

Adding Policies to your apps with Open Policy Agent framework



Wojciech Barczyński, VP of Engineering
wojciechb@spacelift.io

Problem

Chasing the rabbit:

- Policies
- Configuration
- but also product plans and features



Challenge

At Spacelift:

- We build an Infra-as-a-Code SaaS for power users.
- We need a safe and flexible way for users to customize our platform

Potential solutions

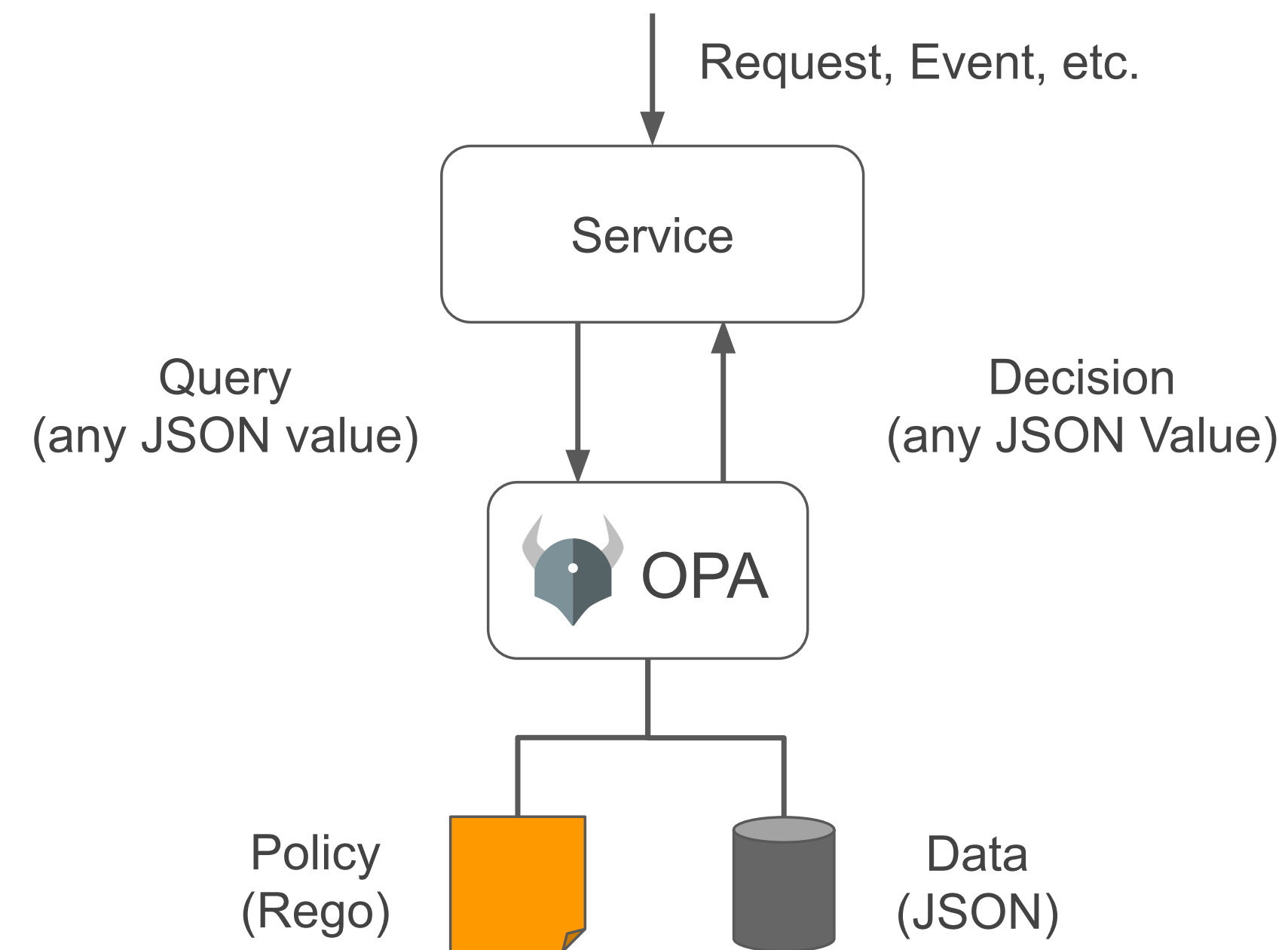
- Endless forms
- Markup language

Potential solutions

- Scripting language embedded

Open Policy Agent

1. Policy-as-a-Code
2. Query/transformation language (rego)
3. Works on loosely structured input & data
4. With JSON support



Demo

play.openpolicyagent.org

Demo

Input:

```
{  
  "session": {  
    "login": "wojciech12",  
    "teams": ["DevOps"],  
    "member": true  
  }  
}
```


Demo

Input:

```
{
  "request": {
    "remote_ip": "string - IP of the user trying to log in",
    "timestamp_ns": "number - current Unix timestamp in nanoseconds"
  },
  "session": {
    "login": "string - username of the user trying to log in",
    "member": "boolean - is the user a member of the account",
    "name": "string - full name of the user trying to log in - may be empty",
    "teams": ["string - names of teams the user is a member of"]
  }
}
```

Demo

Policy:

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

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

Rego

- Declarative;
- Supports arbitrarily nested documents (e.g. graphs);
- Readable and easier for non-programmers*;

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.
- Build-in functions

Demo

Data - global values:

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

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)
```


Lessons learnt

Open Policy Agent:

- easily integrates with Golang
- implement policy-as-a-code in a safe way

Lessons learnt

Rego requires some time to master:



















- [examples](#) and [docs](#)
- [policy testing](#)

Lessons learnt

Watch out:

- You load input to memory to evaluate policy

Ecosystem

 <p>Kubernetes Admission Control</p>	 <p>Terraform Policy</p>	 <p>Container Network Authorization with Envoy</p>	 <p>Authorization for Java Spring Security</p>	 <p>Styra Declarative Authorization Service</p>	 <p>Container Network Authorization with Istio (at the Edge)</p>
 <p>Strimzi (Apache Kafka on Kubernetes)</p>	 <p>Kafka Topic Authorization</p>	 <p>Custom Application Authorization</p>	 <p>Permit.io</p>	 <p>HTTP API Authorization in PHP</p>	 <p>Fairwinds Insights Configuration Validation Software</p>
 <p>Kubescape Kubernetes security posture scanner</p>	 <p>Kubernetes Authorization</p>	 <p>Ceph Object Storage Authorization</p>	 <p>OPAL (Open Policy Administration Layer)</p>	 <p>SPIRE</p>	 <p>AWS CloudFormation Hook</p>



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.