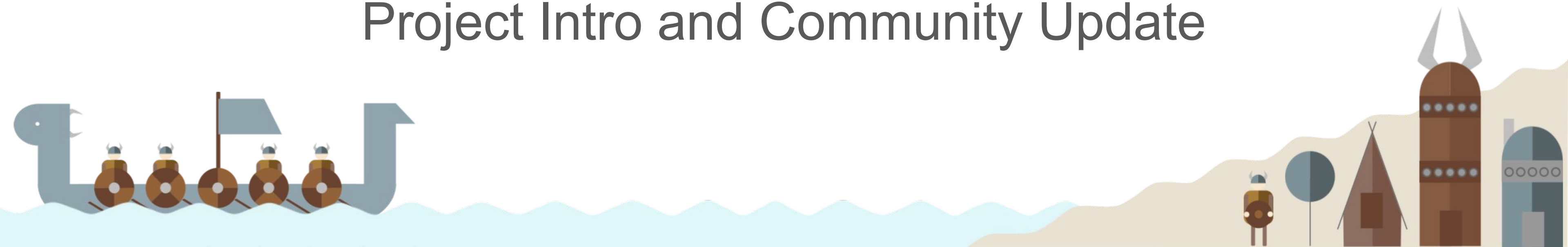
Open Policy Agent

Policy-based control for cloud native environments.

Project Intro and Community Update



Rita Zhang

Engineer at Microsoft
Gatekeeper Maintainer

Rita Zhang on OPA slack

@ritazzhang

Patrick East

Engineer at Styra
OPA Maintainer

Patrick East on OPA slack

@peast907

OPA: Community

Inception

Project started in 2016 at Styra.

Goal

Unify policy enforcement across the stack.

Users

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

Use Cases

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

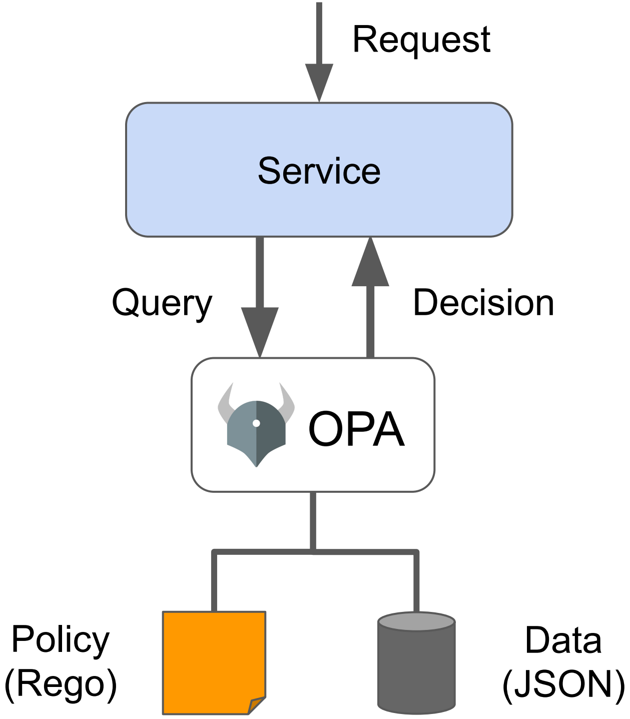
Today

CNCF project (Incubating)

>70 contributors
>1000 slack members
>2K stars
>20 integrations

OPA: What is it?

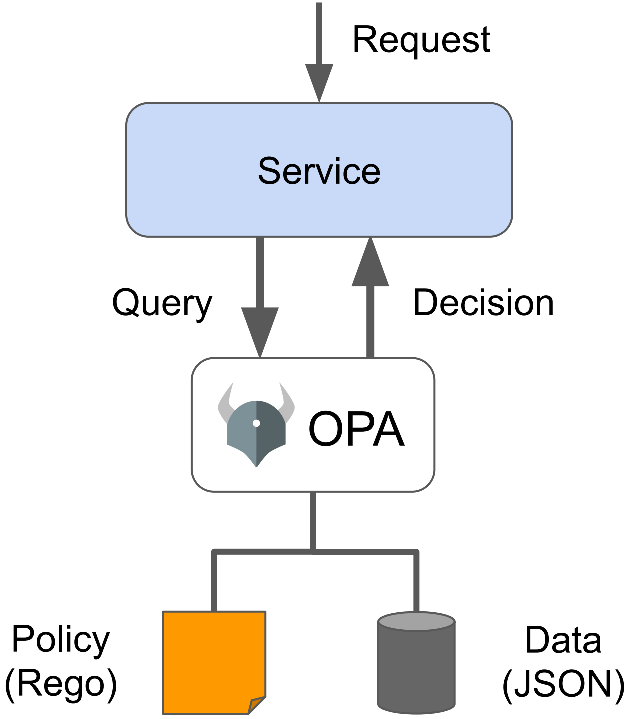
- **Declarative Policy Language (Rego)**
  - ○ Can user X do operation Y on resource Z?
  - ○ What invariants does workload W violate?
  - ○ Which records should bob be allowed to see?



openpolicyagent.org

OPA: What is it?

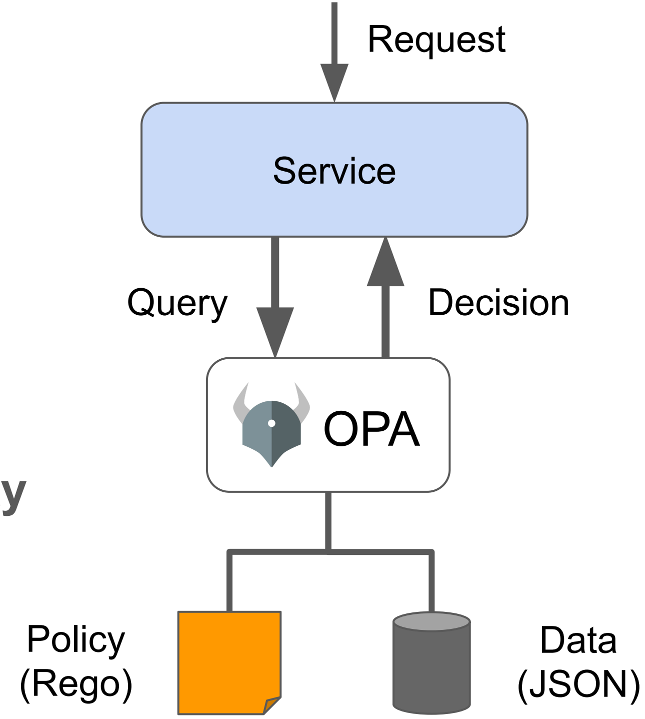
- **Declarative Policy Language (Rego)**
  - Can user X do operation Y on resource Z?
  - What invariants does workload W violate?
  - Which records should bob be allowed to see?
- **Library (Go), sidecar/host-level daemon**
  - Policy and data are kept in-memory
  - Zero decision-time dependencies



openpolicyagent.org

OPA: What is it?

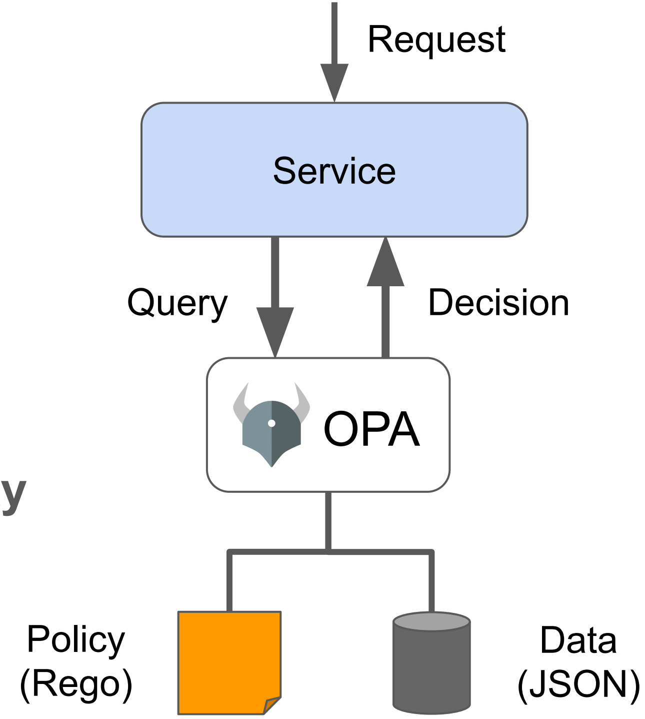
- **Declarative Policy Language (Rego)**
  - Can user X do operation Y on resource Z?
  - What invariants does workload W violate?
  - Which records should bob be allowed to see?
- **Library (Go), sidecar/host-level daemon**
  - Policy and data are kept in-memory
  - Zero decision-time dependencies
- **Management APIs for control & observability**
  - Bundle service API for sending policy & data to OPA
  - Status service API for receiving status from OPA
  - Log service API for receiving audit log from OPA



openpolicyagent.org

OPA: What is it?

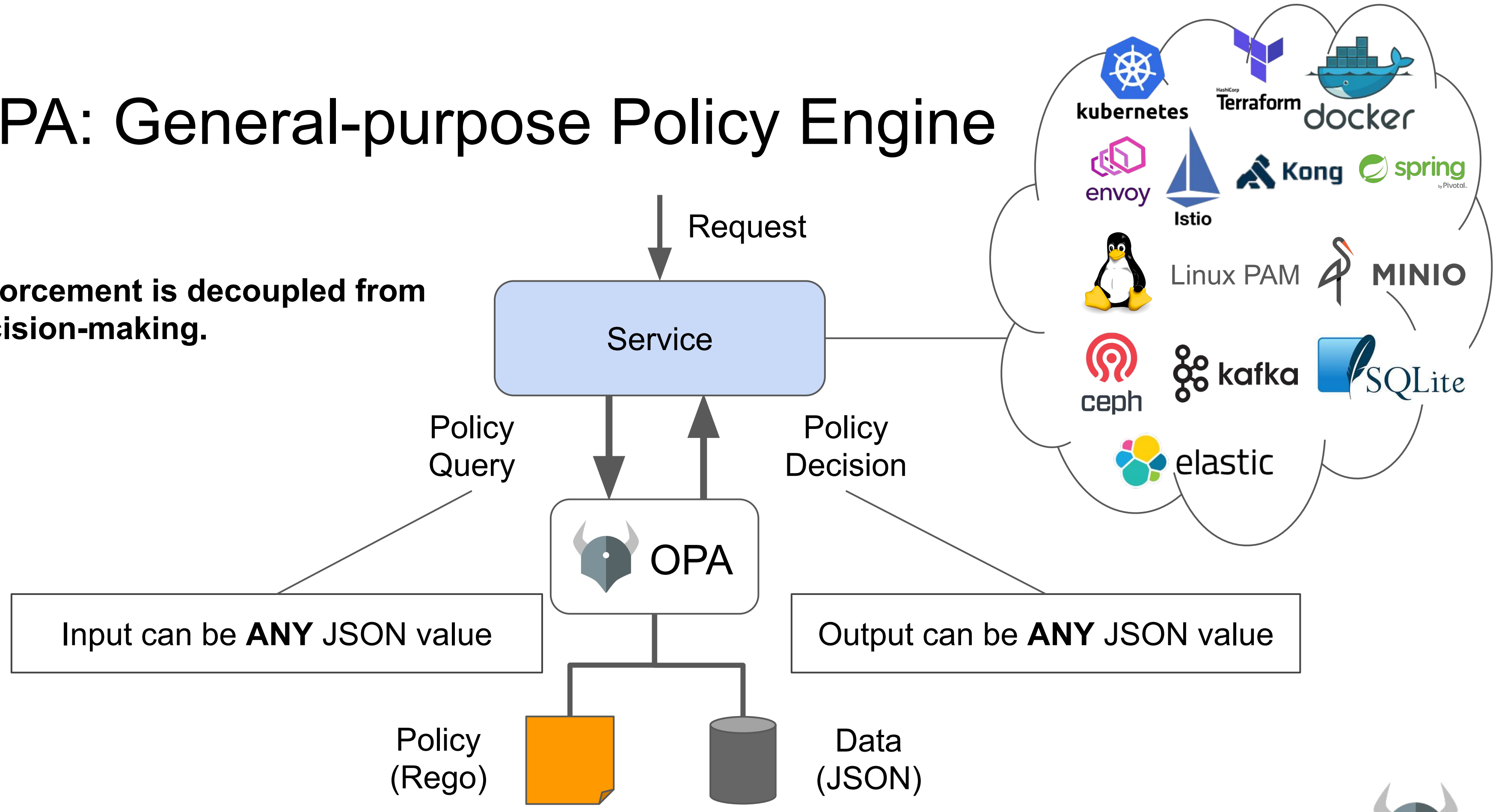
- **Declarative Policy Language (Rego)**
  - Can user X do operation Y on resource Z?
  - What invariants does workload W violate?
  - Which records should bob be allowed to see?
- **Library (Go), sidecar/host-level daemon**
  - Policy and data are kept in-memory
  - Zero decision-time dependencies
- **Management APIs for control & observability**
  - Bundle service API for sending policy & data to OPA
  - Status service API for receiving status from OPA
  - Log service API for receiving audit log from OPA
- **Tooling to build, test, and debug policy**
  - opa run, opa test, opa fmt, opa deps, opa check, etc.
  - VS Code plugin, Tracing, Profiling, etc.



openpolicyagent.org

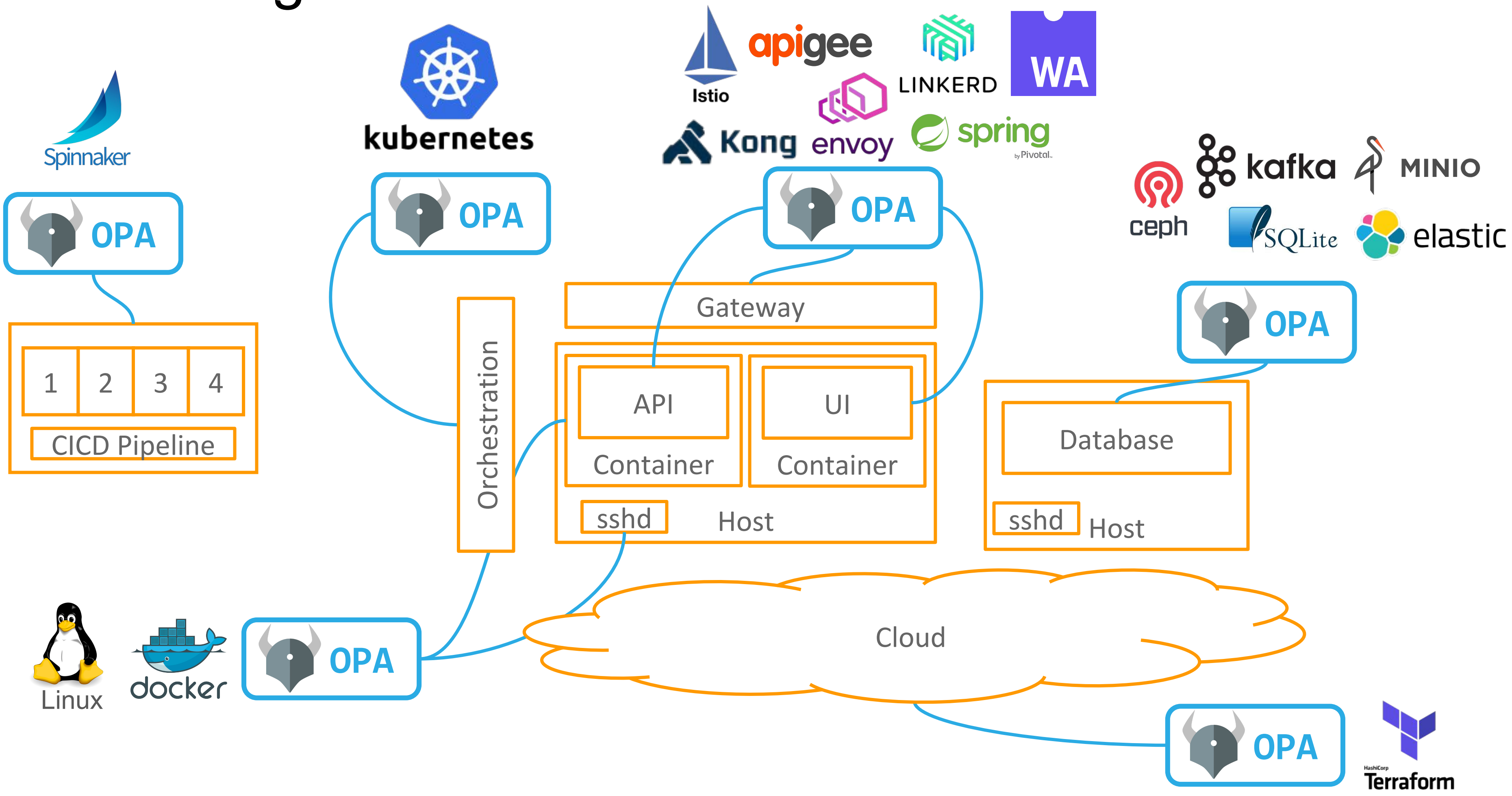
OPA: General-purpose Policy Engine

Enforcement is decoupled from decision-making.



openpolicyagent.org

OPA: Integrations

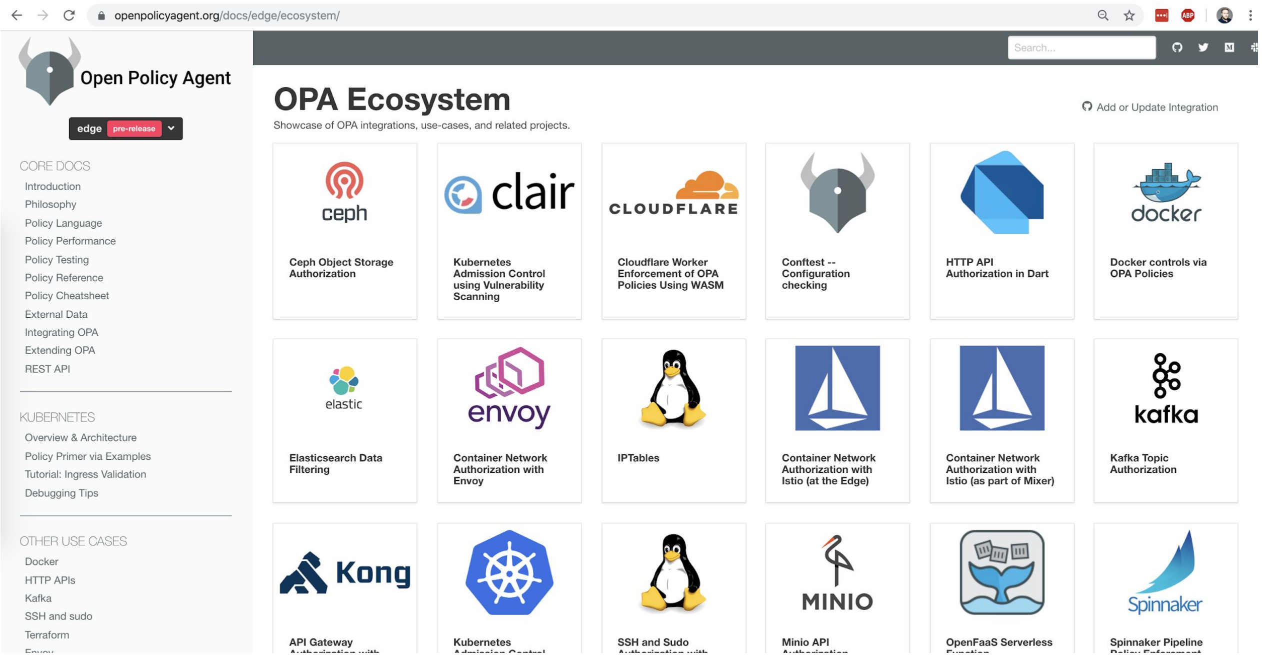


OPA: Example Use-Cases

kubernetes, HashiCorp Terraform, docker	Admission Control	*“Restrict ingress hostnames for payments team.”* *“Ensure container images come from corporate repo.”*
envoy, Istio, Kong, spring by Pivotal	API Authorization	*“Deny test scripts access to production services.”* *“Allow analysts to access APIs serving anonymized data.”*
Linux PAM	SSH & sudo	*“Only allow on-call engineers to SSH into production servers.”*
ceph, kafka, MINIO	Data Protection	*"Trades exceeding $10M must be executed between 9AM and 5PM and require MFA."*
SQLite, elastic	Data Filtering	*"Users can access files for past 6 months related to the region they licensed."*

openpolicyagent.org

OPA: Integration Index - https://bit.ly/32pPWEI



openpolicyagent.org/docs/edge/ecosystem/

Open Policy Agent

edge pre-release

CORE DOCS

- Introduction
- Philosophy
- Policy Language
- Policy Performance
- Policy Testing
- Policy Reference
- Policy Cheatsheet
- 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
- Terraform
- Envoy

Search...

OPA Ecosystem

Add or Update Integration

Showcase of OPA integrations, use-cases, and related projects.

- Ceph Object Storage Authorization
- Kubernetes Admission Control using Vulnerability Scanning
- Cloudflare Worker Enforcement of OPA Policies Using WASM
- Conftest -- Configuration checking
- HTTP API Authorization in Dart
- Docker controls via OPA Policies
- Elasticsearch Data Filtering
- Container Network Authorization with Envoy
- IPTables
- Container Network Authorization with Istio (at the Edge)
- Container Network Authorization with Istio (as part of Mixer)
- Kafka Topic Authorization
- API Gateway
- Kubernetes
- SSH and Sudo
- Minio API
- OpenFaaS Serverless
- Spinnaker Pipeline

openpolicyagent.org

OPA: Whats new?

- CI/CD pipelines
  - Spinnaker
  - Boomerang
  - Terraform
- Public cloud object storage for bundles
  - S3 in particular (OPA features) (and GCS, and OCI)
-

OPA Use-Case: Kubernetes Admission Controller

Gatekeeper

A customizable Kubernetes admission webhook that

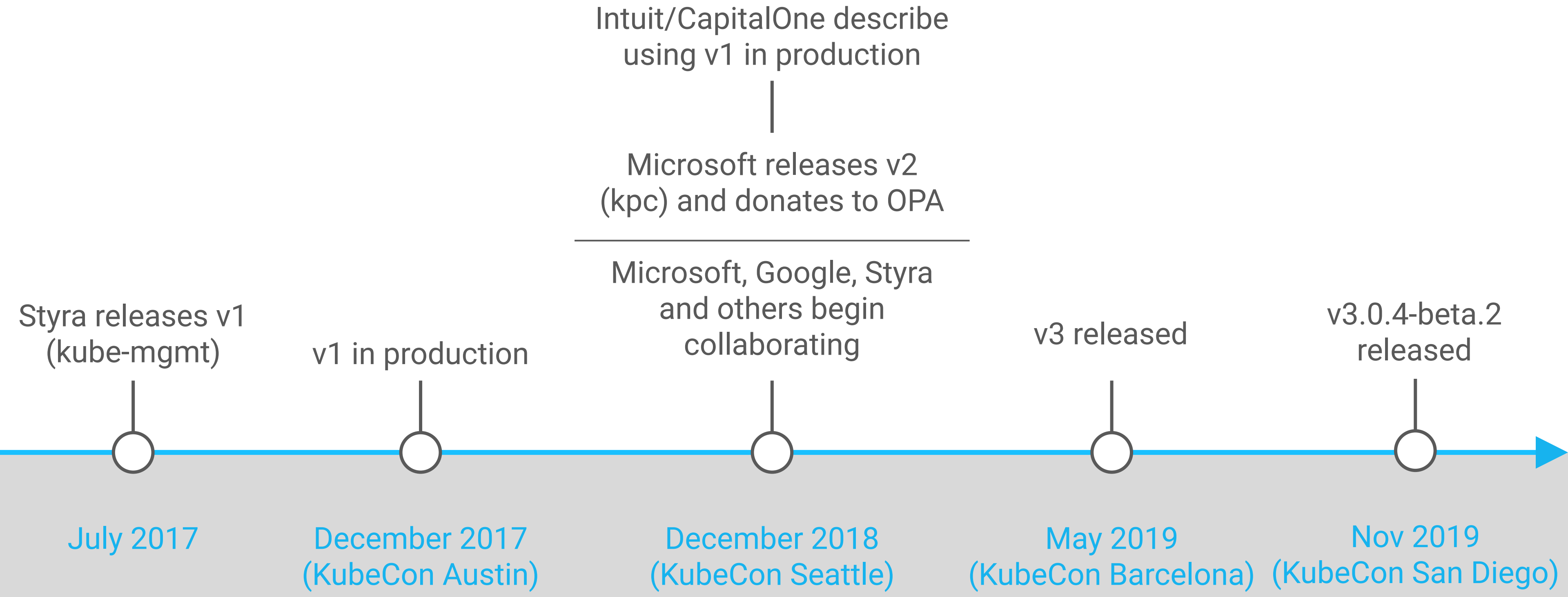
helps enforce policies and strengthen governance

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?

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)

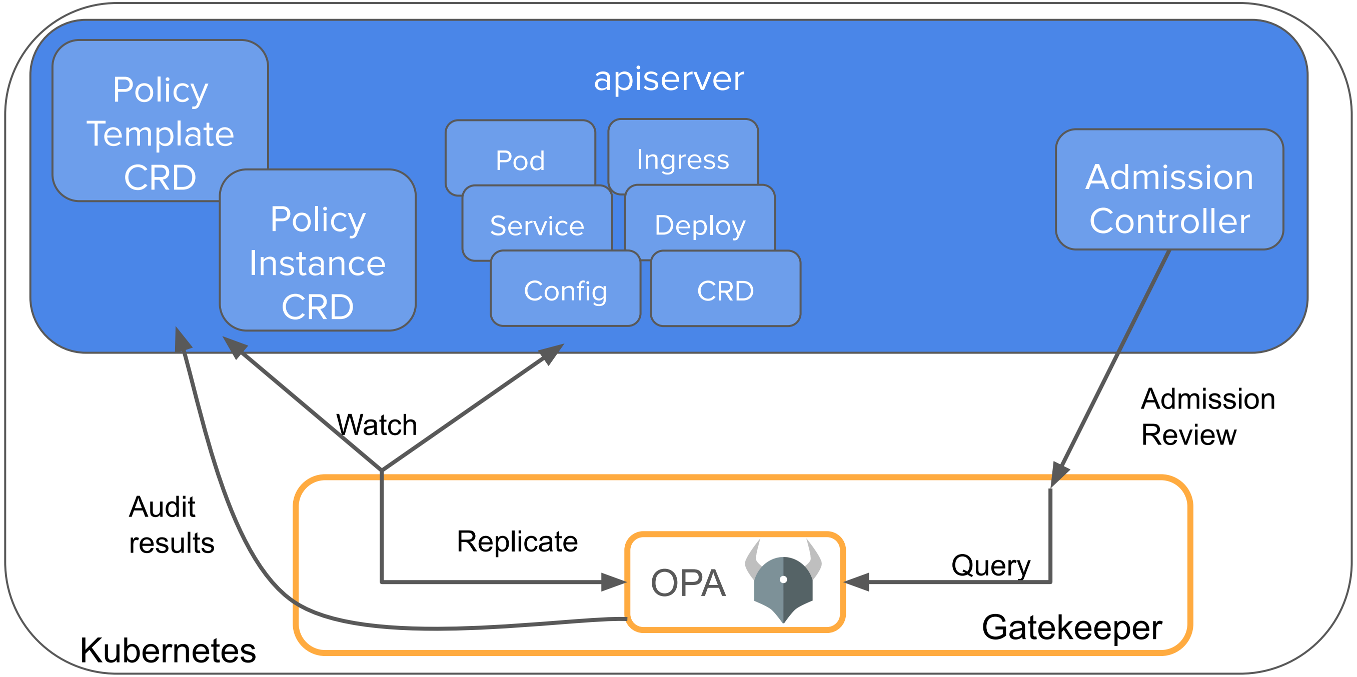
v3 released

May 2019 (KubeCon Barcelona)

v3.0.4-beta.2 released

Nov 2019 (KubeCon San Diego)

Gatekeeper: v3



openpolicyagent.org

Gatekeeper: v1 vs v3

	V1 (aka kube-mgmt)	V3 (aka Constraint framework)
Policy Management	ConfigMap Raw Rego stored in ConfigMaps with syntax-errors reported as annotations	CRD - Constraint template - Constraint Raw Rego stored in Constraint templates
Features	+ Context-aware/referential policies + Validating admission control + Mutating admission control + Multi-source	+ Context-aware/referential + Validating admission control + Audit + Dry run + CI/CD with conftest + Multi-source + Code reuse *Mutating admission control

Gatekeeper: Core Features

- Validating admission control
  - Control what end-users can do on the cluster
- Context-aware/referential policies
- Constraints are parameterized and easily configurable by admins
- ConstraintTemplates provide the source code for constraints
  - Easily shared
  - Testable
  - Developed internally or sourced from the community
- Audit
  - Periodically evaluates resources against constraints
  - Allows for ongoing monitoring of cluster state to aid in detection and remediation of pre-existing misconfigurations

Gatekeeper: Latest Updates

- Dry run
  - Test canary releases in a cluster in stages without impacting the cluster and your users
  - Gain confidence for our policies for admins before enforcing them; gradual rollout
- Namespace Selector
  - Narrow the scope of resources a constraint can enforce to certain namespaces only
- Policy library
  - Community developed policies
  - Pod security policies
- Multi-source constraint template
- Metrics

Demo:
Agile Bank

- Building the greatest P2P money transfer app to-date
- Highly regulated industry
- Both developers and admins are unhappy

Photo by Armando Arauz on Unsplash

Agile Bank's Governance Policies

- All namespaces must have a label that lists a point-of-contact
- All pods must have an upper bound for resource usage
- All images must be from an approved repository
- Services must all have globally unique selectors
- Ingresses must all have globally unique hostnames

Demo

Gatekeeper: Status

- Beta
- Come help!
    - Issues
    - Feedback
    - User stories
    - Development

Cooking... but tasty

Gatekeeper: Potential Growth

- Production ready
- Mutation
- External Data
- More audit features
- More metrics
- More policies
- Developer tooling
- Authorization? (likely separate project, same general semantics)

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

Thank You!

More Sessions this week!!

- Every day! — Meet the Maintainer: OPA
- Tuesday 11:50am — Applying Policy Throughout The Application Lifecycle with Open Policy Agent
- Tuesday 2:25pm — Enforcing Automatic mTLS With Linkerd and OPA Gatekeeper
- Wednesday 5:20pm — OPA Deep Dive
- Thursday 10:55am — How Yelp Moved Security From the App to the Mesh with Envoy and OPA
- Thursday 2:25pm — SIG Auth Update and Deep Dive
- Thursday 4:25pm — Enforcing Service Mesh Structure using OPA Gatekeeper
- Thursday 5:20pm — Kubernetes Policy Enforcement Using OPA At Goldman Sachs

... and more! Check the schedule!