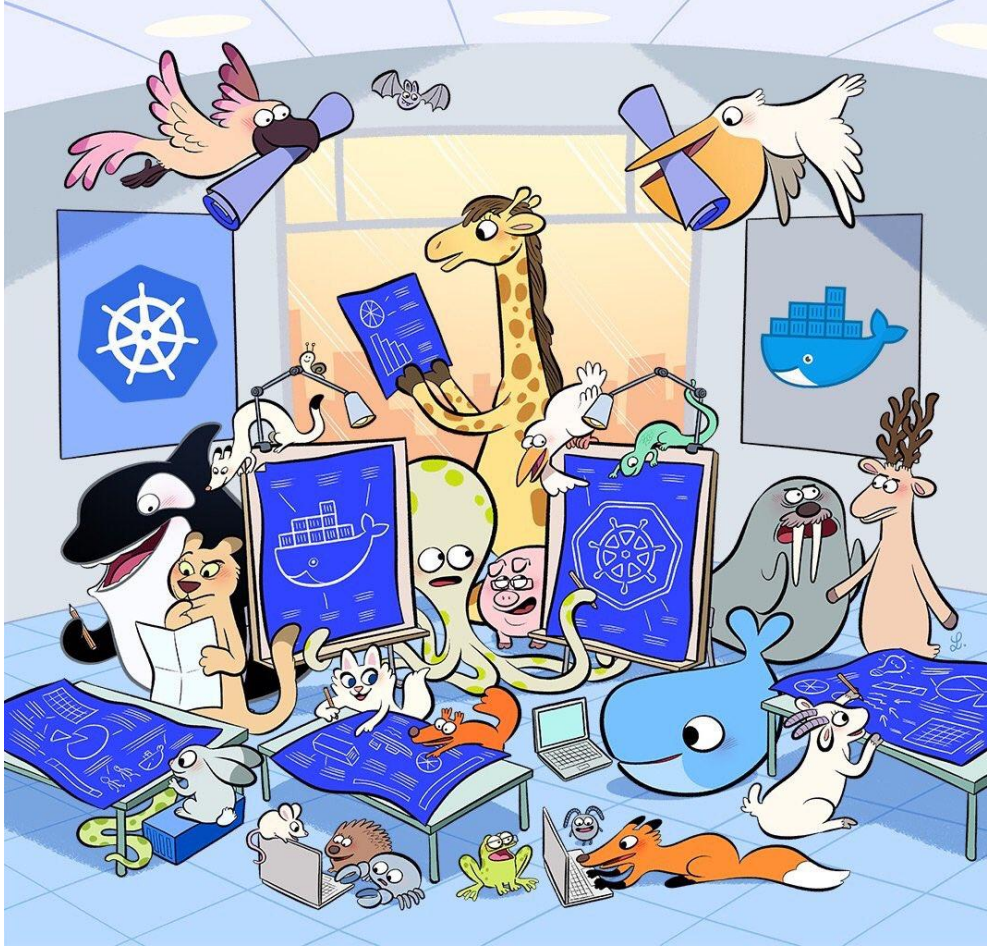
Docker, Kubernetes & Istio

Tips, tricks & tools



Aurélie Vache - @aurelievache / Kevin Davin - @davinkevin

Why this talk?

- Existing talks about Kubernetes for beginners and experts
- Soooo many tools exists!
- No talks with docker, k8s and istio
- And because it’s fun topic to share!

Aurélie Vache

@aurelievache

Developer at Continental

Conferences organizer

Duchess France Leader

Mentor Simplon & Elles Bougent

Technical articles writer

KEVIN DAVIN

@davinkevin

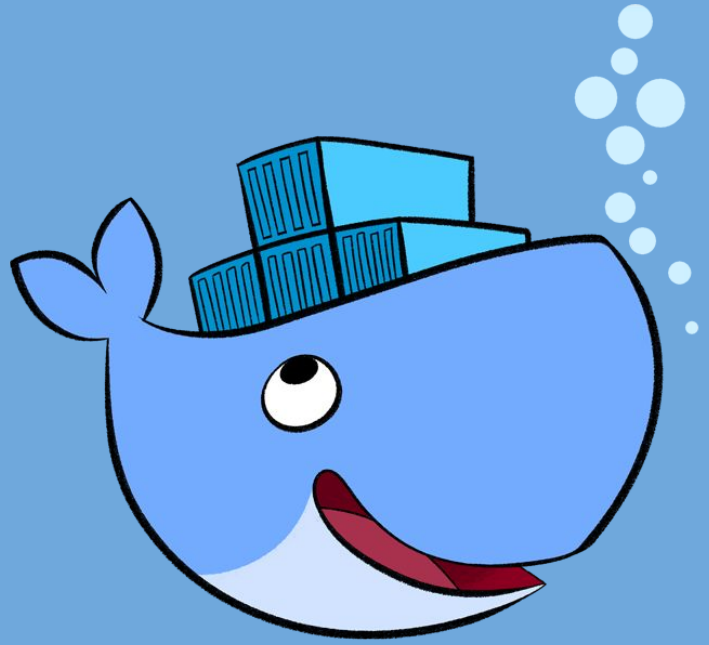
CTO at Stack-Labs

Google **D**eveloper **E**xpert
on Google Cloud

Conferences organizer

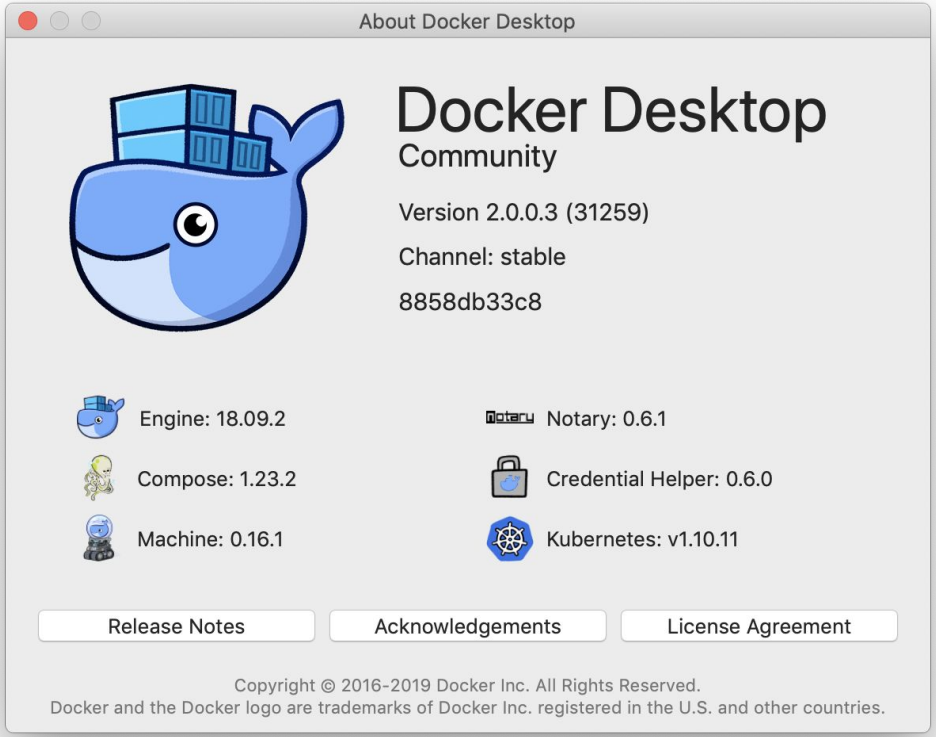
GDG

DevFest Toulouse

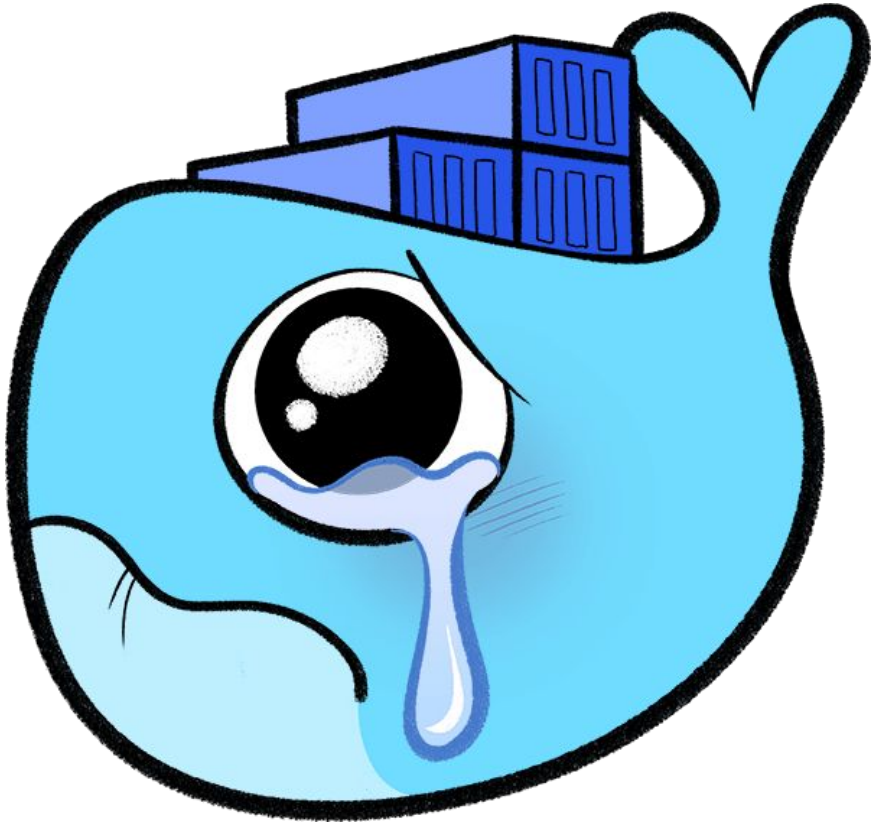


Docker

Use docker for Mac/Windows



Sadly, not available on linux...

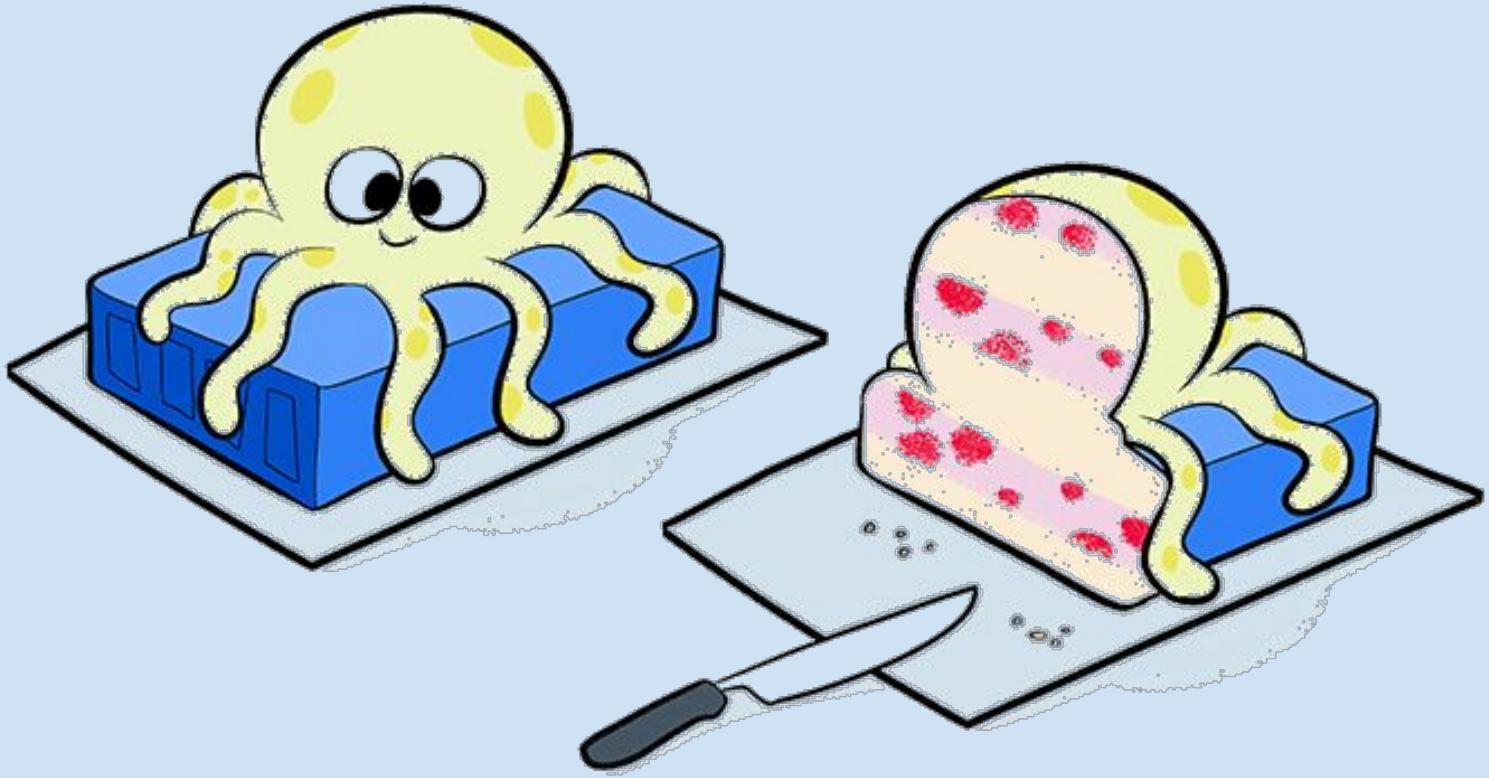


You can use the EDGE version

Docker for mac/windows:
This icon can be your best friends

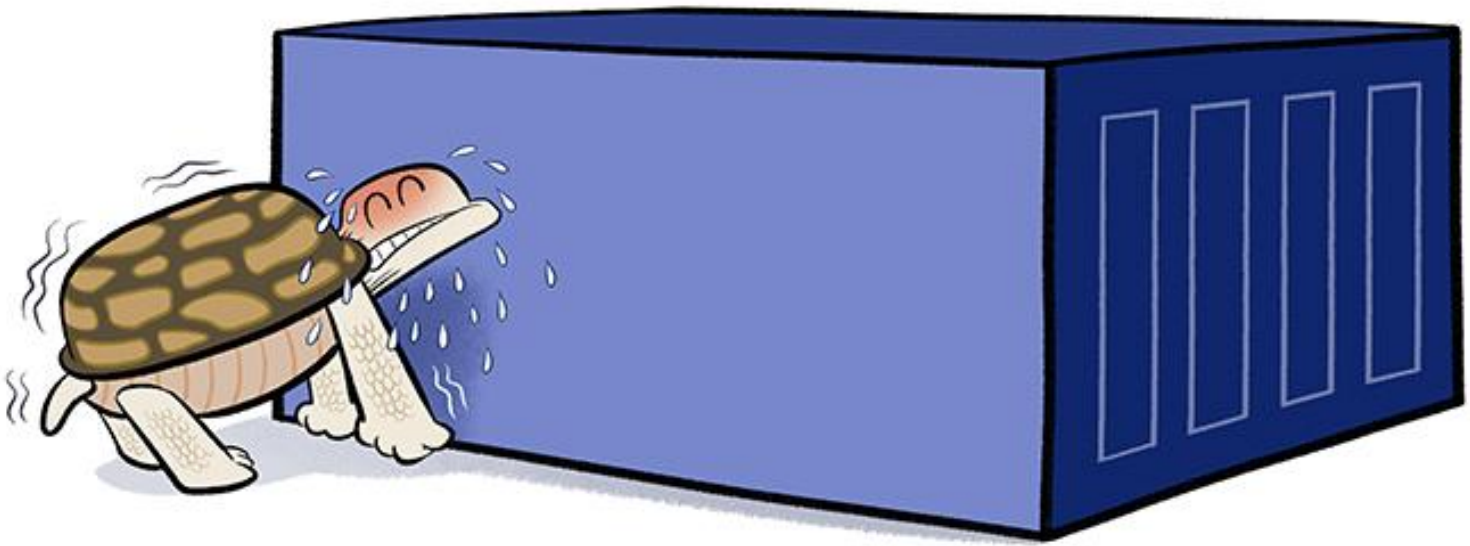
Upgrade your docker stack!

STOP using docker-toolbox



Docker images

How to reduce docker images size?



Keep your Dockerfile simple

```
1176
1177    WORKDIR /opt/podcast-server
1178    ENTRYPOINT ["java","-Djava.security.egd=file:/dev/./urandom",
1179
```

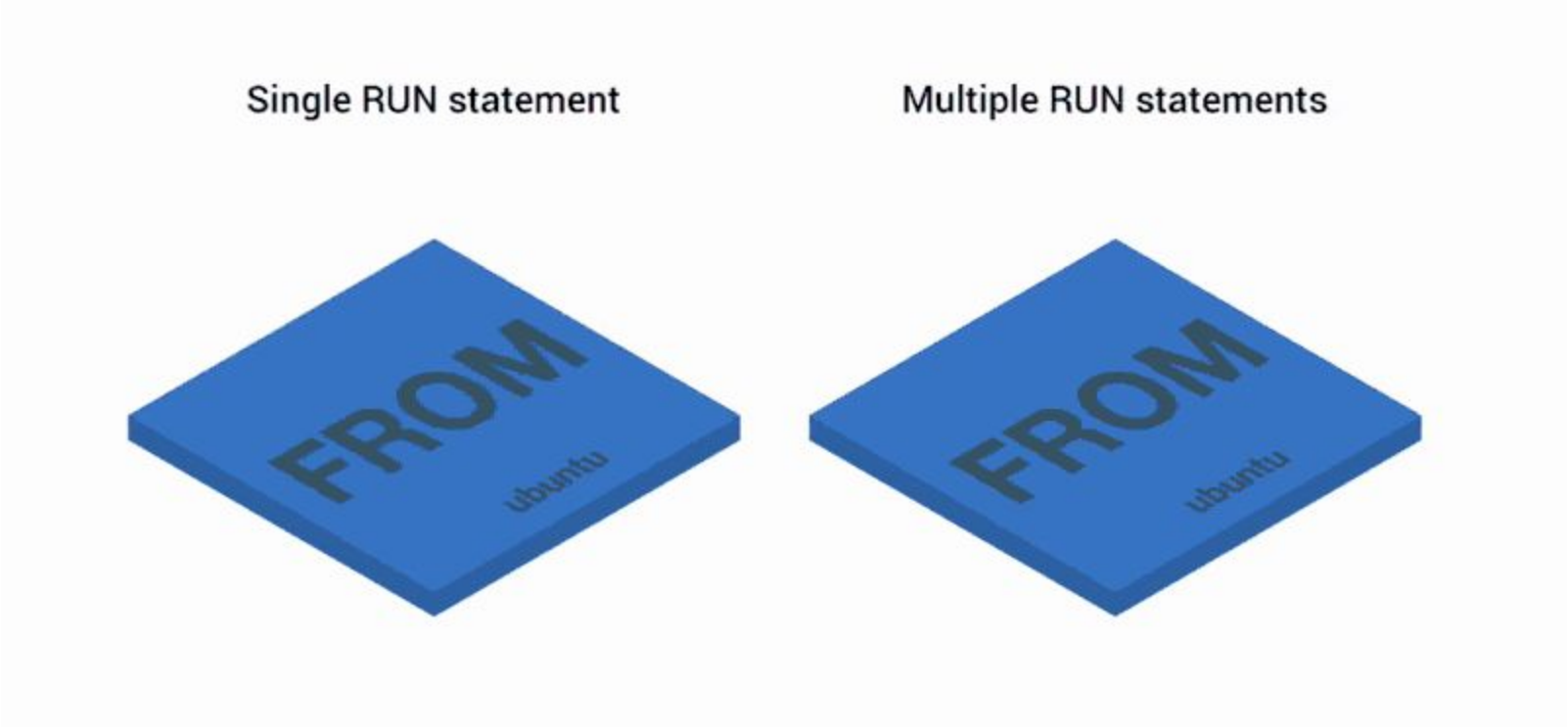
Back to basics

Reduce layers to reduce size

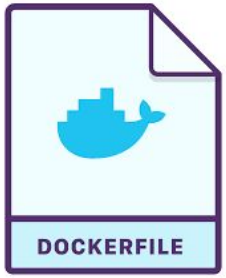
Smaller images =

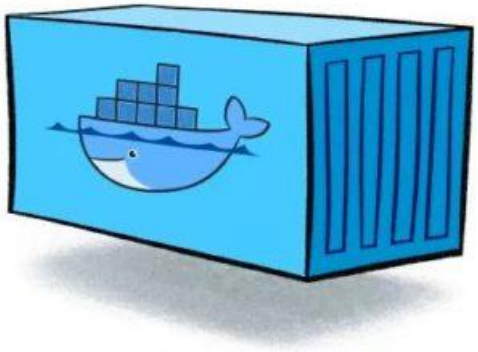
- Faster builds
- Faster deploys
- Smaller attacks surface

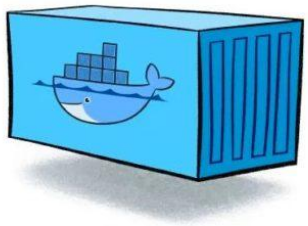
Back to basics
Reduce layers to reduce size



Build smaller images with Multi-stage builds





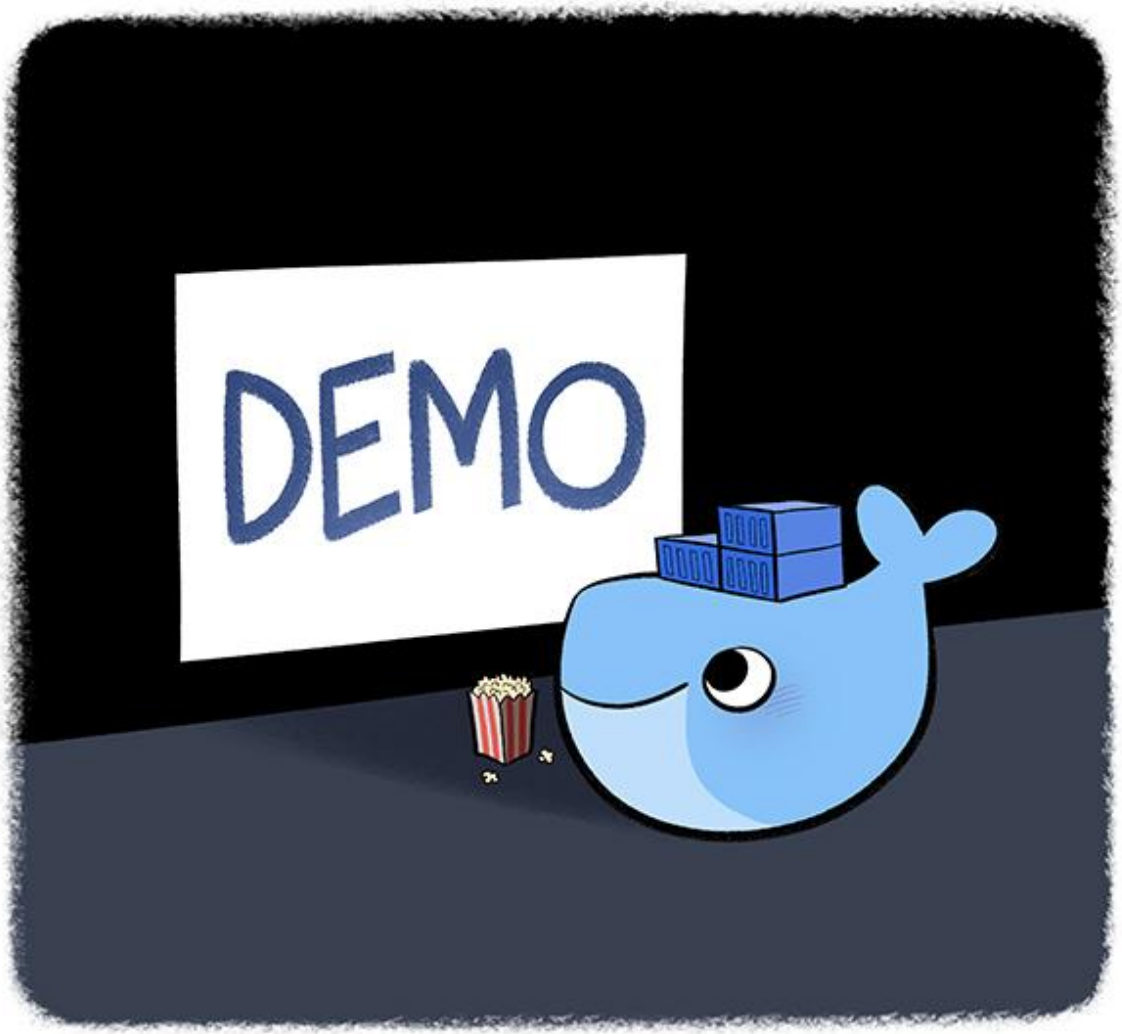


Build environment

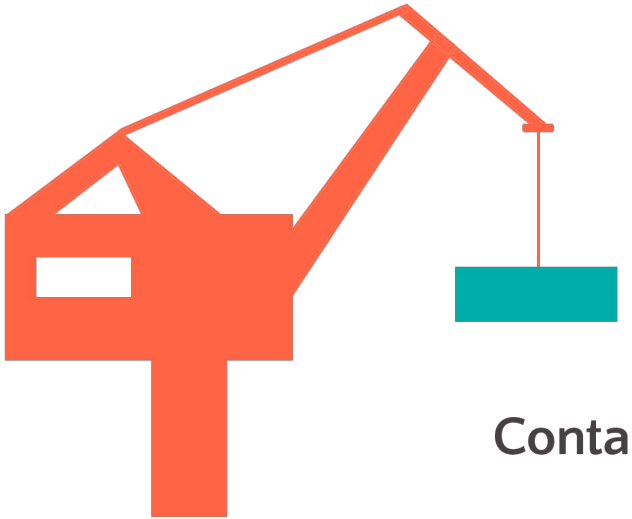
Runtime environment

Build smaller images with Multi-stage builds

```
# Build env
FROM maven:3-jdk-11 AS build
COPY src /app/src
COPY pom.xml /app
RUN mvn -f /app/pom.xml clean package

# Run env
FROM gcr.io/distroless/java:11
COPY --from=build /app/target/app.jar /usr/app/app.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","/usr/app/app.jar"]
```


DEMO

...OR DELETE ALL DOCKERFILE WITH JIB



Jib

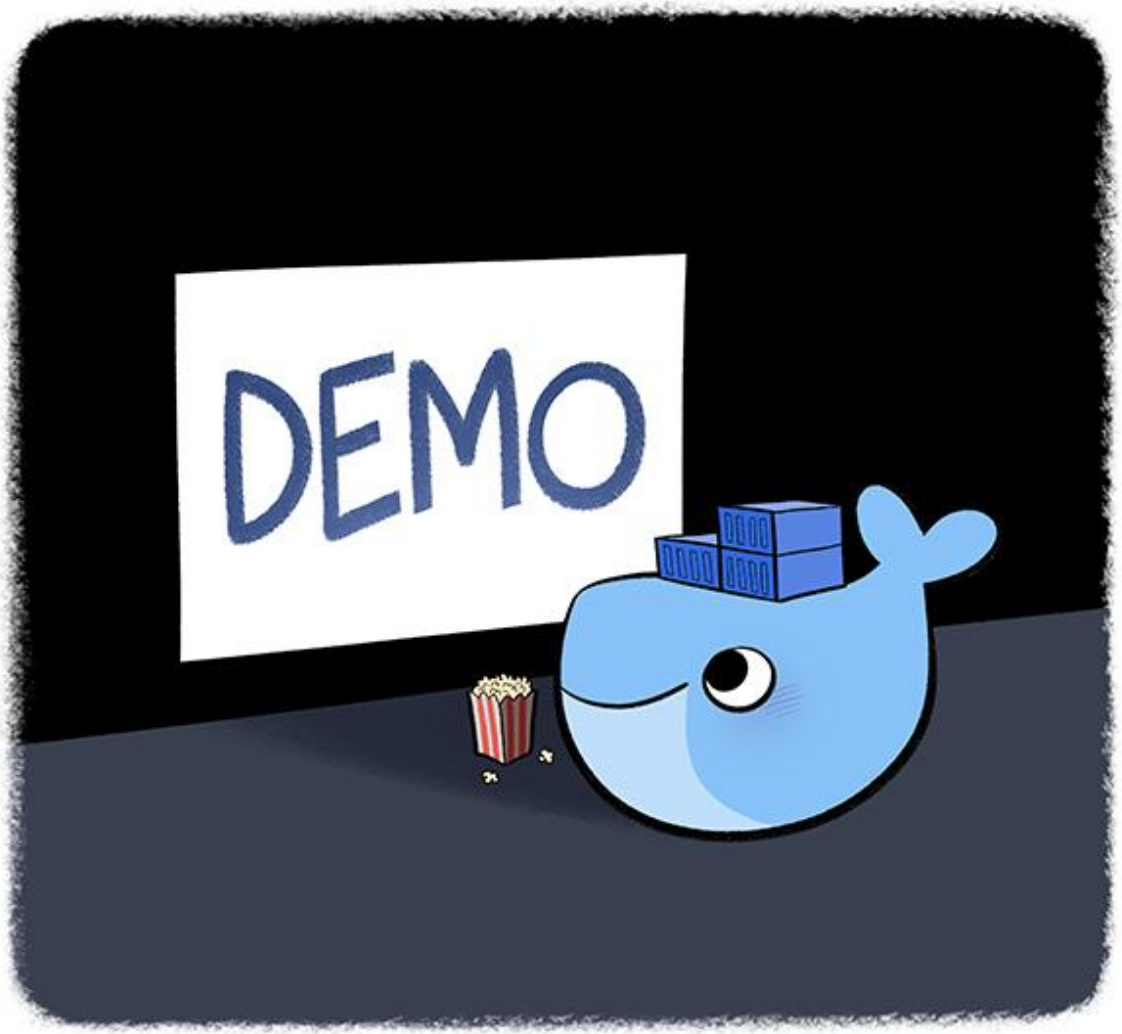
Containerize your Java application.

...OR DELETE ALL DOCKERFILE WITH JIB

```xml
<plugin>
  <groupId>com.google.cloud.tools</groupId>
  <artifactId>jib-maven-plugin</artifactId>
  <version>1.0.1</version>
  <configuration>
    <to>
      <image>myimage</image>
    </to>
  </configuration>
</plugin>
```

```
plugins {
  id 'com.google.cloud.tools.jib' version '1.0.1'
}

jib.to.image = 'gcr.io/my-gcp-project/my-app'
```

maven


DEMO

For any tech, you can create image with Kaniko... without Docker

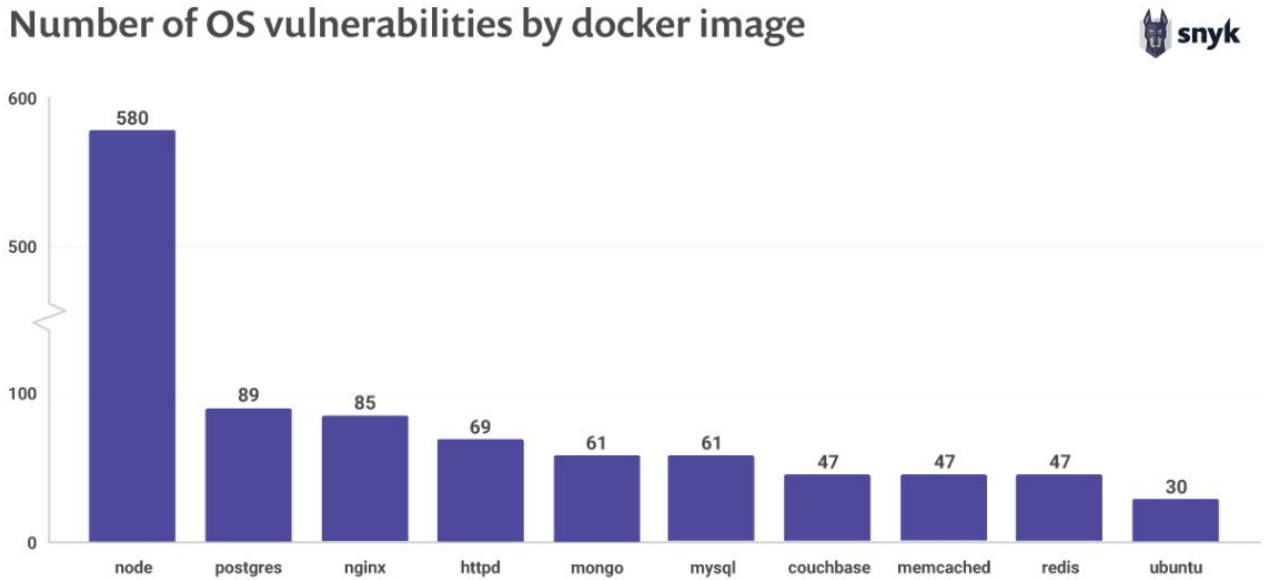
Build with Distroless

Why:

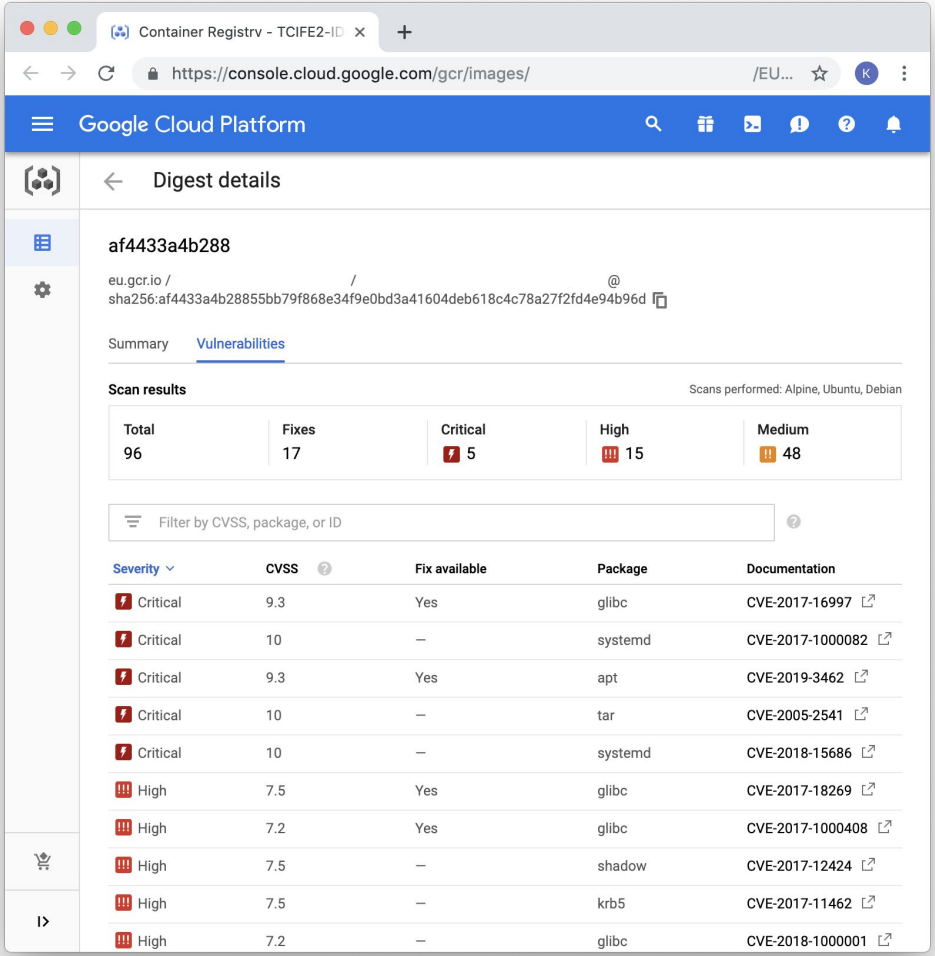
- Small images
- Avoid images vulnerabilities
- Less attack surface
- Existing images for different languages
- ...

... BECAUSE

Top ten most popular docker images each contain at least **30 vulnerabilities**



... BECAUSE


Container Registrv - TCIFE2-ID
https://console.cloud.google.com/gcr/images/
/EU...
Google Cloud Platform
Digest details
af4433a4b288
eu.gcr.io /
/
@
sha256:af4433a4b28855bb79f868e34f9e0bd3a41604deb618c4c78a27f2fd4e94b96d
Summary
Vulnerabilities
Scan results
Scans performed: Alpine, Ubuntu, Debian
Total
96
Fixes
17
Critical
5
High
15
Medium
48
Filter by CVSS, package, or ID
Severity
CVSS
Fix available
Package
Documentation
Critical 9.3 Yes glibc CVE-2017-16997
Critical 10 – systemd CVE-2017-1000082
Critical 9.3 Yes apt CVE-2019-3462
Critical 10 – tar CVE-2005-2541
Critical 10 – systemd CVE-2018-15686
High 7.5 Yes glibc CVE-2017-18269
High 7.2 Yes glibc CVE-2017-1000408
High 7.5 – shadow CVE-2017-12424
High 7.5 – krb5 CVE-2017-11462
High 7.2 – glibc CVE-2018-1000001

... BECAUSE

OPENJDK/JDK-11-SLIM

Scan results

Scans performed: Alpine, Ubuntu, Debian

Total	Fixes	Critical	High	Medium
96	17	5	15	48

DISTROLESS/JAVA:11

Scan results

Scans performed: Alpine, Ubuntu, Debian

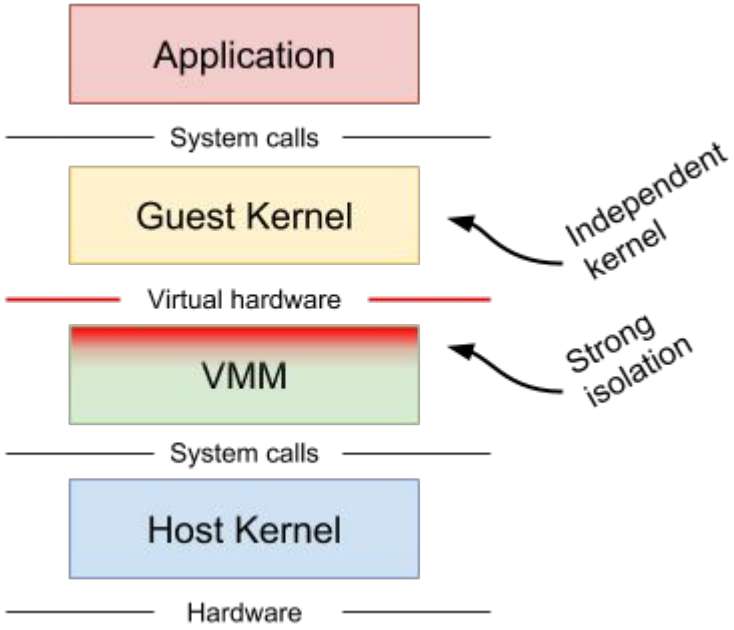
Total	Fixes	Critical	High	Medium
21	0	0	3	13

PROCESSES IN CONTAINERS SHOULD NOT RUN AS ROOT!

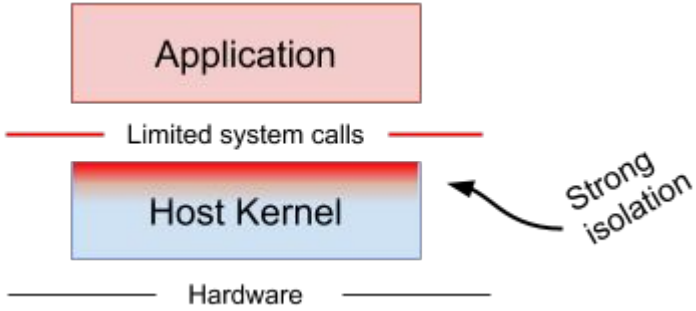

```
FROM <base image>
RUN groupadd -g 999 appuser && \
    useradd -r -u 999 -g appuser appuser
USER appuser
... <rest of Dockerfile> ...
```

USE GVISOR?

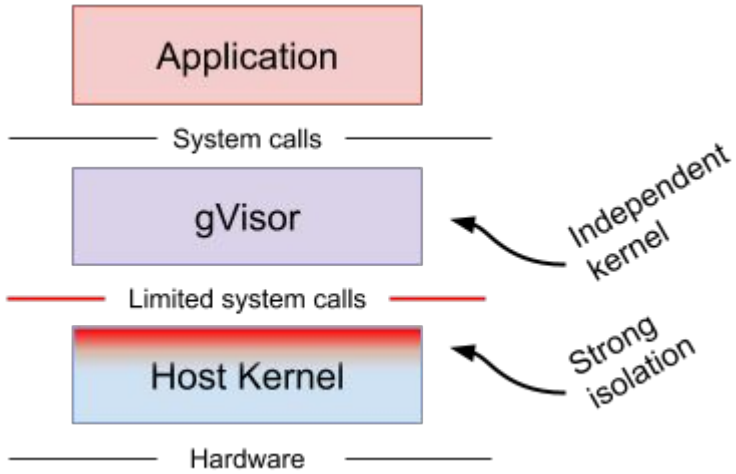
WITH VIRTUALISATION



WITH CONTAINER



WITH gVISOR


Application
System calls
gVisor
Independent kernel
Limited system calls
Host Kernel
Strong isolation
Hardware

About gVisor

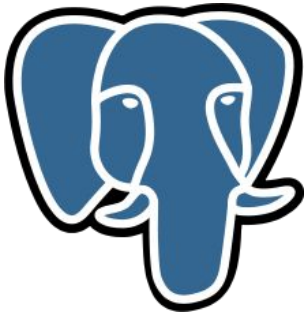
Ludovic Champenois
@ludoch

gVisor github.com/google/gvisor is the security sandbox used in App Engine Java8 (and also the deprecated Java7 as well)... It is the reason why it took a few years to offer Java 8, as the entire stack got replaced, while in flight. Now, is this a toy? Hell no... Battle tested.

Configure docker to use gVisor

Docker usages

Simplify your day to day job...

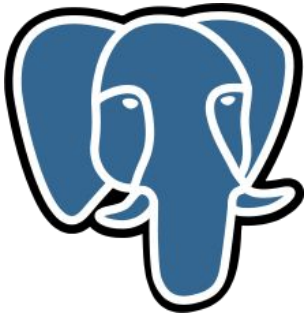


```
$ docker run -it --rm -p 5432:5432 \
  -e POSTGRES_PASSWORD=test-password \
  -e POSTGRES_USER=proxyuser \
  -e POSTGRES_DB=postgres \
  postgres:9.6.10-alpine
```

```
$ docker run --rm -it \
  -p 9000:9000 \
  minio/minio server /data
```

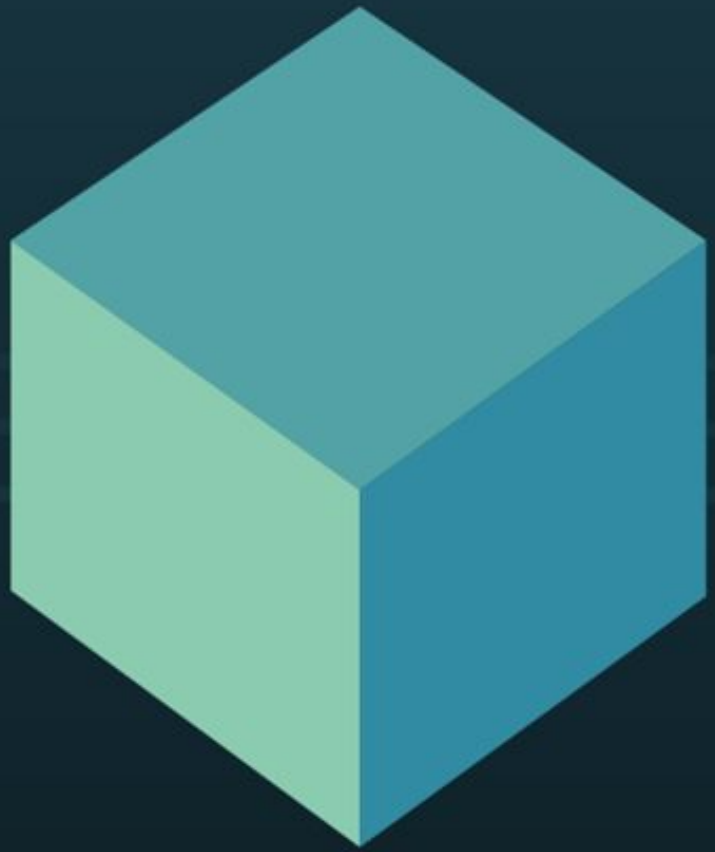
```
$ docker run --rm -it -p 9000:9000 my_wonderful_app/ui
```

-IT --RM?

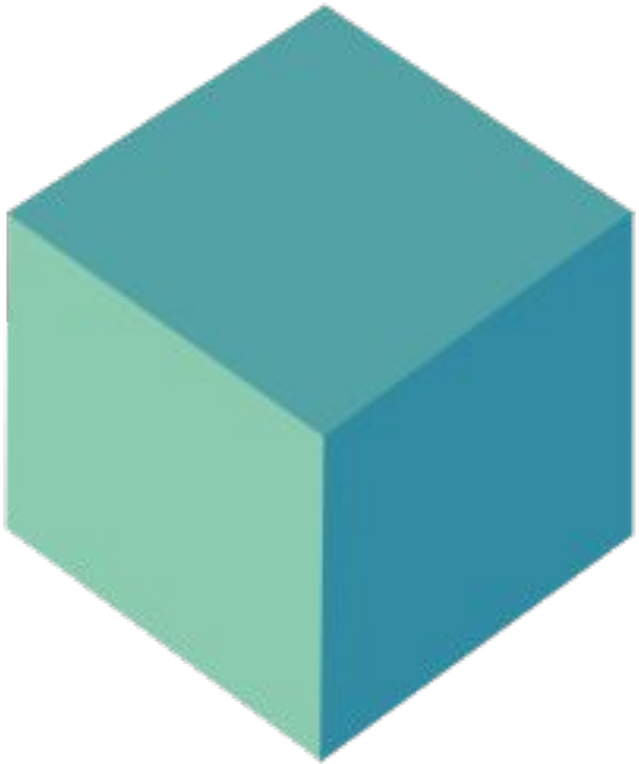


```
$ docker run -it --rm -p 5432:5432 \
  -e POSTGRES_PASSWORD=test-password \
  -e POSTGRES_USER=proxyuser \
  -e POSTGRES_DB=postgres \
  postgres:9.6.10-alpine
```

-i = interactive
-t = allocate a tty
--rm = Automatically remove the container when it exits



TESTCONTAINERS



Unit Test with containers

- Simple Java (& JVM compatible) system around Docker
- Multiple databases support
- Support for Docker Compose
- Other container of your choice (with configuration)

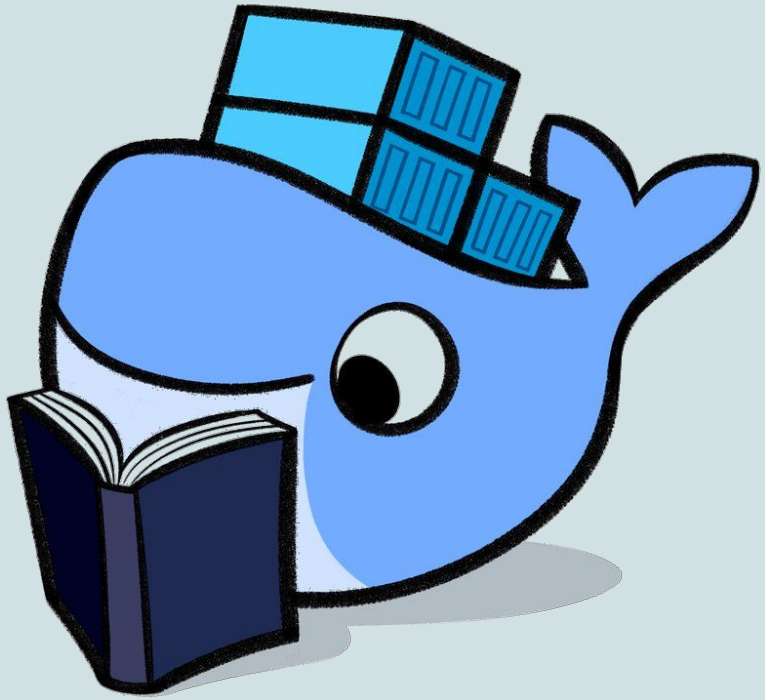
```java
@Testcontainers
class MyTestcontainersTests {

   @Container
   private PostgreSQLContainer postgresqlContainer = new PostgreSQLContainer()
           .withDatabaseName("foo")
           .withUsername("foo")
           .withPassword("secret");

   @Test
   void test() {
       assertThat(postgresqlContainer.isRunning()).isTrue();
   }

}
```

Use CI based on Container!

```
image: ruby:2.2

services:
  - postgres:9.3

before_script:
  - bundle install

test:
  script:
  - bundle exec rake spec
```

```
before_script:
  - bundle install

test:2.1:
  image: ruby:2.1
  services:
  - postgres:9.3
  script:
  - bundle exec rake spec

test:2.2:
  image: ruby:2.2
  services:
  - postgres:9.4
  script:
  - bundle exec rake spec
```

```
image: ruby:2.2

services:
  - my-custom-repository.com/postgres:9.3

before_script:
  - bundle install

test:
  script:
  - bundle exec rake spec
```



Docker best practices

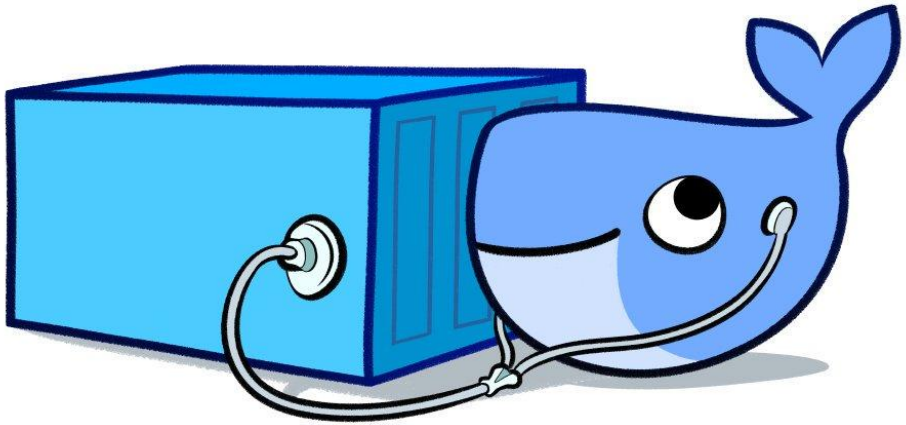
Don't hardcode Passwords

Provide creds as environment variables at runtime

Dockerfile:

```
FROM busybox
ARG user
RUN echo "user is $user"
build image command
```

```
$ docker build --build-arg user=moby -t
test_arguments -f path/to/dockerfile .
```



Inspect docker images

Dive

Usage:

```
$ dive gcr.io/distroless/java
```

Or

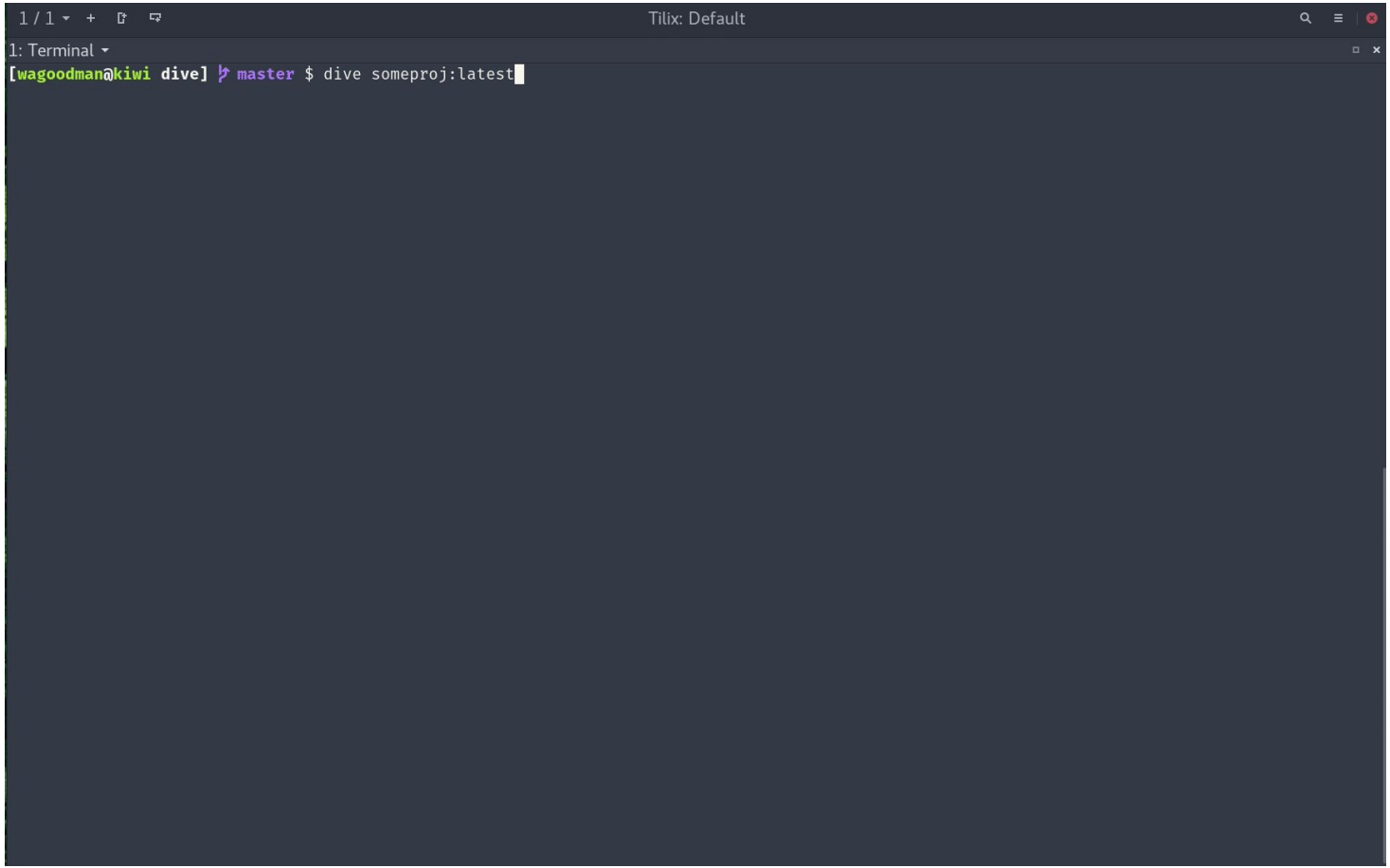
```
$ dive build -t my-image .
```

In CI/CD chain:

```
CI=true dive my-image
```

https://github.com/wagoodman/dive

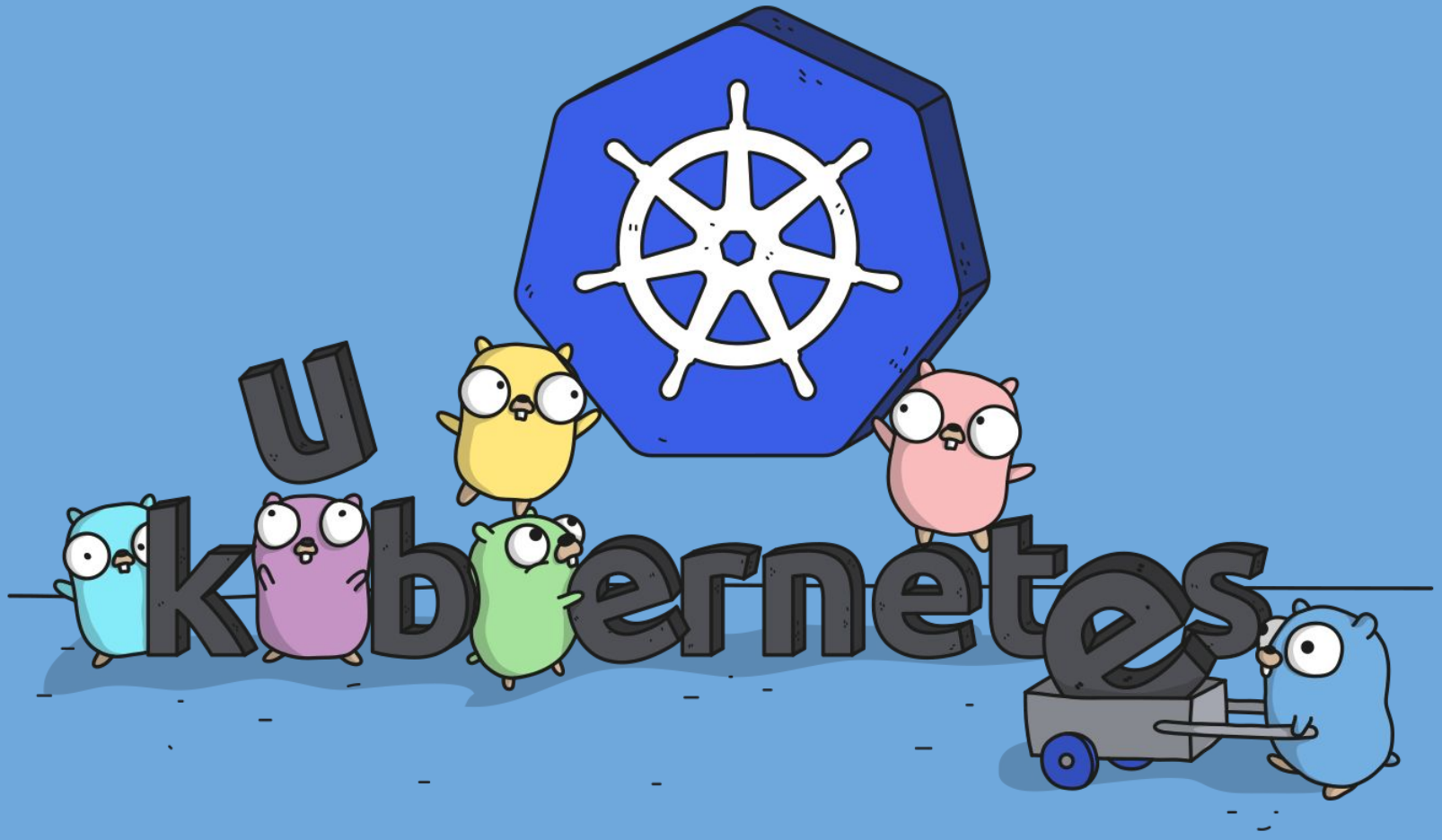
Inspect docker images



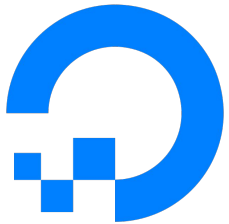
Use trusted images ☆

Why use official images on Docker Hub?

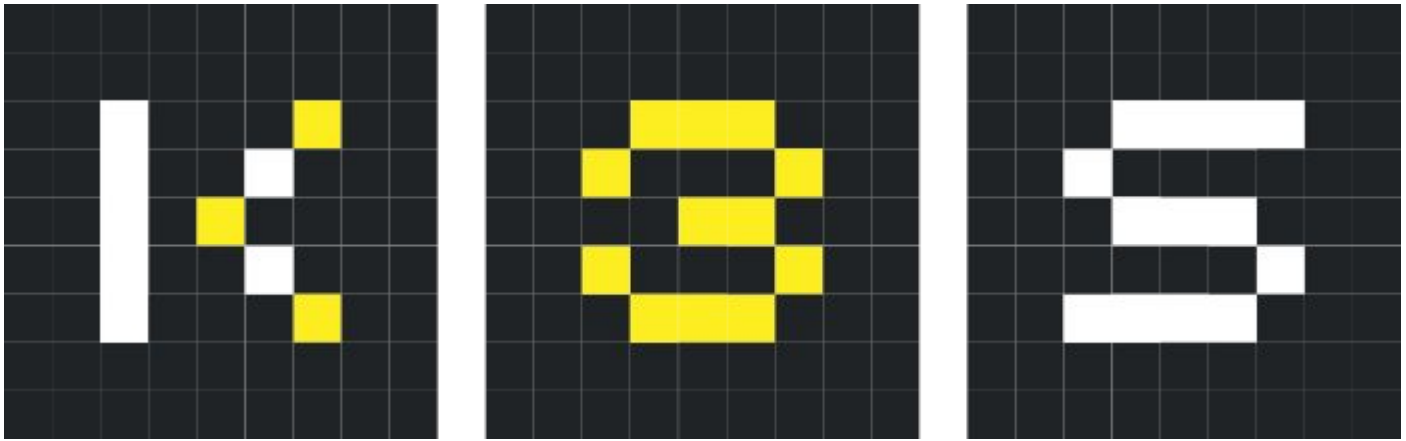
- Vulnerability scanning
- For new Docker users


u
kubernetes

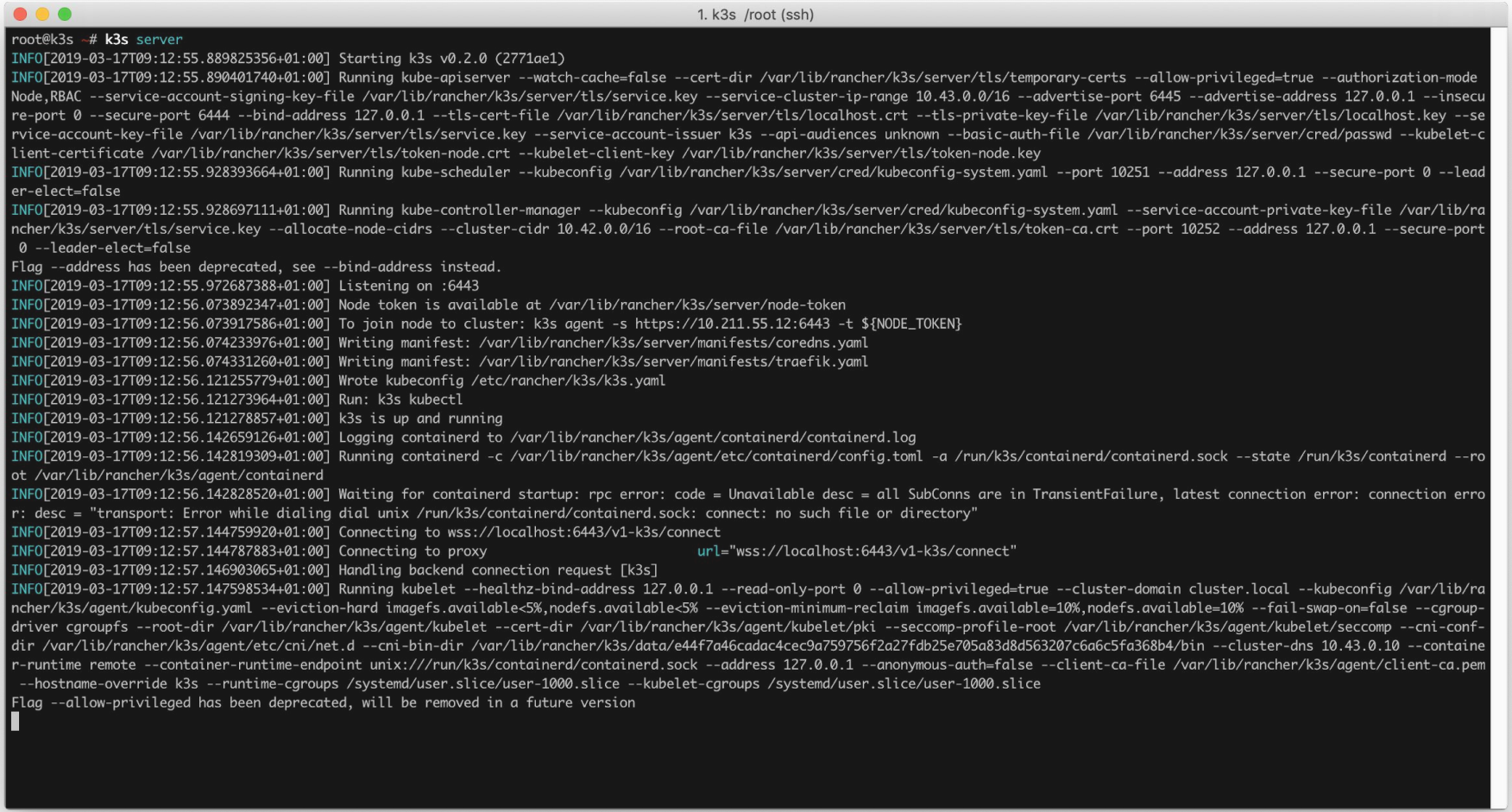
USE A MANAGED SERVICE



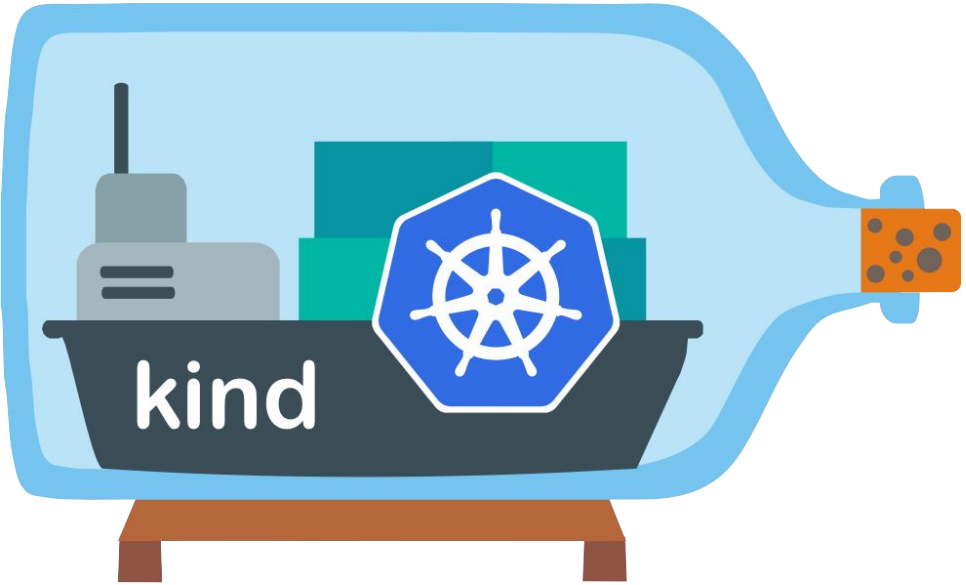
You can use K3S for specific use-case



- CI
- IoT
- ARM
- DEV


1. k3s /root (ssh)
root@k3s ~# k3s server
INFO[2019-03-17T09:12:55.889825356+01:00] Starting k3s v0.2.0 (2771ae1)
INFO[2019-03-17T09:12:55.890401740+01:00] Running kube-apiserver --watch-cache=false --cert-dir /var/lib/rancher/k3s/server/tls/temporary-certs --allow-privileged=true --authorization-mode Node,RBAC --service-account-signing-key-file /var/lib/rancher/k3s/server/tls/service.key --service-cluster-ip-range 10.43.0.0/16 --advertise-port 6445 --advertise-address 127.0.0.1 --insecure-port 0 --secure-port 6444 --bind-address 127.0.0.1 --tls-cert-file /var/lib/rancher/k3s/server/tls/localhost.crt --tls-private-key-file /var/lib/rancher/k3s/server/tls/localhost.key --service-account-key-file /var/lib/rancher/k3s/server/tls/service.key --service-account-issuer k3s --api-audiences unknown --basic-auth-file /var/lib/rancher/k3s/server/cred/passwd --kubelet-client-certificate /var/lib/rancher/k3s/server/tls/token-node.crt --kubelet-client-key /var/lib/rancher/k3s/server/tls/token-node.key
INFO[2019-03-17T09:12:55.928393664+01:00] Running kube-scheduler --kubeconfig /var/lib/rancher/k3s/server/cred/kubeconfig-system.yaml --port 10251 --address 127.0.0.1 --secure-port 0 --leader-elect=false
INFO[2019-03-17T09:12:55.928697111+01:00] Running kube-controller-manager --kubeconfig /var/lib/rancher/k3s/server/cred/kubeconfig-system.yaml --service-account-private-key-file /var/lib/rancher/k3s/server/tls/service.key --allocate-node-cidrs --cluster-cidr 10.42.0.0/16 --root-ca-file /var/lib/rancher/k3s/server/tls/token-ca.crt --port 10252 --address 127.0.0.1 --secure-port 0 --leader-elect=false
Flag --address has been deprecated, see --bind-address instead.
INFO[2019-03-17T09:12:55.972687388+01:00] Listening on :6443
INFO[2019-03-17T09:12:56.073892347+01:00] Node token is available at /var/lib/rancher/k3s/server/node-token
INFO[2019-03-17T09:12:56.073917586+01:00] To join node to cluster: k3s agent -s https://10.211.55.12:6443 -t ${NODE_TOKEN}
INFO[2019-03-17T09:12:56.074233976+01:00] Writing manifest: /var/lib/rancher/k3s/server/manifests/coredns.yaml
INFO[2019-03-17T09:12:56.074331260+01:00] Writing manifest: /var/lib/rancher/k3s/server/manifests/traefik.yaml
INFO[2019-03-17T09:12:56.121255779+01:00] Wrote kubeconfig /etc/rancher/k3s/k3s.yaml
INFO[2019-03-17T09:12:56.121273964+01:00] Run: k3s kubectl
INFO[2019-03-17T09:12:56.121278857+01:00] k3s is up and running
INFO[2019-03-17T09:12:56.142659126+01:00] Logging containerd to /var/lib/rancher/k3s/agent/containerd/containerd.log
INFO[2019-03-17T09:12:56.142819309+01:00] Running containerd -c /var/lib/rancher/k3s/agent/etc/containerd/config.toml -a /run/k3s/containerd/containerd.sock --state /run/k3s/containerd --root /var/lib/rancher/k3s/agent/containerd
INFO[2019-03-17T09:12:56.142828520+01:00] Waiting for containerd startup: rpc error: code = Unavailable desc = all SubConns are in TransientFailure, latest connection error: connection error: desc = "transport: Error while dialing dial unix /run/k3s/containerd/containerd.sock: connect: no such file or directory"
INFO[2019-03-17T09:12:57.144759920+01:00] Connecting to wss://localhost:6443/v1-k3s/connect
INFO[2019-03-17T09:12:57.144787883+01:00] Connecting to proxy url="wss://localhost:6443/v1-k3s/connect"
INFO[2019-03-17T09:12:57.146903065+01:00] Handling backend connection request [k3s]
INFO[2019-03-17T09:12:57.147598534+01:00] Running kubelet --healthz-bind-address 127.0.0.1 --read-only-port 0 --allow-privileged=true --cluster-domain cluster.local --kubeconfig /var/lib/rancher/k3s/agent/kubeconfig.yaml --eviction-hard imagefs.available<5%,nodefs.available<5% --eviction-minimum-reclaim imagefs.available=10%,nodefs.available=10% --fail-swap-on=false --cgroup-driver cgroupfs --root-dir /var/lib/rancher/k3s/agent/kubelet --cert-dir /var/lib/rancher/k3s/agent/kubelet/pki --seccomp-profile-root /var/lib/rancher/k3s/agent/kubelet/seccomp --cni-conf-dir /var/lib/rancher/k3s/agent/etc/cni/net.d --cni-bin-dir /var/lib/rancher/k3s/data/e44f7a46cadac4cec9a759756f2a27fdb25e705a83d8d563207c6a6c5fa368b4/bin --cluster-dns 10.43.0.10 --container-runtime remote --container-runtime-endpoint unix:///run/k3s/containerd/containerd.sock --address 127.0.0.1 --anonymous-auth=false --client-ca-file /var/lib/rancher/k3s/agent/client-ca.pem --hostname-override k3s --runtime-cgroups /systemd/user.slice/user-1000.slice --kubelet-cgroups /systemd/user.slice/user-1000.slice
Flag --allow-privileged has been deprecated, will be removed in a future version

https://k3s.io



Or Kind

Aka “Kubernetes IN Docker"

A tool for running local Kubernetes clusters

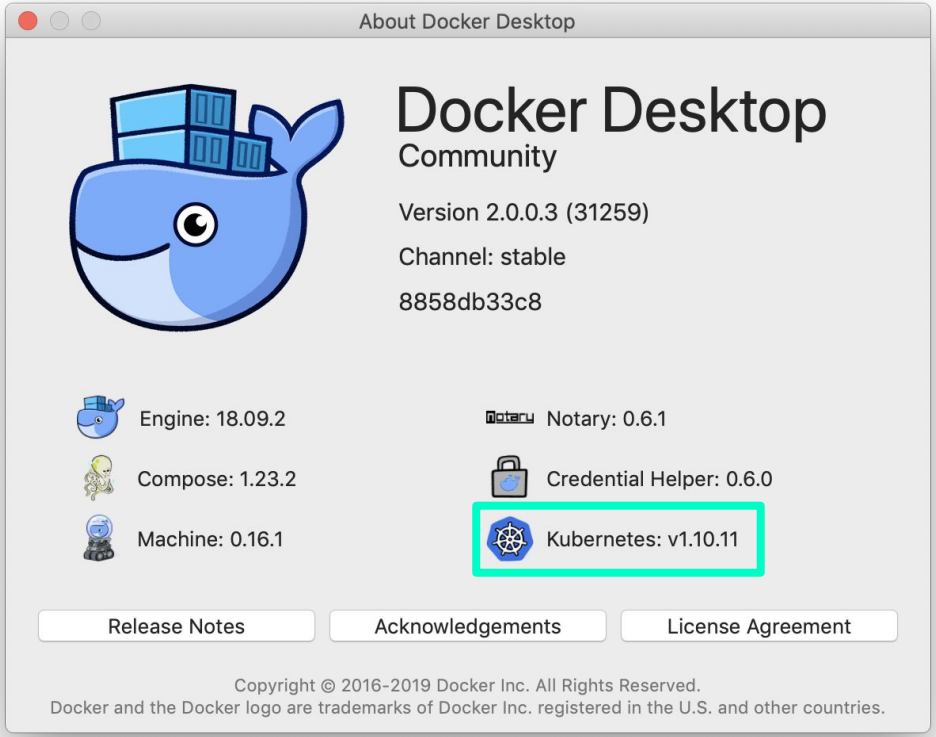
Usage:

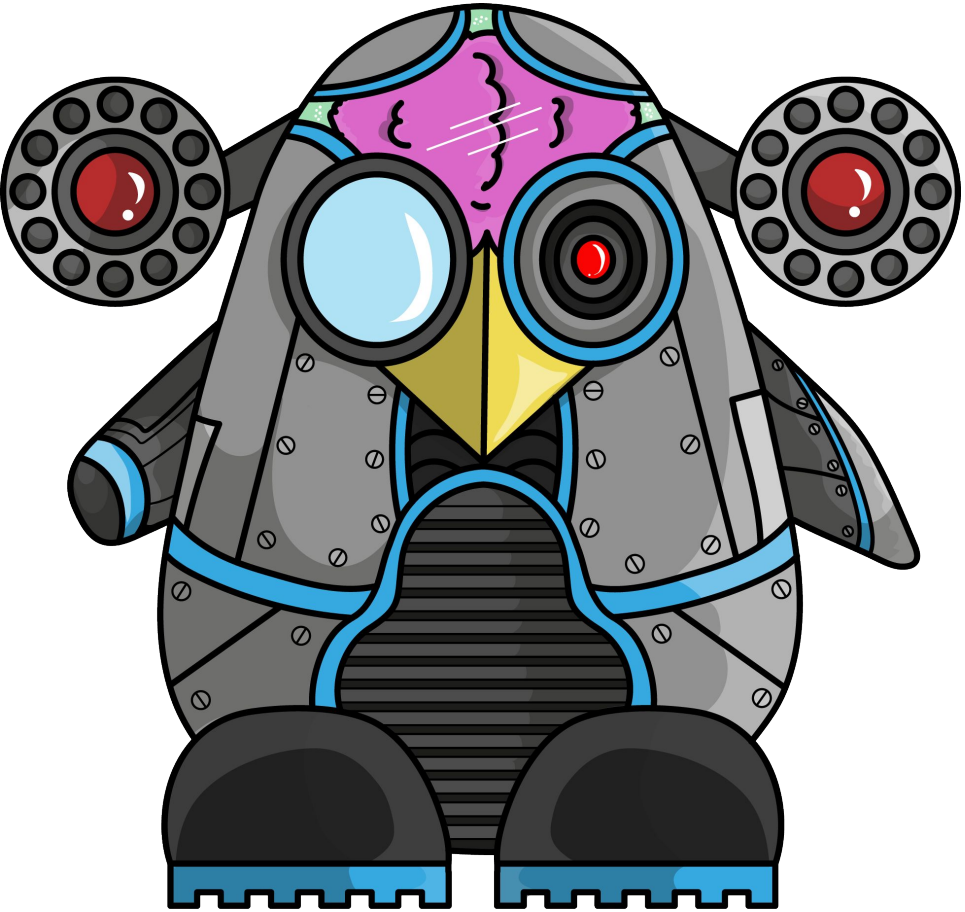
```
$ go get -u sigs.k8s.io/kind
&& kind create cluster
```

That’s it!!

https://github.com/kubernetes-sigs/kind/

AND FOR DEV, YOU CAN USE DOCKER...





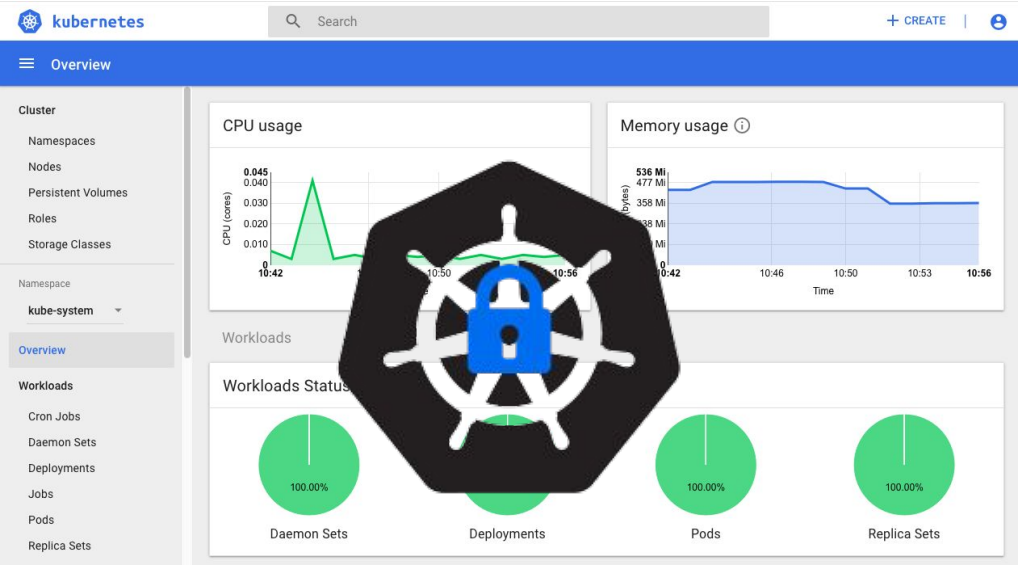
Upgrade to latest version your cluster

Why?

Not only new features but **security**!

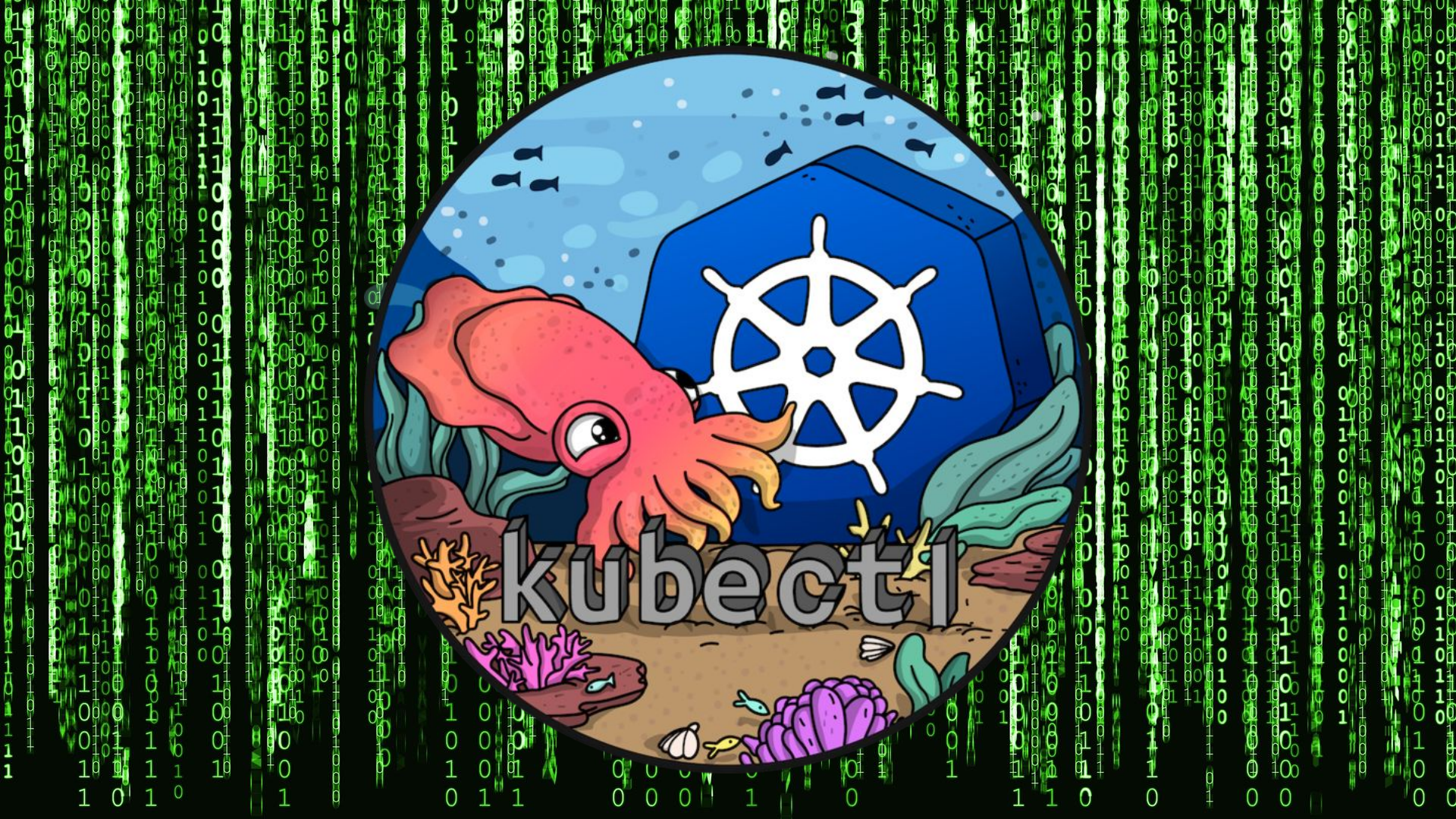
Remember: CVE-2018-1002105, CVE-2019-5736, CVE-2019-1002100 ...

Secure your dashboard!



Don’t ignore the basics:

Don’t expose k8s dashboard to internet without authentication and with elevated privileges!


kubectl

Alias all the thing!

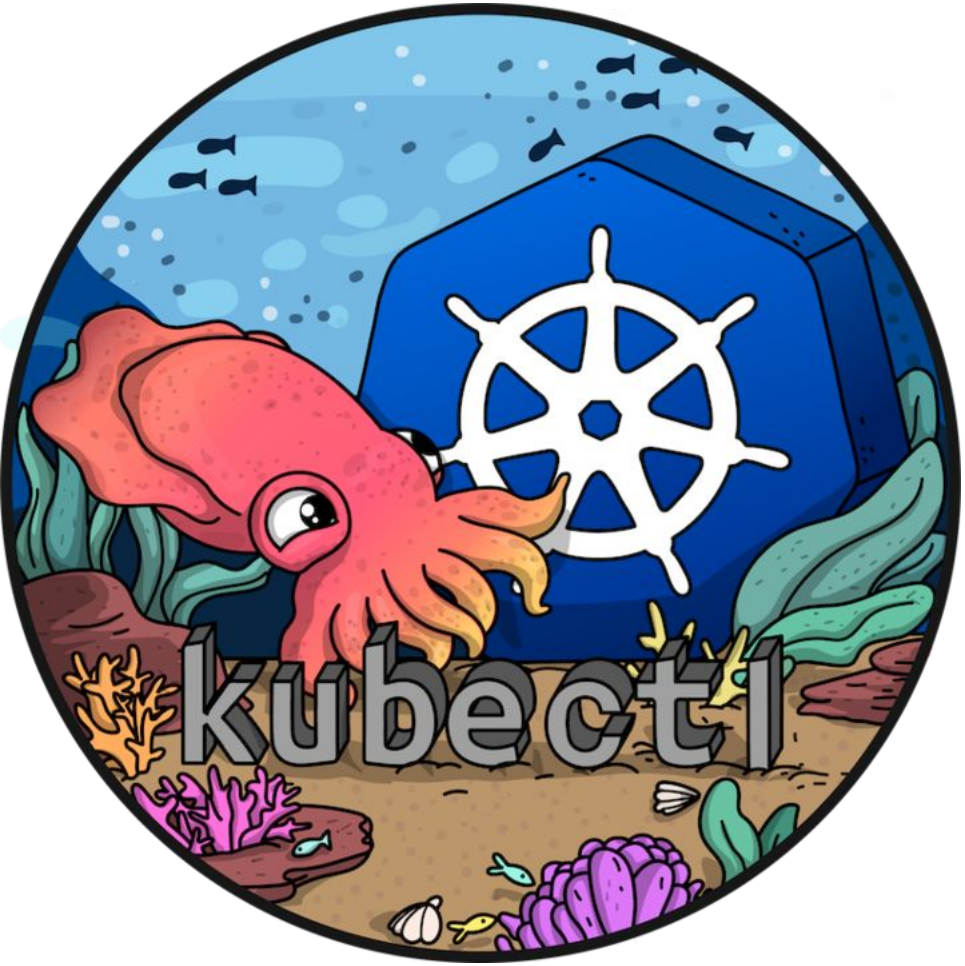
```
$ alias k='kubectl'
$ alias kub='kubectl'
```

And use autocompletion!

```
$ kubectl completion bash > /etc/bash_completion.d/kubectl
```

Compatible with **Bash**, **Zsh** and **Fish**

https://kubernetes.io/docs/tasks/tools/install-kubectl/#enabling-shell-autocompletion



Upgrade to latest Version your Kubectl

Use a latest version of kubectl, same version as your cluster (if not, potential problems…)

```
$ kubectl version
Client Version: version.Info{Major:"1",
Minor:"12", GitVersion:"v1.12.1",...}
Server Version: version.Info{Major:"1",
Minor:"12", GitVersion:"v1.12.6",...}
```

use multiple Kubeconfigs at once

Kubeconfig files are structured YAML files so, you can't just append them to get one big kubeconfig file.

The trick:

```
KUBECONFIG=file1:file2:file3
```

KUBECTX

https://github.com/ahmetb/kubectx

KUBENS

https://github.com/ahmetb/kubectx

Kube-ps1

Allow to add Kubernetes context & namespace in prompt

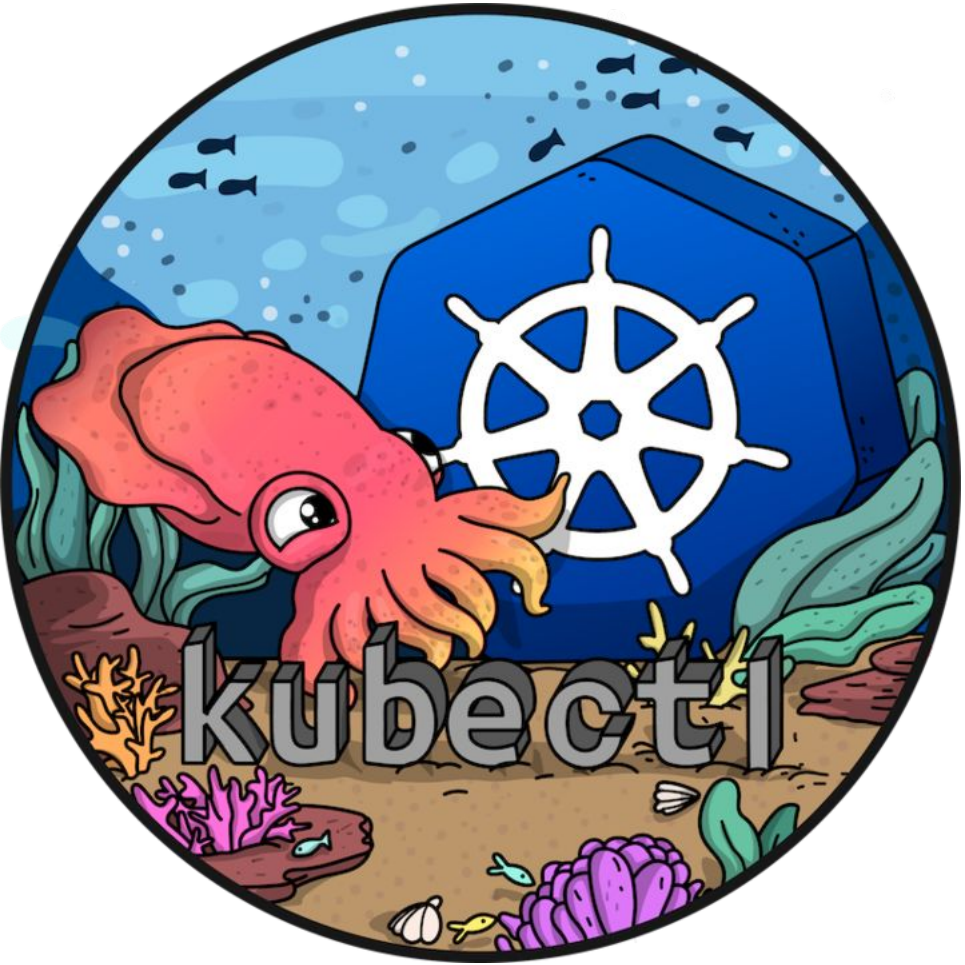
https://github.com/jonmosco/kube-ps1

Wait deployment to complete

```
$ kubectl wait --for=condition=complete job/${JOB_NAME} --timeout=120s
```

KUBESPY

https://github.com/pulumi/kubespy



Watch pods running

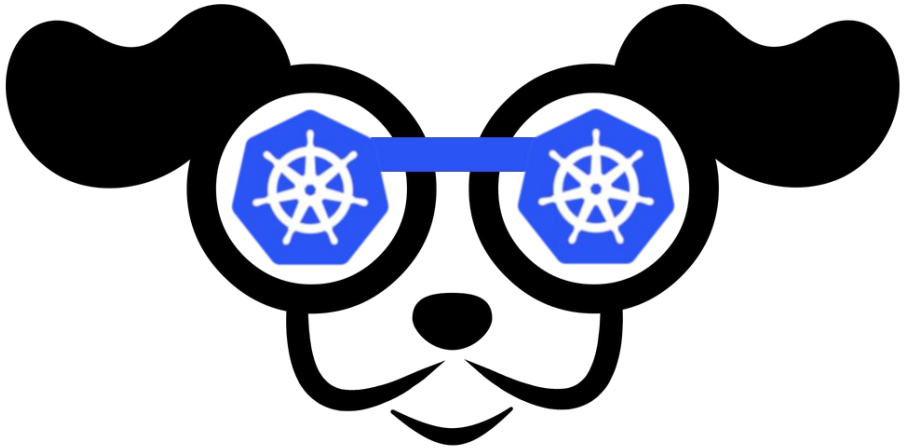
Usage:

```
$ kubectl get pod --watch
```

Or

```
$ watch kubectl get pod
```

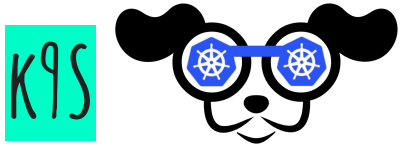
K9S



Provides a curses based terminal UI to interact with your Kubernetes clusters.

Easier to navigate, observe and manage your applications.

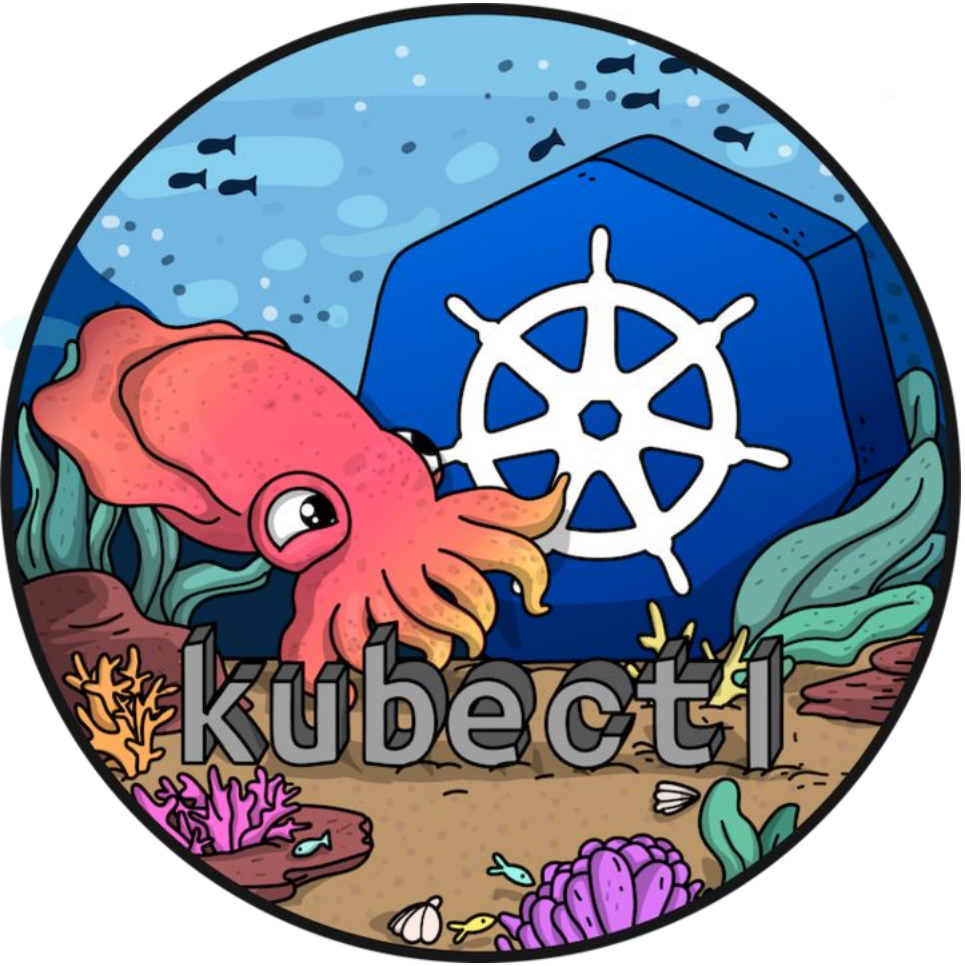
https://k9ss.io




```
Context:      minikube                <?>      Help          <0> all
Cluster:      minikube                <ctrl-d> Delete        <1> kube-system
User:         minikube                <d>      Describe      <2> default
K9s Version:  0.1.6                   <e>      Edit
K8s Version:  v1.13.2                 <l>      Logs
CPU:          10%(-)                  <s>      Shell
MEM:          20%(+)                  <v>      View
```

Pods(all)[12]

NAMESPACE	NAME	READY	STATUS	RESTARTS	CPU	MEM	IP	NODE	QOS	AGE
default	nginx-6988c9989f-wwz6d	1/1	Running	0			172.17.0.6	192.168.64.83	Guaranteed	87s
kube-system	coredns-86c58d9df4-dkhf2	1/1	Running	0	3m	8Mi	172.17.0.3	192.168.64.83	Burstable	17h
kube-system	coredns-86c58d9df4-jt79s	1/1	Running	0	2m(-)	8Mi	172.17.0.2	192.168.64.83	Burstable	17h
kube-system	etcd-minikube	1/1	Running	0	24m(-)	53Mi	192.168.64.83	192.168.64.83	BestEffort	17h
kube-system	kube-addon-manager-minikube	1/1	Running	0	7m(+)	17Mi(-)	192.168.64.83	192.168.64.83	Burstable	17h
kube-system	kube-apiserver-minikube	1/1	Running	0	47m(-)	383Mi	192.168.64.83	192.168.64.83	Burstable	17h
kube-system	kube-controller-manager-minikube	1/1	Running	0	49m(-)	55Mi(+)	192.168.64.83	192.168.64.83	Burstable	17h
kube-system	kube-proxy-pjh2p	1/1	Running	0	4m(-)	10Mi	192.168.64.83	192.168.64.83	BestEffort	17h
kube-system	kube-scheduler-minikube	1/1	Running	0	15m(-)	12Mi	192.168.64.83	192.168.64.83	Burstable	17h
kube-system	kubernetes-dashboard-ccc79bfc9-qgnck	1/1	Running	0	0m	11Mi	172.17.0.4	192.168.64.83	BestEffort	17h
kube-system	metrics-server-6fc4b7bcff-hp6pm	1/1	Running	0	1m	14Mi	172.17.0.5	192.168.64.83	BestEffort	17h
kube-system	storage-provisioner	1/1	Running	0	0m	13Mi	192.168.64.83	192.168.64.83	BestEffort	17h



Delete all non-running pods

In case you don't want to wait pods kill/start one by one.

```
$ kubectl delete po
--field-selector=status.phase!='Running'
```

Write your own kubectl subcommand

Why?

Allow to extend kubectl with new functionality.

How?

Just add executable file name started with kubectl- in your $PATH

Krew

Package manager for kubectl plugin (brew but for kubectl). Extends kubectl with new commands.

Usage:

```
$ kubectl krew search
$ kubectl krew install clean
$ kubectl toto # <3
```

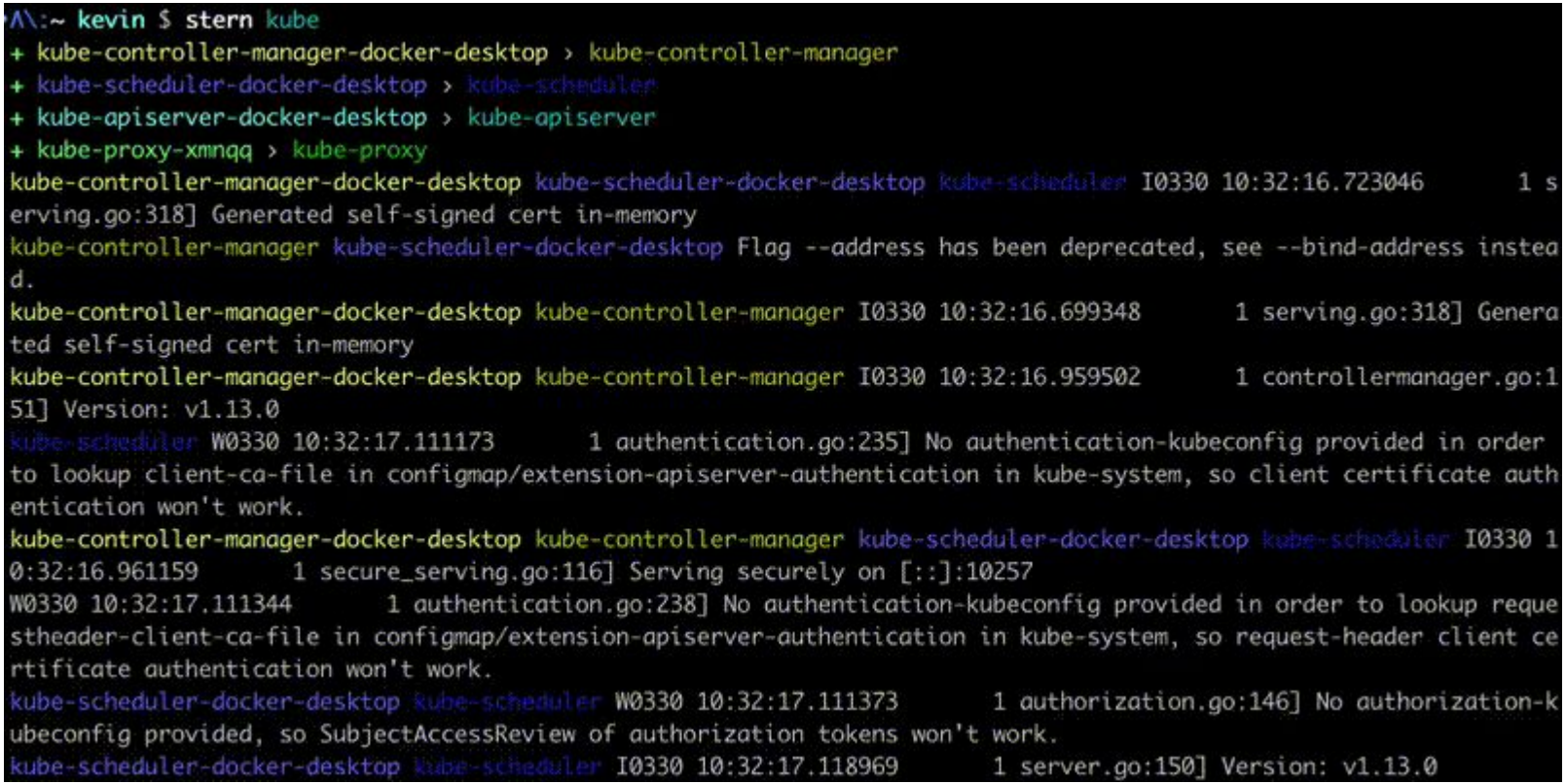
https://github.com/kubernetes-sigs/krew


LOGS, LOGS, LOGS

Watch logs of container

```
$ kubectl logs POD_NAME
```

Stern

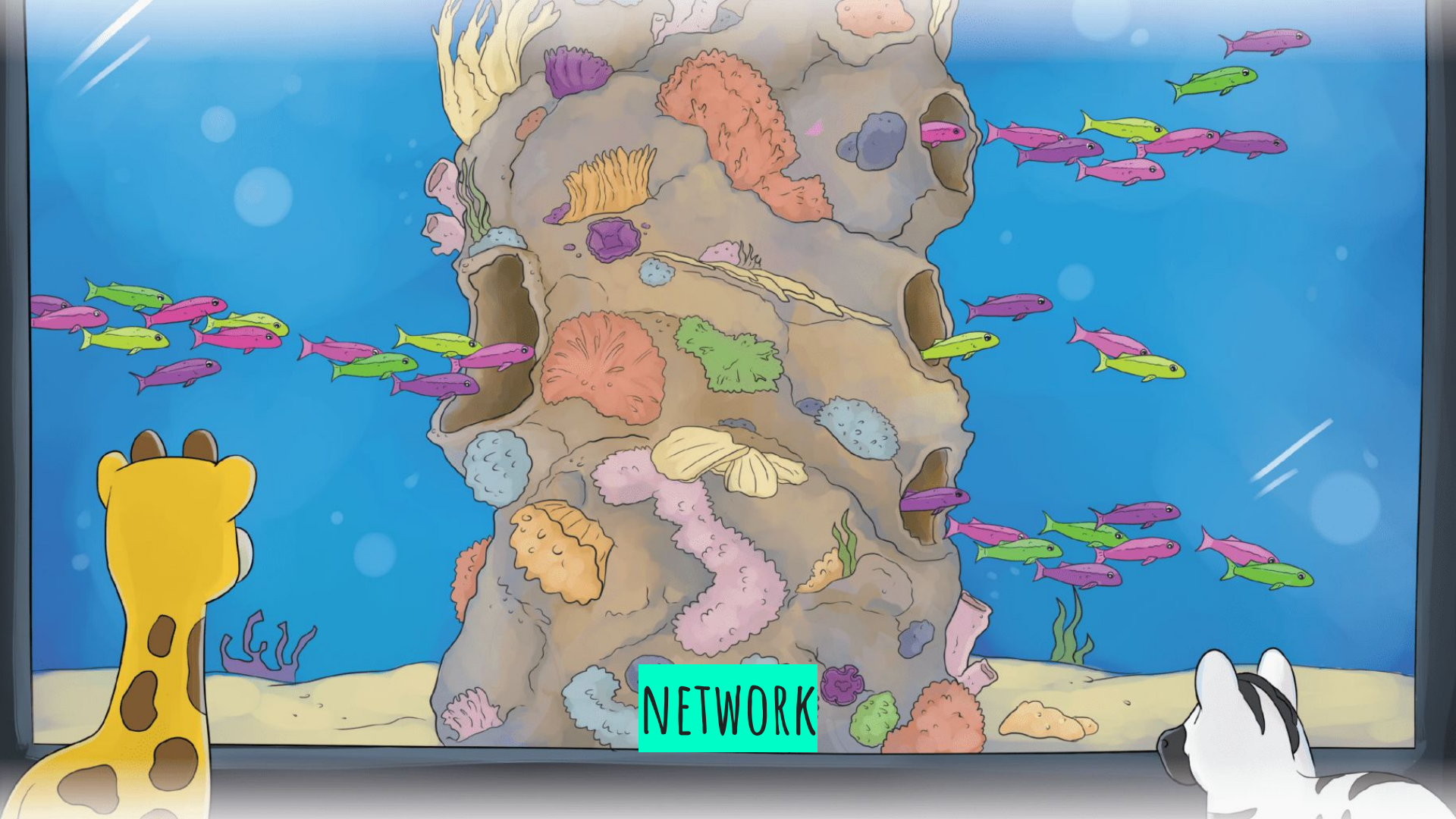


https://github.com/wercker/stern

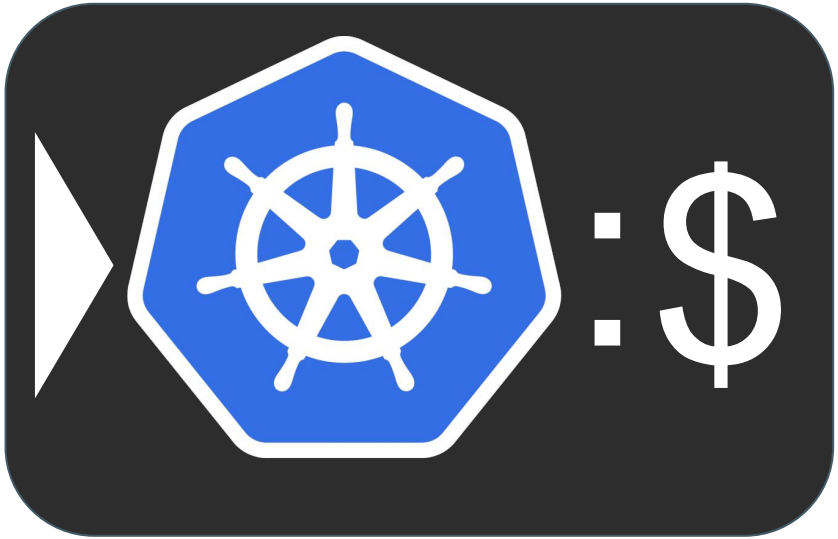
Watch logs of a previous terminated container

Thanks to -p option:

```
$ kubectl logs POD_NAME -p
```

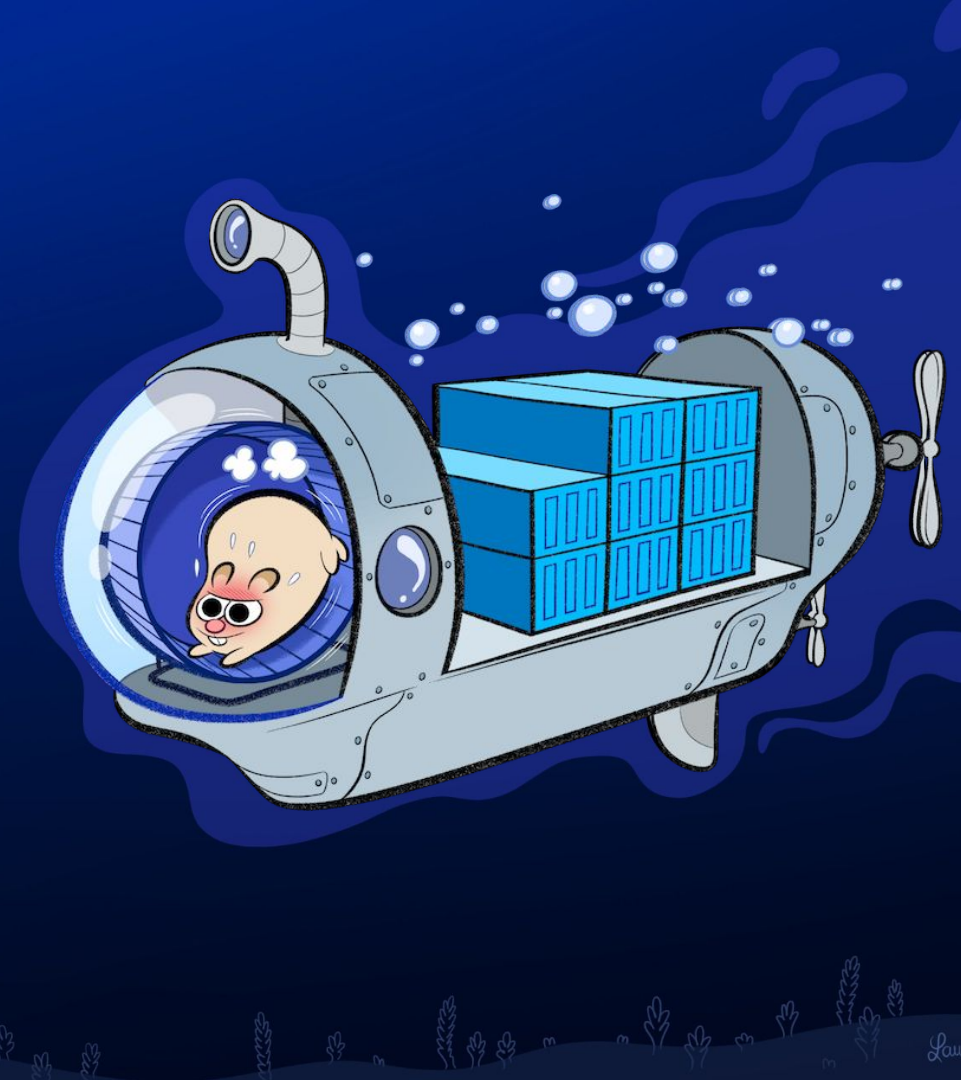

NETWORK

Run a shell in a new pod



Useful in order to examine the kubernetes environment from the inside

```
$ kubectl run -it shell --image
my-image/with-tools --restart
Never --rm -- sh
```



KUBECTL PORT-FORWARD

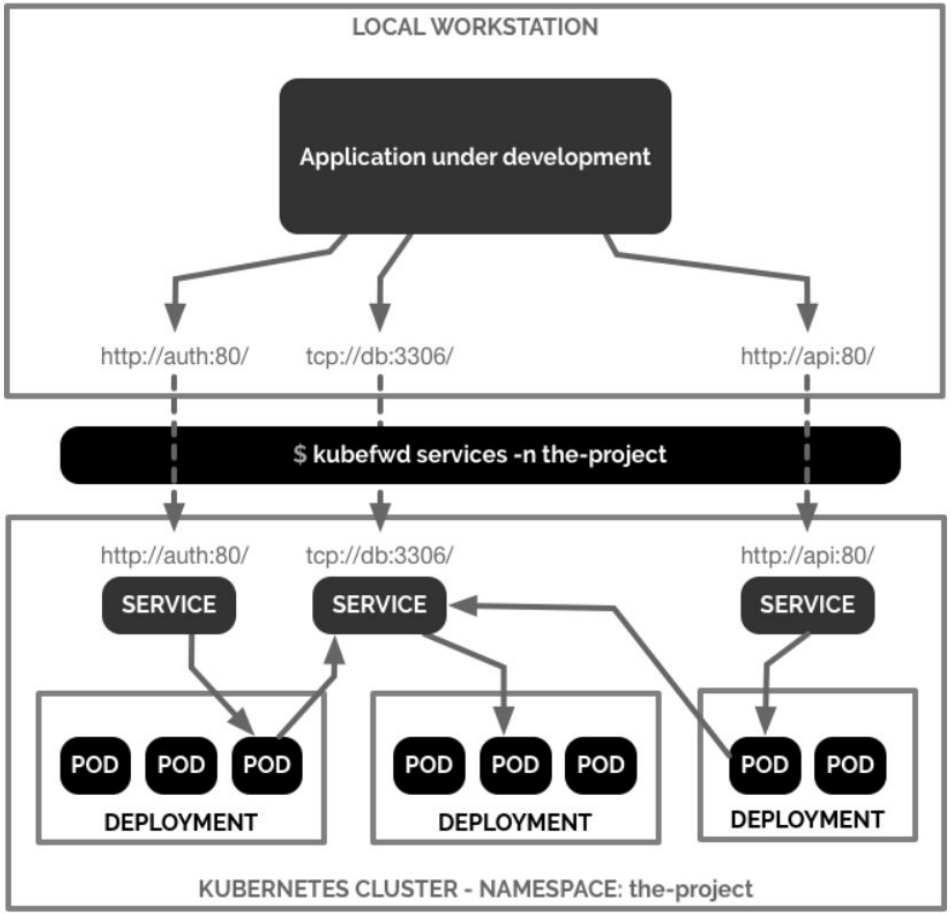
- Allow to connect to a single Service|Pods into your cluster

Usage:

```
$ kubectl port-forward svc/SERVICE_NAME 3000:3000
```

Or

```
$ kubectl port-forward POD_NAME 8080:8080
```



KUBEFWD

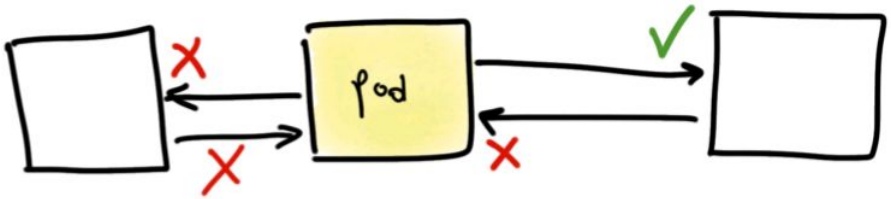
Kubernetes bulk port-forwarding.
Allow to exposes **all** services locally

```
$ sudo kubefwd services -n ns
```

Local access to a Service named `ok` listening on port 80 in `the-project` Namespace on a remote Kubernetes cluster:

```
$ curl http://ok:80
```

https://github.com/txn2/kubefwd



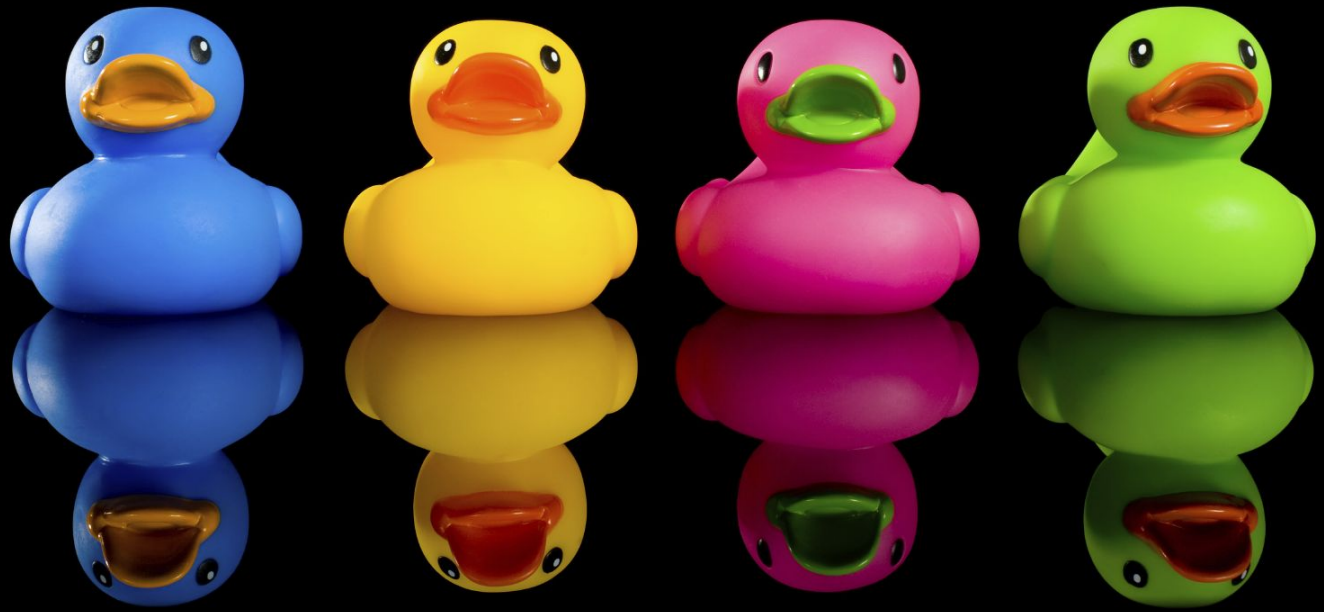
Network Policies

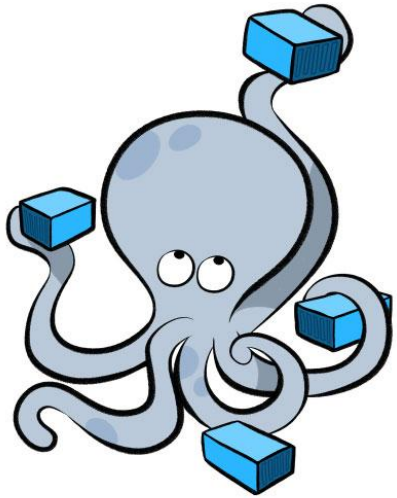
Control communication between pods in Kubernetes cluster.

Gotchas:

- Traffic is allowed by default
- Network policies are scoped by namespaces
- Stable since v1.7 (June 2017)
- Limited to IP (no domain name)

Customization /templating





Kompose

Tool to move from docker compose to kubernetes

Usage:

```
$ kompose convert
```

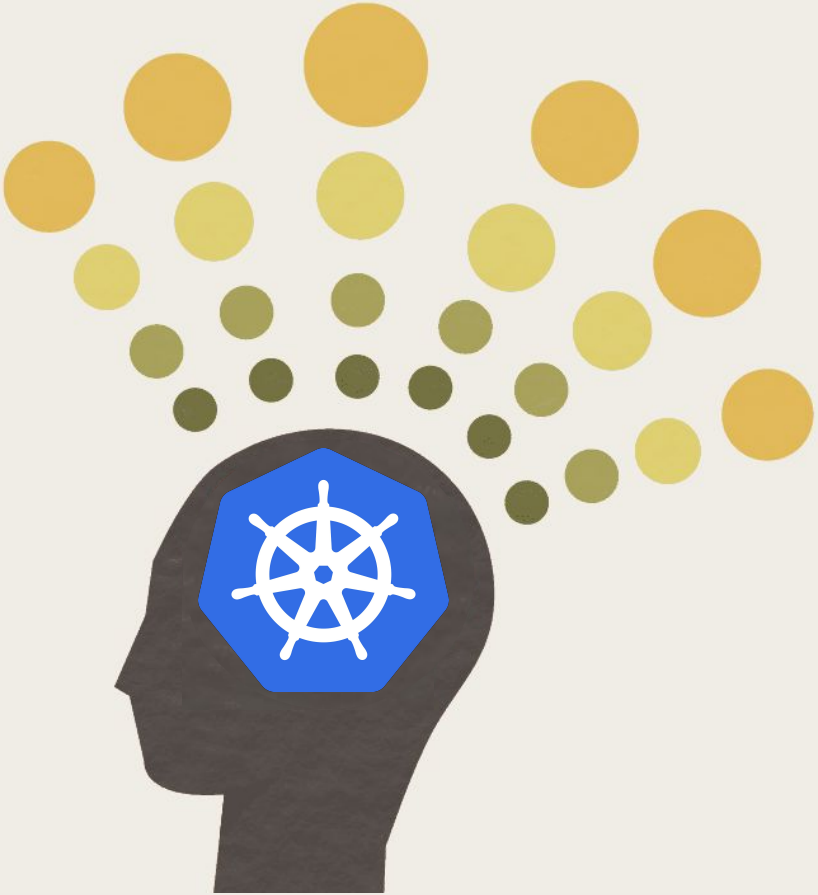
Or directly:

```
$ kompose up
```

https://github.com/kubernetes/kompose


HELM


ellen




KUSTOMIZE
kubectl

Base - deployment.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: kustomize-app
spec:
 replicas: 1
 selector:
   matchLabels:
     serving: "true"
 template:
   metadata:
     labels:
       serving: "true"
   spec:
     containers:
       - name: app
         image: gcr.io/foo/kustomize:latest
         imagePullPolicy: IfNotPresent
         ports:
           - containerPort: 8080
             name: http
             protocol: TCP
```

mixin foo-bar

mixin secrets

mixin env

mixin replica

Base

mixin env - custom-env.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: kustomize-app
spec:
 template:
   spec:
     containers:
       - name: app
         env:
           - name: MESSAGE_BODY
             value: by Kustomize ❤️
           - name: MESSAGE_FROM
             value: overlay 'custom-env'
```

mixin replica - replica.yaml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: kustomize-app
spec:
 replicas: 10
```

kustomization.yaml

```yaml
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization

bases:
  - ../../base

patchesStrategicMerge:
  - custom-env.yaml
  - replica.yaml
  - secret.yaml
  - foo-bar.yaml
```

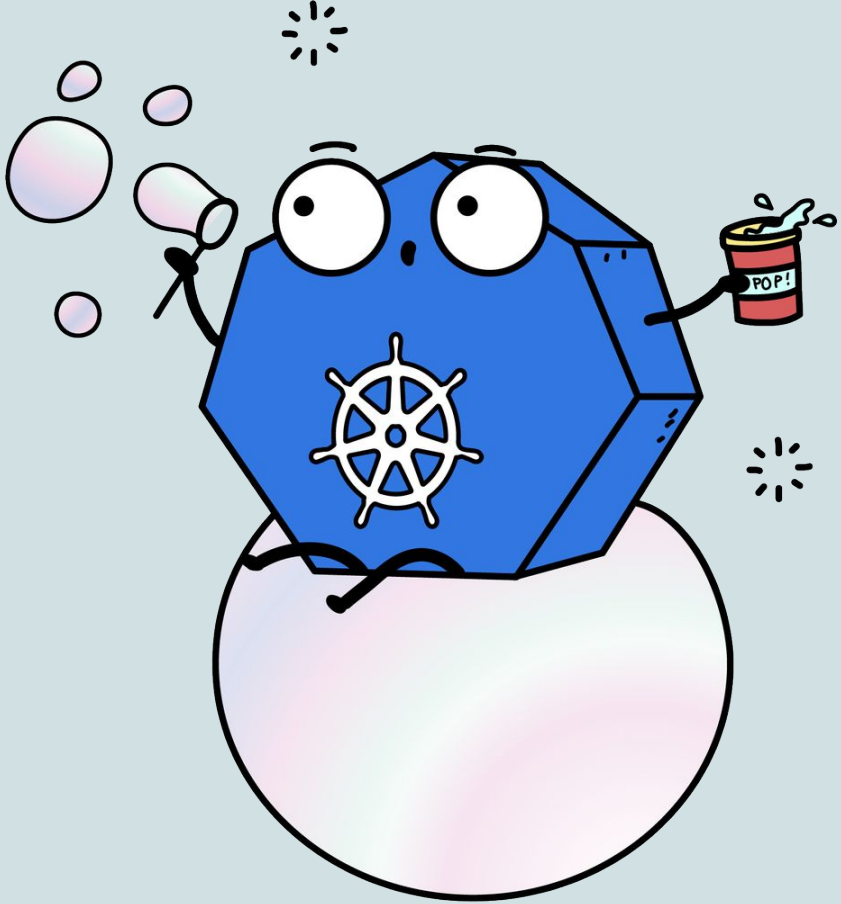
```
$ kustomize build /src/main/k8s/overlay/prod
```

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: kustomize-app
spec:
 replicas: 10
 selector:
   matchLabels:
     serving: "true"
 template:
   metadata:
     labels:
       serving: "true"
   spec:
     containers:
       - name: app
         env:
           - name: MESSAGE_BODY
             value: by Kustomize ❤️
           - name: MESSAGE_FROM
             value: overlay 'custom-env'
         image: gcr.io/foo/kustomize:latest
         imagePullPolicy: IfNotPresent
         ports:
           - containerPort: 8080
             name: http
             protocol: TCP
```

```
$ kubectl apply -k /src/main/k8s/overlay/prod
```

KUSTOMIZE

- No template!
- Your YAML are usable without Kustomize
- Work with inheritance and mixins
- Automatic hashs on config|secrets to trigger redeploy
- Fork friendly
- built-in **kubectl 1.14**

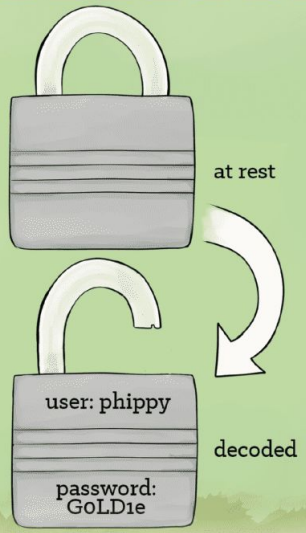


BEST PRACTICES

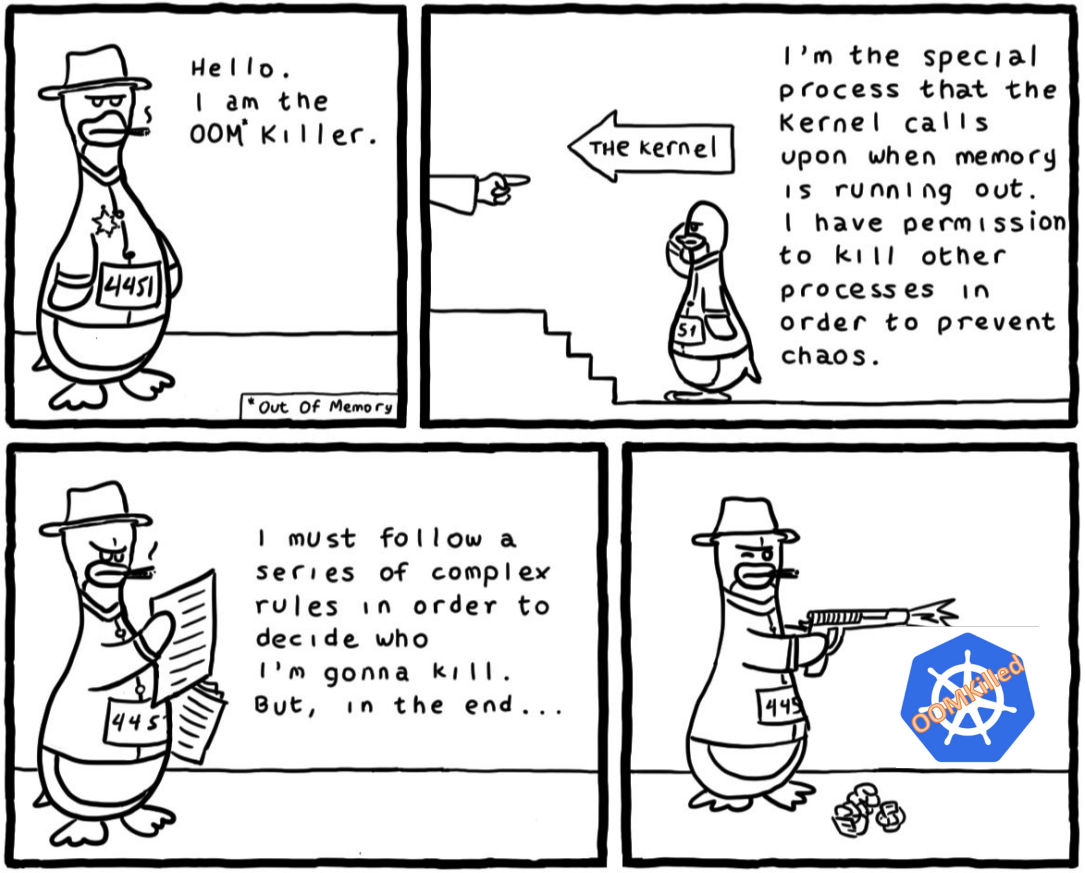
WE REPEAT, DON'T HARDCODE PASSWORDS!

Secrets

- Secrets are Base 64 encoded "at rest" but the data is automatically decoded when attached to a Pod
- Secrets can be attached as files or environment variables
- Use add-on encryption providers for locking your data



WHY OPTIMIZE KUBERNETES RESOURCES?




```yaml
resources:
    requests:
        memory: "64Mi"
        cpu: "20m"
    limits:
        memory: "128Mi"
        cpu: "500m"
```

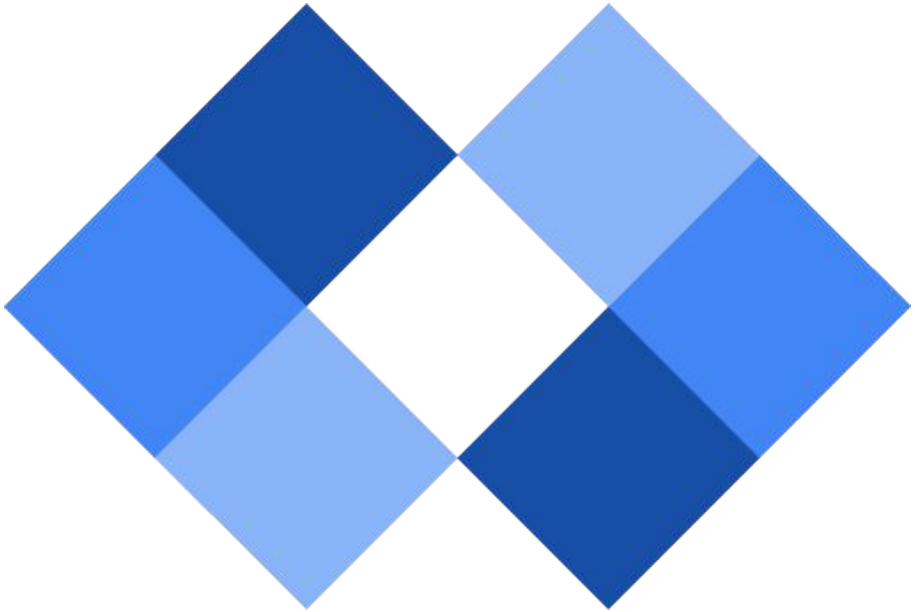
HOW TO SET RELEVANT RESOURCES REQUESTS /LIMITS?

Display Resource (CPU/Memory/Storage) usage of pods

Usage:

```
$ kubectl top po
NAME                                CPU(cores)   MEMORY(bytes)
bash-6dc7f844bb-4j2qd               8m           60Mi
details-v1-6764bbc7f7-xpk62         9m           67Mi
httpbin-f455f64c4-h8qrs             7m           87Mi
ratings-v1-7bc85949-zgn5v           14m          65Mi
reviews-v1-fdbf674bb-g2kz5          8m           152Mi
```

Write, build, deploy & operate directly in your IDE



Google Cloud Code

- Code completion
- Templates
- K8s explorer
- Continuous deployment
- Logs
- Debug
- ...

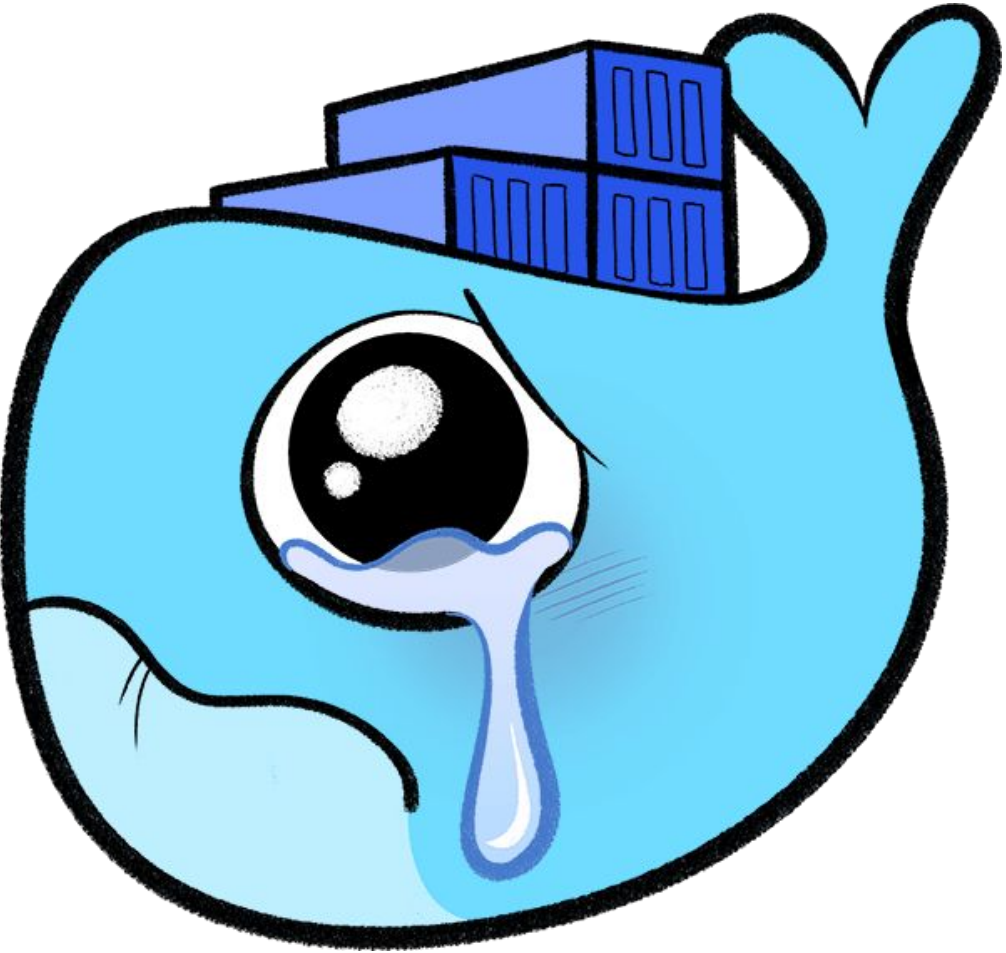
Write, build, deploy & operate directly from your IDE

Kubernetes and VS Code: Zero to Deployed (Cloud Next '19)

1 875 vues

66 1 PARTAGER ENREGISTRER

https://www.youtube.com/watch?v=Ns0fHKuv7_Y



Kubernetes, yes, but not for storage

Not recommended for stateful app (storage like postgresql, cassandra …)

Kube-hunter

Kubernetes penetration testing tool.

https://github.com/aquasecurity/kube-hunter

Ip v6 ready

- Since v1.9: supports IPv6-only clusters
- v1.13: IPv6-friendly CoreDNS
- Next big challenge: dual stack support for both IPv4 and IPv6.

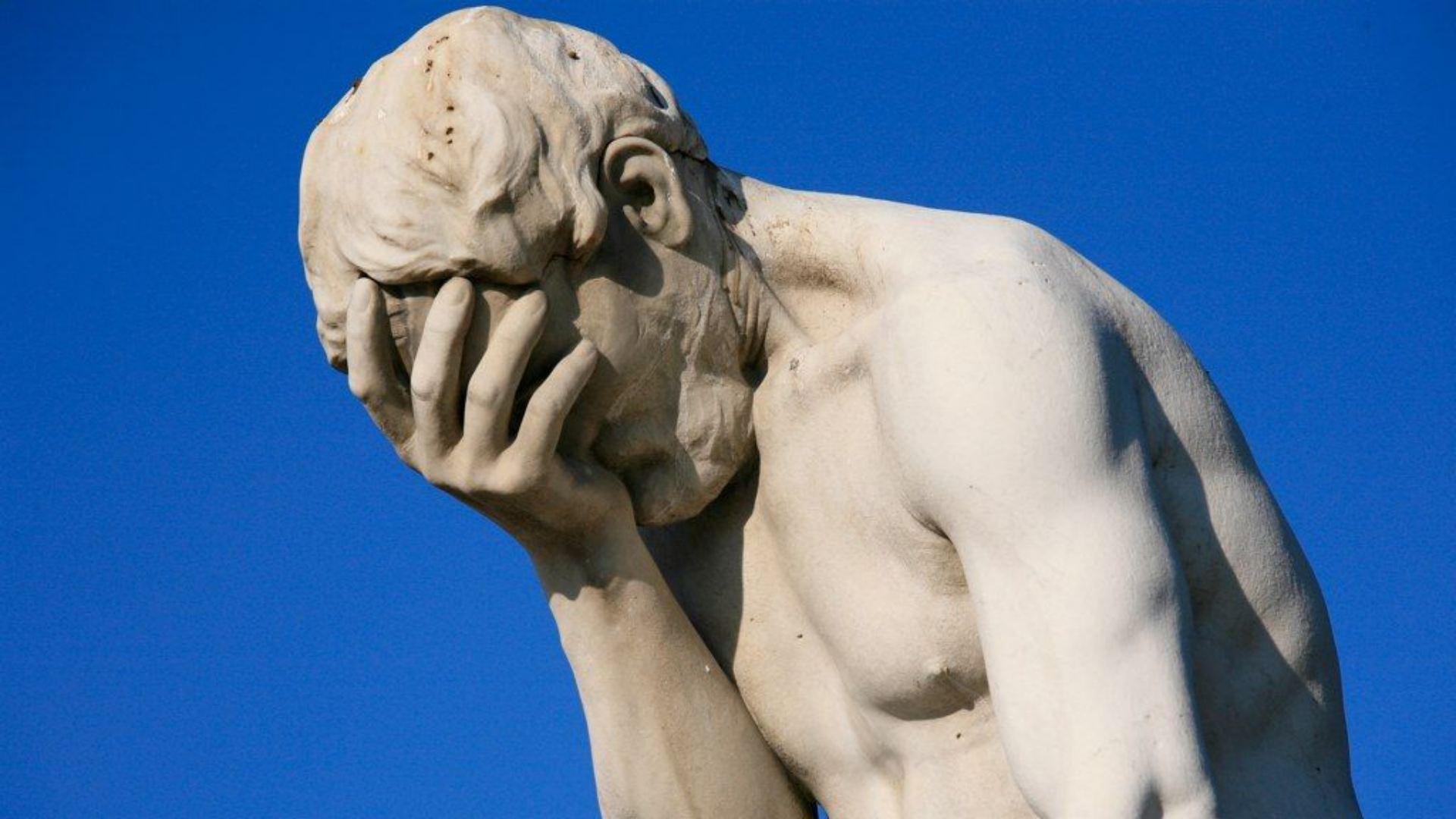
+

Vscode extensions

- Kubernetes VS Code extensions warning requests resources limits
- Red Hat YAML plugin

Istio

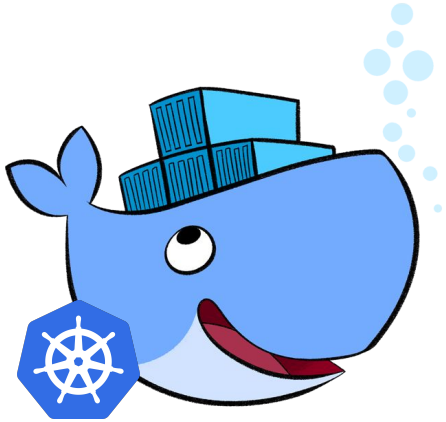
YAML



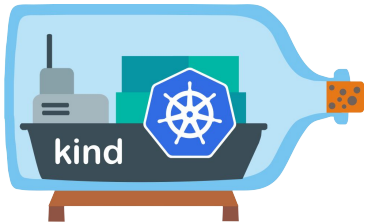
With **349** parameters

or with **5** profiles

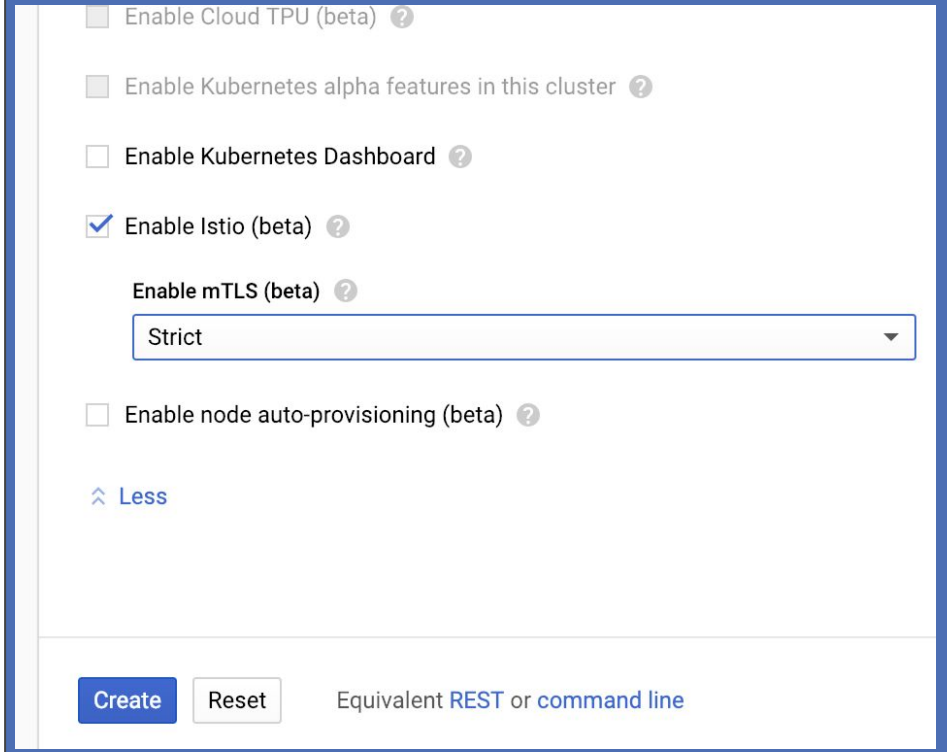
Compatibility



And others...



Istio is one click away



Use the istioctl command line tool

```
/\:~ kevin $ istioctl version
version.BuildInfo{Version:"1.1.1", GitRevision:"2b1331886076df103179e3da5dc9077fed59c989", User:"root", Host:"7077232d-4
c6c-11e9-813c-0a580a2c0506", GolangVersion:"go1.10.4", DockerHub:"docker.io/istio", BuildStatus:"Clean", GitTag:"1.1.0-1
7-g2b13318"}
```

Get an overview of the mesh

```
/\:~ kevin $ kub istio proxy-status
NAME                                                   CDS        LDS        EDS               RDS          PILOT                           VERSION
istio-egressgateway-6555655585-jj4mm.istio-system      SYNCED     SYNCED     SYNCED (100%)     NOT SENT     istio-pilot-6d9b655646-htg9f    1.1.0
istio-ingressgateway-74484b55f4-sfl5j.istio-system     SYNCED     SYNCED     SYNCED (100%)     SYNCED       istio-pilot-6d9b655646-htg9f    1.1.0
search-6f8444b969-k48mq.default                        SYNCED     SYNCED     SYNCED (50%)      SYNCED       istio-pilot-6d9b655646-htg9f    1.1.0
ui-v1-75f8dcf9b9-kcdf6.default                         SYNCED     SYNCED     SYNCED (50%)      SYNCED       istio-pilot-6d9b655646-htg9f    1.1.0
ui-v2-7bbd8b9c7c-qz2zk.default                         SYNCED     SYNCED     SYNCED (50%)      SYNCED       istio-pilot-6d9b655646-htg9f    1.1.0
```

Debugging istio

```
$ istioctl proxy-config route ui-v2-7bbd8b9c7c-qz2zk --name 80 -o json | jq '.[].virtualHosts[] | select(.name | contains("search"))'
```


```
{
  "name": "search.default.svc.cluster.local:80",
  "domains": [
    "search.default.svc.cluster.local",
    "search.default.svc.cluster.local:80"
  ],
  "routes": [
    {
      "match": {
        "prefix": "/"
      },
      "route": {
        "cluster": "outbound|80|version-1|search.default.svc.cluster.local",
        "timeout": "0s",
        "retryPolicy": {
          "retryOn": "connect-failure,refused-stream,unavailable,cancelled,resource-exhausted,retriable-status-codes",
          "numRetries": 2,
          "retryHostPredicate": [
            {
              "name": "envoy.retry_host_predicates.previous_hosts"
            }
          ],
          "hostSelectionRetryMaxAttempts": "3",
          "retriableStatusCodes": [
            503
          ]
        },
        "maxGrpcTimeout": "0s"
      },
      "metadata": {
        "filterMetadata": {
```

Follow performance of service

```
›Λ\:~ kevin $ kub istio experimental metrics search
                                WORKLOAD    TOTAL RPS    ERROR RPS  P50 LATENCY  P90 LATENCY  P99 LATENCY
                                  search        6.311        0.000          2ms          4ms          6ms
```

Istio 1.1 news

New Validate command

Added the istioctl validate command for offline validation of Istio Kubernetes resources.

Usage:

```
$ istioctl validate
```

Istio 1.1 news

Lin Sun
@linsun_unc

Abonné

We are changing @IstioMesh v1.1 default to allow all outbound traffic by default because we believe many of our users spent hours to figure out the missing service entries when moving their #microservices to #istio

Traduire le Tweet

04:48 - 21 févr. 2019

8 Retweets **25** J'aime

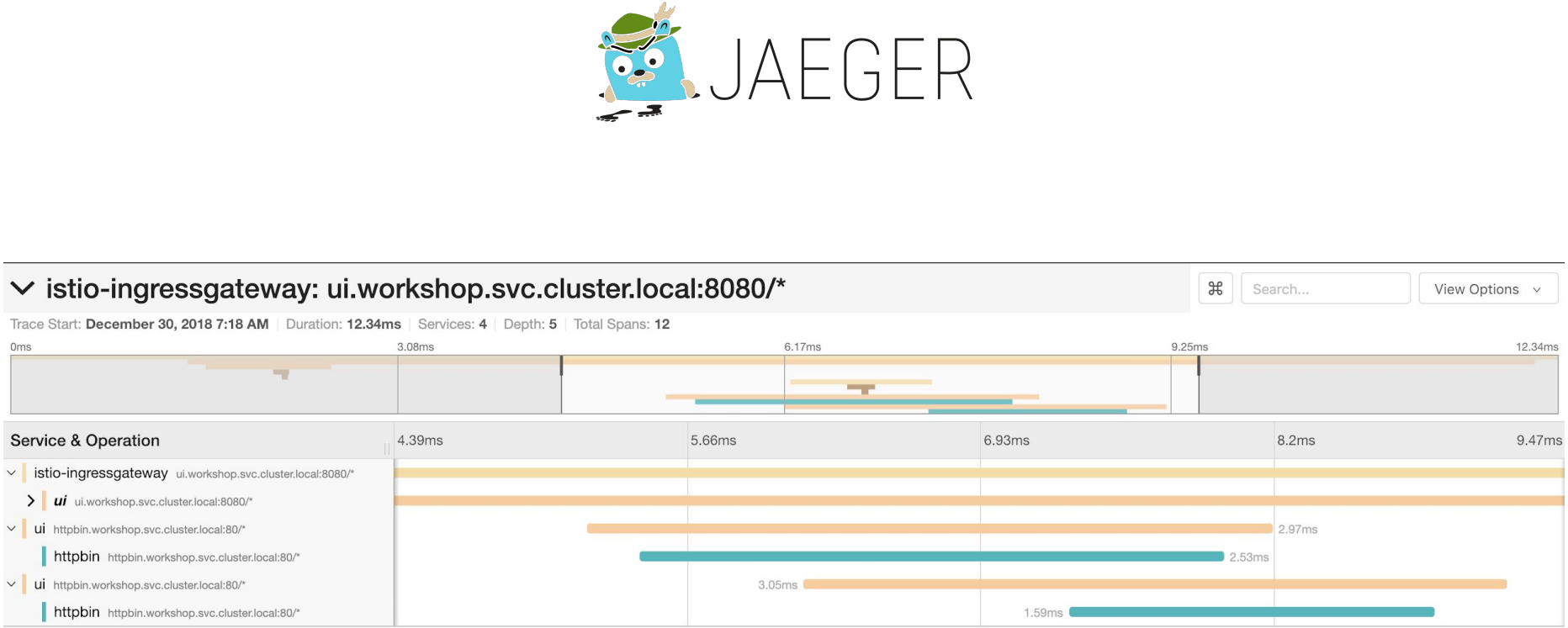
5 8 25

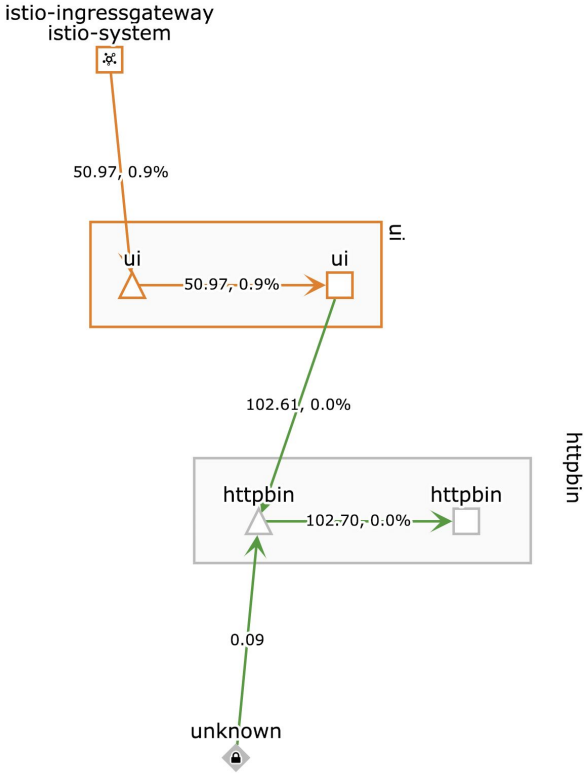
Deny all communication between pods

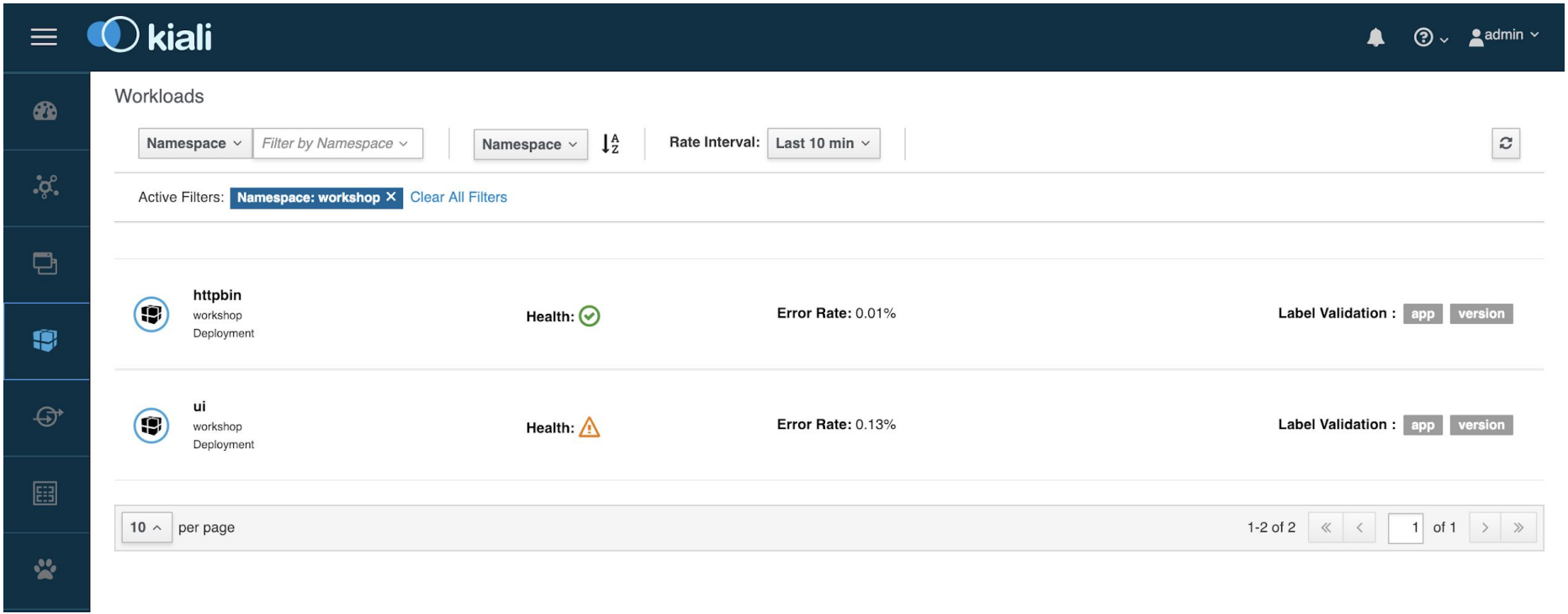
Use great tools to follow activity in your cluster...

JAEGER

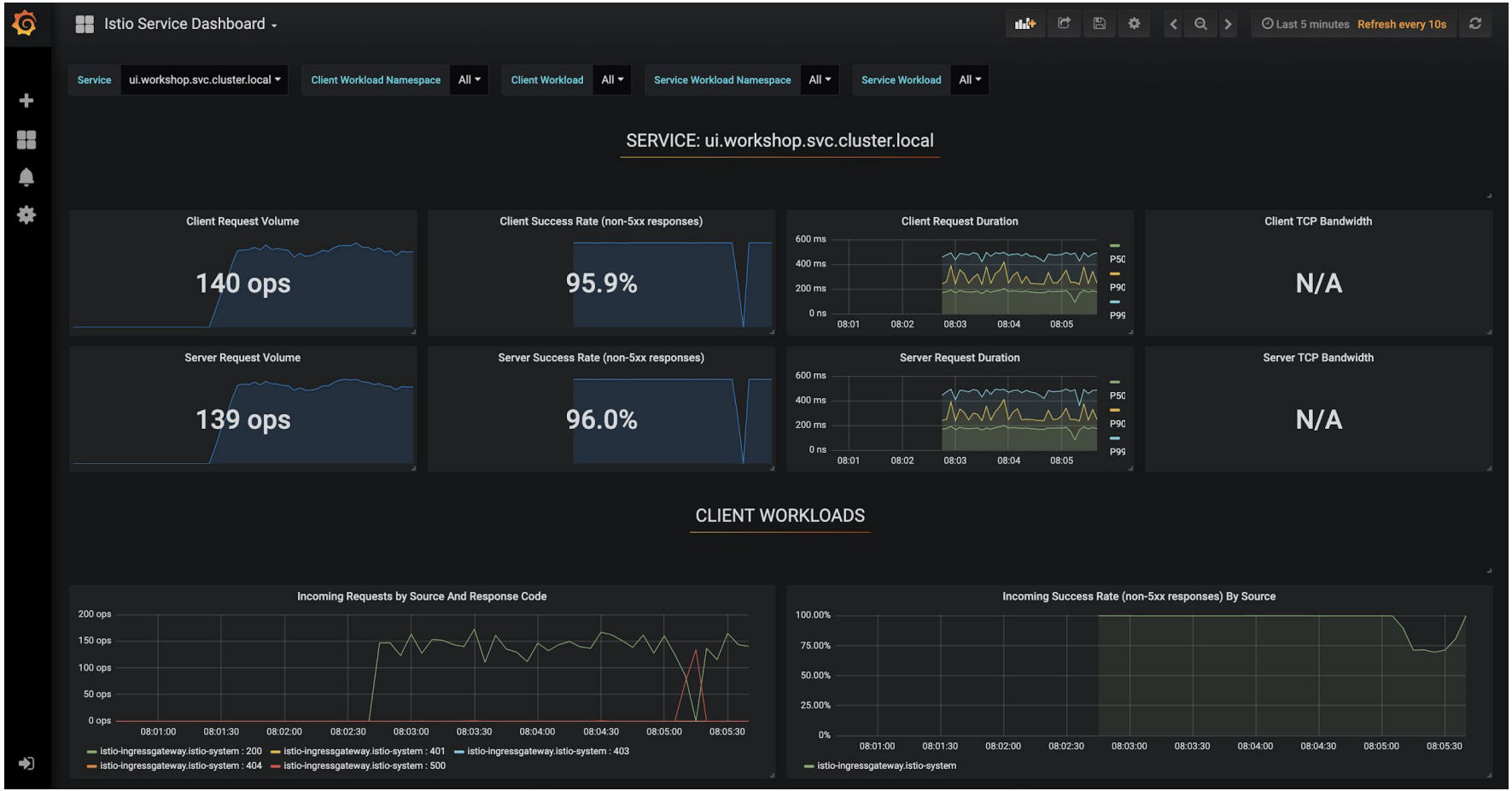
Grafana


JAEGER
istio-ingressgateway: ui.workshop.svc.cluster.local:8080/*
Search...
View Options
Trace Start: December 30, 2018 7:18 AM | Duration: 12.34ms | Services: 4 | Depth: 5 | Total Spans: 12
0ms
3.08ms
6.17ms
9.25ms
12.34ms
Service & Operation
4.39ms
5.66ms
6.93ms
8.2ms
9.47ms
istio-ingressgateway ui.workshop.svc.cluster.local:8080/*
ui ui.workshop.svc.cluster.local:8080/*
ui httpbin.workshop.svc.cluster.local:80/*
2.97ms
httpbin httpbin.workshop.svc.cluster.local:80/*
2.53ms
ui httpbin.workshop.svc.cluster.local:80/*
3.05ms
httpbin httpbin.workshop.svc.cluster.local:80/*
1.59ms


istio-ingressgateway
istio-system
50.97, 0.9%
ui
ui
ui
50.97, 0.9%
102.61, 0.0%
httpbin
httpbin
httpbin
102.70, 0.0%
0.09
unknown


kiali
admin
Workloads
Namespace
Filter by Namespace
Namespace
Rate Interval:
Last 10 min
Active Filters:
Namespace: workshop
Clear All Filters
httpbin
workshop
Deployment
Health:
Error Rate: 0.01%
Label Validation :
app
version
ui
workshop
Deployment
Health:
Error Rate: 0.13%
Label Validation :
app
version
10
per page
1-2 of 2
1
of 1

Grafana


Istio Service Dashboard
Last 5 minutes
Refresh every 10s
Service
ui.workshop.svc.cluster.local
Client Workload Namespace
All
Client Workload
All
Service Workload Namespace
All
Service Workload
All
SERVICE: ui.workshop.svc.cluster.local
Client Request Volume
140 ops
Client Success Rate (non-5xx responses)
95.9%
Client Request Duration
600 ms
400 ms
200 ms
0 ns
08:01
08:02
08:03
08:04
08:05
P50
P90
P99
Client TCP Bandwidth
N/A
Server Request Volume
139 ops
Server Success Rate (non-5xx responses)
96.0%
Server Request Duration
600 ms
400 ms
200 ms
0 ns
08:01
08:02
08:03
08:04
08:05
P50
P90
P99
Server TCP Bandwidth
N/A
CLIENT WORKLOADS
Incoming Requests by Source And Response Code
200 ops
150 ops
100 ops
50 ops
0 ops
08:01:00
08:01:30
08:02:00
08:02:30
08:03:00
08:03:30
08:04:00
08:04:30
08:05:00
08:05:30
istio-ingressgateway.istio-system : 200
istio-ingressgateway.istio-system : 401
istio-ingressgateway.istio-system : 403
istio-ingressgateway.istio-system : 404
istio-ingressgateway.istio-system : 500
Incoming Success Rate (non-5xx responses) By Source
100.00%
75.00%
50.00%
25.00%
0%
08:01:00
08:01:30
08:02:00
08:02:30
08:03:00
08:03:30
08:04:00
08:04:30
08:05:00
08:05:30
istio-ingressgateway.istio-system

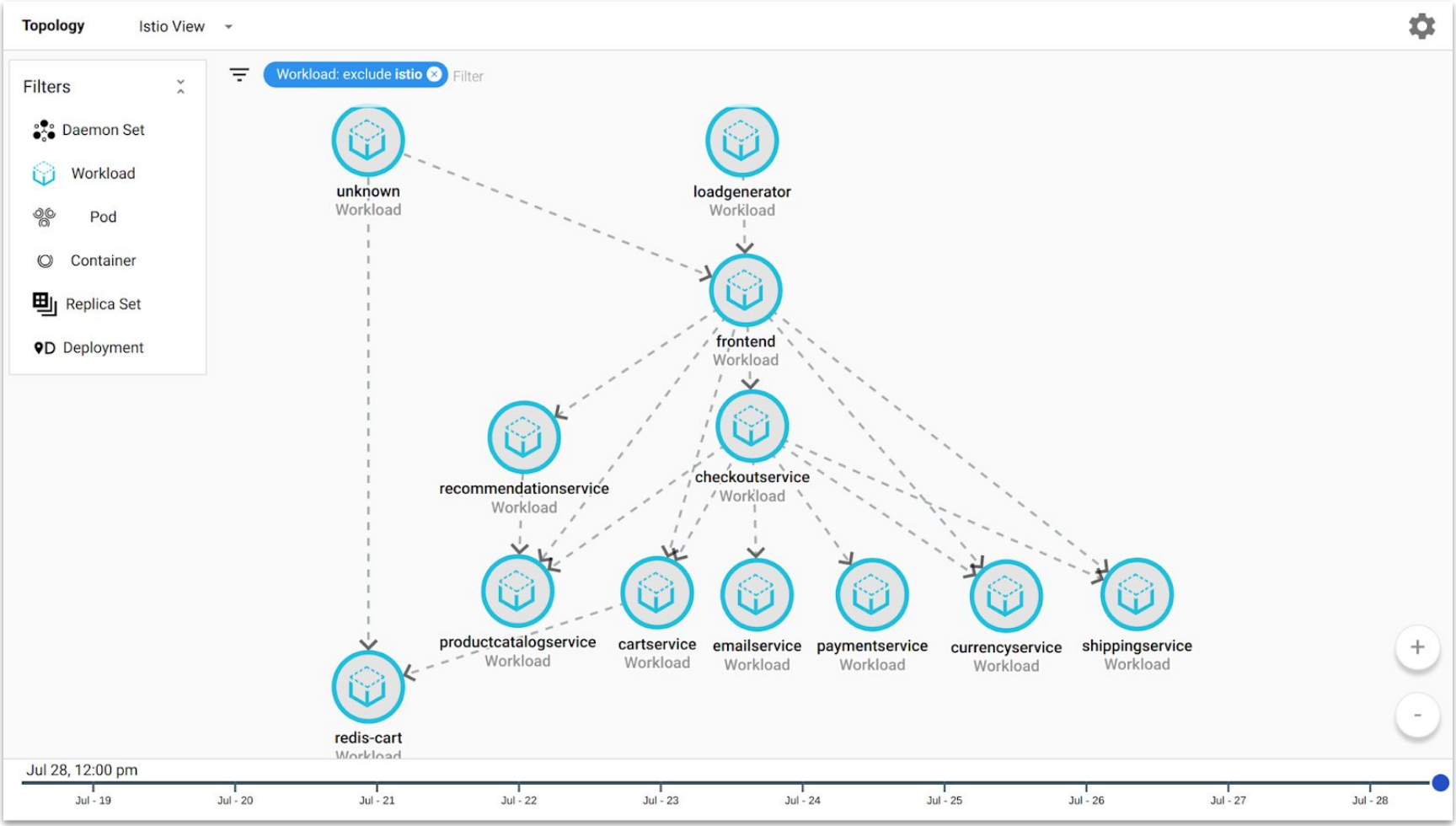
...BUT WITH CAUTION, YOU HAVE TO MAINTAIN THEIR STATE!

JAEGER

kiali

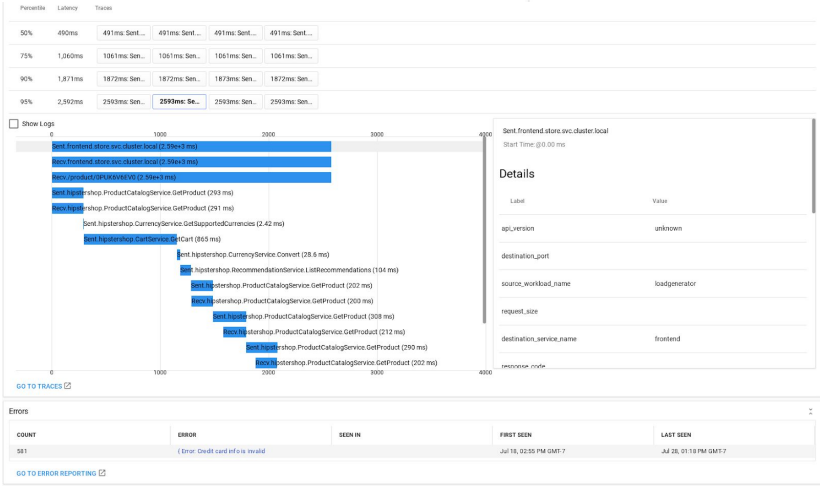
Grafana

...OR USE THE MANAGED VERSIONS OF THEM!


Topology
Istio View
Filters
Daemon Set
Workload
Pod
Container
Replica Set
Deployment
Workload: exclude istio
Filter
unknown
Workload
loadgenerator
Workload
frontend
Workload
recommendationservice
Workload
checkoutservice
Workload
productcatalogservice
Workload
cartservice
Workload
emailservice
Workload
paymentservice
Workload
currencyservice
Workload
shippingservice
Workload
redis-cart
Workload
Jul 28, 12:00 pm
Jul - 19
Jul - 20
Jul - 21
Jul - 22
Jul - 23
Jul - 24
Jul - 25
Jul - 26
Jul - 27
Jul - 28


Latency, 95% < 3025ms in Rolling 30 Days
Service level indicators
5 min interval (mean)
Error budget
5 min interval (next older)
Service level objective compliance
5 min interval (next older)


Metrics
Filter...
Suggested Filters:
Group By: project_id
Group By: request_operation
Group By: response_code
Group By: source_workload_name
Group By: source_workload_namespace
Request Count
by project id, response code, request operation, source workload name, source workload namespace (sum)
sum
1 min interval (sum)
Response Latencies
by project id, response code, request operation, source workload name, source workload namespace (sum)
1 min interval (sum)


Percentile
Latency
Traces
50%
490ms
75%
1,060ms
90%
1,871ms
95%
2,592ms
Show Logs
Details
GO TO TRACES
Errors
COUNT
ERROR
SEEN IN
FIRST SEEN
LAST SEEN
GO TO ERROR REPORTING

Help me, I receive 404 and 503 error http code!

Help me, I receive 404 and 503 error http code!

1 Port name must start by **http-**, **http2-**, **tcp-**, **udp-** ...

Help me, I receive 404 and 503 error http code!

1. Port name must start by **http-**, **http2-**, **tcp-**, **udp-** ...

2. Check pilot is **running** / **scale** pilot

```
⋀\:~ kevin $ kub get pods istio-pilot-6d9b655646-htg9f -n istio-system
NAME                             READY   STATUS    RESTARTS   AGE
istio-pilot-6d9b655646-htg9f   2/2     Running   0          106m
```

Help me, I receive 404 and 503 error http code!

1. Port name must start by **http-**, **http2-**, **tcp-**, **udp-** ...
2. Check pilot is **running** / **scale** pilot
3. Use **distributed tracing and logs** to follow your request through envoy

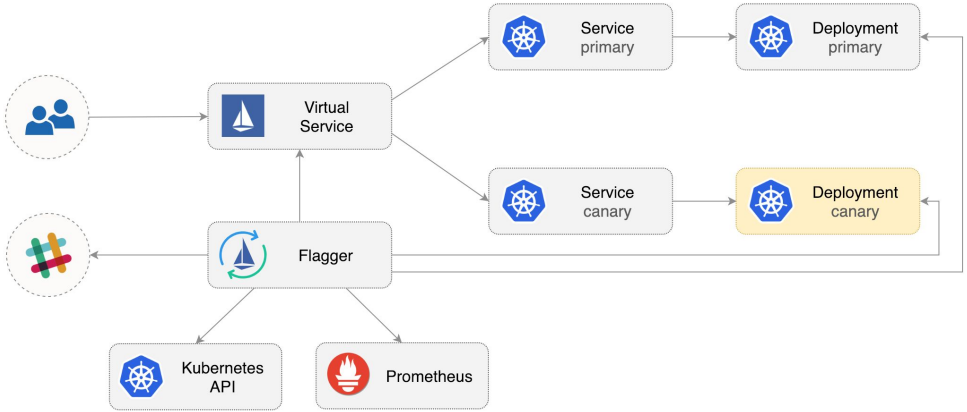
Sometimes you need to manage exceptions

```
$ kubectl label namespace toto
istio-injection=disabled
```

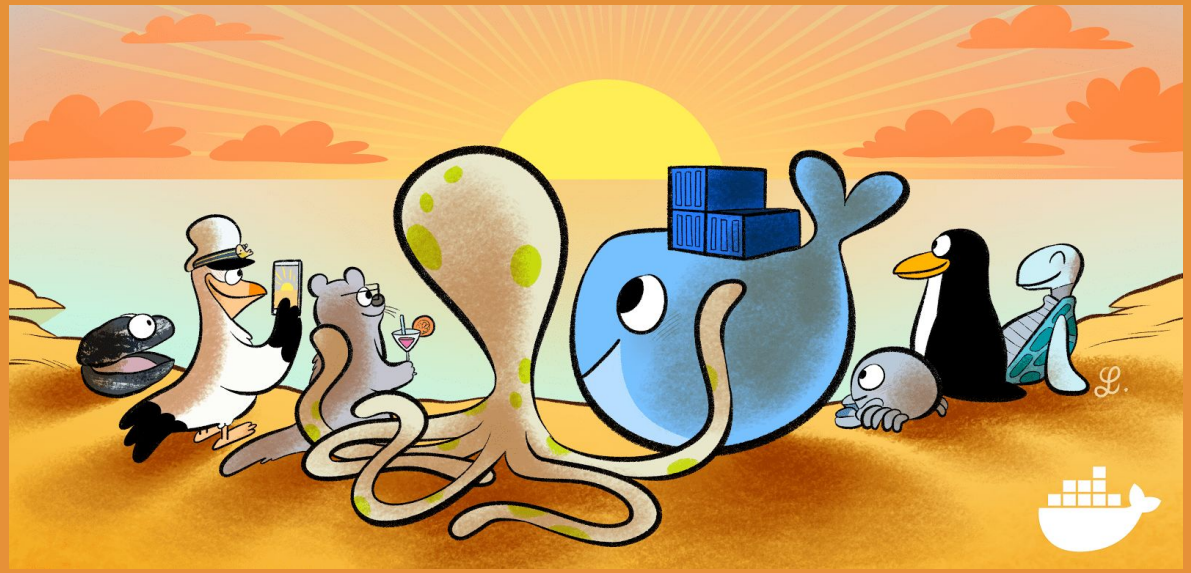
Or

```
spec:
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
```

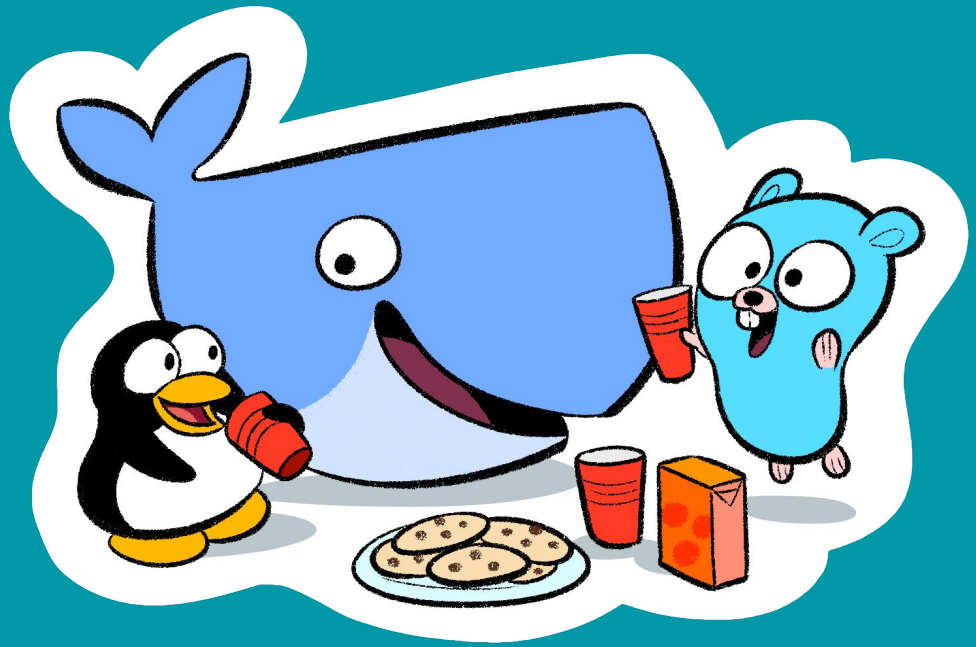
FLAGGER


Service
primary
Deployment
primary
Virtual
Service
Service
canary
Deployment
canary
Flagger
Kubernetes
API
Prometheus

. . .



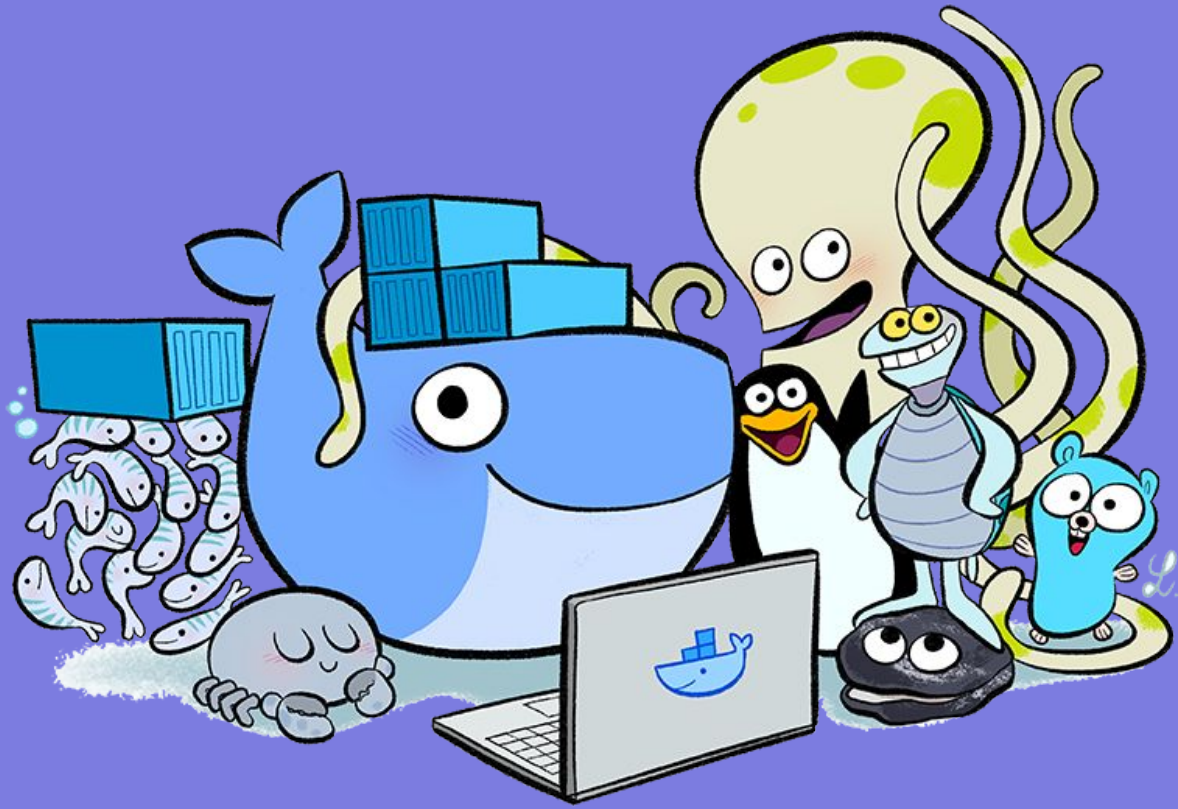
Conclusion



http://bit.ly/docker-k8s-Istio-tips-tricks

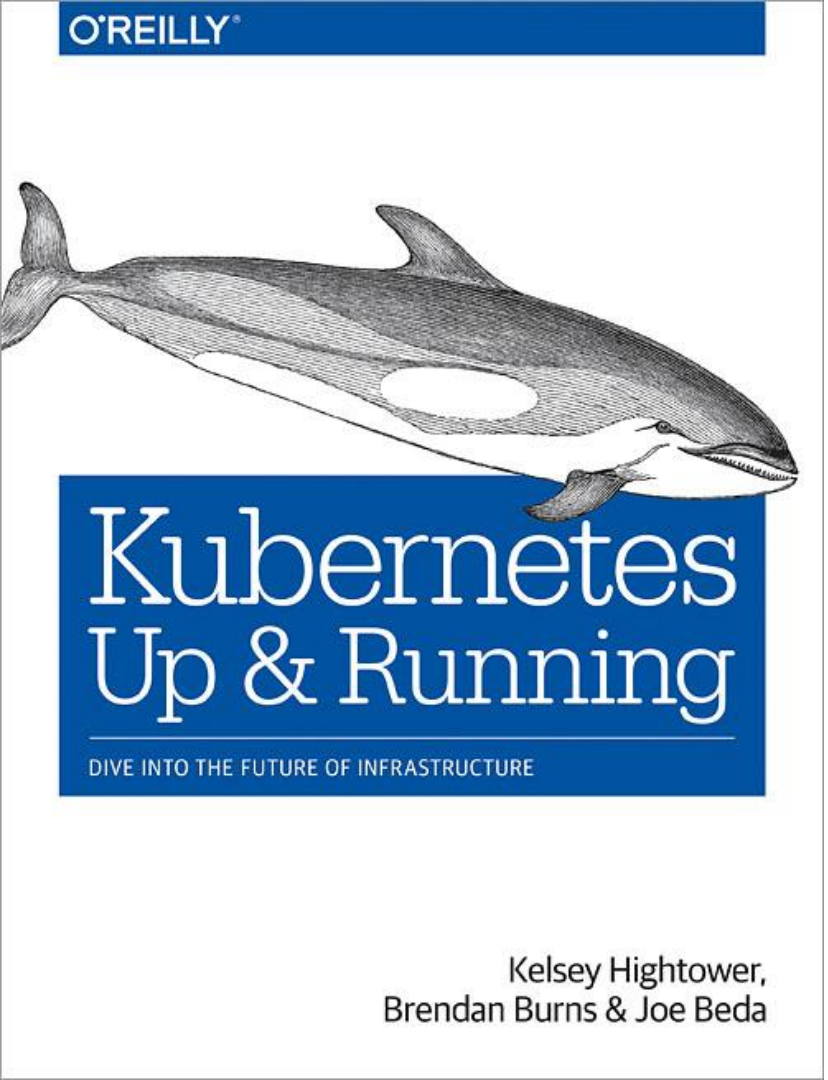
$ DOCKER BUILD "THANKS-YOU"

$ KUBECTL GET STICKERS



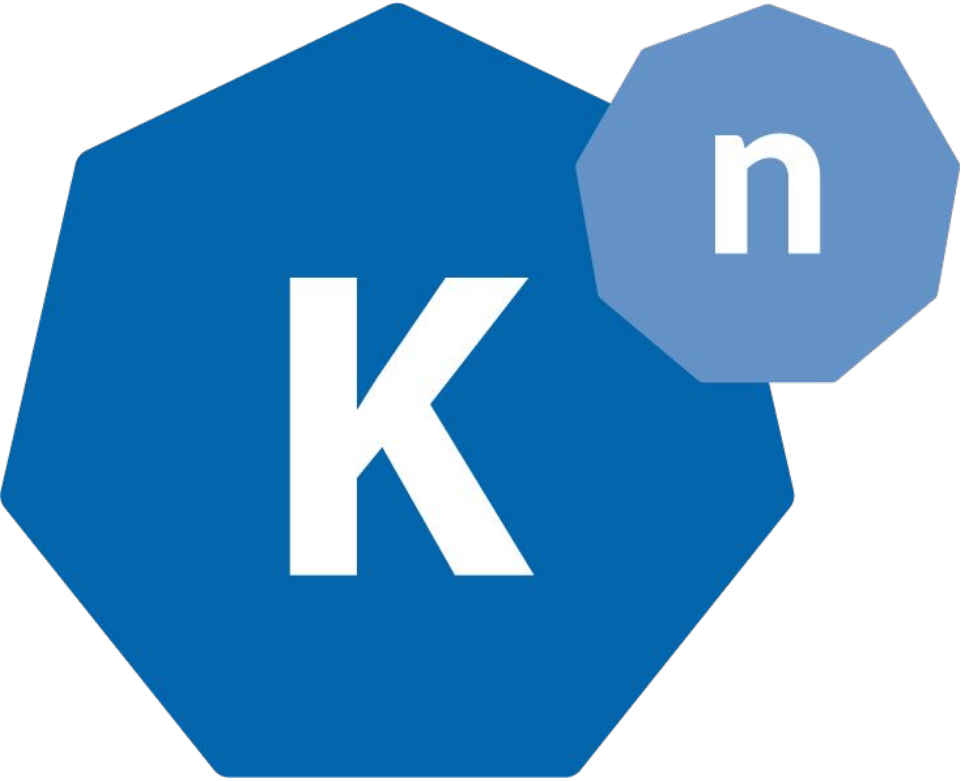
$ KUBECTL APPLY -F QUESTIONS.YAML

Bonus track



Resources

- Kubedex
- https://kubernetespodcast.com
- Phippy goes to zoo: a kubernetes story
- https://kubectl.docs.kubernetes.io/
- discuss.kubernetes.io
- discuss.istio.io
- operatorhub.io
- https://groups.google.com/forum/m/#!msg/kubernetes-announce/

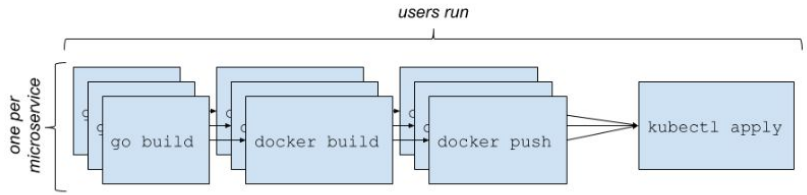


What about FaaS on K8s?

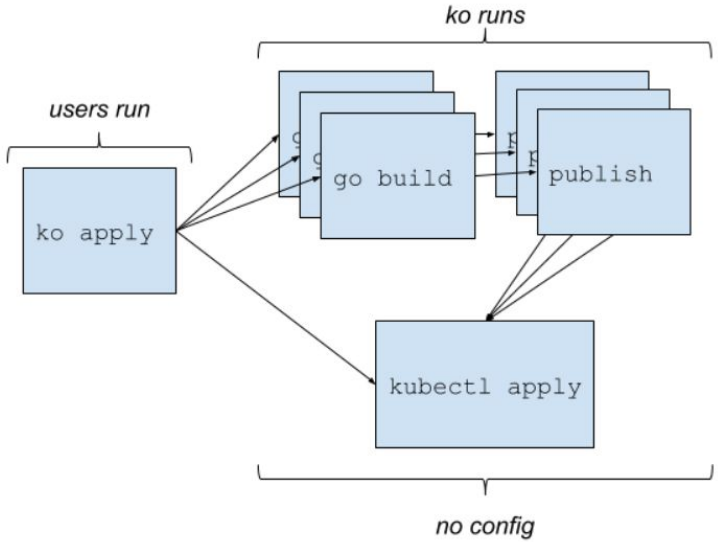
Knative!

Ko: Fast kubernetes microservices development in Go

common way:



ko approach:




HELM


BONUS

Force recreate pods

In order to recreate pods during Helm upgrade in case of configmap or secret changes

```
$ helm upgrade xxx --recreate-pods
```

Or with annotations in YAML files:

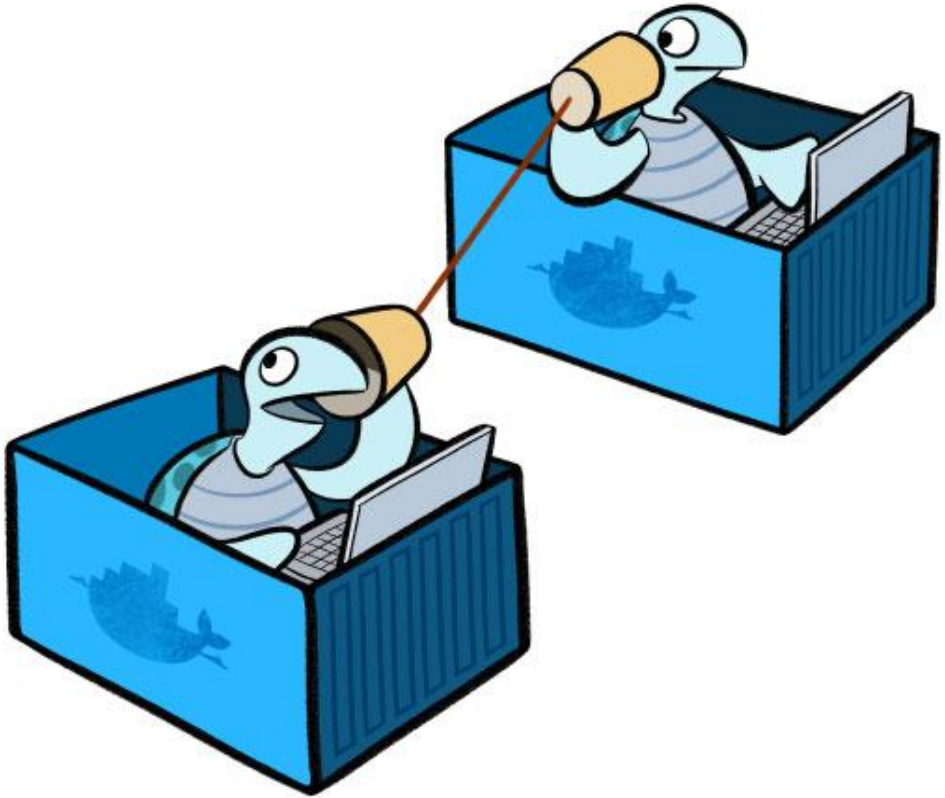
```
spec:
  template:
    metadata:
      annotations:
        checksum/configmap-config: {{ include (print $.Template.BasePath “/configmap-config.yaml”) . |
sha256sum }}
```

Validate docker compose

Validate and view compose file

Usage:

```
$ docker-compose config
```



Why a service mesh?

- Traffic management
- Security
- Observability
- Platform support
- Integration & custom

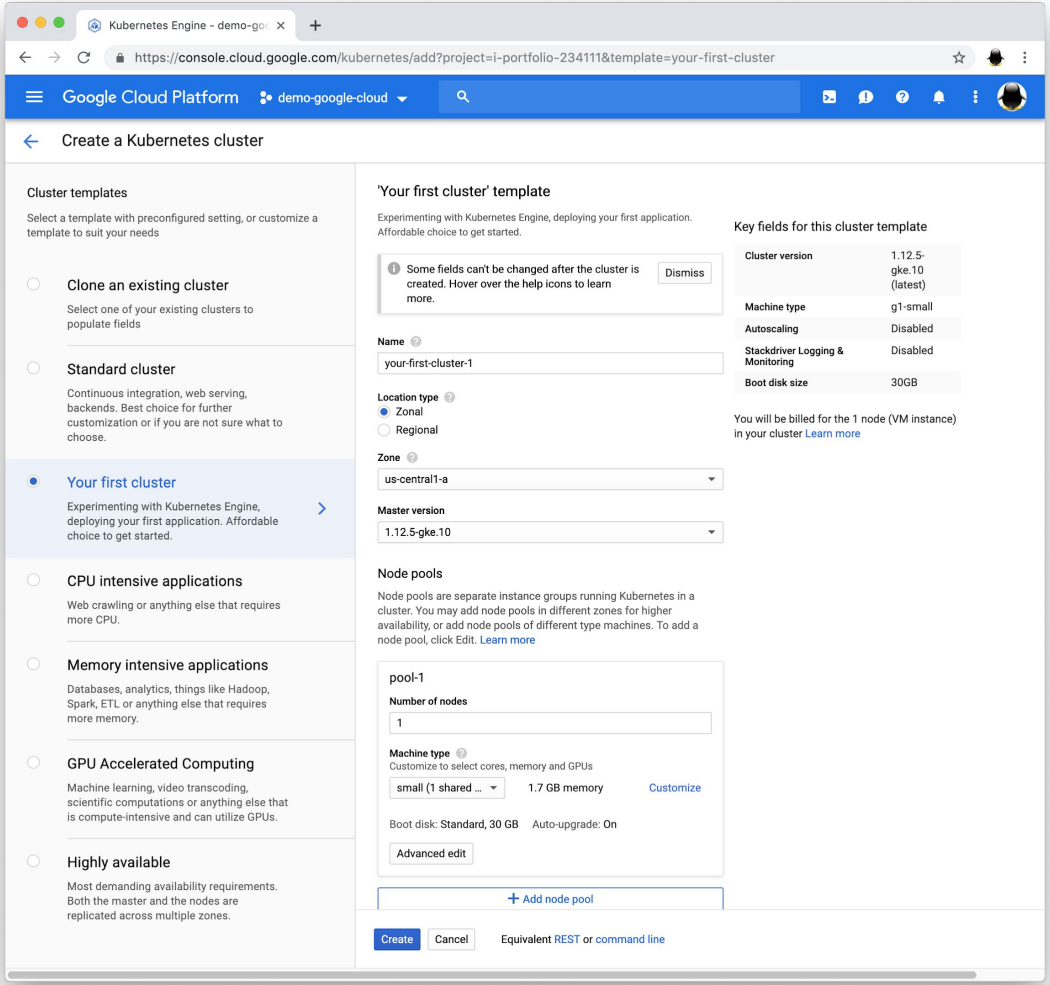
With Grafana, Prometheus, JaegerTracing..

Use .dockerignore when doing ADD / COPY

Use tini

A tiny but valid ‘init’ for containers

https://github.com/krallin/tini


Kubernetes Engine - demo-go
https://console.cloud.google.com/kubernetes/add?project=i-portfolio-234111&template=your-first-cluster
Google Cloud Platform
demo-google-cloud
Create a Kubernetes cluster
Cluster templates
Select a template with preconfigured setting, or customize a template to suit your needs
Clone an existing cluster
Select one of your existing clusters to populate fields
Standard cluster
Continuous integration, web serving, backends. Best choice for further customization or if you are not sure what to choose.
Your first cluster
Experimenting with Kubernetes Engine, deploying your first application. Affordable choice to get started.
CPU intensive applications
Web crawling or anything else that requires more CPU.
Memory intensive applications
Databases, analytics, things like Hadoop, Spark, ETL or anything else that requires more memory.
GPU Accelerated Computing
Machine learning, video transcoding, scientific computations or anything else that is compute-intensive and can utilize GPUs.
Highly available
Most demanding availability requirements. Both the master and the nodes are replicated across multiple zones.
'Your first cluster' template
Experimenting with Kubernetes Engine, deploying your first application. Affordable choice to get started.
Some fields can't be changed after the cluster is created. Hover over the help icons to learn more.
Dismiss
Name
your-first-cluster-1
Location type
Zonal
Regional
Zone
us-central1-a
Master version
1.12.5-gke.10
Node pools
Node pools are separate instance groups running Kubernetes in a cluster. You may add node pools in different zones for higher availability, or add node pools of different type machines. To add a node pool, click Edit. Learn more
pool-1
Number of nodes
1
Machine type
Customize to select cores, memory and GPUs
small (1 shared ...
1.7 GB memory
Customize
Boot disk: Standard, 30 GB
Auto-upgrade: On
Advanced edit
Add node pool
Create
Cancel
Equivalent REST or command line
Key fields for this cluster template
Cluster version
1.12.5-gke.10 (latest)
Machine type
g1-small
Autoscaling
Disabled
Stackdriver Logging & Monitoring
Disabled
Boot disk size
30GB
You will be billed for the 1 node (VM instance) in your cluster Learn more

- **Preambule (A)**

- **Docker**
- Docker, l’outil (K)
- Docker et ses images (A)
- Docker et ses usages (K)
- Docker, les best practices… (A)

- **Kubernetes**
- Kubernetes, à manager ou installer (K)
- Kubectl, la ligne de commande (A+K)
- Kub Log (K)
- Kub Réseau (A)
- Kub templating avec Kustomize (K)
- Kub, les autres best practices (A)

- **Istio**
- Intro/Install (K)
- Help me (A)