KubeCon | CloudNativeCon

Europe 2023

Open Policy Agent

Maintainers talk

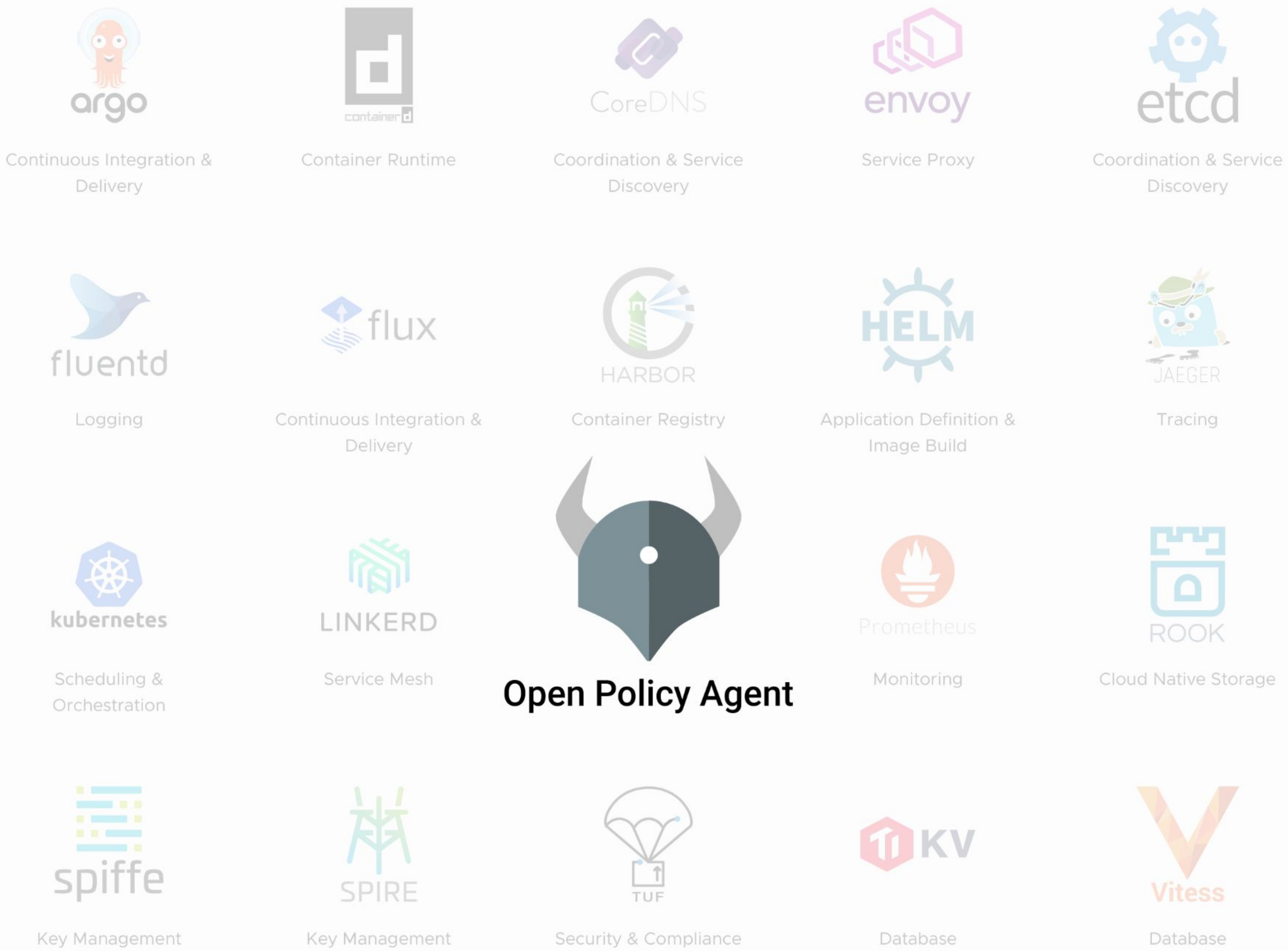
Charlie Egan, Styra, @charlieegan3
Rita Zhang, Microsoft, @ritazzhang

Agenda

- Introduction to Open Policy Agent
- OPA Project Updates & Upcoming Roadmap

- Introduction to Gatekeeper
- Gatekeeper Project Updates

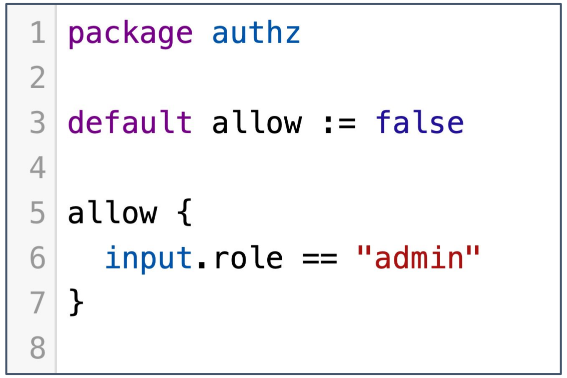
Open Policy Agent: Summary



argo	Continuous Integration & Delivery
containerd	Container Runtime
CoreDNS	Coordination & Service Discovery
envoy	Service Proxy
etcd	Coordination & Service Discovery
fluentd	Logging
flux	Continuous Integration & Delivery
HARBOR	Container Registry
HELM	Application Definition & Image Build
JAEGER	Tracing
kubernetes	Scheduling & Orchestration
LINKERD	Service Mesh
Open Policy Agent	
Prometheus	Monitoring
ROOK	Cloud Native Storage
spiffe	Key Management
SPIRE	Key Management
TUF	Security & Compliance
TiKV	Database
Vitess	Database

Open Policy Agent: Summary

Domain specific Policy Language (Rego)



```
package authz

default allow := false

allow {
  input.role == "admin"
}

```

+

Policy Server

APIs

- **Policy evaluation**
- **Policy Reloading**
- **Decision logging**

+

Language SDKs

Via Native SDK

GO

Via Wasm SDKs

JS

Java

python

.NET Core

+

Community Integrations

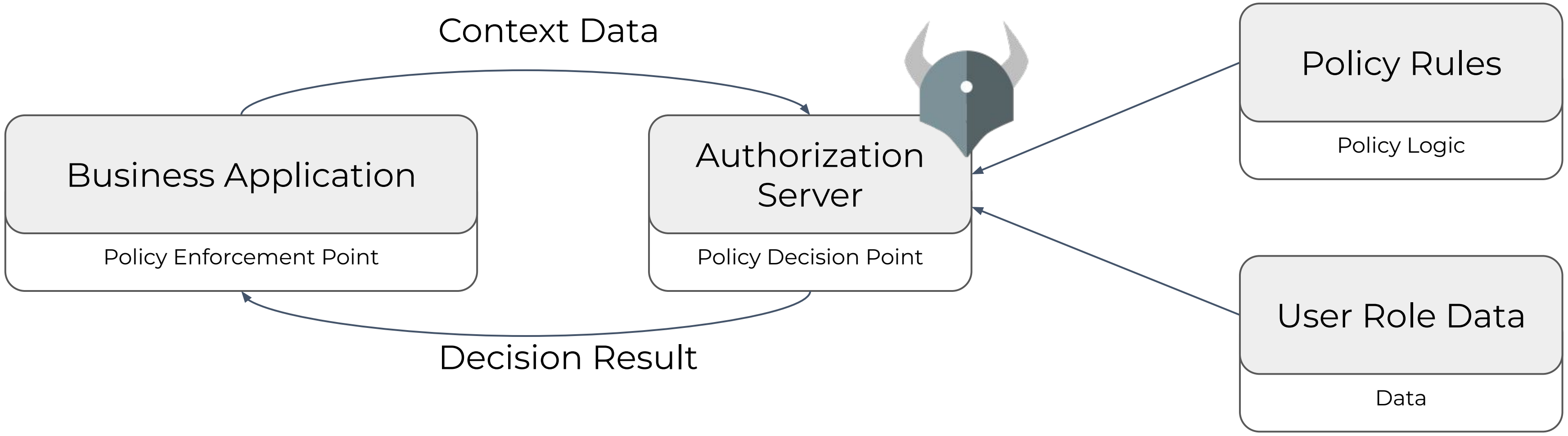
- **Gatekeeper**
- **conftest**

=

OPA!

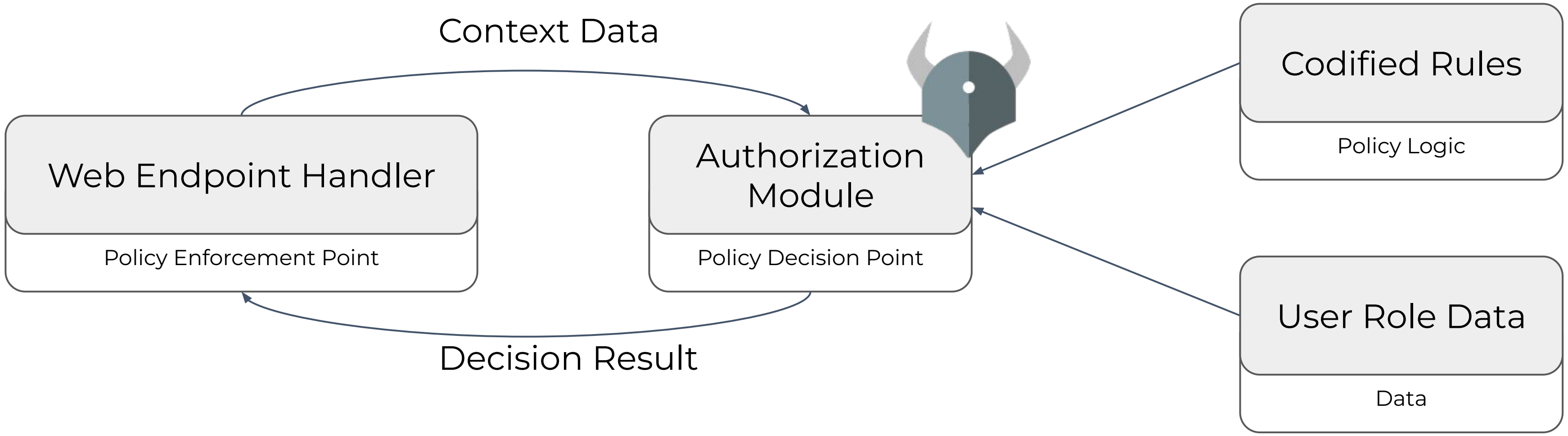
Open Policy Agent: Summary

As part of a **distributed system**



Open Policy Agent: Summary

Inside a **single application**



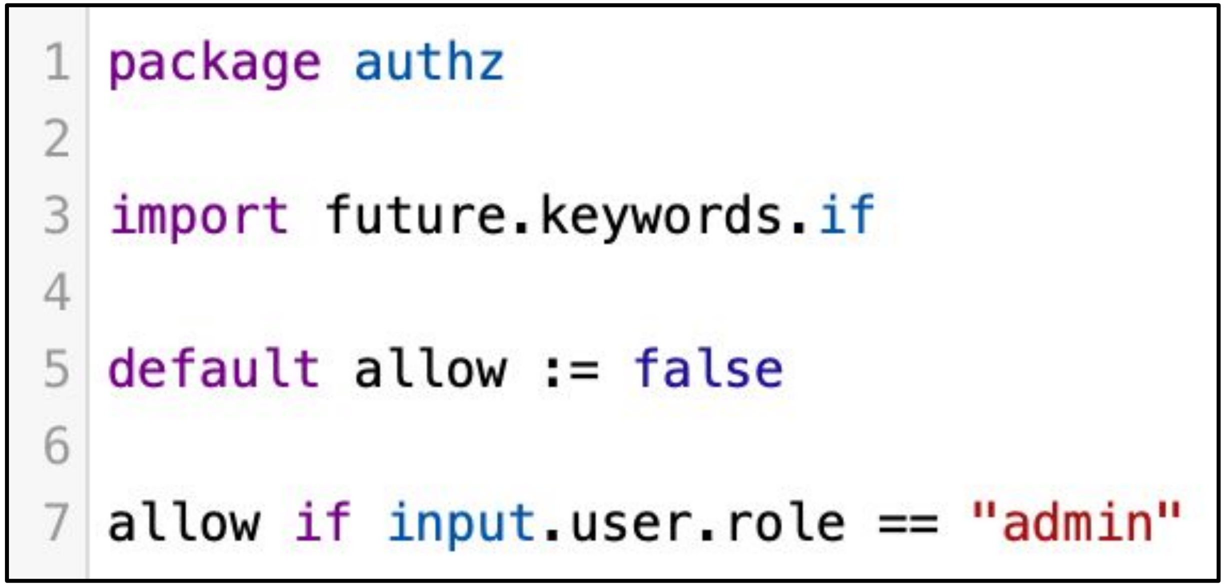
Open Policy Agent: Summary

Common *Policy Enforcement Points*

- Your application (via REST API, Go module or OPA CLI)
- Kubernetes API server (for k8s CRUD operations)
  - See Gatekeeper!
- CI/CD runs where IaC resources are being changed
  - See OPA confest!
- Envoy Proxy
  - See open-policy-agent/opa-envoy-plugin

Open Policy Agent: Summary

example.rego



```
package authz

import future.keywords.if

default allow := false

allow if input.user.role == "admin"
```

Input:

```
{
    "user": {
        "email": "alice@example.com",
        "role": "admin"
    }
}
```

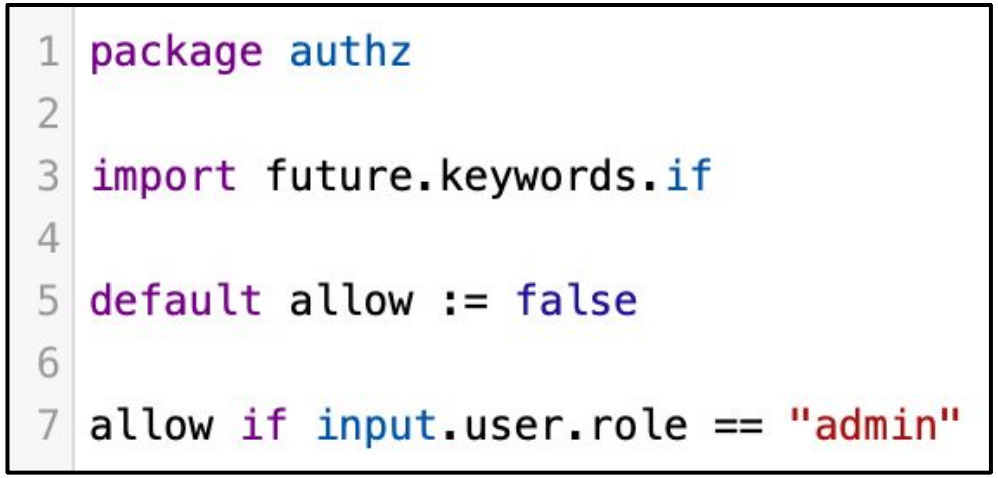
Open Policy Agent: Summary

Example Request:

```
POST /v0/data/authz/allow HTTP/1.1
Content-Type: application/json
{
    "user": {
        "email": "alice@example.com",
        "role": "admin"
    }
}
```

Example Response:

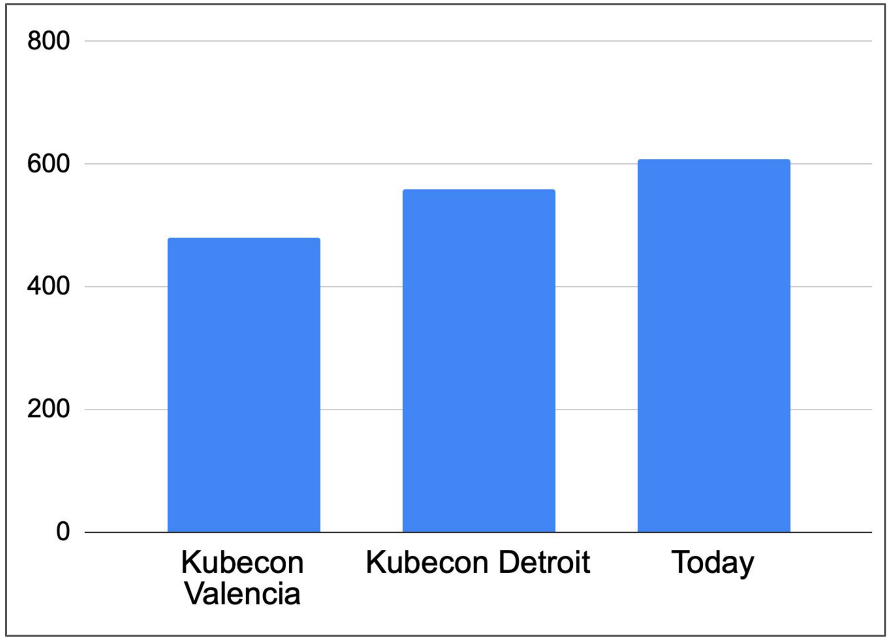
```
HTTP/1.1 200 OK
Content-Type: application/json
true
```



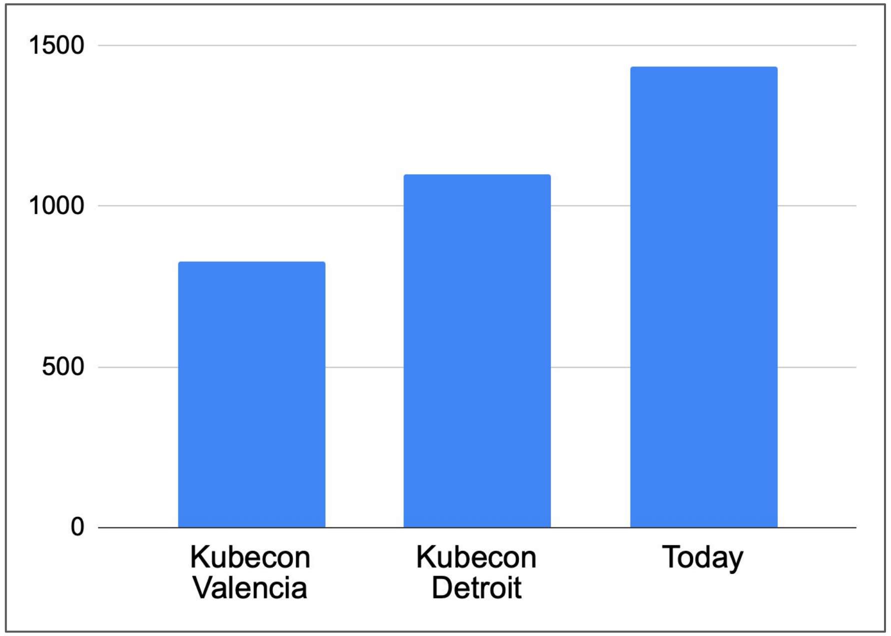
```
package authz

import future.keywords.if

default allow := false

allow if input.user.role == "admin"
```

Open Policy Agent: Community

Contributors from all OPA projects



Projects Using OPA as a Library



- 25 new integrations
- 6 new public corporate adopters
- Now over 7000 users registered in the OPA Slack

OPA Slack

Open Policy Agent: Project Updates

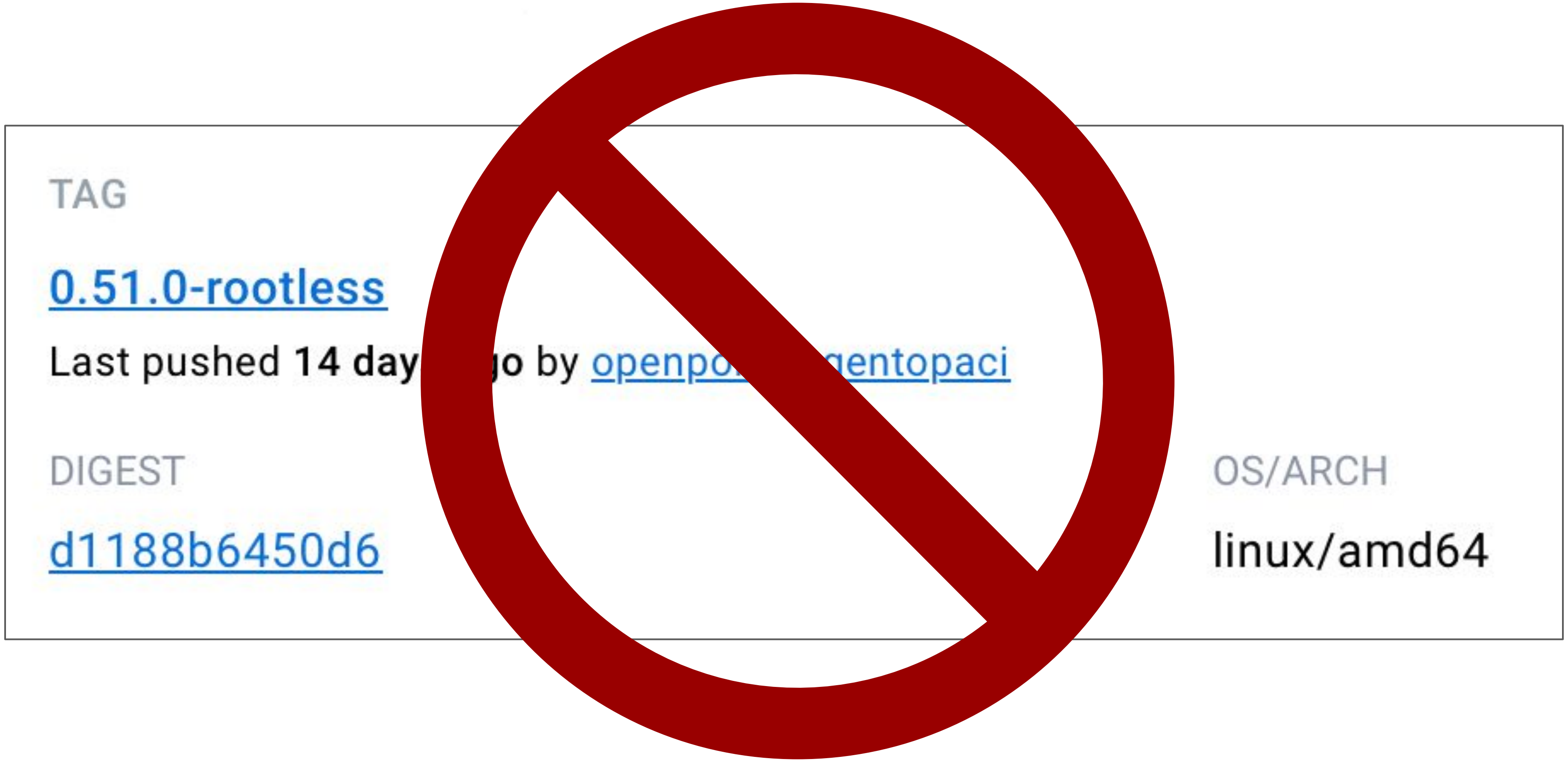
6 releases since the last KubeCon

- v0.46.1
- v0.47.0
- v0.48.0
- v0.49.0
- **v0.50.0**
- v0.51.0

OPA Slack

Open Policy Agent: Project Updates

PSA: All published OPA images now run with a non-root uid/gid



TAG

0.51.0-rootless

Last pushed 14 day go by openpo gentopaci

DIGEST	OS/ARCH
d1188b6450d6	linux/amd64

Please update your deployments to use the regular images

Open Policy Agent: Project Updates

- 255+ PRs merged since last KubeCon
- Rego Built-in Functions
  - **json.verify_schema & json.match_schema**
  - object.keys
  - time.format
  - graphql.schema_is_valid
  - net.cidr_is_valid
- **“Refs in rule heads”**

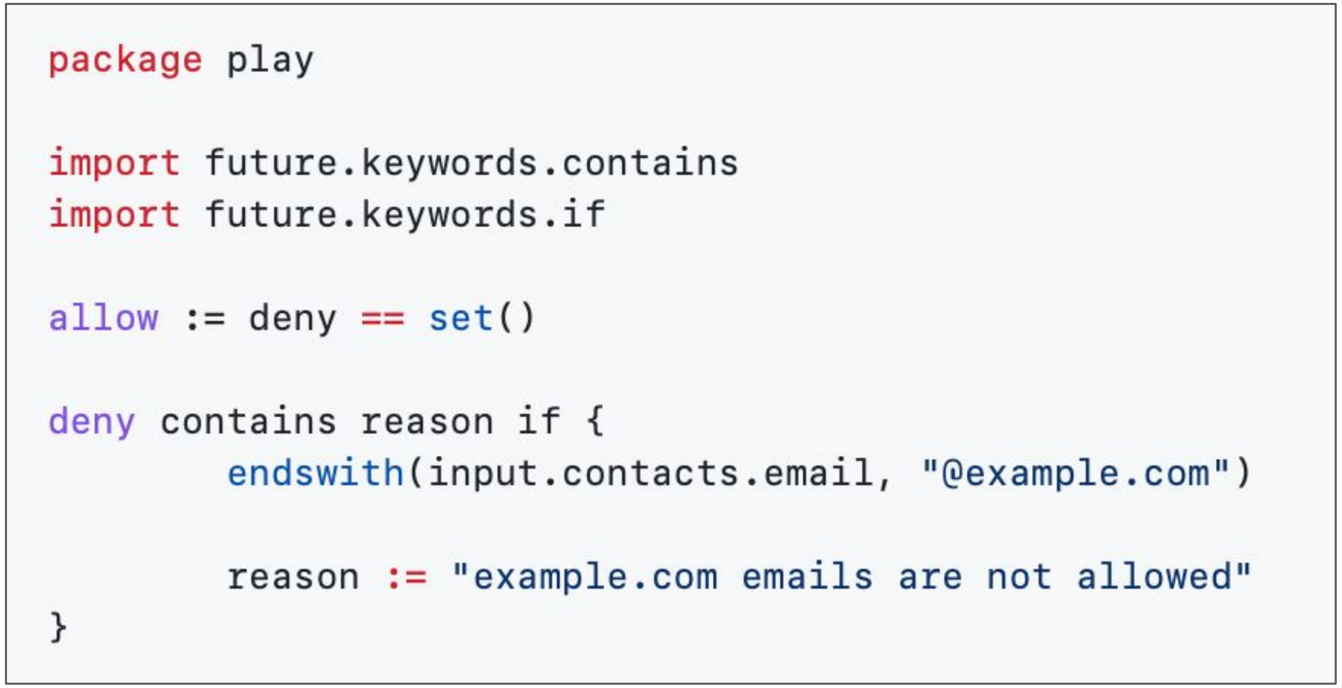
Open Policy Agent: Project Updates

- AWS Signature v4A Request Signing API (Multi Region)
- Drop decision logs based on policy
- Shorthand to load remote bundles via `opa run`:
  - Before: `opa run -s --set "services.default.url=https://example.com" \`
    ```
    --set "bundles.example.service=default" \
    --set "bundles.example.resource=/bundles/bundle.tar.gz" \
    --set "bundles.example.persist=true"
    ```
  - Now: `opa run -s https://example.com/bundles/bundle.tar.gz`
- OPA monitoring-related updates:
  - Surface unauthorized request count from OPA HTTP API authz handler via Status API
  - Surface decision log errors via Status API
- Lots of performance improvements under the hood

Open Policy Agent: JSON Schemas

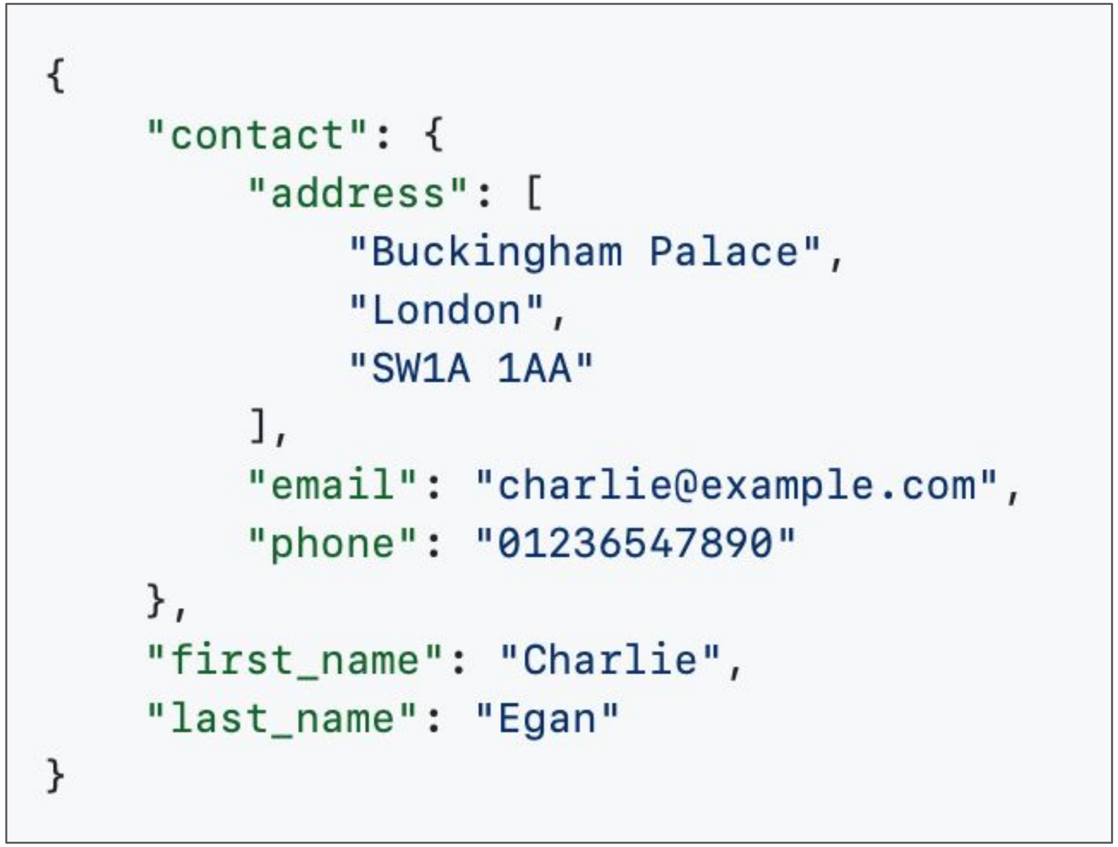
Can you spot the mistake?

Policy



```
package play

import future.keywords.contains
import future.keywords.if

allow := deny == set()

deny contains reason if {
        endswith(input.contacts.email, "@example.com")

        reason := "example.com emails are not allowed"
}
```

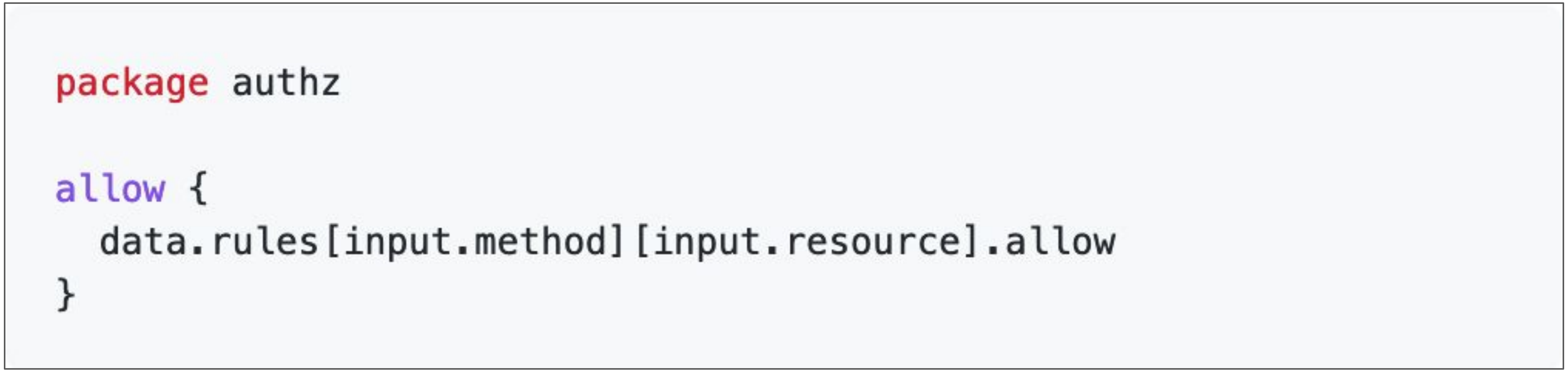
Input Data



```
{
    "contact": {
        "address": [
            "Buckingham Palace",
            "London",
            "SW1A 1AA"
        ],
        "email": "charlie@example.com",
        "phone": "01236547890"
    },
    "first_name": "Charlie",
    "last_name": "Egan"
}
```

- https://play.openpolicyagent.org/p/vEhmww673Z

Open Policy Agent: “Refs in rule heads”

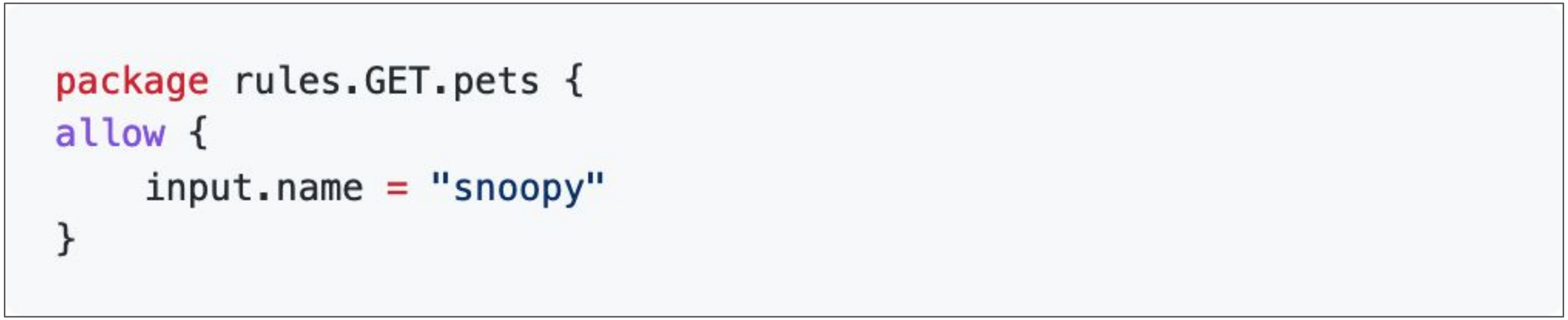


```
package authz

allow {
  data.rules[input.method][input.resource].allow
}
```

```
POST /v0/data/authz/allow HTTP/1.1
Content-Type: application/json
{
     "method": "GET",
     "resource": "pets",
     "user": "snoopy"
}
```

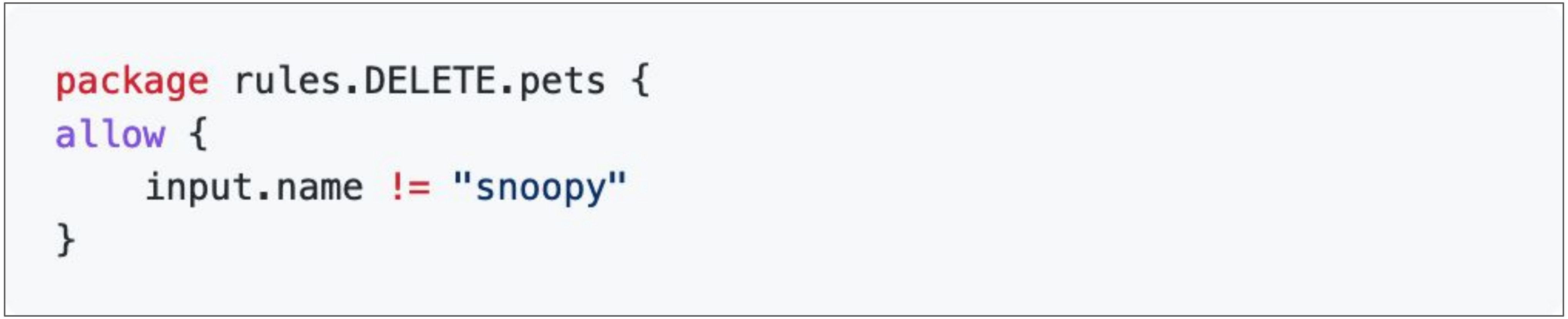
Open Policy Agent: “Refs in rule heads”

get_pets.rego



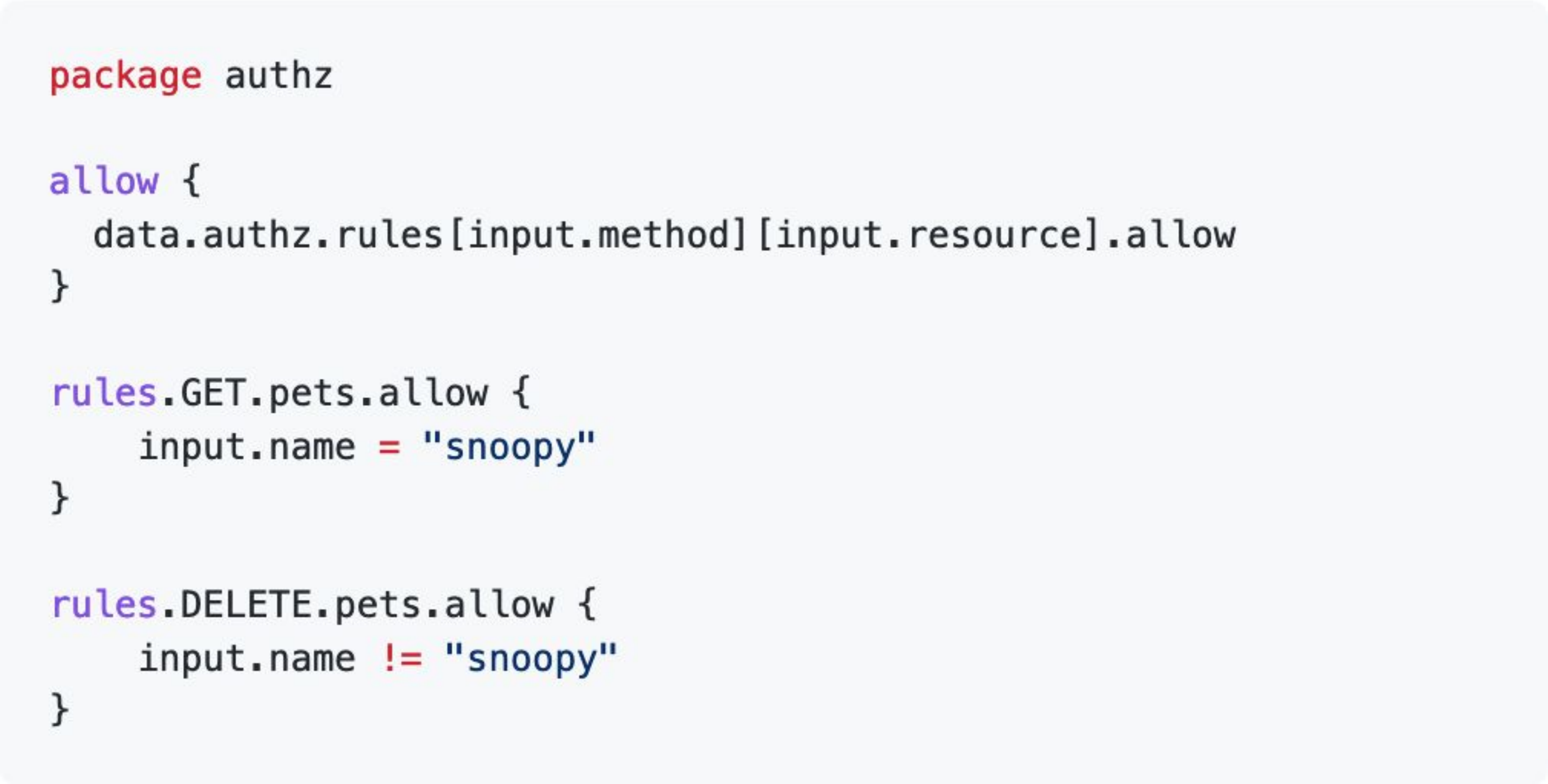
```
package rules.GET.pets {
allow {
    input.name = "snoopy"
}
```

delete_pets.rego



```
package rules.DELETE.pets {
allow {
    input.name != "snoopy"
}
```

Open Policy Agent: “Refs in rule heads”



```
package authz

allow {
  data.authz.rules[input.method][input.resource].allow
}

rules.GET.pets.allow {
     input.name = "snoopy"
}

rules.DELETE.pets.allow {
     input.name != "snoopy"
}
```

Open Policy Agent: Roadmap

2023 Q2

- Decision Log Perf Predictability
- **Ellipsis Operator**
- Authn plugins for OCI downloader
- Refs Heads with multiple vars
- Watch mode for OPA test command
- **Schema Validation for Input Data**
- Honor default keyword on functions

2023 Q3

- Optimize Flag on Tooling
- **Test Result Diffs**
- Undefined Handling
- Index Multiple Expressions
- Warn on unknown config options
- Relax config check w/ Discovery
- PGP sign verification built-ins
- *http.send* improvements

2023 Q4/2024 Q1

- Complexity Analysis
- Dependency Management
- Rule Tracing
- Loop Invariants
- Index membership checks

Find the roadmap link in the main README: https://github.com/open-policy-agent/opa#want-to-learn-more-about-opa

🟨 Performance

🟪 Distribution

🟩 Runtime

🟦 Language

🟥 Tooling

Issues labelled good first issue or help-wanted are good candidates for first contribution.

OPA Use-Case: Kubernetes Admission Webhook

Open Policy Agent Gatekeeper

Gatekeeper

A customizable Kubernetes admission webhook

that helps enforce policies and strengthen governance

Major updates since last KubeCon
since 3.11.x

Open Policy Agent Gatekeeper Motivations

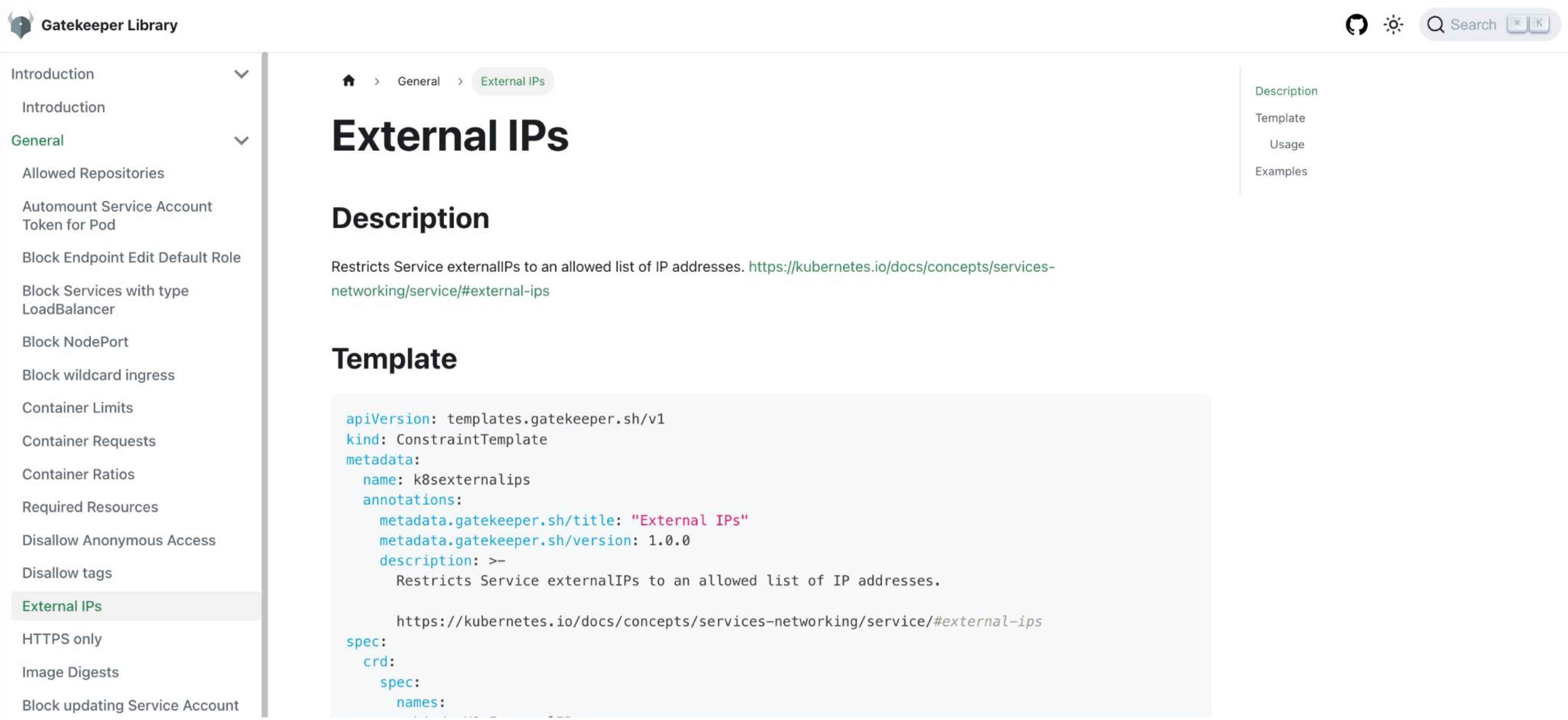
- Control what end-users can do on the cluster
- Help ensure clusters are in conformance with company policies
- Preview the effect of policy changes in production clusters to prevent impacts on existing workloads

How do we help ensure conformance without sacrificing agility and autonomy?

- Policy as code
- Validating admission webhook
- Mutating admission webhook
- Audit
- Gator CLI for shift left
- External Data
- Community policy library

Community Policy Library

https://open-policy-agent.github.io/gatekeeper-library/website/ &
https://artifacthub.io/packages/search?org=gatekeeper



- Introduction
  - Introduction
- General
  - Allowed Repositories
  - Automount Service Account Token for Pod
  - Block Endpoint Edit Default Role
  - Block Services with type LoadBalancer
  - Block NodePort
  - Block wildcard ingress
  - Container Limits
  - Container Requests
  - Container Ratios
  - Required Resources
  - Disallow Anonymous Access
  - Disallow tags
  - External IPs
  - HTTPS only
  - Image Digests
  - Block updating Service Account

External IPs

Description

Restricts Service externalIPs to an allowed list of IP addresses. https://kubernetes.io/docs/concepts/services-networking/service/#external-ips

Template

```
apiVersion: templates.gatekeeper.sh/v1
kind: ConstraintTemplate
metadata:
  name: k8sexternalips
  annotations:
    metadata.gatekeeper.sh/title: "External IPs"
    metadata.gatekeeper.sh/version: 1.0.0
    description: >-
      Restricts Service externalIPs to an allowed list of IP addresses.

      https://kubernetes.io/docs/concepts/services-networking/service/#external-ips
spec:
  crd:
    spec:
      names:
```

CVE-2020-8554: Man in the middle using LoadBalancer or ExternalIPs

Gatekeeper: Project Updates

2 releases since the last KubeCon

- v3.11
- **v3.12**

Updates

Features

- External data is promoted to beta; TLS/mTLS is now required to communicate with external data providers
- Gator CLI is promoted to beta, now supports trace, AdmissionReview and specifying an OCI artifact
- **New AssignImage mutator to enable replacement of image registry or tag**
- **Added Multi-engine support to allow integration with k8s CEL ValidatingAdmissionPolicy in the future**
- Emit violation events in the involved/violating objects namespace
- Enable exempt namespace suffix
- Expanded resources now have generated mock names
- Constraint annotations and resource labels are available in logs

New Alpha Feature: AssignImage Demo

```
apiVersion:
mutations.gatekeeper.sh/v1alpha1
kind: AssignImage
metadata:
 name: assign-container-image-registry
spec:
 applyTo:
 - groups: [ "" ]
   kinds: [ "Pod" ]
   versions: [ "v1" ]
 location: "spec.containers[name:*].image"
 parameters:
   assignDomain: "mycompany.registry.io"
 match:
   source: "All"
   scope: Namespaced
   kinds:
   - apiGroups: [ "*" ]
     kinds: [ "Pod" ]
```

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx
spec:
 containers:
 - name: nginx
   image: nginx
   imagePullPolicy:
IfNotPresent
```

```
$ kubectl apply -f
pod/nginx created
…
 - image: mycompany.registry.io/nginx
```

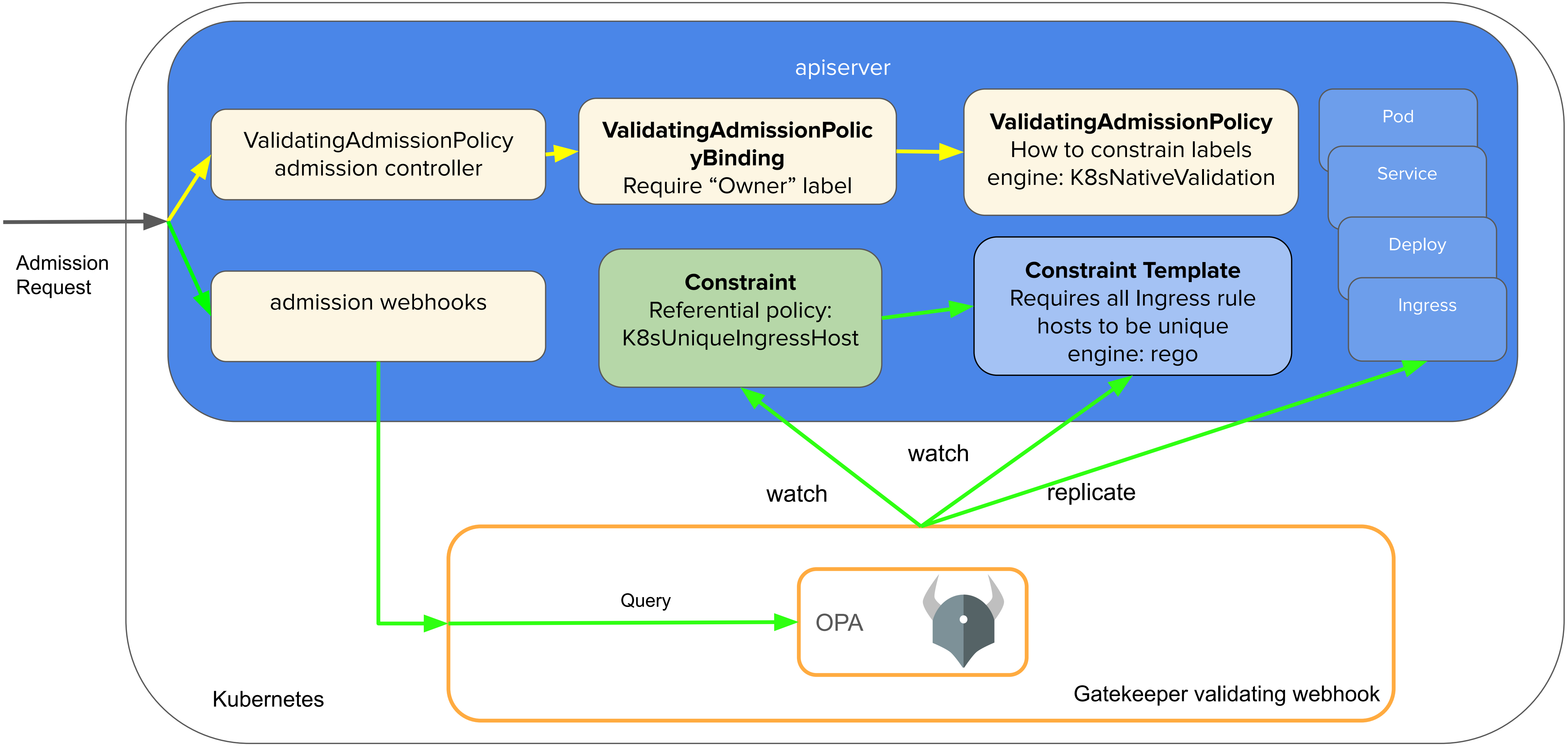
Motivations for Multi-engine support

- K8s v1.26, alpha feature ValidatingAdmissionPolicy (based on CEL), a declarative, in-process alternative to validating admission webhooks
- When to use what?
  - ValidatingAdmissionPolicy
    - in-tree/native in-process
    - reduce admission request latency
    - improve reliability and availability
    - able to fail closed without impacting availability
    - reduce operation burdens of webhooks
    - language: CEL
  - Gatekeeper
    - Audit
    - Referential policies
    - External data
    - Mutation
    - Shift left validation using Gator CLI
    - Complex rules that CEL cannot handle
    - Community policy library
    - multi-engine: OPA and more
    - multi-language: Rego and more
- **Is there a way to get best of both worlds?**

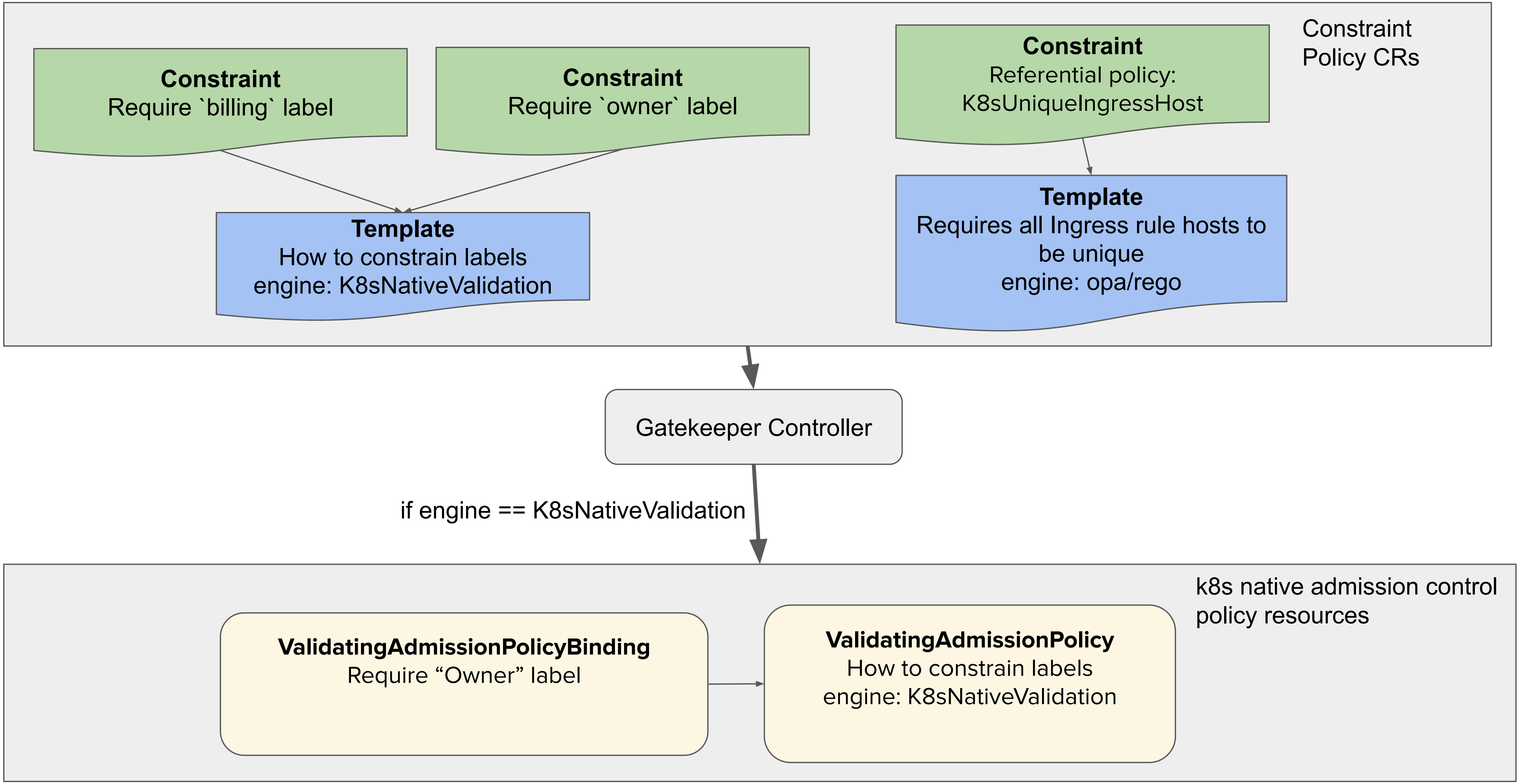
Coexistence: Multi-engine support (WIP)

- Need an abstraction layer to simplify the user experience, allowing users to write policy in the language they are familiar with ⇒ Constraint Framework
  - multi-language, multi-target policy enforcement
    - languages: rego, CEL
    - targets: kubernetes admission, terraform
  - portable policies and coexistence of numerous policy implementations
  - the core constraint template and constraint functionality for Gatekeeper today
- Added multiple engines support in Constraint Framework to enable more engines in addition to OPA
- **Together with Gatekeeper and gator CLI, we get audit and shift left validations for *ValidatingAdmissionPolicy* for free**
- e.g.
  - Kubernetes *ValidatingAdmissionPolicy* based on CEL [issue #2682]
  - Starlark [issue #2618]

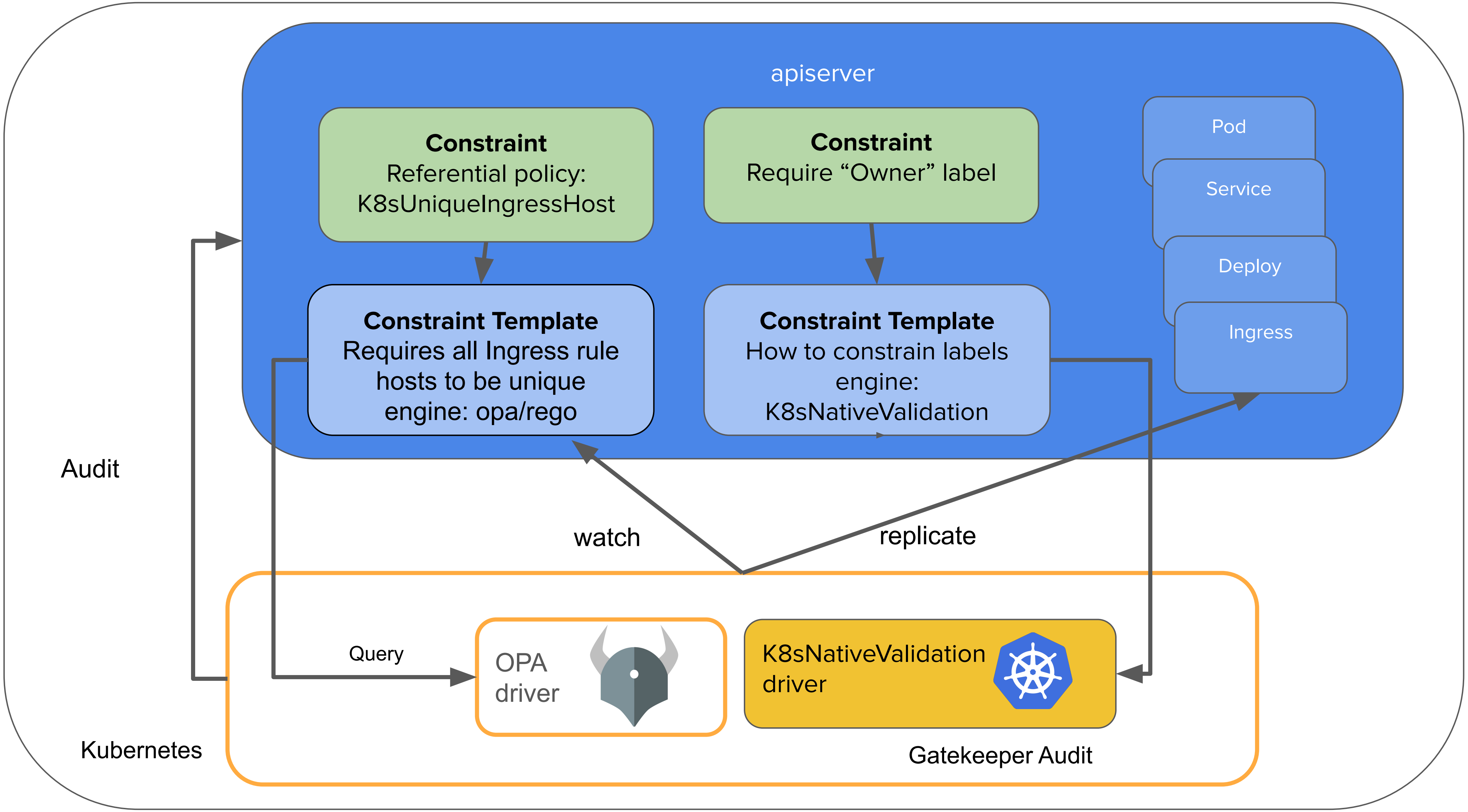
Multi Engine Validating Admission Policies


apiserver
ValidatingAdmissionPolicy admission controller
ValidatingAdmissionPolicyBinding
Require “Owner” label
ValidatingAdmissionPolicy
How to constrain labels
engine: K8sNativeValidation
Pod
Service
Deploy
Ingress
Admission Request
admission webhooks
Constraint
Referential policy: K8sUniqueIngressHost
Constraint Template
Requires all Ingress rule hosts to be unique
engine: rego
watch
watch
replicate
Query
OPA
Kubernetes
Gatekeeper validating webhook

Future: Gatekeeper - A Front End for K8s Policies



Multi Engine Audit Policies



Gatekeeper Multi-engine: What’s next?

- Adopt K8sNativeValidation policies with minimal changes
- Bring K8sNativeValidation to audit (Gatekeeper), shift left (gator CLI)
- Update GK-library to support K8sNativeValidation based policies
- Support K8sNativeValidation based policies for older k8s versions
- gator support for raw K8sNativeValidation based rules and K8sNativeValidation based Constraint Template
- More engines!

Open Policy Agent

Thank YOU Contributors!

Join Us!

Open Policy Agent

openpolicyagent.org
github.com/open-policy-agent/opa

OPA Gatekeeper

github.com/open-policy-agent/gatekeeper

Community

slack.openpolicyagent.org

Open Policy Agent

Questions?

Sponsor Shout-Out!

Thank you to our Session Recording Sponsor:

KubeCon | CloudNativeCon

Europe 2023

Enjoy the Session!