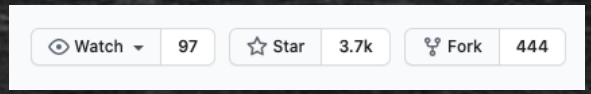
Introdução:
Open Policy Agent

Agenda

- O que é e como funciona?
- OPA + Kubernetes
- Demo
- Q&A

O que é o OPA?

Construído pela Styra em 2016



O projeto Open Policy Agent (OPA, pronounced "oh-pa") é um projeto open source, usado para geração de política de seguraça multi stack

Linguagem declarativa de alto nivel = Politica como Código

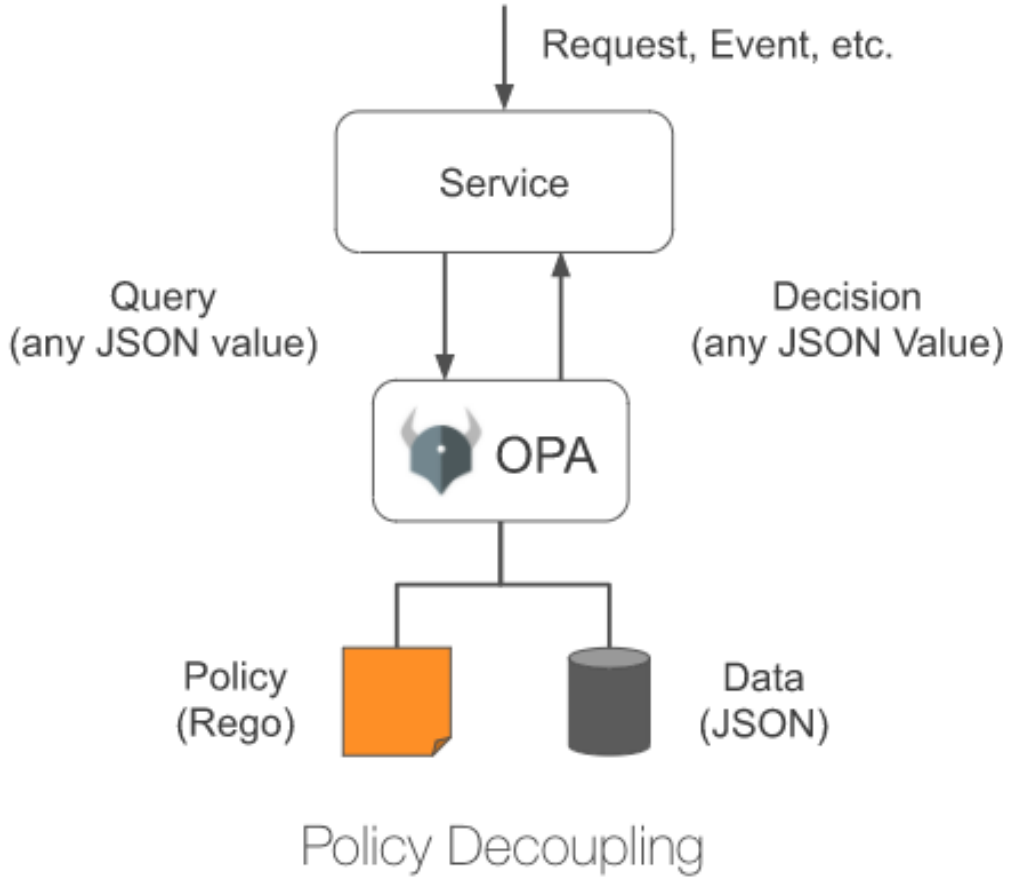
Unifica a aplicação de politicas com suporte multi stack

O que é o OPA?

OPA e seu Eco-Sistema

https://www.openpolicyagent.org/docs/latest/ecosystem/

Como o Opa funciona?

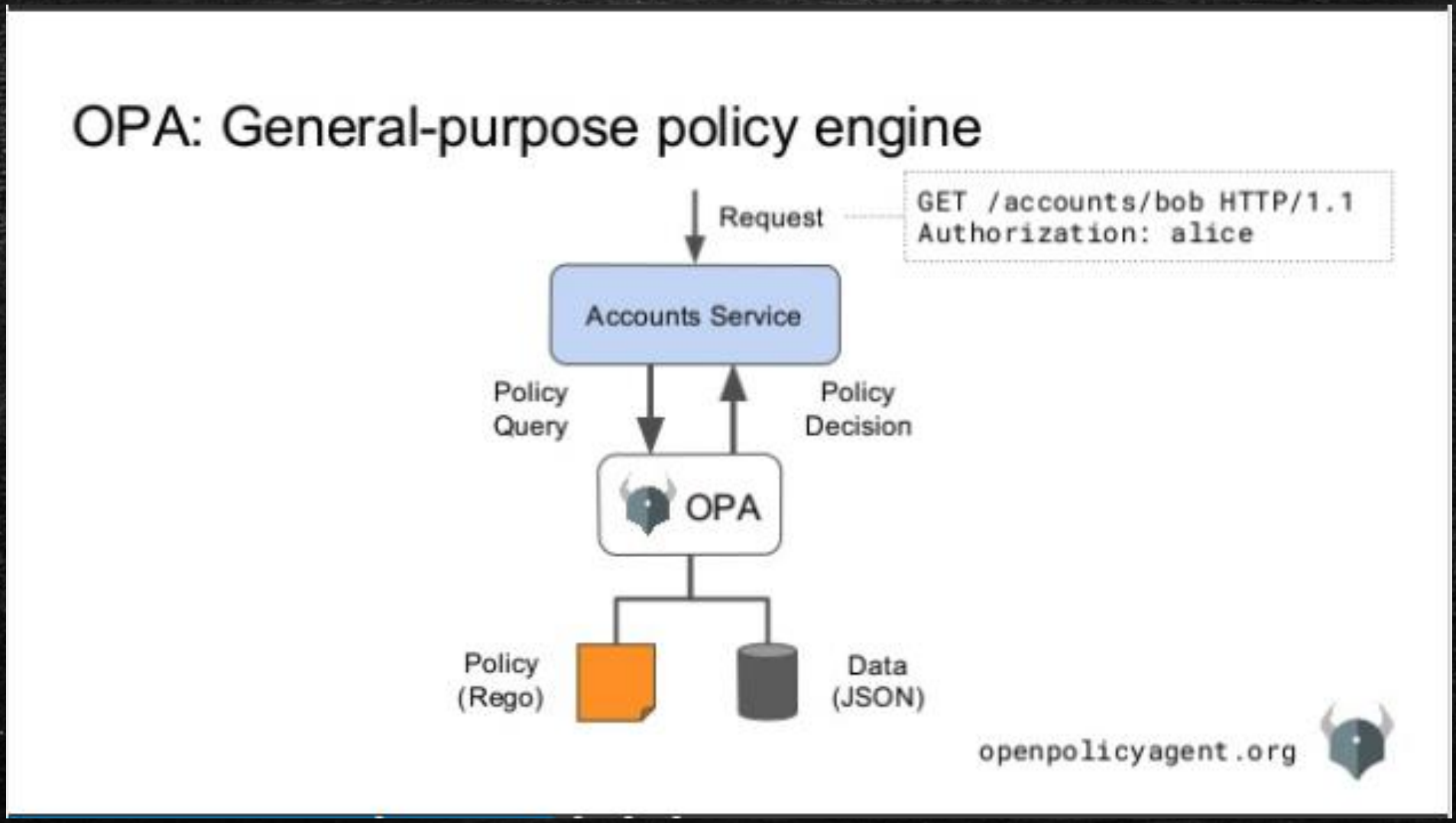


Policy Decoupling

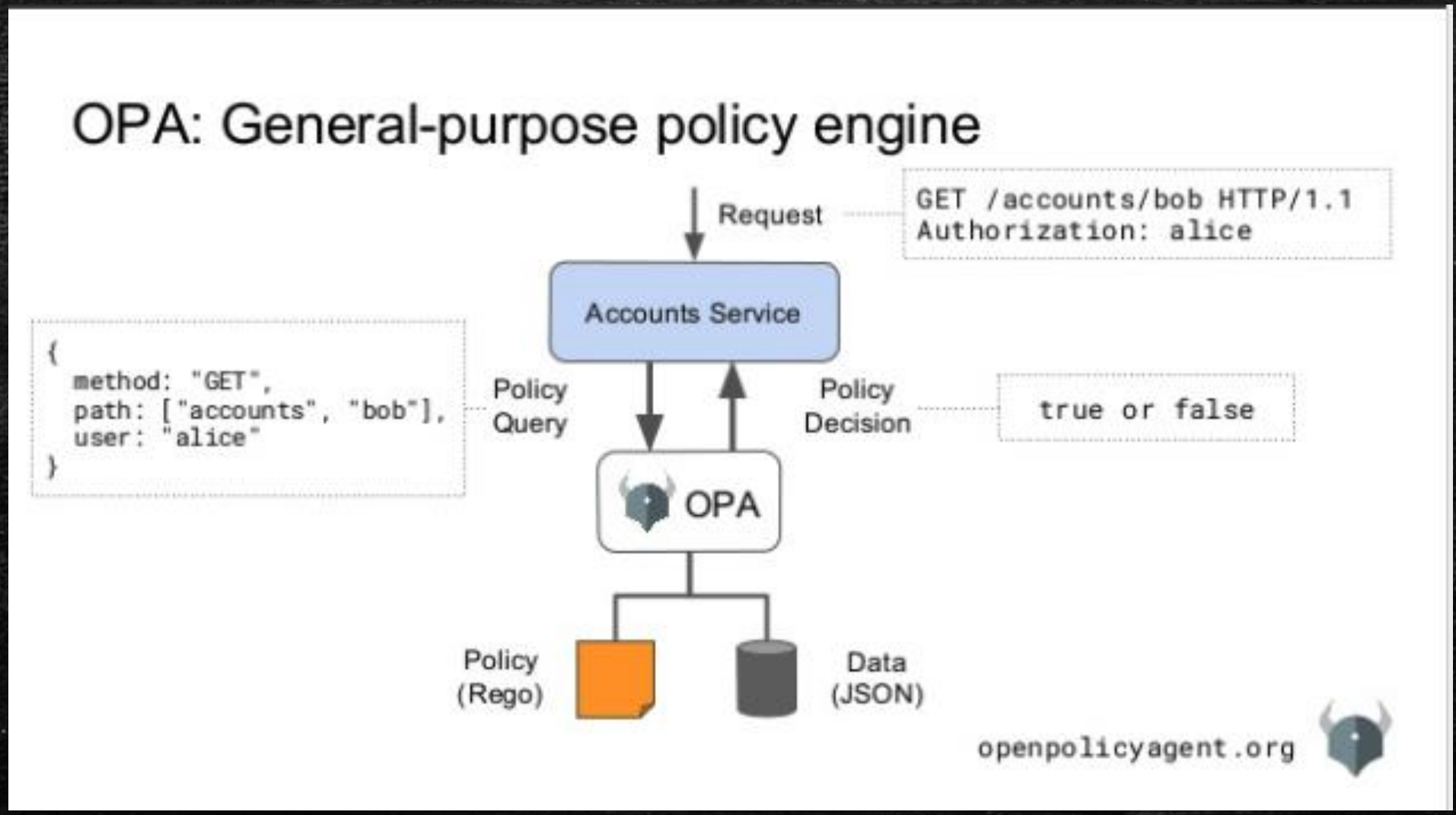
Como o Opa funciona?

kubernetes Terraform docker	Admission Control	*"Restrict ingress hostnames for payments team."* *"Ensure container images come from corporate repo."*
envoy Istio Kong spring	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."*

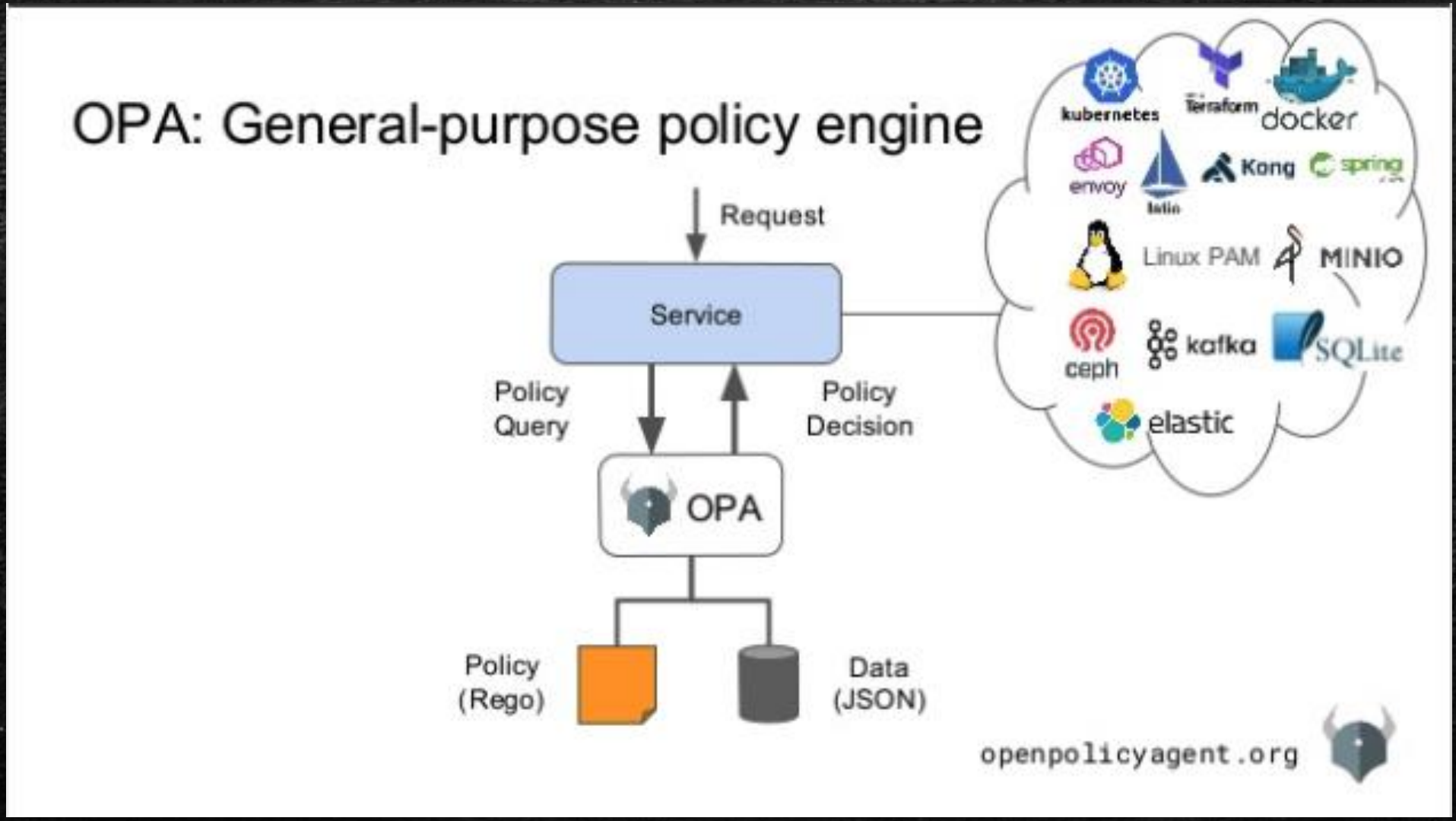
Como o Opa funciona?



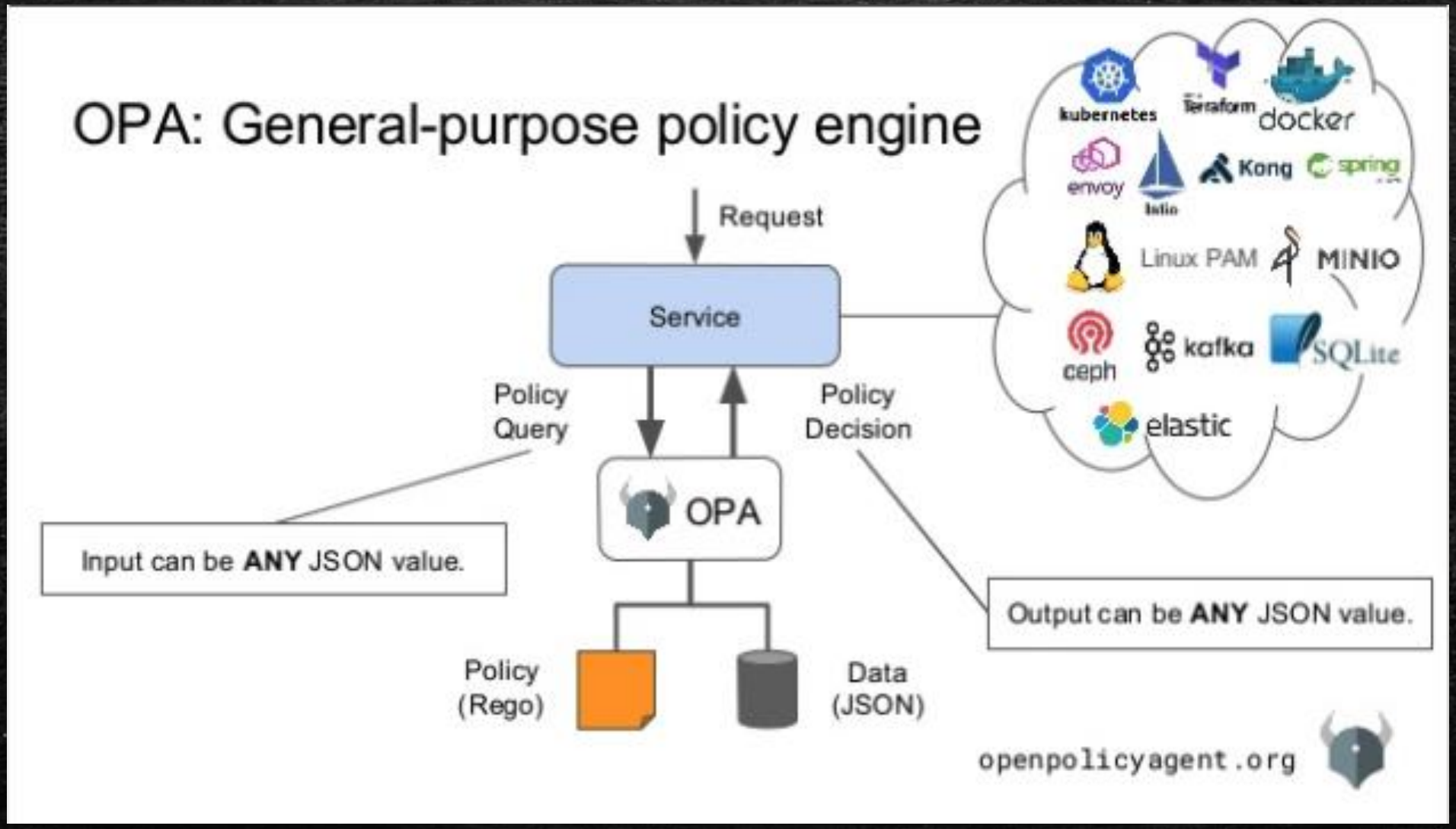
Como o Opa funciona?



Como o Opa funciona?



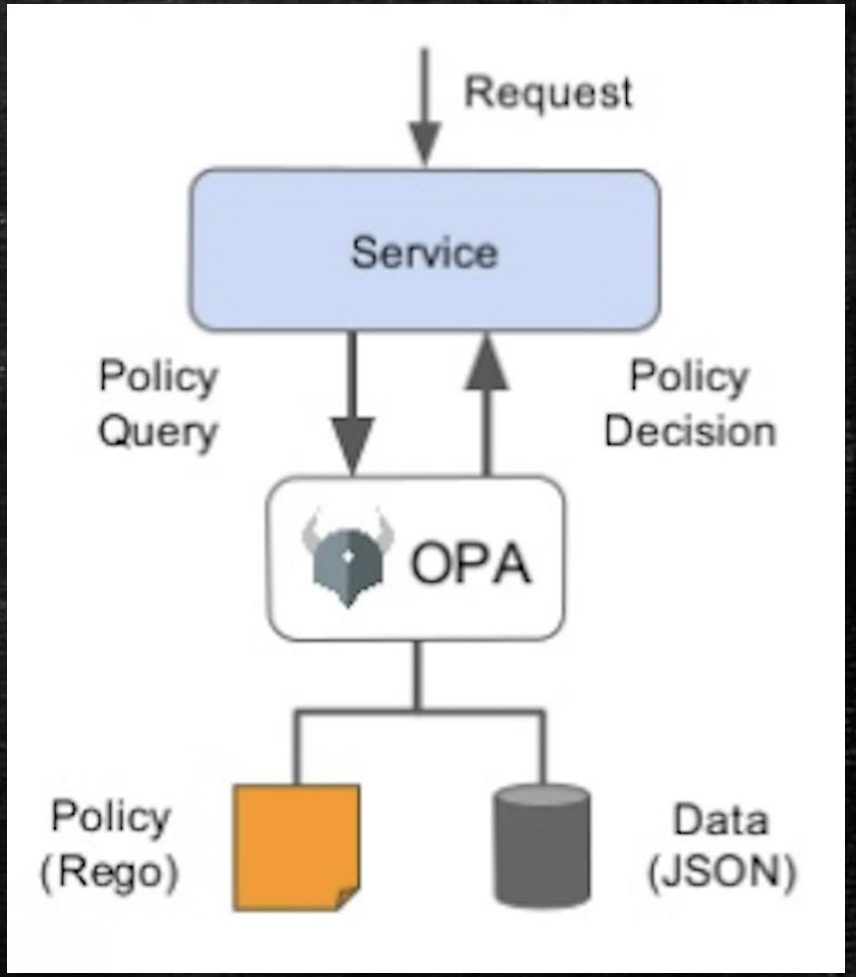
Como o Opa funciona?



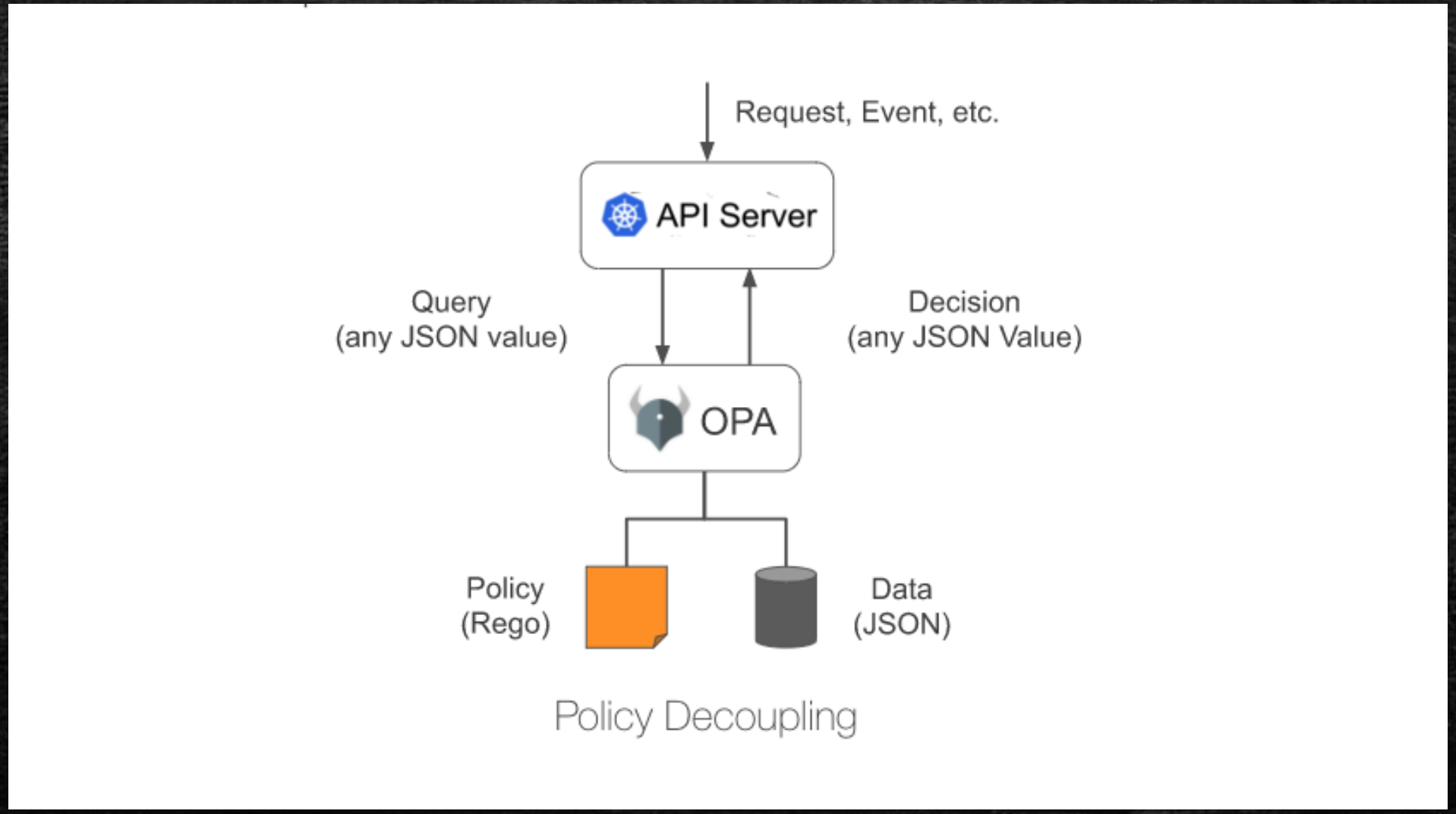
Como o Opa funciona?

Linguagem de Politicas (REGO)

* O usuário X pode fazer a operação Y no recurso Z?
* Quais recursos o usuário frank esta autorizado a visualizar?



OPA + Kubernetes



OPA + Kubernetes

Para uso no Kubernetes é um requisito ter instalado um

Admission Controller

OPA + Kubernetes

An admission controller is a piece of code that intercepts requests to the Kubernetes API server prior to persistence of the object, but after the request is authenticated and authorized.

Admission Controller = Intercepta requests + toma decisões

OPA + Kubernetes

O que podemos fazer com OPA e um Admission Control?

Politicas como:

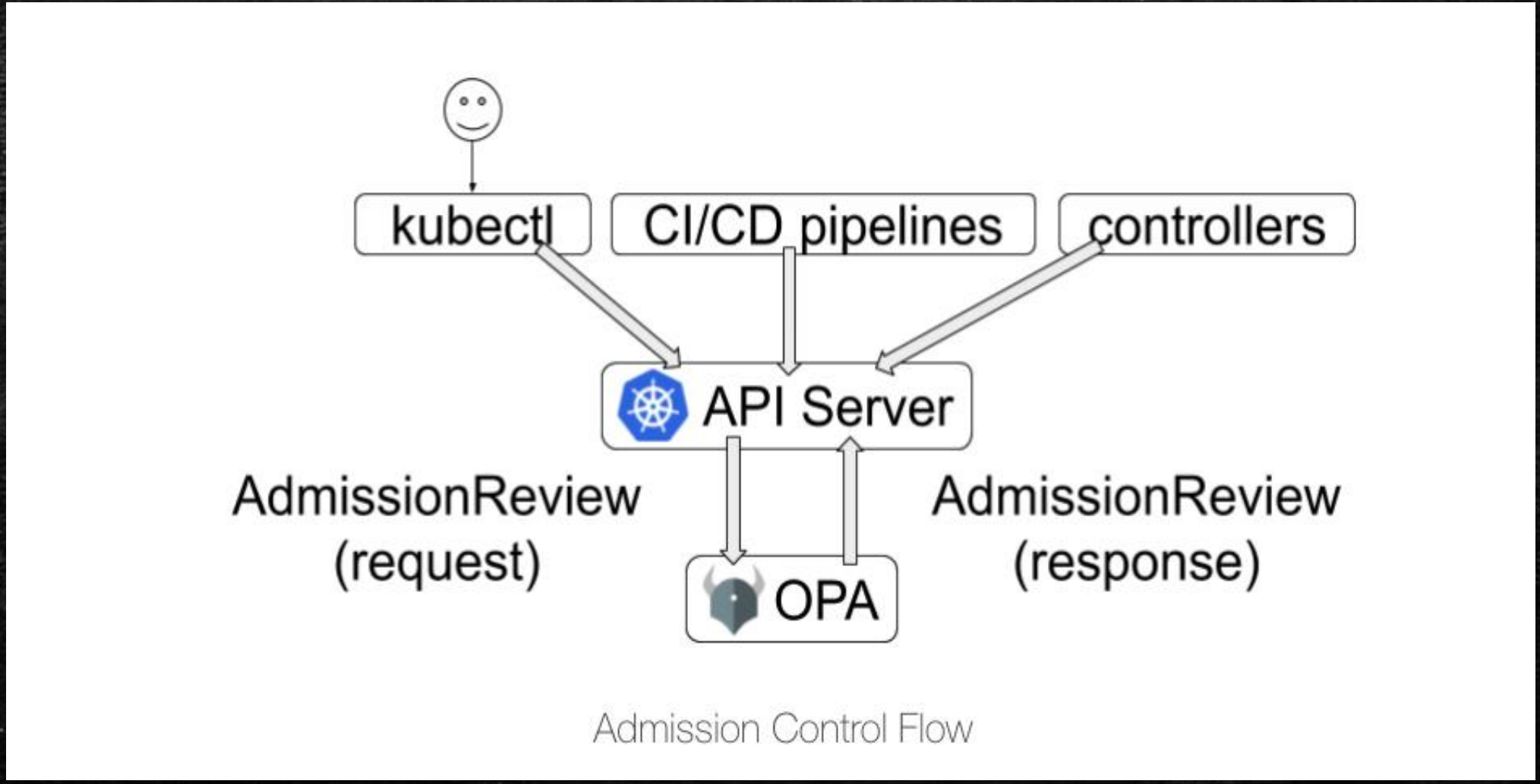
* Exigir labels especificos em determinados recursos dos Kubernetes.
* Exigir que os containers apenas executem imagens que venha de um registry interno.
* Exigir que os pods tenham o securityContext configurado.

OPA + Kubernetes

Operações de Mutate:

* "Injetar" containers sidecar nos Pods.
* Adicionar annotations em todos ou em alguns resources.
* Modificar o registry das imagens dos containers, substituindo pelo registry local.

OPA + Kubernetes



OPA + Kubernetes

Rego Playground Examples

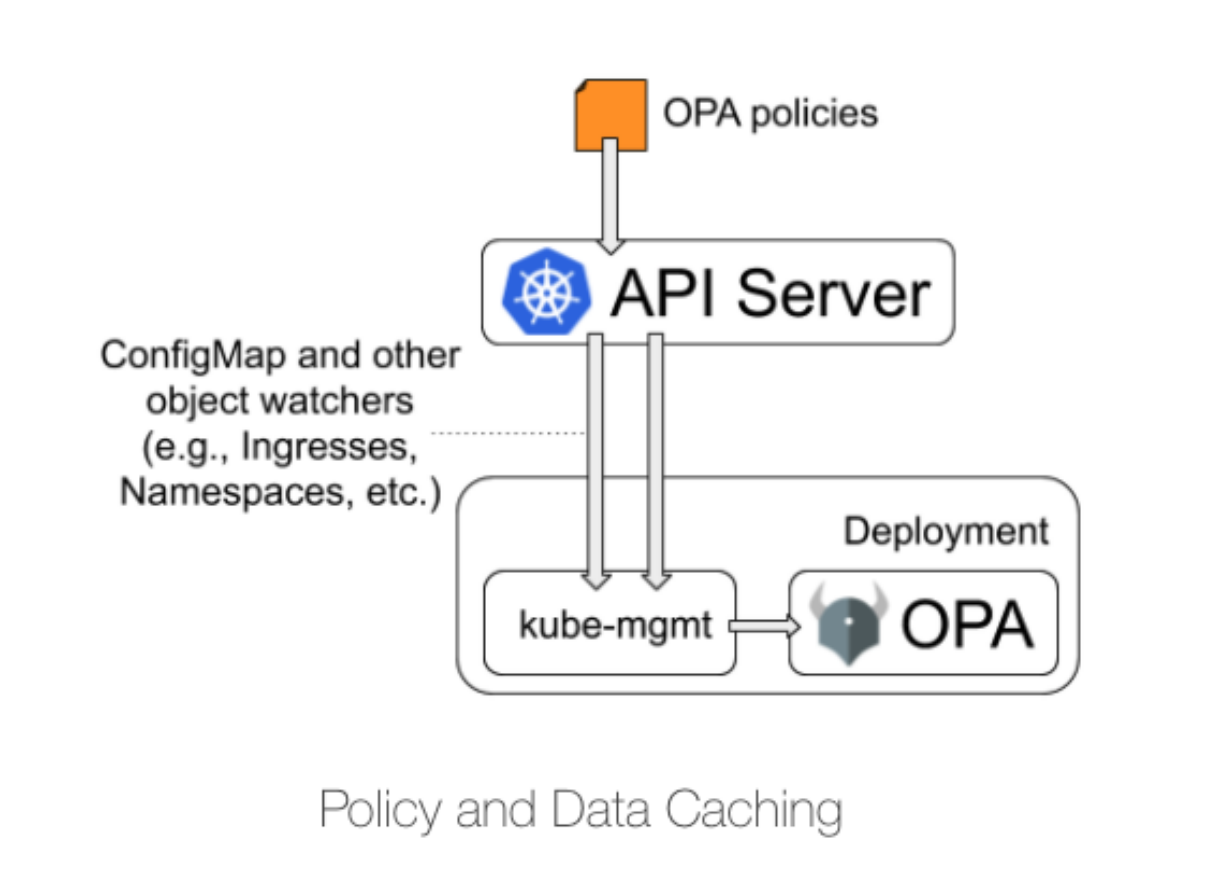
OPA + Kubernetes

O documento de input contém os seguintes campos:

input.request.kind specifies the type of the object (e.g., Pod, Service, etc.)
input.request.operation specifies the type of the operation, i.e., CREATE, UPDATE, DELETE.
input.request.object contains the entire Kubernetes object.
input.request.oldObject specifies the previous version of the Kubernetes object on UPDATE and DELETE.

OPA + Kubernetes

kube-mgmt



OPA + Kubernetes

It's Demo Time

Referencias:

https://www.openpolicyagent.org/docs/latest/ecosystem/

https://www.openpolicyagent.org/docs/latest/kubernetes-introduction/

https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/

https://blog.openpolicyagent.org/the-rego-playground-977566855cec

Obrigado!