Open Policy Agent (OPA)

Unified Cloud-native Policy Control

Hi, I'm Ash

Software Engineer @ styra

Maintainer @

> "I care about developing software that can be readily deployed, scaled, managed and is secure by-default."

Hi, I'm Oren

Software Engineer @ VMware
Maintainer @

> “ Making accessible software to solve real-world problems ”

openpolicyagent.org

Agenda

- Overview
    - Community
    - What is OPA ?
    - OPA Roadmap
    - Subproject Updates
        - Conftest
        - Gatekeeper

OPA: Community

Inception

Project started in 2016 at Styra.

Goal

Unify policy enforcement across the stack.

Users

Netflix
Medallia
Chef
Cloudflare
Pinterest
Intuit
Capital One
...and many more.

Use Cases

- Admission control
- Authorization
  - ACLs
  - RBAC
  - IAM
  - ABAC
- Risk management
- Data Protection
- Data Filtering

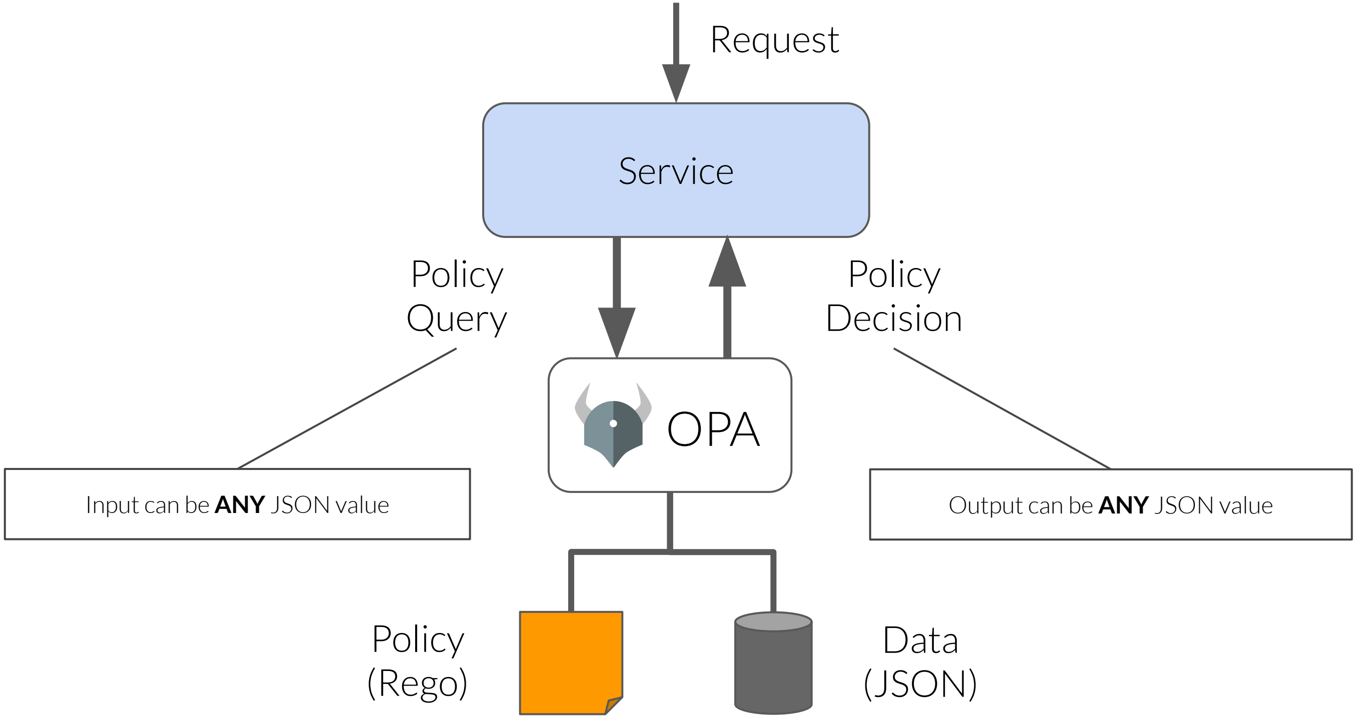
Today

CNCF project (Graduated)

100+ contributors
3000+ slack members
4500+ stars
20+ integrations

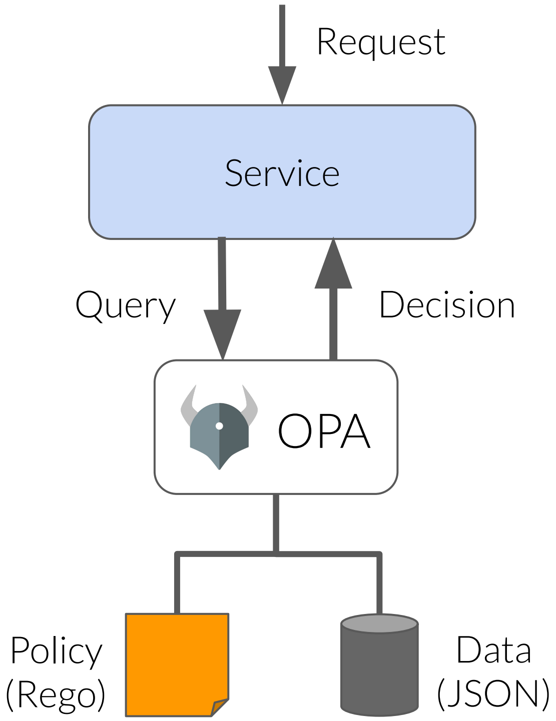
What Is OPA?

OPA: General-purpose policy engine



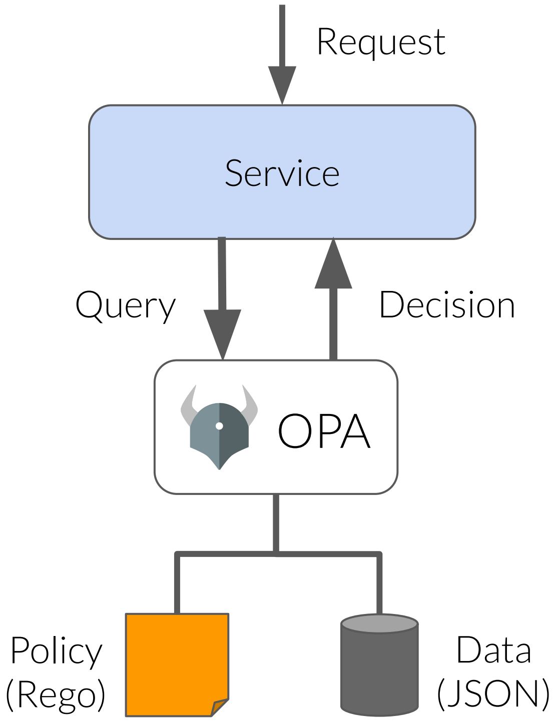
OPA: Features

- Declarative Policy Language (Rego)
- Library (Go), sidecar/host-level daemon, WASM
- Management APIs for control & visibility
- Tooling to build, test, and debug policies



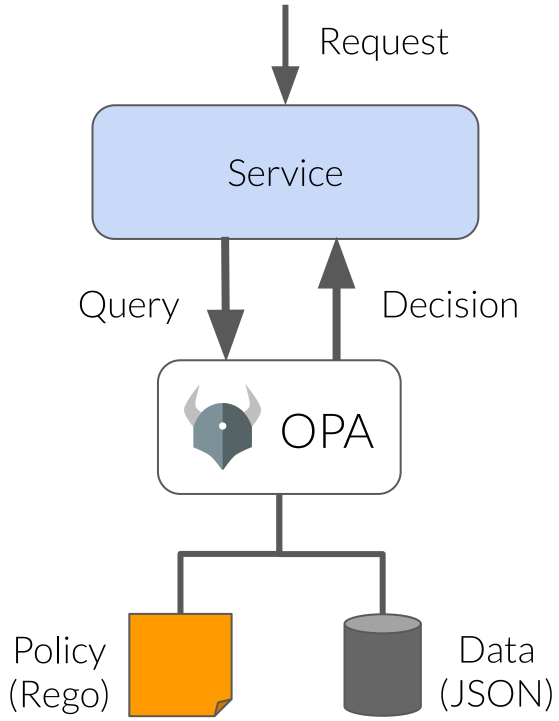
OPA: Features

- Declarative Policy Language (Rego)
- Library (Go), sidecar/host-level daemon, WASM
- Management APIs for control & visibility
- Tooling to build, test, and debug policies



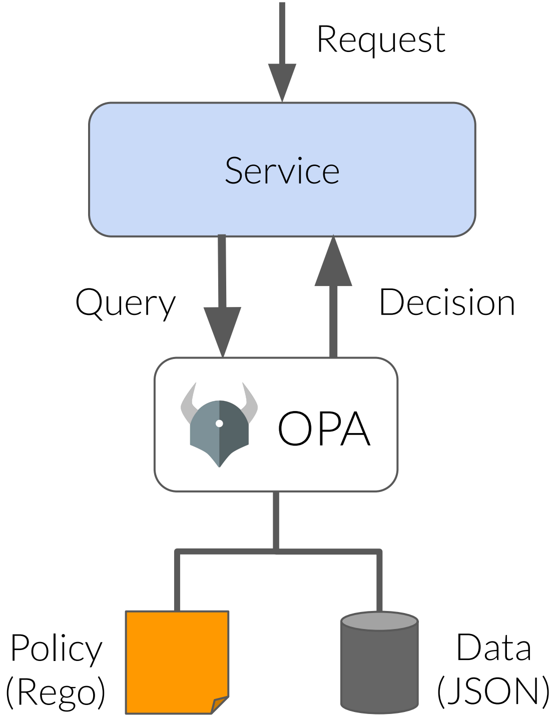
OPA: Features

- Declarative Policy Language (Rego)
- Library (Go), sidecar/host-level daemon, WASM
- Management APIs for control & visibility
- Tooling to build, test, and debug policies



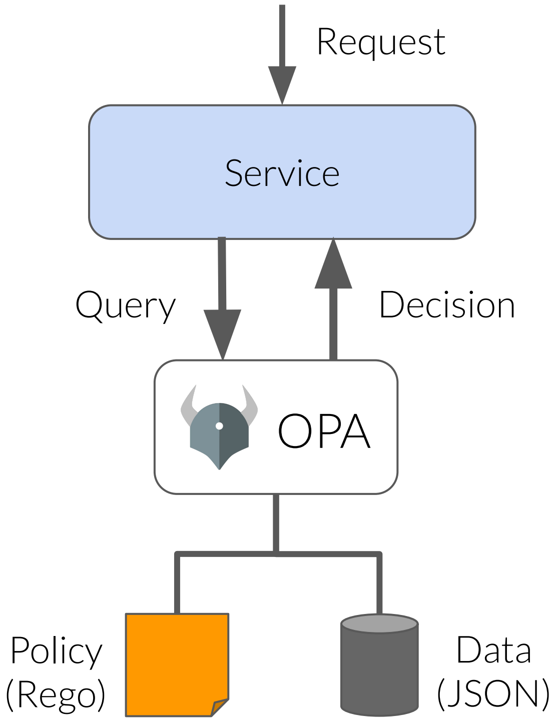
OPA: Features

- Declarative Policy Language (Rego)
- Library (Go), sidecar/host-level daemon, WASM
- Management APIs for control & visibility
- Tooling to build, test, and debug policies

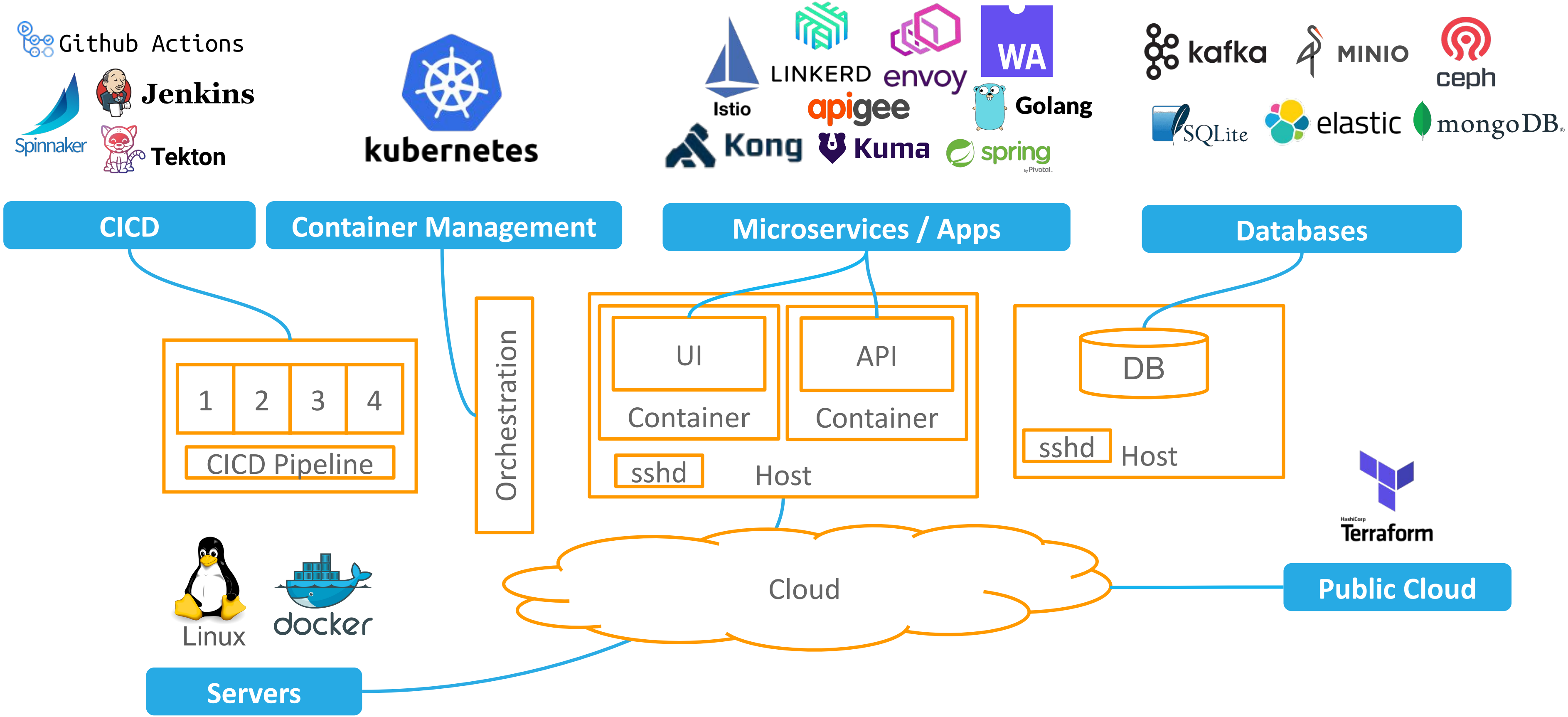


OPA: Features

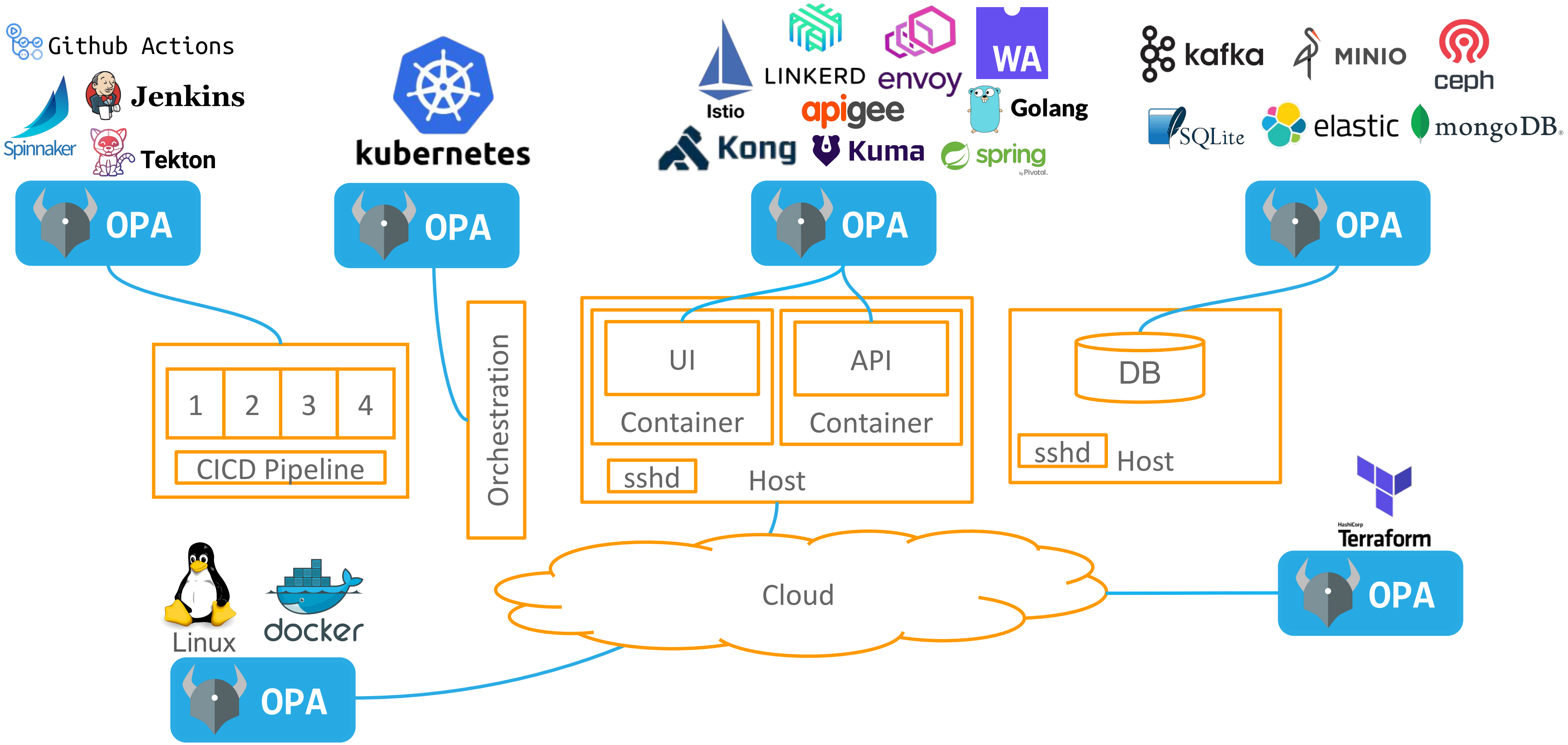
- Declarative Policy Language (Rego)
- Library (Go), sidecar/host-level daemon, WASM
- Management APIs for control & visibility
- Tooling to build, test, and debug policies



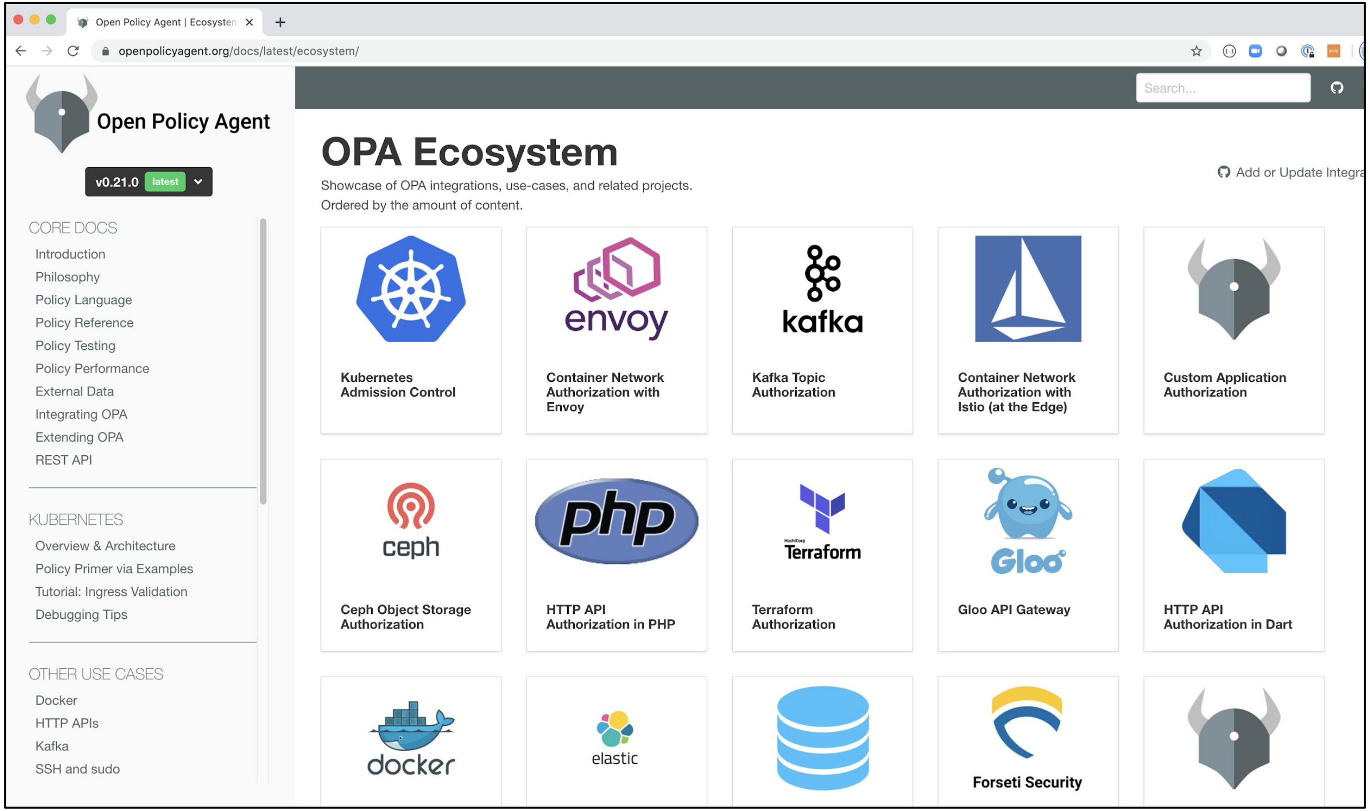
Cloud-Native Diversity



OPA: Unified Authorization for Cloud-Native



OPA: Integration Index



Open Policy Agent | Ecosystem

openpolicyagent.org/docs/latest/ecosystem/

Search...

Open Policy Agent

v0.21.0 latest

CORE DOCS

- Introduction
- Philosophy
- Policy Language
- Policy Reference
- Policy Testing
- Policy Performance
- External Data
- Integrating OPA
- Extending OPA
- REST API

KUBERNETES

- Overview & Architecture
- Policy Primer via Examples
- Tutorial: Ingress Validation
- Debugging Tips

OTHER USE CASES

- Docker
- HTTP APIs
- Kafka
- SSH and sudo

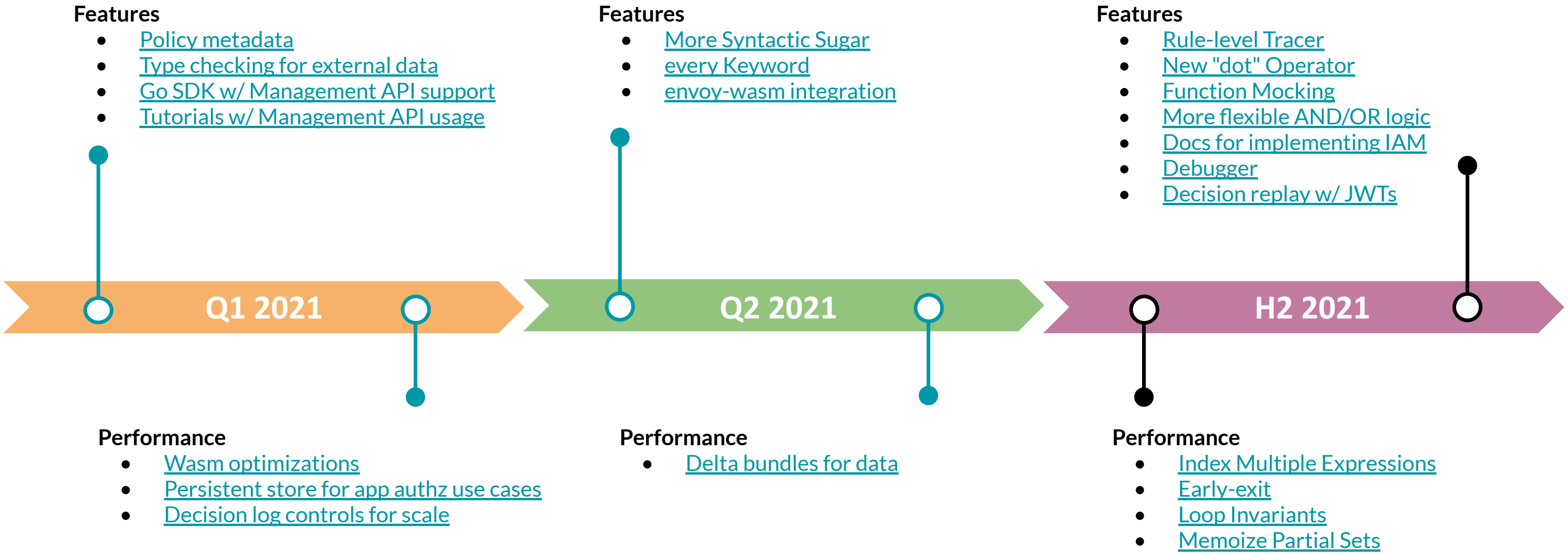
OPA Ecosystem

Add or Update Integra

Showcase of OPA integrations, use-cases, and related projects.
Ordered by the amount of content.

- Kubernetes Admission Control
- Container Network Authorization with Envoy
- Kafka Topic Authorization
- Container Network Authorization with Istio (at the Edge)
- Custom Application Authorization
- Ceph Object Storage Authorization
- HTTP API Authorization in PHP
- Terraform Authorization
- Gloo API Gateway
- HTTP API Authorization in Dart

OPA: Roadmap



Features

- Policy metadata
- Type checking for external data
- Go SDK w/ Management API support
- Tutorials w/ Management API usage

Performance

- Wasm optimizations
- Persistent store for app authz use cases
- Decision log controls for scale

Features

- More Syntactic Sugar
- every Keyword
- envoy-wasm integration

Performance

- Delta bundles for data

Features

- Rule-level Tracer
- New "dot" Operator
- Function Mocking
- More flexible AND/OR logic
- Docs for implementing IAM
- Debugger
- Decision replay w/ JWTs

Performance

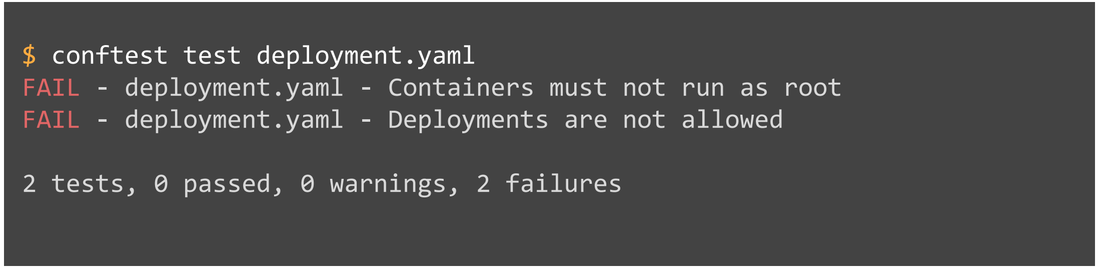
- Index Multiple Expressions
- Early-exit
- Loop Invariants
- Memoize Partial Sets

Subproject Updates

Conftest

Conftest uses OPA to provide a user experience optimised for developers wanting to test all kinds of configuration files.

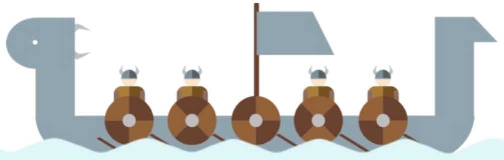
www.conftest.dev



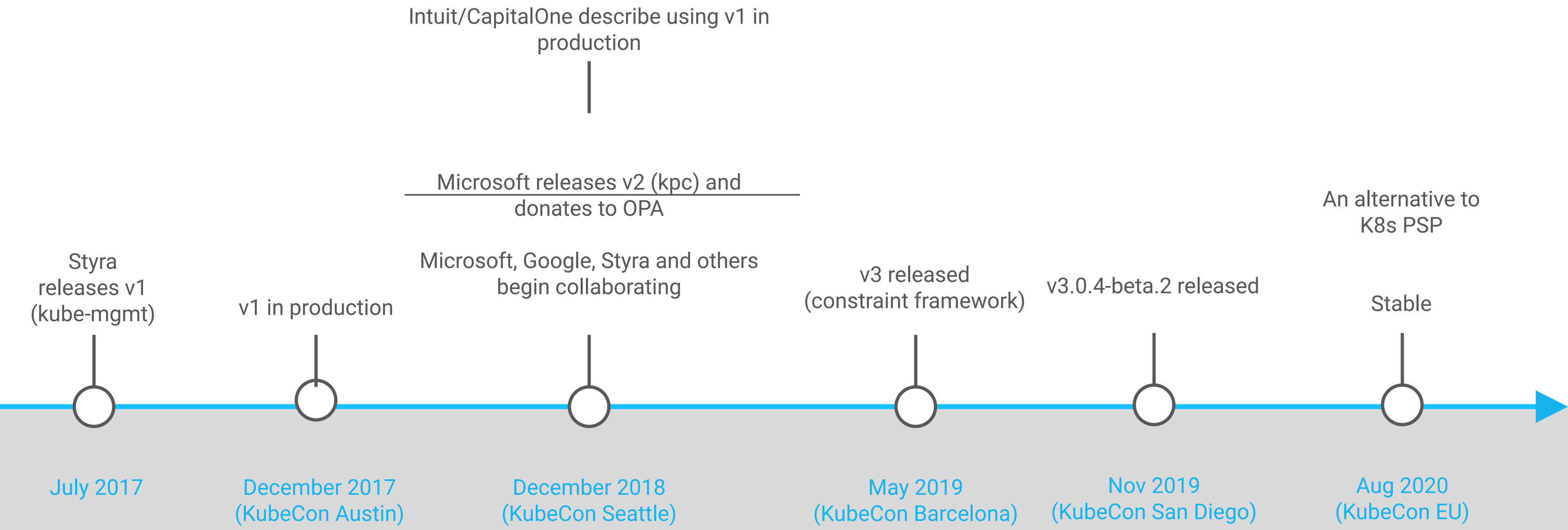
```
$ conftest test deployment.yaml
FAIL - deployment.yaml - Containers must not run as root
FAIL - deployment.yaml - Deployments are not allowed

2 tests, 0 passed, 0 warnings, 2 failures
```

- Supports XDG specification for plugins
- Official Conftest Docker images now available at *openpolicyagent/conftest*
- Coming Soon ! Make available the configuration file folder name and structure to the policy

Gatekeeper



Gatekeeper: How We Got Here



Styra releases v1 (kube-mgmt)

July 2017

v1 in production

December 2017 (KubeCon Austin)

Intuit/CapitalOne describe using v1 in production

Microsoft releases v2 (kpc) and donates to OPA

Microsoft, Google, Styra and others begin collaborating

December 2018 (KubeCon Seattle)

v3 released (constraint framework)

May 2019 (KubeCon Barcelona)

v3.0.4-beta.2 released

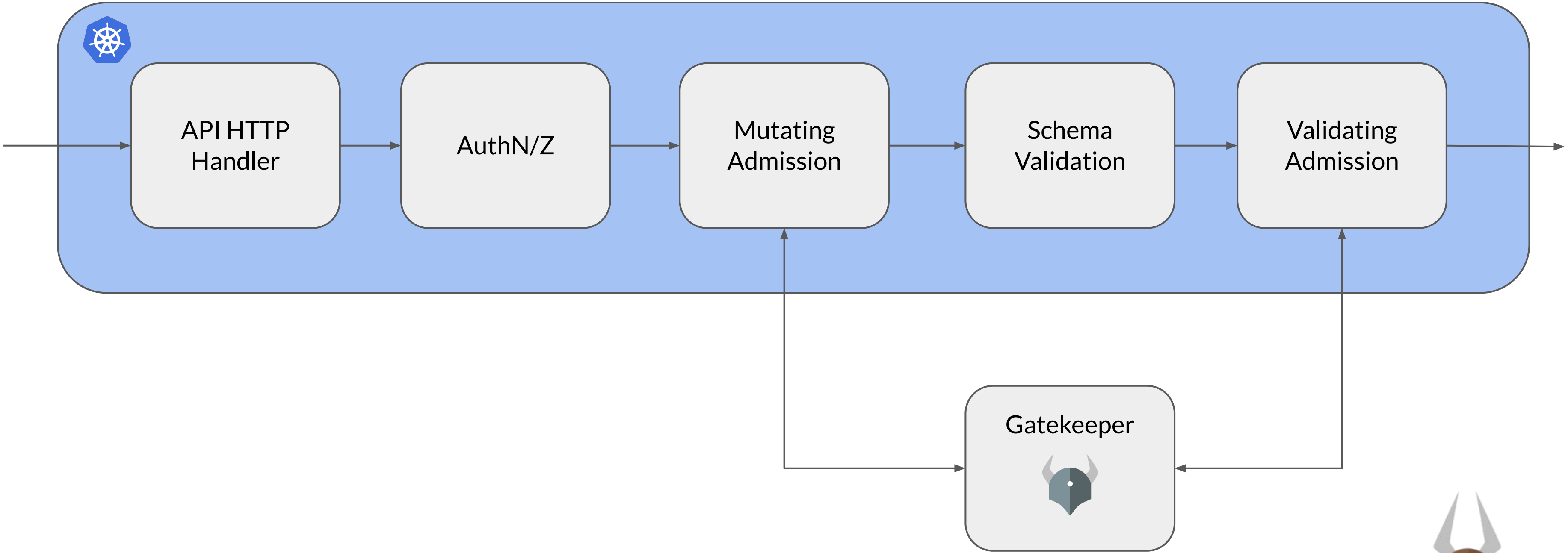
Nov 2019 (KubeCon San Diego)

An alternative to K8s PSP

Stable

Aug 2020 (KubeCon EU)

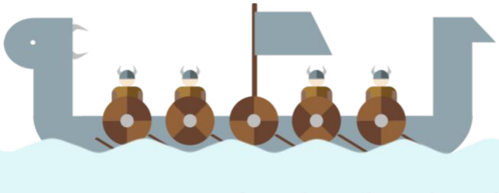
Admission Request Flow



Gatekeeper: Core Features

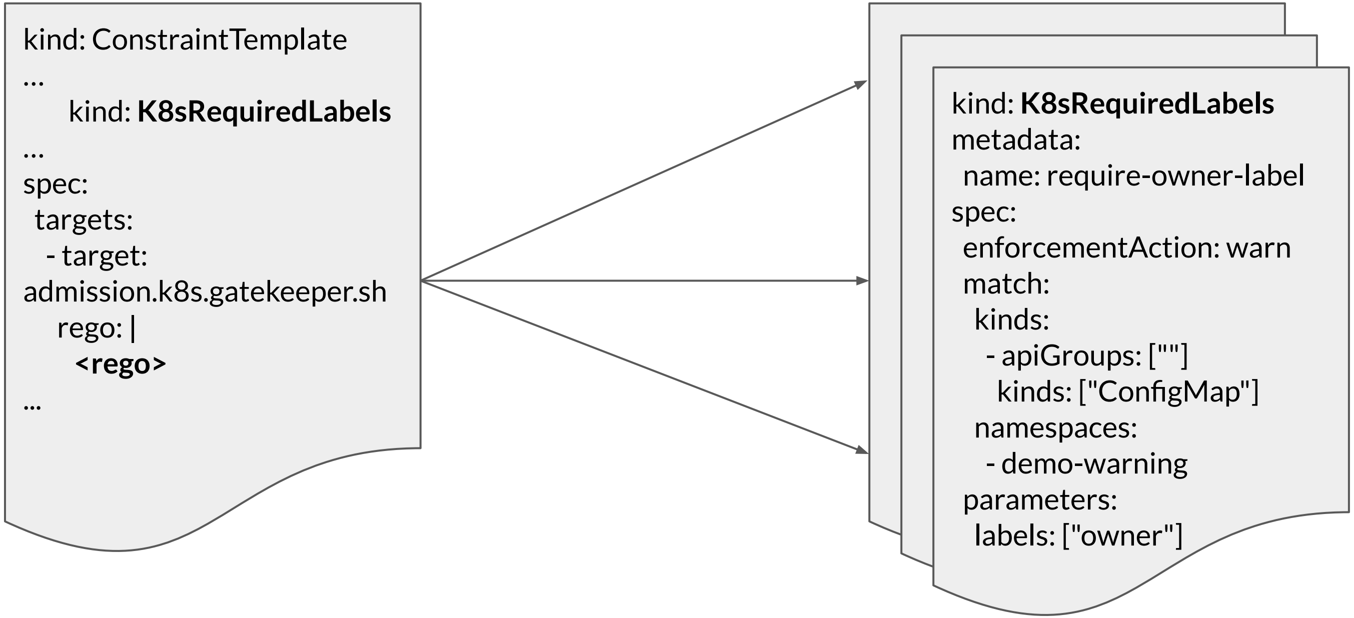
Photo by Judith Prins on Unsplash

- Validating admission control
  - Control what end-users can do on the cluster
- Context-aware/referential policies
- Write policies via configuration, not code.
  - ConstraintTemplates - source code for rego rules and schema for Constraints and their parameters
    - Testable
    - Developed internally or sourced from the community, easily shared
  - Constraints are parameterized and easily configurable by admins
- Audit
  - Periodically evaluates resources against constraints
  - Allows for ongoing monitoring of cluster state to aid in detection and remediation of pre-existing misconfigurations
- Dry run
    - Gain confidence in new policies before enforcing them; gradual rollout



Constraint Framework

Policy reuse, made easy



```
kind: ConstraintTemplate
…
    kind: K8sRequiredLabels
…
spec:
 targets:
  - target:
admission.k8s.gatekeeper.sh
   rego: |
    <rego>
…
```

```
kind: K8sRequiredLabels
metadata:
 name: require-owner-label
spec:
 enforcementAction: warn
 match:
  kinds:
   - apiGroups: [""]
    kinds: ["ConfigMap"]
  namespaces:
   - demo-warning
 parameters:
  labels: ["owner"]
```

Alpha Feature: Mutation

- Mechanism for modifying inbound requests
  - Apply secure defaults
  - Resolve ambiguous settings
  - Enhance functionality / sidecar injection
  - Tag resources with metadata

Project Updates

- Alpha mutation support
- Gatekeeper Operator - under development!
- Constraints support warning enforcement mode [k8s 1.19+]
- Improved documentation
- Reduced memory consumption
- Cache warming improvements
- Constraint library refactoring
- ...and much much more!

Demo

What’s next?

- Mutation -> Stable
- External Data Providers -> Alpha
- Tooling
- Refine metrics
- More policies
- World domination?

Thanks!

Open Policy Agent	openpolicyagent.org
Conftest	conftest.dev
Gatekeeper	open-policy-agent.github.io/gatekeeper/website/docs
	slack.openpolicyagent.org
	github.com/open-policy-agent