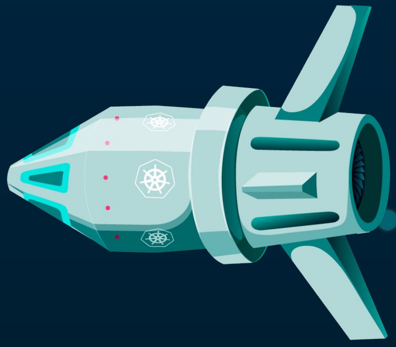
datree



A Deep Dive Into Kubernetes Schema Validation

OWASP New Zealand

Thank You to Our Sponsors and Hosts!

OWASP NEW ZEALAND
owasp.org.nz

QUANTUM SECURITY

AUT

CyberCX

DATACOM

snyk

Auth0

Checkmarx

HCL AppScan

kordia®

LATERAL SECURITY

MICRO FOCUS®

Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA™
Information Security

Cobalt

LACEWORK.

SecureFlag

Without them, OWASP New Zealand Day couldn't happen

What is Kubernetes Schema validation?

Tēnā koutou katoa – טנא קאוטו קאטואה
Nō Iharaira ahau – נו איהררידה אחהו
Ko Eyar Zilberman taku ingoa – קו אייר זילברמן טאקו אינגואה
Tēnā koutou, tēnā koutou, tēnā koutou katoa

–––

Hello everyone – שלום לכולם
Thank you for joining me – תודה שהצטרפתם אלי
To hear my session – לשמוע את ההרצאה שלי

$ whoami

👋 I’m Eyar Zilberman

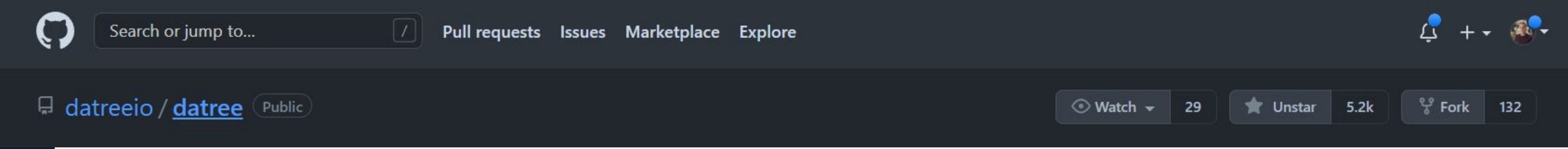
🎩 I’m a developer & YAML engineer

🎩 I’m co-founder and leading the product @ Datree

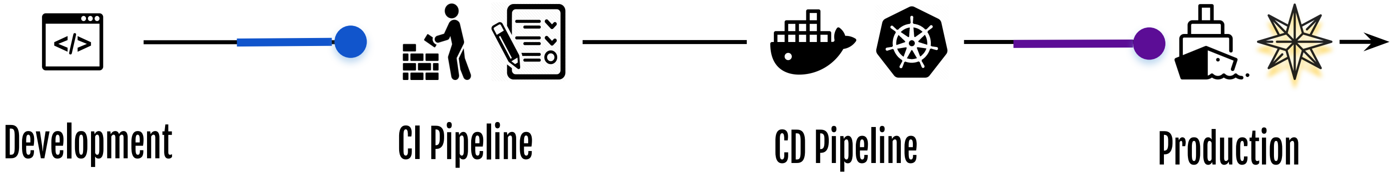
🎩 I founded and orgenzing the biggest GitHub Users Group (IL)

😍 I love RegEx

😨 But hate SQL



datreeio / datree Public



Development

CI Pipeline

CD Pipeline

Production

What is Kubernetes Schema validation?

🧪 Set of “unit tests” to verify manifest contains the correct properties (key:value)

[x] K8s.yaml

```
apiVersion: apps/v1
kind: deployment
metaData:
  name: rss-site
  nameSpace: test
  labels:
    app: web
```

[v] K8s.yaml

```
apiVersion: apps/v1
kind: Deployment
metaData:
  name: rss-site
  namespace: test
  labels:
    app: web
```

🚢 The schema definition is provided by the community

What is not part of the schema validation?

- YAML syntax validation
  - E.g. correct indentation
- Best practices
  - E.g. each container has a configured Memory and CPU limit set
- Team/org policies
  - E.g. pull all images from private registry (artifactory.io/nginx:1.16.8)
- Some validations that you expect to be part of the schema
  - E.g. no spoilers!

I’m sold! How do I use it?

Good news 😊

- Activated by default when you apply configs to your cluster

Bad news 😔

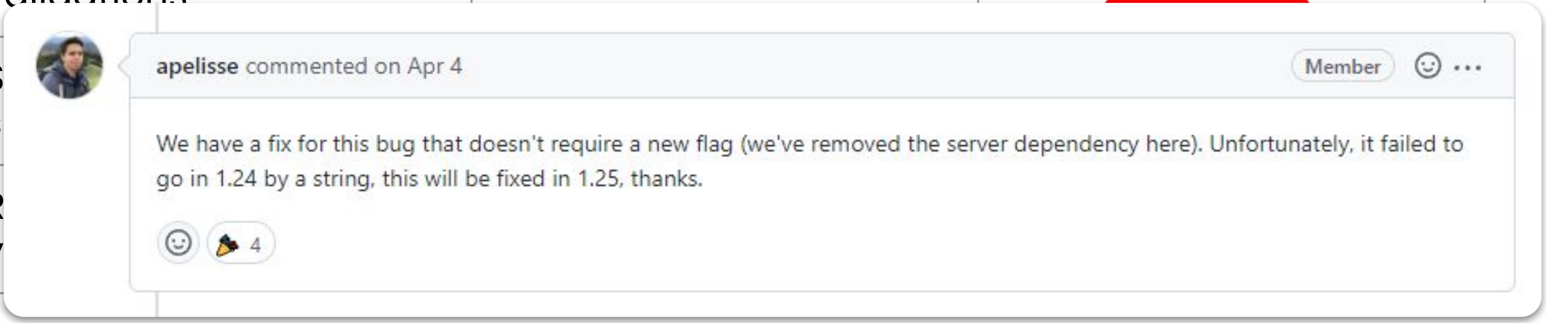
- It’s too late!

⬅️ How to check it earlier (“shift-left”)?

- `kubectl --dry-run=client/server`

kubectl server vs. client

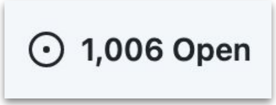
Parameter	Server mode	lient mod
Preform schema validation?	Yes	Ye
Preform extra validations?	Yes	
S s		
R y		



apelisse commented on Apr 4

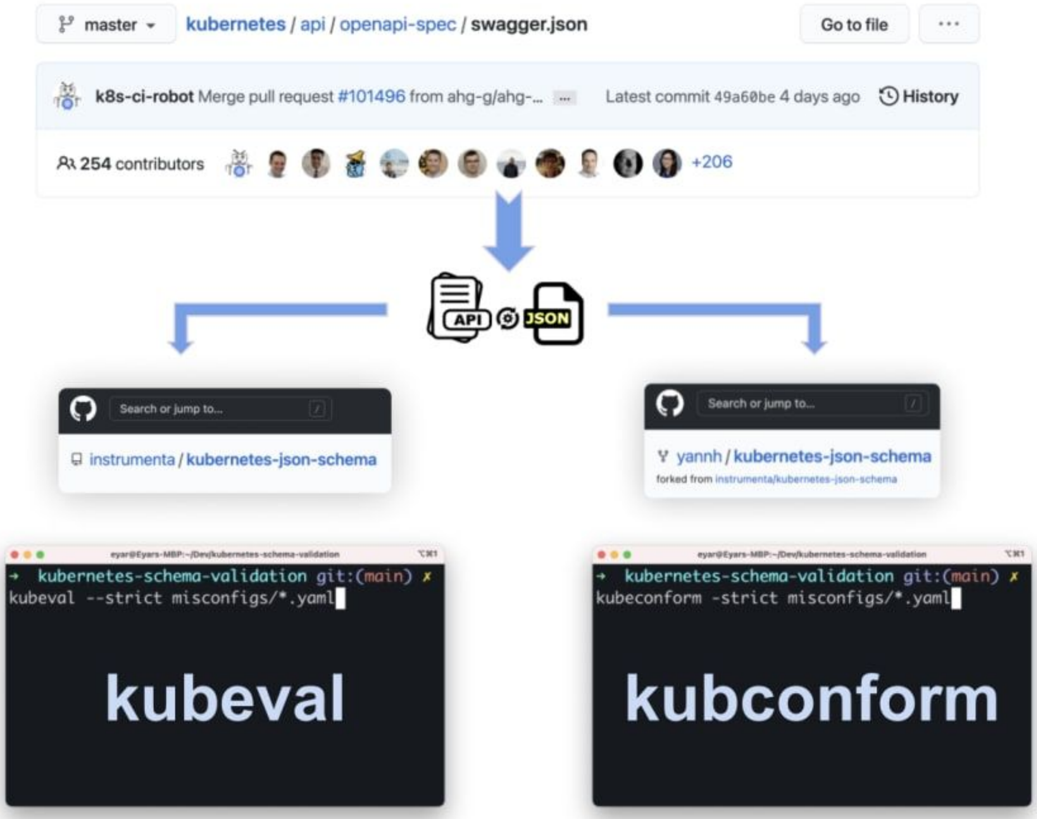
We have a fix for this bug that doesn't require a new flag (we've removed the server dependency here). Unfortunately, it failed to go in 1.24 by a string, this will be fixed in 1.25, thanks.

BUG: kubernetes/kubernetes/issues/51475



1,006 Open

Open-source to the rescue!



master kubernetes / api / openapi-spec / swagger.json

k8s-ci-robot Merge pull request #101496 from ahg-g/ahg-... Latest commit 49a60be 4 days ago History

254 contributors +206

instrumenta / kubernetes-json-schema

yannh / kubernetes-json-schema
forked from instrumenta/kubernetes-json-schema

```
eyar@Eyars-MBP:~/Dev/kubernetes-schema-validation
→  kubernetes-schema-validation git:(main) ✗
kubeval --strict misconfigs/*.yaml
```

kubeval

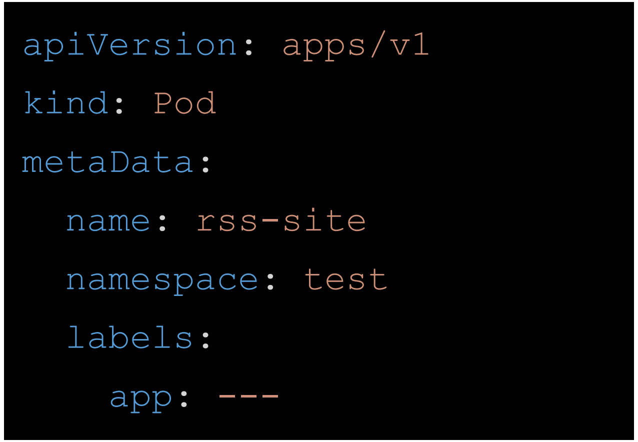
```
eyar@Eyars-MBP:~/Dev/kubernetes-schema-validation
→  kubernetes-schema-validation git:(main) ✗
kubeconform -strict misconfigs/*.yaml
```

kubconform

kubectl vs. open-source

Let’s QA - take #1

invalid-labels-value.yaml



```yaml
apiVersion: apps/v1
kind: Pod
metaData:
  name: rss-site
  namespace: test
  labels:
    app: ---
```

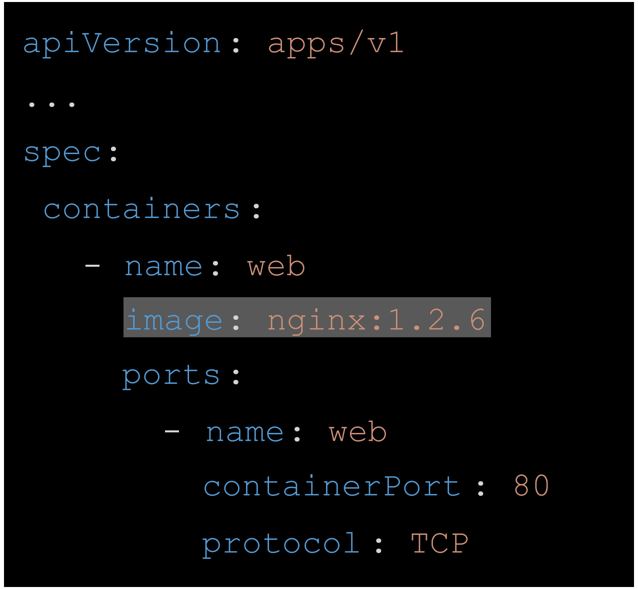
[Catching] kubectl --dry-run=server

[Not catching] kubeval / kubeconform

```
The Pod "invalid-labels-value" is invalid: metadata.labels: Invalid value: "---": a valid label must be an empty string or consist of alphanumeric characters, '-', '' or '.', and must start and end with an alphanumeric character (e.g. 'MyValue', or 'my_value', or '12345', regex used for validation is '(([A-Za-z0-9][-A-Za-z0-9.]*)?[A-Za-z0-9])?')
```

Let’s QA - take #2

missing-image.yaml



```
apiVersion: apps/v1
...
spec:
 containers:
    - name: web
      image: nginx:1.2.6
      ports:
        - name: web
          containerPort: 80
          protocol: TCP
```

[Catching] kubectl --dry-run=server

[Not catching] kubeval / kubeconform

What is not part of the schema validation?

- YAML syntax validation
    - E.g. correct indentation
- Best practices
    - E.g. each container has a configured Memory and CPU limit set
- Team/org policies
    - E.g. pull all images from private registry (artifactory.io/nginx:1.16.8)
- Some validations that you expect to be part of the schema
    - E.g. no spoilers!

Winner?

A connection to your cluster is allowed?

kubectl --dry-run=server

A connection to your cluster is *NOT* allowed?

Kubeval or Kubeconform

kubeval vs. kubeconform

Kubernetes versions support

👎 Kubeval - instrumenta/kubernetes-json-schema

(last commit: 133f848 on April 29, 2020)

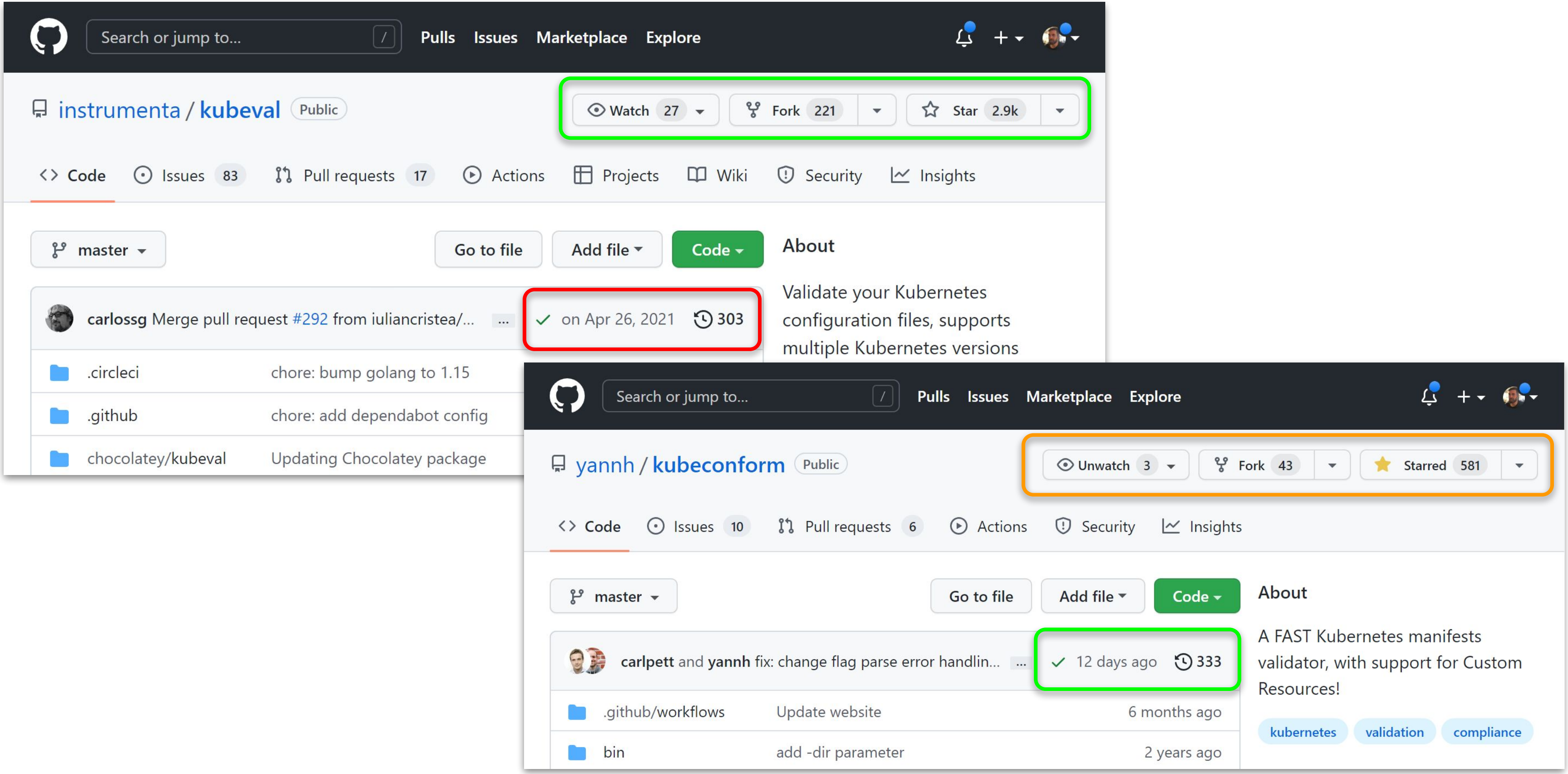
- v1.5.0 - v1.18.1

👍 Kubeconform - yannh/kubernetes-json-schema

(last commit: 14652b0on Jun 17, 2022)

- v1.15.0 - v1.24.2

Community



Search or jump to... / Pulls Issues Marketplace Explore

instrumenta / kubeval Public

Watch 27 · Fork 221 · Star 2.9k

Code · Issues 83 · Pull requests 17 · Actions · Projects · Wiki · Security · Insights

master · Go to file · Add file · Code

carlossg Merge pull request #292 from iuliancristea/... ✓ on Apr 26, 2021 · 303

.circleci	chore: bump golang to 1.15
.github	chore: add dependabot config
chocolatey/kubeval	Updating Chocolatey package

About

Validate your Kubernetes configuration files, supports multiple Kubernetes versions

Search or jump to... / Pulls Issues Marketplace Explore

yannh / kubeconform Public

Unwatch 3 · Fork 43 · Starred 581

Code · Issues 10 · Pull requests 6 · Actions · Security · Insights

master · Go to file · Add file · Code

carlpett and yannh fix: change flag parse error handlin... ✓ 12 days ago · 333

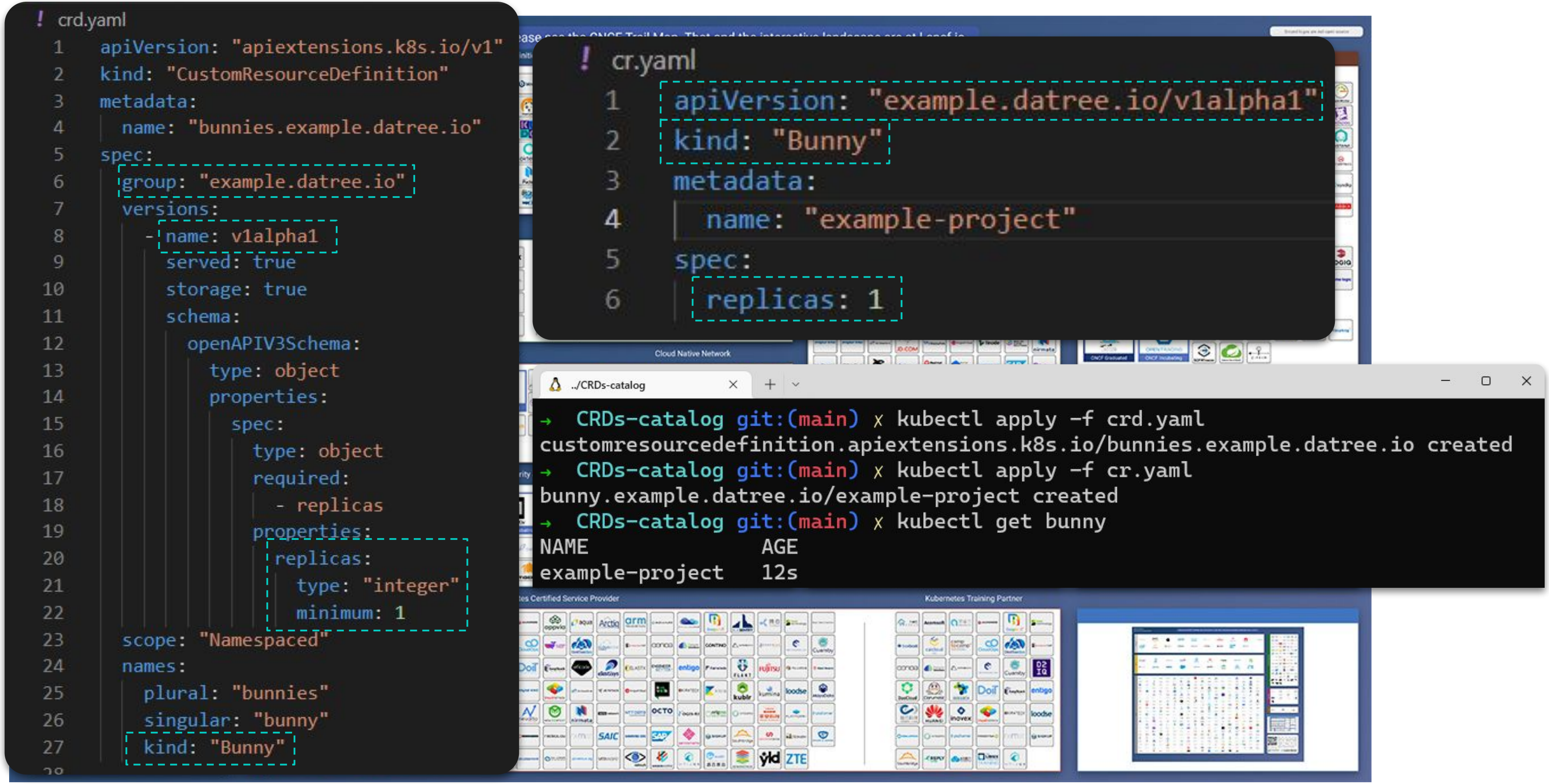
.github/workflows	Update website	6 months ago
bin	add -dir parameter	2 years ago

About

A FAST Kubernetes manifests validator, with support for Custom Resources!

kubernetes · validation · compliance

CRDs support



crd.yaml

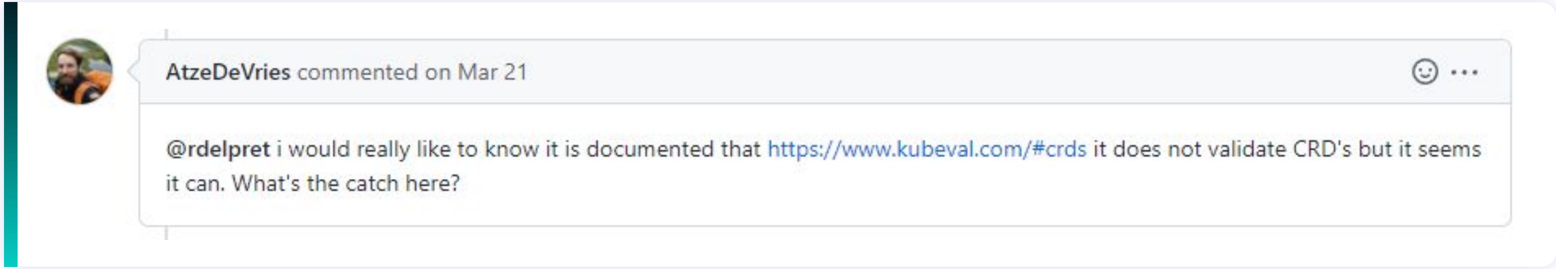
```yaml
apiVersion: "apiextensions.k8s.io/v1"
kind: "CustomResourceDefinition"
metadata:
  name: "bunnies.example.datree.io"
spec:
  group: "example.datree.io"
  versions:
    - name: v1alpha1
      served: true
      storage: true
      schema:
        openAPIV3Schema:
          type: object
          properties:
            spec:
              type: object
              required:
                - replicas
              properties:
                replicas:
                  type: "integer"
                  minimum: 1
  scope: "Namespaced"
  names:
    plural: "bunnies"
    singular: "bunny"
    kind: "Bunny"
```

cr.yaml

```yaml
apiVersion: "example.datree.io/v1alpha1"
kind: "Bunny"
metadata:
  name: "example-project"
spec:
  replicas: 1
```

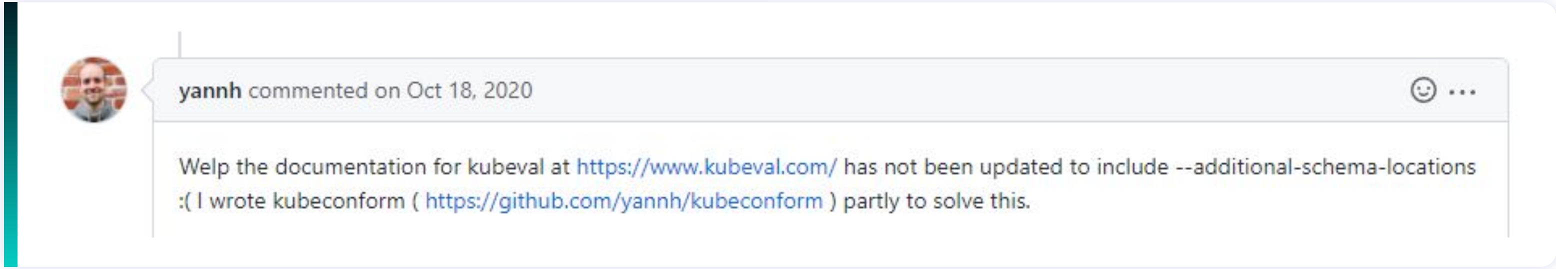
```
→ CRDs-catalog git:(main) ✗ kubectl apply -f crd.yaml
customresourcedefinition.apiextensions.k8s.io/bunnies.example.datree.io created
→ CRDs-catalog git:(main) ✗ kubectl apply -f cr.yaml
bunny.example.datree.io/example-project created
→ CRDs-catalog git:(main) ✗ kubectl get bunny
NAME              AGE
example-project   12s
```

CRDs support



AtzeDeVries commented on Mar 21

@rdelpret i would really like to know it is documented that https://www.kubeval.com/#crds it does not validate CRD's but it seems it can. What's the catch here?



yannh commented on Oct 18, 2020

Welp the documentation for kubeval at https://www.kubeval.com/ has not been updated to include --additional-schema-locations :(I wrote kubeconform (https://github.com/yannh/kubeconform) partly to solve this.

Winner?

kubeconform!

Strategies for validating Kubernetes schema

⬅️ Shift-left

The sooner, the better but not at all cost.

Prefer to restrict access to your cluster.

🚔 Fill the gap

Run with a policy enforcement tool to fill server side validation.

E.g. Datree / Conftest / Kyverno / Etc.

⏳ Version upgrade

Each K8s version is supported for only 14 months.

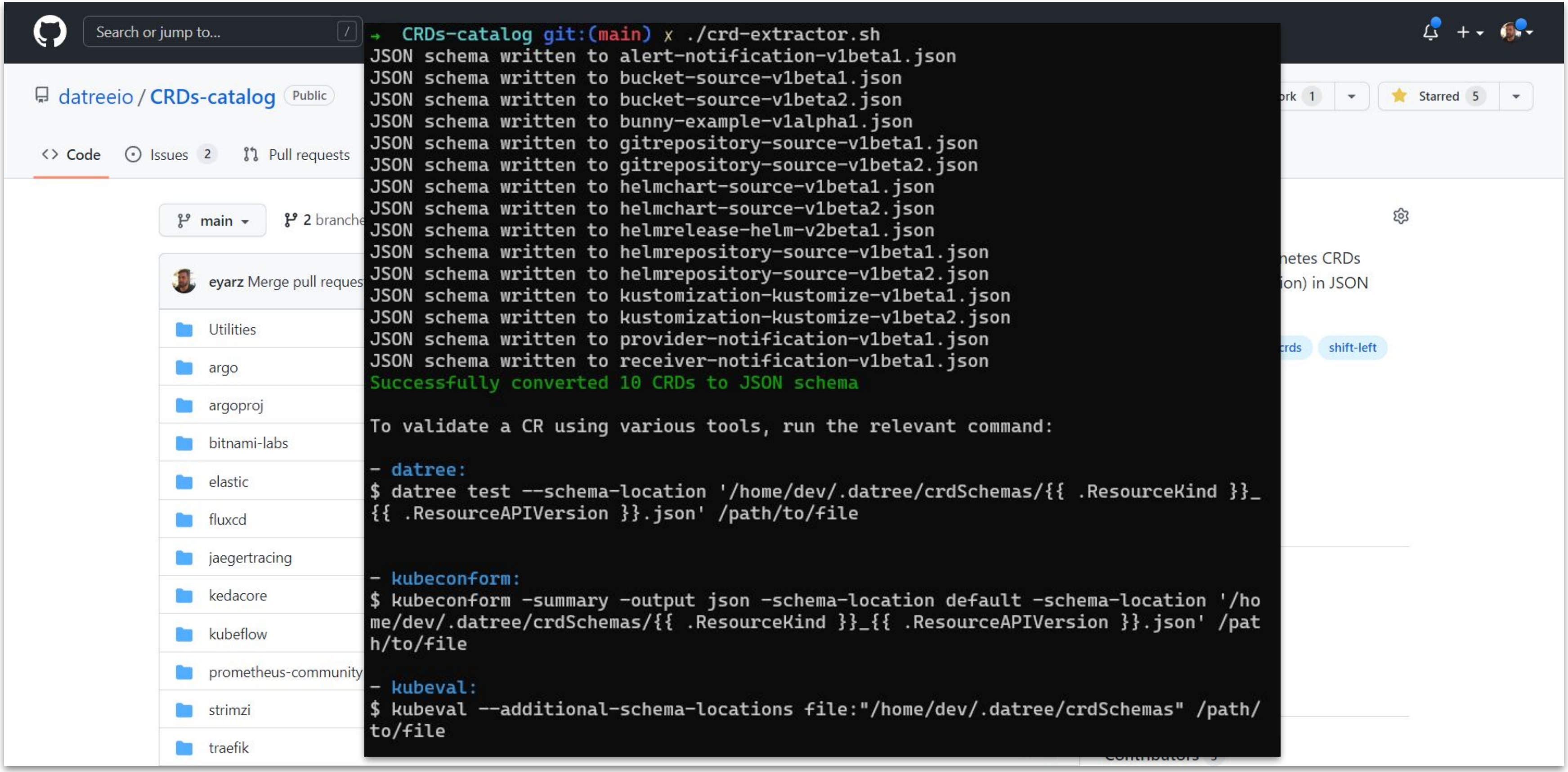
Every release, there are API changes (deprecation).

🙈 Validate CRDs

Extract CRDs, convert to JSON Schema & configure as source.

This is why we started the CRDs-catalog project

CRDs-catalog project



```
→  CRDs-catalog git:(main) ✗ ./crd-extractor.sh
JSON schema written to alert-notification-v1beta1.json
JSON schema written to bucket-source-v1beta1.json
JSON schema written to bucket-source-v1beta2.json
JSON schema written to bunny-example-v1alpha1.json
JSON schema written to gitrepository-source-v1beta1.json
JSON schema written to gitrepository-source-v1beta2.json
JSON schema written to helmchart-source-v1beta1.json
JSON schema written to helmchart-source-v1beta2.json
JSON schema written to helmrelease-helm-v2beta1.json
JSON schema written to helmrepository-source-v1beta1.json
JSON schema written to helmrepository-source-v1beta2.json
JSON schema written to kustomization-kustomize-v1beta1.json
JSON schema written to kustomization-kustomize-v1beta2.json
JSON schema written to provider-notification-v1beta1.json
JSON schema written to receiver-notification-v1beta1.json
Successfully converted 10 CRDs to JSON schema

To validate a CR using various tools, run the relevant command:

- datree:
$ datree test --schema-location '/home/dev/.datree/crdSchemas/{{ .ResourceKind }}_
{{ .ResourceAPIVersion }}.json' /path/to/file


- kubeconform:
$ kubeconform -summary -output json -schema-location default -schema-location '/ho
me/dev/.datree/crdSchemas/{{ .ResourceKind }}_{{ .ResourceAPIVersion }}.json' /pat
h/to/file

- kubeval:
$ kubeval --additional-schema-locations file:"/home/dev/.datree/crdSchemas" /path/
to/file
```

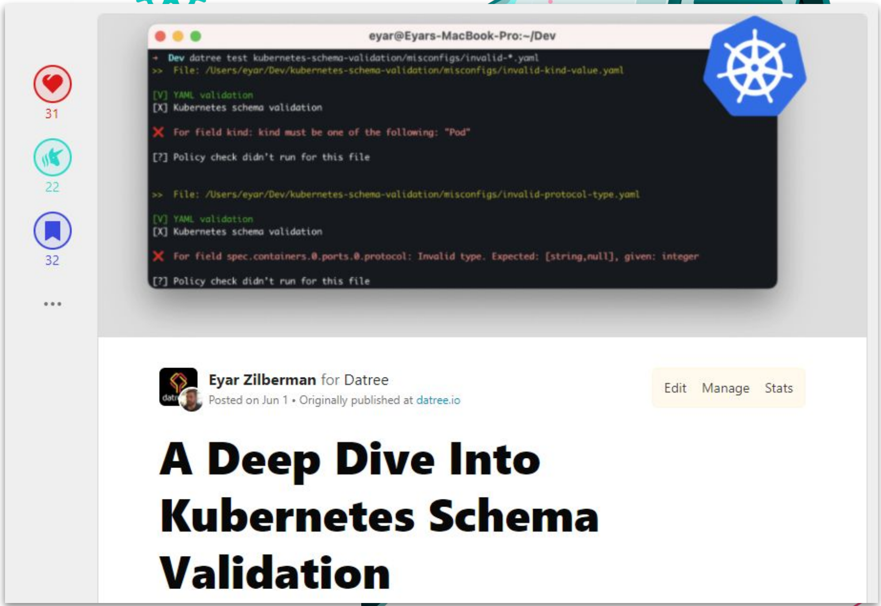
Where to find me

GitHub: eyarz

Email: eyar@datree.io

Linkedin: eyar-zilberman

eyarz / pink-bunny-ears Public



```
→  Dev datree test kubernetes-schema-validation/misconfigs/invalid-*.yaml
>>  File: /Users/eyar/Dev/kubernetes-schema-validation/misconfigs/invalid-kind-value.yaml

[V] YAML validation
[X] Kubernetes schema validation

❌  For field kind: kind must be one of the following: "Pod"

[?] Policy check didn't run for this file


>>  File: /Users/eyar/Dev/kubernetes-schema-validation/misconfigs/invalid-protocol-type.yaml

[V] YAML validation
[X] Kubernetes schema validation

❌  For field spec.containers.0.ports.0.protocol: Invalid type. Expected: [string,null], given: integer

[?] Policy check didn't run for this file
```

Eyar Zilberman for Datree

Posted on Jun 1 • Originally published at datree.io

A Deep Dive Into Kubernetes Schema Validation

datree

Thank You