Istio in the Enterprise

What’s new and upcoming in 2020

CONTAINERS DEVELOPER SUMMIT - ONLINE

Ram Vennam
IBM Cloud Kubernetes Service
Technical Offering Manager
ramvennam

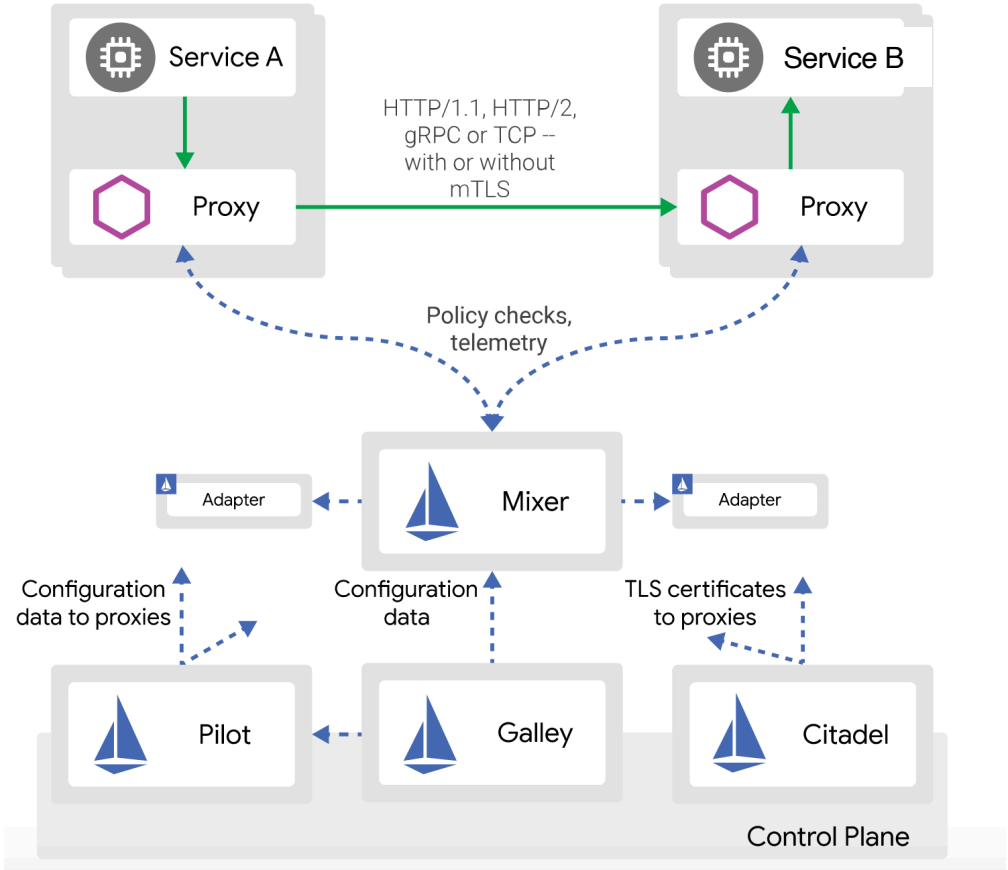
IBM

Challenges with Microservices

- Security
- Canary deployments
- A/B testing
- Retries and Circuit breaking
- Rate limiting
- Fault injection
- Policy management
- Telemetry

The “old” Istio

https://archive.istio.io/v1.1/docs/concepts/what-is-istio/

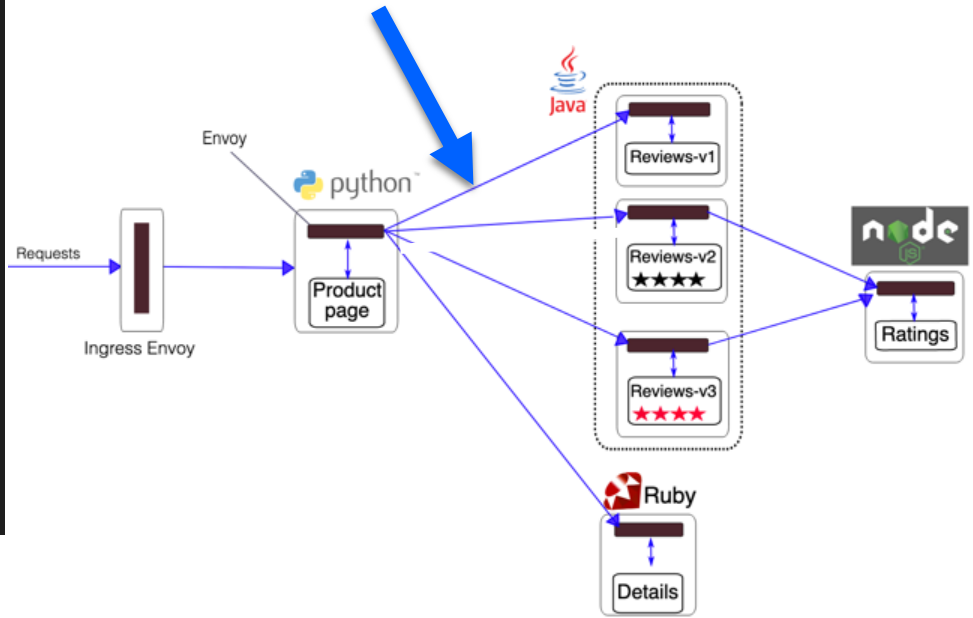


Virtual Service - Traffic Shifting

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
    - reviews
  http:
  - route:
    - destination:
        host: reviews
        subset: v1
      weight: 95
    - destination:
        host: reviews
        subset: v3
      weight: 5
```

95% -> v1

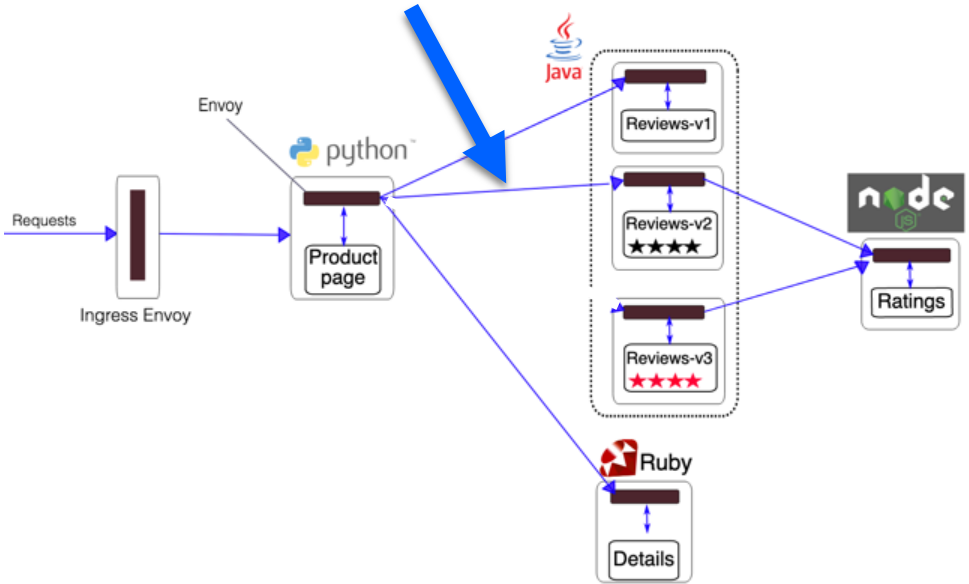
5% -> v3



Virtual Service - Request Routing

```yaml
apiVersion: networking.istio.io/v1alpha
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
    - reviews
  http:
  - match:
    - headers:
        end-user:
          exact: jason
    route:
    - destination:
        host: reviews
        subset: v2
  - route:
    - destination:
        host: reviews
        subset: v1
```

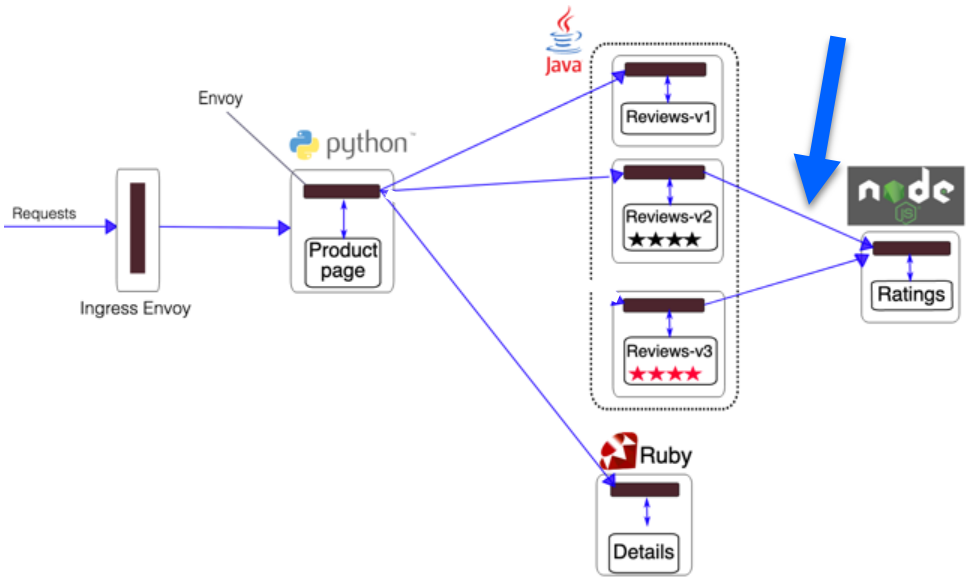
Canary Testing:
Route user:jason to reviews:v2
Others still get reviews:v1



Virtual Service – Delay and Fault Injection

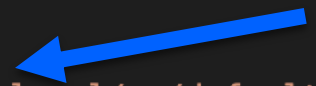
```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: ratings
spec:
  hosts:
  - ratings
  http:
  - match:
    - headers:
        end-user:
          exact: jason
    fault:
      delay:
        percent: 100
        fixedDelay: 7s
    route:
    - destination:
        host: ratings
        subset: v1
  - route:
    - destination:
        host: ratings
        subset: v1
```

Inject 7 second delay



Control Access

```yaml
apiVersion: "security.istio.io/v1beta1"
kind: "AuthorizationPolicy"
metadata:
  name: "details-viewer"
  namespace: default
spec:
  selector:
    matchLabels:
      app: details
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/default/sa/bookinfo-productpage"]
    to:
    - operation:
        methods: ["GET"]
```



Community feedback

- Incremental adoption is difficult
- Difficult to debug when things aren’t working
- Installation is difficult (too many knobs)
- Scaling problems with 1000+ services
- Performance issues with Policy enforcement

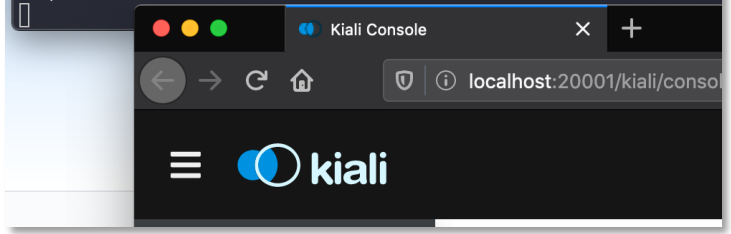
Usability Improvements

- istioctl UX commands
  - describe
  - dashboard
  - metrics
  - add-to-mesh
  - analyze
  - upgrade

More on the way!

```
~/istio-1.5.1/bin 🏎 $ ./istioctl x describe service productpage
Service: productpage
   Port: http 9080/HTTP targets pod port 9080
Pod is PERMISSIVE, clients configured automatically


Exposed on Ingress Gateway http://169.62.15.138
VirtualService: bookinfo
   /productpage, /static*, /login, /logout, /api/v1/products*
```

```
~/istio-1.5.1 🏎 $ istioctl dashboard kiali
http://localhost:20001/kiali
```




```
~/istio-1.5.1/samples/bookinfo/networking 🏎 $ istioctl analyze -k virtual-service-reviews-bad.yaml
Error [IST0101] (VirtualService reviews.default) Referenced host+subset in destinationrule not found: "reviews+v1"
Error [IST0101] (VirtualService reviews.default) Referenced host+subset in destinationrule not found: "reviews+v4"
Error: Analyzers found issues when analyzing namespace: default.
See https://istio.io/docs/reference/config/analysis for more information about causes and resolutions.
```

Improved Performance

Mixer is deprecated

Policy Control

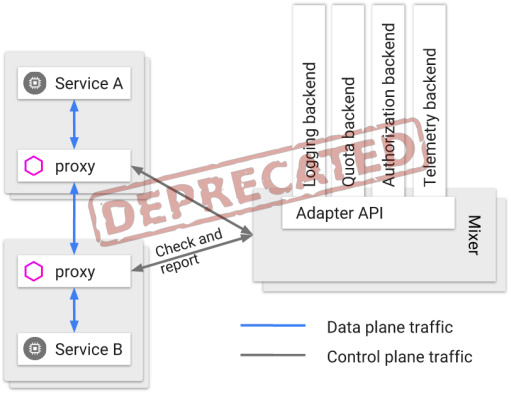
- Replaced by Authentication and Authorization policies

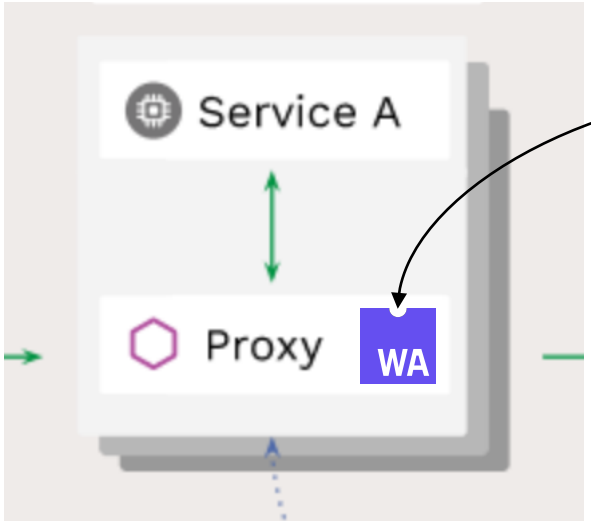
Telemetry

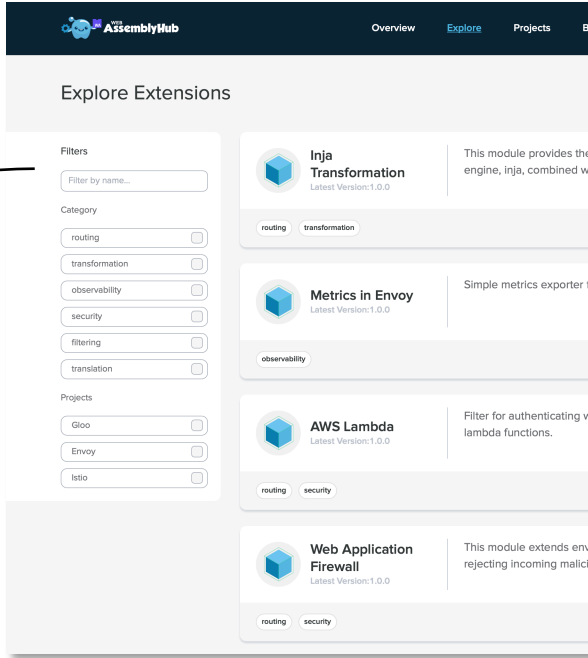
- Telemetry V2 – directly exported

Extensions

- WebAssembly to extend Envoy
- The WebAssembly Hub
- Mixer adapters being ported!





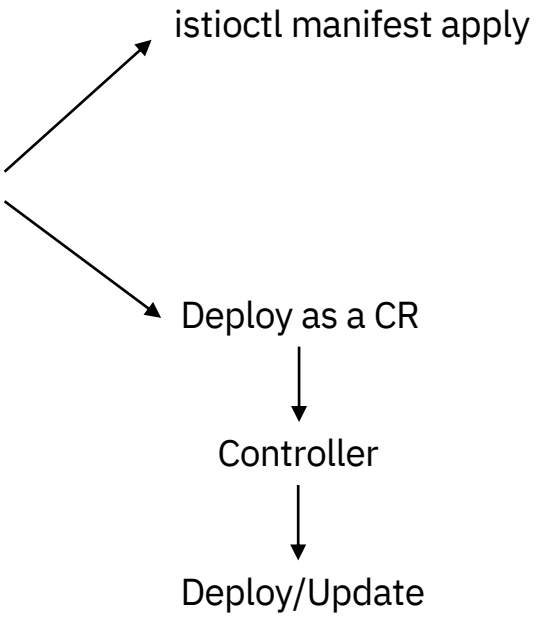


Simplified Installation

- Operator API - IstioOperator
- Human-triggered: istioctl manifest apply
- Machine-triggered: Server side controller
- Helm installation deprecated

- Improved upgrade and canary options coming!

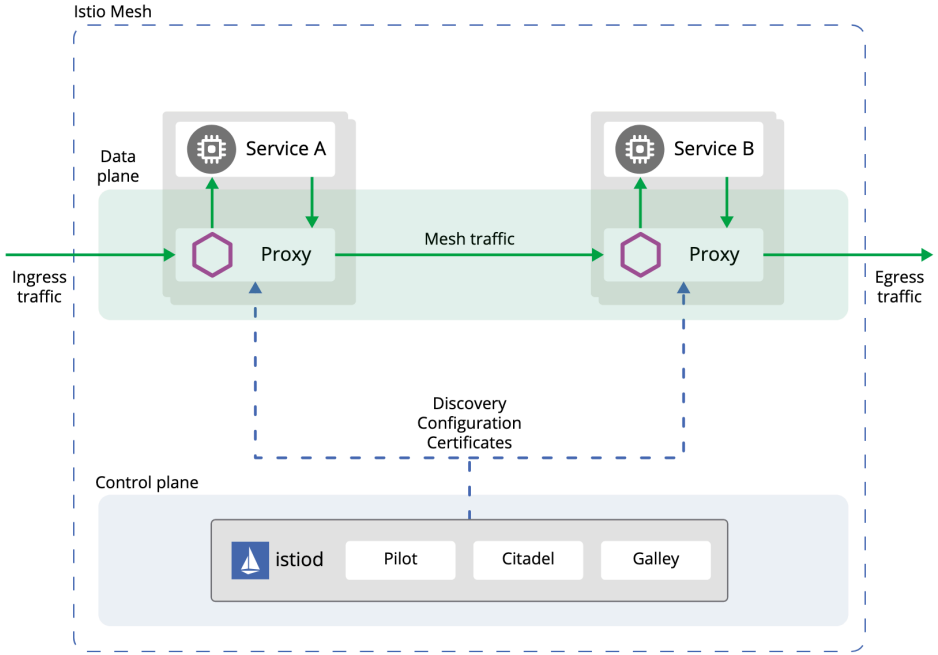
```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
spec:
  components:
    egressGateways:
    - name: istio-egressgateway
      enabled: true
      k8s:
        resources:
          requests:
            cpu: 10m
            memory: 40Mi

    ingressGateways:
    - name: istio-ingressgateway
      enabled: true
      k8s:
        resources:
          requests:
            cpu: 10m
            memory: 40Mi

    policy:
      enabled: false
      k8s:
        resources:
          requests:
            cpu: 10m
            memory: 100Mi

    telemetry:
      k8s:
        resources:
          requests:
            cpu: 50m
            memory: 100Mi
```



Fewer moving parts

istiod

- Easier operation of the control plane
- Improve performance
- Reduced internal API footprint




```
istio-citadel-58c44d6964-vfbln
istio-galley-66555fc6c5-dm9x6
istio-ingressgateway-bd9cf87c8-nrmsr
istio-pilot-7d76d8c7fc-kk6sv
istio-policy-8d654bbbf-78qgm
istio-sidecar-injector-56b7656fd8-vlh5m
istio-telemetry-5bc7b7c84d-ttvdf
prometheus-66c5887c86-5jjbn
```

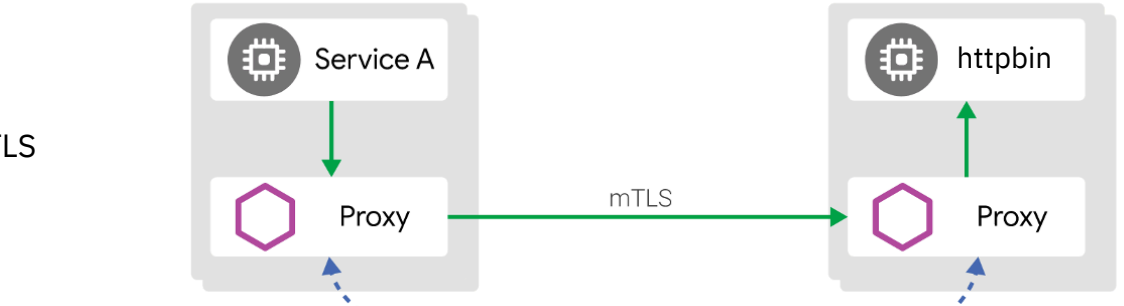
1.4 default profile

```
istio-ingressgateway-85576dff98-xmx9t
istiod-5cbfb7db8f-fvmz2
prometheus-65fb99c564-l7ltq
```

1.5 default profile

Automatic mutual TLS

- Configures client proxies to send mutual TLS traffic to mesh workloads automatically
- DestinationRule resource not needed!
- Supports incremental adoption




```yaml
apiVersion: "networking.istio.io/v1alpha3"
kind: "DestinationRule"
metadata:
  name: "httpbin"
spec:
  host: "httpbin.bar.svc.cluster.local"
  trafficPolicy:
    tls:
      mode: ISTIO_MUTUAL
```

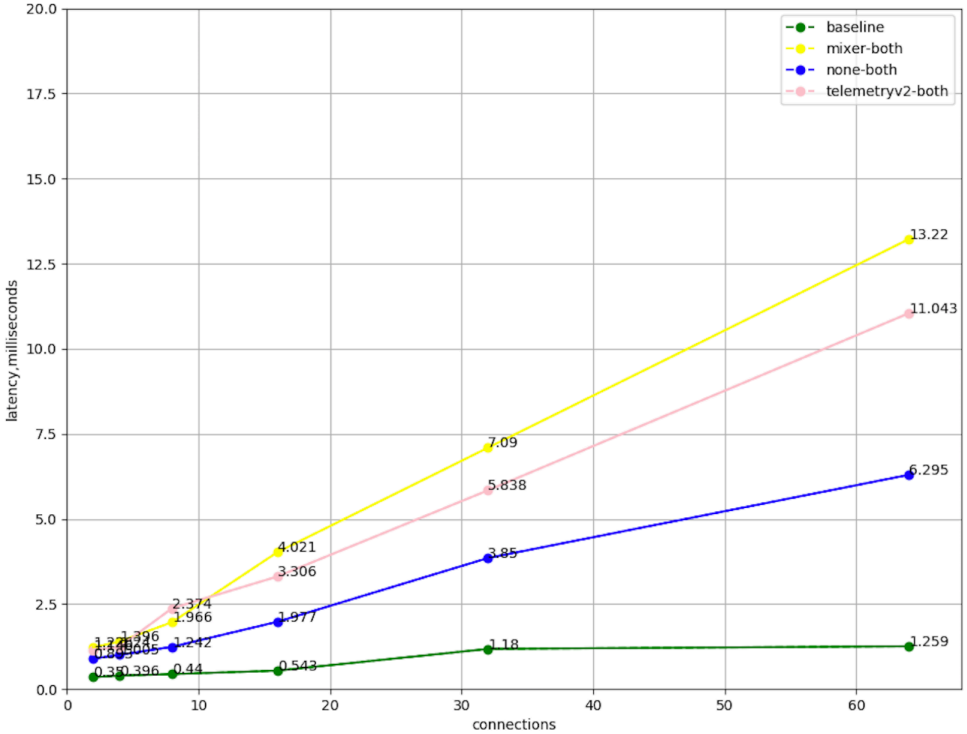
```yaml
apiVersion: "authentication.istio.io/v1alpha1"
kind: "Policy"
metadata:
  name: "httpbin"
spec:
  targets:
  - name: httpbin
  peers:
  - mtls: {}
```

No longer needed!

Performance

Load test with **1000** services and **2000** sidecars with 70,000 mesh-wide requests per second:

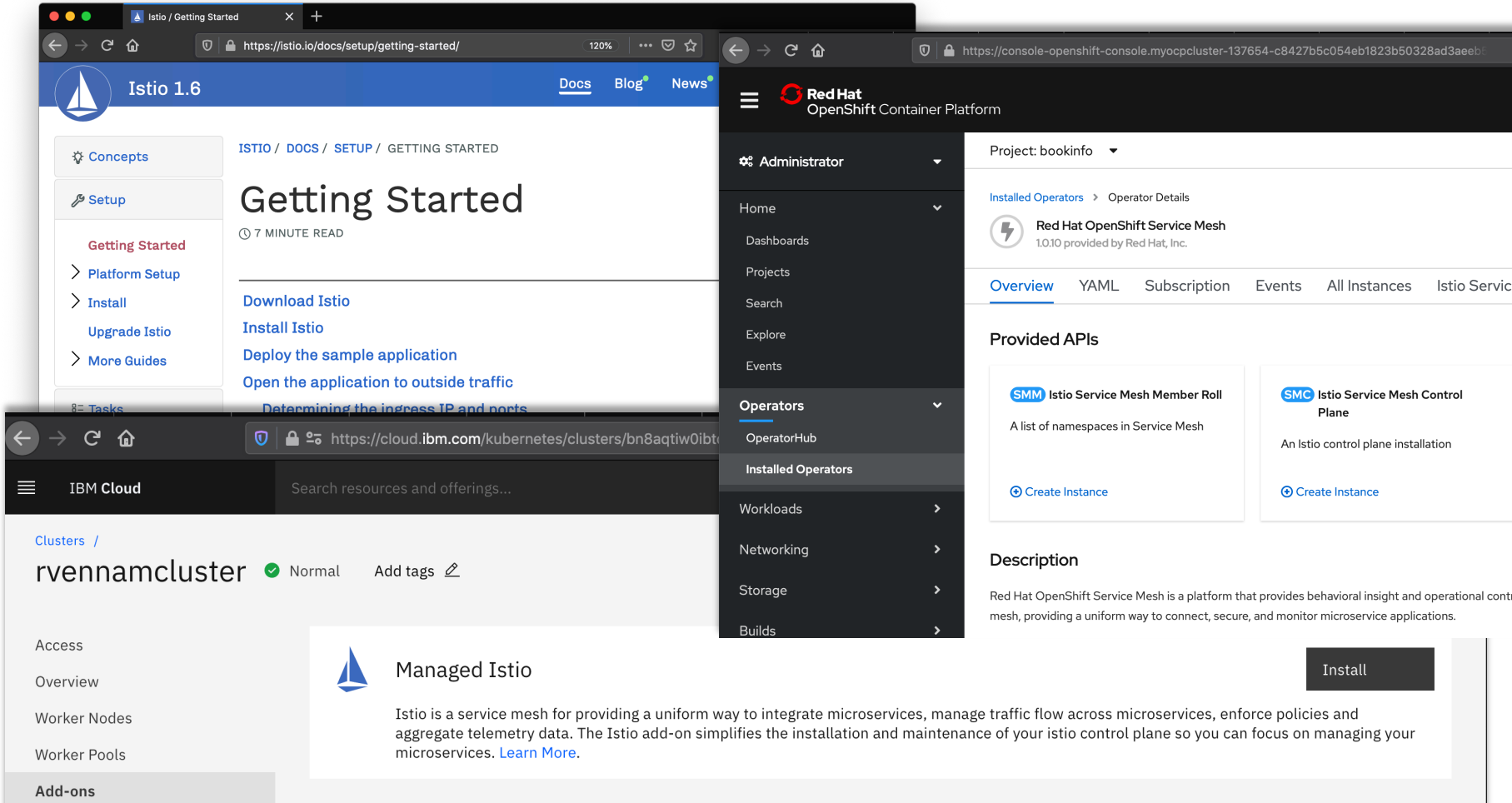
- Proxy uses **0.5 vCPU** and **50 MB memory** per 1000 rps
- Proxy adds **2.8 ms latency** (1 kB payload at 1000 rps using 16 connections.)
- Pilot uses **1 vCPU** and 1.5 GB of memory
- YMMV!



P90 latency vs client connections

https://istio.io/docs/ops/deployment/performance-and-scalability/

Thank you


Istio / Getting Started
https://istio.io/docs/setup/getting-started/
Istio 1.6
Docs
Blog
News
Concepts
Setup
Getting Started
Platform Setup
Install
Upgrade Istio
More Guides
ISTIO / DOCS / SETUP / GETTING STARTED
Getting Started
7 MINUTE READ
Download Istio
Install Istio
Deploy the sample application
Open the application to outside traffic
https://console-openshift-console.myocpcluster-137654-c8427b5c054eb1823b50328ad3aeeb
Red Hat
OpenShift Container Platform
Administrator
Home
Dashboards
Projects
Search
Explore
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Project: bookinfo
Installed Operators
Operator Details
Red Hat OpenShift Service Mesh
1.0.10 provided by Red Hat, Inc.
Overview
YAML
Subscription
Events
All Instances
Provided APIs
SMM Istio Service Mesh Member Roll
A list of namespaces in Service Mesh
Create Instance
SMC Istio Service Mesh Control Plane
An Istio control plane installation
Create Instance
Description
Red Hat OpenShift Service Mesh is a platform that provides behavioral insight and operational
mesh, providing a uniform way to connect, secure, and monitor microservice applications.
https://cloud.ibm.com/kubernetes/clusters/bn8aqtiw0ibt
IBM Cloud
Search resources and offerings...
Clusters /
rvennamcluster
Normal
Add tags
Access
Overview
Worker Nodes
Worker Pools
Add-ons
Managed Istio
Install
Istio is a service mesh for providing a uniform way to integrate microservices, manage traffic flow across microservices, enforce policies and aggregate telemetry data. The Istio add-on simplifies the installation and maintenance of your istio control plane so you can focus on managing your microservices. Learn More.