Open Policy Agent

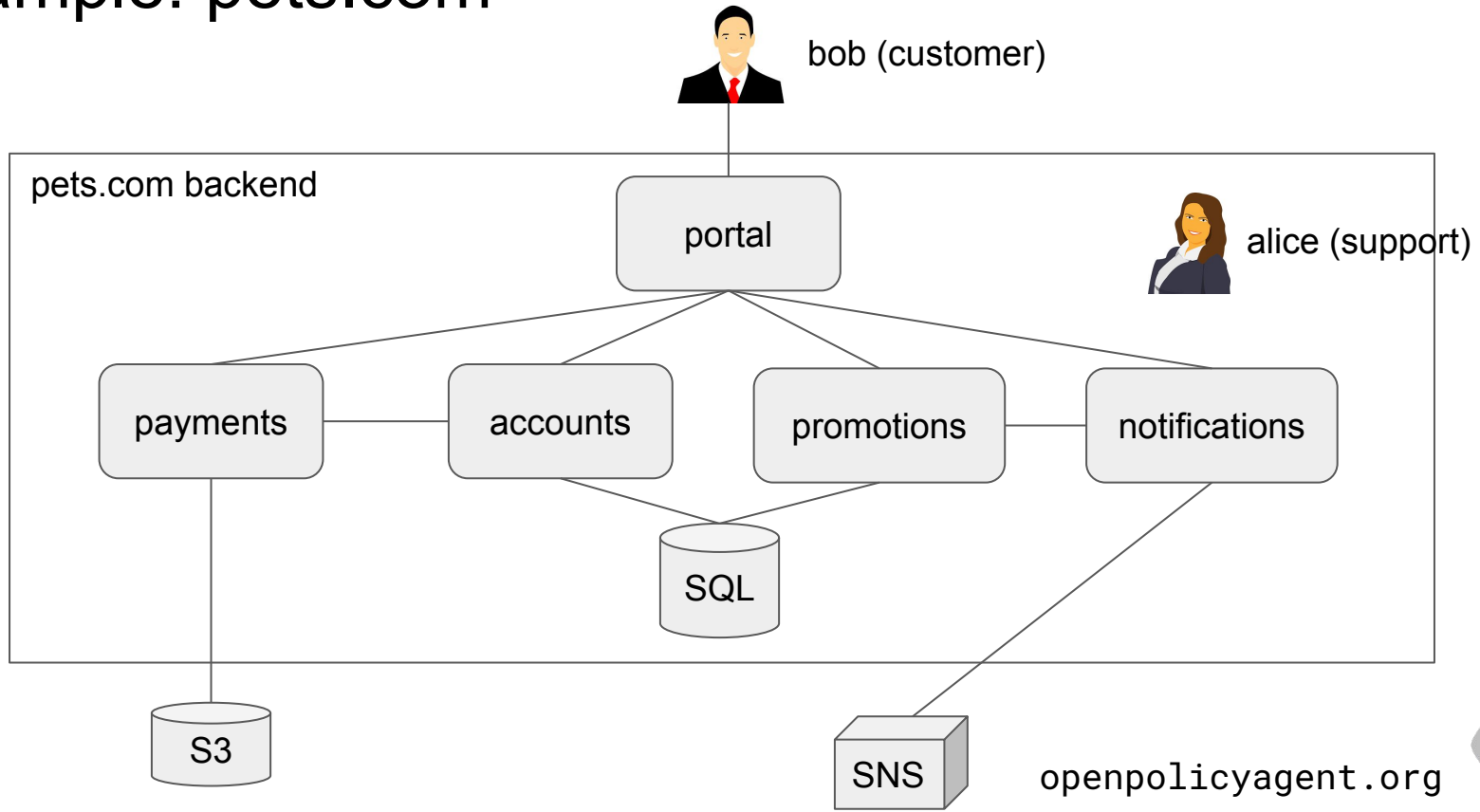
Deep Dive @ KubeCon Seattle 2018

who am I?

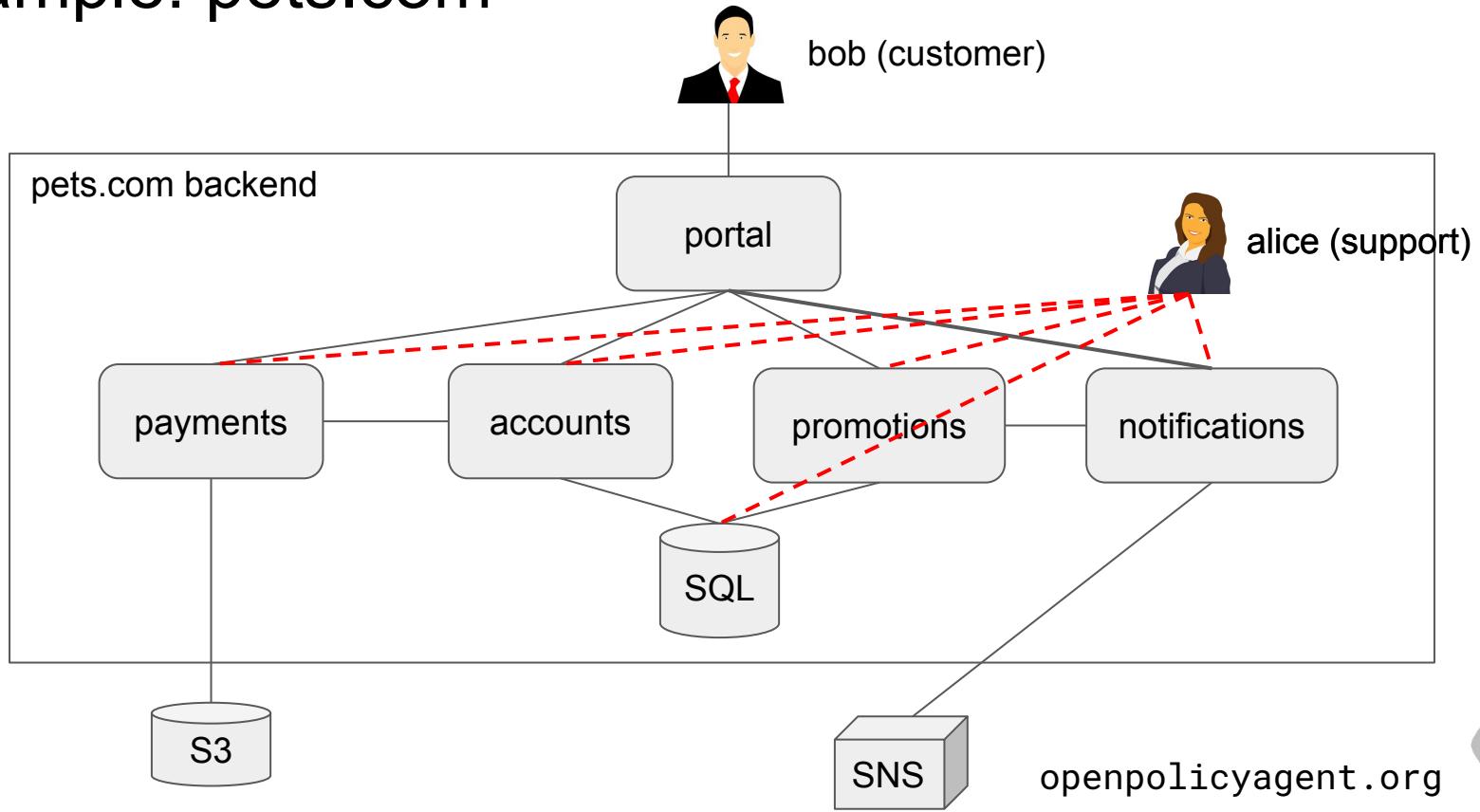
- Engineer @ Styra
- Co-founder of Open Policy Agent
- @sometorin
- Based in SF
- Happy to see some rain
    - Originally from Vancouver C A

openpolicyagent.org

Example: pets.com

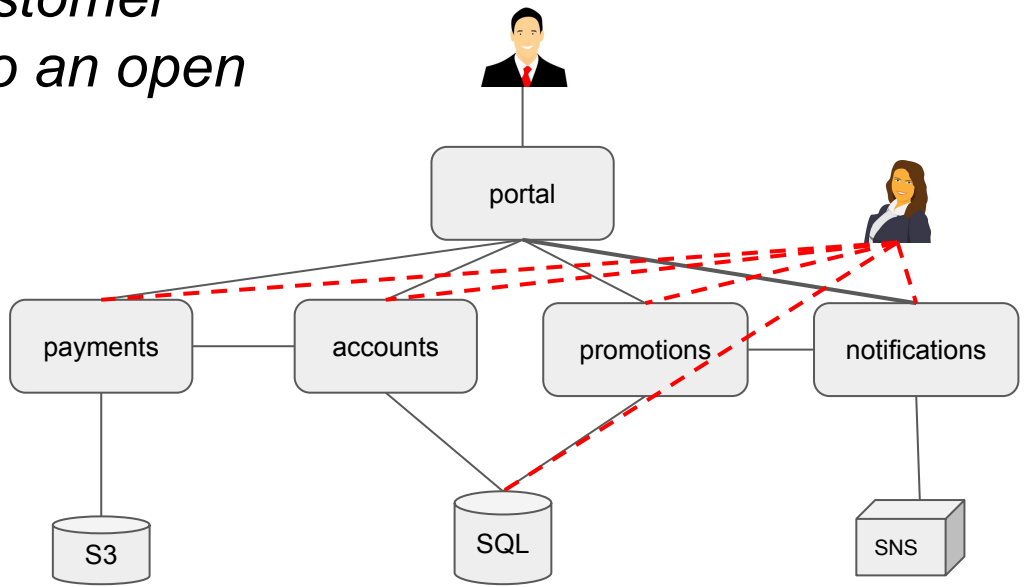


Example: pets.com



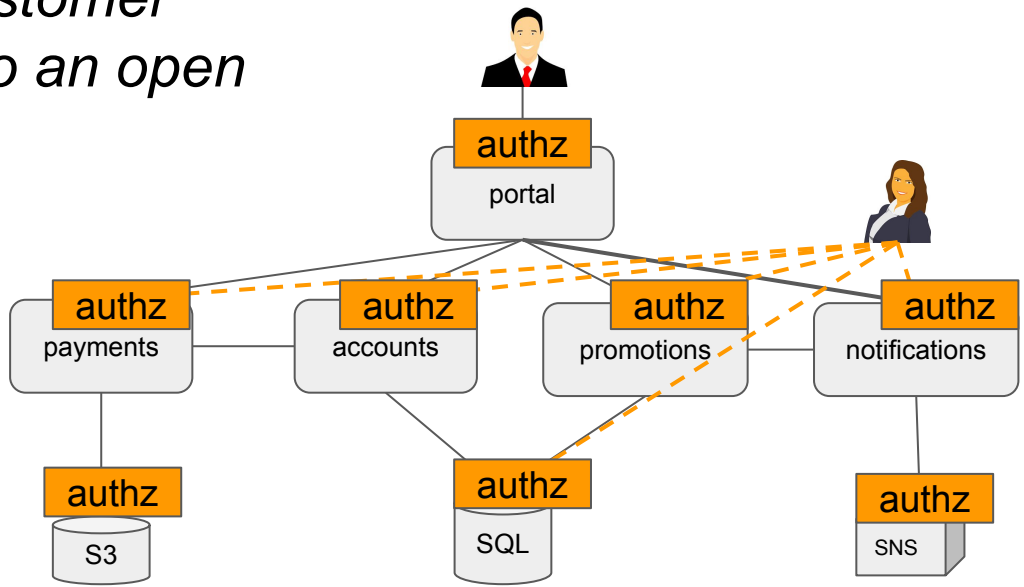
Example: pets.com

"Support staff can view customer data if they are assigned to an open ticket for that customer."



Example: pets.com

"Support staff can view customer data if they are assigned to an open ticket for that customer."

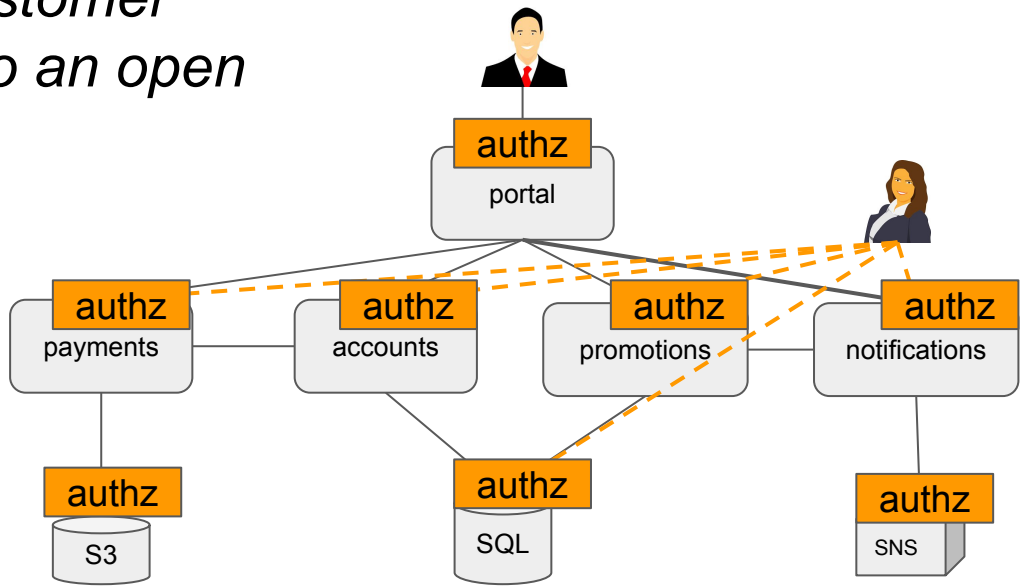


openpolicyagent.org

Example: pets.com

"Support staff can view customer data if they are assigned to an open ticket for that customer."

- How do you enforce new policies from infosec, compliance, or legal?
- How do you delegate control to your end-users?
- How do you roll-out policy changes?
- How do you leverage context, e.g., HR DB?
- How do you render UIs based on policy?
- How do you test your policies for correctness?
- What about 100+ services written in Java, Ruby, ...



openpolicyagent.org

OPA: General-purpose policy engine

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

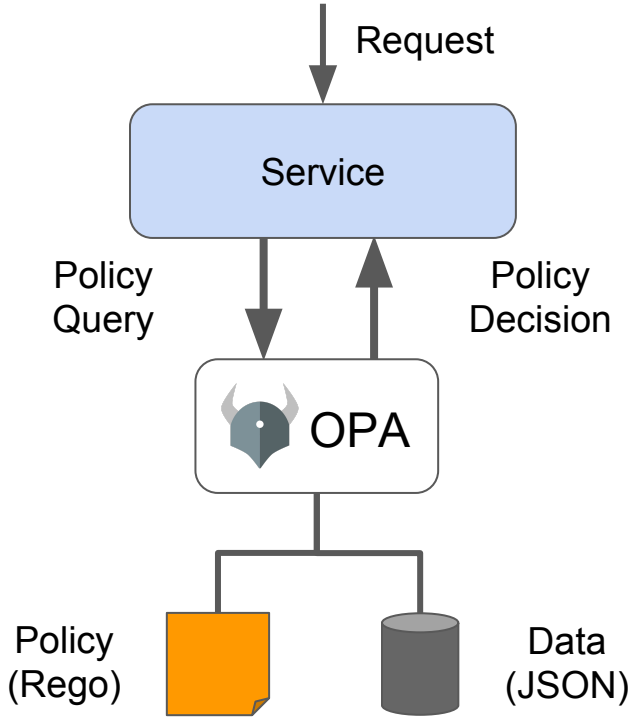
Today

CNCF project (Sandbox)

36 contributors
400 slack members
1.6K stars
20+ integrations

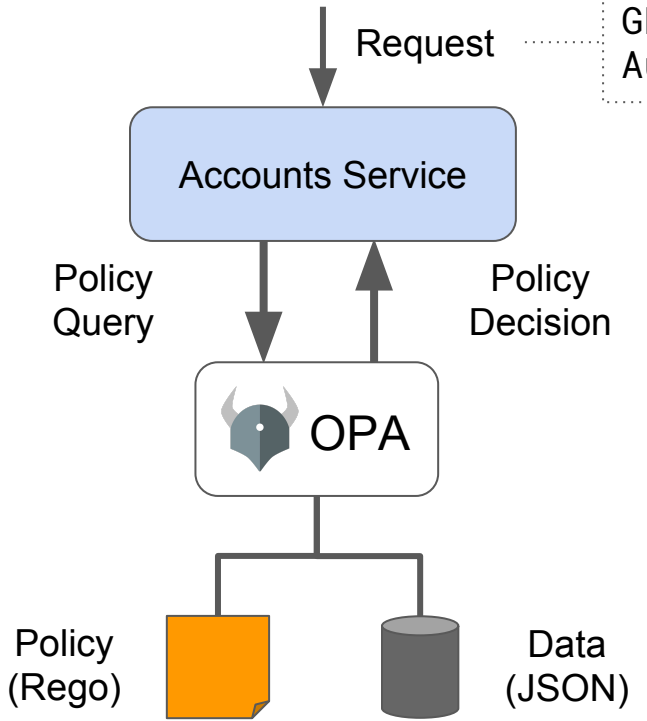
How does OPA work?

OPA: General-purpose policy engine



openpolicyagent.org

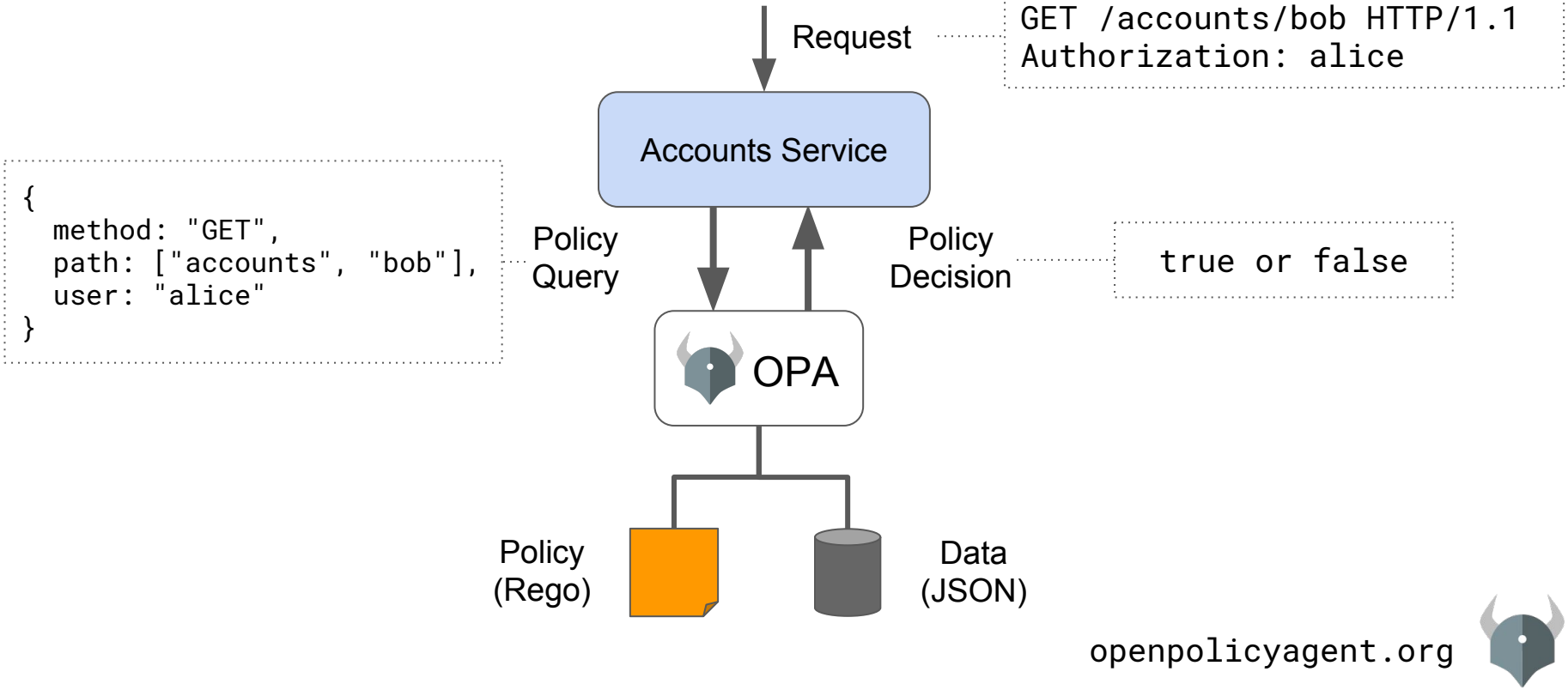
OPA: General-purpose policy engine




```
GET /accounts/bob HTTP/1.1
Authorization: alice
```

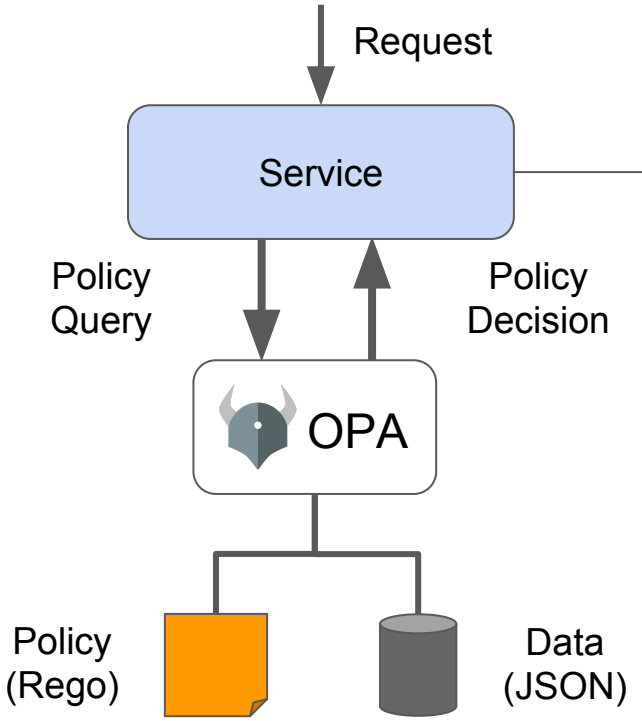
openpolicyagent.org

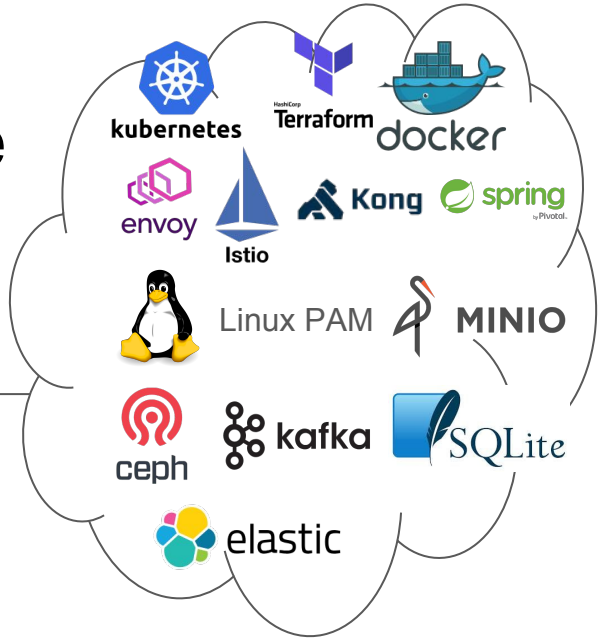
OPA: General-purpose policy engine



openpolicyagent.org

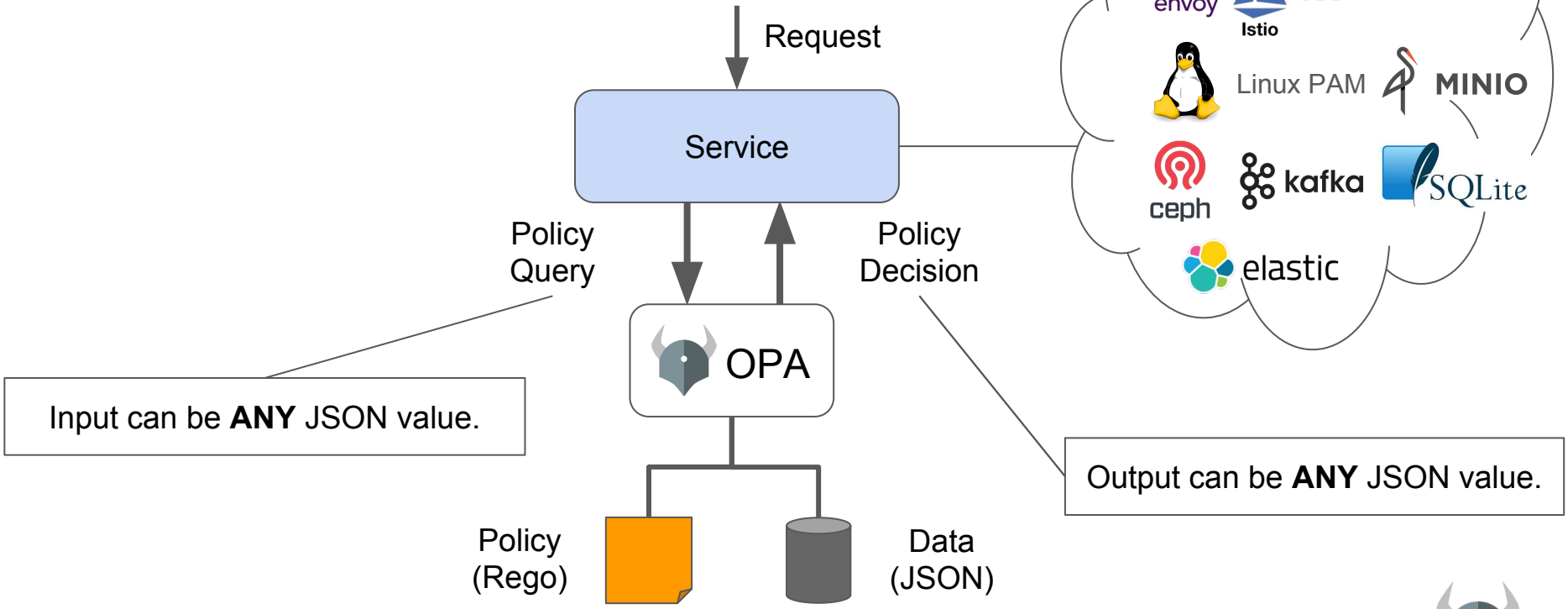
OPA: General-purpose policy engine





openpolicyagent.org

OPA: General-purpose policy engine

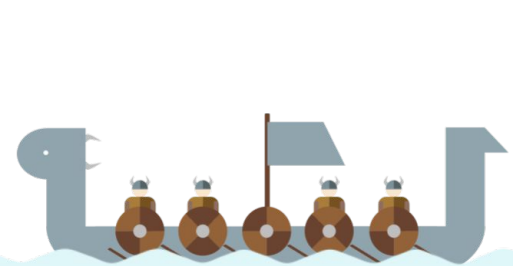


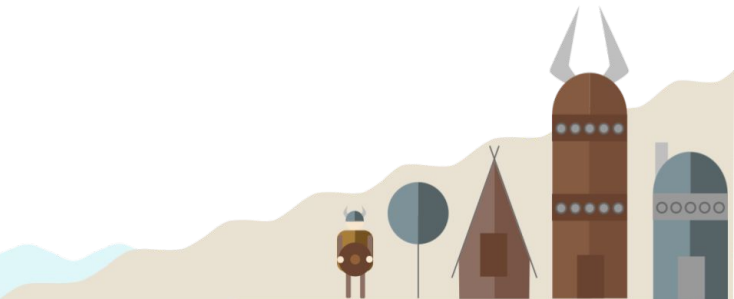
openpolicyagent.org

Hands on!

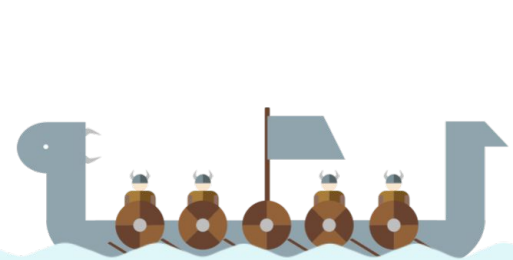
Example Policy

1. Users can view their own accounts.
2. Support can view accounts if they are assigned to an open ticket on that account.



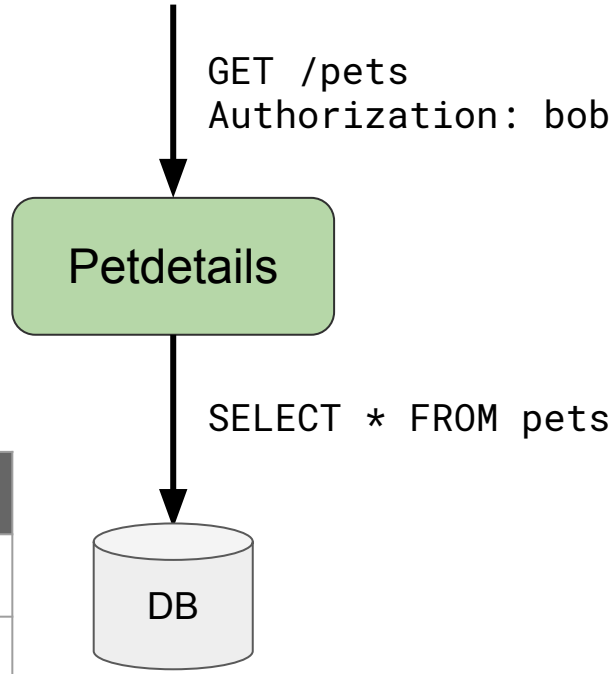


New features & use cases



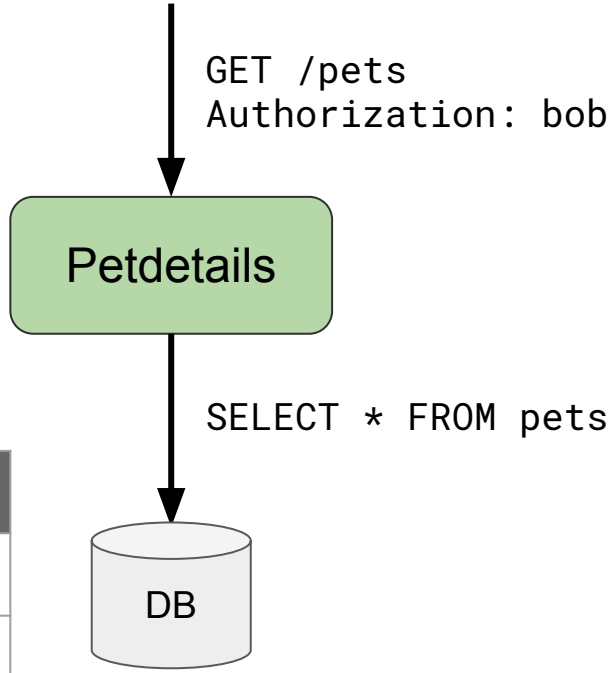
OPA & Data Filtering

Example Scenario



name	owner	age
Fluffy	Bob	7
Muffin	Alice	3
King	Janet	12

Example Scenario



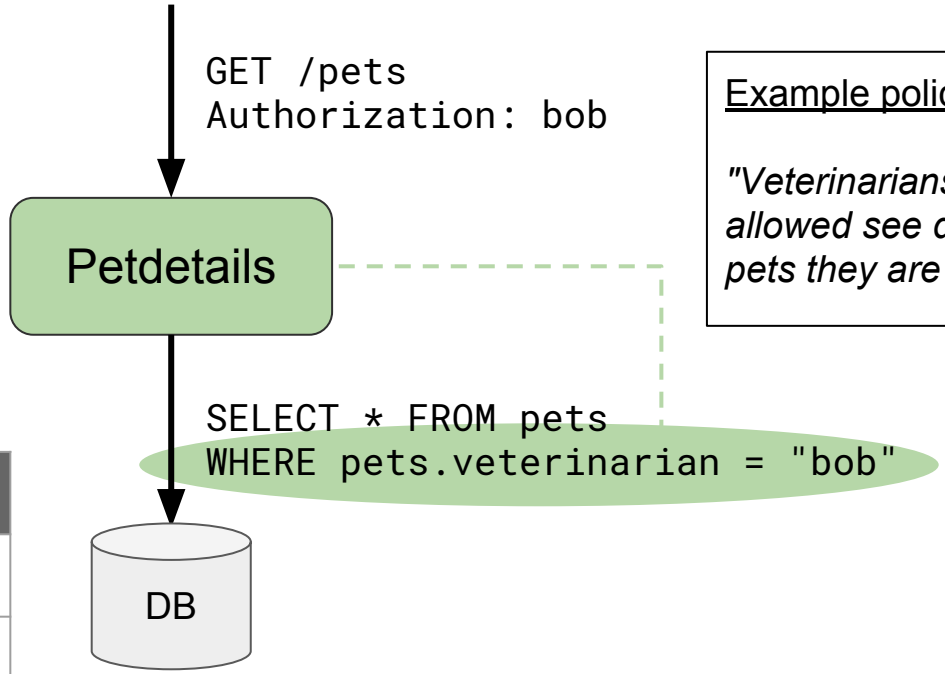
Example policy:

"Veterinarians are allowed see details of pets they are treating."

name	owner	age
Fluffy	Bob	7
Muffin	Alice	3
King	Janet	12

openpolicyagent.org

Example Scenario



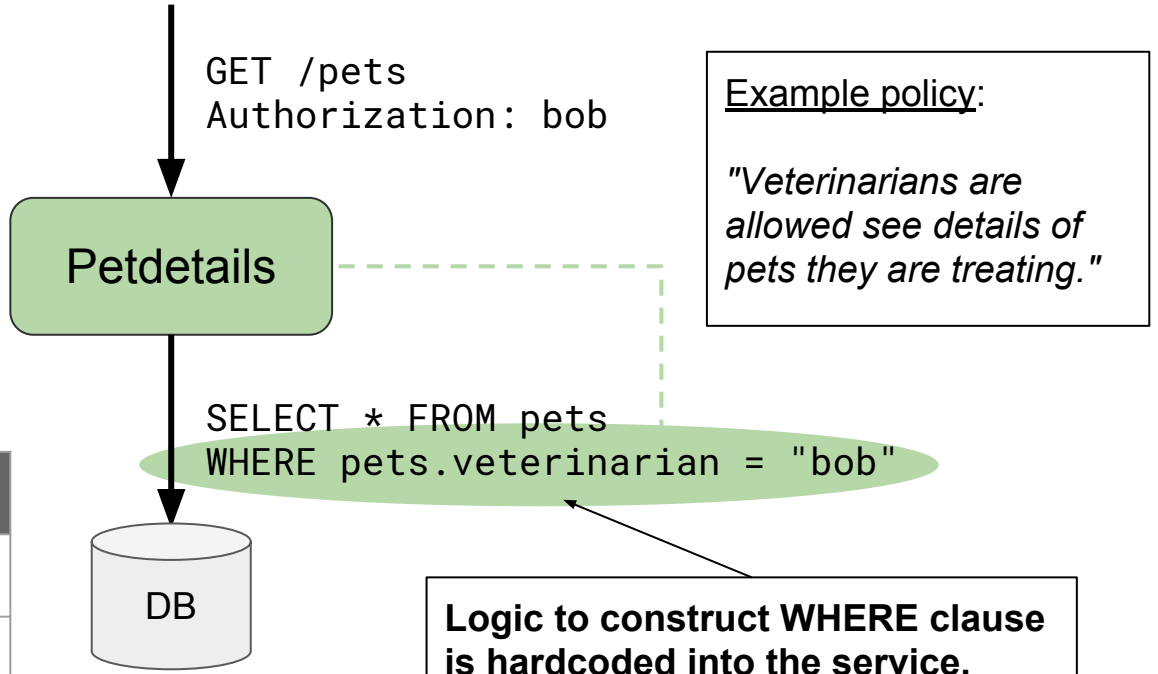
Example policy:

"Veterinarians are allowed see details of pets they are treating."

name	owner	age
Fluffy	Bob	7
Muffin	Alice	3
King	Janet	12

openpolicyagent.org

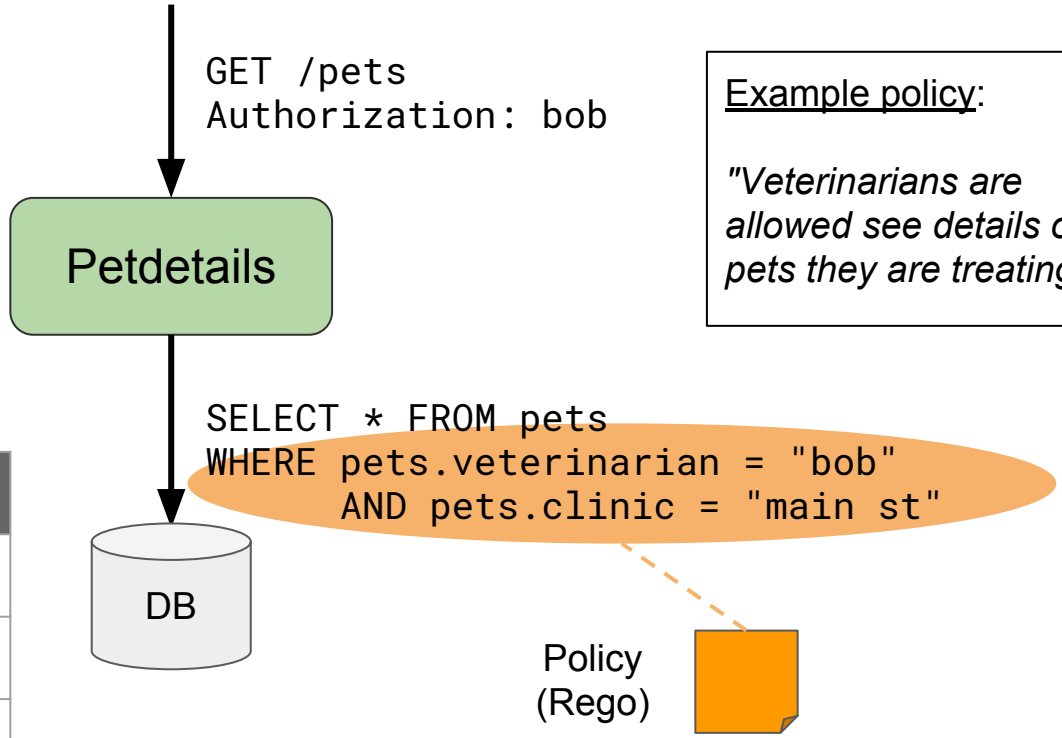
Example Scenario



name	owner	age
Fluffy	Bob	7
Muffin	Alice	3
King	Janet	12

openpolicyagent.org

Example Scenario



Example policy:

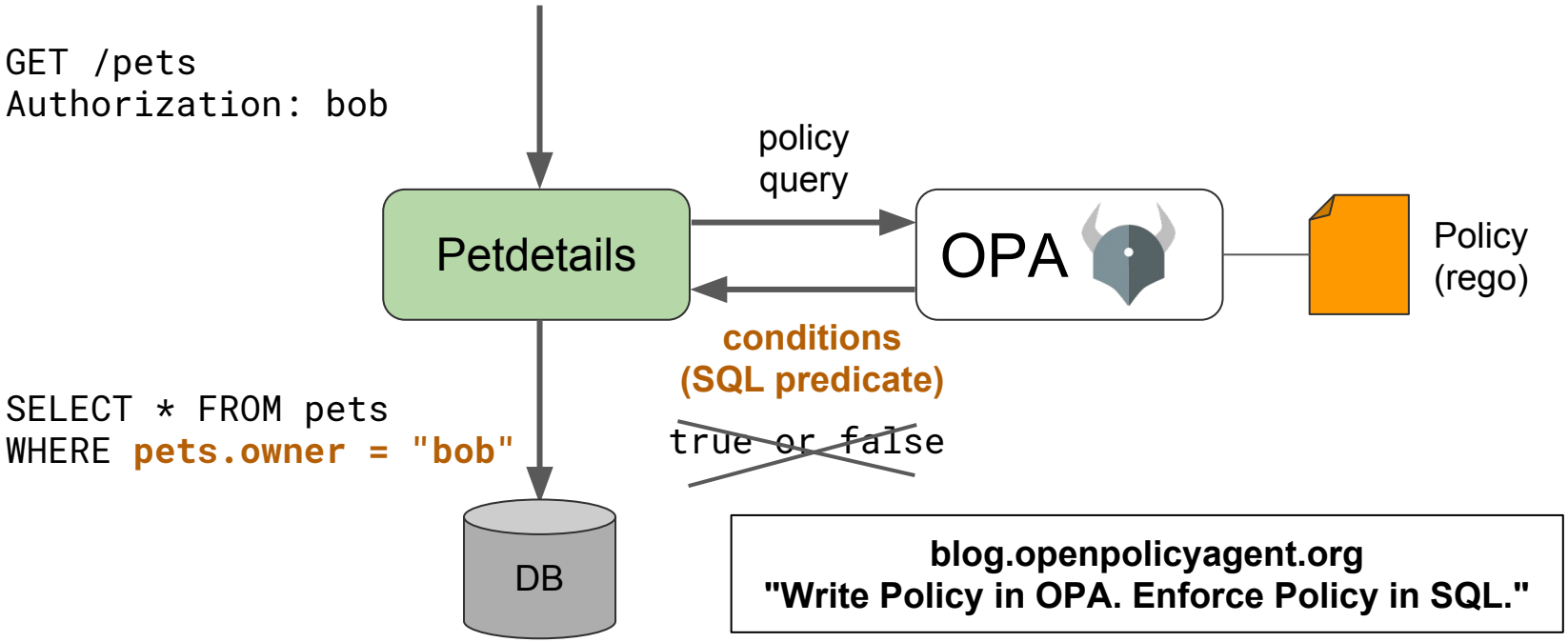
"Veterinarians are allowed see details of pets they are treating."

name	owner	age
Fluffy	Bob	7
Muffin	Alice	3
King	Janet	12

openpolicyagent.org

Demo

Partial Evaluation & SQL Translation



OPA & WebAssembly

What is WebAssembly (Wasm)?

- Binary instruction format for virtual machines
  - Safe, efficient, open
- Compilation target for C, C++, Rust, Go, ...
- Supported by Chrome, Safari, Firefox, and IE
- Non-web embeddings
  - IoT
  - Desktop/mobile
  - **Servers**
  - Blockchain!

What does Wasm have to do with OPA?

- Library integrations are simpler
  - Less overhead (performance)
  - Less operational complexity (security, monitoring)

- Some platforms are more likely to embed Wasm runtimes than OPA
  - Cloudflare announced support for Wasm workers earlier this year
  - Envoy considering including a Wasm runtime

- How do you enforce policies in serverless and edge computing environments?

Demo

Thank You!

slack.openpolicyagent.org

open-policy-agent/opa

tsandall/kubecon-seattle-2018

Contributing? Say hello! Or see low-hanging-fruit and help-wanted issues.

openpolicyagent.org