A Field Guide for Safe Istio Upgrades

Ram Vennam / @RamVennam / Field Engineer @ Solo.io

About me

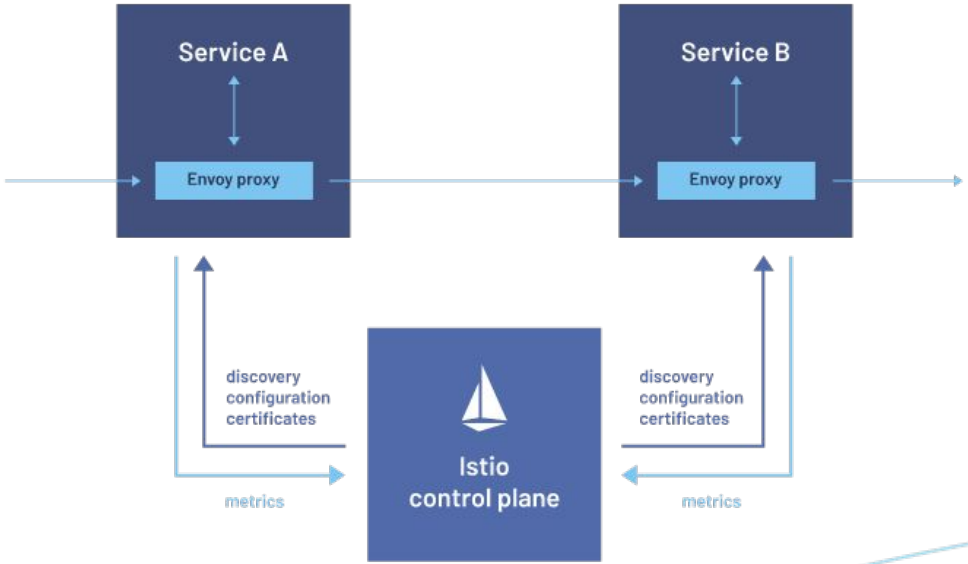
Field Engineering Lead, N.Amer, Solo.io

@RamVennam

ram.vennam@solo.io

https://www.linkedin.com/in/ramvennam/

Istio


Service A
Envoy proxy
Service B
Envoy proxy
discovery
configuration
certificates
metrics
Istio
control plane
discovery
configuration
certificates
metrics

What gets installed?

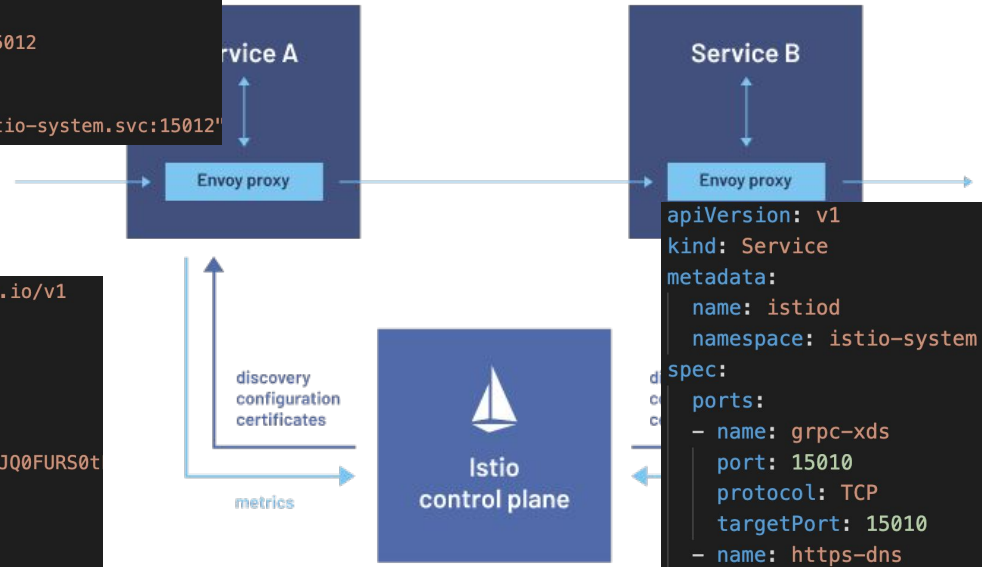
```
istioctl manifest generate --set profile=default
```

```
(istioctl manifest generate -f ~/istio-1.13.2/manifests/profiles/default.yaml)
```

CustomResourceDefinition	15
Deployment	2
Service	2
ValidatingWebhookConfiguration	1
MutatingWebhookConfiguration	1
ConfigMap	2
ServiceAccount	4
ClusterRole/ClusterRoleBinding	5
Role/RoleBinding	3
EnvoyFilter	6
HorizontalPodAutoscaler	2
PodDisruptionBudget	2

How are they wired together?

```yaml
apiVersion: v1
kind: Pod
spec:
  containers:
  - env:
    - name: CA_ADDR
      value: istiod.istio-system.svc:15012
    - name: PROXY_CONFIG
      value: |
        {"discoveryAddress":"istiod.istio-system.svc:15012"
```



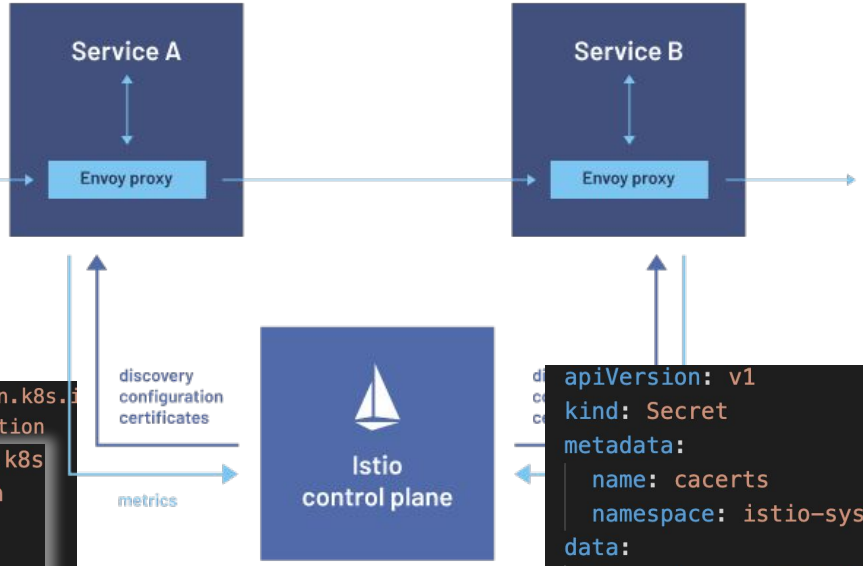

```yaml
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  name: istio-sidecar-injector
webhooks:
- clientConfig:
    caBundle: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0t
    service:
      name: istiod
      namespace: istio-system
      path: /inject
      port: 443
  admissionReviewVersions:
```

```yaml
apiVersion: v1
kind: Service
metadata:
  name: istiod
  namespace: istio-system
spec:
  ports:
  - name: grpc-xds
    port: 15010
    protocol: TCP
    targetPort: 15010
  - name: https-dns
    port: 15012
    protocol: TCP
    targetPort: 15012
  - name: https-webhook
    port: 443
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: istiod-6cf8687ccd-6qfsc
  labels:
    app: istiod
    istio: pilot
```

Certs

```
apiVersion: v1
kind: ConfigMap
data:
  root-cert.pem: |
    -----BEGIN CERTIFICATE-----
    MIIE9TCCAt2gAwIBAgIRALzm/F1TOIs9sB
    FDESMBAGA1UEChMJZ2xvby1tZXNoMB4XDT
    MjAxNFowFDESMBAGA1UEChMJZ2xvby1tZX
    Ag8AMIICCgKCAgEA2qWX9IMTbqSjISOpDM
    2NpfREzV9xZGF3gKAm5nWT1CwuMjKSmxv+
    KOiWM4kGy2biSfeYH5DD5qiDDRwzWw3OFi
```




```
apiVersion: admissionregistration.k8s.i
kind: ValidatingWebhookConfiguration
```

```
apiVersion: admissionregistration.k8s
kind: MutatingWebhookConfiguration
metadata:
  name: istio-sidecar-injector
webhooks:
- clientConfig:
    caBundle: LS0tLS1CRUdJTiBDRVJUSUZ
    service:
```

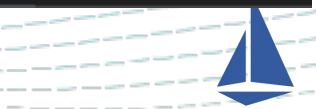
```
apiVersion: v1
kind: Secret
metadata:
  name: cacerts
  namespace: istio-system
data:
  ca-cert.pem: LS0tLS1CRUdJTiBDRV
  ca-key.pem: LS0tLS1CRUdJTiBSU0
  cert-chain.pem: LS0tLS1CRUdJTi
  root-cert.pem: LS0tLS1CRUdJTiB
```

Best Practice: Separate IstioOperator

```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  name: production-istio
  namespace: istio-system
spec:
  profile: minimal
  hub: $REPO
  tag: $ISTIO_IMAGE
  meshConfig:
    accessLogEncoding: JSON
    enableTracing: false
    defaultConfig:
      holdApplicationUntilProxyStarts: true
      proxyMetadata:
        ISTIO_META_DNS_CAPTURE: "true"
        ISTIO_META_DNS_AUTO_ALLOCATE: "true"
    outboundTrafficPolicy:
      mode: ALLOW_ANY
    trustDomain: $CLUSTER_NAME
    rootNamespace: istio-config
  components:
    pilot:
      enabled: true
      k8s:
        replicaCount: 2
        resources:
          requests:
            cpu: 200m
            memory: 200Mi
        strategy:
```

```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  name: ingress-gateway
  namespace: istio-system
spec:
  profile: empty
  hub: $REPO
  tag: $ISTIO_IMAGE
  components:
    ingressGateways:
    # Enable the default ingress gateway
      - name: istio-ingressgateway
        namespace: istio-ingress
        enabled: true
        label:
          istio: ingressgateway
          version: $REVISION
          app: istio-ingressgateway
          topology.istio.io/network: $CLUSTER_NAME
        k8s:
          hpaSpec:
            maxReplicas: 5
            metrics:
              - resource:
                  name: cpu
                  targetAverageUtilization: 60
                type: Resource
            minReplicas: 2
            scaleTargetRef:
```

```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  name: eastwest-gateway
  namespace: istio-system
spec:
  profile: empty
  hub: $REPO
  tag: $ISTIO_IMAGE
  components:
    ingressGateways:
      - name: istio-eastwestgateway
        namespace: istio-eastwest
        enabled: true
        k8s:
          service:
            ports:
              # Port for multicluster mTLS passthrough;
              - port: 15443
                targetPort: 15443
                name: tls
          overlays:
            - apiVersion: apps/v1
              kind: Deployment
              name: istio-eastwestgateway
              patches:
                # Sleep 25s on pod shutdown to allow connectio
                - path: spec.template.spec.containers.[name:is
                  value:
                    preStop:
                      exec:
```



Before you upgrade: Capture state

Analyze and address any issues

```
istioctl analyze --all-namespaces
```

```
istioctl proxy-status
```

Precheck

```
istioctl x precheck
```

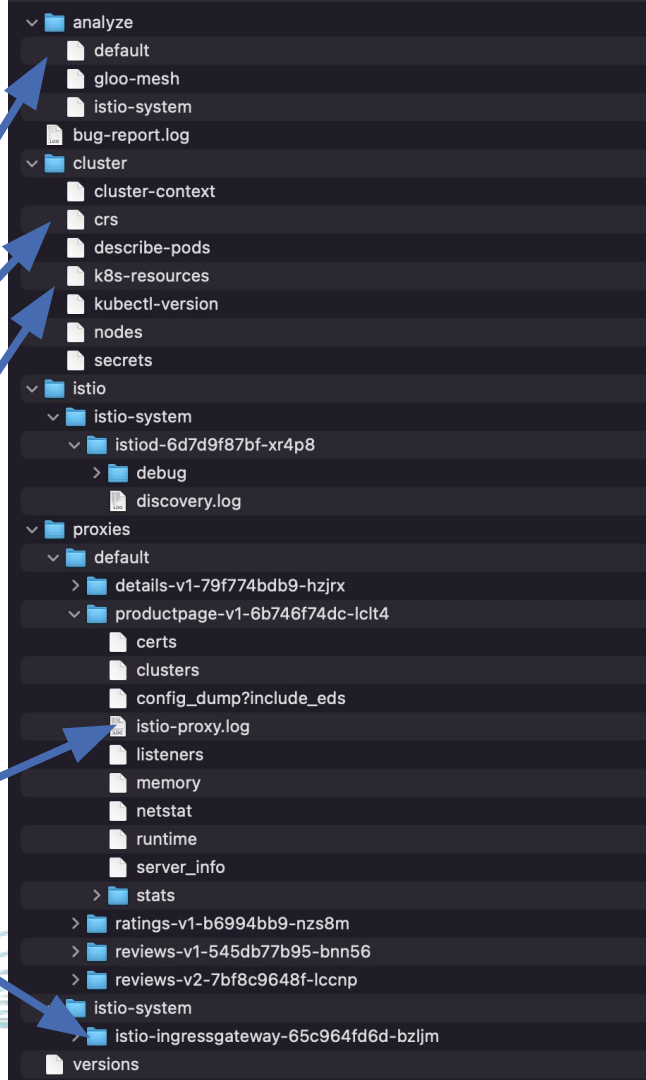
Backup Istio CR's

```
kubectl get istio-io --all-namespaces -oyaml
```

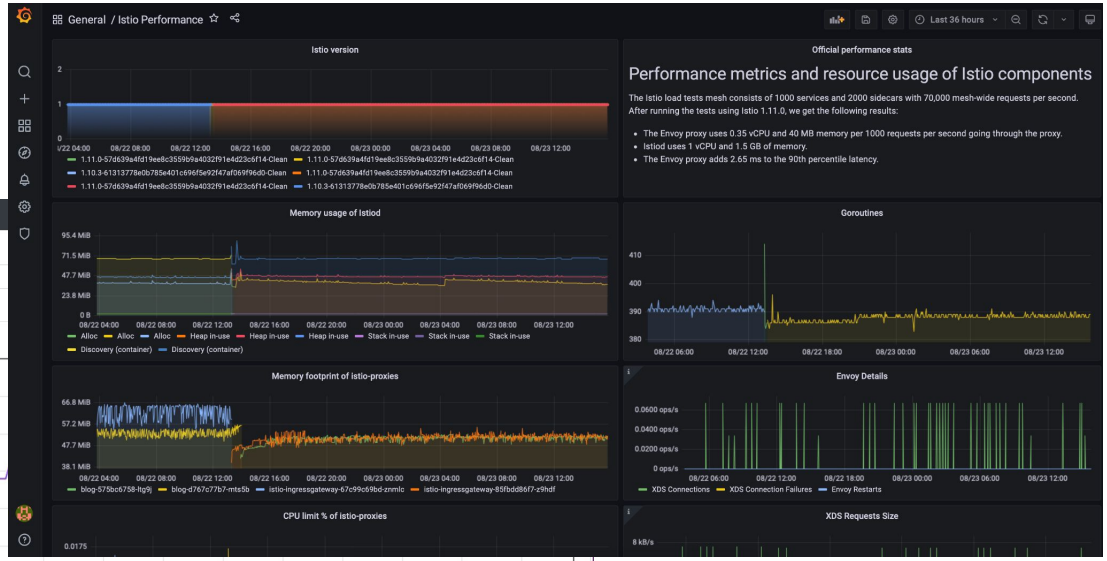

Before you upgrade: Capture state

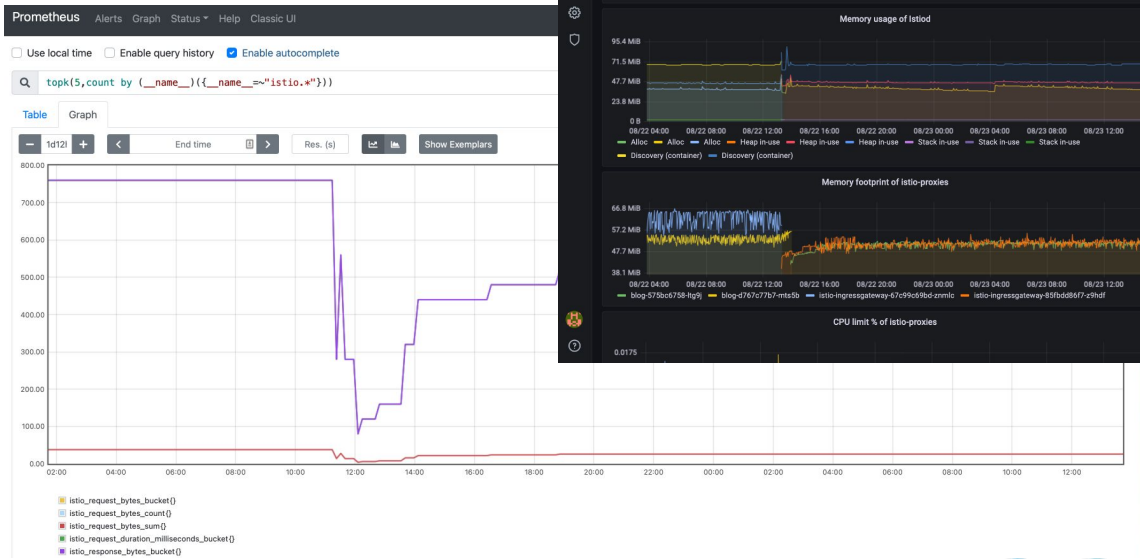
Capture everything:

```
istioctl bug-report
```



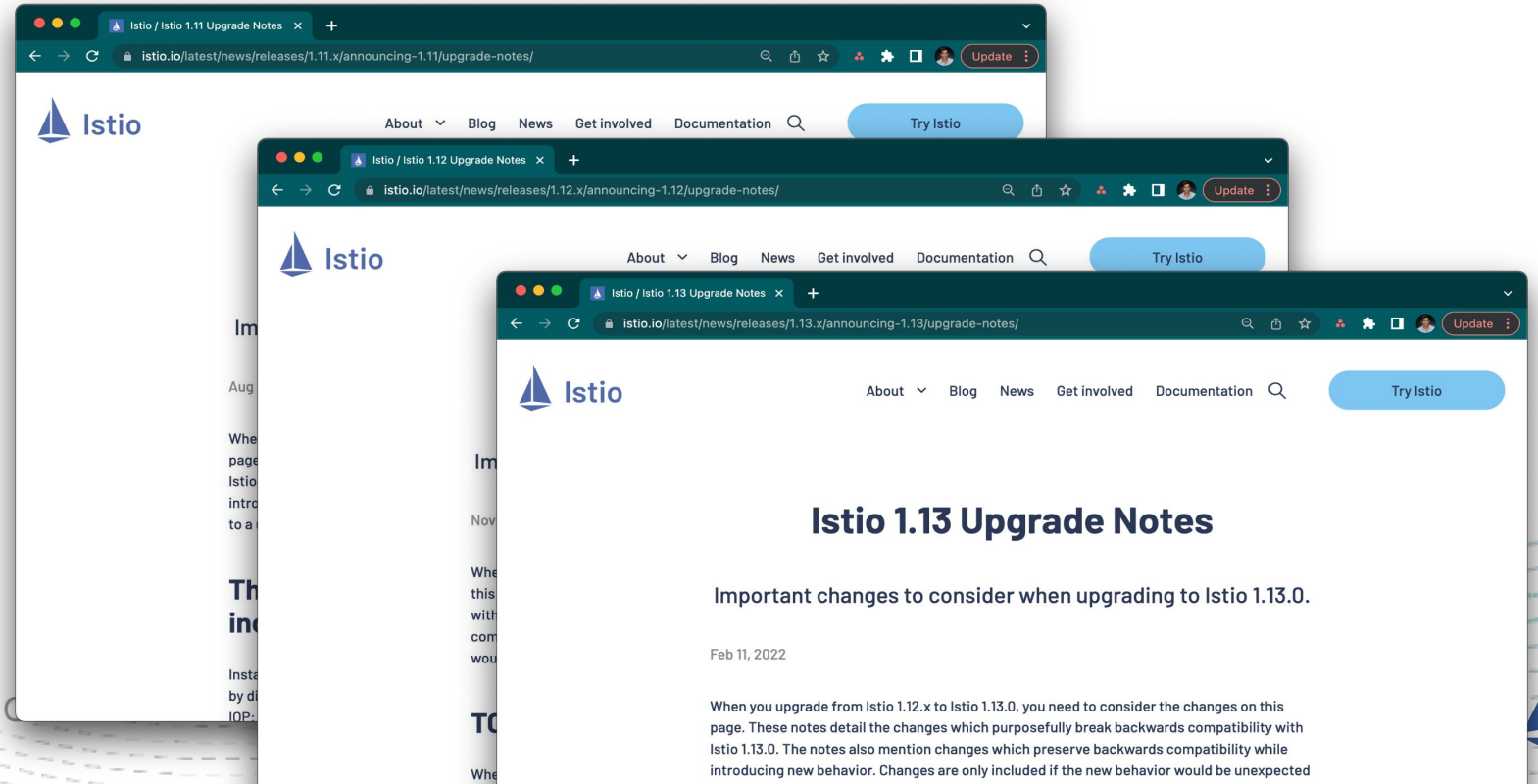
Before you upgrade: Dashboards





https://krisztianfekete.org/upgrading-to-istio-1.11/

Before you upgrade:
Upgrade Notes (Different from release announcements and change notes)



Special attention

- EnvoyFilters
- EnvoyFilters
- EnvoyFilters!
- IstioOperator customizations
  - overlays
  - meshConfig
  - Compare:

```
~/istio-1.11.5/bin/istioctl manifest generate -f myIstioInstall.yaml
~/istio-1.12.6/bin/istioctl manifest generate -f myIstioInstall.yaml
```

- Resource annotations

```
kubectl get deploy -o yaml | grep 'istio.io'
```


istioctl upgrade

```
istioctl upgrade -f istiodIstioOperator.yaml

istioctl upgrade -f ingressGatewayIstioOperator.yaml

istioctl upgrade -f ewGatewayIstioOperator.yaml

kubectl rollout restart deployment -n myns

istioctl proxy-status
```

https://www.solo.io/blog/navigating-istio-config-toolkit/

Problems after upgrade

Analyze

```
istioctl analyze --all-namespaces
```

Check the logs

Compare proxy config with previous

```
istioctl proxy-config <clusters|listeners|routes|...>
```

```
istioctl bug-report
```

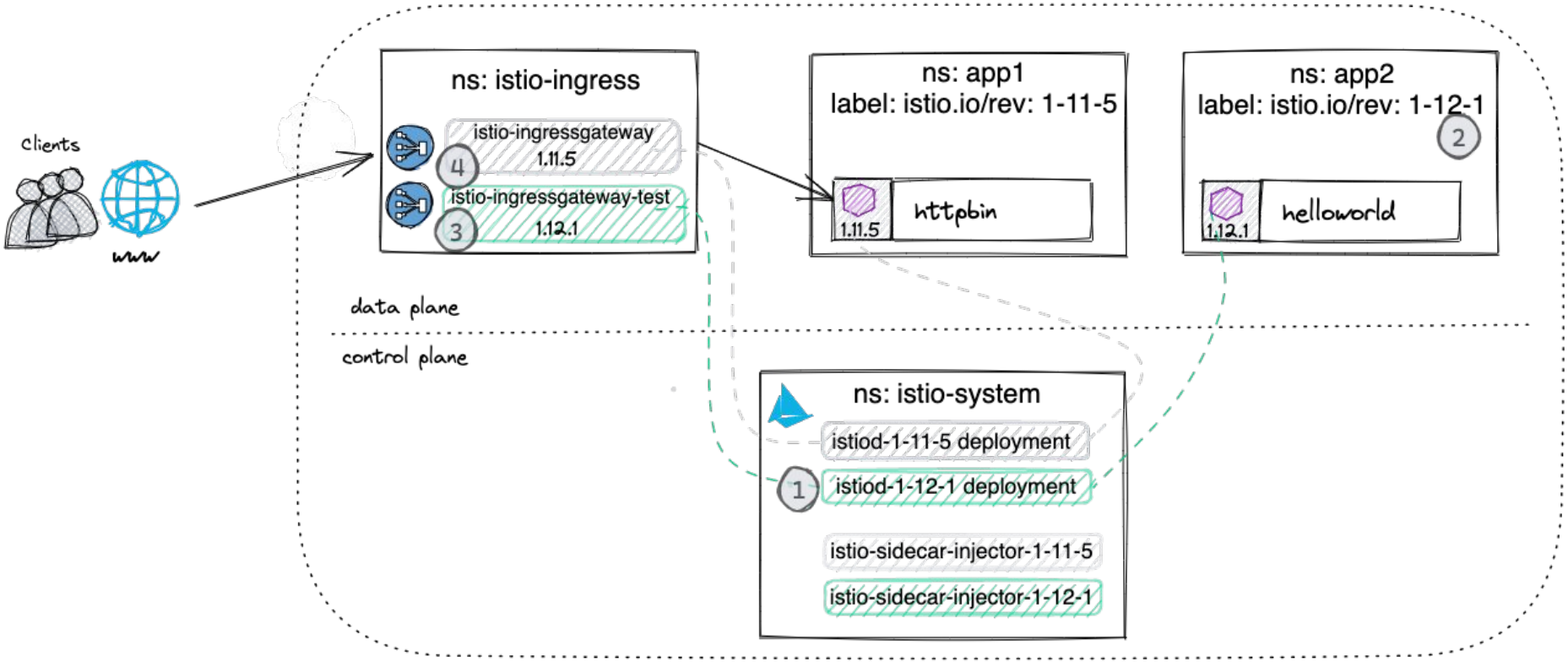
Troubleshoot

https://istio.io/latest/docs/ops/common-problems/

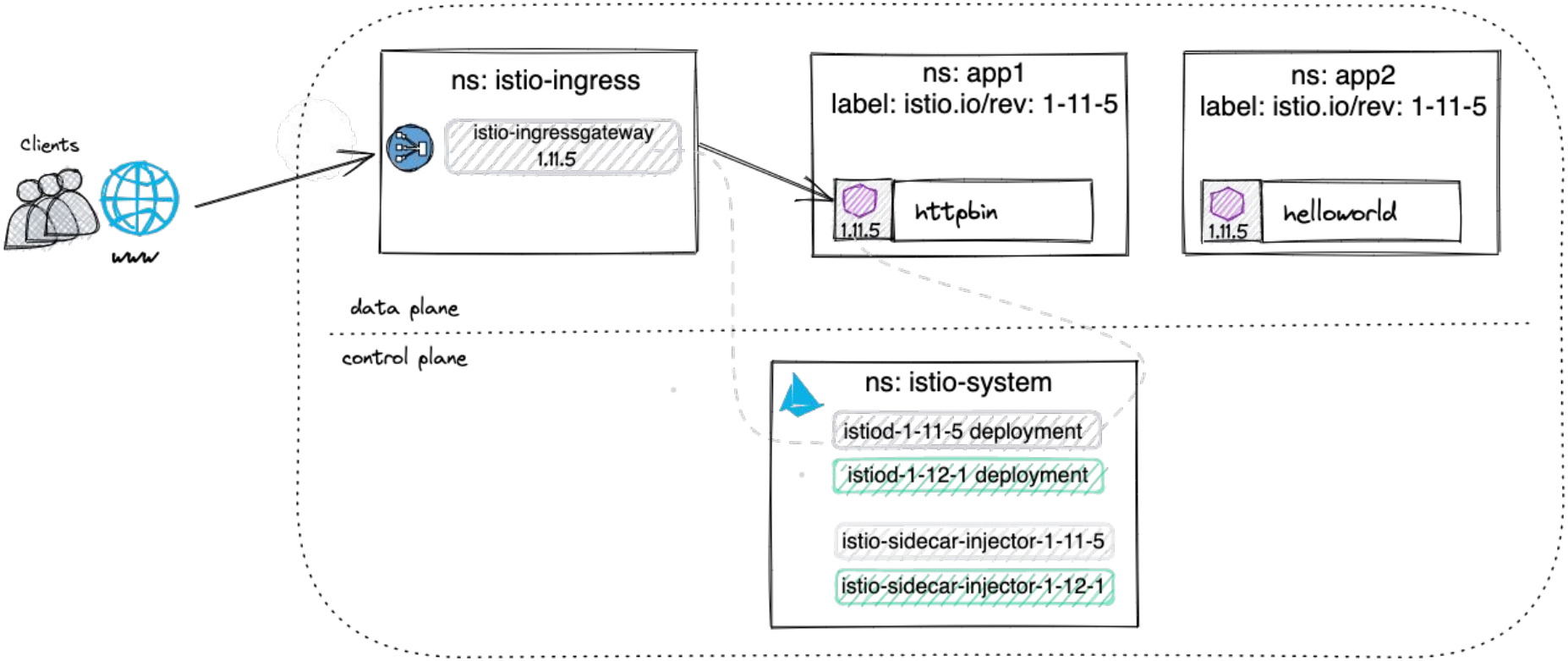
https://istio.io/latest/docs/ops/diagnostic-tools/

Revisions

Revisions

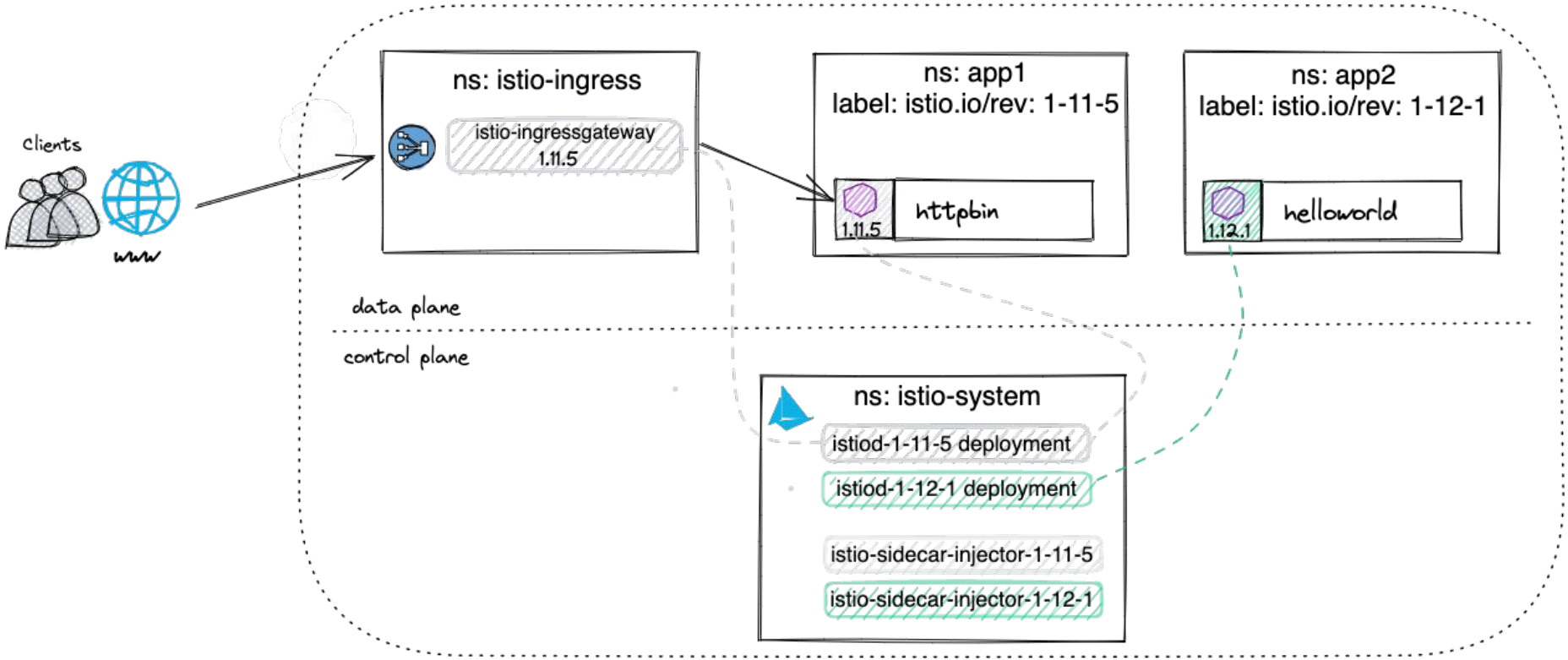

clients
www
ns: istio-ingress
istio-ingressgateway
1.11.5
4
istio-ingressgateway-test
1.12.1
3
ns: app1
label: istio.io/rev: 1-11-5
1.11.5
httpbin
ns: app2
label: istio.io/rev: 1-12-1
2
1.12.1
helloworld
data plane
control plane
ns: istio-system
istiod-1-11-5 deployment
1
istiod-1-12-1 deployment
istio-sidecar-injector-1-11-5
istio-sidecar-injector-1-12-1

Revisions: Step 1



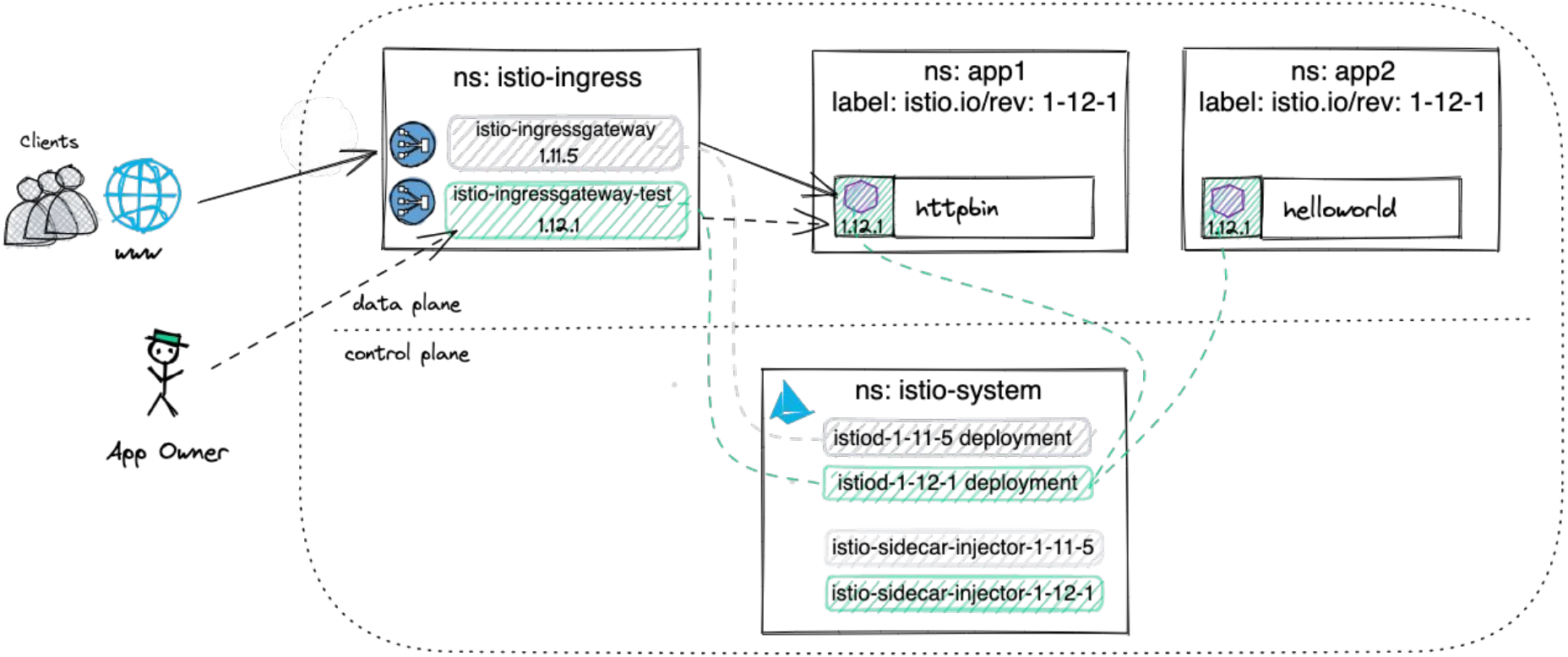

```
istioctl install -f istiodIstioOperator.yaml --revision 1-12-1
istioctl x revision list
```

Revisions: Step 2



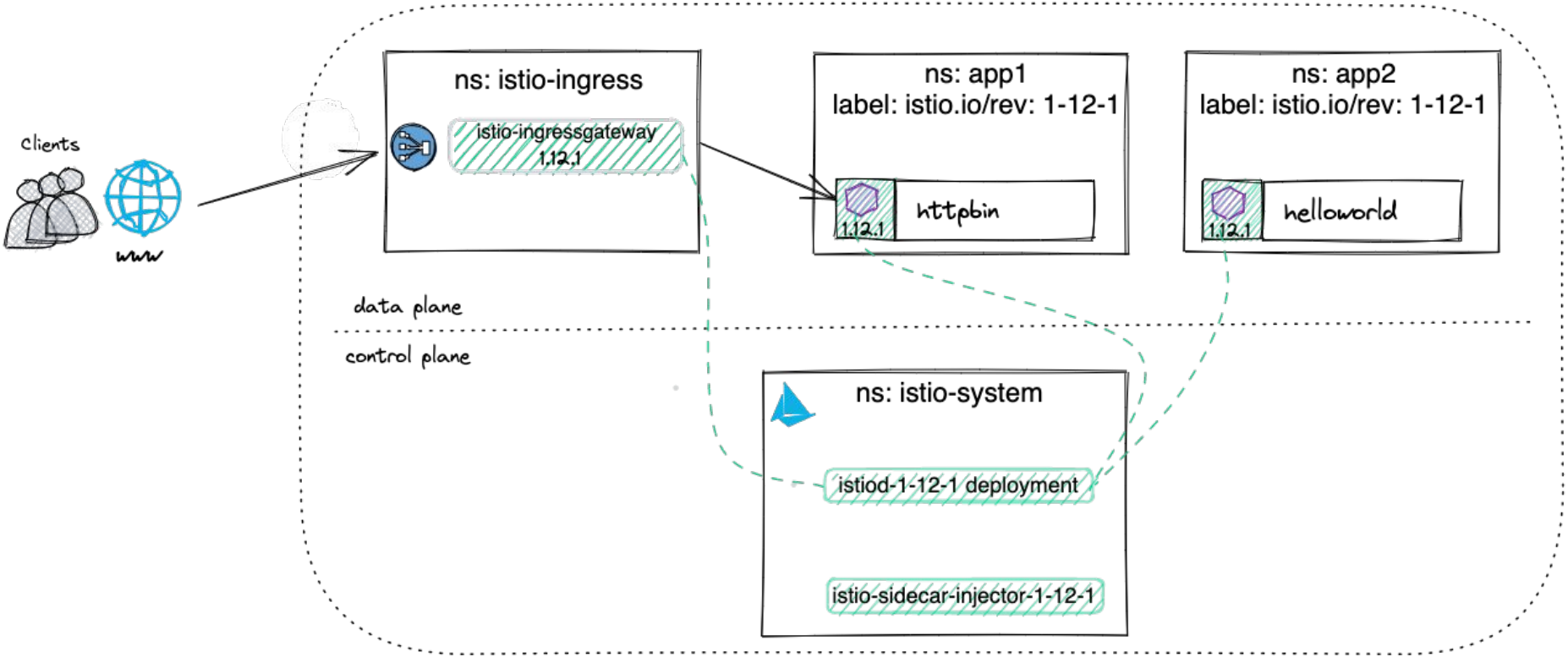

```
kubectl label namespace app2 istio.io/rev=1-12-1 --overwrite
kubectl rollout restart deployment -n app2
istioctl proxy-status
```

Revisions: Step 3



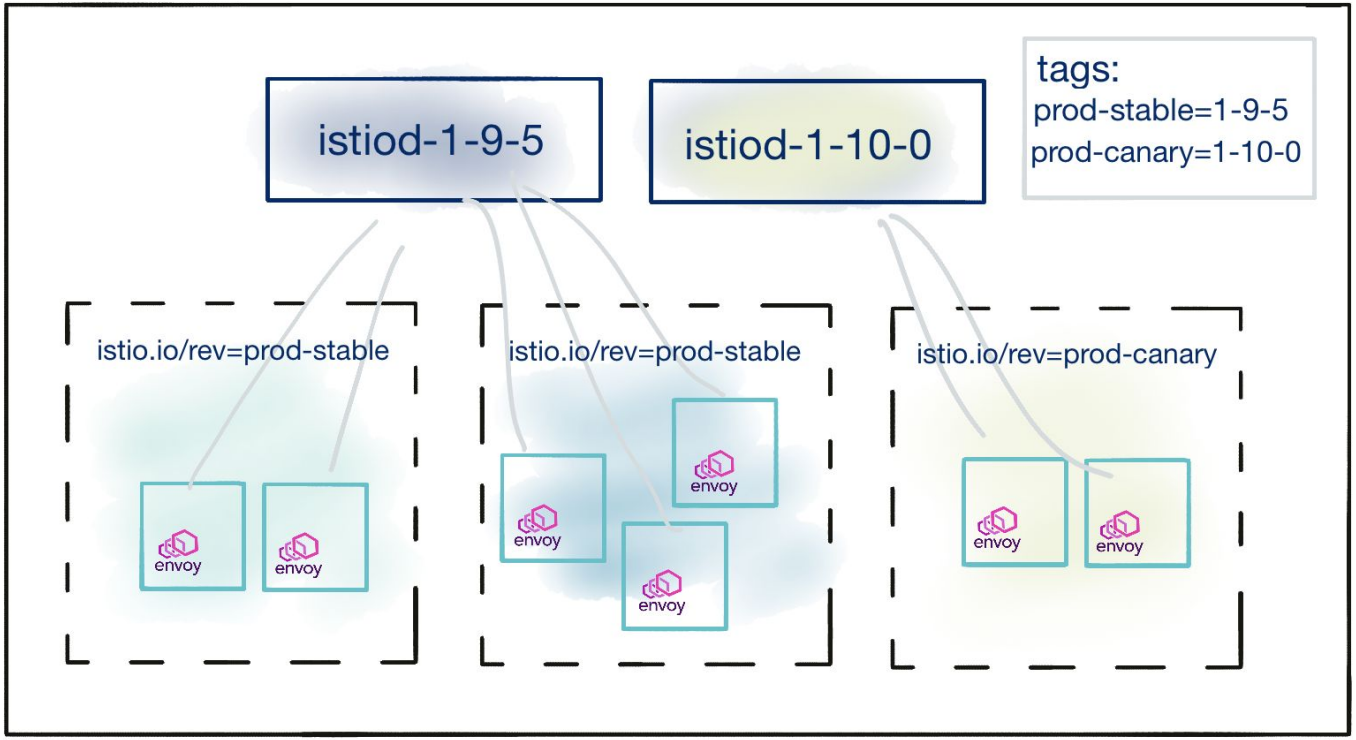

```
istioctl install -y -f ingress-gateway-test.yaml --revision 1-12-1
```

Revisions: Step 4



Revision tags

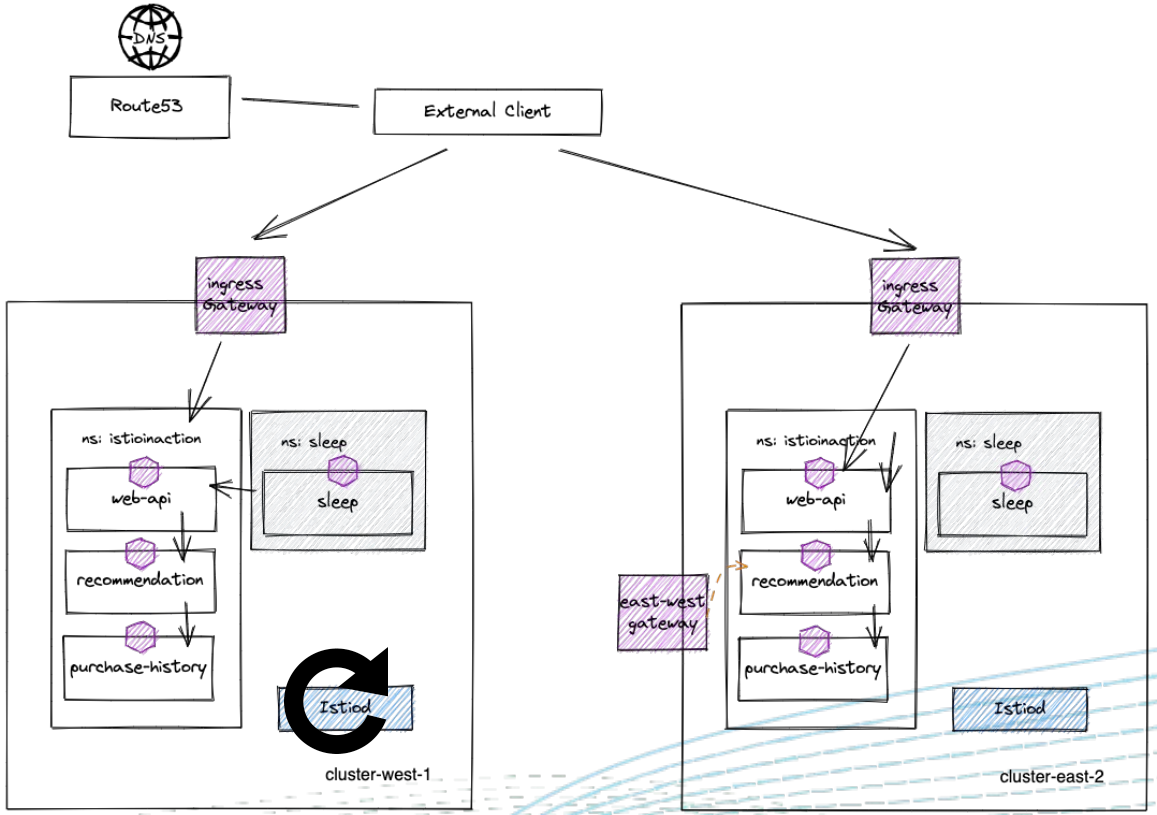
```
istioctl x revision tag list

TAG          REVISION NAMESPACES
prod-stable 1-9-5    istioinaction
prod-canary 1-10-0   istioinaction-canary
```



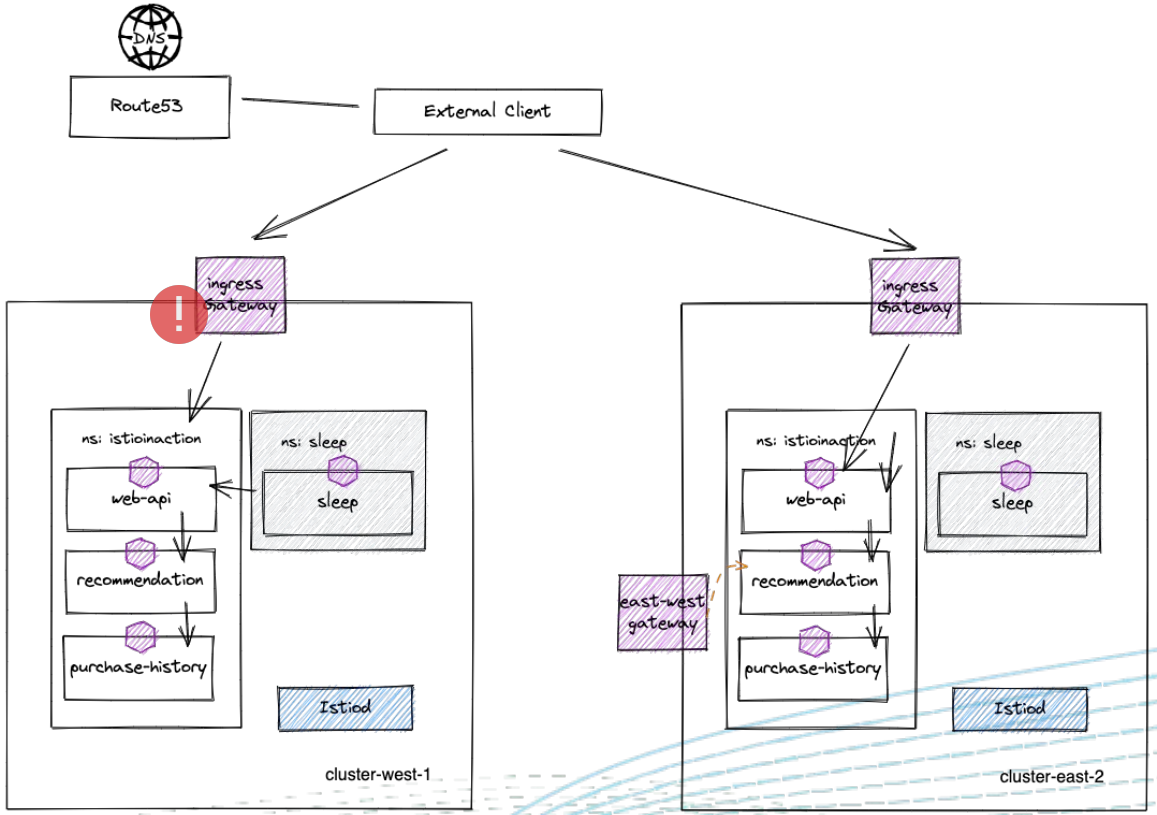
https://istio.io/latest/blog/2021/revision-tags/

Multi-Cluster

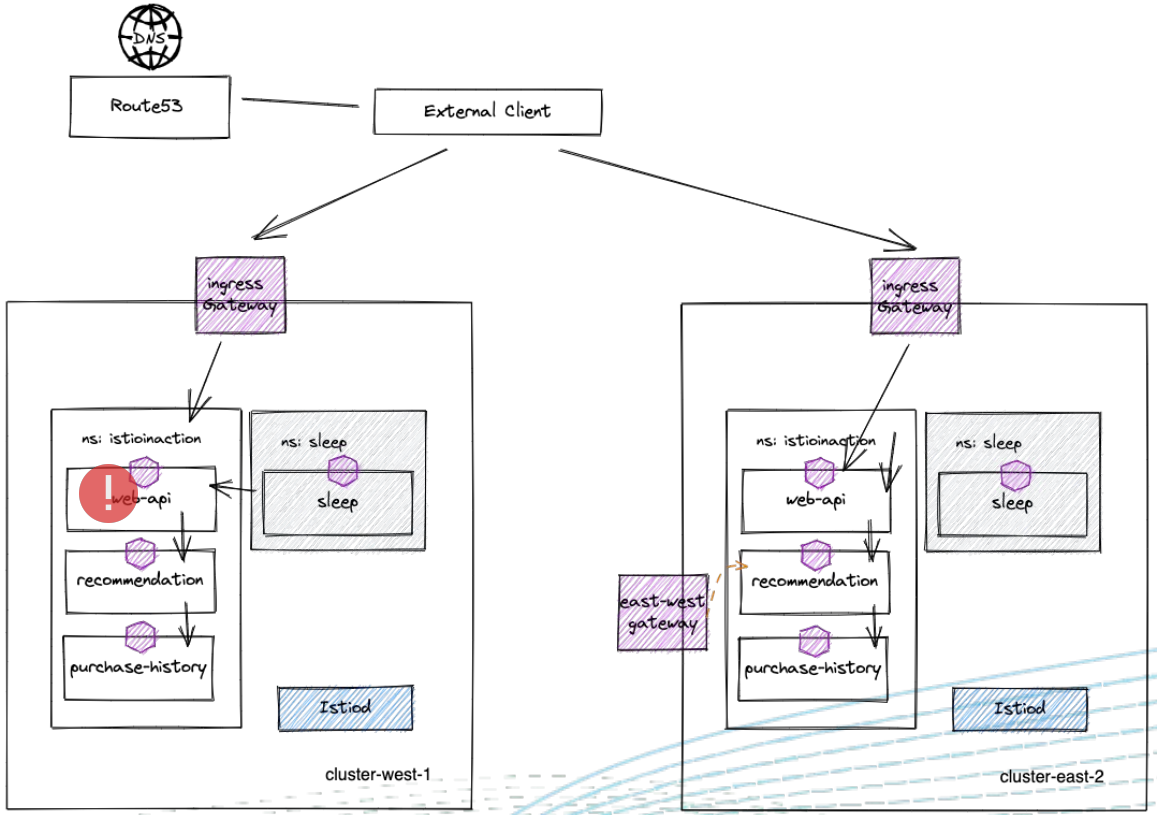
One cluster at a time



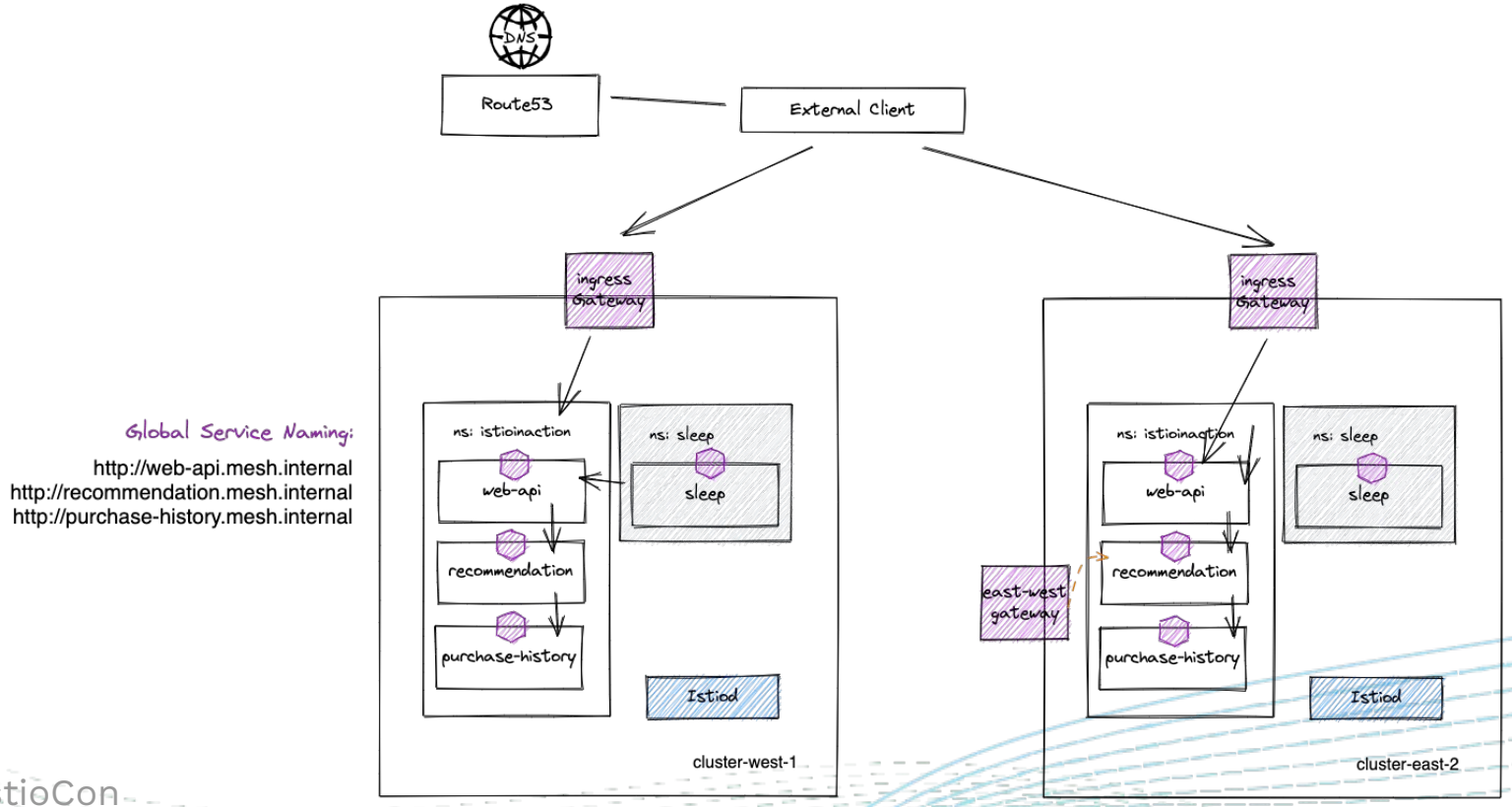
Cluster Failover



Workload Failover



Global Service



Cross cluster routing (multiple networks)

cluster1:

```yaml
apiVersion: networking.istio.io/v1beta1
kind: ServiceEntry
metadata:
  name: global-web-api
  namespace: istioinaction
spec:
  addresses:
  - 250.120.4.179
  hosts:
  - web-api.mesh.internal
  location: MESH_INTERNAL
  ports:
  - name: grpc-7000
    number: 7000
    protocol: GRPC
    targetPort: 7000
  resolution: STATIC
  workloadSelector:
    labels:
      app: web-api
```

```yaml
apiVersion: networking.istio.io/v1beta1
kind: WorkloadEntry
metadata:
  name: global-web-api
  namespace: istioinaction
spec:
  address: 34.82.32.121
  labels:
    app: web-api
  locality: us-west1
  ports:
    grpc-7000: 15443
```

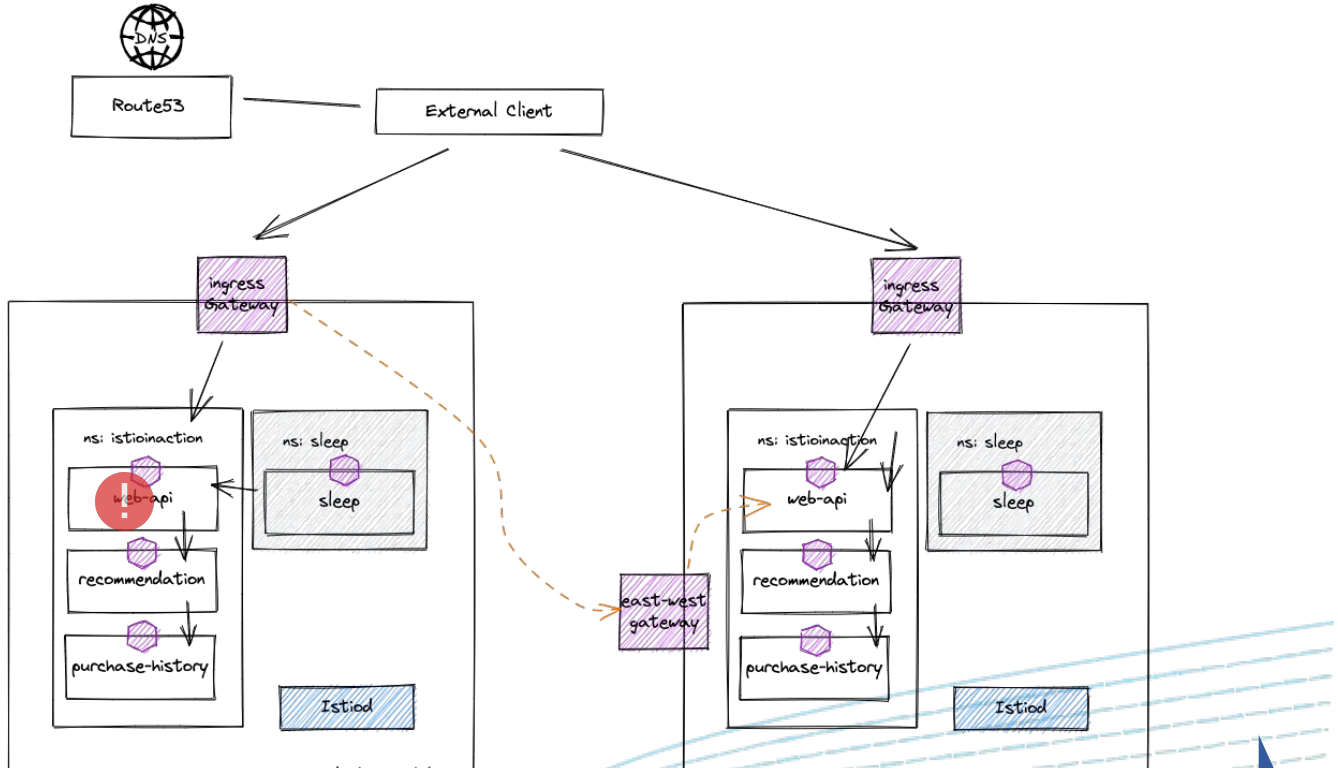
cluster2:

```yaml
apiVersion: networking.istio.io/v1beta1
kind: Gateway
metadata:
  name: eastwestgateway
  namespace: istio-gateways
spec:
  selector:
    app: istio-ingressgateway
    istio: eastwestgateway
  servers:
  - hosts:
    - ...
    name: eastwest-istio-eastwestgateway-
    port:
      name: tls
      number: 15443
      protocol: TLS
    tls:
      mode: AUTO_PASSTHROUGH
```



```
$ istioctl pc endpoints istio-ingressgateway-78b995cf66-24td6.istio-gateways --cluster "outbound|7000||web-ui.mesh.internal"
ENDPOINT                STATUS      OUTLIER CHECK     CLUSTER
10.16.1.53:7000         HEALTHY     OK                outbound|7000||web-api.mesh.internal   (LOCAL)
34.82.32.121:15443      HEALTHY     OK                outbound|7000||web-api.mesh.internal   (REMOTE)
```

Front-end Failover

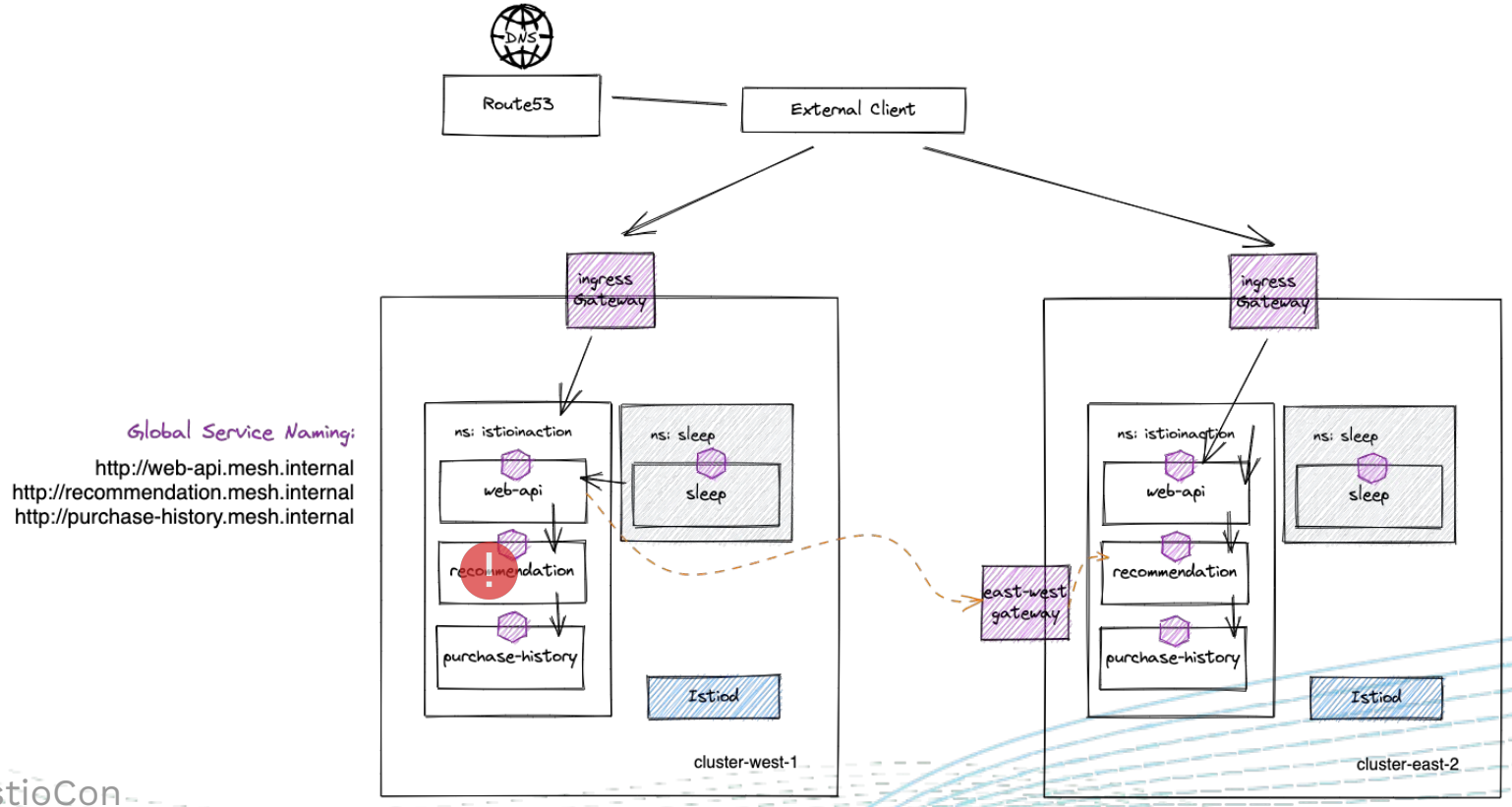


Global Service Naming:

http://web-api.mesh.internal
http://recommendation.mesh.internal
http://purchase-history.mesh.internal


```
$ istioctl pc endpoints istio-ingressgateway-78b995cf66-24td6.istio-gateways --cluster "outbound|7000||web-ui.mesh.internal"
ENDPOINT                STATUS      OUTLIER CHECK     CLUSTER
10.16.1.53:7000         HEALTHY     OK                outbound|7000||web-api.mesh.internal   (LOCAL)
34.82.32.121:15443      HEALTHY     OK                outbound|7000||web-api.mesh.internal   (REMOTE)
```

Back-end Failover



We're Hiring!

- Founded in 2017 by Idit Levine
- Based in Cambridge, MA
  with multiple locations around the globe
- Industry leaders in application networking, service mesh, and modern API gateway technologies
- Open-Core, "Enterprise" Subscription model

Growing fast with happy customers

350+% bookings growth y/y

98%+ renewal rate

Well Funded

$171.5M venture financing

$1 Billion valuation

Altimeter Redpoint true Ventures

solo.io

Gloo Application Networking Platform

Simplify your application networking with unified control, reliability, observability, extensibility, and security

Gloo Edge ENTERPRISE · Gloo · Gloo Mesh ENTERPRISE

Solo Istio/Envoy Community Leadership

Idit Levine
Founding API gateway WG-Istio

Lin Sun
Founding Istio project maintainer, Technical Oversight Committee (TOC), Steering Committee

Christian Posta
Founding community member, Istio Steering Committee, author Istio in Action

Ram Vennam
Founding Istio Steering Committee member

Yuval Kohavi
Renowned security researcher, Founding API Gateway WG-Istio, Contributor Envoy

Nick Nellis
First to run Istio in production, current contributor and maintainer

Neeraj Poddar
Istio Steering and TOC member. Co-founded Istio Product Security Working Group.

Greg Hanson
Founding Istio Maintainer, Product Security WG Lead, Istio Release Manager

Thank you!

@RamVennam
https://www.linkedin.com/in/ramvennam/