



A secure software supply chain for OPA policies

Omri Gazitt ([@omrig](https://twitter.com/omrig), github.com/ogazitt)
co-founder / CEO, [@aserto_com](https://aserto.com)

February 1, 2023



OPA policies are important artifacts that need to be secured

Use cases

- K8s admission control ([gatekeeper](#))
- Configuration policy ([conftest](#))
- General decision engine ([opa](#))
- App/API authz ([topaz](#))

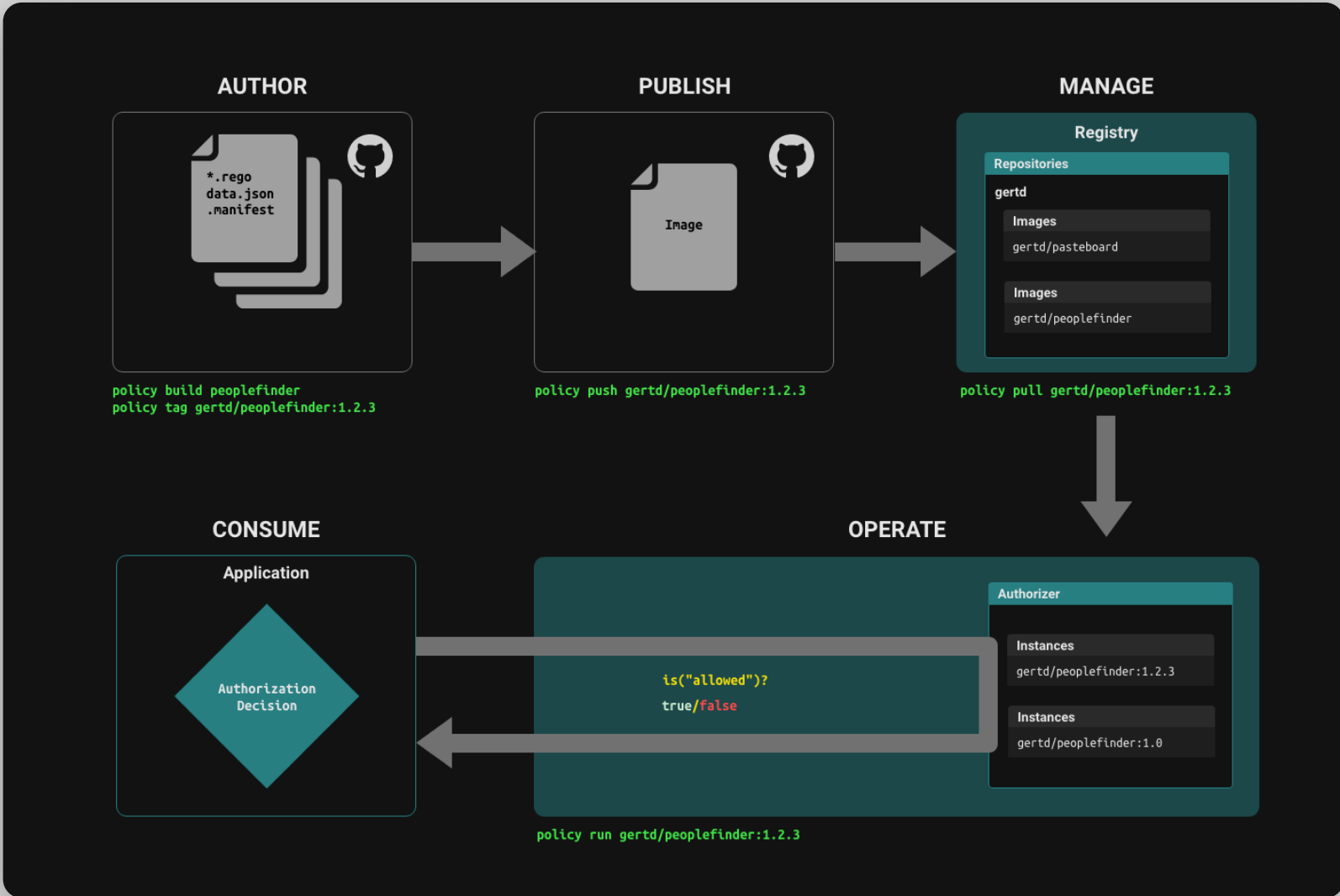
Requirements

- Standard image format ■ ■ [Open Container Initiative](#)
- Build/tag/push/pull ■ ■ ■ ■ [Open Policy Containers](#)
- Metadata ■ ■ ■ ■ ■ ■ ■ ■ [OCI annotations](#)
- Integrity / signing ■ ■ ■ ■ ■ [Sigstore](#)

LF / CNCF projects



policy: a docker-style workflow for OPA policies




CLOUD NATIVE
COMPUTING FOUNDATION



policy: a docker-style workflow for OPA policies

<https://gist.github.com/ogazitt/46f43fc7810d15d68db5964cf84f40ed>

 **policy CLI**

Raw

```
1  brew install opcr-io/tap/policy
2
3  echo $PAT | policy login -s ghcr.io -u <GitHub-account> --password-stdin
4
5  mkdir ./demo && cd ./demo
6
7  policy templates apply policy-template
8
9  tree .
10
11 policy build -t ghcr.io/<org>/policy-template:1.0.0 ./src
12
13 policy images
14
15 policy push ghcr.io/<org>/policy-template:1.0.0
```




CLOUD NATIVE
COMPUTING FOUNDATION



cosign: sign policy images, verify signatures

<https://gist.github.com/ogazitt/2d26d88026d13456238058aff9af2ffb>

 **cosign.sh**

Raw

```
1  brew install cosign
2
3  echo $PAT | docker login -u <GitHub-account> ghcr.io --password-stdin
4
5  cosign initialize
6
7  cosign generate-key-pair
8
9  cosign sign --key cosign.key ghcr.io/<org>/policy-template:1.0.0
10
11 cosign verify --key cosign.pub ghcr.io/<org>/policy-template:1.0.0
```





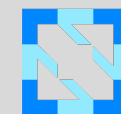
opa: run a policy image

```
$ opa run -c ./opa-config.yaml
```

<https://gist.github.com/ogazitt/315728a13a9b964f81e6cbd18b39faf9>

```
opa-config.yaml
Raw
1  services:
2    ghcr-registry:
3      url: https://ghcr.io
4      type: oci
5      credentials:
6        bearer:
7          scheme: "Bearer"
8          token: "<PAT>"
9
10  bundles:
11    authz:
12      service: ghcr-registry
13      resource: ghcr.io/<org>/policy-template:1.0.0
```

Docs: <https://openpolicycontainers.com/docs/opa>



CLOUD NATIVE
COMPUTING FOUNDATION



topaz: run a policy image

<https://gist.github.com/ogazitt/adb54dacb377892b779ba117efead577>

 **topaz.sh**

Raw

```
1 brew install aserto-dev/tap/topaz
2
3 topaz install
4
5 topaz configure -d -s -r ghcr.io/<org>/policy-template:1.0.0 policy-template
6
7 ## edit ~/.config/topaz/cfg/config.yaml to reflect GHCR auth info
8 ## see https://gist.github.com/ogazitt/315728a13a9b964f81e6cbd18b39faf9
9
10 topaz run
```

Docs:

<https://topaz.sh>

<https://openpolicycontainers.com/docs/topaz>

Feedback?
Go here:



Questions?
Find me!



Omri Gazitt (@[omrig](#), omri@aserto.com, github.com/ogazitt)

Community Slack: aserto.com/slack