Open Policy Agent

Deep Dive @ KubeCon Barcelona 2019

Who Are We?

Tim Hinrichs

Co-founder & CTO at Styra
Co-creator of OPA

@tim on OPA
@tlhinrichs

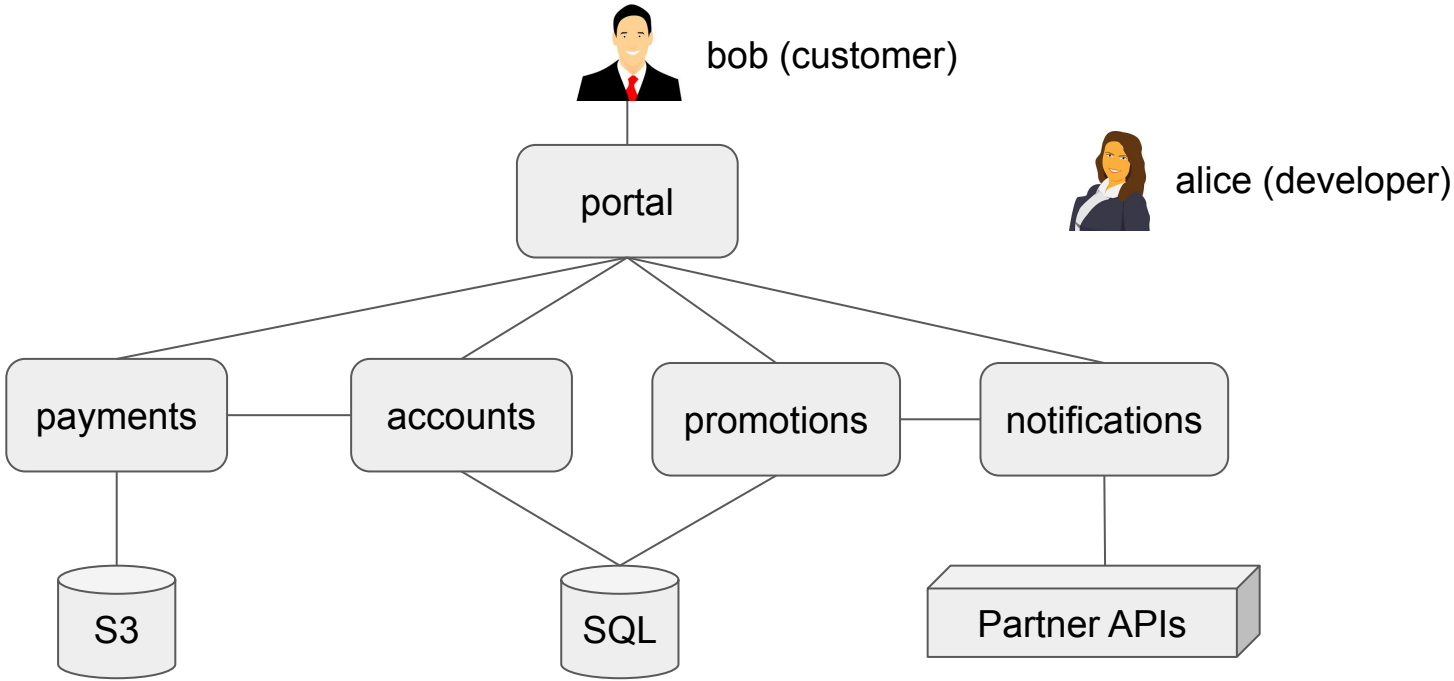
Torin Sandall

Engineer at Styra
Co-creator of OPA

@tsandall on OPA
@sometorin

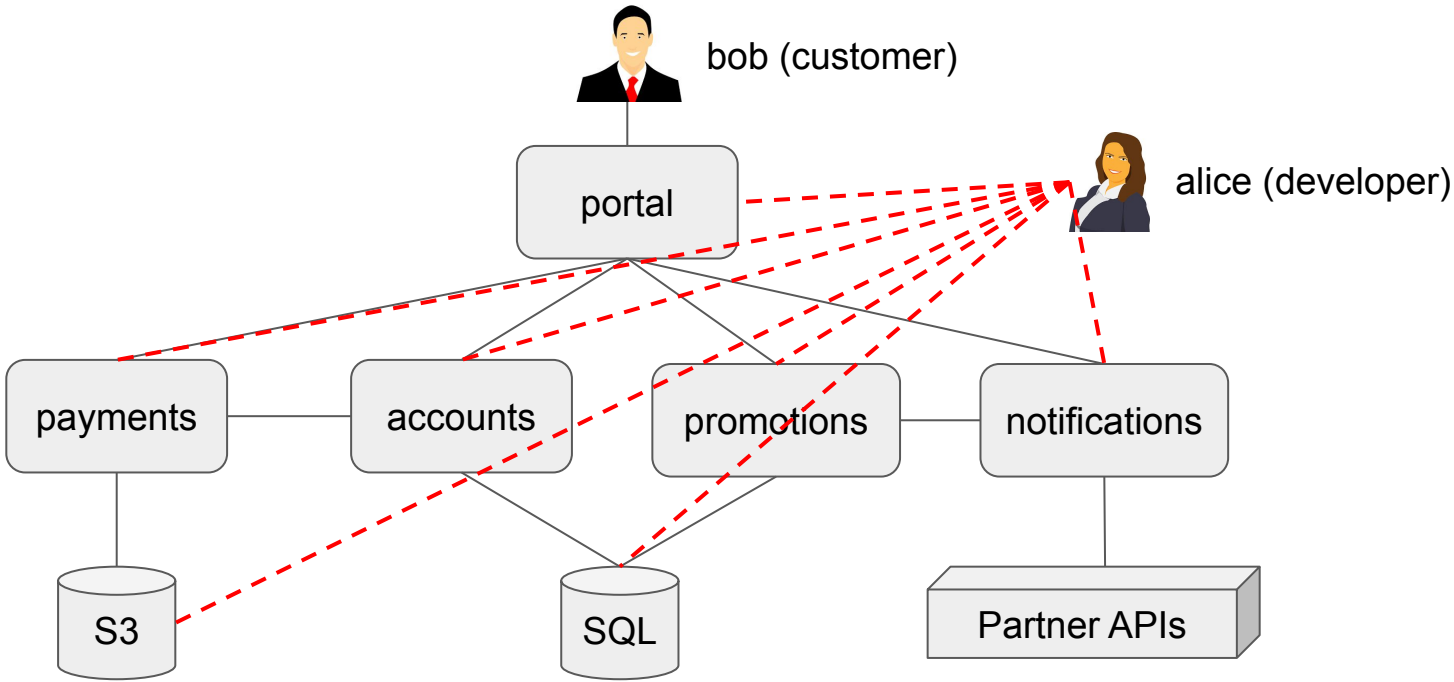
openpolicyagent.org

Example: Application



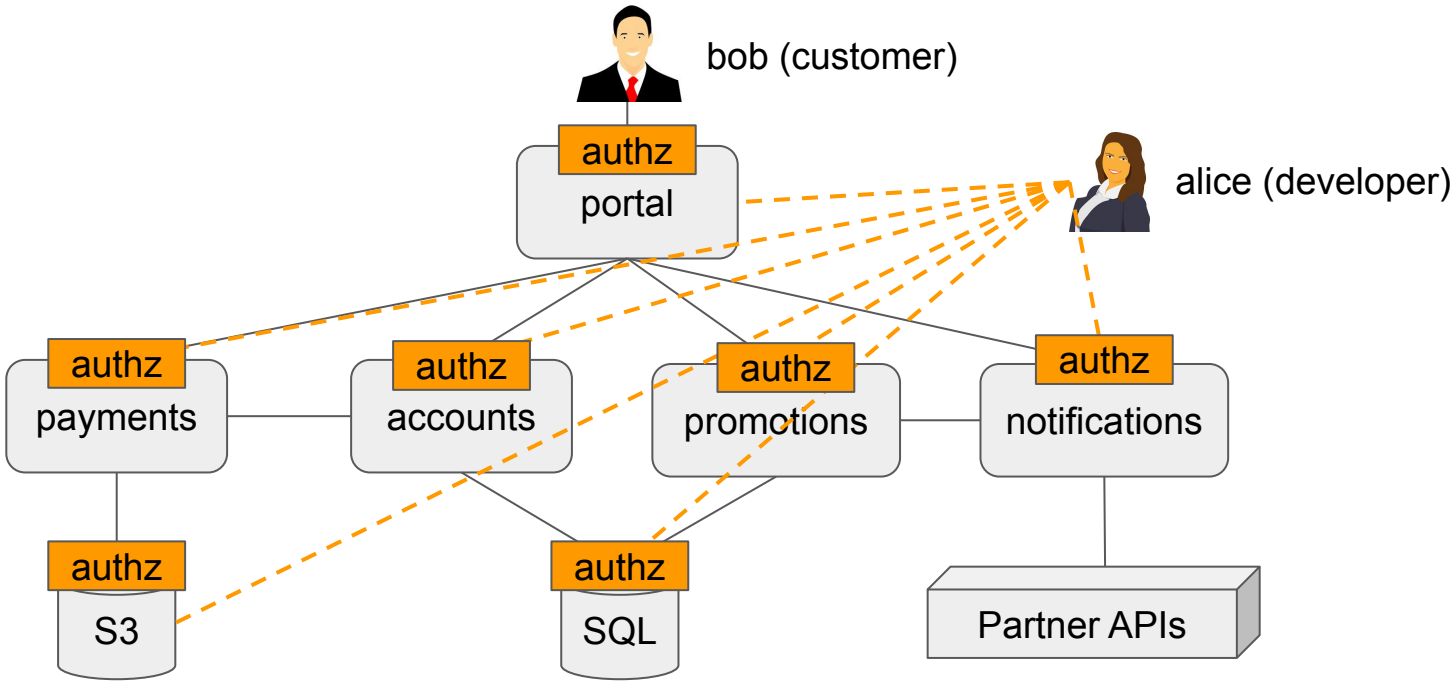
openpolicyagent.org

Example: Application



openpolicyagent.org

Example: Application

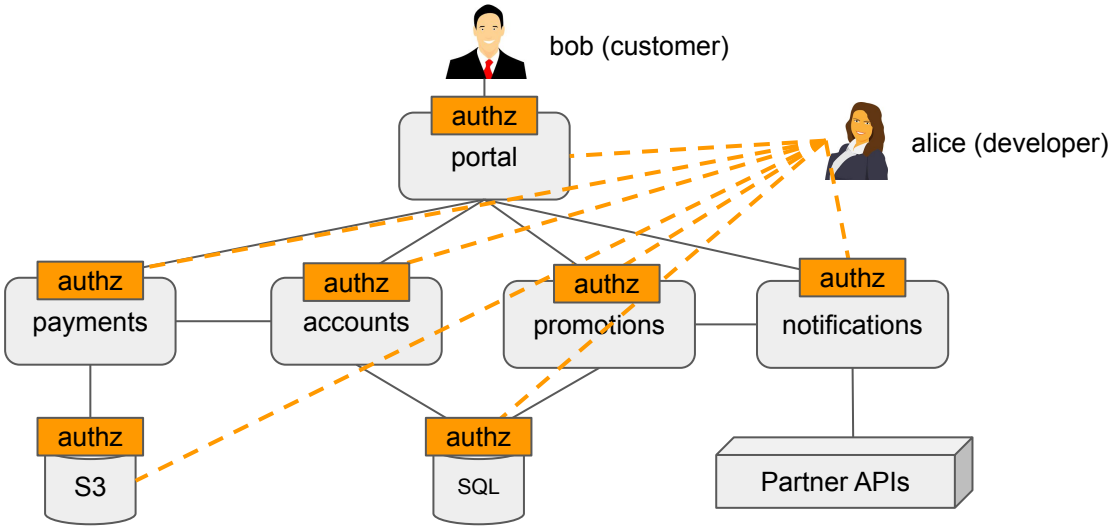


openpolicyagent.org

Example: Application

Obvious questions...

- 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/User 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

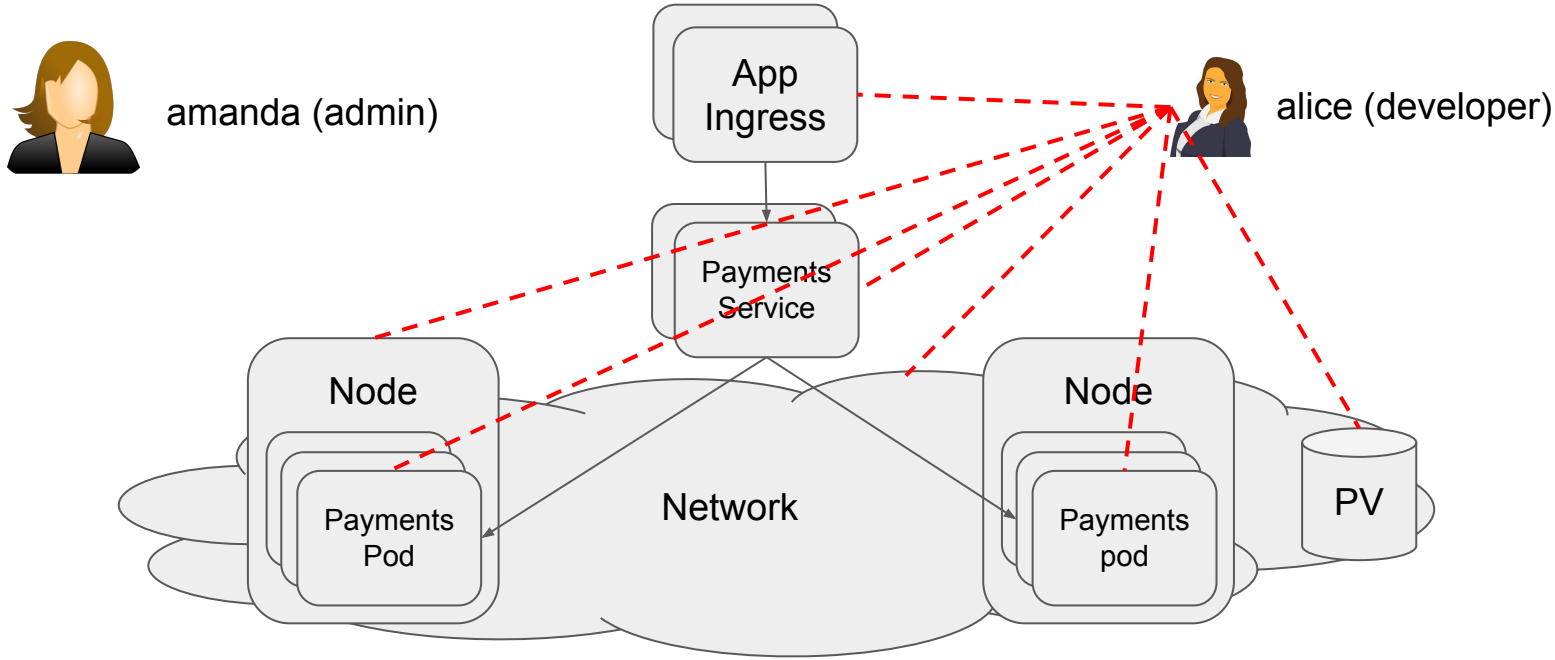
Example: Kubernetes Platform

amanda (admin)

alice (developer)

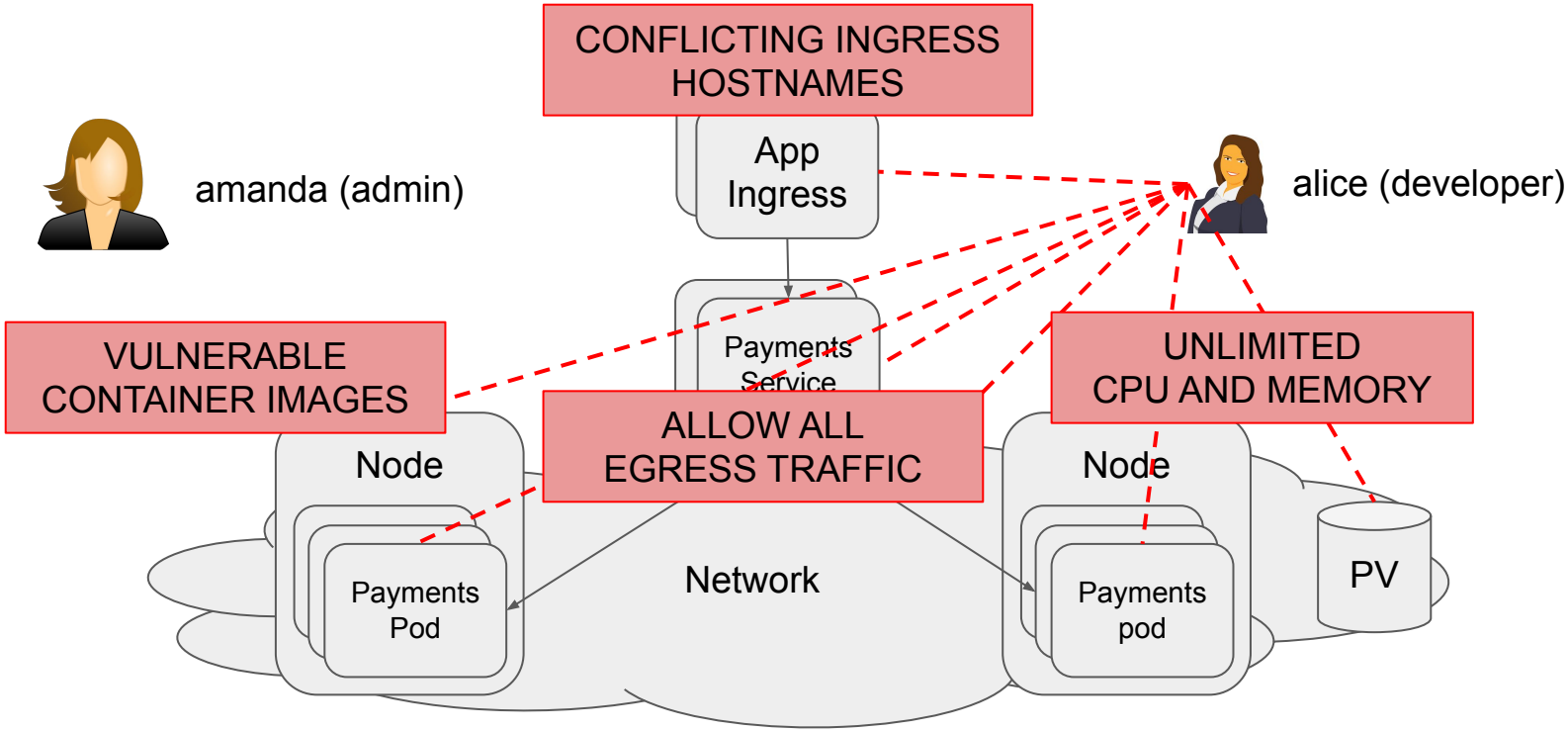
openpolicyagent.org

Example: Kubernetes Platform



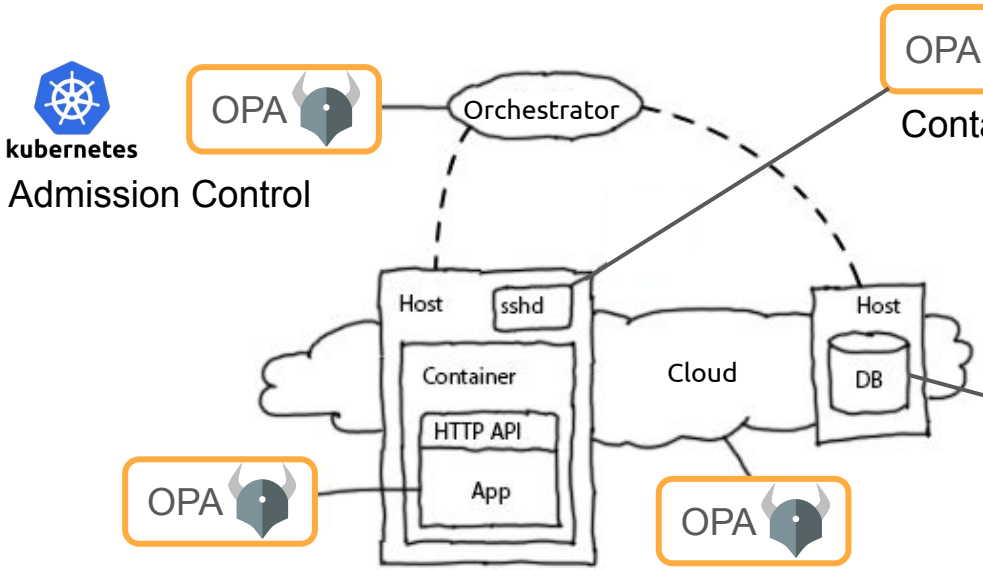
openpolicyagent.org

Example: Kubernetes Platform



openpolicyagent.org

OPA: Unified Policy Enforcement Across the Stack



kubernetes

Admission Control

OPA

Container Execution, SSH, sudo

docker

Linux

OPA

Data Protection & Data Filtering

ceph

kafka

MINIO

SQLite

elastic

OPA

Microservice APIs

OPA

Risk Management

Istio

LINKERD

spring

Kong

envoy

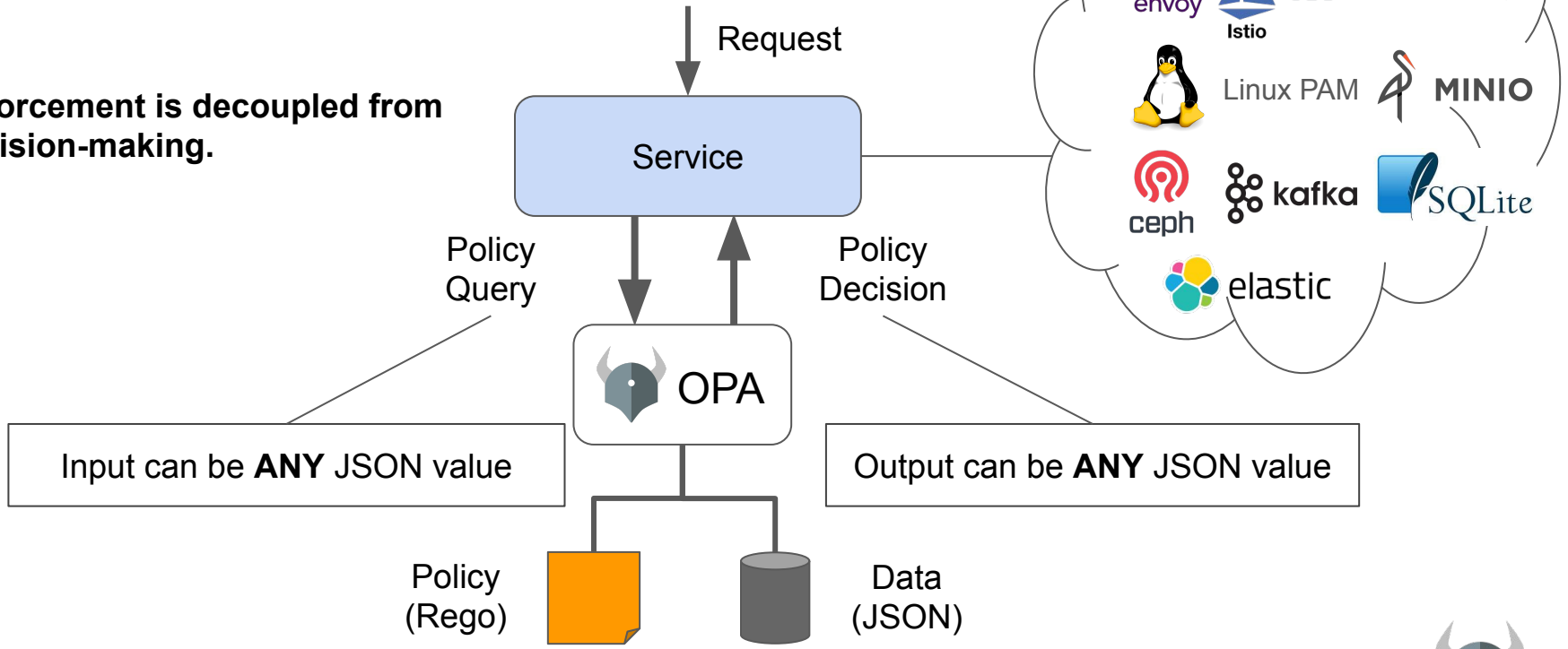
Terraform

Forseti Security

openpolicyagent.org

OPA: General-purpose Policy Engine

Enforcement is decoupled from decision-making.



openpolicyagent.org

Community Update

Community Growth

KubeCon Copenhagen May 2018

Joined CNCF Sandbox

410 commits (93% Styra)

~1,000 image pulls per week

200 slack users, 400 stars

KubeCon Barcelona May 2019

Promoted to CNCF Incubating 🎉

480 commits (75% Styra, 7% Chef, 5% Cisco, 13% other)

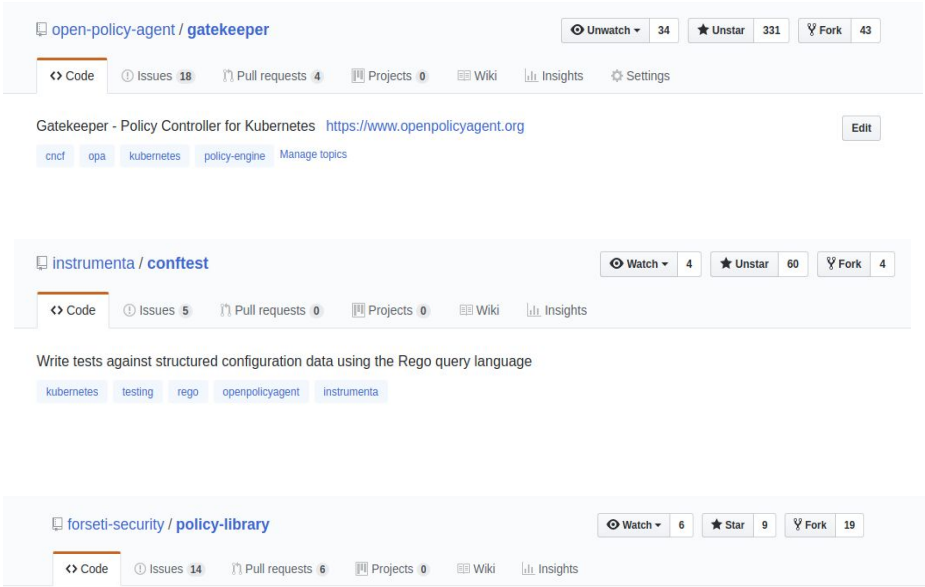
~25,000 image pulls per week

>800 slack users, >2,000 stars

~150 public repos containing .rego files

Community Highlights: Configuration Guardrails

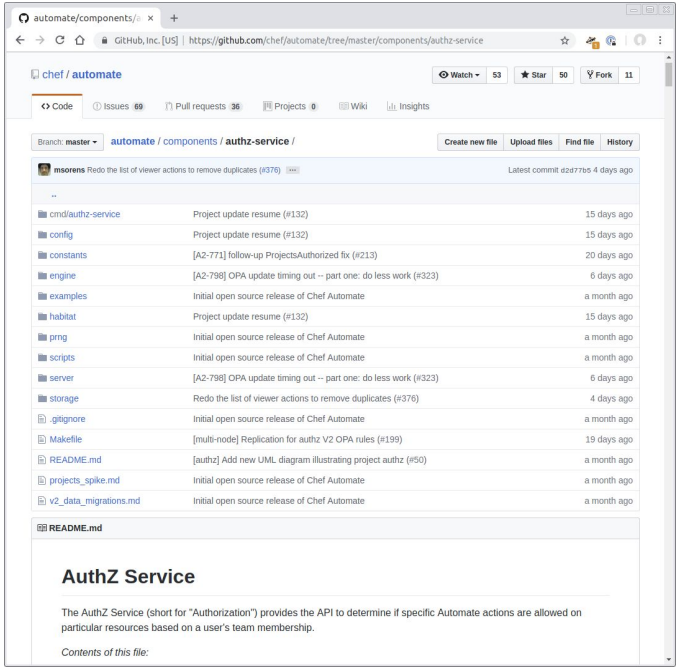
- Fine-grained policies for compute/network/storage resources.
  - Disallow ALLOW ALL egress traffic rules...
  - Require CPU & memory limits...
  - Prevent ingress conflicts...
  - Block public image registries…
- Kubernetes, GCP, Terraform, or any structured data (conftest)
- Duality: Enforcement/Audit



openpolicyagent.org

Community Highlights: Chef Automate IAM

- RBAC & Project-scope access control models
- Well-documented architecture
- Introspection (Who Can Do What?)
- Uses Partial Evaluation optimization



github.com/chef/automate/tree/master/components/authz-service

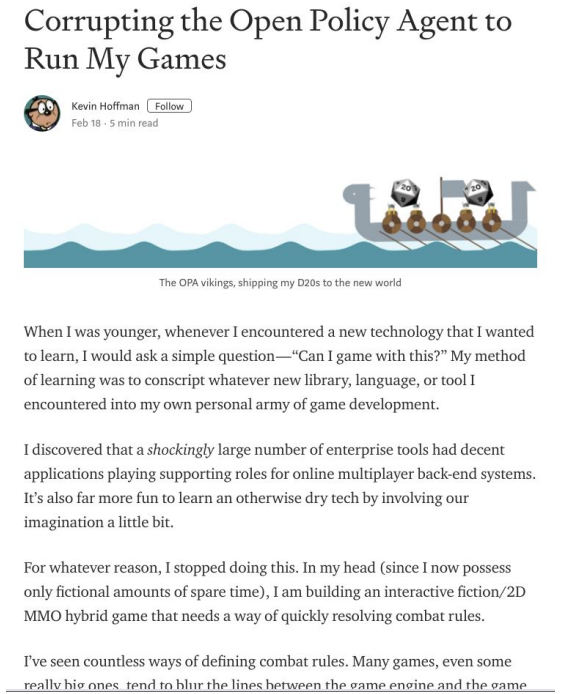
openpolicyagent.org

Community Highlights: RPG Engine

"OPA is like a 'deferred brain' to which I can pass relevant information and get decisions in return."

@KevinHoffman

Link: https://bit.ly/2M0AfB6



Corrupting the Open Policy Agent to Run My Games

Kevin Hoffman Follow
Feb 18 · 5 min read

The OPA vikings, shipping my D20s to the new world

When I was younger, whenever I encountered a new technology that I wanted to learn, I would ask a simple question—"Can I game with this?" My method of learning was to conscript whatever new library, language, or tool I encountered into my own personal army of game development.

I discovered that a *shockingly* large number of enterprise tools had decent applications playing supporting roles for online multiplayer back-end systems. It's also far more fun to learn an otherwise dry tech by involving our imagination a little bit.

For whatever reason, I stopped doing this. In my head (since I now possess only fictional amounts of spare time), I am building an interactive fiction/2D MMO hybrid game that needs a way of quickly resolving combat rules.

I've seen countless ways of defining combat rules. Many games, even some really big ones, tend to blur the lines between the game engine and the game

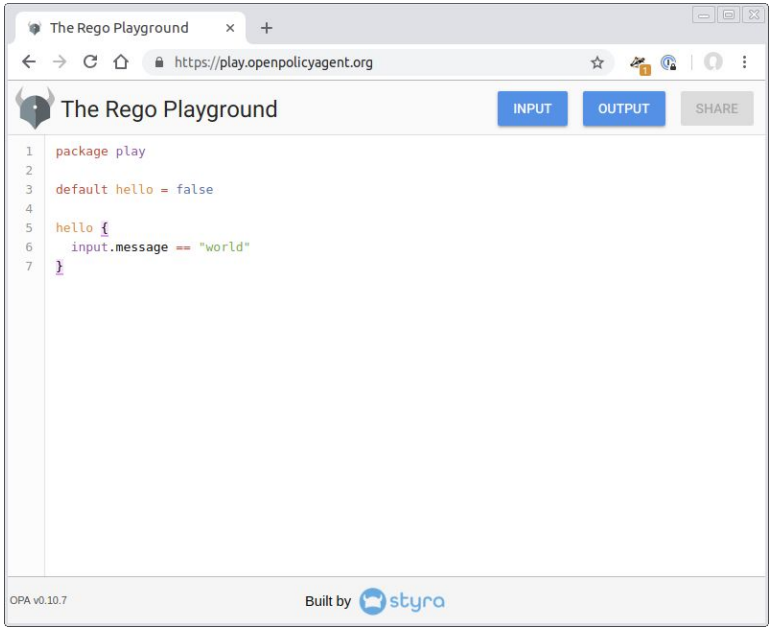
openpolicyagent.org

Recent Developments

play.openpolicyagent.org

- Experiment with policies in your browser
- Fast feedback loop
- Publish/share links to policy snippets

Example: https://play.openpolicyagent.org/p/16rXXc0HAF



v0.11: Improved Debugging: `notes` trace filter

- `trace(msg)` built-in function is useful for debugging purposes
- Problem: Default tracing output is extremely verbose
- New "notes" filter surfaces output and relevant context

Before

```
$ opa eval -d notes.rego 'data' -f pretty --explain=full
Enter data.kubecon.deep_dive = _
| Eval data.kubecon.deep_dive = _
| Index data.kubecon.deep_dive = _ (matched 1 rule)
| Enter data.kubecon.deep_dive
| | Eval data.kubecon.room_8_1_g3
| | Index data.kubecon.room_8_1_g3 (matched 1 rule)
| | Enter data.kubecon.room_8_1_g3
| | | Eval true
| | | Exit data.kubecon.room_8_1_g3
| | Eval data.kubecon.wednesday
| | Index data.kubecon.wednesday (matched 1 rule)
| | Enter data.kubecon.wednesday
| | | Eval true
| | | Exit data.kubecon.wednesday
| | Eval data.kubecon.time_is_11am
| | Index data.kubecon.time_is_11am (matched 1 rule)
| | Enter data.kubecon.time_is_11am
| | | Eval time.now_ns(__local3__)
| | | Eval time.clock(__local3__, __local4__)
| | | Eval [__local0__, __local1__, __local2__] = __local4__
| | | Eval sprintf("the time is %v:%v:%v", [__local0__, __local1__,
__local2__], __local5__)
| | | Eval trace(__local5__)
| | | Note "the time is 23:22:34"
```

After

```
$ opa eval -d notes.rego 'data' -f pretty --explain=notes
Enter data.kubecon.deep_dive = _
| Enter data.kubecon.deep_dive
| | Enter data.kubecon.time_is_11am
| | | Note "the time is 23:23:2"
undefined
```

openpolicyagent.org

v0.11: Language Improvements: some keyword

- By default variables capture globals
  - becomes a problem in large packages
  - := operator resolve this in many cases
  - some keyword handles remaining ones

Before

```
user = "alice"

allow {
    input.method = "GET"
    input.path = ["users", user]
    input.user = user
}
```

After

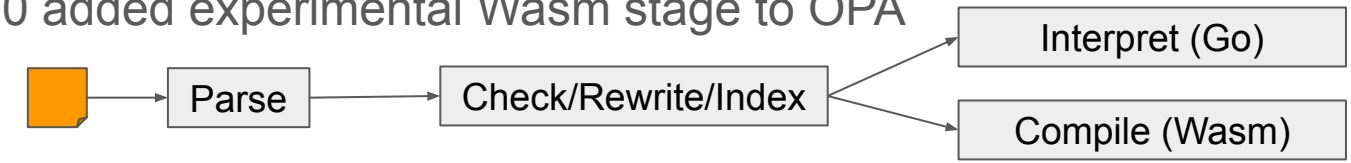
```
user = "alice"

allow {
    some user
    input.method = "GET"
    input.path = ["users", user]
    input.user = user
}
```

openpolicyagent.org

v0.11: Native Integrations: WebAssembly progress

- WebAssembly (Wasm) is an instruction format for virtual machines
  - Provides a safe/efficient/portable runtime for policy evaluation
  - Goal: enable library embeddings of OPA policies in any language/runtime

- v0.10 added experimental Wasm stage to OPA



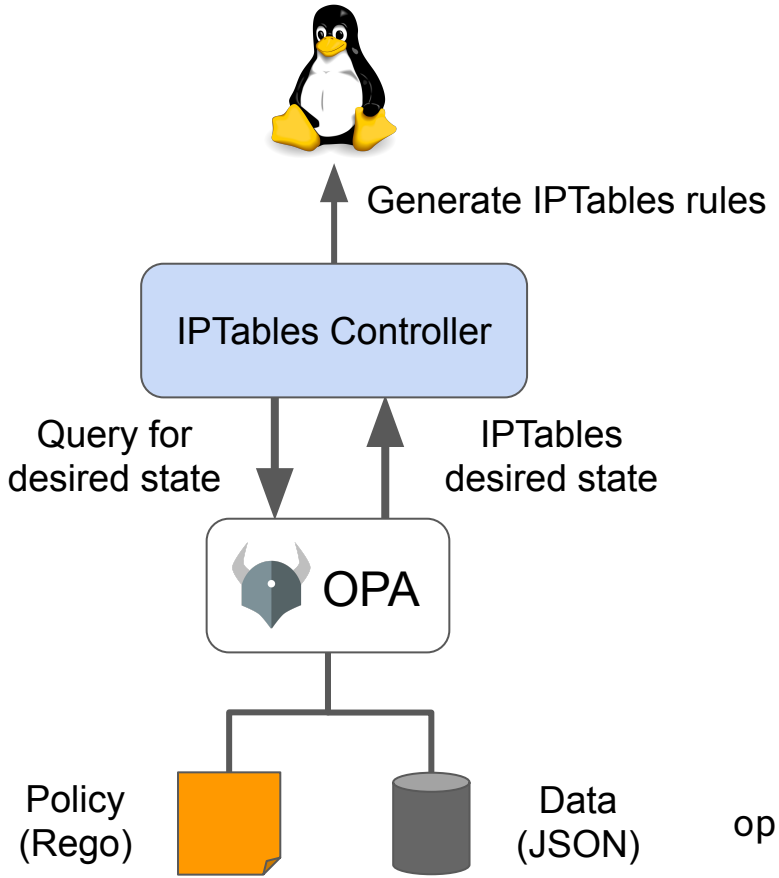
- v0.11 expands the fragment of Rego supported by the Wasm stage
  - All types of rules (ordered/unordered, default, partial sets/objects) now supported

- Example: open-policy-agent/contrib/wasm (CDN example)

Looking forward

Google Summer of Code: IPTables integration

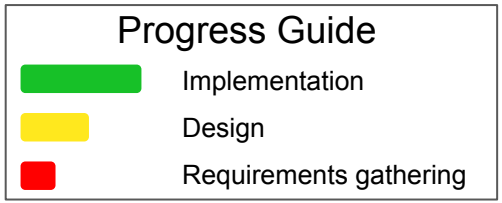
@Urvil Patel
@The Crushinator

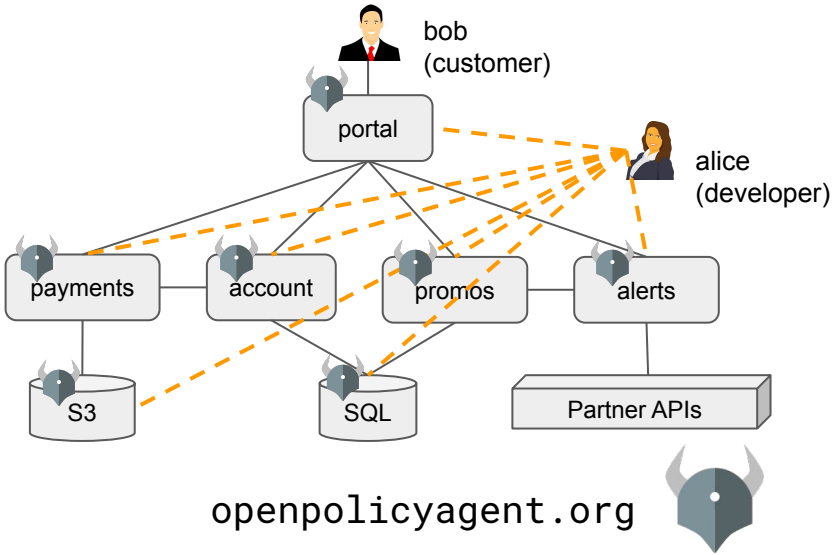


openpolicyagent.org

Use Case: Application & End-user Authorization

Questions	OPA Answers and Progress
How do you enforce new policies from infosec, compliance, or legal?	Policy-as-code
How do you delegate control to your end-users?	Hierarchical models Delegation models
How do you roll-out policy changes?	REST API, Bundle API
How do you leverage context, e.g., HR DB?	In-memory JSON data-store Data-filtering Data-fetching
How do you render UIs based on policy?	WASM compilation
How do you test your policies for correctness?	Unit tests
What about 100+ services written in Java, Ruby, ...	Daemon WASM compilation





Help Us Improve Discoverability

- More examples online
  - Policy libraries for Forseti and Gatekeeper help
- Slack and stackoverflow: better together
  - Slack is currently the primary medium for Q&A
  - Fast responses, >800 people
  - Not archived/searchable
  - Please start asking questions on Stack Overflow and tag with open-policy-agent

+

Tuesday, May 21

11:55	Unit Testing Your Kubernetes Configurations Using Open Policy Agent - Gareth Rushgrove, Docker
13:30	Meet The Maintainer: Open Policy Agent - Tim Hinrichs, Styra
14:00	Fine-Grained Permissions in Kubernetes: What's Missing, and How to Fix That - Vallery Lancey, Lyft & Seth McCombs, Triller (Description: open policy agent)
14:50	Intro: Open Policy Agent - Rita Zhang, Microsoft & Max Smythe, Google

Wednesday, May 22

11:05	Deep Dive: Open Policy Agent - Torin Sandall & Tim Hinrichs, Styra
13:30	Meet The Maintainer: Open Policy Agent - Patrick East, Styra
15:30	Meet The Maintainer: Open Policy Agent - Torin Sandall, Styra

Thursday, May 23

09:29	Keynote: From COBOL to Kubernetes: A 250 Year Old Bank's Cloud-Native Journey - Laura Rehorst, Product Owner - Stratus Platform, ABN AMRO Bank NV & Mike Ryan, DevOps Consultant, backtothelab.io (Description: open policy agent)
14:50	Protecting the Data Lake - Ash Narkar, Styra, Inc (Description: open policy agent)

Q&A

Torin Sandall

Engineer at Styra
Co-creator of OPA

@tsandall on OPA
@sometorin

Tim Hinrichs

Co-founder & CTO at Styra
Co-creator of OPA

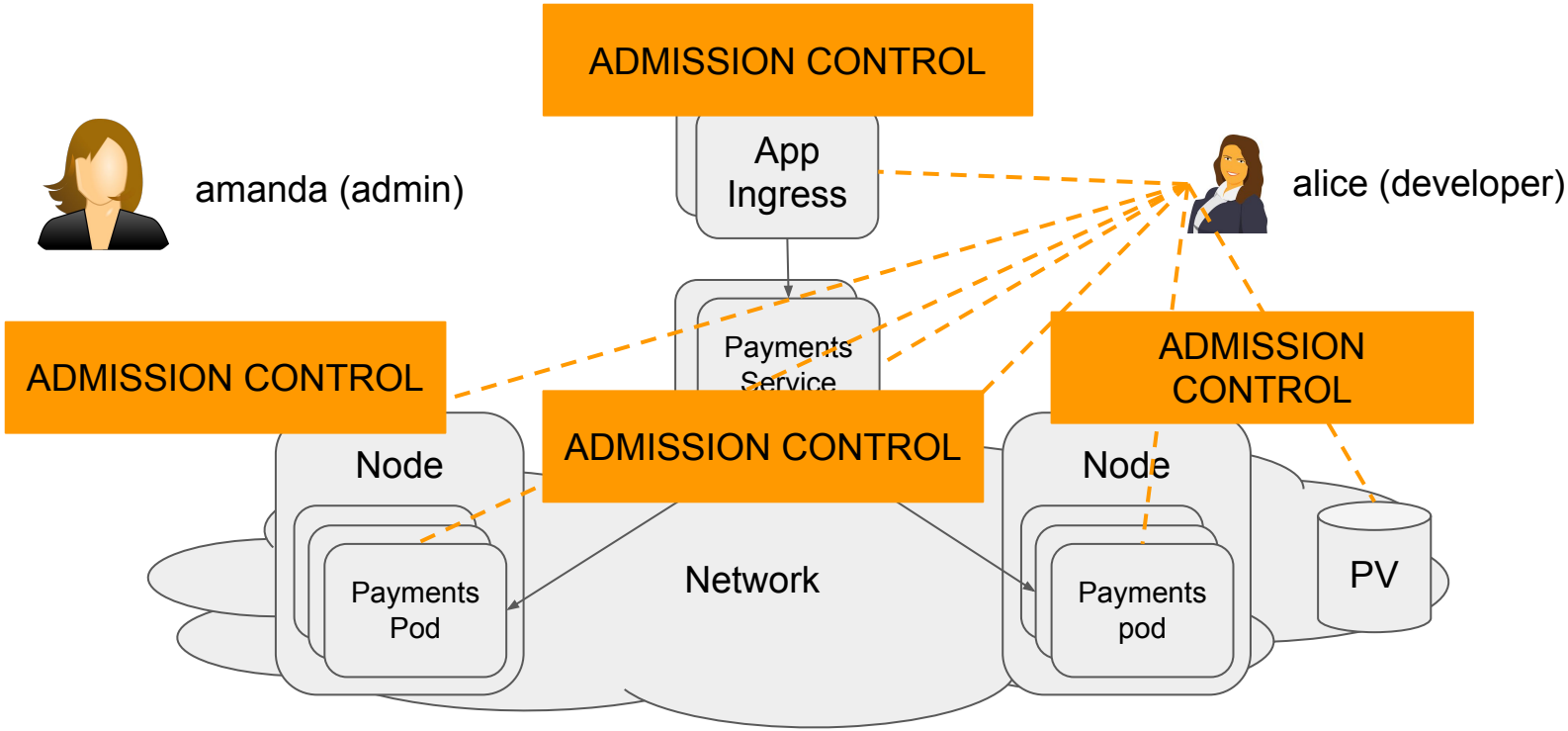
@tim on OPA
@tlhinrichs

openpolicyagent.org

v0.11: More Improvements

- Improved performance with Prepared queries
  - TODO add numbers
- Improved configuration override (--set=bundle.name:mybundle)
- New documentation!
  - Rego cheat sheet
  - Kubernetes admission control guide
  - FAQ updated with tips for
    - writing high performance policies
    - resolving safety errors
    - structuring policies
    - ...and more.

Example: Kubernetes Platform



openpolicyagent.org