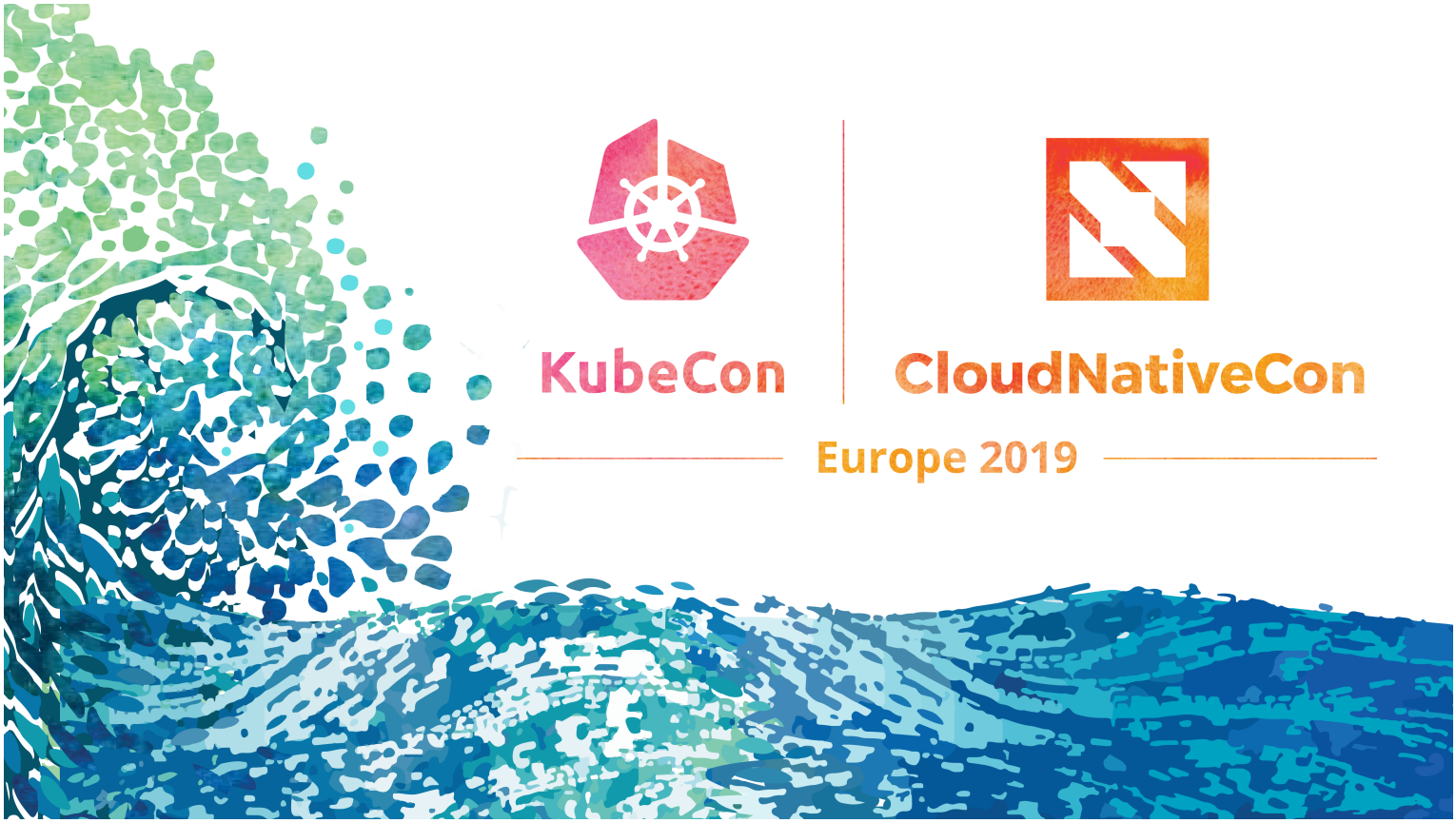

KubeCon
CloudNativeCon
Europe 2019

KubeCon | CloudNativeCon Europe 2019

Istio on Knative Lessons Learned

How Istio is Fit for Serverless Platform

Ying Chun Guo & Iris Ding, IBM China

About us

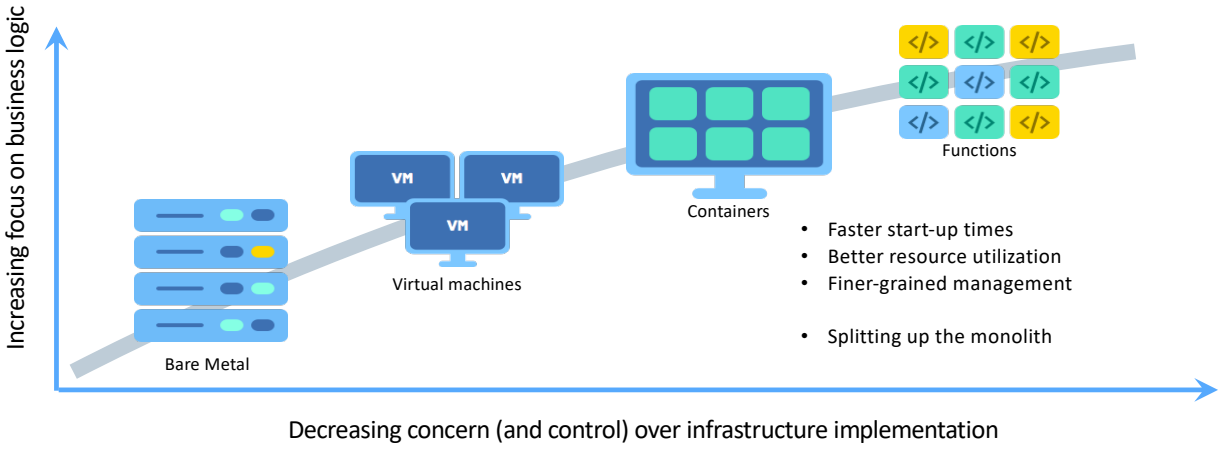
Ying Chun Guo “Daisy” @daisy-ycguo
Interested in Serverless
Contribute to Knative, Apache OpenWhisk

Shao Jun Ding “Iris” @irisdingbj
Interested in Service Mesh
Contribute to Isito

Agenda

- Serverless and Knative
- Service Mesh and Istio
- Benefits of Istio on Knative
- Costs of Istio on Knative
- Summary

Serverless


Increasing focus on business logic
Bare Metal
VM
VM
VM
Virtual machines
Containers
Functions
Faster start-up times
Better resource utilization
Finer-grained management
Splitting up the monolith
Decreasing concern (and control) over infrastructure implementation

Properties of Serverless

- Stateless
- Event Driven
- Auto-scaled / Scale-to-zero
- Short Lived
- Reduced Cost
- Faster Time to Market

To make your own Serverless platform.....

Open Source Serverless Project

Kubernetes

Knative

APACHE OpenWhisk

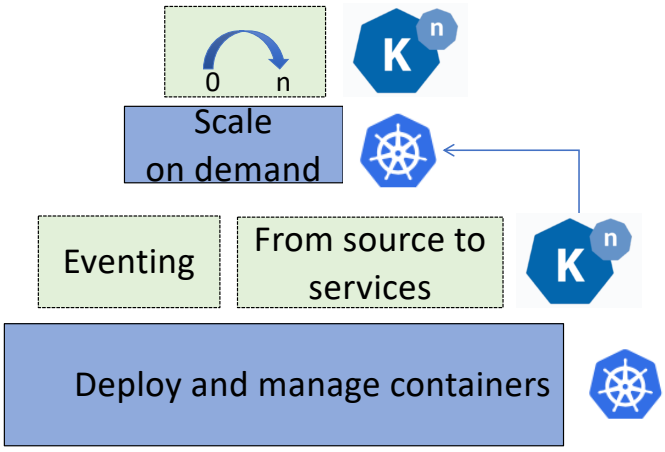
Kubeless

riff

OPENFAAS

Knative – Bring Serverless to Kubernetes

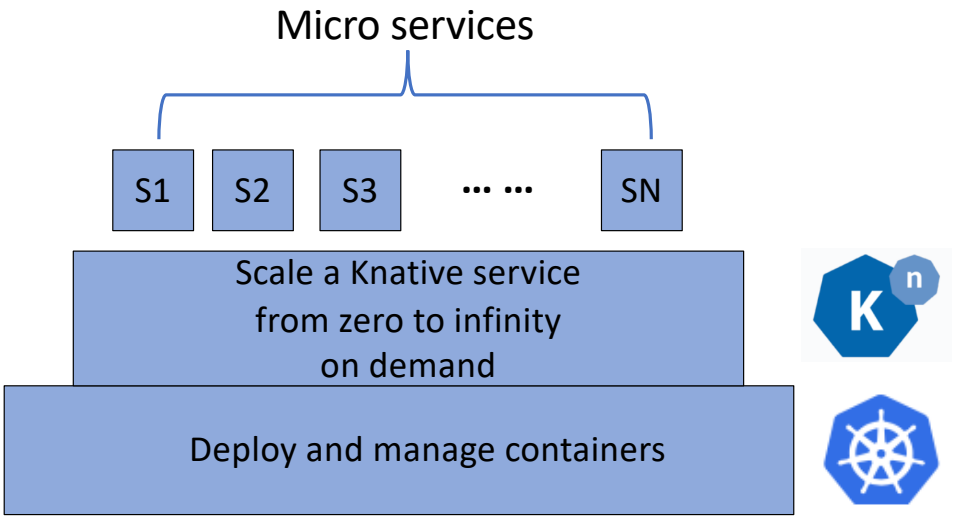
- Knative Building
- Knative Serving
- Knative Eventing



Micro services on Knative

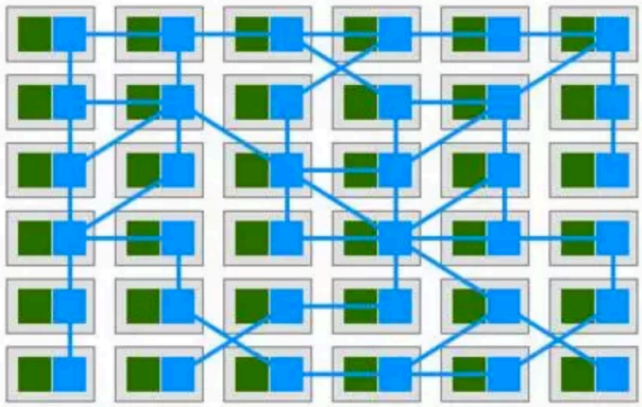
Users want to …

- Locate a service by a host name and path
- Control the traffics
- Secure services access
- Logging, monitoring, and tracing
- ……



Service Mesh

A service mesh provides a **transparent** and **language-independent** network for connecting, observing, securing and controlling the connectivity between services.



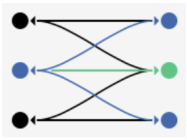
Istio

KubeCon CloudNativeCon Europe 2019

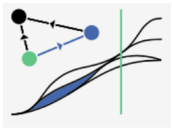
An open service mesh platform to connect, observe, secure, and control microservices.

Istio

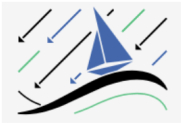
An open service mesh platform to connect, observe, secure, and control microservices.



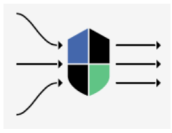
Connect: Traffic Control, Discovery, Load Balancing, Resiliency



Observe: Metrics, Logging, Tracing

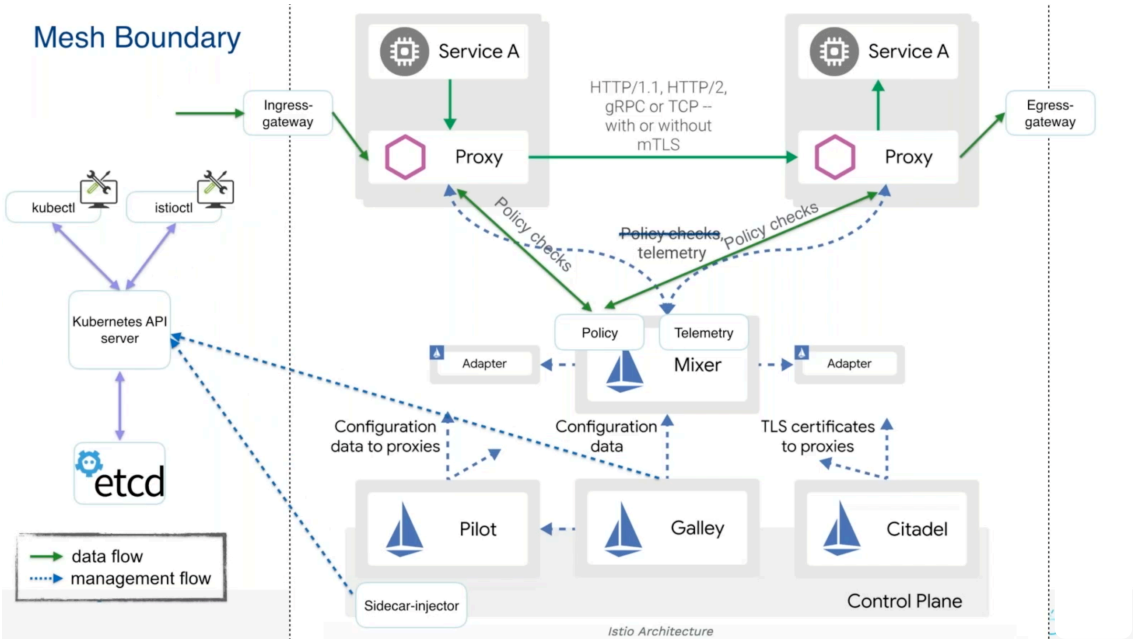


Secure: Encryption (TLS), Authentication, and Authorization of service-to-service communication

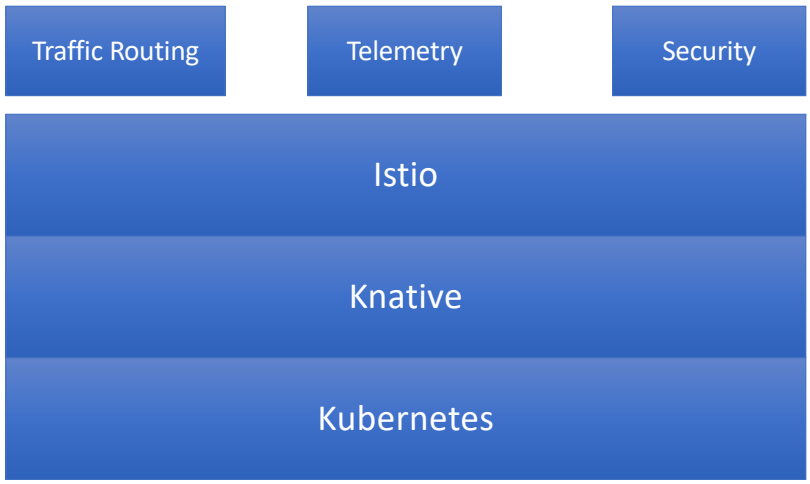


Control: Policy Enforcement

Istio architecture



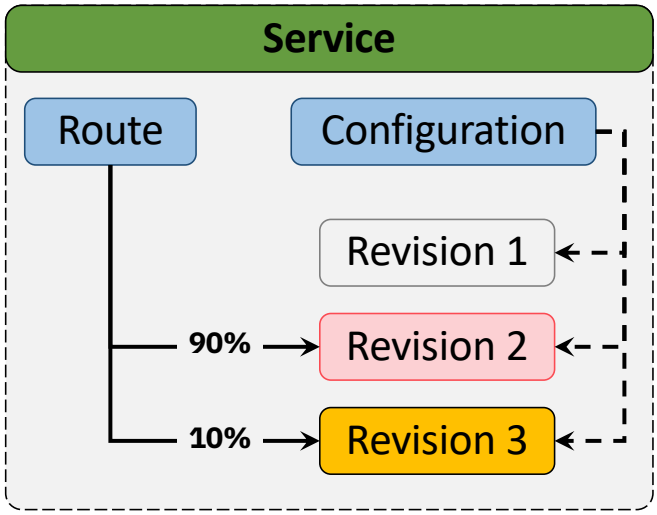
Istio on Knative



Knative basic concepts

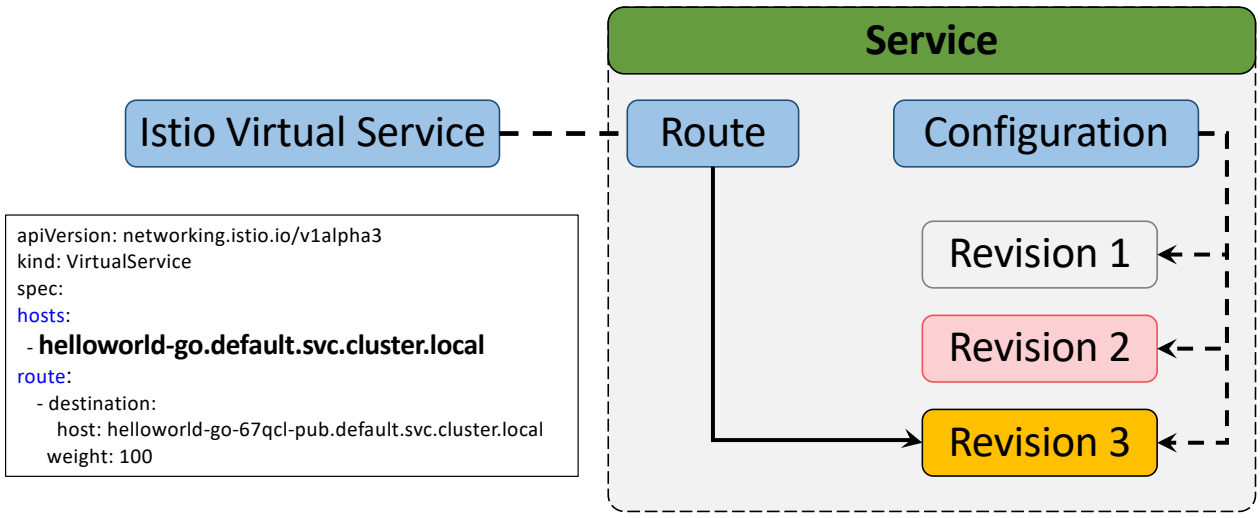
Manages the hosting aspects of your app

- **Service** - manages the lifecycle of app
- **Configuration** - manage history of app
- **Revision** - A snapshot of your app
  - Config and image
- **Route** - Endpoint and network traffic management



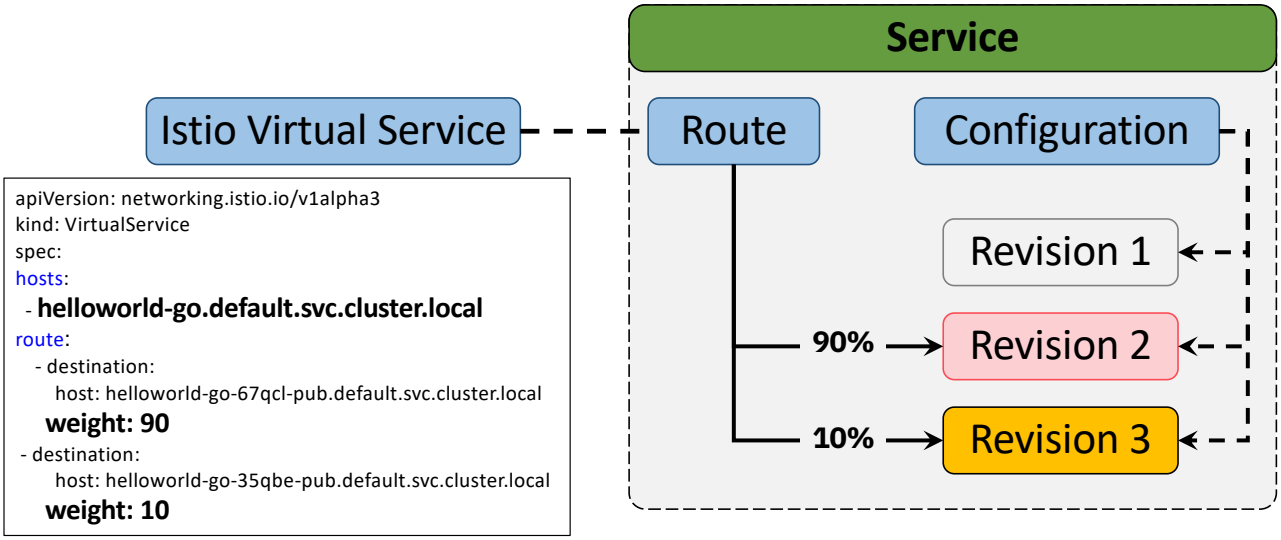
Traffic routing (1)

An Istio Virtual Service will be created for every Route

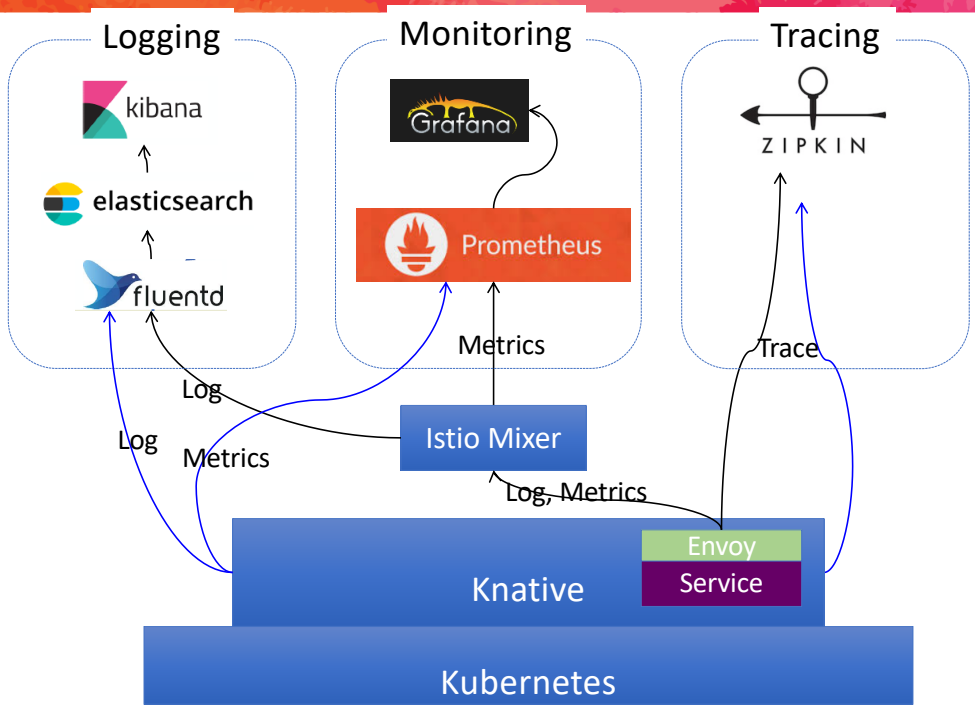


Traffic routing (2)

An Istio Virtual Service will be created for every Route



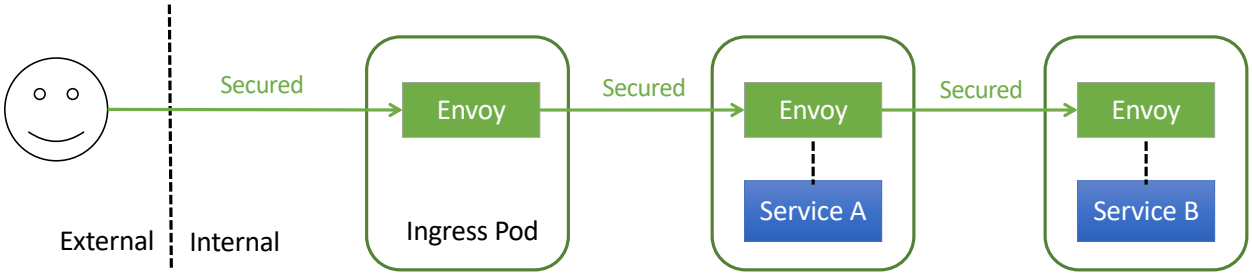
Telemetry


Logging
kibana
elasticsearch
fluentd
Monitoring
Grafana
Prometheus
Tracing
ZIPKIN
Metrics
Trace
Log
Log
Metrics
Istio Mixer
Log, Metrics
Envoy
Service
Knative
Kubernetes

Security

With side car injected：

- Can turn on mutual TLS, which secures service-to-service traffic within the cluster.
- Can turn on Gateway TLS with Secret Discovery Service (SDS)
- Can use the Istio authorization policy, controlling the access to each Knative service based on Istio service roles.



Benefits summary

- Istio taking care of Service Mesh
  - Traffic control
  - Secure services access
  - Telemetry
- It makes Knative **focus** on serverless

Benefits come at a price……

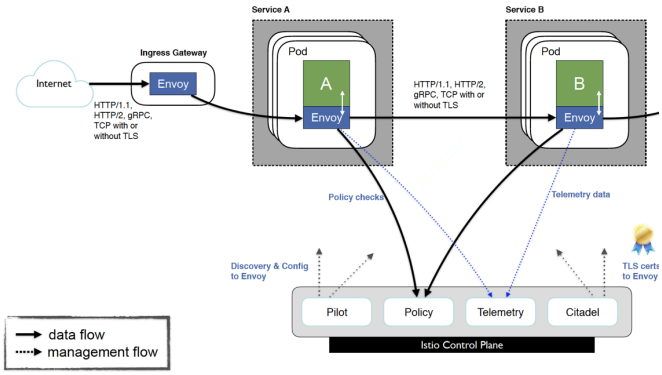
Any costs?

Choices of Istio installation

- Full Istio
- Full Istio with CNI plugin
- Full Istio without Policy
- Minimal Istio

Full Istio

- Full Istio with sidecar using init-container



7.316s : pod_creating

2.374s : container_startup_istio-init

6.558s : container_startup_istio-proxy

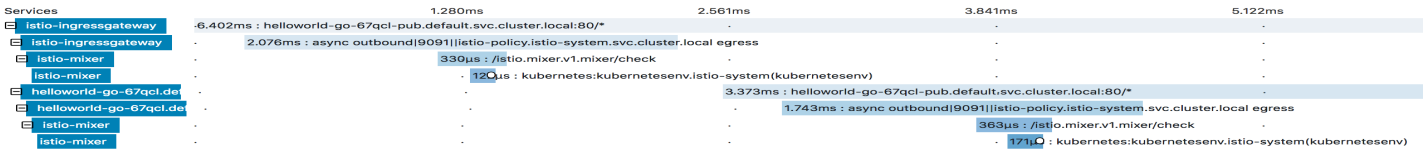
6.611s : container_startup_queue-proxy

3.377s : container_startup_user-container

Long cold start-up time

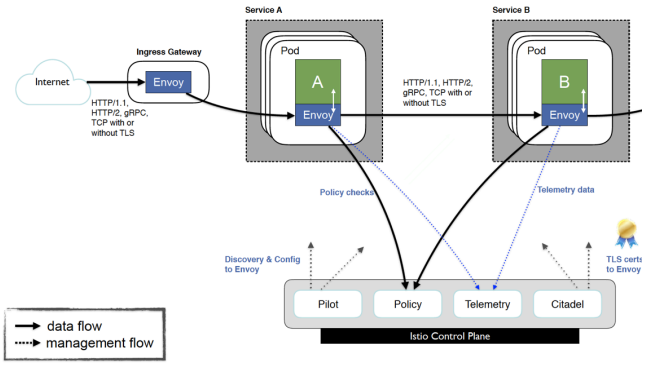
✓ Enjoy control and observability

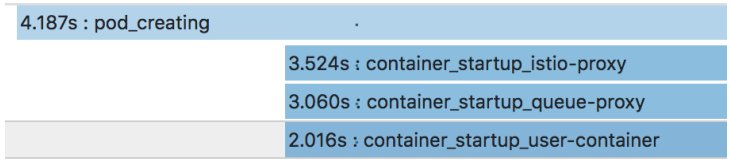
Additional latency for policy check



Full Istio with CNI plugin

- Full Istio with sidecar using CNI plugin



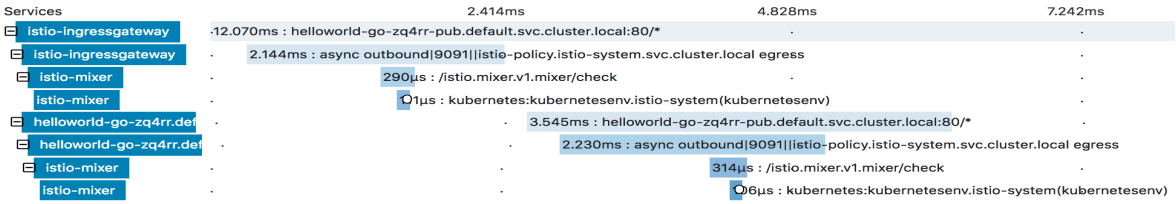


Long cold start-up time

✓ Enjoy control and observability

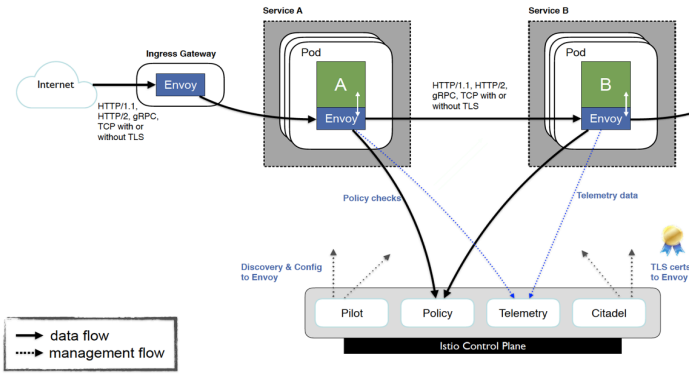
✓ Remove security requirement for pod

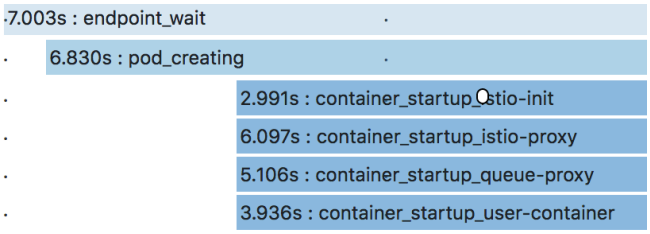
Additional latency for policy check



Full Istio without policy

- Full Istio with sidecar using init-container
- Policy disabled

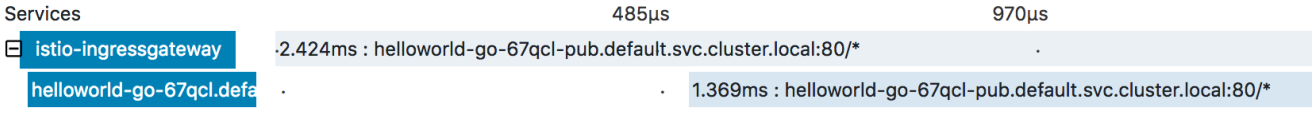




Long cold start-up time

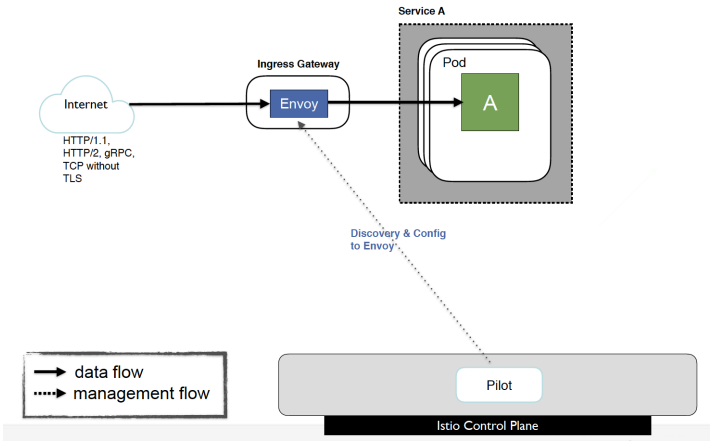
✓ Enjoy traffic control & observability

✓ No additional check Latency



Minimal Istio

- Minimal Istio without sidecar



1.611s : pod_creating

1.196s : container_startup_queue-proxy

1.133s : container_startup_user-container

✓ Short cold start-up time
No control and observability

✓ No additional latency

Trade-off by yourself

Istio	Costs			Benefits			
	Long cold start up time	Additional latency in response time	NET_ADMIN capabilities	Traffic Routing	Policy Control	Security	Telemetry
Full Istio	🔴	🔴	🔴	🟢	🟢	🟢	🟢
Full Istio with CNI Plugin	🔴	🔴		🟢	🟢	🟢	🟢
Full Istio without policy	🔴		🔴	🟢		🟢	🟢
Minimal Istio without Sidecar				🟢			◗

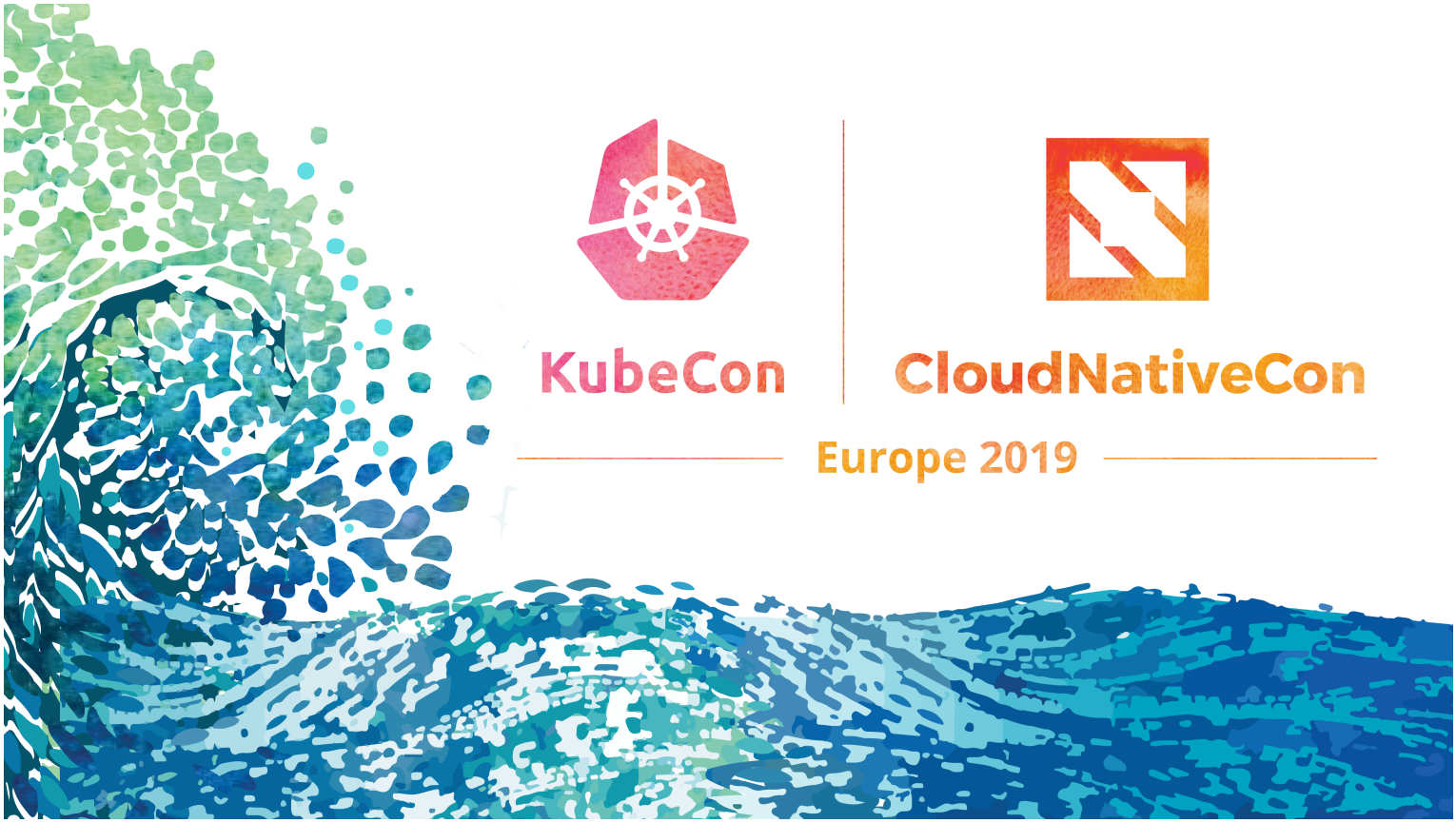
Recap

- Istio is a good complement of Knative.
- Carefully selection of Istio
  - ✓Manual sidecar injection.
  - ✓Disable policy if possible.
  - ✓Use CNI plugin if security restriction(Alpha).

KubeCon | CloudNativeCon

Europe 2019

Thank you!


KubeCon
CloudNativeCon
Europe 2019