

Adding Policies to your Golang app with Open Policy Agent framework



Wojciech Barczyński, VP of Engineering
wojciechb@spacelift.io

Problem

Chasing the rabbit:

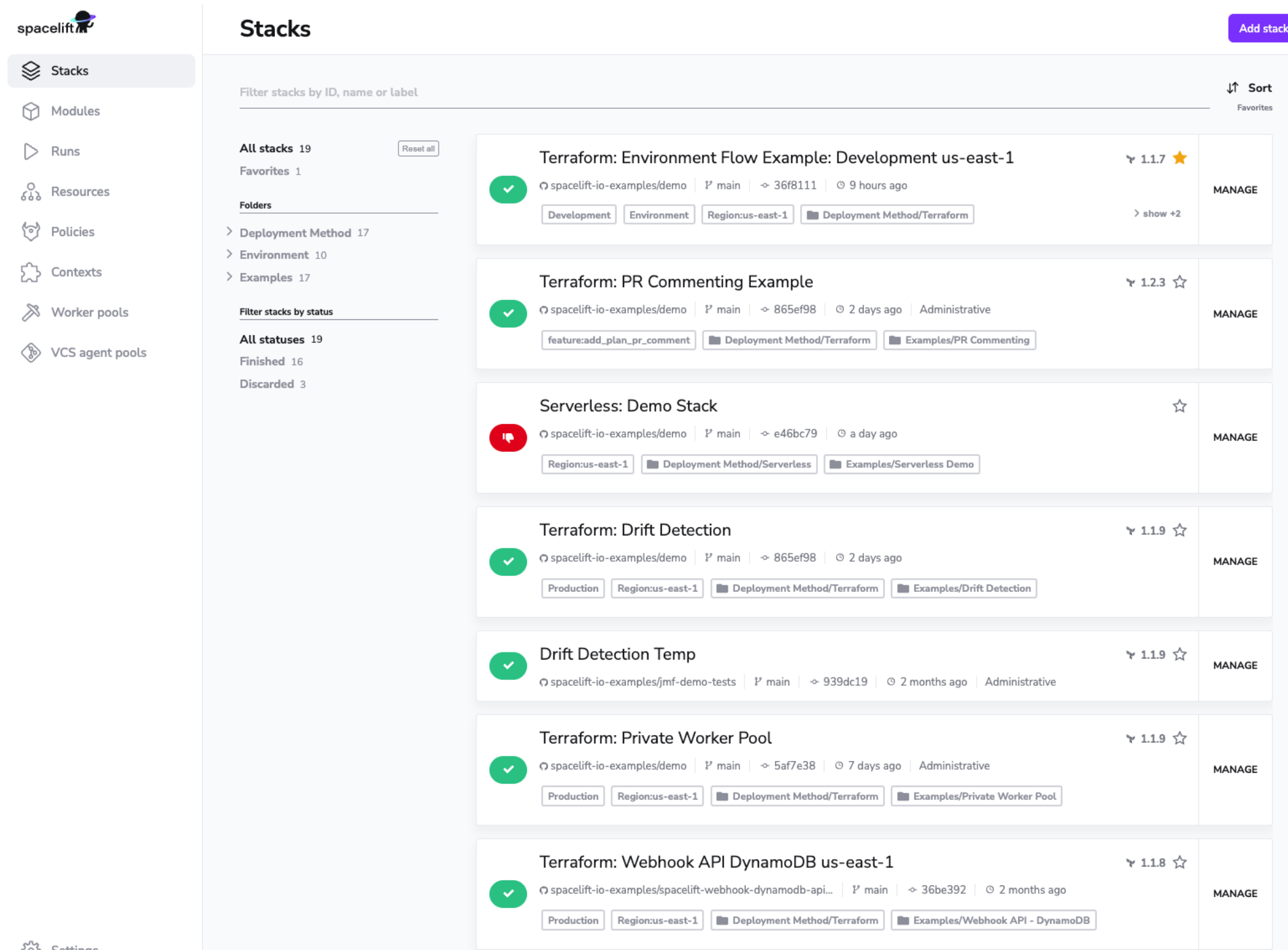
- Policies
- Configuration
- but also product plans and features



Building your own app

Spacelift.io:

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



Potential solutions

- Endless forms
- Markup language

Potential solutions

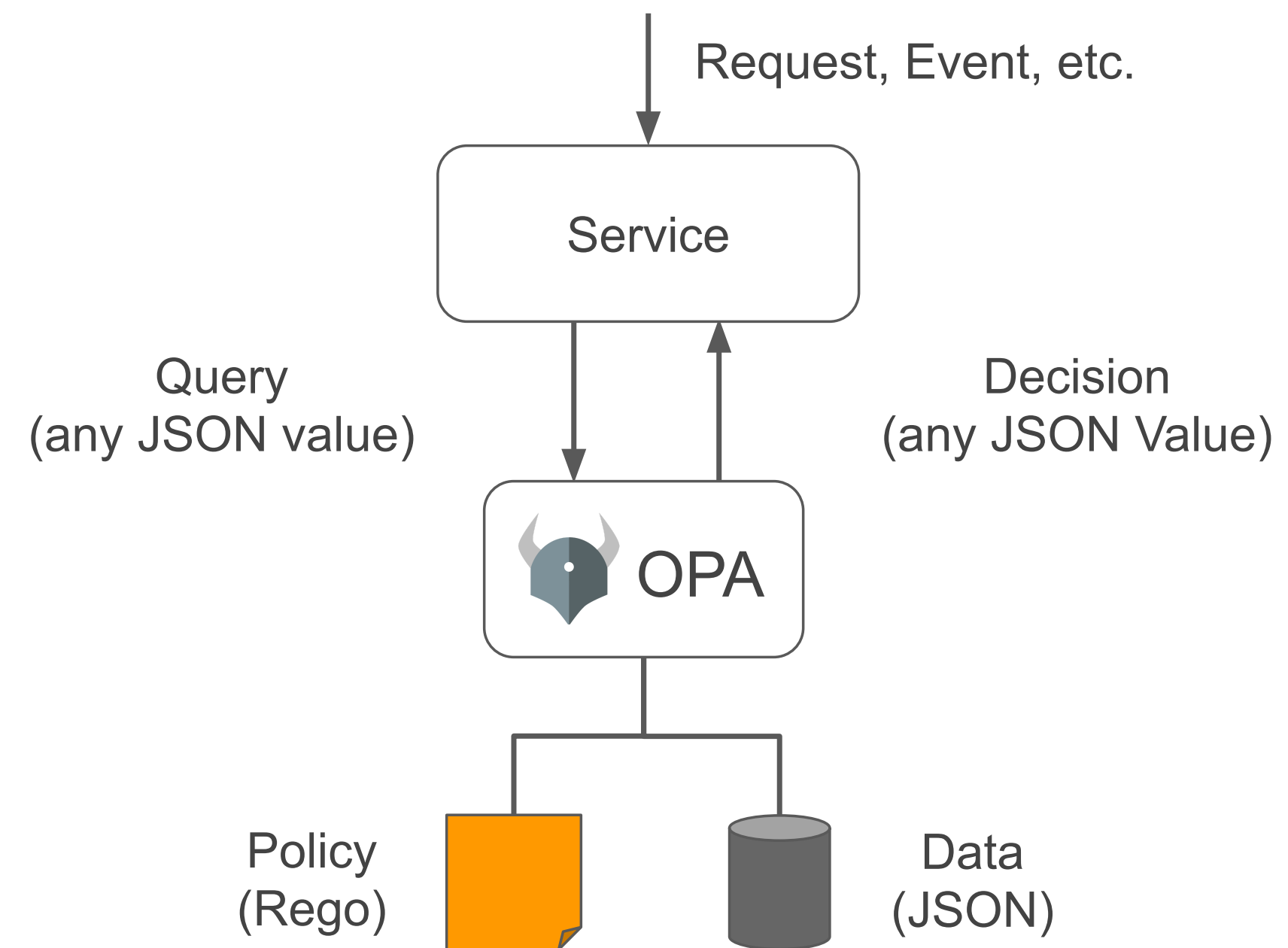
- Scripting language embedded

Policy-as-a-code

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

Open Policy Agent

1. Rego -
query/transformation
language;
2. Works on loosely
structured
3. JSON support



Open Policy Agent



Created by



openpolicyagent.org



Demo

play.openpolicyagent.org

Demo

Input:

```
{  
  "session": {  
    "login": "natalia12",  
    "teams": ["Platform"],  
    "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[_] == "Platform" }
allow { teams[_] == "Engineering" }
deny  { not input.session.member }
```

Rego

- Readable and easier for non-programmers*;
- Declarative;
- Inspired by [Datalog](#);
- Safe and guaranteed to terminate.

Rego

- Build-in functions ([docs](#)):
`sort, array.concat, json.filter,`
`strings.any_suffix_match, ...;`
- You can add your own functions.

Demo

Data - global values:

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

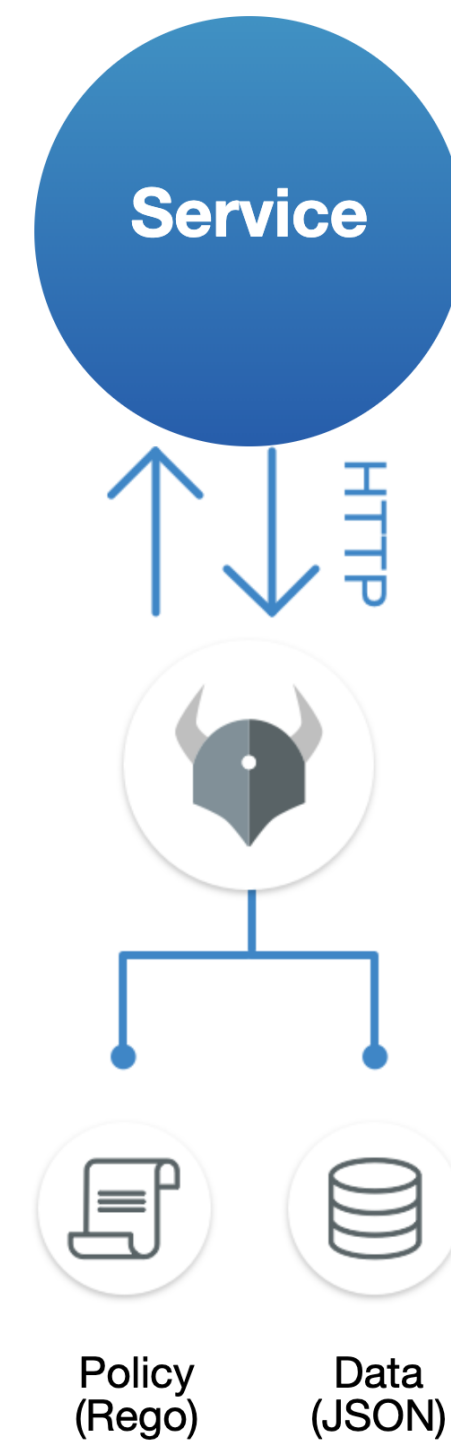
Demo

More complex examples:

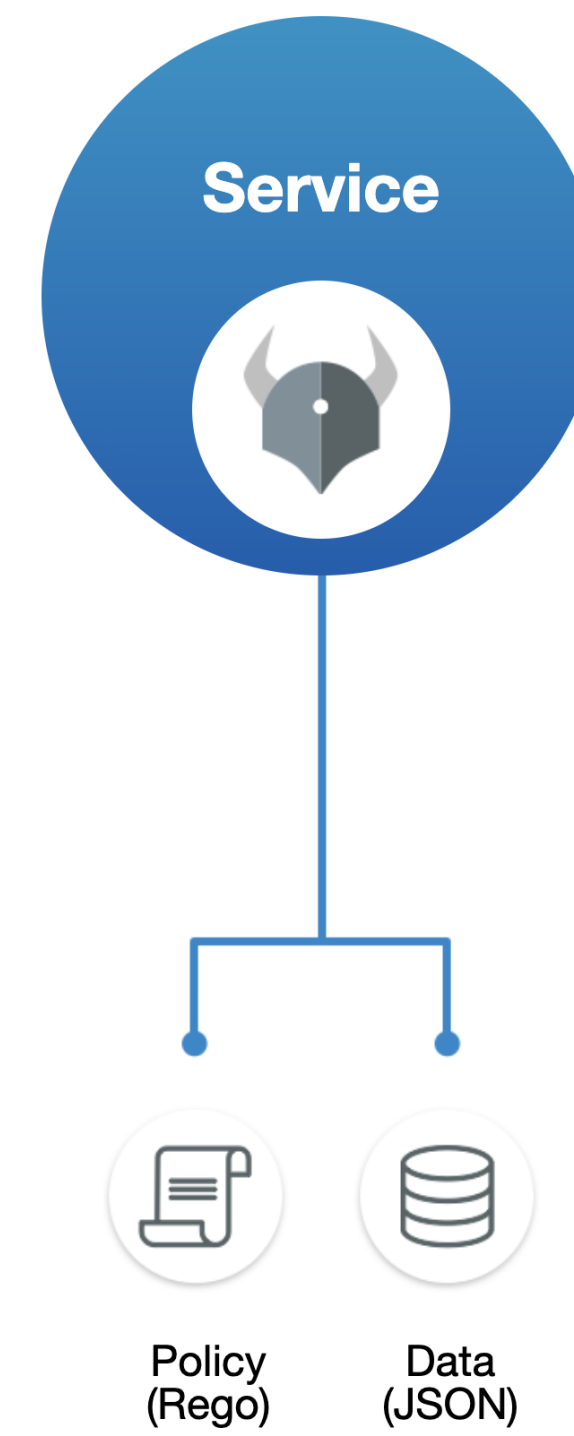
- Login & time restriction
- Approve
- Plan
- rule for conftest
- .. can get complex

Your app/tool

Daemon



Library



Library: Golang & Wasm (experimental).

Golang & OPA

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

See [docs](#).

Golang & OPA

Let's dive into the code.

Golang & OPA

Security:

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

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


Golang & OPA

Custom functions:

```
r := rego.New(  
    rego.Query(`x = hello("natalia")`),  
    rego.Function1(  
        &rego.Function{  
            Name: "hello",  
            Decl: types.NewFunction(types.Args(types.S), types.  
        },  
        func(_ rego.BuiltinContext, a *ast.Term) (*ast.Term, error) {  
            if str, ok := a.Value.(ast.String); ok {  
                return ast.StringTerm("hello, " + string(str))  
            }  
            return nil, nil  
        })  
    )  
)
```

Lessons learnt

Open Policy Agent:

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

Lessons learnt

Rego requires 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

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>

DX, Platform & infa teams

- Enforce best practices
- Encourage other teams to contribute

see e.g, [confest](#)



Thank you. Questions?

Wojciech Barczynski
wojciechb@spacelift.io

github:
[wojciech12/talk_policies_for_your_apps_with_OpenPolicyAgent](https://github.com/wojciech12/talk_policies_for_your_apps_with_OpenPolicyAgent)



Hiring

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

Backup *slides*

Checkers & linters

Kubernetes, Terraform, and many others:

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

Alternatives

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