

A black and white photograph of a hand scratching a vinyl record on a turntable. The hand is positioned on the left side of the record, with fingers spread. The turntable is on the right, and the record is spinning. The background is dark and out of focus, showing some light sources.

K8s Admission Controllers from scratch

By Steve Giguere

bridgecrew
BY PRISMA CLOUD

Meet the Proctors



Steve Giguere

Developer Advocate - Bridgecrew



Matt Johnson

DevRel Lead - Prisma Cloud



Angela Gizzi

Technical Marketing - PANW

An admission controller is a piece of code that intercepts requests to the Kubernetes API server before the persistence of the object, but after the request is authenticated and authorized.

*Validating Admission Controllers are the last line of
defense to block potentially dangerous
misconfigurations from making it into your cluster and
save you from yourself*

Type of Dynamic Admission Controllers

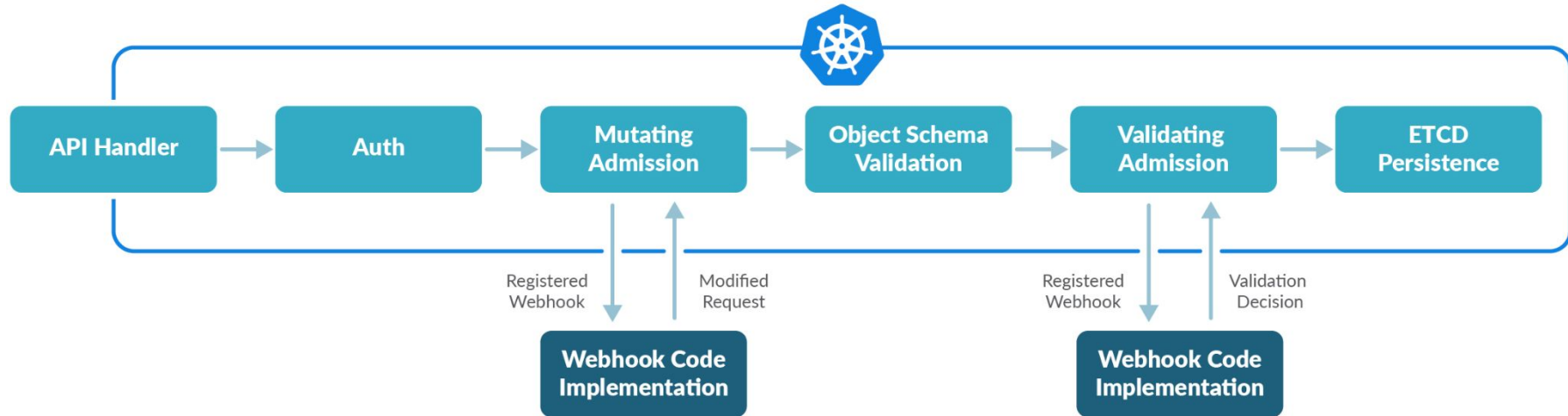
Validating Admission Webhook (our workshop)

- This admission controller calls webhooks, passing an Admission Review request to validate an incoming Kubernetes manifest matching the webhook's Admission Configuration. If the webhook rejects the request, the request fails and the object is not persisted in the cluster

Mutating Admission Webhook (not used in this workshop)

- This admission controller calls webhooks, which may modify/mutate (as implied by the name) the object if it desired. Note these run before Validation Admission Webhooks.

Anatomy of an admission controller

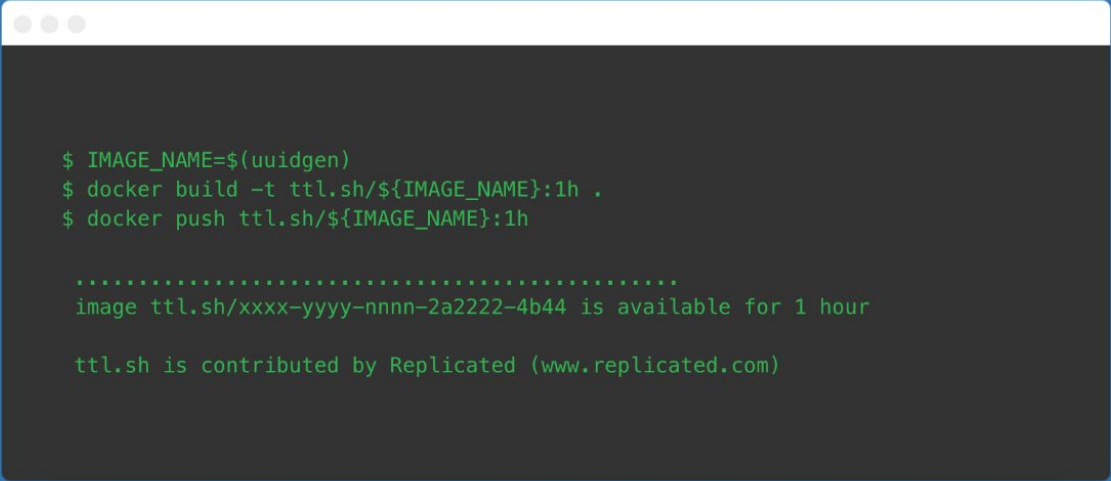


Credit: Sysdig

Our Admission Controller Container

- Gunicorn
- WSGI.py (conductor)
- Python based Flask application receiving on a single /validate route
 - All of the above built into a container image
- Admission Configuration
- K8s Deployment
- TLS Certs
 - Deployed as K8s secret
- K8s Service
 - ClusterIP

Anonymous & ephemeral Docker image registry



```
$ IMAGE_NAME=$(uuidgen)
$ docker build -t ttl.sh/${IMAGE_NAME}:1h .
$ docker push ttl.sh/${IMAGE_NAME}:1h

.....
image ttl.sh/xxxx-yyyy-nnnn-2a2222-4b44 is available for 1 hour

ttl.sh is contributed by Replicated (www.replicated.com)
```

Free to use. No need to sign-up. Open source.

What We Don't Cover

- The vast list of built-in Kubernetes admission controllers
- The new alpha feature of validating admission controller using CEL
 - CEL = Common Expression Language
- How to create a Python based Flask application
 - We provide a basic frameworks for you
- Deep knowledge of K8s manifests
 - We do teach how to generate some manifests
 - We also provide manifests where generation isn't possible
- Kubectl deep dive
 - All commands are provided with explanation

Prerequisites

- A laptop
- A Kubernetes cluster (**provided**)
- Fundamental knowledge of the Python programming language
- Basic knowledge of 'kubectl'
- Our Instruqt workshop invitation
- Also posted in the CNCF slack channel
 - **#cnsc-ac-workshop**

<https://play.instruqt.com/bridgecrew/invite/ppgm8jb1av8d>



Takeaways

- The value of admission controllers
- The basics of how an admission controller works
- How to build a basic admission controller to block, based on a simple rule
- What a secure K8s manifest looks like!
- How to take that to the next level by adding a policy as code engine (Checkov)
- Policy consistency across the SDLC is important!
- Whorf, the result of our own Admission Controller journey

Let's get started!

We'd love to hear from you!

Leave us your feedback below and come visit us to chat more & pick up some swag at **Booth G11**.

1-Minute Feedback Form:

