SpringOne Platform by Pivotal

Policy Enforcement on Kubernetes with OPA

October 7–10, 2019
Austin Convention Center
Aleks Saul & Jaime Gonzalez Aguilar

Who we are

Aleks Saul
Sr. Platform Architect, Pivotal Inc.
@alekssaul

Jaime Gonzalez Aguilar
Advisory Platform Architect, Pivotal Inc.
@jaimegag

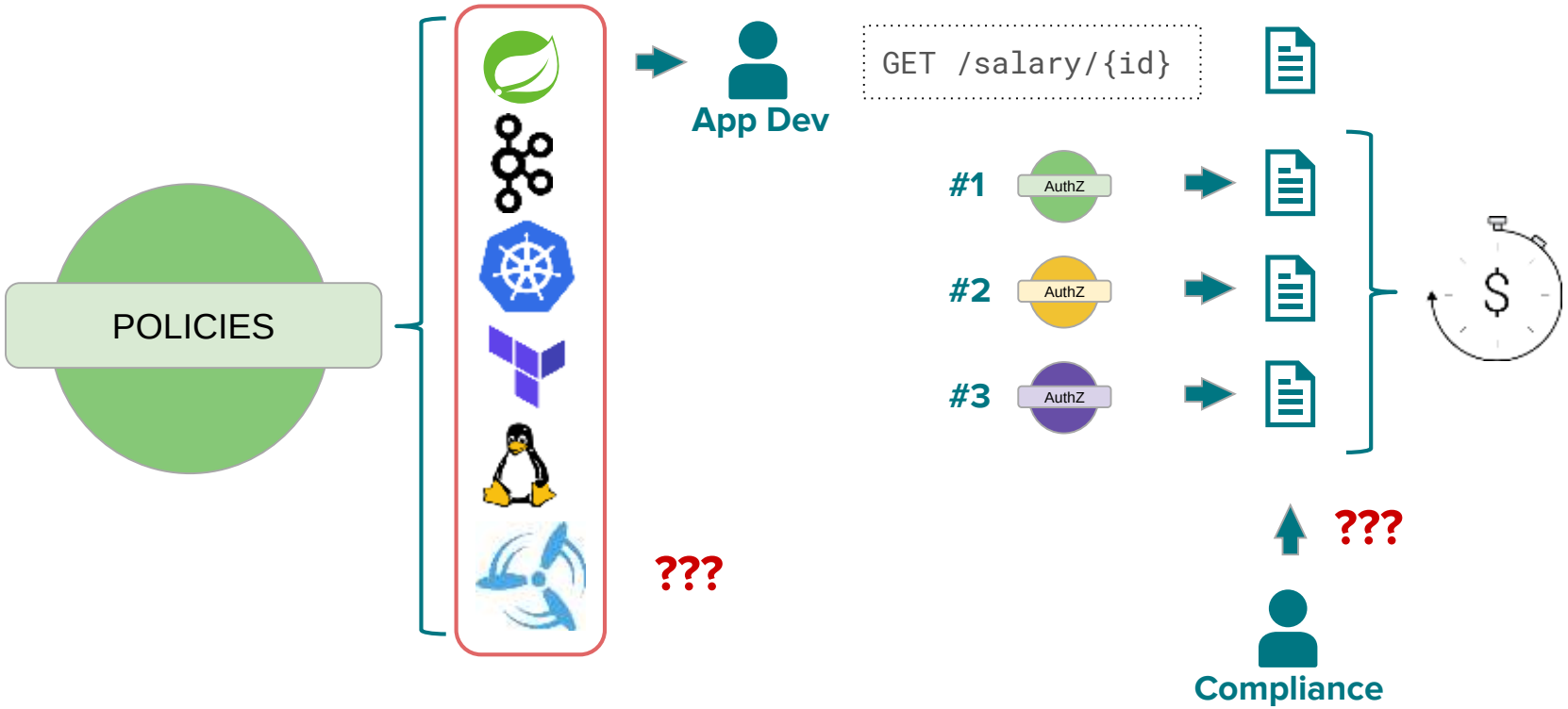
Agenda

- The Why, What and How of OPA
- OPA Use Cases
- Kubernetes Use Case
- Demo
- Q & A

What is OPA?

Open Policy Agent

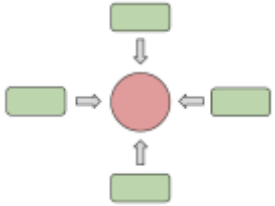
openpolicyagent.org



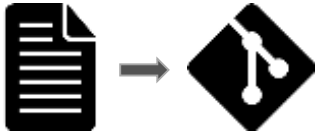
Why OPA?

Decouple policy from software

Unify policy enforcement across the stack

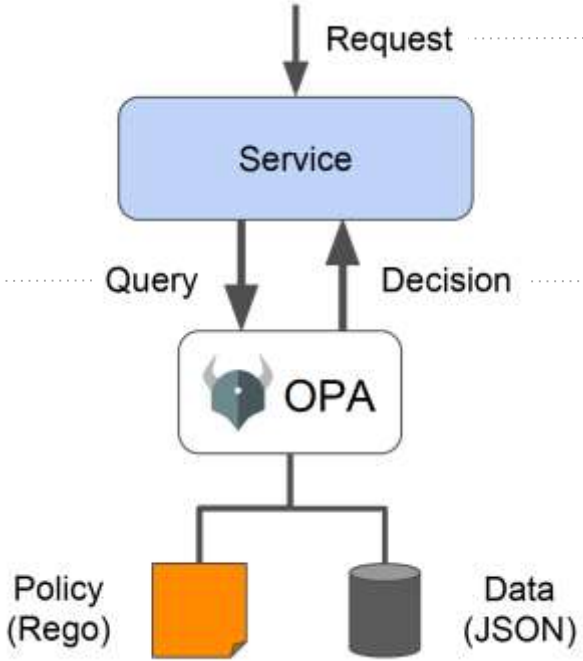


Manage Policy - as - Code



OPA: General-purpose Policy Engine

```
{
  “method”: “GET”,
  “path”: [“salary”, “bob”],
  “User”: “alice”
}
```




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

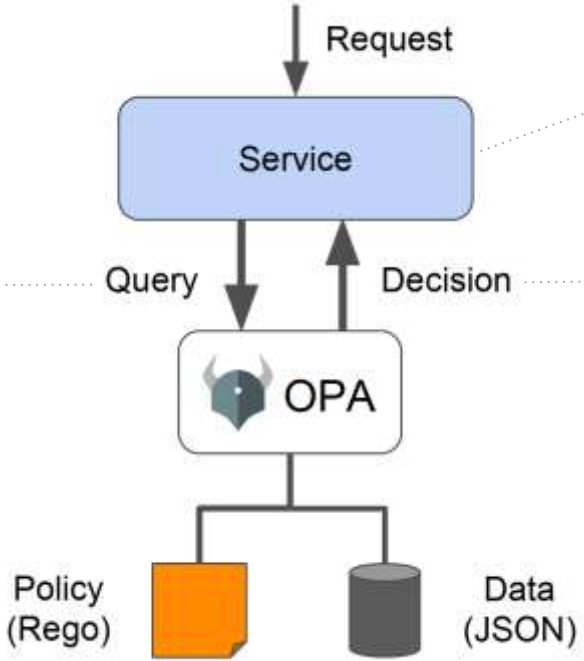
```
true or false
```

openpolicyagent.org

OPA: General-purpose Policy Engine

"Service" refers to any of:
- API Gateway
- Kubernetes API Service
- Custom Service
- CI/CD pipeline script
- etc

Input can be ***any*** JSON value:



Output can be ***any*** JSON value

openpolicyagent.org

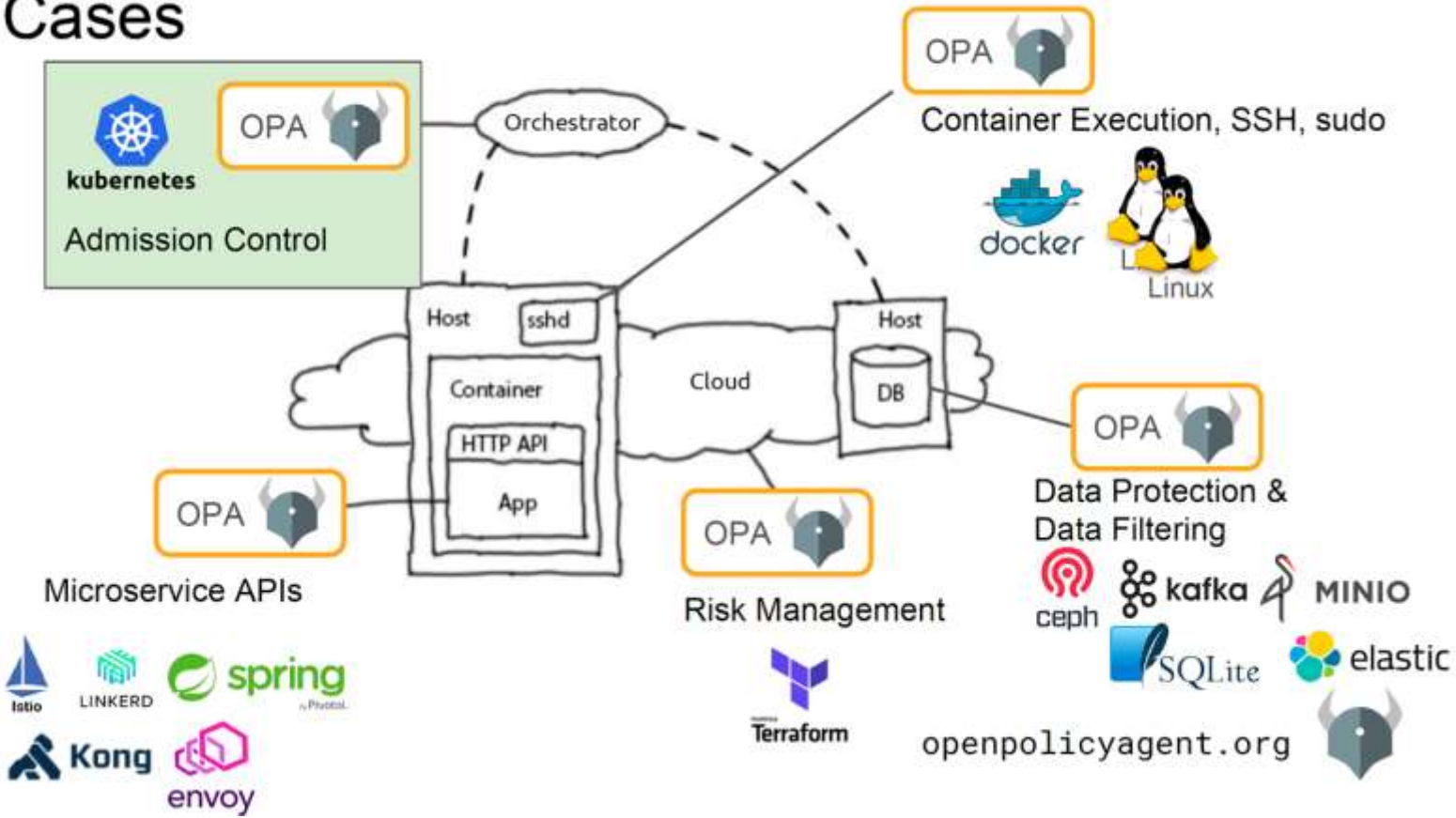
Rego: OPA's policy language

- Easy to read and write
- Declarative
- Handles complex data

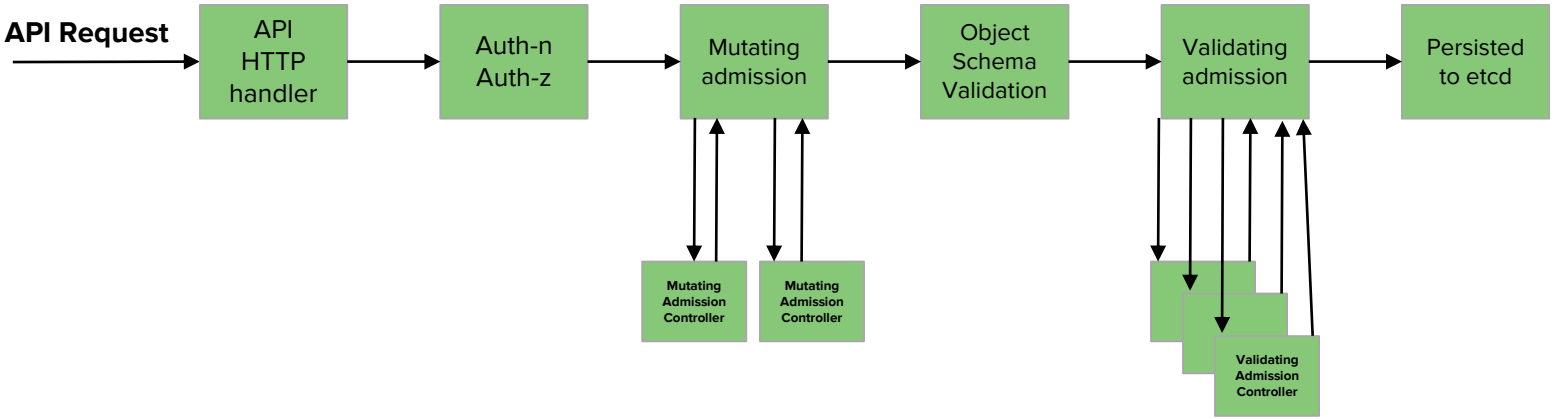
```
package kubernetes.admission

deny[msg] {
  input.request.kind.kind == "Pod"
  image :=
    input.request.object.spec.containers[_].image
  not startswith(image, "hooli.com/")
  msg := sprintf("image fails to come from trusted
    registry: %v", [image])
}
```

Use Cases



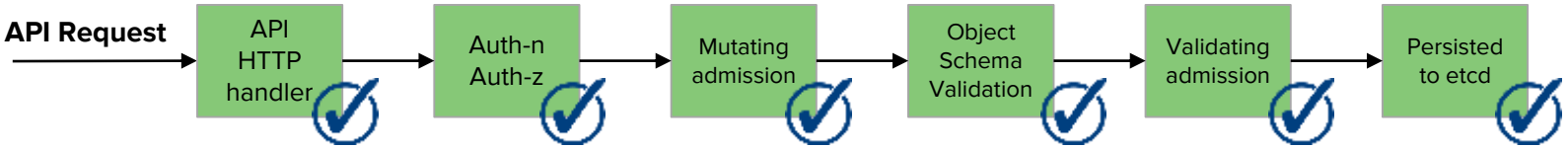
OPA In Kubernetes - Why is it needed?



Kubernetes API request workflow

** Further information available in:
https://kubernetes.io/blog/2019/03/21/a-guide-to-kubernetes-admission-controllers/

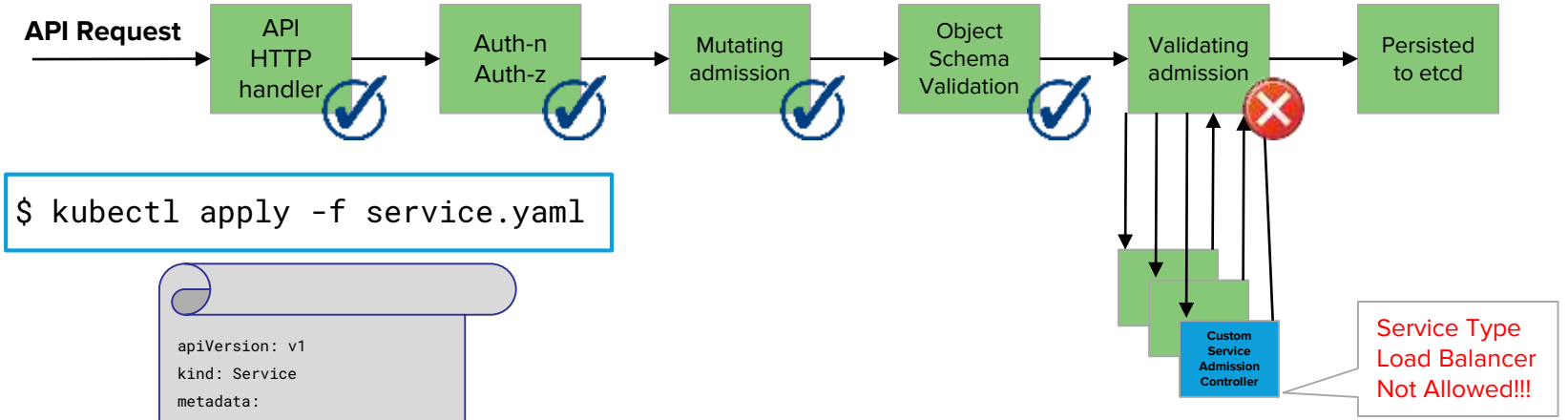
OPA In Kubernetes - Why is it needed?



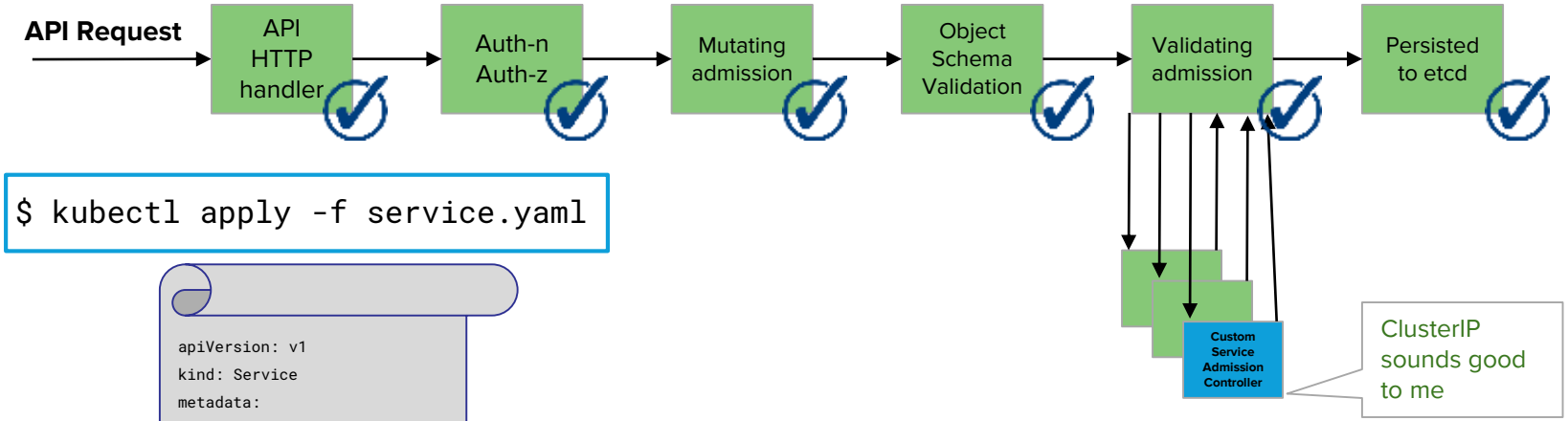

```
$ kubectl apply -f service.yaml
```

```
apiVersion: v1
kind: Service
metadata:
 name: coolapp
 labels:
   app: coolapp
spec:
 ports:
 - name: coolapp
   port: 80
 selector:
   app: coolapp
 type: LoadBalancer
```

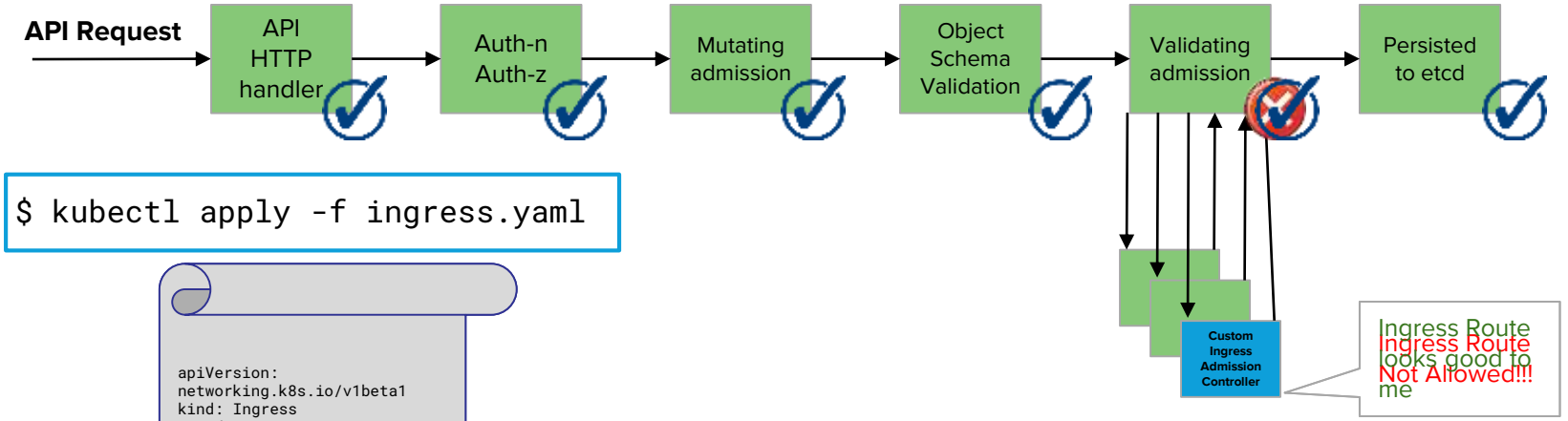
OPA In Kubernetes - Why is it needed?



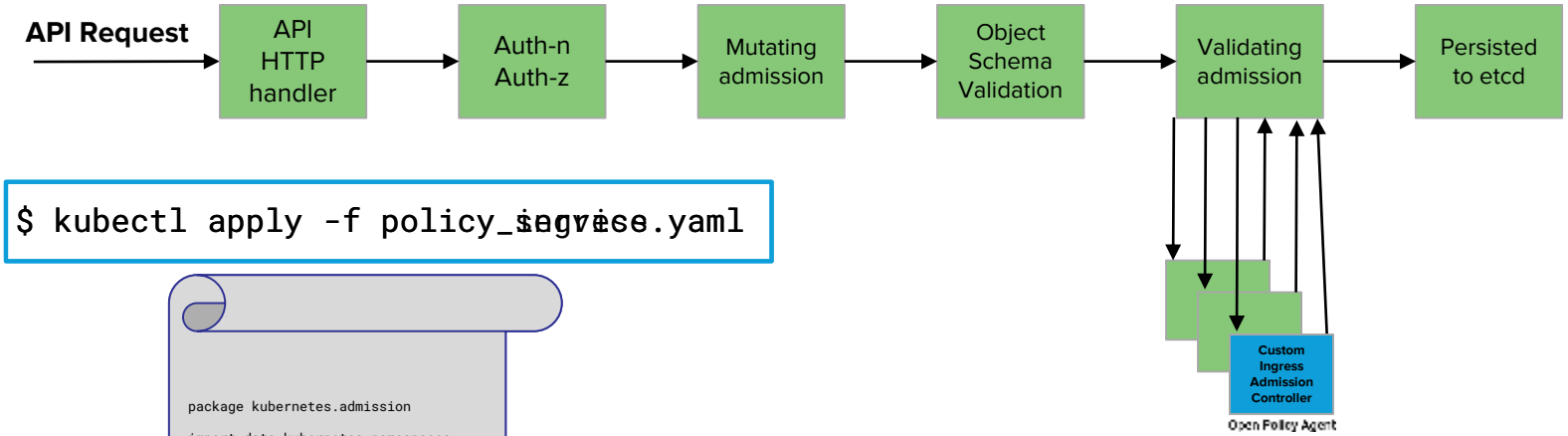
OPA In Kubernetes - Why is it needed?



OPA In Kubernetes - Why is it needed?



OPA In Kubernetes - Why is it needed?



Kubernetes Use Cases

- ServiceType
  - Restrict Cloud Load Balancer
  - Restrict Cloud Load Balancer to internal only
- Registry Whitelist/blacklist
- Ingress
  - Validate domain
  - Validate TLS
- NetworkPolicy validation

Demo!

- Show Harbor Registry and Image Repository
- Show OPA Admission Controller
- Show and deploy Policy
- Attempt to deploy Pod and show failure
- Change to fulfill Policy, deploy Pod and show success

Thank You!

Aleks
@alekssaul

Jaime
@jaimegag

@OpenPolicyAgent

https://www.openpolicyagent.org/

https://github.com/open-policy-agent

Open Policy Agent Summit - (KubeCon NA 2019)

San Diego, CA November 18, 2019