CRDs All the Way Down - Using OPA for Complex CRD Validation and Defaulting

Puja Abbassi - @puja108

18.11.2019

Giant Swarm

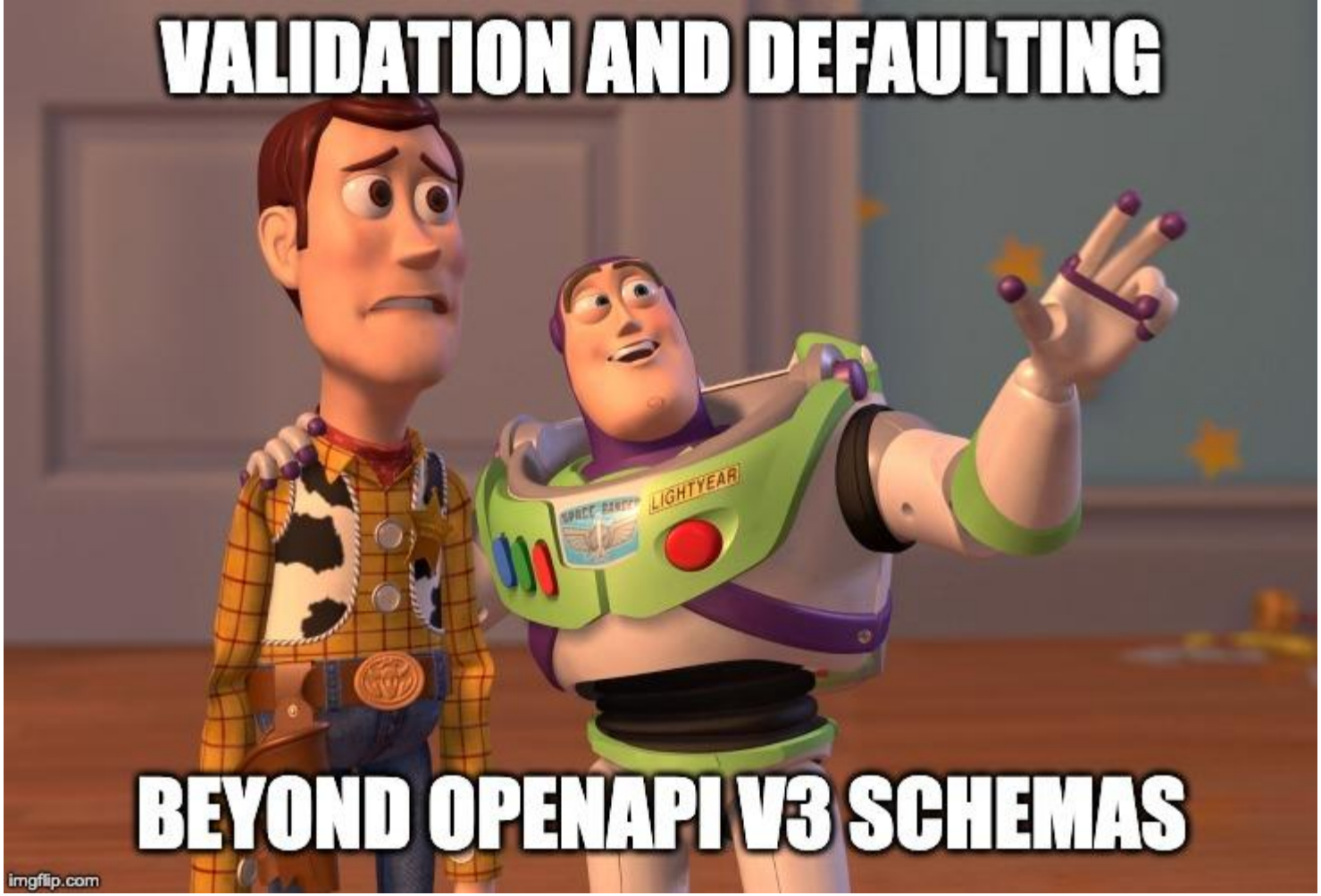
TLDR:
CRDs are becoming
the API

- "All new APIs are CRDs"
- "Eventually everything becomes a CRD"
- "CRD will need to get more powerful"
  - Tim Hockin ~1 year ago

Watch the whole talk at https://youtu.be/ji0FWzFwNhA

Validation and Defaulting are important in APIs

1. Are required fields filled?
2. Are fields filled correctly?
3. Are there additional fields that need filling?


VALIDATION AND DEFAULTING
LIGHTYEAR
BEYOND OPENAPI V3 SCHEMAS
imgflip.com

Validation beyond regex, lists, and min/max

- Validation against dynamic list(s) of possible values
  - Values are kept outside K8s
  - Values are kept as K8s resources or CRDs

Defaulting beyond static, single values

- Defaulting based on dynamic data
- Defaulting based on Context
  - Namespace, user,...
- Defaulting Metadata (labels, annotations)

Real Life Use Case for Inspiration

App CRD (UX optimized)

```
apiVersion: application.giantswarm.io/v1alpha1
kind: App
metadata:
  name: my-cool-prometheus
  namespace: dev1
spec:
  catalog: giantswarm
  name: prometheus
```

App CRD - defaulting config

```
apiVersion: application.giantswarm.io/v1alpha1
kind: App
metadata:
  name: my-cool-prometheus
  namespace: dev1
spec:
  catalog: giantswarm
  name: prometheus
```

default config

```
kubeconfigRef:
  apiVersion: core/v1
  kind: Secret
  namespace: dev1
  name: dev1-kubeconfig
```

App CRD - validation 1st step

```
apiVersion: application.giantswarm.io/v1alpha1
kind: App
metadata:
  name: my-cool-prometheus
  namespace: dev1
spec:
  catalog: giantswarm
  name: prometheus
```

does this catalog even exist?

App CRD - validation 2nd step

```
apiVersion: application.giantswarm.io/v1alpha1
kind: App
metadata:
  name: my-cool-prometheus
  namespace: dev1
spec:
  catalog: giantswarm
  name: prometheus
```


does this app exist in said catalog?

App CRD - defaulting version

```
apiVersion: application.giantswarm.io/v1alpha1
kind: App
metadata:
  name: my-cool-prometheus
  namespace: dev1
spec:
  catalog: giantswarm
  name: prometheus
  version: 3.2.1
```

default latest stable version

Open Policy Agent (OPA)

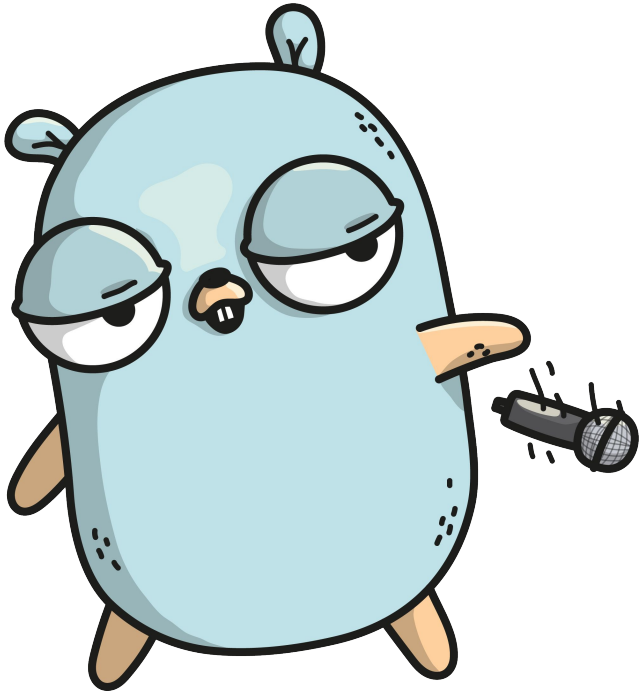
Why to use OPA?

- #nocode
- Single Agent for executing rules
- Rego is relatively easy to write and read

Vision

- OPA/Gatekeeper as quasi-default K8s addon
- Every CRD comes with its validation and defaulting rules as OPA rego rules OOTB

Thank you!



- Sounds cool?
- Stay in touch
  - Twitter: @puja108
  - Github: puja108
  - Slack/Discuss: puja

Picture: Ashley McNamara - https://github.com/ashleymcnamara/gophers/