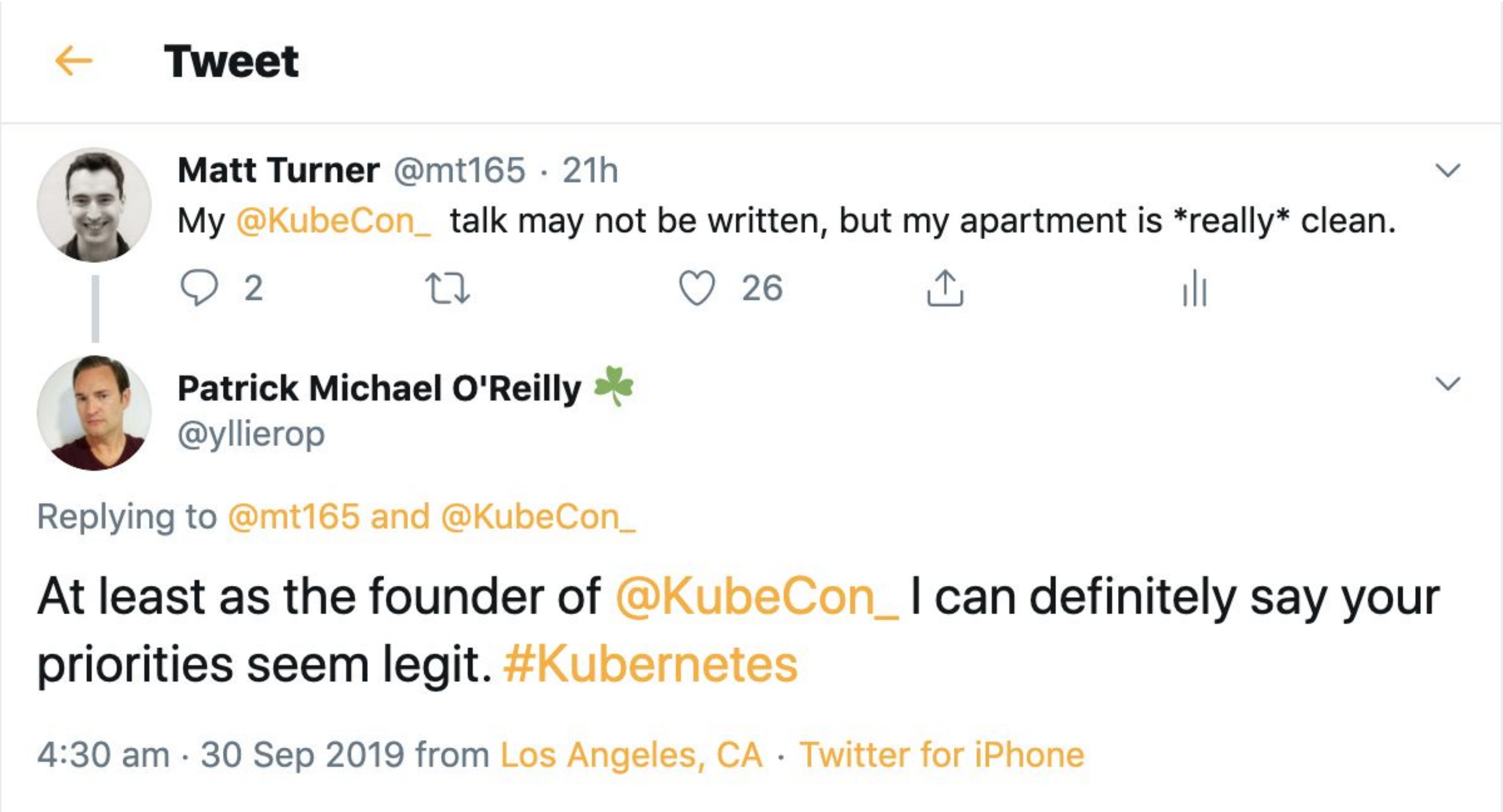
Walk-through: Debugging an RBAC Problem in Istio

(but without the swearing)

Matt Turner

@mt165 | mt165.co.uk

KubeCon, San Diego California | November 2019 *no fucking promises



Matt Turner @mt165 · 21h

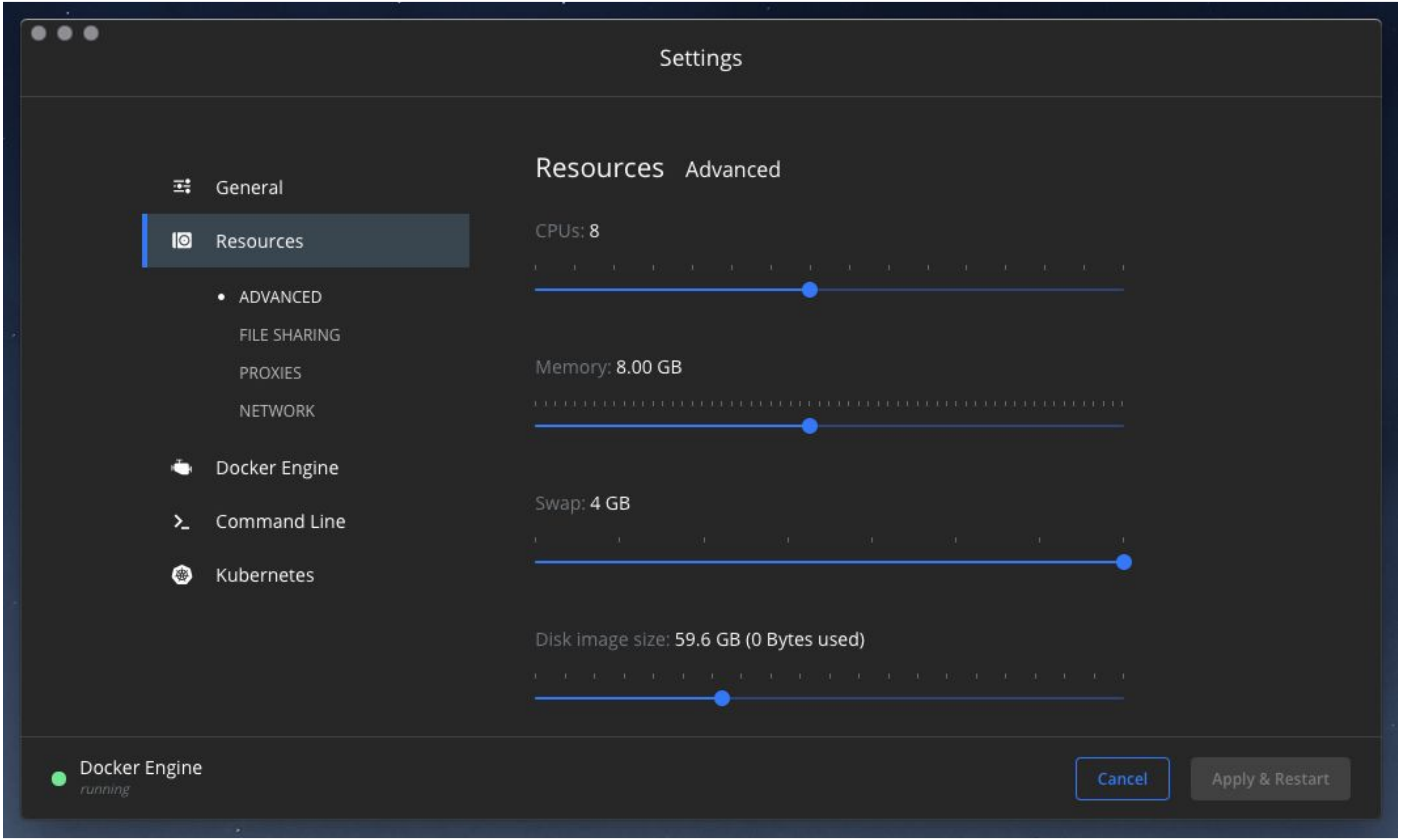
My @KubeCon_ talk may not be written, but my apartment is *really* clean.

Patrick Michael O'Reilly ☘️
@yllierop

Replying to @mt165 and @KubeCon_

At least as the founder of @KubeCon_ I can definitely say your priorities seem legit. #Kubernetes

4:30 am · 30 Sep 2019 from Los Angeles, CA · Twitter for iPhone



Settings

Resources Advanced

CPUs: 8

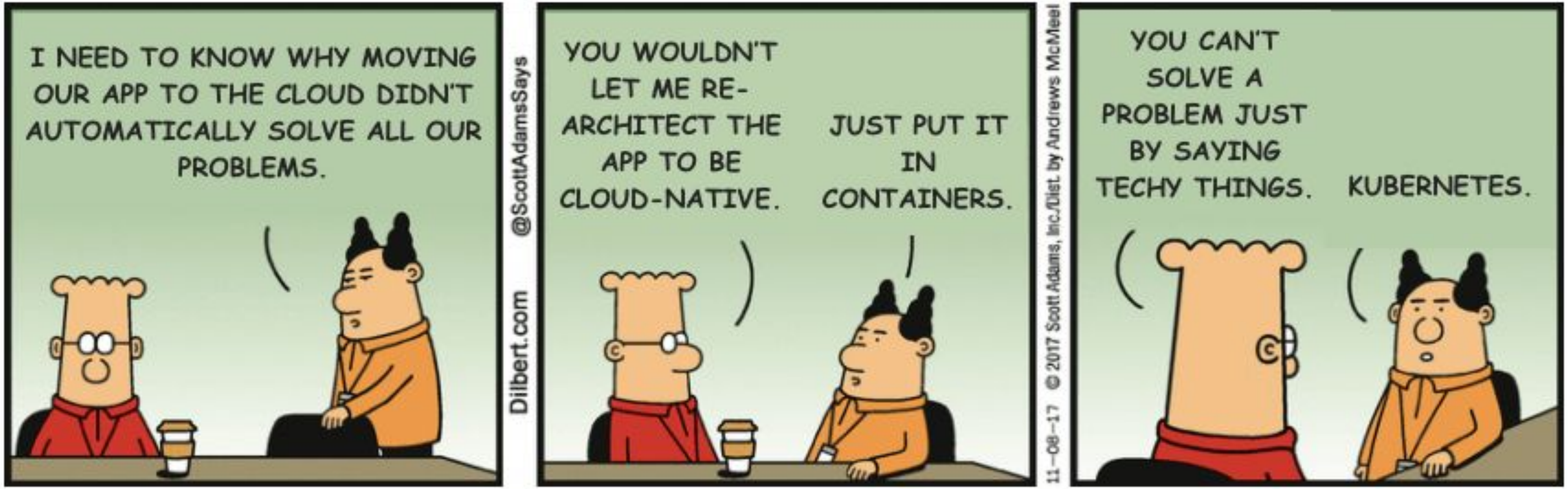
Memory: 8.00 GB

Swap: 4 GB

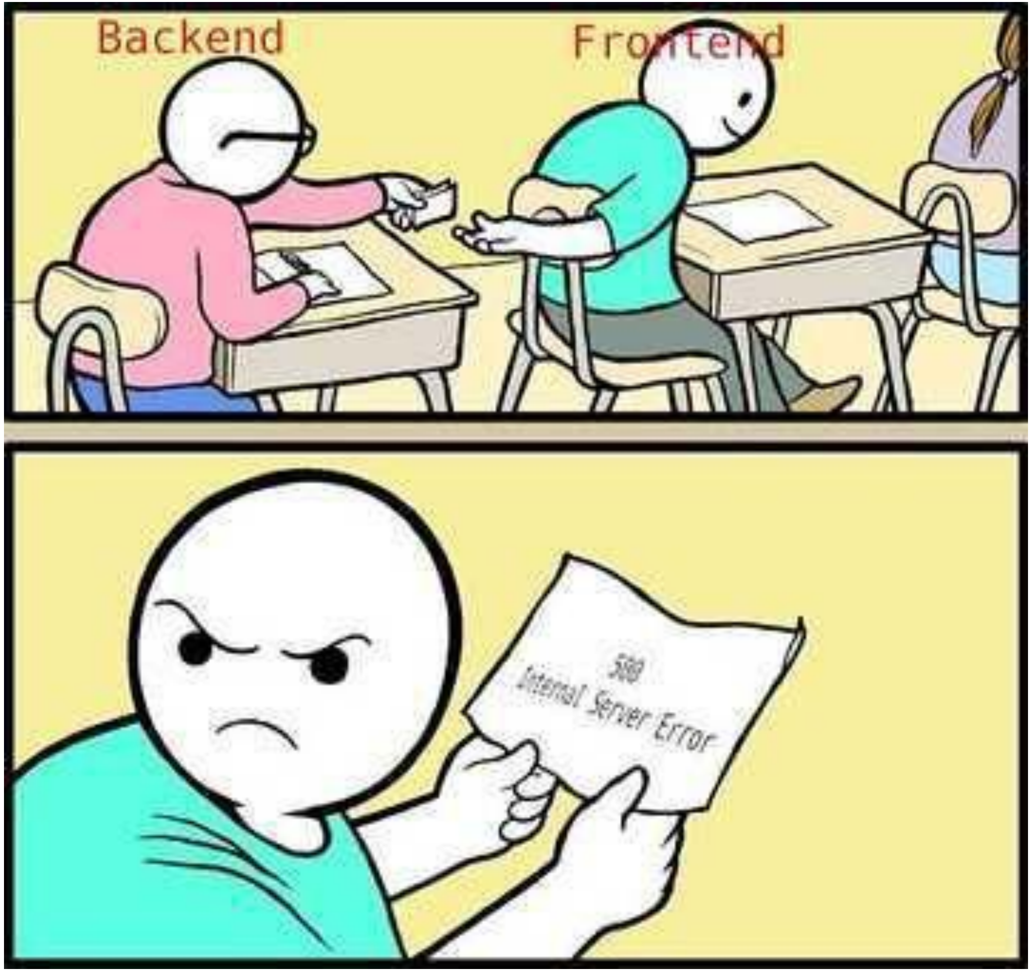
Disk image size: 59.6 GB (0 Bytes used)

Docker Engine
running

Introduction


I NEED TO KNOW WHY MOVING OUR APP TO THE CLOUD DIDN'T AUTOMATICALLY SOLVE ALL OUR PROBLEMS.
@ScottAdamsSays
Dilbert.com
YOU WOULDN'T LET ME RE-ARCHITECT THE APP TO BE CLOUD-NATIVE.
JUST PUT IT IN CONTAINERS.
© 2017 Scott Adams, Inc./Dist. by Andrews McMeel
11-08-17
YOU CAN'T SOLVE A PROBLEM JUST BY SAYING TECHY THINGS.
KUBERNETES.

RBAC: 20, 21


Backend
Frontend
500
Internal Server Error

Forking Shirtballs

Debuggability =
Observability X Controllability

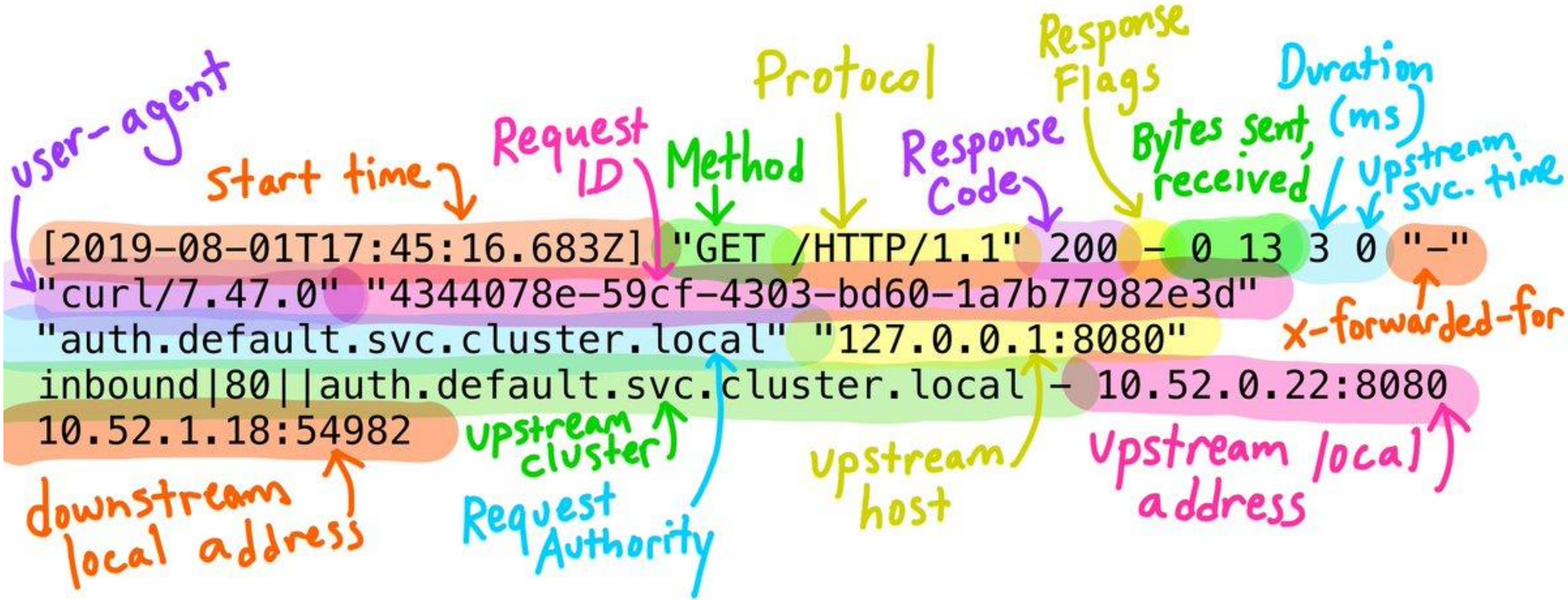
Observability

“... the behaviour of the entire system can be determined by only looking at its inputs and outputs” - Kalman, 1961

The software has a model of the world, which may be wrong.

You have a model of its model, which may be wrong.

Envoy Logs: 30



```
[2019-08-01T17:45:16.683Z] "GET /HTTP/1.1" 200 - 0 13 3 0 "-"
"curl/7.47.0" "4344078e-59cf-4303-bd60-1a7b77982e3d"
"auth.default.svc.cluster.local" "127.0.0.1:8080"
inbound|80||auth.default.svc.cluster.local - 10.52.0.22:8080
10.52.1.18:54982
```

engarde!

Traffic Dump: 31

ksniff!

It’s all meshed up!

Controllability

Permissive RBAC: 32

Change One Thing At A Time
R-BACk on: 20

Follow the Pipeline: 33

Hone in: 34, 35

Guess and check: 36

¿What the actual fuck?

Why? Can do end-user, port, etc based authz

ServiceRole[Binding] will be gone from 1.6, replaced with AuthorizationPolicy

One more: Don’t Panic!

Thanks!

@mt165

Slides
Videos
Demo code

mt165.co.uk