OPA Gatekeeper
Policy and Governance for Kubernetes

Torin Sandall (Styra)
Craig Peters GH & SL: @craiglpeters Twitter: @peterscraig (Microsoft)
Who am I?

Who are you?

https://k8s.af/ much?
Remember the Dream?

My clusters are beautiful and clean.
I’ve configured RBAC...
and built all the runbooks and playbooks.

Open them up to the developers!
Oh my!

Who created that namespace?
What are all these pods?
Where did these containers come from?
How can I clean all this up?
What have I done?!?!?!
In a dynamic Kubernetes environment where

- More than two teams are working against one cluster
- One team is working against more than two clusters
- Clusters operate on multiple clouds

How do you

- Limit the use of unsafe images
- Understand who is creating and owning what resources
- Keep users from stepping on each others objects
- Ensure that logging, monitoring, and other observability is applied consistently
- Keep a handle on costs
**Possible Solutions**

**Wikis, Spreadsheets, and Tribal Knowledge**

---

**Role-based Access Control (RBAC)**

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: [""] # "" indicates the core API group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```
Possible Solutions

Wikis, Spreadsheets, and Tribal Knowledge

Role-based Access Control (RBAC)

apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
  - "pods"
  verbs:
  - "get"
  - "watch"
  - "list"
What is Admission Control?

- Kubernetes API Server
- Admission Control
- Authentication
- Authorization
- Resource Quota
- Webhook
- etcd

```
kubectl apply -f myapp.yaml
```

External Admission Controller
What is Admission Control?

Example Policies

- Block privileged containers
- Block external image registries
- Restrict egress rules
- Prevent ingress conflicts
- Require "owner" and "team" labels
- Require cpu & memory limits
- ...and many more.

```yaml
metadata:
  name: frontend
labels:
  contact: name@example.com
spec:
  replicas: 5
selector:
  app: frontend
template:
  metadata:
    name: frontend
  labels:
    app: frontend
  spec:
    containers:
    - name: proxy
      image: nginx
```
Building admission controllers is hard...

- Hundreds of lines of Go
  - See Liz Rice's Keynote from KubeCon Seattle 2018
- Policies change over time → Maintaining controllers is expensive
- Policies need to be flexible
  - and parameterized for different environments
- Policies need to leverage external data
- What about audit? What about dry-run and CI?
Demo
How does OPA Gatekeeper work?

1. Kubernetes
2. Policy CRDs
3. Admission Webhook
4. Gatekeeper

- **Apiserver**
  - Pod
  - Service
  - Config
- **Admission Review**
- **OPA**
  - Replicate
  - Query
- **metadata**:
  - name: frontend
  - labels:
    - contact: name@example.com
  - spec:
    - replicas: 5
    - selector:
      - app: frontend
    - template:
      - metadata:
      - name: frontend
      - labels:
        - app: frontend
      - spec:
      - containers:
        - name: proxy
        - image: nginx
### OPA vs. OPA Gatekeeper: CRDs & Policy Library

<table>
<thead>
<tr>
<th>OPA</th>
<th>OPA Gatekeeper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies are loaded via configmaps</td>
<td>Policies are loaded via CRDs</td>
</tr>
<tr>
<td>No standard policy library</td>
<td>Policy definitions (templates) are separate from parameters (constraints). Policies can be instantiated without writing Rego.</td>
</tr>
<tr>
<td>Admins write policies from scratch</td>
<td>Project includes standard library of policies</td>
</tr>
</tbody>
</table>
OPA vs. OPA Gatekeeper: Auditing the cluster

<table>
<thead>
<tr>
<th>OPA</th>
<th>OPA Gatekeeper</th>
</tr>
</thead>
</table>
| • OPA only answers policy queries  
• OPA does not include an auditing component | • Gatekeeper periodically queries OPA to check for violations on existing resources  
• Audit results are reported on CRDs |

![Diagram showing API server, Audit controller, and OPA Gatekeeper](image_url)
Project Status

- Alpha
- Come help!
  - Issues
  - Feedback
  - User stories
  - Development

Cooking... but tasty
Potential Growth

• Mutation
• External Data
• Authorization? (likely separate project, same general semantics)
• More audit features
• Metrics
• Developer tooling
Thank You

Open Policy Agent Community
Andrew Block (Red Hat)
Craig Hooper (Commonwealth Bank AU)
Lachlan Evenson (Microsoft)
Nikhil Bhatia (Confluent, ex-Microsoft)
Marc Campbell (Replicated)
Dexter Horthy (Replicated)
Tim Hinrichs (Styra)
Torin Sandall (Styra)
Max Smythe (Google)
Rita Zhang (Microsoft)
Q&A       Join Us!

Open Policy Agent
openpolicyagent.org
github.com/open-policy-agent/opa

OPA Gatekeeper
github.com/open-policy-agent/gatekeeper

Community
slack.openpolicyagent.org
#kubernetes-policy

Meetings Tue @2p Pacific