

Introduction to Open Policy Agent



Wojciech Barczyński, VP of Engineering
wojciechb@spacelift.io

Problem

Chasing the rabbit:

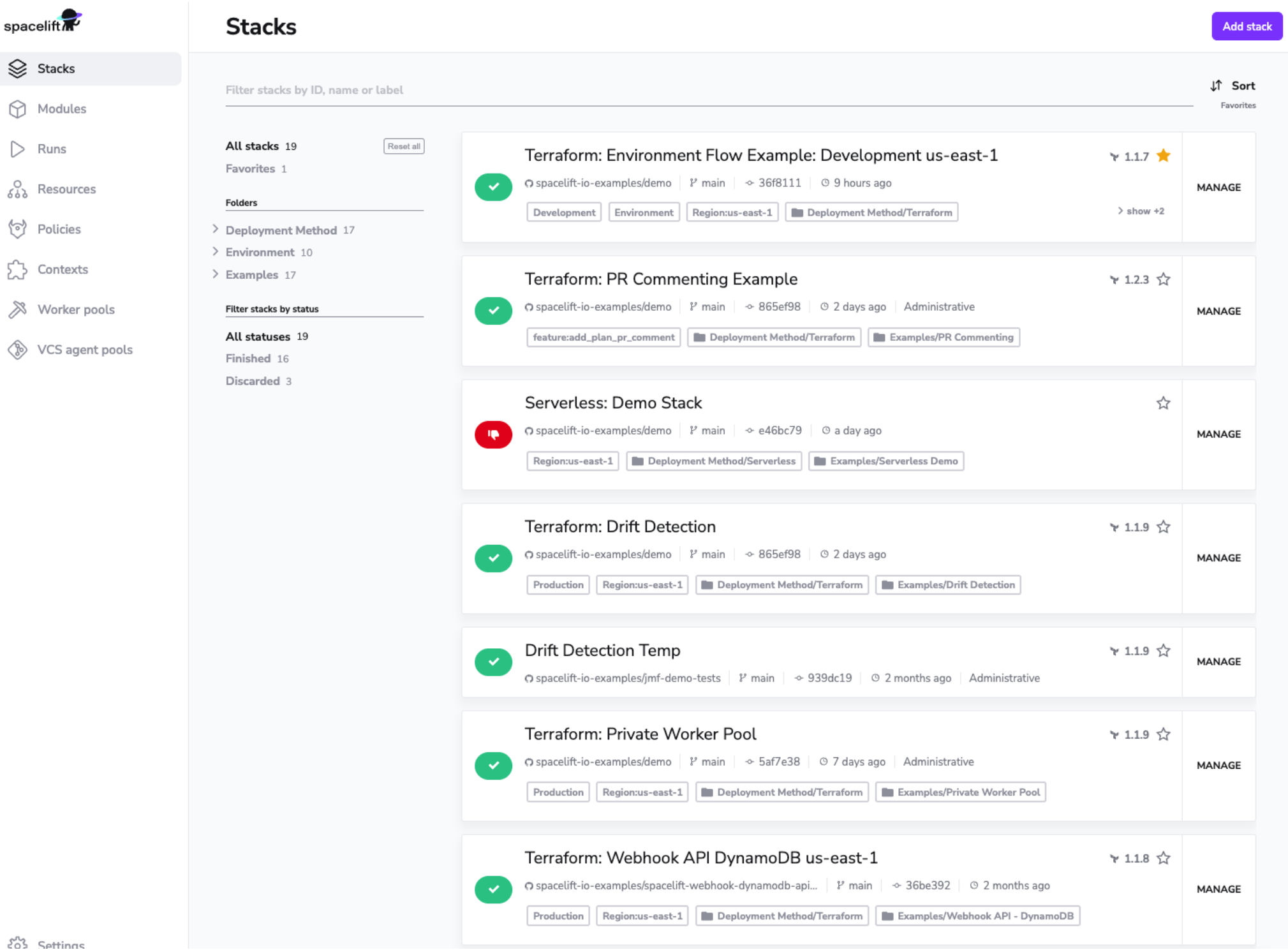
- Policies
- Configuration
- and ofc secure



Building your own app

Spacelift.io:

- SaaS
- for Infra-as-a-Code
- Power users



Infra / platform teams

- Share/enforce best practices
- Enable other teams to contribute

Potential solutions

- Endless forms
- Markup language

Potential solutions

- Scripting language embedded

Policy as-a-code

- Dedicated language with safety guarantees
- Work on loosely structured data
- have a JSON support

Open Policy Agent



Created by

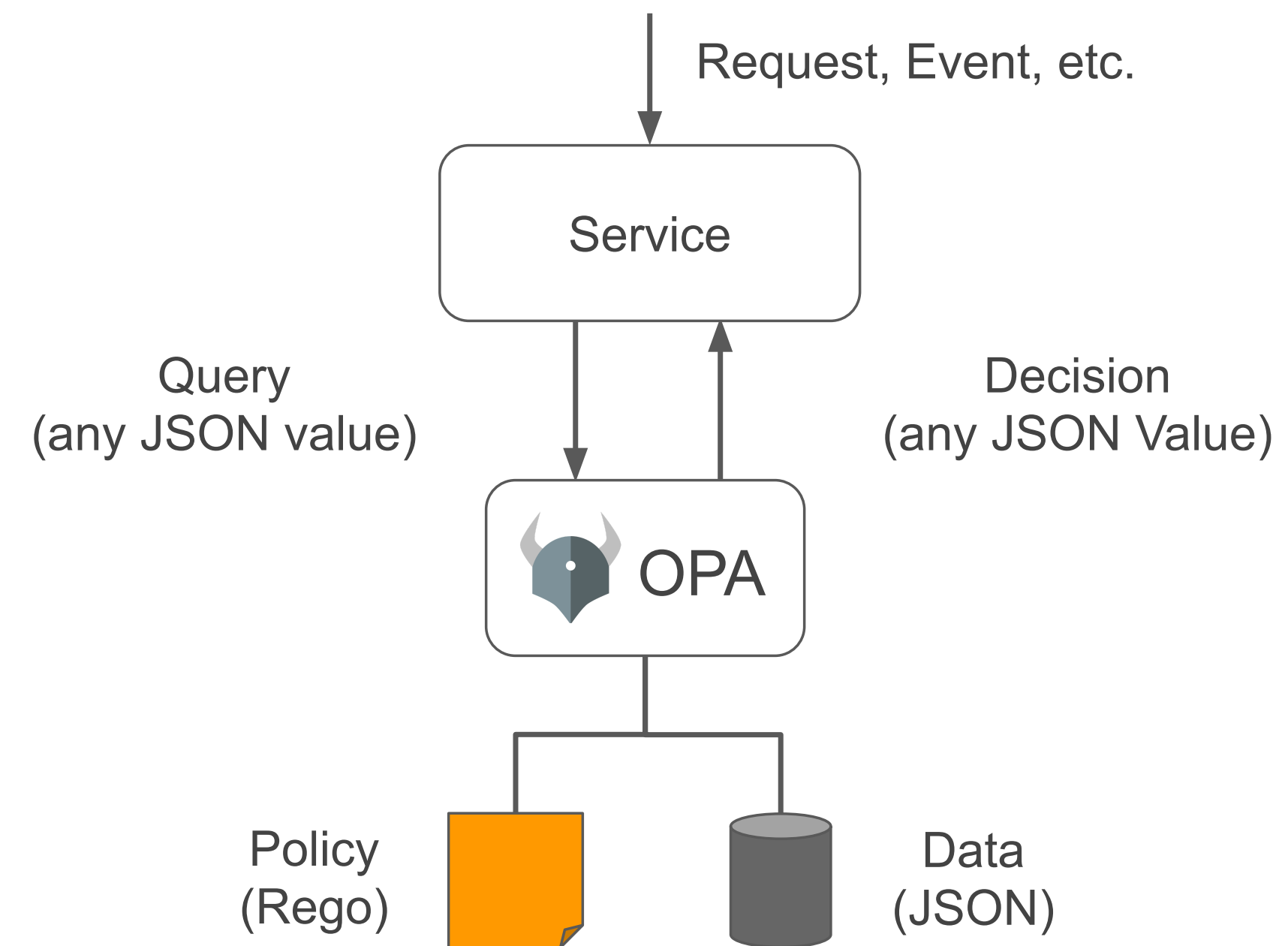


openpolicyagent.org



Open Policy Agent

1. Query/transformation language (rego)
2. Works on loosely structured data
3. With JSON and graph support



Demo

play.openpolicyagent.org

Demo

Input:

```
{  
  "session": {  
    "login": "natalia@example.com",  
    "teams": ["DevOps"],  
    "member": true  
  }  
}
```

Demo

Policy:

```
package talk_opa
teams := input.session.teams

admin { teams[_] == "DevOps" }
allow { teams[_] == "Engineering" }
deny  { not input.session.member }
```

Rego

- Readable and easier for non-programmers*;
- Declarative;
- Inspired by [Datalog](#)

Rego

- extended with support for arbitrary structured documents;
- Build-in functions;

Rego

- You can run the custom code safe:
 - non Turing-complete (no loops or conditionals);
 - guaranteed to terminate;
 - ensures that queries are correct and unambiguous.

Demo

Data - global values:

```
{  
  "maintenance": false,  
  "region": "eu-west-1"  
}
```

Ecosystem



Kubernetes Admission Control



Terraform Policy



Container Network Authorization with Envoy



Authorization for Java Spring Security



Styra Declarative Authorization Service



Container Network Authorization with Istio (at the Edge)



Strimzi (Apache Kafka on Kubernetes)



kafka

Kafka Topic Authorization



Custom Application Authorization



Permit.io



HTTP API Authorization in PHP



Fairwinds Insights Configuration Validation Software



Kubescape

Kubescape Kubernetes security posture scanner



Kubernetes Authorization



ceph

Ceph Object Storage Authorization



OPAL (Open Policy Administration Layer)



SPIRE

SPIRE



AWS CloudFormation Hook

Checkers & linters

Kubernetes, Terraform, and many others:

- [conftest](#)
- [kics.io](#)

Checkers & linters

conftest

```
package main

import data.kubernetes

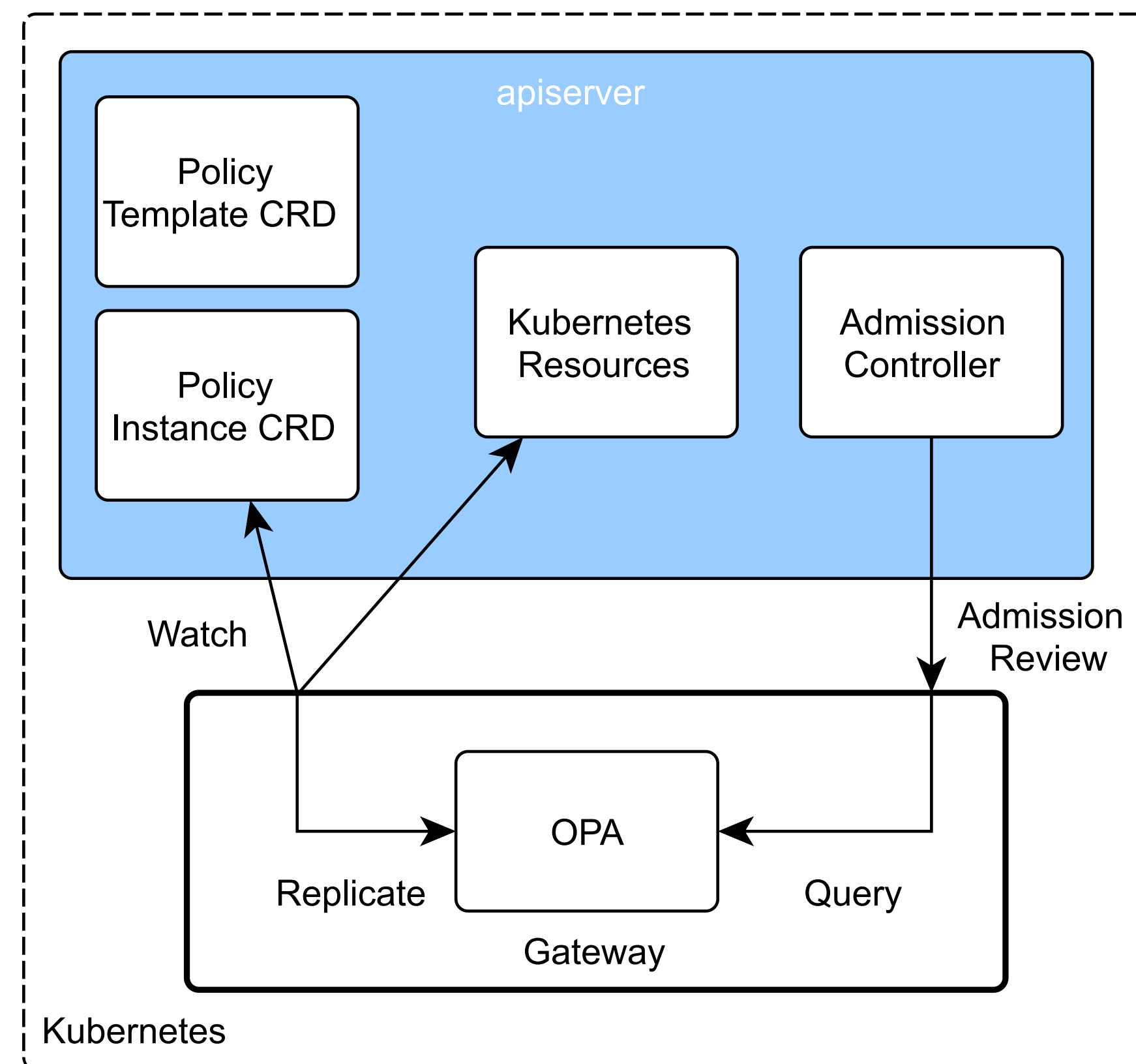
name = input.metadata.name

deny[msg] {
    kubernetes.is_deployment
    not input.spec.template.spec.securityContext.runAsNonRoot

    msg = sprintf("must not run as root in Deploy %s", [name])
}
```

Kubernetes

Admission hooks:



Kubernetes

```
package kubernetes.admission
operations = {"CREATE", "UPDATE"}

input_container[c] {
  c := input.request.object.spec.template.spec.containers[_]
}

deny[reason] {
  input.request.kind.kind == "Deployment"
  operations[input.request.operation]
  input_container[container]
  not container.resources.limits.cpu
  reason := sprintf("no cpu limit for container %v", [container])
}
```

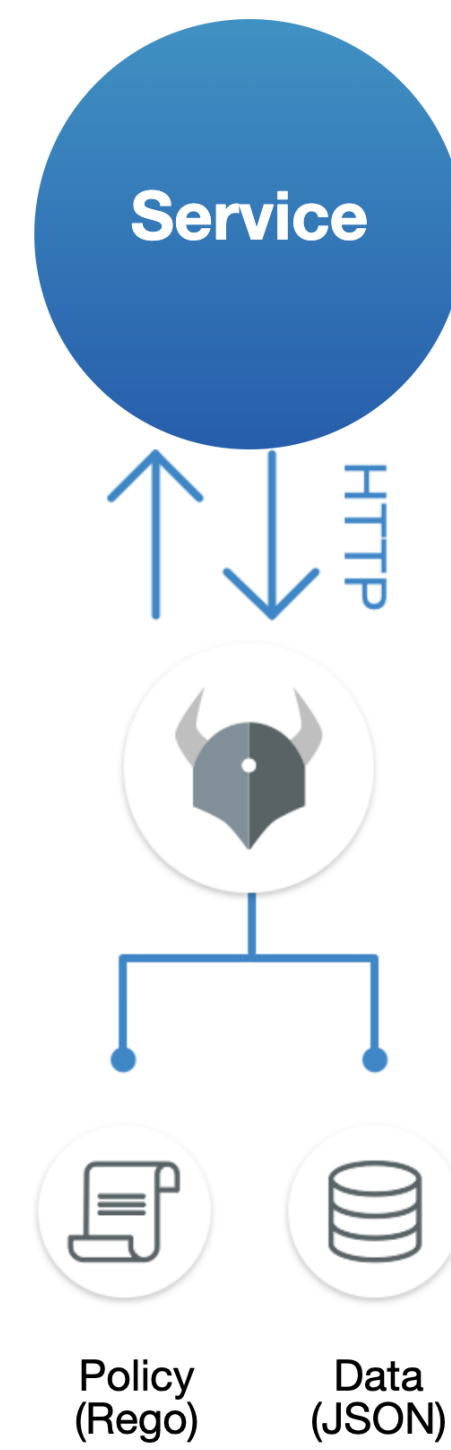
Kubernetes

OPA integrations:

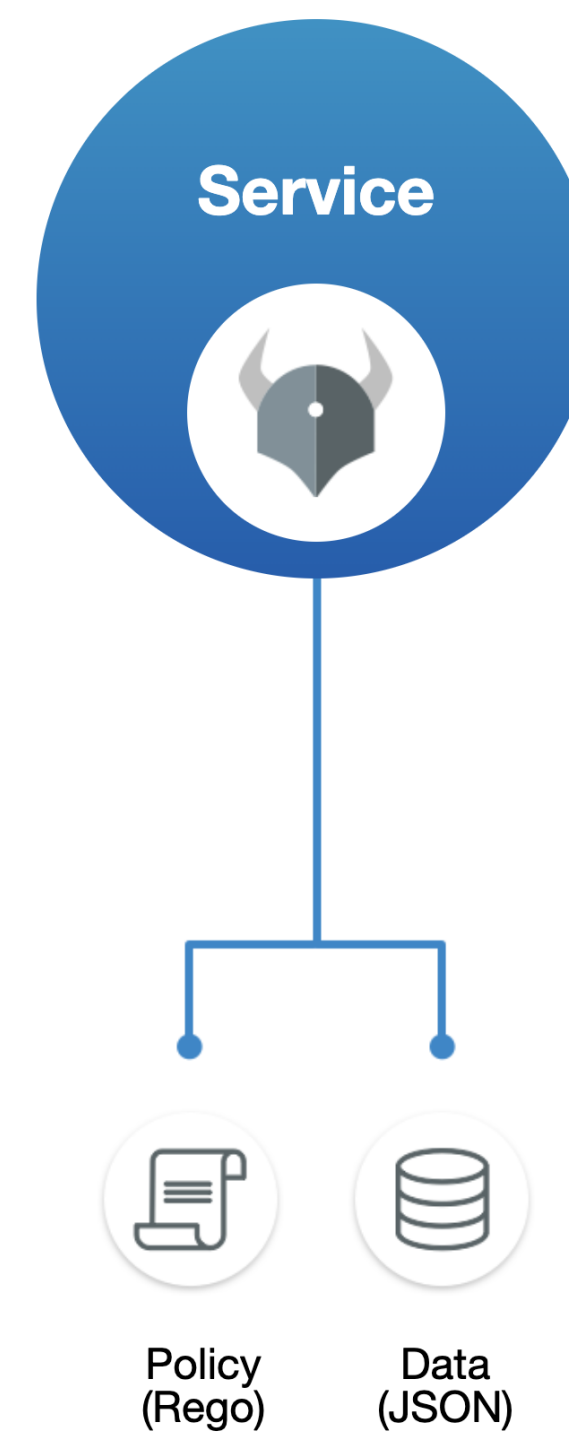
- Istio
- Envoy

Your app/tool

Daemon



Library



Golang & OPA

- Golang lib - embed OPA
- Golang SDK - high level API

See [docs](#)

Golang & OPA

Let's dive into [the code](#).

Golang & OPA

```
var (  
    unsafeBuiltins = map[string]struct{}{  
        "http.send":          {},  
        "opa.runtime":         {},  
        "rego.parse_module":   {},  
        "time.now_ns":         {},  
        "trace":               {},  
    }  
)
```

```
rego.UnsafeBuiltins(unsafeBuiltins)
```


Golang & OPA

You can also add your custom functions for your customer to use, see [docs](#).

Lessons learnt

Open Policy Agent:

- easily integrates with Golang
- implement policy-as-a-code in a safe way
- not only for policies

Lessons learnt

Rego requires some time to master:

1. Policy workbench with samples
2. Examples and docs
3. Policy testing

Lessons learnt

Styra, for example, provides an interactive builder:

- Policy Builder

Alternatives

- [cuelang](#)
- [kyverno](#)
- [Sentinel](#)



Slides and code:

github.com/wojciech12

Wojciech Barczynski
wojciechb@spacelift.io



Hiring

(Go) Backend and Frontend developers
with a passion for building tools
for other engineers.