.140   80:32149/TCP   5d
```

```
NAME                              READY   STATUS    RESTARTS   AGE
guestbook-v1-89cd4b7c7-frscs      2/2     Running   0          5d
guestbook-v2-56d98b558c-mzbxk     2/2     Running   0          5d
```

```
kubectl label namespace default istio-injection=enabled
```

```
NAME              STATUS   AGE    ISTIO-INJECTION
default           Active   271d   enabled
istio-system      Active   5d2h
...
```

# Resources for traffic management

virtualservice-all-v1.yaml

```yaml
apiVersion: networking.istio.io/v1alp
kind: VirtualService
metadata:
  name: virtual-service-guestbook
spec:
  hosts:
    - '*'
  gateways:
    - guestbook-gateway
  http:
    - route:
        - destination:
            host: guestbook
            subset: v1
```

guestbook-destination.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: destination-rule-guestbook
spec:
  host: guestbook
  subsets:
  - name: v1
    labels:
      version: "1.0"
  - name: v2
    labels:
      version: "2.0"
```

guestbook-gateway.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: guestbook-gateway
spec:
  selector:
    istio: ingressgateway # use istio default
  servers:
  - port:
      number: 80
      name: http
      protocol: HTTP
    hosts:
    - "*"
```

# A/B Testing, Canary Deployments

virtualservice-test.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: virtual-service-guestbook
spec:
  hosts:
    - '*'
  gateways:
    - guestbook-gateway
  http:
    - match:
        - headers:
            user-agent:
              regex: '.*Firefox.*'
      route:
        - destination:
            host: guestbook
            subset: v2
    - route:
        - destination:
            host: guestbook
            subset: v1
```

virtualservice-80-20.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: virtual-service-guestbook
spec:
  hosts:
    - '*'
  gateways:
    - guestbook-gateway
  http:
    - route:
        - destination:
            host: guestbook
            subset: v1
          weight: 80
        - destination:
            host: guestbook
            subset: v2
          weight: 20
```

# Fault Injection

03-half-second-timeout.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
        host: reviews
        subset: v2
    timeout: 0.5s
```

03-jason-7s-delay.yaml

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ratings
spec:
  hosts:
  - ratings
  http:
  - match:
    - headers:
        end-user:
          exact: jason
    fault:
      delay:
        percentage:
          value: 100.0
        fixedDelay: 7s
    route:
    - destination:
        host: ratings
        subset: v1
  - route:
    - destination:
        host: ratings
        subset: v1
```

# Circuit Breaker

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: httpbin
spec:
  host: httpbin
  trafficPolicy:
    connectionPool:
      tcp:
        maxConnections: 1
      http:
        http1MaxPendingRequests: 1
        maxRequestsPerConnection: 1
    outlierDetection:
      consecutiveErrors: 1
      interval: 1s
      baseEjectionTime: 3m
      maxEjectionPercent: 100
```

# What’s next?

2019 Istio Themes

- Project Sustainability
- Layering and Extensibility
- Improved Experience
- Performance and Scalability

Getting started:

https://github.com/IBM/istio101

https://github.com/IBM/microservices-traffic-management-using-istio

https://istio.io/docs/setup/getting-started/

# Should you?

Pro:
- Clean separation of network policies from coding
- Traffic management
- Security policies
- Observability

Con:
- Extra control plane to manage
  - Failures
  - Upgrades
- Performance overhead/resource usage
  - Request processing
  - Network latency

# Thank you

Richard Bakker
Technical Sales
—
richard.bakker@nl.ibm.com
+31-6-22 940 585
ibm.com