Applying Policy Throughout The Application Lifecycle with Open Policy Agent

Gareth Rushgrove

snyk

Gareth Rushgrove

Director, Product Management, Snyk

Devops Weekly curator

Open Source contributor

@garethr

snyk

Agenda

01 What do we mean by policy

02 Introducing OPA and Conftest

03 Applying policy to a project

04 Policy in CI

05 Policy in production

snyk

Policy and software development

What do we mean by policy?

snyk

policy

noun [C]
UK /ˈpɒl.ə.si/ **US** /ˈpɑː.lə.si/

a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a group of people, a business organization, a government, or a political party.

Cambridge Dictionary

snyk

policy

noun [C]
UK /ˈpɒl.ə.si/ **US** /ˈpɑː.lə.si/

a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a group of people, a business organization, a government, or a political party.

Cambridge Dictionary

All Go projects should have been updated to use Go 1.13

snyk

policy

noun [C]
UK /ˈpɒl.ə.si/ **US** /ˈpɑː.lə.si/

a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a group of people, a business organization, a government, or a political party.

Cambridge Dictionary

All Go projects should have been updated to use Go 1.13

Our open source projects should all use the Apache 2.0 license

snyk

policy

noun [C]
UK /ˈpɒl.ə.si/ **US** /ˈpɑː.lə.si/

a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a group of people, a business organization, a government, or a political party.

Cambridge Dictionary

All Go projects should have been updated to use Go 1.13

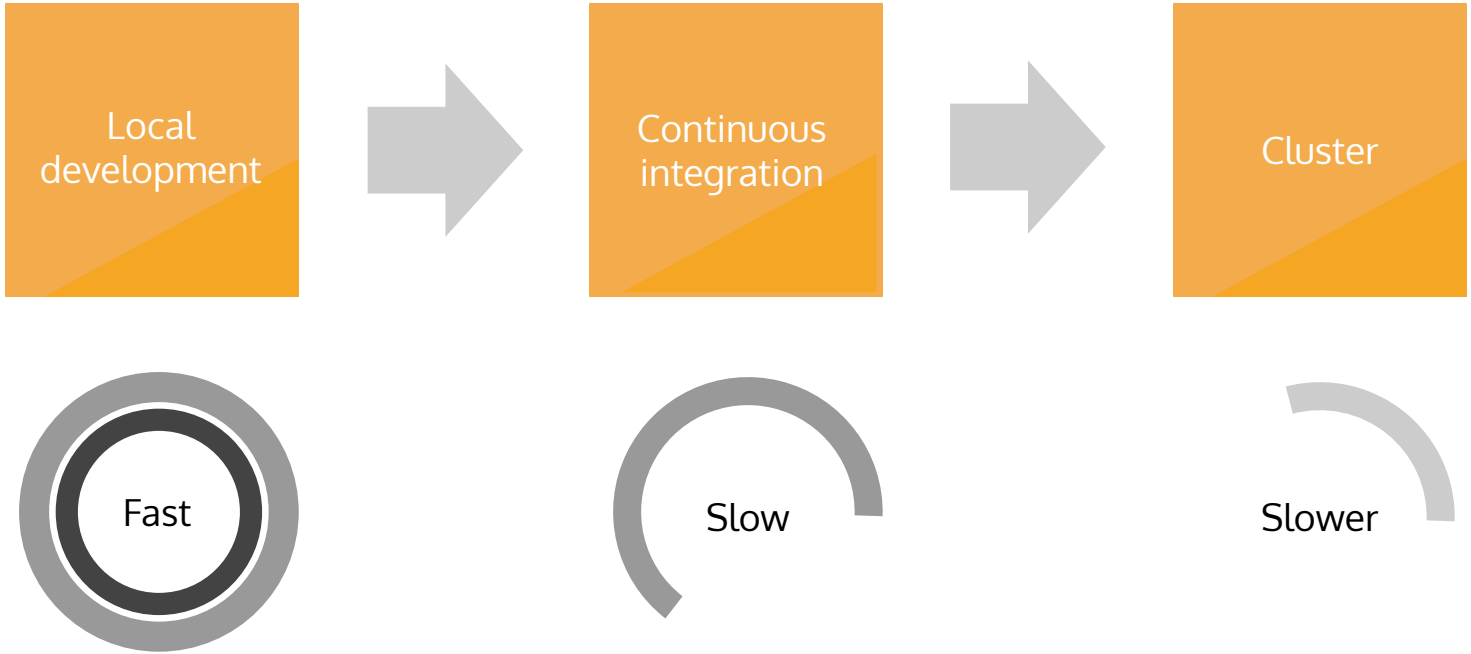
Our open source projects should all use the Apache 2.0 license

Dockerfiles should all have a maintainers label and not use FROM with images tagged latest

snyk

Where in our application lifecycle do we enforce policy?

The importance of developer feedback



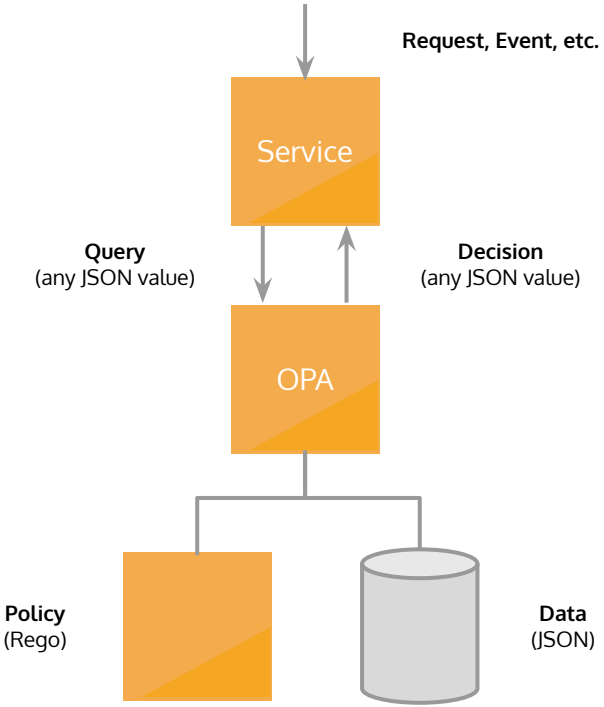
Open Policy Agent and Conftest

A quick introduction

snyk

What is Open Policy Agent?

github.com/open-policy-agent/opa



- An open source policy engine
- A CNCF incubating project
- Usable as a library and a service
- A vibrant open source community community
- Provides a declarative DSL for authoring policy (Rego)

Vincent Janelle
@randomfrequency

Replying to @garethr

It's my new favourite hammer.

7:15 PM - 5 May 2019

A quick example
Let’s suggest some places to eat this evening

```
// Where should we eat while at KubeCon in San Diego?
{
  "restaurants": [
    "Campfire",
    "Galaxy Taco",
    "Olive Garden",
    "Dija Mara",
    "Mikkeller",
    "Wrench and Rodent"
  ]
}
```

A quick example
Let’s describe a policy for our culinary preferences

```
deny["We can't go somewhere with unlimited breadstick"] {
  input.restaurants[_] = "Olive Garden"
}
```

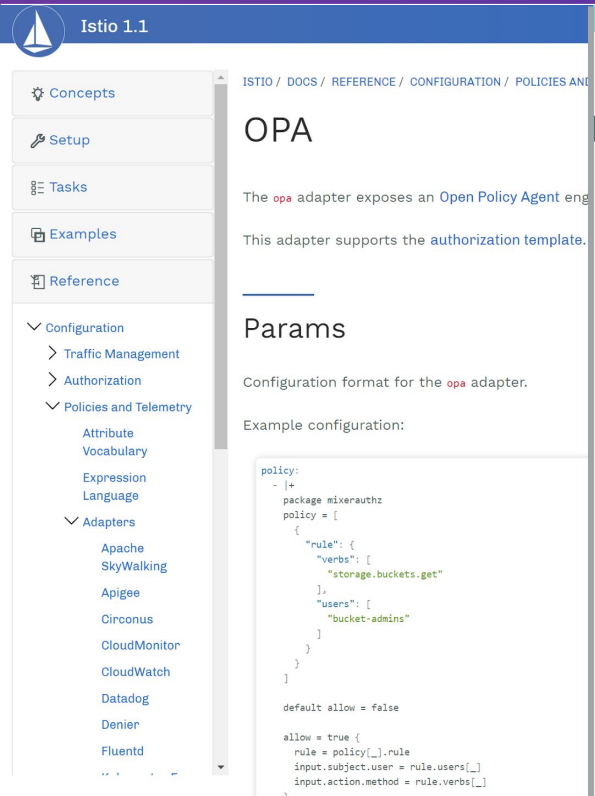
We should **deny** any input for which

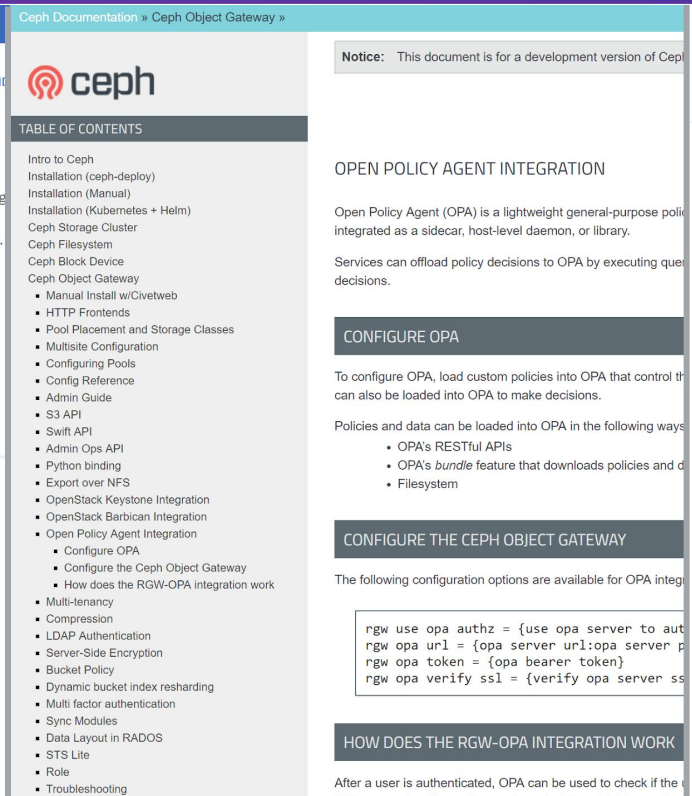
The “**restaurants**” list

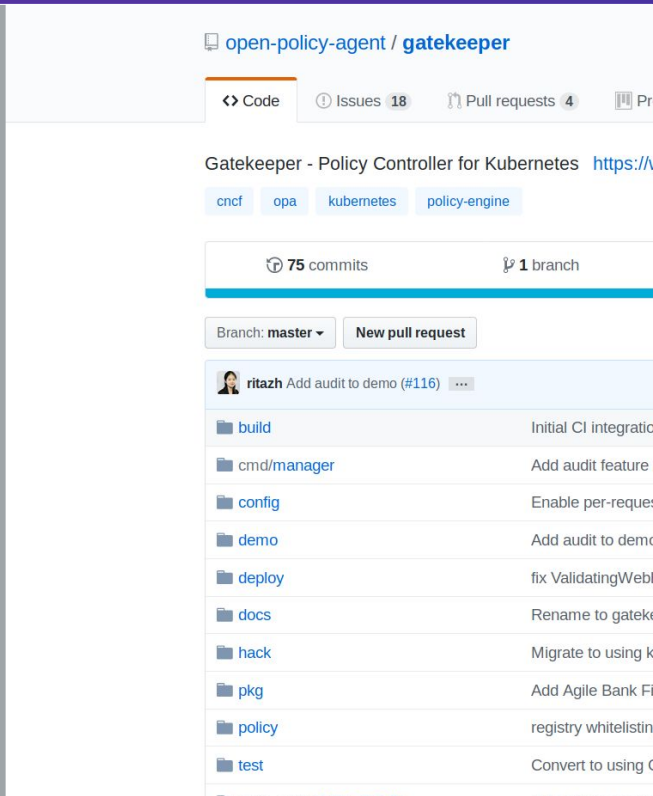
Contains a value of “**Olive Garden**”

snyk

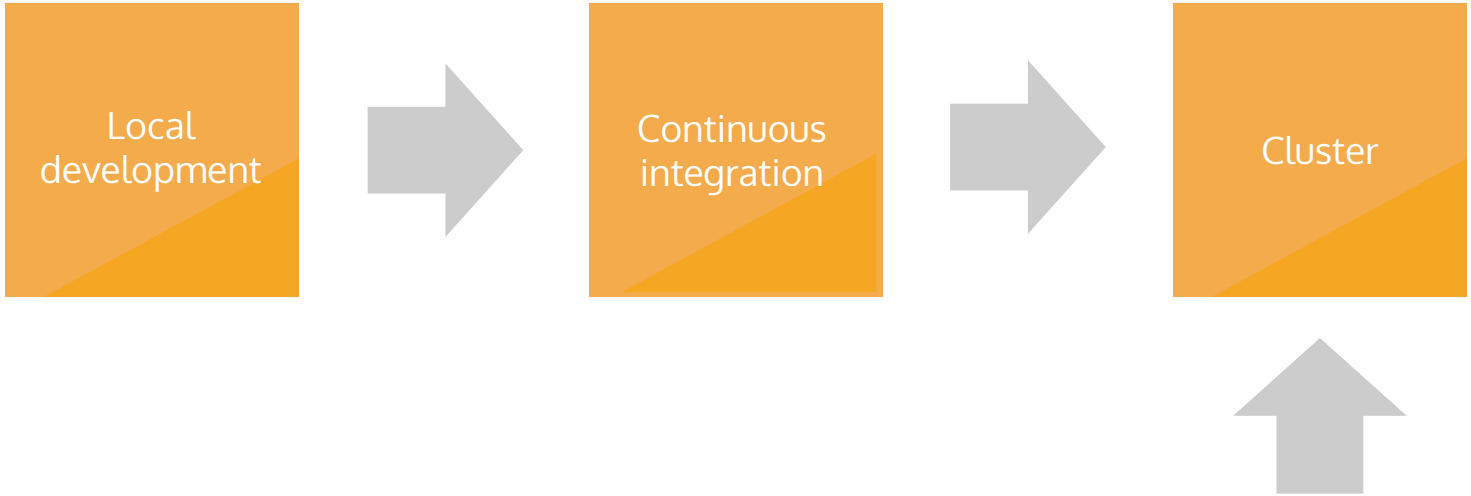
Open Policy Agent
Integrated into services



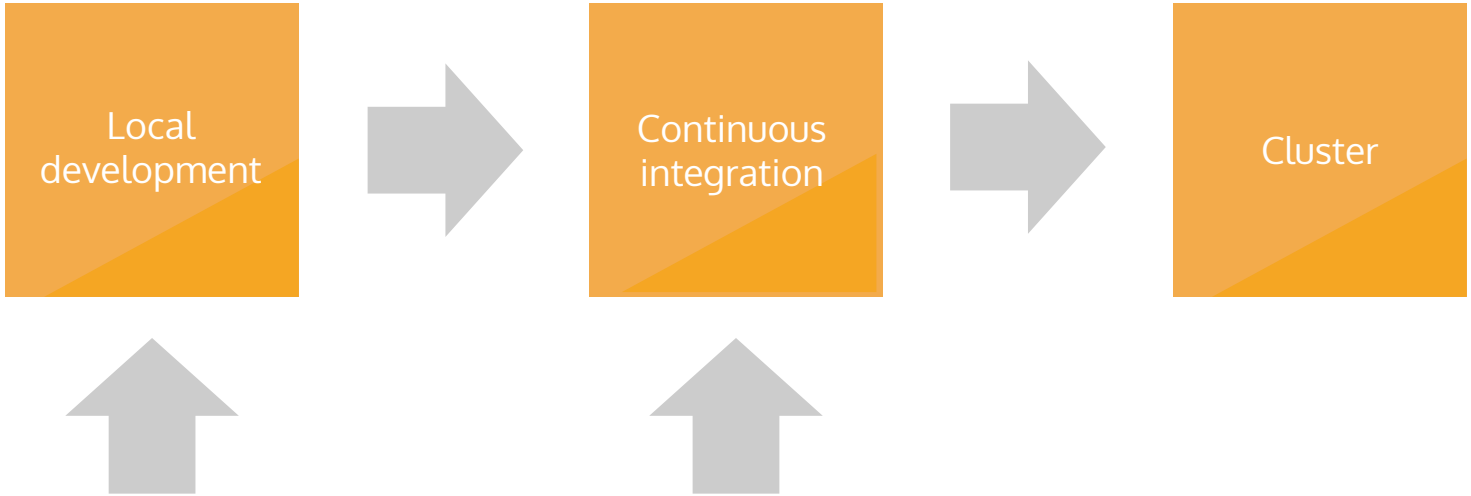




Open Policy Agent
Usage today in the Kubernetes community

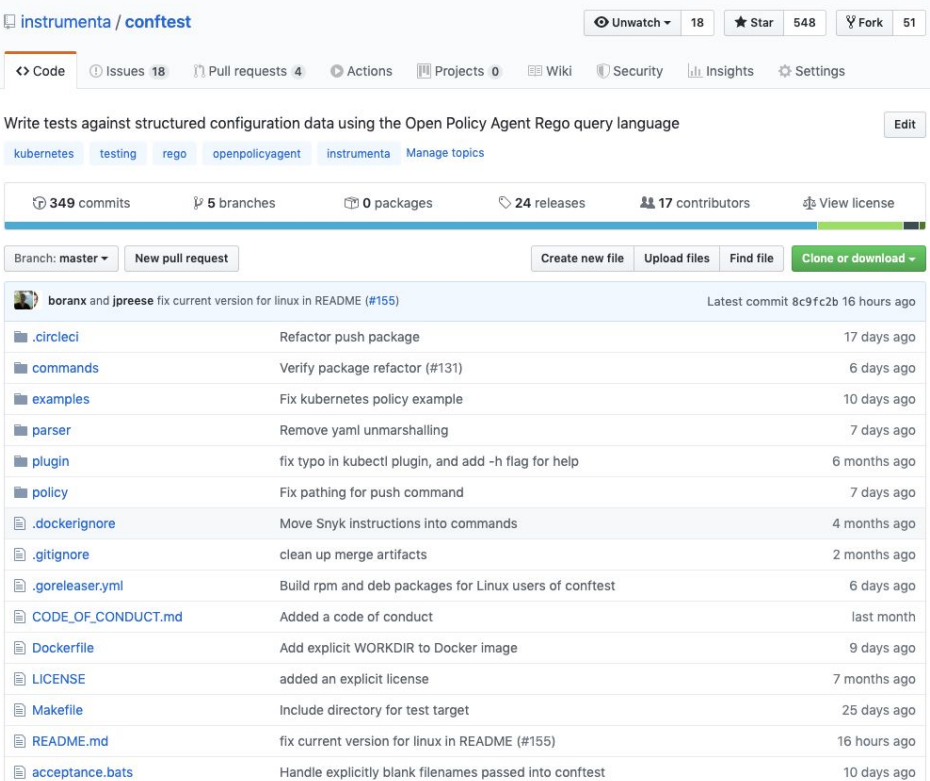


Open Policy Agent
Shifting policy left



What if we could use Open Policy Agent here **as well**?

Conftest
Introduced at KubeCon Barcelona



instrumenta / conftest

Unwatch 18 | Star 548 | Fork 51

Code | Issues 18 | Pull requests 4 | Actions | Projects 0 | Wiki | Security | Insights | Settings

Write tests against structured configuration data using the Open Policy Agent Rego query language

Edit

kubernetes | testing | rego | openpolicyagent | instrumenta | Manage topics

349 commits | 5 branches | 0 packages | 24 releases | 17 contributors | View license

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

boranx and jpreese fix current version for linux in README (#155) — Latest commit 8c9fc2b 16 hours ago

.circleci	Refactor push package	17 days ago
commands	Verify package refactor (#131)	6 days ago
examples	Fix kubernetes policy example	10 days ago
parser	Remove yaml unmarshalling	7 days ago
plugin	fix typo in kubectl plugin, and add -h flag for help	6 months ago
policy	Fix pathing for push command	7 days ago
.dockerignore	Move Snyk instructions into commands	4 months ago
.gitignore	clean up merge artifacts	2 months ago
.goreleaser.yml	Build rpm and deb packages for Linux users of conftest	6 days ago
CODE_OF_CONDUCT.md	Added a code of conduct	last month
Dockerfile	Add explicit WORKDIR to Docker image	9 days ago
LICENSE	added an explicit license	7 months ago
Makefile	Include directory for test target	25 days ago
README.md	fix current version for linux in README (#155)	16 hours ago
acceptance.bats	Handle explicitly blank filenames passed into conftest	10 days ago

What is Conftest?

github.com/instrumenta/conftest

```
$ conftest
Test your configuration files using Open Policy Agent

Usage:
  conftest [command]

Available Commands:
  help        Help about any command
  parse       Print out structured data from your input
  pull        Download individual policies
  push        Upload OPA bundles to an OCI registry
  test        Test your configuration files using Open P
  update      Download policy from registry
  verify      Verify Rego unit tests
```

- Developer-focused UX for config policy
- An open source project built on top of OPA
- Easy to use with different inputs (JSON, YAML, INI, HCL, TOML, CUE, Dockerfile)
- Build to be used as a testing tool (JSON, TAP and plain text output)
- Built-in tools for sharing policy (via Git, OCI registries, S3 and more)

Conftest
A simple CLI tool for asserting policy

```
$ conftest test restaurants.json -p restaurants.rego
FAIL - restaurants.json - We can't go somewhere with unlimited breadstick
```

snyk

Conftest
Integrated into developer tools

GitHub

GitHub Action

Conftest

v0.4.0 Latest version

Conftest

A GitHub Action for using Conftest in your workflows.

You can use the action as follows:

```
on: push
name: Validate
jobs:
  conftest:
    runs-on: ubuntu-latest
    steps:
    - uses: actions/checkout@master
    - name: test
      uses: instrumenta/conftest-action@master
      with:
        files: deployment.yaml
```

The Conftest Action has a small number of properties which map to the parameters for Conftest itself. These are passed to the action using `with`, as demonstrated with `files` in the above example.

Property	Default	Description
files	-	*Required* which files to test
policy	policy	Where to find the policy folder or files

TEKTON

tektoncd / catalog

Watch 11 | Star 58 | Fork 49

Code | Issues 20 | Pull requests 8 | Actions | Projects 0 | Wiki | Security | Insights

Branch: master | catalog / conftest /

Create new file | Upload files | Find file | History

garethr and tekton-robot Be explicit about files being a string — Latest commit e049b02 6 days ago

..		
OWNERS	Add initial OWNERS to some folders	17 days ago
README.md	Follow up commit to resolve README issues for conftest tasks	17 days ago
conftest.yaml	Be explicit about files being a string	4 days ago
helm-conftest.yaml	A new task related to Conftest which makes testing Helm charts easier	19 days ago

README.md

Conftest

These tasks make it possible to use Conftest within your Tekton pipelines. Conftest is a tool for testing configuration files using Open Policy Agent.

Installation

In order to use Conftest with Tekton you need to first install the task.

```
kubectl apply -f https://raw.githubusercontent.com/tektoncd/catalog/master/conftest/conftest.yaml
```

Conftest also has a Helm plugin, which redners the Helm chart before applying the policy. For that task use:

```
kubectl apply -f https://raw.githubusercontent.com/tektoncd/catalog/master/conftest/helm-conftest.yaml
```

Usage

circleci

Explore Orbs / kenfdev/conftest-orb

kenfdev/conftest-orb@0.0.9

Report This Orb

Easily integrate Conftest View this orb's source: https://github.com/kenfdev/conftest-orb

Orb Created: October 19, 2019 | Version Published: October 21, 2019 | Releases: 0.0.9

See Orb Licensing

Orb Quick Start Guide

1. Use CircleCI version 2.1 at the top of your .circleci/config.yml file.

```
version: 2.1
```

Copy This Code

If you do not already have Pipelines enabled, you'll need to go to Project Settings -> Advanced Settings and turn it on.

2. Add the `orbs` stanza below your version, invoking the orb:

```
orbs:
  conftest-orb: kenfdev/conftest-orb@0.0.9
```

Copy This Code

3. Use `conftest-orb` elements in your existing workflows and jobs.
4. Opt-in to use of third-party orbs on your organization's Security settings page.

Read more in the docs here.

Usage Examples

simple

Runs conftest tests against the target file.

Demo

snyk

Applying policy to a real project

Enforcing development standards

snyk

Python application example
Check Python development environment settings

```
package pipfile

deny[msg] {
    version := to_number(input.requires.python_version)
    version < 3
    msg := sprintf("Should be using Python 3, currently Using Python %v", [version])
}

deny[msg] {
    not input.source[i].verify_ssl = true
    name := input.source[i].name
    msg := sprintf("You must verify SSL for %v", [name])
}
```

snyk

Python application example
Check Python development environment settings

```
$ conftest test --input toml --namespace pipfile Pipfile
FAIL - Pipfile - You must verify SSL for pypi
FAIL - Pipfile - Should be using Python 3, currently Using Python 2.
```

snyk

Python application example
Check we are using specific testing tools

```
$ conftest test --namespace pytest pytest.ini
WARN - pytest.ini - Consider enforcing type checking when running tests
WARN - pytest.ini - Consider enabling coverage reporting for test
```

snyk

Python application example
Check the Dockerfile for policy issues

```
$ conftest test --namespace docker Dockerfile
FAIL - Dockerfile - Using latest tag on base image python
```

snyk

Python application example
Run unit tests for our policies

```
$ conftest verify
PASS - policy/policy/pytest_test.rego - data.pytest.test_require_black
PASS - policy/policy/pytest_test.rego - data.pytest.test_require_isort
PASS - policy/policy/pytest_test.rego - data.pytest.test_require_isort_and_black
PASS - policy/policy/pytest_test.rego - data.pytest.test_recommend_coverage
PASS - policy/policy/pytest_test.rego - data.pytest.test_recommend_type_checker
PASS - policy/policy/pytest_test.rego - data.pytest.test_valid_with_required_options
PASS - policy/policy/pytest_test.rego - data.pytest.test_no_warnings_with_recommended_option
```

snyk

Python application example
Check policy in our Python unit tests

```
def test_policy(conftest):
    run = conftest.verify()
    assert run.success

def test_pytest_config(conftest):
    run = conftest.test("pytest.ini", namespace="pytest")
    assert run.success

def test_kubernetes_manifest_for_warnings(conftest):
    run = conftest.test("snyky.yaml")
    result = run.results[0]
    assert not result.Warnings
```

snyk

Demo

snyk

Kubernetes security policy

Applying general purpose tools to Kubernetes

snyk

The current configuration explosion **Kubernetes YAML files**

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-kubernetes
spec:
  replicas: 3
  selector:
    matchLabels:
      app: hello-kubernetes
  template:
    metadata:
      labels:
        app: hello-kubernetes
    spec:
      containers:
       - name: hello-kubernetes
```

~1.7 million

Kubernetes configuration files public on GitHub

snyk

Prior-art
KubeSec

KUBESEC.IO
from **control**plane

Search...

index

- containers[] .resources .limits .cpu
- containers[] .resources .limits .memory
- containers[] .resources .requests .cpu
- containers[] .resources .requests .memory
- containers[] .securityContext .capabilities .add | index("SYS_ADMIN")
- containers[] .securityContext .capabilities .drop | index("ALL")
- containers[] .securityContext .privileged == true
- containers[] .securityContext .readOnlyRootFilesystem == true
- containers[] .securityContext .runAsNonRoot == true
- containers[] .securityContext .runAsUser > 10000
- securityContext capabilities
- Service Accounts

KUBESEC.IO – V2

🚨 v1 API is deprecated, please read the release notes 🚨

Security risk analysis for Kubernetes resources

Live Demo

Submit this YAML to Kubesec

```
apiVersion: v1
kind: Pod
metadata:
```

Shared policies
Porting KubeSec rules to Rego

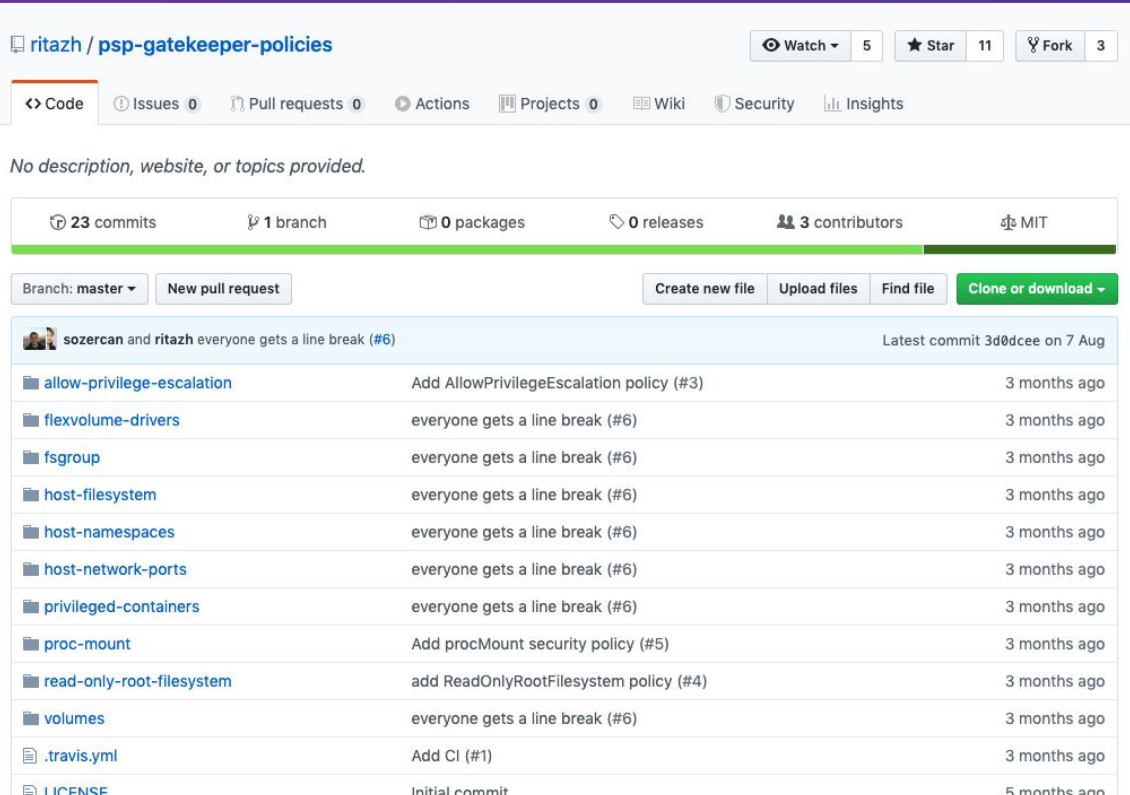
```
package main

import data.lib.kubernetes

# https://kubesec.io/basics/spec-hostnetwork/
deny[msg] {
    kubernetes.pods[pod]
    pod.spec.hostNetwork
    msg = kubernetes.format(sprintf("The %s %s is connected to the host network", [kubernetes.kind, kuber
}
```

snyk

Shared policies
PodSecurityPolicy in Rego



ritazh / psp-gatekeeper-policies

Watch 5 | Star 11 | Fork 3

Code | Issues 0 | Pull requests 0 | Actions | Projects 0 | Wiki | Security | Insights

No description, website, or topics provided.

23 commits | 1 branch | 0 packages | 0 releases | 3 contributors | MIT

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

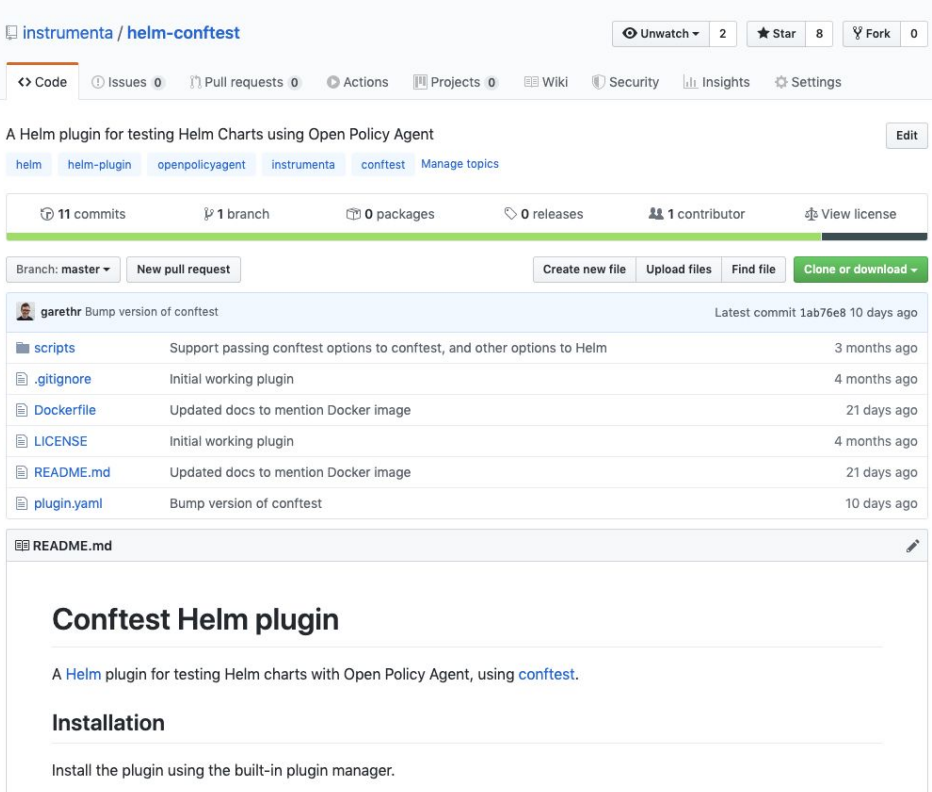
sozercan and **ritazh** everyone gets a line break (#6) — Latest commit 3d0dcee on 7 Aug

allow-privilege-escalation	Add AllowPrivilegeEscalation policy (#3)	3 months ago
flexvolume-drivers	everyone gets a line break (#6)	3 months ago
fsgroup	everyone gets a line break (#6)	3 months ago
host-filesystem	everyone gets a line break (#6)	3 months ago
host-namespaces	everyone gets a line break (#6)	3 months ago
host-network-ports	everyone gets a line break (#6)	3 months ago
privileged-containers	everyone gets a line break (#6)	3 months ago
proc-mount	Add procMount security policy (#5)	3 months ago
read-only-root-filesystem	add ReadOnlyRootFilesystem policy (#4)	3 months ago
volumes	everyone gets a line break (#6)	3 months ago
.travis.yml	Add CI (#1)	3 months ago
LICENSE	Initial commit	5 months ago

Demo

snyk

Conftest
Helm plugin



instrumenta / helm-conftest

Unwatch 2 | Star 8 | Fork 0

Code | Issues 0 | Pull requests 0 | Actions | Projects 0 | Wiki | Security | Insights | Settings

A Helm plugin for testing Helm Charts using Open Policy Agent

Edit

helm | helm-plugin | openpolicyagent | instrumenta | conftest | Manage topics

11 commits | 1 branch | 0 packages | 0 releases | 1 contributor | View license

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

garethr Bump version of conftest — Latest commit 1ab76e8 10 days ago

scripts	Support passing conftest options to conftest, and other options to Helm	3 months ago
.gitignore	Initial working plugin	4 months ago
Dockerfile	Updated docs to mention Docker image	21 days ago
LICENSE	Initial working plugin	4 months ago
README.md	Updated docs to mention Docker image	21 days ago
plugin.yaml	Bump version of conftest	10 days ago

README.md

Conftest Helm plugin

A Helm plugin for testing Helm charts with Open Policy Agent, using conftest.

Installation

Install the plugin using the built-in plugin manager.

Conftest
Helm plugin

```
$ helm conftest snyky
FAIL - snyky in the Deployment garethr/snyky has an image, snyky, using the latest tag
FAIL - snyky in the Deployment snyky does not have a memory limit set
FAIL - snyky in the Deployment snyky does not have a CPU limit set
FAIL - snyky in the Deployment snyky doesn't drop all capabilities
FAIL - snyky in the Deployment snyky is not using a read only root filesystem
FAIL - snyky in the Deployment snyky allows priviledge escalation
FAIL - snyky in the Deployment snyky is running as root
Error: plugin "conftest" exited with error
```

snyk

Policy in CI

Always be enforcing

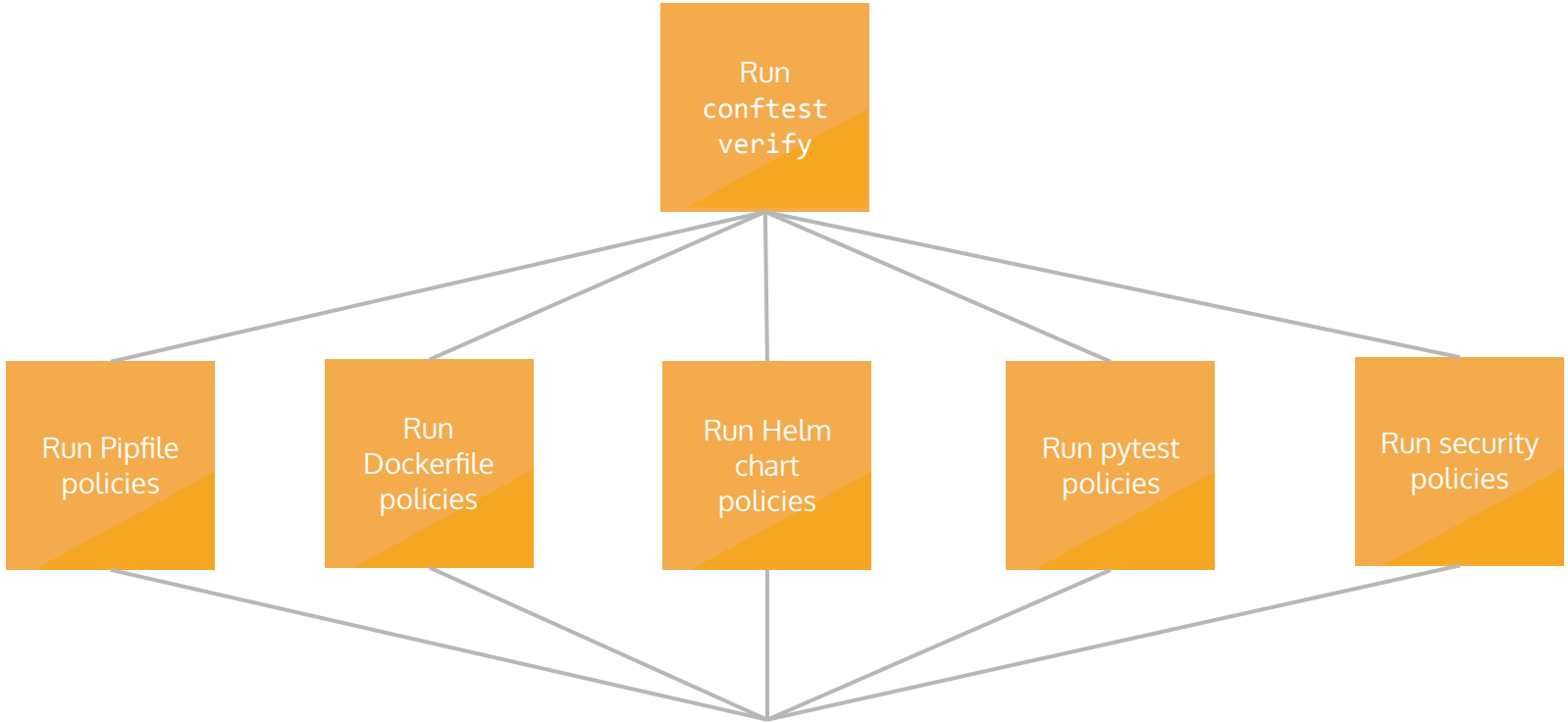
snyk

Tekton Pipeline
Describe a pipeline to run our policy

```
apiVersion: tekton.dev/v1alpha1
kind: Pipeline
metadata:
  name: snyky-pipeline
spec:
  resources:
    - name: source-repo
      type: git
  tasks:
    - name: conftest-verify
      taskRef:
        name: conftest-verify
      resources:
        inputs:
          - name: source
            resource: source-repo
    - name: pipfile-conftest
```

snyk

Tekton Pipeline
Policy CI graph



Tekton Pipeline
Start a pipeline run

```
$ tkn pipeline start snyky-pipeline
? Choose the git resource to use for source-repo: snyky-git
(https://github.com/garethr/snyky.git)
Pipelinerun started: snyky-pipeline-run-xrg96

In order to track the pipelinerun progress run:
tkn pipelinerun logs snyky-pipeline-run-xrg96 -f -n default
```

snyk

Tekton Pipeline
View the pipeline logs

```
$ tkn pipelinerun logs snyky-pipeline-run-xrg96 -f -n default
...
[pytest-conftest : conftest] WARN - pytest.ini - Consider enforcing type checking when running tests
[pytest-conftest : conftest] WARN - pytest.ini - Consider enabling coverage reporting for tests

[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_require_blac
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_require_isor
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_require_isor
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_recommend_co
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_recommend_ty
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_valid_with_r
[conftest-verify : conftest-verify] PASS - policy/policy/pytest_test.rego - data.pytest.test_no_warnings_
...
```

snyk

Demo

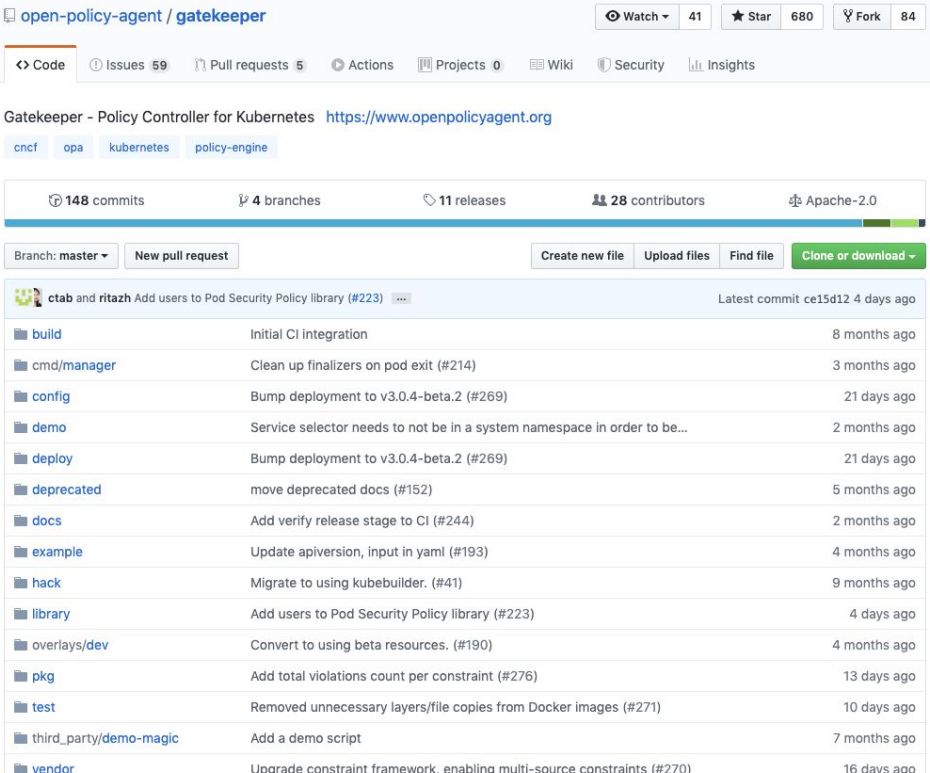
snyk

Policy in production

Gates and auditing

snyk

Gatekeeper
Policy controller for Kubernetes



open-policy-agent / gatekeeper

Watch 41 | Star 680 | Fork 84

Code | Issues 59 | Pull requests 5 | Actions | Projects 0 | Wiki | Security | Insights

Gatekeeper - Policy Controller for Kubernetes https://www.openpolicyagent.org

cncf | opa | kubernetes | policy-engine

148 commits | 4 branches | 11 releases | 28 contributors | Apache-2.0

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

ctab and ritazh Add users to Pod Security Policy library (#223) ... Latest commit ce15d12 4 days ago

build	Initial CI integration	8 months ago
cmd/manager	Clean up finalizers on pod exit (#214)	3 months ago
config	Bump deployment to v3.0.4-beta.2 (#269)	21 days ago
demo	Service selector needs to not be in a system namespace in order to be...	2 months ago
deploy	Bump deployment to v3.0.4-beta.2 (#269)	21 days ago
deprecated	move deprecated docs (#152)	5 months ago
docs	Add verify release stage to CI (#244)	2 months ago
example	Update apiversion, input in yaml (#193)	4 months ago
hack	Migrate to using kubebuilder. (#41)	9 months ago
library	Add users to Pod Security Policy library (#223)	4 days ago
overlays/dev	Convert to using beta resources. (#190)	4 months ago
pkg	Add total violations count per constraint (#276)	13 days ago
test	Removed unnecessary layers/file copies from Docker images (#271)	10 days ago
third_party/demo-magic	Add a demo script	7 months ago
vendor	Upgrade constraint framework, enabling multi-source constraints (#270)	16 days ago

Gatekeeper
Constraints and ConstraintTemplates

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: securitycontrols
spec:
  crd:
    spec:
      names:
        kind: SecurityControls
        listKind: SecurityControlsList
        plural: securitycontrols
        singular: securitycontrol
  targets:
  - libs:
    - |
      package lib.kubernetes
      default is_gatekeeper = false
```

snyk

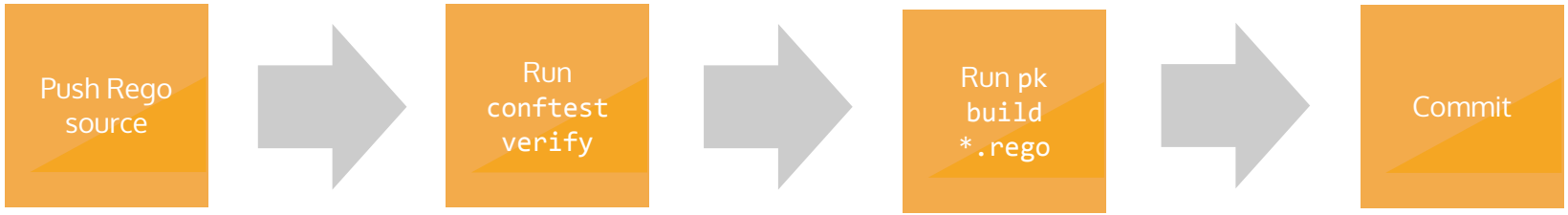
Gatekeeper
Generating ConstraintTemplates from Rego

```
$ pk build SecurityControls.rego
[SecurityControls] Generating a ConstraintTemplate from "SecurityControls.rego"
[SecurityControls] Searching "lib" for additional rego files
[SecurityControls] Adding library from "lib/kubernetes.rego"
[SecurityControls] Saving to "SecurityControls.yaml"
```

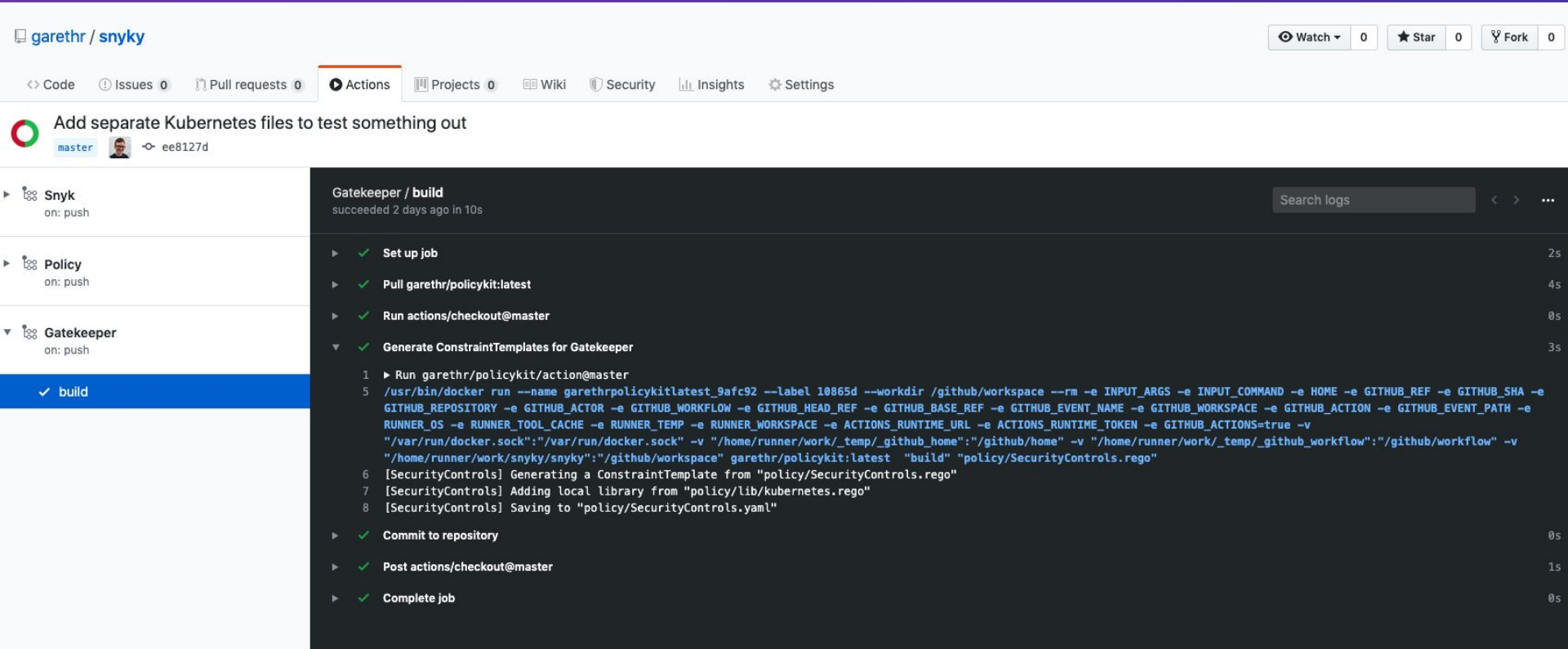
snyk

Gatekeeper
Keeping ConstraintTemplates up-to-date

GitHub Actions



Gatekeeper
Keeping ConstraintTemplates up-to-date



Gatekeeper
Block deployments with policy violations

```
$ kubectl apply -f deployment.yaml
Error from server ([denied by enforce-deployment-and-pod-security-controls] nginx in the
Deployment nginx-deployment does not have a memory limit set
[denied by enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment
does not have a CPU limit set
[denied by enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment
doesn't drop all capabilities
[denied by enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment
is not using a read only root filesystem
[denied by enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment
is running as root): error when creating "deployment.yaml": admission webhook
"validation.gatekeeper.sh" denied the request: [denied by
enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment does not
have a memory limit set
[denied by enforce-deployment-and-pod-security-controls] nginx in the Deployment nginx-deployment
does not have a CPU limit set
```

snyk

Gatekeeper
Audit running workloads against defined policy

```
$ kubectl get SecurityControls audit-deployment-and-pod-security-controls -o yaml
...
  - enforcementAction: dryrun
    kind: Deployment
    message: nginx in the Deployment nginx-deployment doesn't drop all capabilities
    name: nginx-deployment
    namespace: audit
  - enforcementAction: dryrun
    kind: Deployment
    message: nginx in the Deployment nginx-deployment is not using a read only root
      filesystem
    name: nginx-deployment
    namespace: audit
  - enforcementAction: dryrun
    kind: Deployment
    message: nginx in the Deployment nginx-deployment allows privilege escalation
```

snyk

Demo

snyk

Conclusions and the future

If all you remember is...

Policy throughout the application lifecycle

Make adopting good development practice easier

Continuously enforce policy, and provide fast feedback to developers

Gate your clusters against violations, and continuously audit workloads

1. Open Source is pretty great

OPA makes building on top easy. Conftest went from me hacking on something to 6 core maintainers in 6 months.

Thanks tsandall, xchapter7x, brendanjryan, Proplex, jpreese, boranx and Blokje5

snyk

2. A Policy Toolkit

OPA and Conftest are not tool or platform specific. That leaves lots of room for more domain specific tools built on-top.

3. Lets get sharing

A lot of policy is at the organisation or community level, not per project. Lots of potential for reuse and sharing. **This is the next frontier for policy as code.**

Thanks

And any questions?

snyk