



Life Outside the Cluster:

Adding Virtual Machines to an Envoy Service Mesh

Ameer Abbas and Megan O'Keefe

21 November 2019





Ameer

- Solutions Architect, Google Cloud
- Hybrid Cloud, Service Mesh



Megan

- Developer Relations Engineer, Google Cloud
- Containers, Service Mesh

@askmeegs  

Agenda

Why service mesh?

Why add VMs to the mesh?

Istio + VMs - How it works

Demo

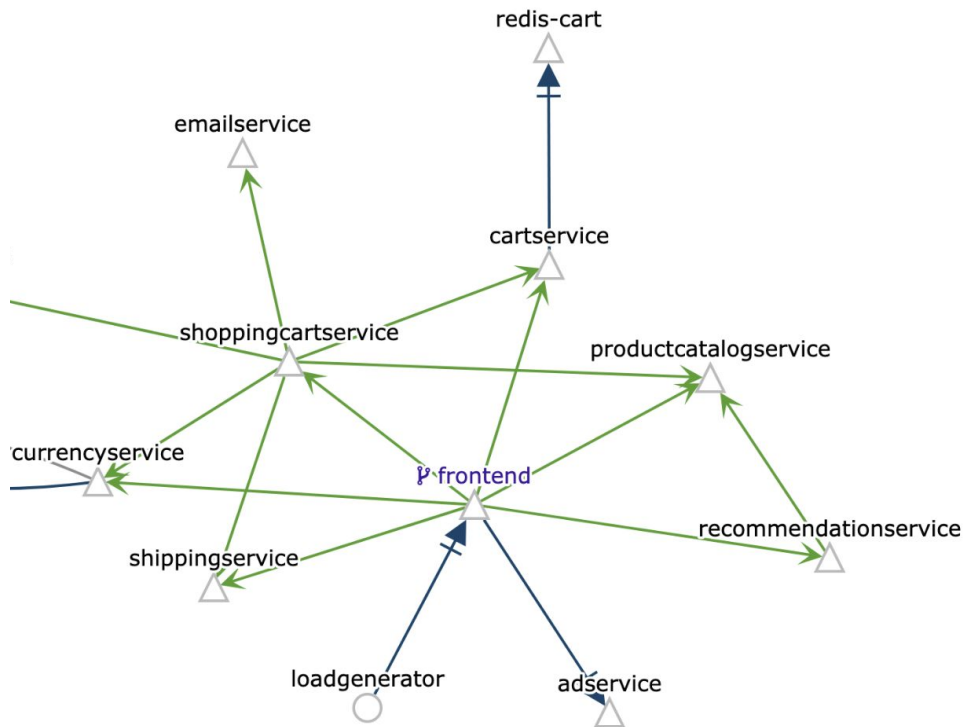
Best Practices

Why Service Mesh?

More services = more complexity

Need consistent **policy enforcement**

Need consistent **metrics aggregation**



A service mesh provides a **transparent** and **language-independent** way to flexibly and easily **automate** application network functions.

Service Mesh Toolbox

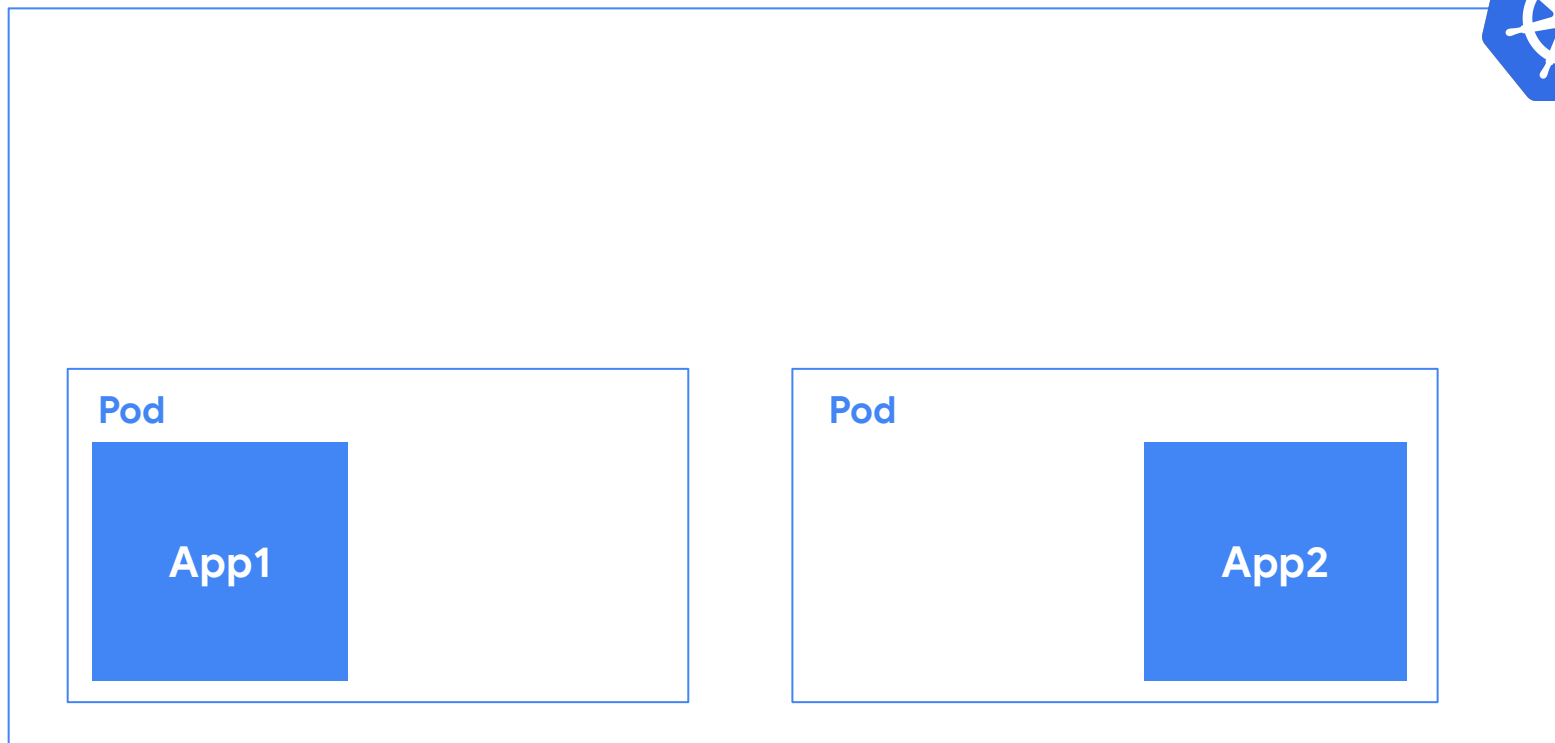
Envoy: an open-source, high performance, configurable L7 proxy



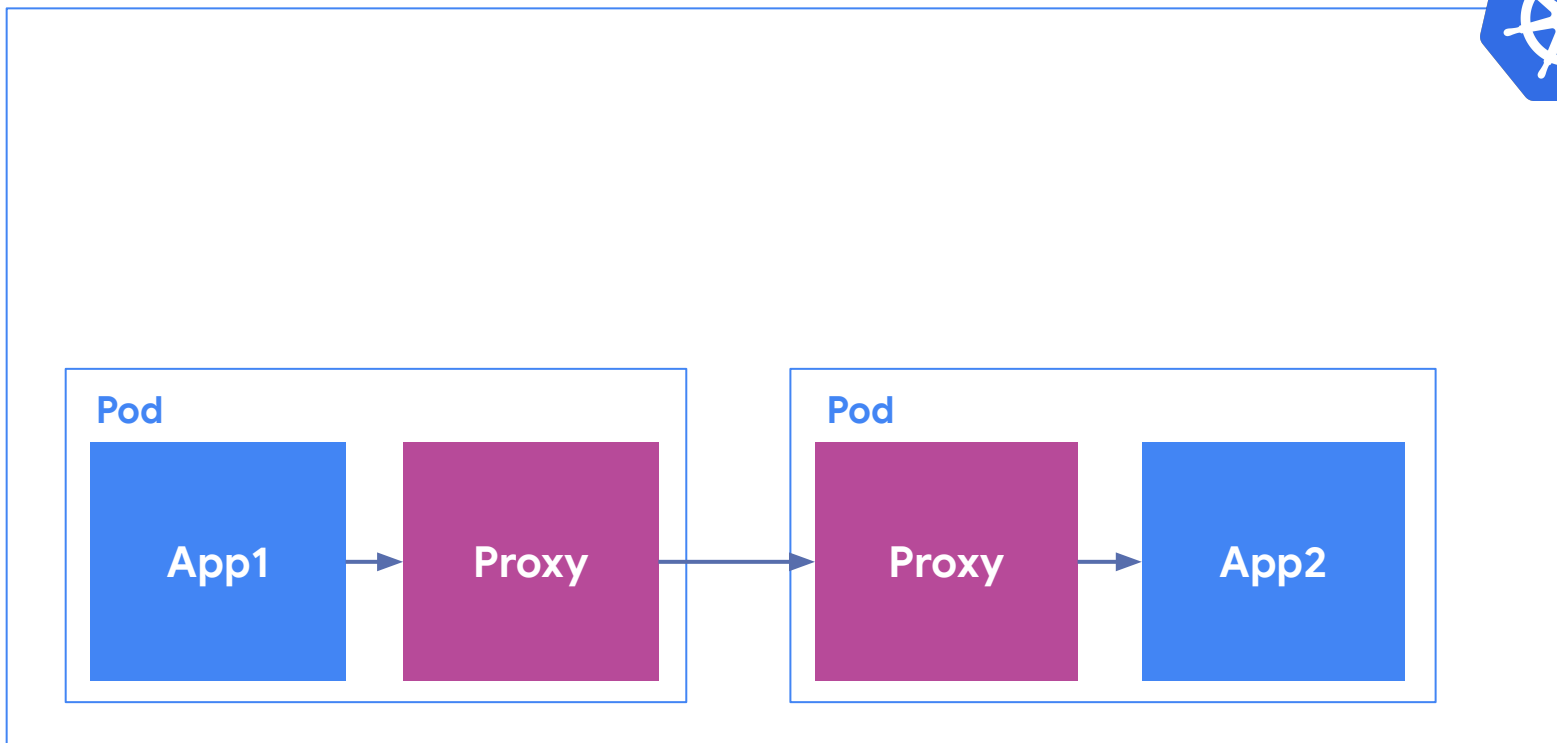
Istio: an open-source service mesh tool. Injects a **sidecar** Envoy proxy into Kubernetes pods. **Proxies mediate** all traffic. Istio configures Envoys, collects metrics.



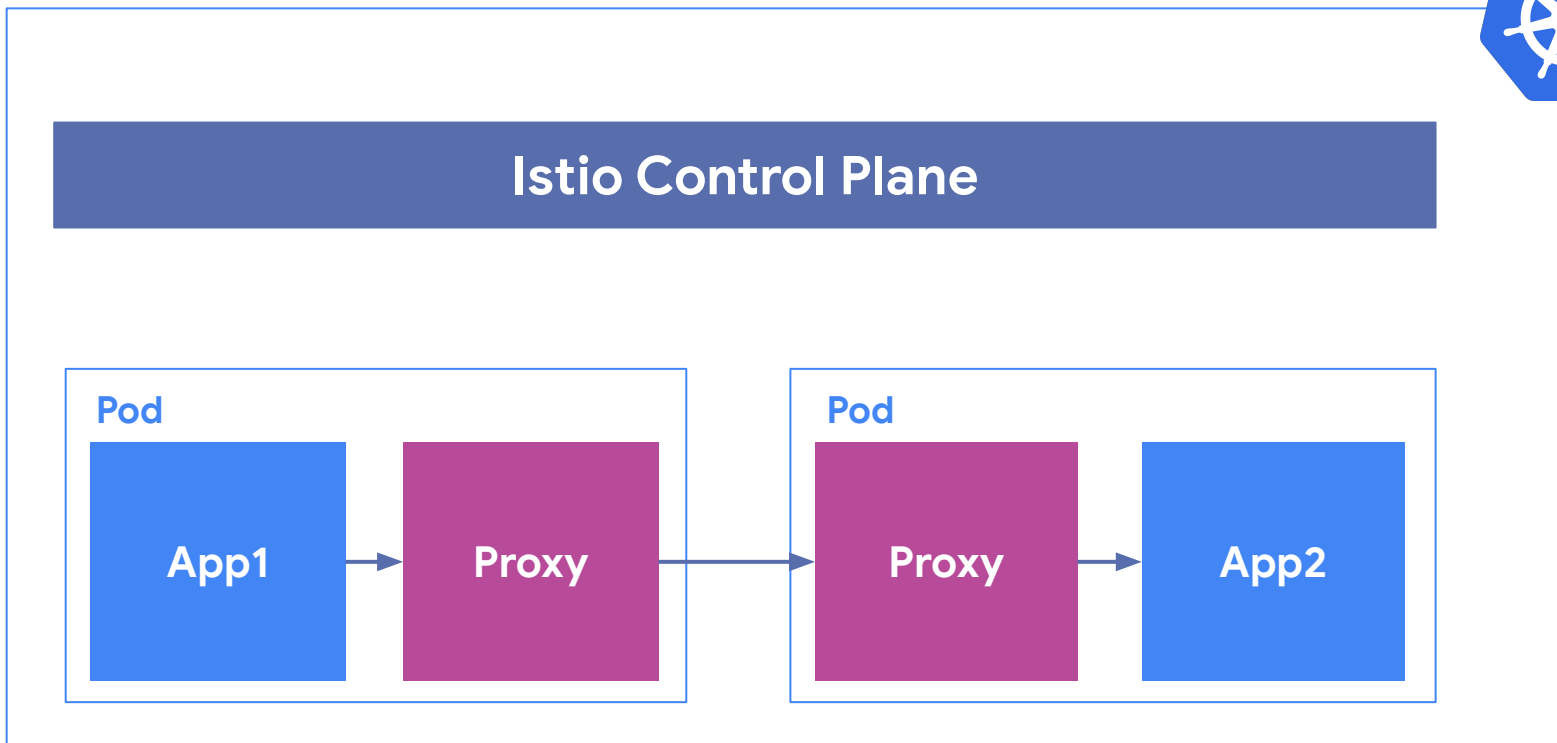
How Istio Works



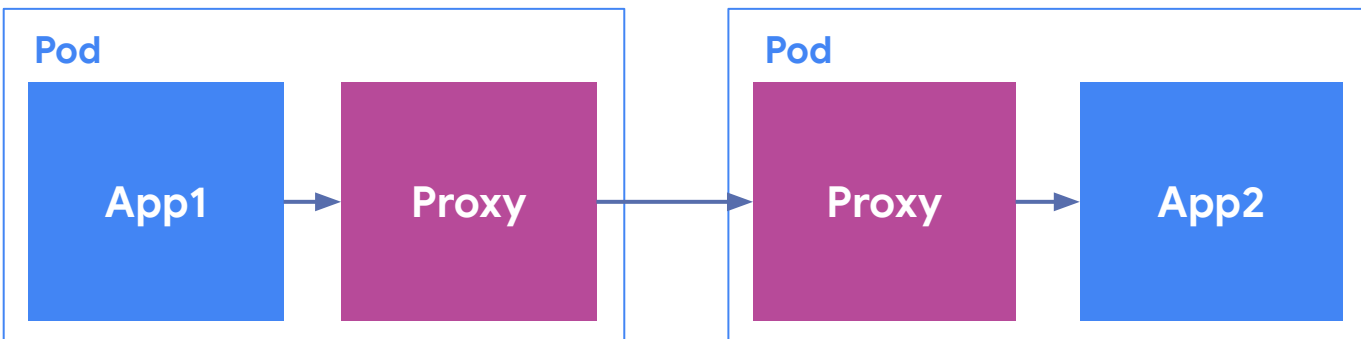
How Istio Works



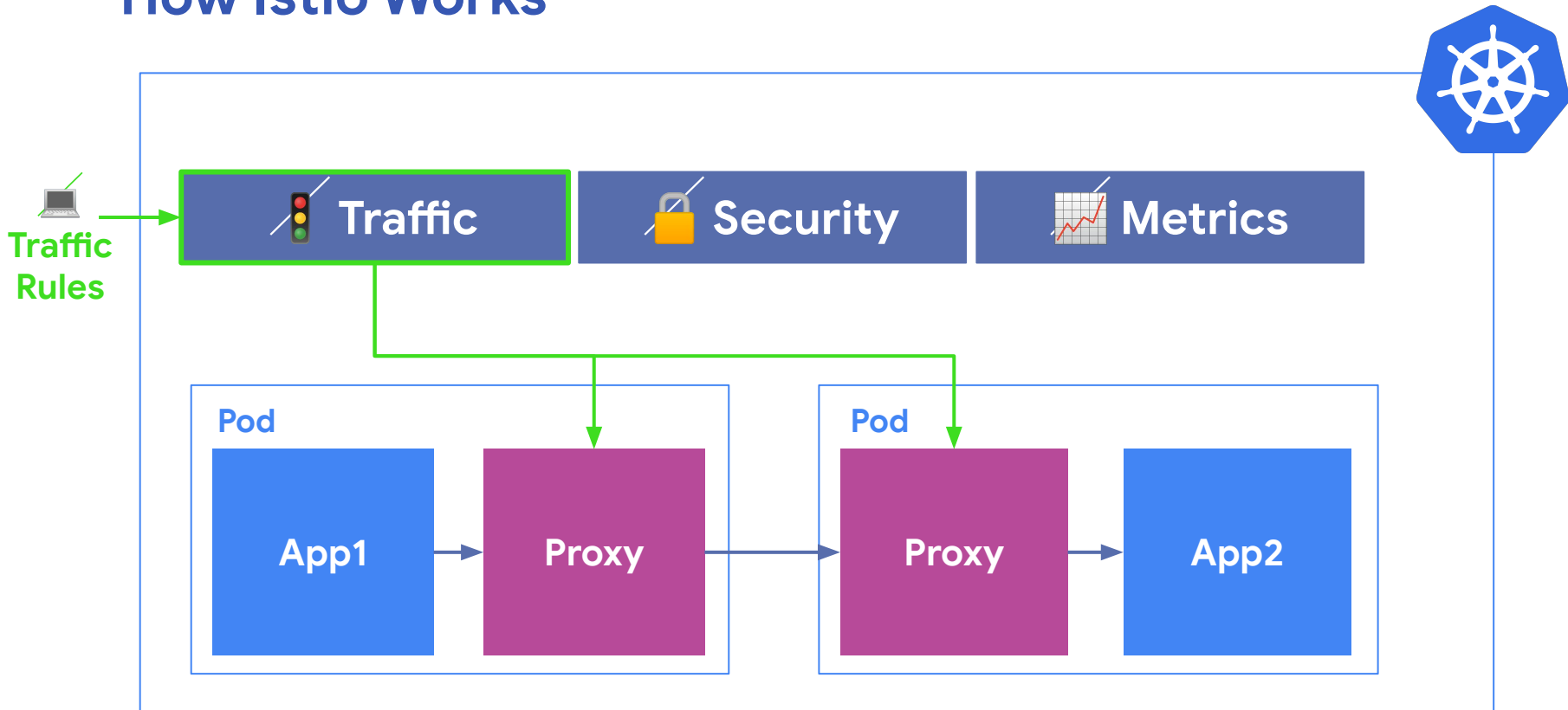
How Istio Works



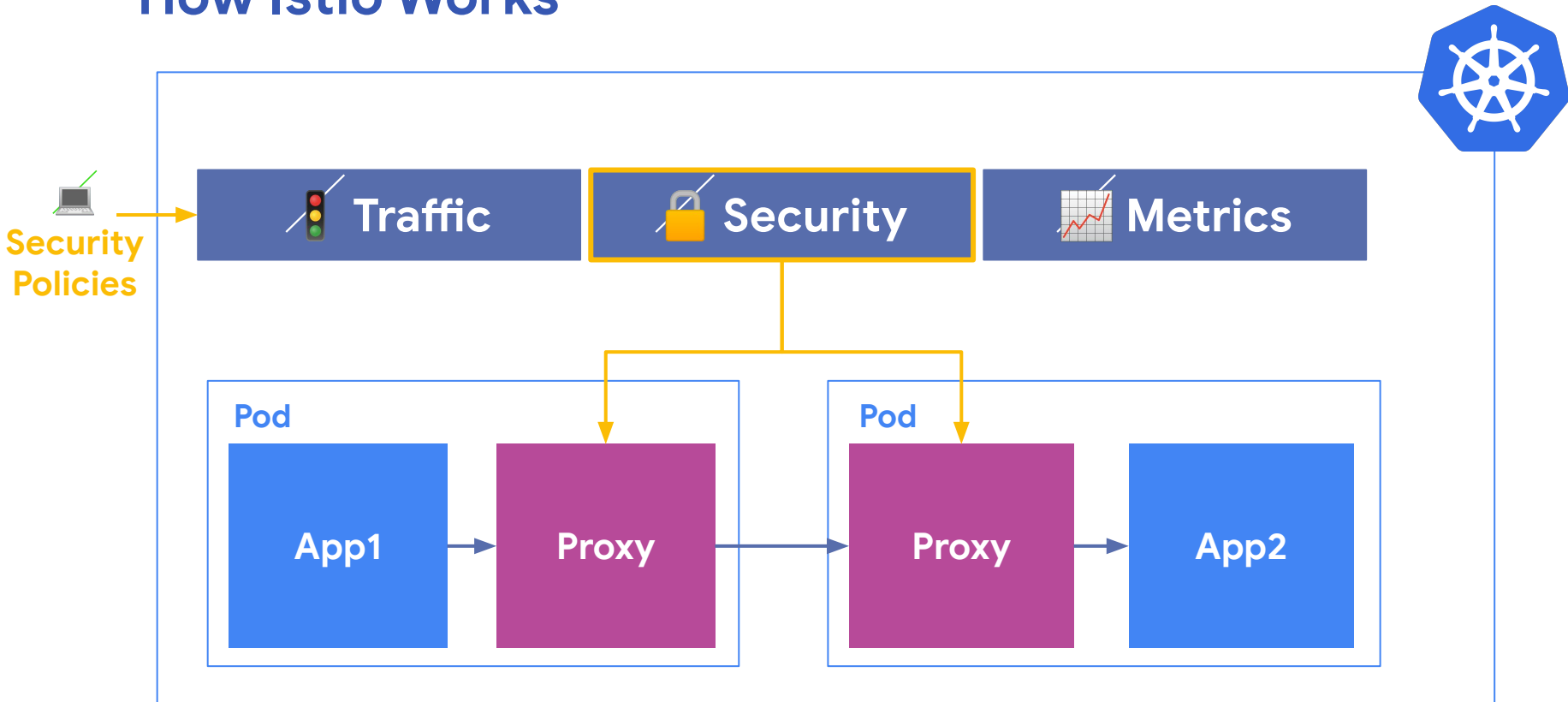
How Istio Works



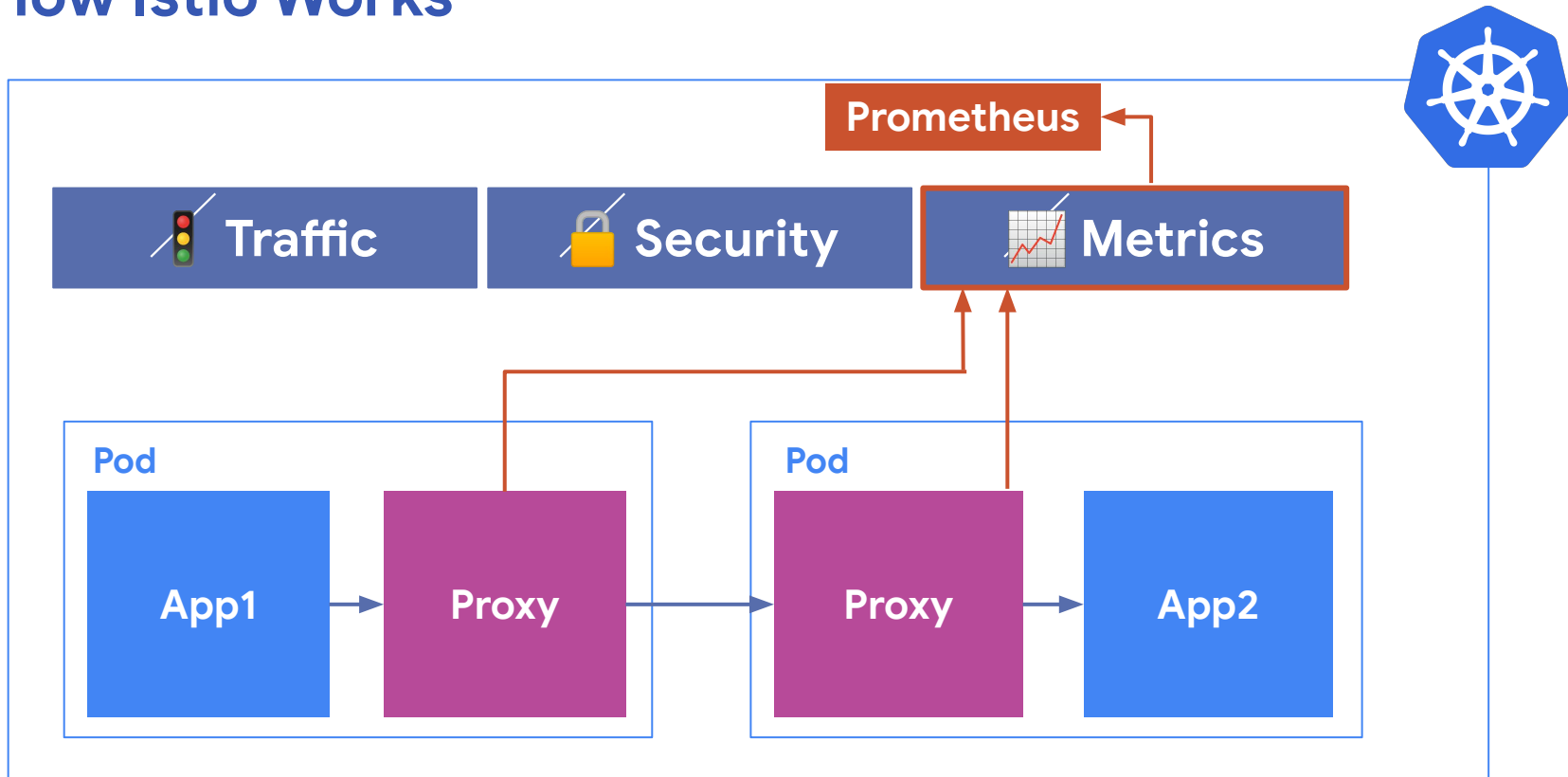
How Istio Works



How Istio Works



How Istio Works



Why add VMs to the mesh?

Observability - see VM metrics alongside containers

Security: enforce the same policies in the same way, across compute environments

Traffic management: load balancing for VMs, failover, A/B testing, modern rollouts for VM services

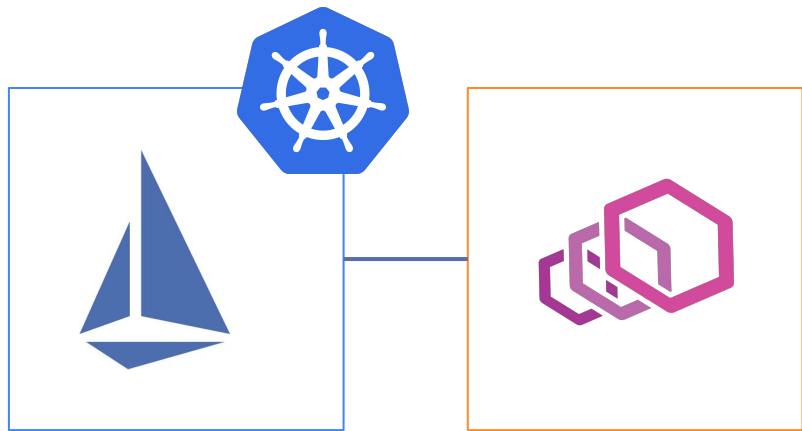


Istio + VMs

Install the **Istio proxy** (Envoy) on a VM.

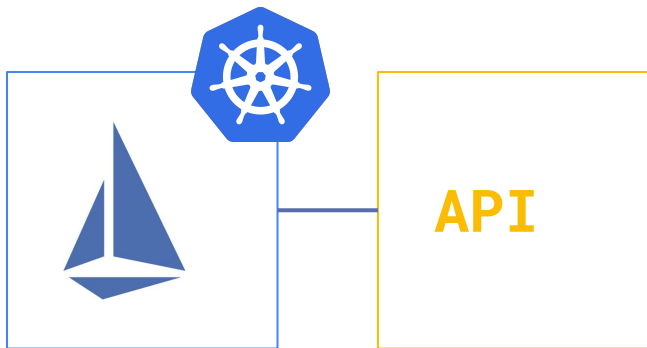
Configure the proxy to call home to the **Istio control plane** running in Kubernetes, set up VM certs for mutual TLS

Add a "selector-less" **Service** and an Istio **ServiceEntry** to the Kubernetes cluster (resolve K8s DNS for the VM)

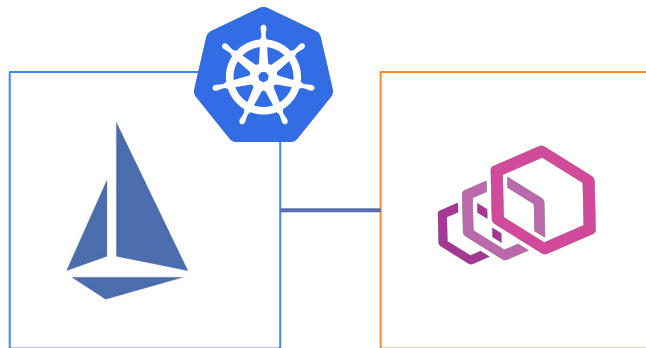


Istio + VMs

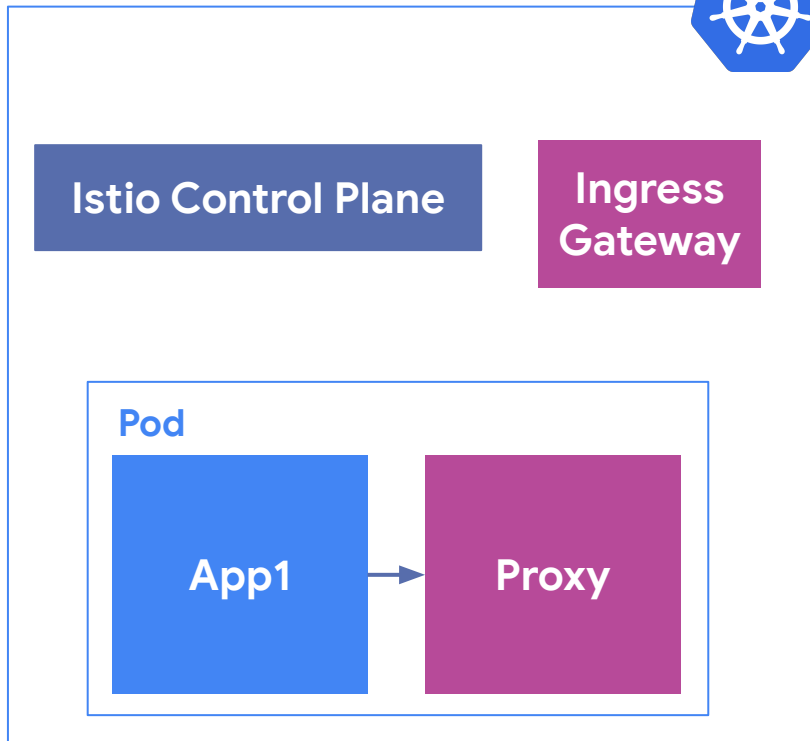
MESH_EXTERNAL ServiceEntry:
For **External APIs** or services you do not own. Can only get client-side metrics.



MESH_INTERNAL ServiceEntry:
Directly add a service to the mesh, by deploying a **sidecar proxy on the VM**. Full Istio functionality, metrics



Istio + VMs



Virtual Machine

Send Pod IP range,
service account
certs to VM

Istio + VMs



`istioctl register`



Istio Control Plane

Ingress
Gateway

Pod

App2

Proxy

Virtual Machine

→ ~ istioctl register --help

Registers a service instance (e.g. VM) joining the mesh

Usage:

```
istioctl register <svcname> <ip> [name1:]port1 [name2:]port2 ... [flags]
```

Flags:

-a, --annotations strings	List of string annotations to apply if creating a service/endpoint; e.g. -a foo=bar,test,x=y
-h, --help	help for register
-l, --labels strings	List of labels to apply if creating a service/endpoint; e.g. -l env=prod,vers=2
-s, --serviceaccount string	Service account to link to the service (default "default")

```
apiVersion: v1
kind: Service
metadata: ...
spec:
  clusterIP: 10.0.28.196
  ports:
  - name: "3550"
    port: 3550
    protocol: TCP
    targetPort: 3550
  sessionAffinity: None
  type: ClusterIP ← selector-less Service
status:
  loadBalancer: {}
```

Istio + VMs



create ServiceEntry
for VM service ↓

Istio Control Plane

Ingress
Gateway

Pod

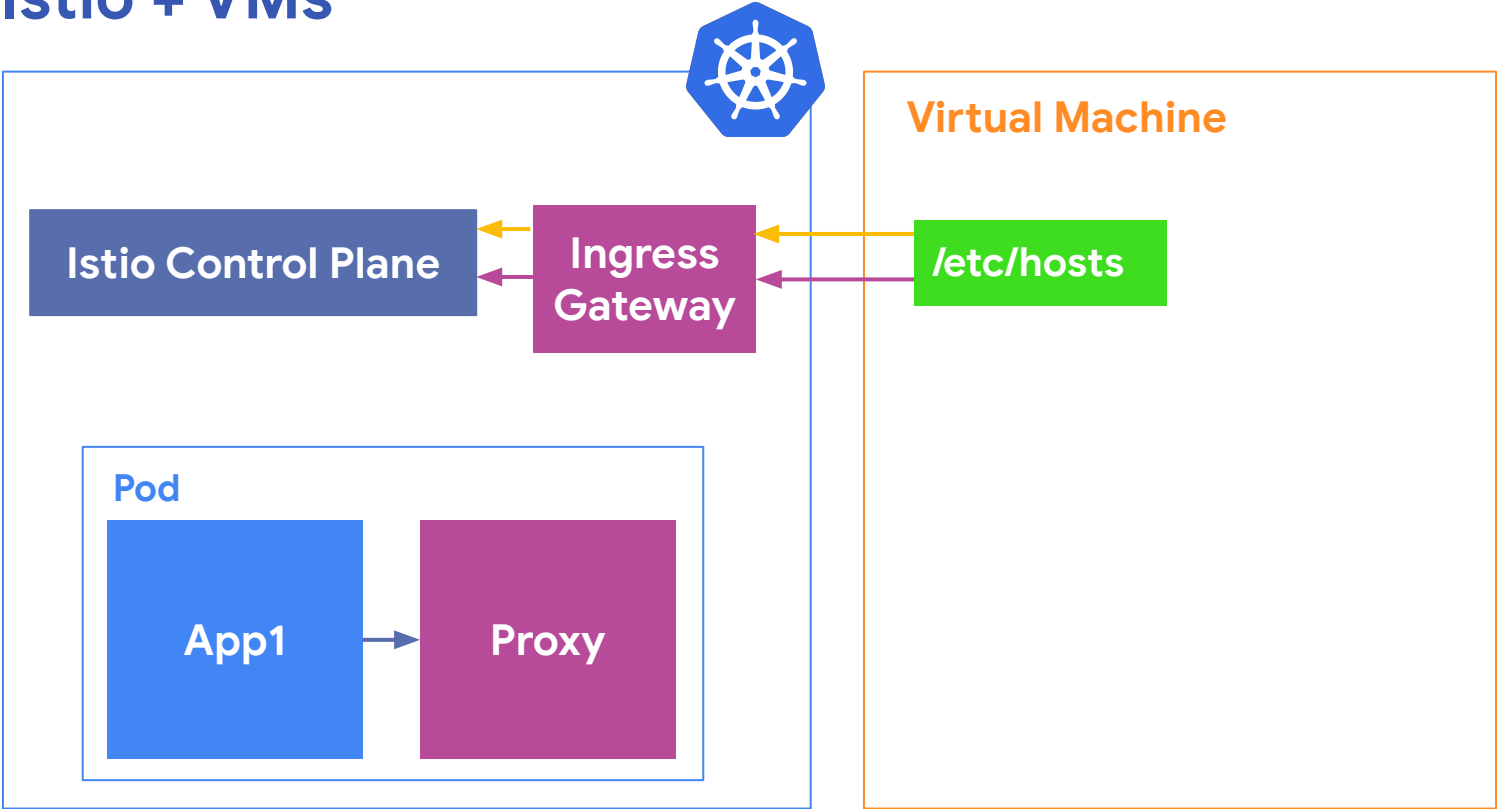
App1

Proxy

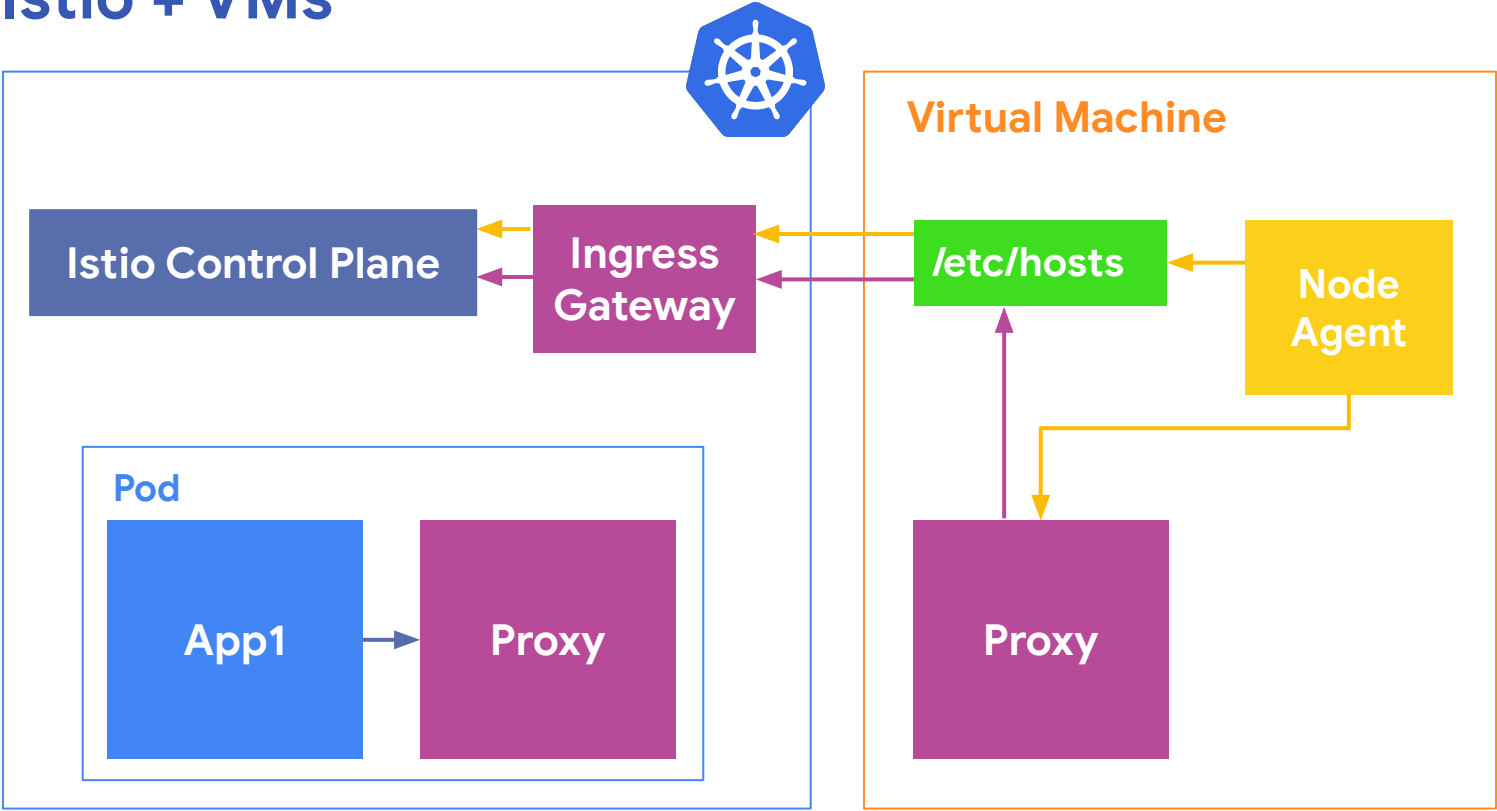
Virtual Machine

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata: ...
spec:
  endpoints:
    - address: 10.128.0.13 ← VM IP Address
      labels:
        app: productcatalogservice
        version: v1
      ports:
        grpc: 3550
  hosts:
    - productcatalogservice.default.svc.cluster.local
  ports:
    - name: grpc
      number: 3550
      protocol: GRPC
  resolution: STATIC
```

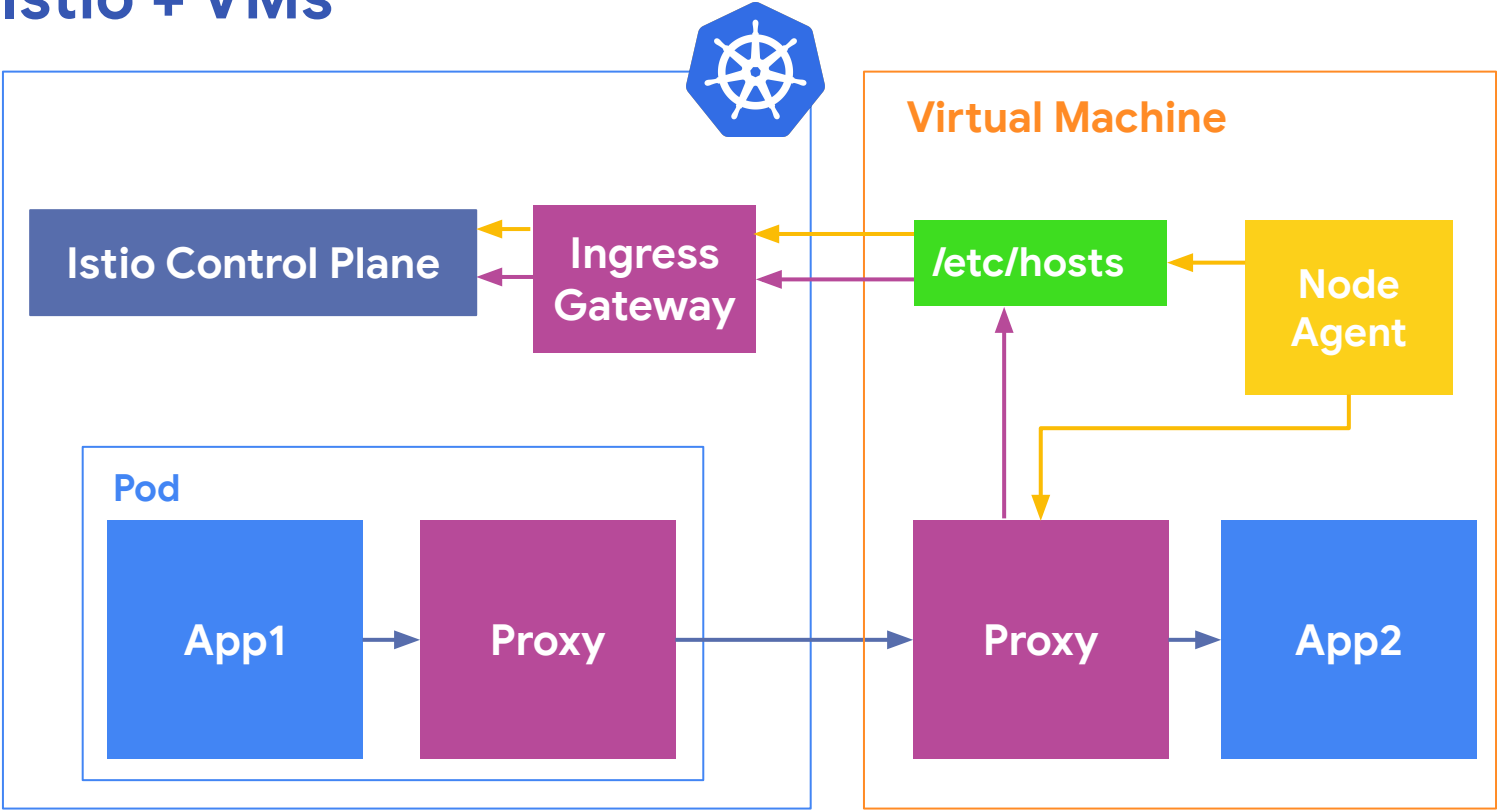
Istio + VMs



Istio + VMs

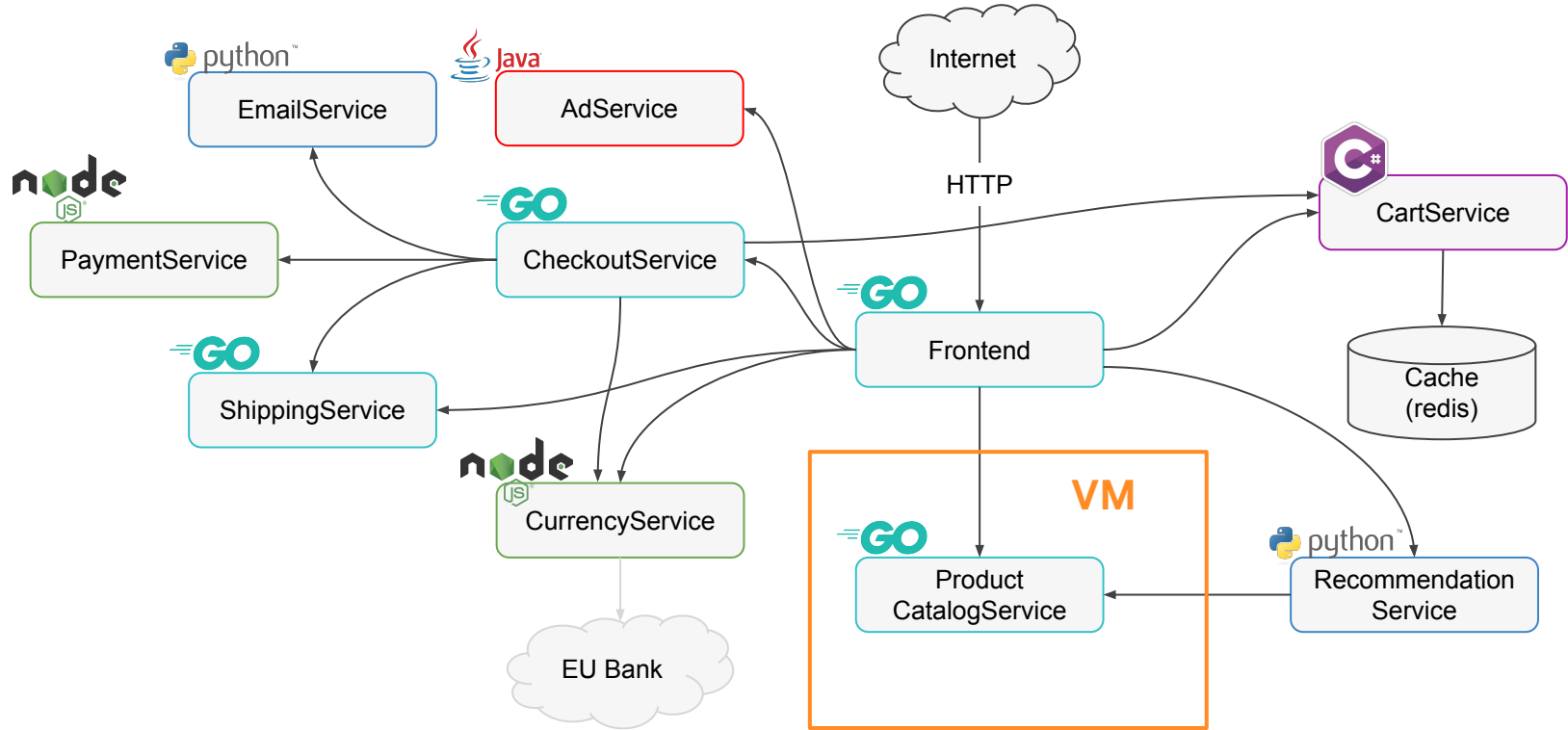


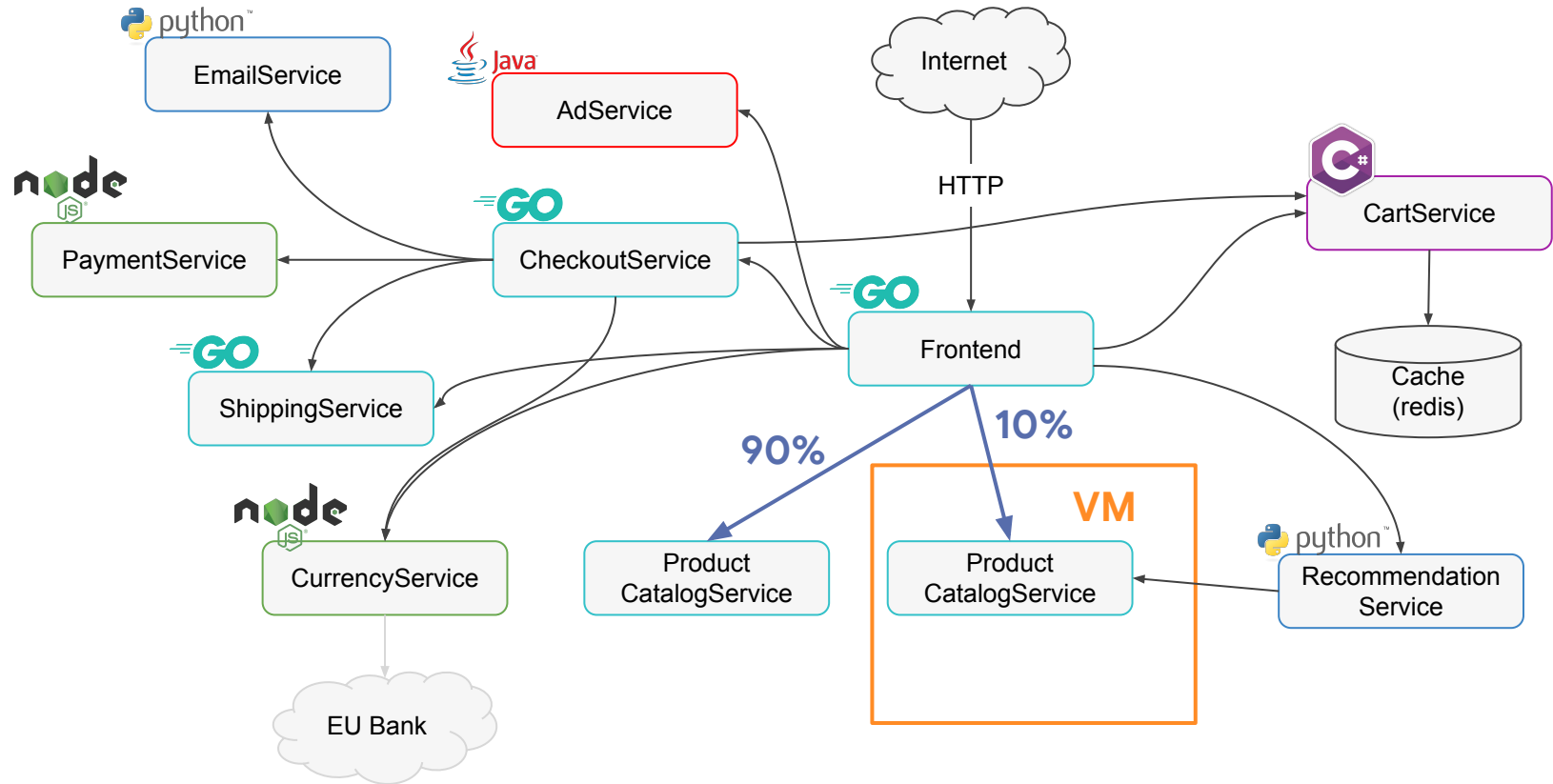
Istio + VMs



Demo







Best Practices

Migrate from VMs to containers using **VirtualServices**. Progressively send % of traffic to the migrated workload.

Observability first, policy second. Look at golden signals (latency, error rate) right away. Then turn on mTLS.

Use ingress for pilot and citadel (Never expose directly). You can use GCP **InternalLoadbalancer** instead of the public Ingress Gateway



Resources

Try it out:

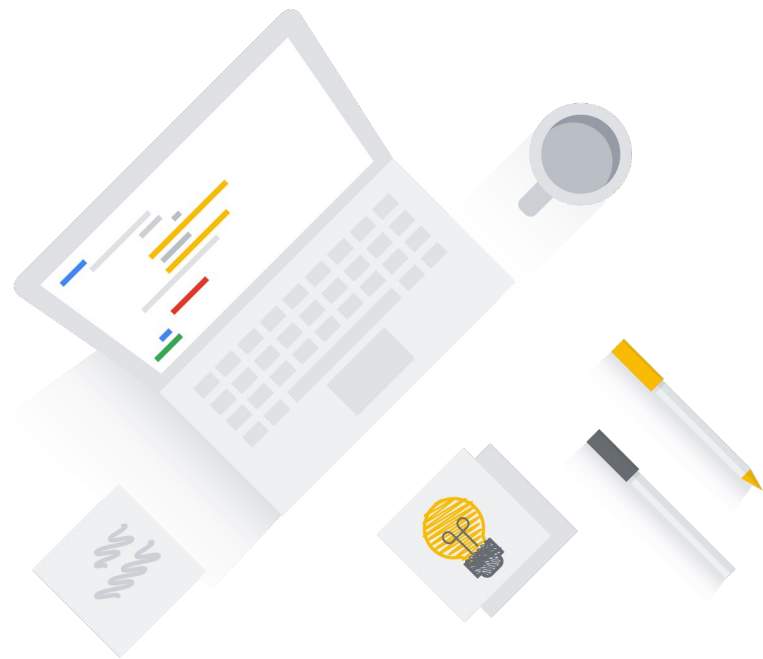
bit.ly/istio-samples

Read the docs:

bit.ly/istio-vm-docs

Slides:

bit.ly/life-outside-the-cluster



Get Involved

Want to help build the future of Istio and VMs?

[Join the Istio Environments Working Group!](#)

discuss.istio.io

istio.slack.com 



Thank you!