Istio + Gatekeeper

Ernest Wong
Software Engineer
Microsoft

Mathieu Benoit
DevRel Engineer
Google

IstioCon

Agenda

What's Gatekeeper?

Enforce Istio's best practices

Demos

Resources

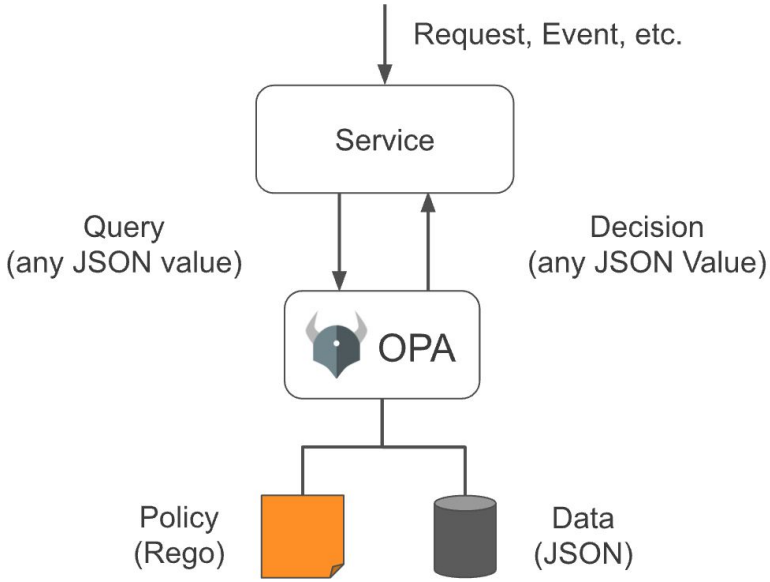
Q&A

What are Policies?

- Govern the behavior of a software system
- Policy examples:
  - Only allow deployment of container images from gcr.io
  - Services must not use `type: LoadBalancer` in a Kubernetes cluster
- Security, compliance, software supply chain
- Policy **evaluation** and **enforcement**

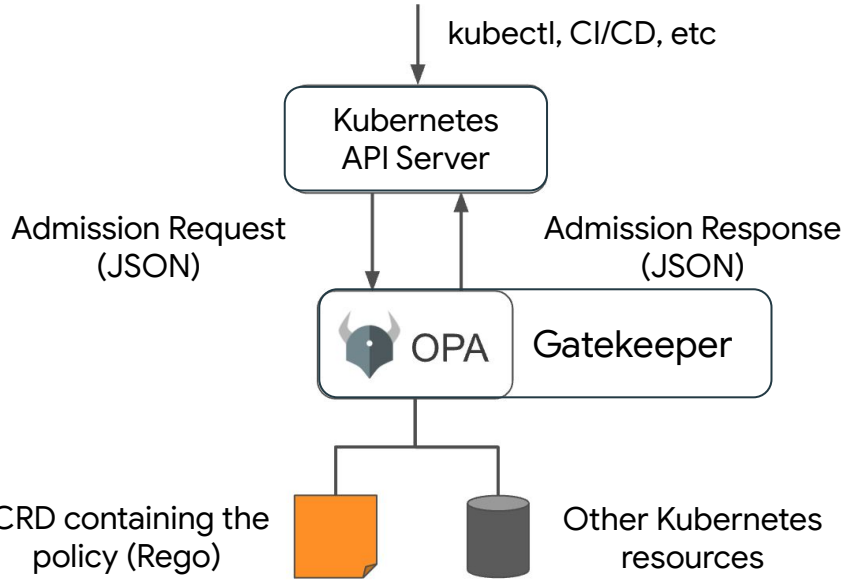
Open Policy Agent (OPA)

- Declarative, general-purpose policy engine
- Graduated from CNCF in 2021
- Features
  - Policy evaluation
  - Policy as code (Rego)
  - Context-aware



Gatekeeper

- Kubernetes Admission Controller that extends OPA
- Policy **enforcement**
- Mutations, External Data, etc



Constraint Templates

- Contains the Rego policy
- Schema of the constraint (policy)
- Analogy: Classes in object-oriented programming

```yaml
apiVersion: templates.gatekeeper.sh/v1
kind: ConstraintTemplate
metadata:
  annotations:
    description: Requires that service port names have a prefix from a specified list.
  name: allowedserviceportname
spec:
  crd:
    spec:
      names:
        kind: AllowedServicePortName
      validation:
        openAPIV3Schema:
          type: object
          properties:
            prefixes:
              description: Prefixes of allowed service port names.
              items:
                type: string
              type: array
```

Constraint Templates

- Contains the Rego policy
- Schema of the constraint (policy)
- Analogy: Classes in object-oriented programming

```
targets:
- target: admission.k8s.gatekeeper.sh
  rego: |
    package istio.guardrails.allowedserviceportname

    violation[{"msg": msg}] {
      service := input.review.object
      port := service.spec.ports[_]
      prefixes := input.parameters.prefixes
      not is_prefixed(port, prefixes)
      msg := sprintf("the service port name <%v> has a disallowed prefix,
        allowed prefixes are %v", [port.name, prefixes])
    }

    is_prefixed(port, prefixes) {
      prefix := prefixes[_]
      startswith(port.name, prefix)
    }
```

Constraints

- Instance of a Constraint Template
- Analogy: Objects in object-oriented programming

```yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: AllowedServicePortName
metadata:
  name: port-name-constraint
spec:
  enforcementAction: deny
  match:
    kinds:
    - apiGroups:
      - ""
      kinds:
      - Service
  parameters:
    prefixes:
    - http
    - grpc
    - tcp
```

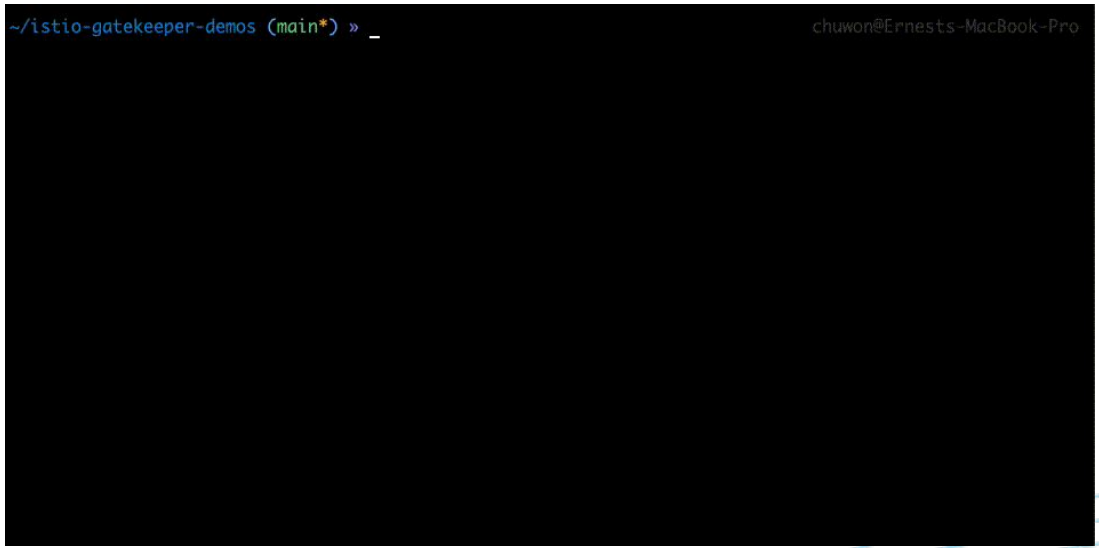
Referential Policies

- Sync different types of resources into Gatekeeper's cache
- Multi-object, complex policies

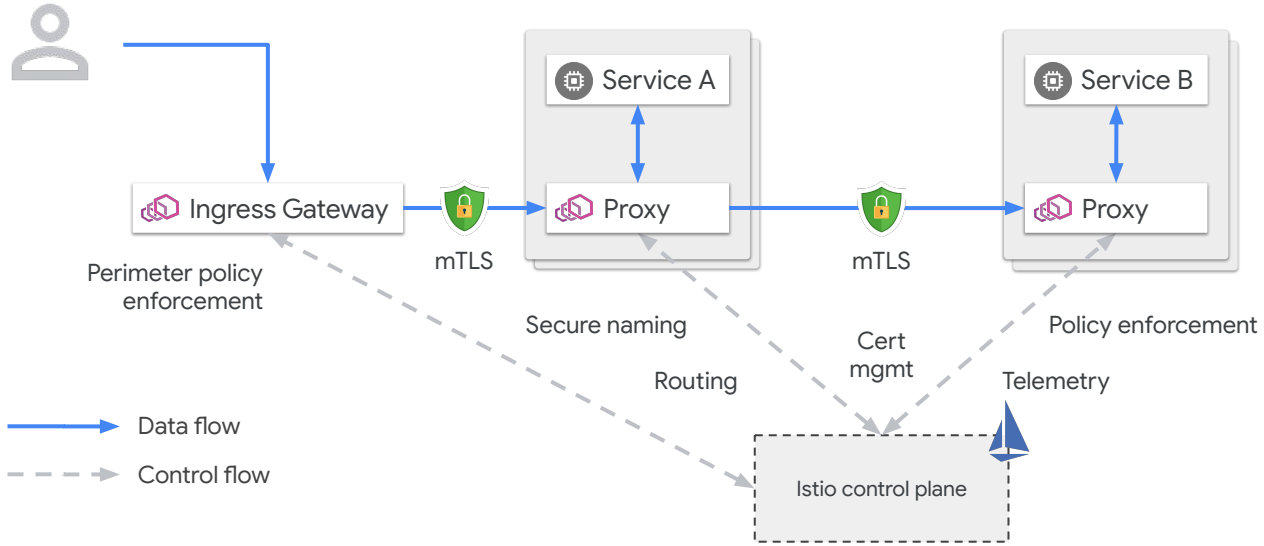
```yaml
apiVersion: config.gatekeeper.sh/v1alpha1
kind: Config
metadata:
  name: config
  namespace: gatekeeper-system
spec:
  sync:
    syncOnly:
      - group: ""
        version: "v1"
        kind: "Namespace"
      - group: "security.istio.io"
        version: "v1beta1"
        kind: "PeerAuthentication"
      - group: "security.istio.io"
        version: "v1beta1"
        kind: "AuthorizationPolicy"
```

Gator CLI

CLI for unit-testing Constraint Templates and Constraints locally



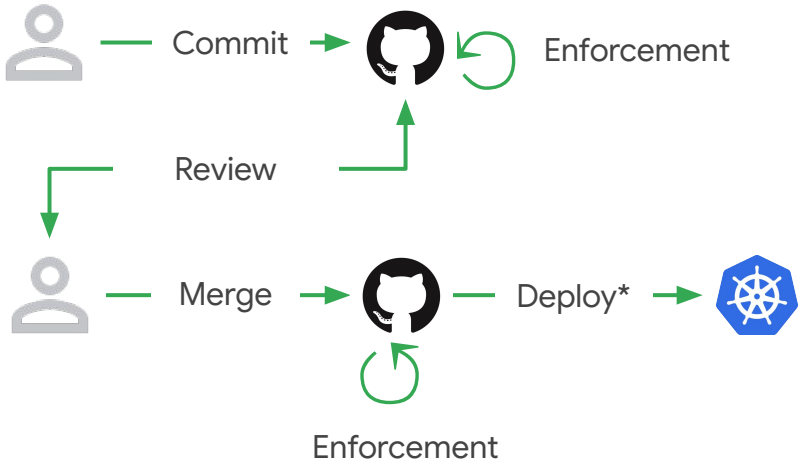
Istio makes your clusters more secure



Let's enforce Istio's security best practice

- Enforce sidecar proxies injection
  - `K8sRequiredLabels`
  - `SidecarInjectionAnnotation`
- Enforce `STRICT` mTLS
  - `PeerAuthnMeshStrictMtls`
  - `PeerAuthnStrictMtls`
  - `DestinationRuleTLSEnabled`
- Enforce `AuthorizationPolicies`
  - `AuthzPolicyDefaultDeny`
- Enforce `Service` port name
  - `AllowedServicePortName`
- And there is more, choose what's important for you from there!

Shift enforcement left



* push or pull

Resources

- Resources of the demos: https://github.com/mathieu-benoit/istio-gatekeeper-demos
- Watch other sessions at IstioCon 2022, a lot of them talk about Security best practices with Istio

- Istio
- Istio security best practices
- Gatekeeper
- kpt gatekeeper
- The Rego Playground

Q&A

Thank you!