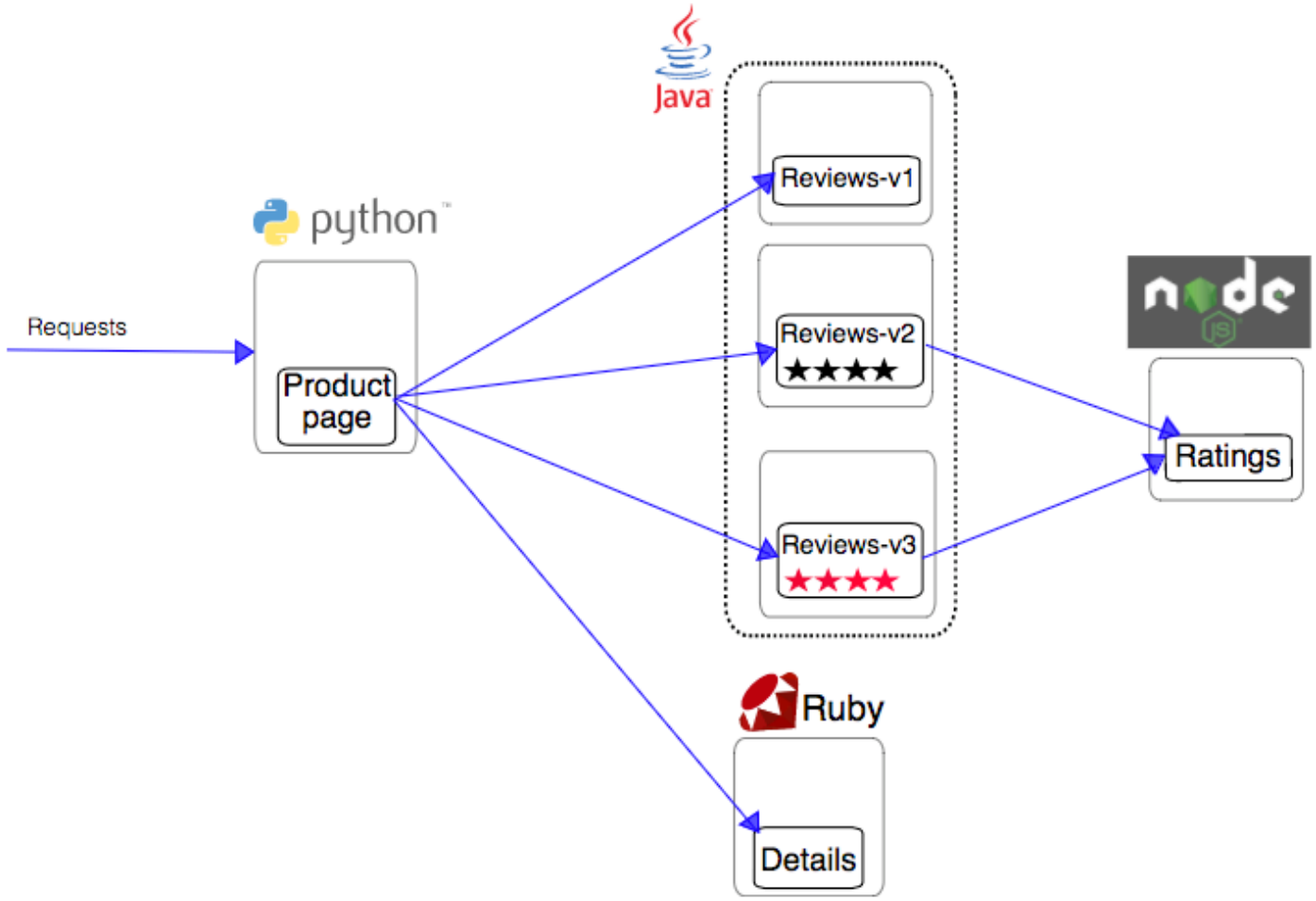
KubeCon

North America 2017

IoK: Istio-on-Kubernetes Follow Along: https://goo.gl/puZkNK

Daneyon Hansen
Twitter: @daneyonhansen
Software Engineer, Cisco

Sample App: BookInfo



Istio Architecture

=

Istio

Sidecar Proxy Injection

- **Manually**: istioctl client:

```
$ kubectl create -f <(istioctl kube-inject -f <your-app-spec>.yaml)
```

Sidecar Proxy Injection

- **Automatically:** **Initializer Controller** injects the proxy into a Pod before deployment.
  - Start kube-apiserver with the following flags:

```
--admission-control=apiserver.Admission.PluginNames=Initializers,…
--runtime-config=admissionregistration.k8s.io/v1alpha1
```

Initializer Pod & Config

https://goo.gl/aAHEaG

Initializer Logs

https://goo.gl/VVaM9a

```
$ kubectl logs istio-initializer-575f457bfb-qbwj6 -n istio-system
W1126 02:42:32.020000       1 client_config.go:529] Neither --kubeconfig nor --master was specified.  Us
I1126 02:42:32.020685       1 main.go:49] version @--
I1126 02:42:32.533425       1 http.go:100] Starting HTTP service at :8083
I1126 02:42:32.533535       1 initializer.go:229] Starting Istio sidecar initializer...
I1126 02:42:32.533545       1 initializer.go:230] Initializer name set to: sidecar.initializer.istio.io
I1126 02:42:32.533788       1 initializer.go:231] Options: (*inject.Config)(0xc42008e3c0)({
 Policy: (inject.InjectionPolicy) (len=7) "enabled",
 IncludeNamespaces: ([]string) (len=1 cap=4) {
  (string) ""
 },
 ExcludeNamespaces: ([]string) <nil>,
 Params: (inject.Params) {
  InitImage: (string) (len=72) "gcr.io/istio-testing/proxy_init:3101ea9d82a5f83b699c2d3245b371a19fa6bef
  ProxyImage: (string) (len=73) "gcr.io/istio-testing/proxy_debug:3101ea9d82a5f83b699c2d3245b371a19fa6be
  Verbosity: (int) 2,
  SidecarProxyUID: (int64) 1337,
  Version: (string) (len=40) "3101ea9d82a5f83b699c2d3245b371a19fa6bef4",
  EnableCoreDump: (bool) false,
  DebugMode: (bool) true,
  Mesh: (*istio_proxy_v1_config.MeshConfig)(0xc4200c4480)(mixer_address:"istio-mixer.istio-system:15004"
  ImagePullPolicy: (string) (len=12) "IfNotPresent",
  IncludeIPRanges: (string) ""
 },
 InitializerName: (string) (len=28) "sidecar.initializer.istio.io"
})
```

```
Supported kinds:
      /v1 ReplicationController
      extensions/v1beta1 Deployment
      extensions/v1beta1 DaemonSet
      extensions/v1beta1 ReplicaSet
      batch/v1 Job
      batch/v2alpha1 CronJob
      apps/v1beta1 StatefulSet
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-ca policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-initializer policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment kube-system/kube-dns policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment kube-system/kubernetes-dashboard policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-mixer policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-pilot policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-ingress policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=DaemonSet kube-system/kube-proxy policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-ca-65c9744685 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-initializer-575f457bfb policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kube-dns-5895d9587 policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kube-dns-7b6cdfd4df policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kubernetes-dashboard-5867bddc4c policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-mixer-747f9b7956 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-pilot-6f7946bf96 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-ingress-5d64d84f4 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/prometheus policy:"false" status:"" &Initializers{Pending
ping istio-system/prometheus due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/prometheus-6c98899bc9 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/zipkin policy:"false" status:"" &Initializers{Pending:[{s
ping istio-system/zipkin due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/zipkin-c866f6d66 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/grafana policy:"false" status:"" &Initializers{Pending:[{
ping istio-system/grafana due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/grafana-574647f54b policy:"false" status:"" nil
```

```
Supported kinds:
      /v1 ReplicationController
      extensions/v1beta1 Deployment
      extensions/v1beta1 DaemonSet
      extensions/v1beta1 ReplicaSet
      batch/v1 Job
      batch/v2alpha1 CronJob
      apps/v1beta1 StatefulSet
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-ca policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-initializer policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment kube-system/kube-dns policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment kube-system/kubernetes-dashboard policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-mixer policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-pilot policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/istio-ingress policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=DaemonSet kube-system/kube-proxy policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-ca-65c9744685 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-initializer-575f457bfb policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kube-dns-5895d9587 policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kube-dns-7b6cdfd4df policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet kube-system/kubernetes-dashboard-5867bddc4c policy:"" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-mixer-747f9b7956 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-pilot-6f7946bf96 policy:"false" status:"" nil
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/istio-ingress-5d64d84f4 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/prometheus policy:"false" status:"" &Initializers{Pending
ping istio-system/prometheus due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/prometheus-6c98899bc9 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/zipkin policy:"false" status:"" &Initializers{Pending:[{s
ping istio-system/zipkin due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/zipkin-c866f6d66 policy:"false" status:"" nil

 ObjectMeta initializer info extensions/v1beta1, Kind=Deployment istio-system/grafana policy:"false" status:"" &Initializers{Pending:[{
ping istio-system/grafana due to policy check
 ObjectMeta initializer info extensions/v1beta1, Kind=ReplicaSet istio-system/grafana-574647f54b policy:"false" status:"" nil
```

Initializer Logs: BookInfo Svcs

```
 Kind=Deployment default/details-v1 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
espacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/details-v1-9d9b86d48 policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
 Kind=Deployment default/ratings-v1 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
espacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/ratings-v1-6d8658447b policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
 Kind=Deployment default/reviews-v1 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
espacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/reviews-v1-859c6cb958 policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
 Kind=Deployment default/reviews-v2 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
espacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/reviews-v2-858895796b policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
 Kind=Deployment default/reviews-v3 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
espacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/reviews-v3-85999cd96b policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
 Kind=Deployment default/productpage-v1 policy:"" status:"" &Initializers{Pending:[{sidecar.initializer.istio.io}],Result:nil,}
 namespacePolicy:enabled useDefault:true inject:false status:"" required:true
 Kind=ReplicaSet default/productpage-v1-5dbc7b7576 policy:"" status:"injected-version-3101ea9d82a5f83b699c2d3245b371a19fa6bef4" nil
```

Pod Details for Envoy Sidecar

https://goo.gl/kmfY6g

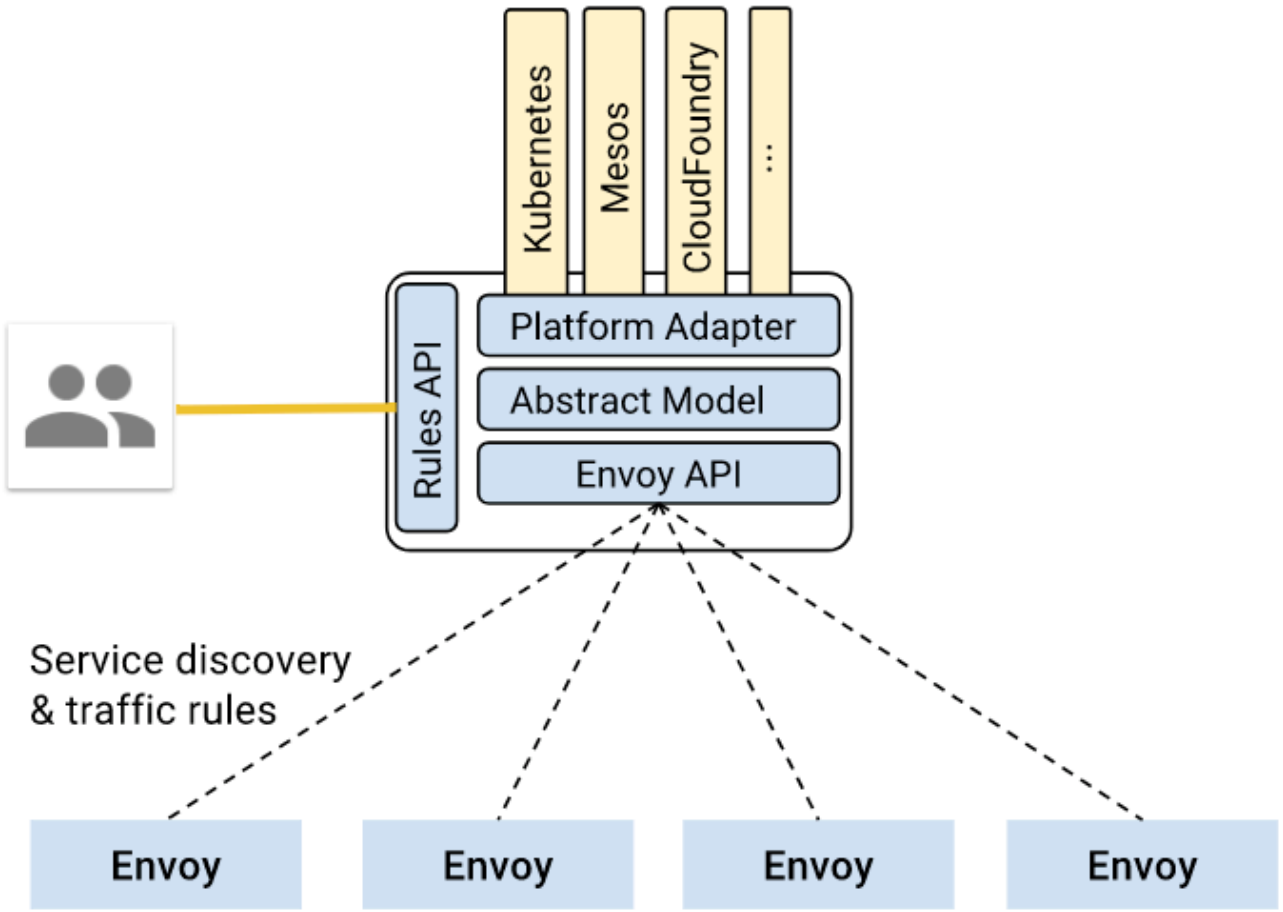
Envoy Sidecar Runtime Config

https://goo.gl/6JNEiT

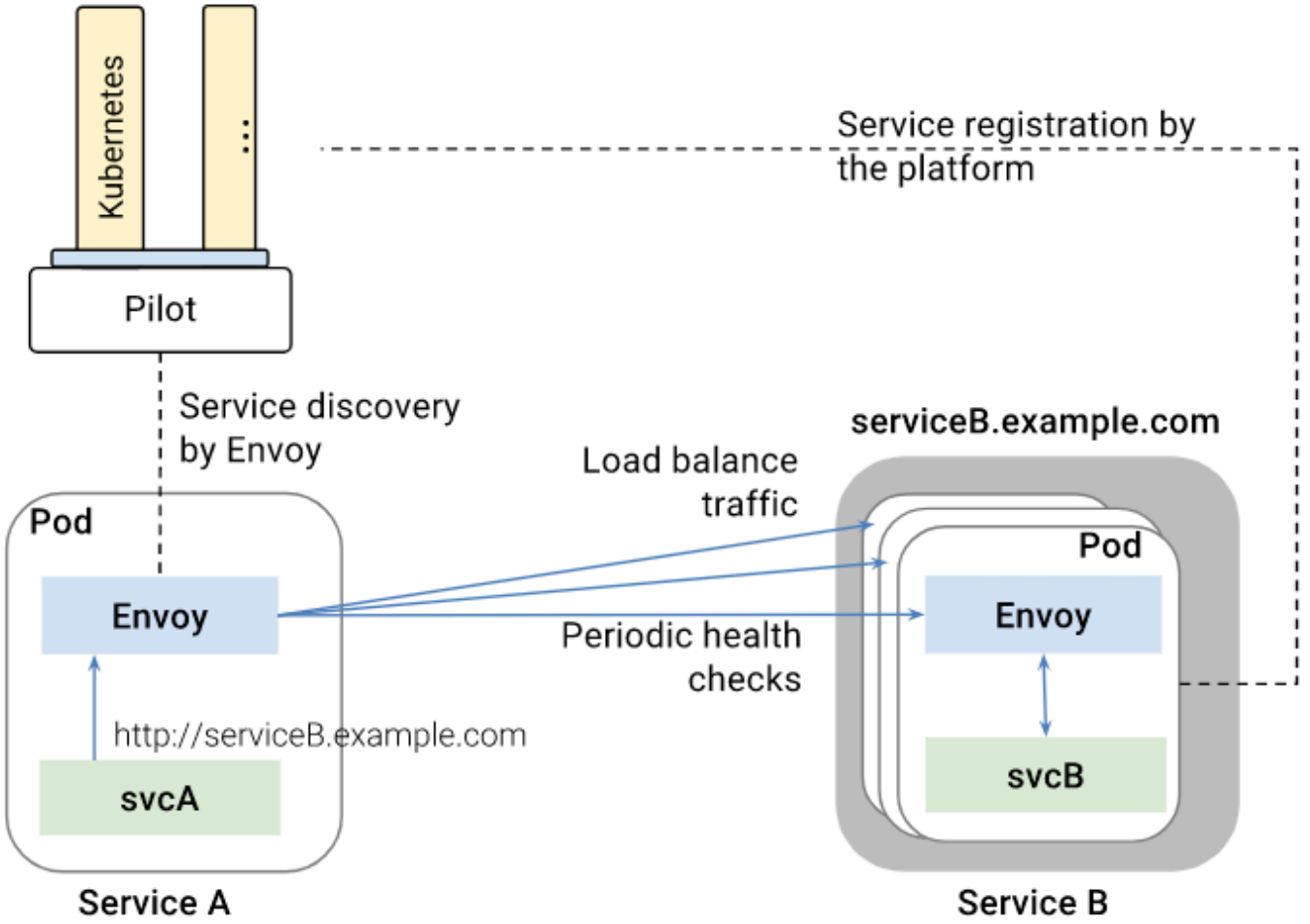
Envoy Runtime Config Details

https://goo.gl/1idW7R

Pilot Architecture



Discovery & Load Balancing



Pilot Configuration

https://goo.gl/BnYe5g

Pilot Logs

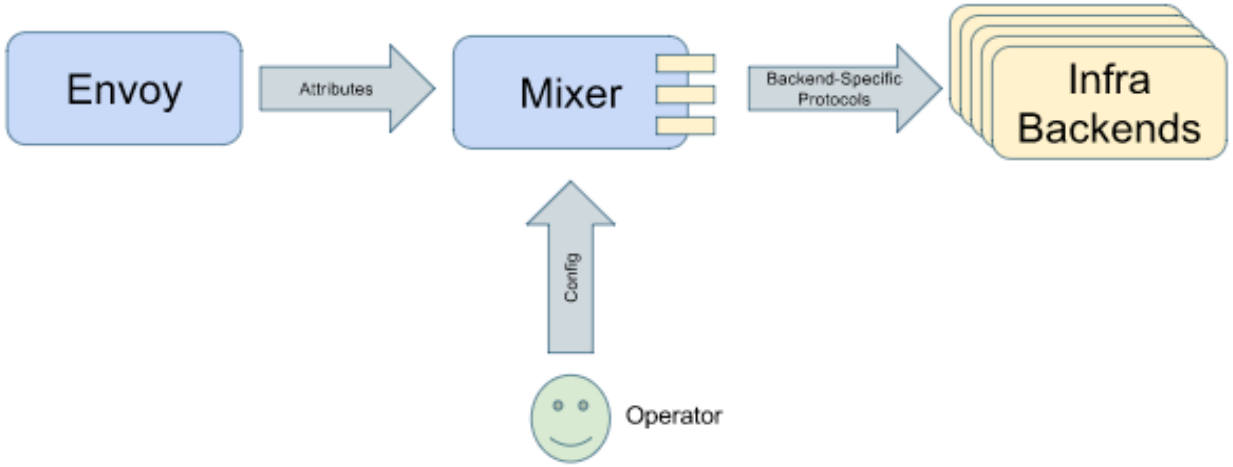
https://goo.gl/BnYe5g

```
$ kubectl logs po/istio-pilot-6f488645dd-52p2f -c discovery -n istio-system
I1117 17:22:53.292240       1 main.go:93] mesh configuration (*istio_proxy_v1_config.MeshConfig)(0xc4200c2990)(mixer_address:"istio-mixer.istio-system:15004" proxy_listen_port:15001
connect_timeout:<seconds:1 > ingress_class:"istio" ingress_service:"istio-ingress" ingress_controller_mode:STRICT auth_policy:MUTUAL_TLS rds_refresh_delay:<seconds:1 >
enable_tracing:true access_log_file:"/dev/stdout" default_config:<config_path:"/etc/istio/proxy" binary_path:"/usr/local/bin/envoy" service_cluster:"istio-proxy" drain_duration:
<seconds:45 > parent_shutdown_duration:<seconds:60 > discovery_address:"istio-pilot.istio-system:15003" discovery_refresh_delay:<seconds:1 > zipkin_address:"zipkin.istio-system:9411"
connect_timeout:<seconds:10 > statsd_udp_address:"istio-mixer.istio-system:9125" proxy_admin_port:15000 control_plane_auth_policy:MUTUAL_TLS > )
I1117 17:22:53.292289       1 main.go:94] version bootstrap@12e74b1a-bb2b-11e7-a0f8-0a580a2c634d-3101ea9d82a5f83b699c2d3245b371a19fa6bef4-3101ea9d82a5f83b699c2d3245b371a19fa6bef4
```

```
I1117 17:22:53.292441       1 main.go:95] flags (main.args) {
 kubeconfig: (string) "",
 meshconfig: (string) (len=22) "/etc/istio/config/mesh",
 namespace: (string) "",
 controllerOptions: (kube.ControllerOptions) {
  WatchedNamespace: (string) "",
  ResyncPeriod: (time.Duration) 1m0s,
  DomainSuffix: (string) (len=13) "cluster.local"
 },
 discoveryOptions: (envoy.DiscoveryServiceOptions) {
  Port: (int) 8080,
  EnableProfiling: (bool) true,
  EnableCaching: (bool) true
 },
 registries: ([]string) (len=1 cap=1) {
  (string) (len=10) "Kubernetes"
 },
 consul: (main.consulArgs) {
  config: (string) "",
  serverURL: (string) ""
 },
 eureka: (main.eurekaArgs) {
  serverURL: (string) ""
 },
 admissionArgs: (admit.ControllerOptions) {
  Descriptor: (model.ConfigDescriptor) <nil>,
  ExternalAdmissionWebhookName: (string) (len=22) "pilot-webhook.istio.io",
  ServiceName: (string) (len=20) "istio-pilot-external",
  ServiceNamespace: (string) "",
  ValidateNamespaces: ([]string) <nil>,
  DomainSuffix: (string) "",
  SecretName: (string) (len=13) "pilot-webhook",
  Port: (int) 443,
  RegistrationDelay: (time.Duration) 5s
 }
}
```

Control Plane: Mixer

Mixer = attribute processing & routing engine



Mixer Config

https://goo.gl/smmHQv

envoy_mixer_auth.json

https://goo.gl/EVFAwF

Mixer Logs

https://goo.gl/smmHQv

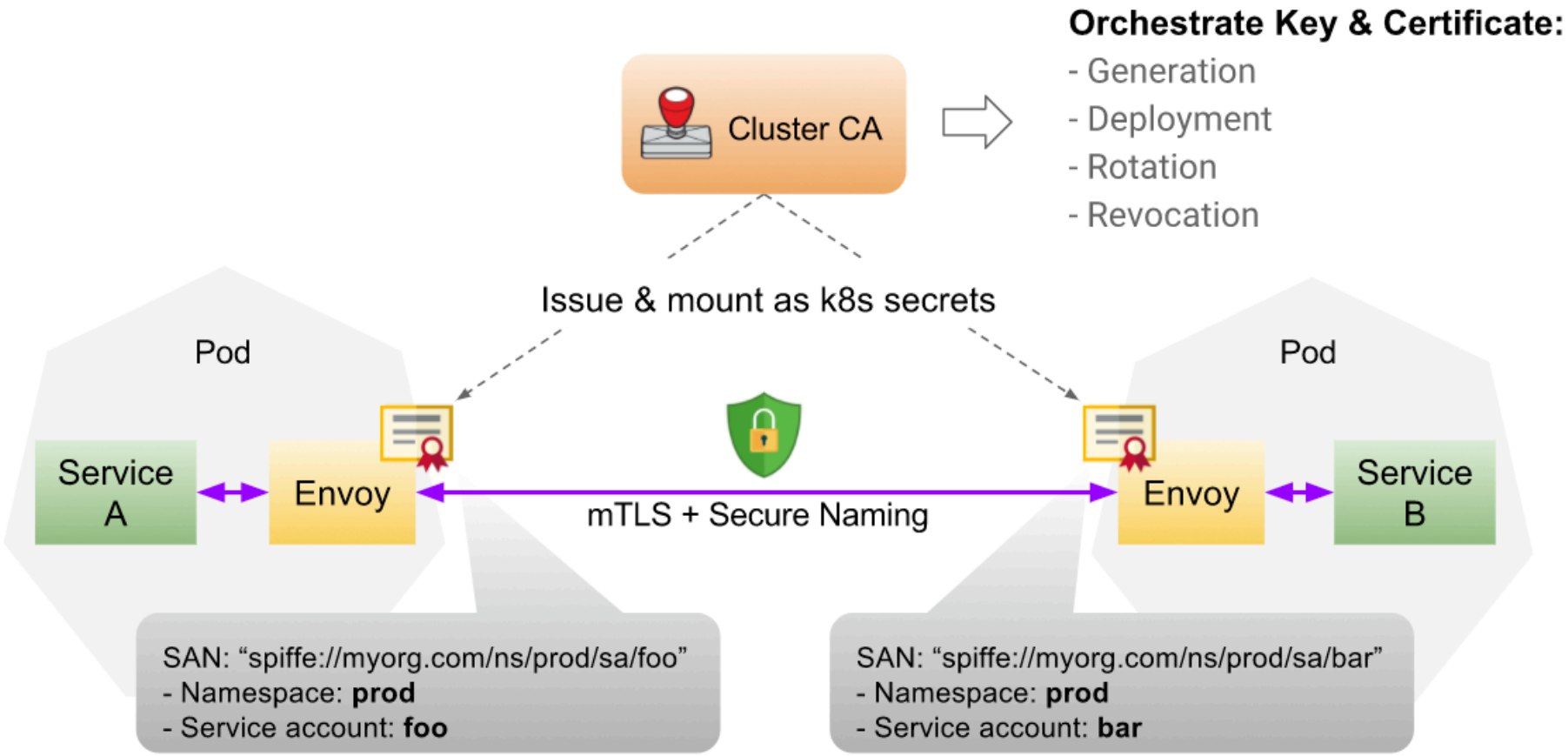
```
$ kubectl logs istio-mixer-599d4469fb-nx97l -n istio-system -c mixer
Mixer started with
maxMessageSize: 1048576
maxConcurrentStreams: 1024
apiWorkerPoolSize: 1024
adapterWorkerPoolSize: 1024
expressionEvalCacheSize: 1024
port: 9091
configAPIPort: 9094
monitoringPort: 9093
singleThreaded: false
compressedPayload: false
traceOutput: http://zipkin:9411/api/v1/spans
serverCertFile:
serverKeyFile:
clientCertFiles:
configStoreURL: fs:///etc/opt/mixer/configroot
configStore2URL: k8s://
configDefaultNamespace: istio-system
configFetchIntervalSec: 5
configIdentityAttribute: destination.service
configIdentityAttributeDomain: svc.cluster.local
useAst: false
stringTablePurgeLimit: 1024
```

```
$ kubectl logs istio-mixer-599d4469fb-nx97l -n istio-system -c mixer
Mixer started with
maxMessageSize: 1048576
maxConcurrentStreams: 1024
apiWorkerPoolSize: 1024
adapterWorkerPoolSize: 1024
expressionEvalCacheSize: 1024
port: 9091
configAPIPort: 9094
monitoringPort: 9093
singleThreaded: false
compressedPayload: false
traceOutput: http://zipkin:9411/api/v1/spans
serverCertFile:
serverKeyFile:
clientCertFiles:
configStoreURL: fs:///etc/opt/mixer/configroot
configStore2URL: k8s://
configDefaultNamespace: istio-system
configFetchIntervalSec: 5
configIdentityAttribute: destination.service
configIdentityAttributeDomain: svc.cluster.local
useAst: false
stringTablePurgeLimit: 1024
```

```
$ kubectl logs istio-mixer-599d4469fb-nx97l -n istio-system -c mixer
Mixer started with
maxMessageSize: 1048576
maxConcurrentStreams: 1024
apiWorkerPoolSize: 1024
adapterWorkerPoolSize: 1024
expressionEvalCacheSize: 1024
port: 9091
configAPIPort: 9094
monitoringPort: 9093
singleThreaded: false
compressedPayload: false
traceOutput: http://zipkin:9411/api/v1/spans
serverCertFile:
serverKeyFile:
clientCertFiles:
configStoreURL: fs:///etc/opt/mixer/configroot
configStore2URL: k8s://
configDefaultNamespace: istio-system
configFetchIntervalSec: 5
configIdentityAttribute: destination.service
configIdentityAttributeDomain: svc.cluster.local
useAst: false
stringTablePurgeLimit: 1024
```

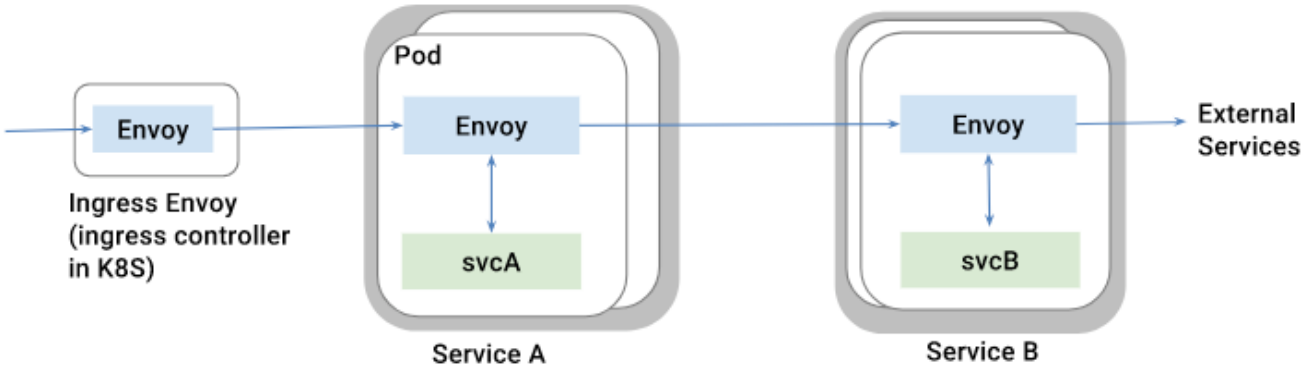
```
I1117 17:37:41.314064       1 grpcServer.go:155] Dispatching to main adapters after running processors
I1117 17:37:41.314159       1 grpcServer.go:156] Attribute Bag:
context.protocol             : http
destination.ip               : [10 192 2 12]
destination.service          : details.default.svc.cluster.local
destination.uid              : kubernetes://details-v1-84cc6f7898-bnczx.default
quota.amount                 : 1
quota.name                   : RequestCount
request.headers              : map[accept:*/* :path:/details/0 :authority:details:9080 user-agent:python-requests/2.18.4 x-b3-
parentspanid:c0fd44c189d3c28c x-request-id:5d4e82dc-46de-9b10-9b12-6d1425257dda x-forwarded-proto:http accept-encoding:gzip, deflate
context:c0fd44c189d3c28c;f889bf4e5e62df96;c0fd44c189d3c28c :method:GET content-length:0 x-b3-traceid:c0fd44c189d3c28c x-b3-sampled:1
spanid:f889bf4e5e62df96]
request.host                 : details:9080
request.method               : GET
request.path                 : /details/0
request.scheme               : http
request.time                 : 2017-11-17 17:37:41.307879462 +0000 UTC
request.useragent            : python-requests/2.18.4
source.ip                    : [10 192 2 17]
source.port                  : 58748
source.uid                   : kubernetes://productpage-v1-7c9854f67d-tdc7w.default
source.user                  : spiffe://cluster.local/ns/default/sa/default
---
destination.labels           : map[app:details pod-template-hash:4077293454 version:v1]
destination.namespace        : default
destination.serviceAccount   : default
source.labels                : map[pod-template-hash:3754109238 version:v1 app:productpage]
source.namespace             : default
source.service               : productpage.default.svc.cluster.local
source.serviceAccount        : default
I1117 17:37:41.314180       1 grpcServer.go:160] Dispatching Check
I1117 17:37:41.314217       1 dispatcher.go:163] Resolved (TEMPLATE_VARIETY_CHECK) 0 actions
I1117 17:37:41.314235       1 grpcServer.go:183] Check returned with ok
I1117 17:37:41.314246       1 grpcServer.go:246] Dispatching Quota2: RequestCount
I1117 17:37:41.314255       1 dispatcher.go:163] Resolved (TEMPLATE_VARIETY_QUOTA) 0 actions
I1117 17:37:41.314265       1 grpcServer.go:227] AccessLog Quota details.default.svc.cluster.local 1/1
I1117 17:37:41.336469       1 grpcServer.go:137] Dispatching Preprocess Check
I1117 17:37:41.336497       1 runtime.go:113] unconditionally resolving for kinds: [attributes]
I1117 17:37:41.336549       1 runtime.go:176] no rules for global/default.svc.cluster.local
I1117 17:37:41.336562       1 runtime.go:176] no rules for global/reviews.default.svc.cluster.local
I1117 17:37:41.336567       1 runtime.go:176] no rules for default.svc.cluster.local/default.svc.cluster.local
I1117 17:37:41.336570       1 runtime.go:176] no rules for default.svc.cluster.local/reviews.default.svc.cluster.local
I1117 17:37:41.336578       1 runtime.go:176] no rules for reviews.default.svc.cluster.local/reviews.default.svc.cluster.local
I1117 17:37:41.336583       1 runtime.go:121] unconditionally resolved configs (err=<nil>): [kubernetes]
```

Security


Orchestrate Key & Certificate:
- Generation
- Deployment
- Rotation
- Revocation
Cluster CA
Issue & mount as k8s secrets
Pod
Pod
Service A
Envoy
mTLS + Secure Naming
Envoy
Service B
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

Ingress

- Ingress resource is used to expose a service outside the cluster
- Gives services externally-reachable URLs, load balance traffic, terminate SSL, etc..
- An Ingress Controller is a daemon deployed as a pod.



Egress

- Istio services are unable to access external services by default
- Egress rules provide access to external services
- Egress rules currently only supports HTTP/HTTPS requests

```
1  apiVersion: config.istio.io/v1alpha2
2  kind: EgressRule
3  metadata:
4    name: google-egress-rule
5  spec:
6    destination:
7      service: www.google.com
8    ports:
9      - port: 443
10       protocol: https
```

Egress

```
1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: istio-inject
5    namespace: istio-system
6  data:
7    config: |-
8      policy: "enabled"
9      namespaces: [""] # everything, aka v1.NamepsaceAll,
10     initializerName: "sidecar.initializer.istio.io"
11     params:
12       initImage: gcr.io/istio-testing/proxy_init:3101ea9
13       proxyImage: gcr.io/istio-testing/proxy_debug:3101e
14       verbosity: 2
15       version: 3101ea9d82a5f83b699c2d3245b371a19fa6bef4
16       meshConfigMapName: istio
17       imagePullPolicy: IfNotPresent
18       debugMode: true
19       includeIPRanges: 10.0.0.0/16
```

The **includeIPRanges** parameter can be used to prevent proxies from intercepting external requests.

Thank You!