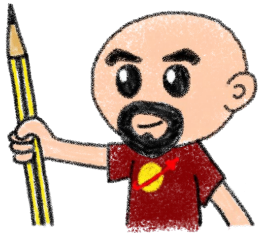
DEVOXX™

I have deployed my app on Minikube... and now what?

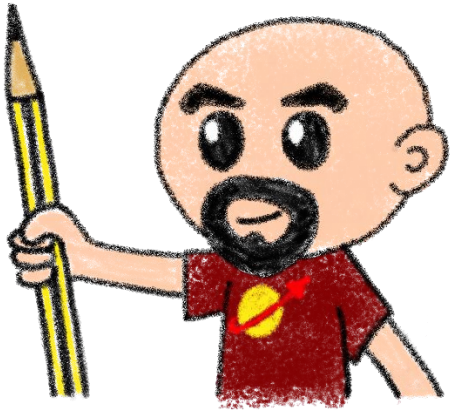
Horacio Gonzalez



OVHcloud

Who are we?

Introducing myself and
introducing OVHcloud

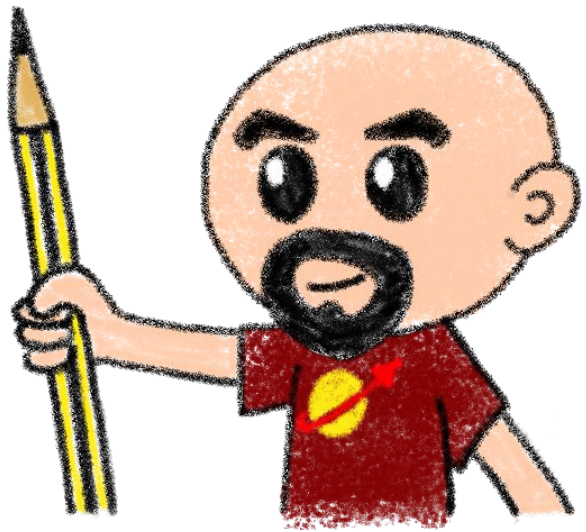


Horacio Gonzalez

@LostInBrittany

Spaniard lost in Brittany.
Developer, speaker,
dreamer, geek

OVHcloud
Team DevRel



DevFest du
Bout du Monde

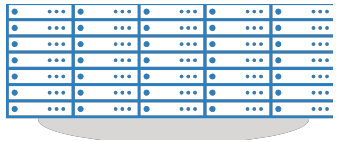
Finist Devs

Google Developers Experts 2019
Web Technologies
GDE
Flutter

OVHcloud: A Global Leader

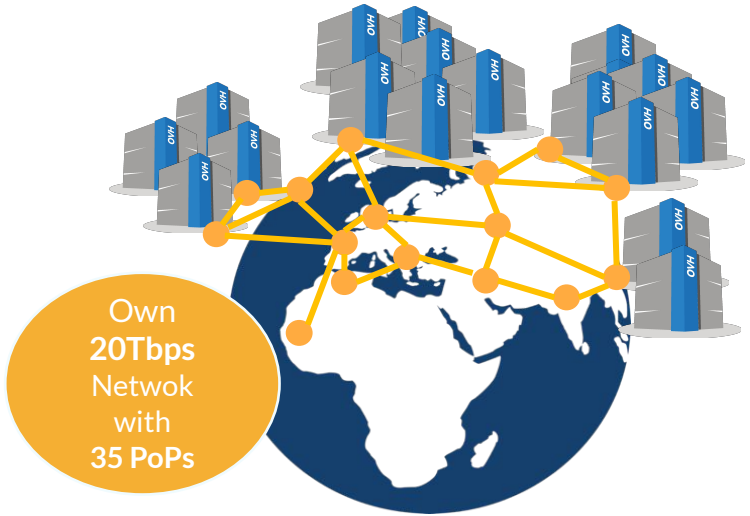
200k Private cloud VMs running

1 **Dedicated IaaS Europe**



Hosting capacity : **1.3M** Physical Servers

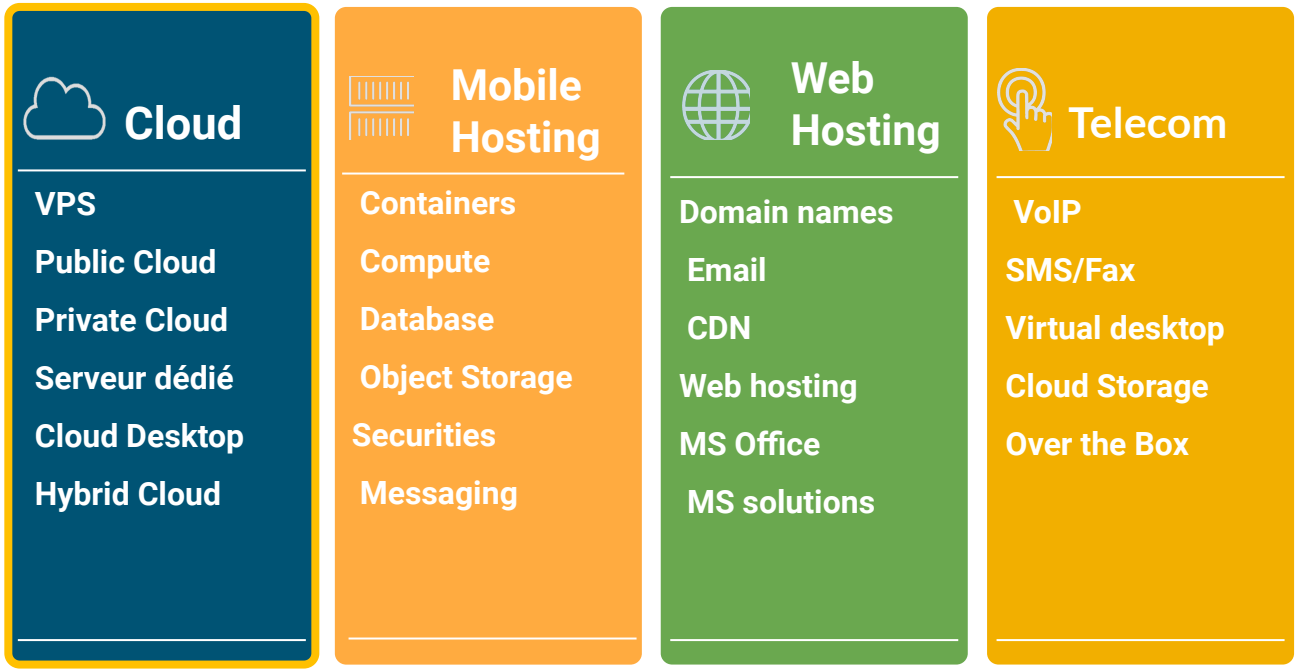
360k Servers already deployed



30 Datacenters

> **1.3M** Customers in **138** Countries

OVHcloud: Our solutions

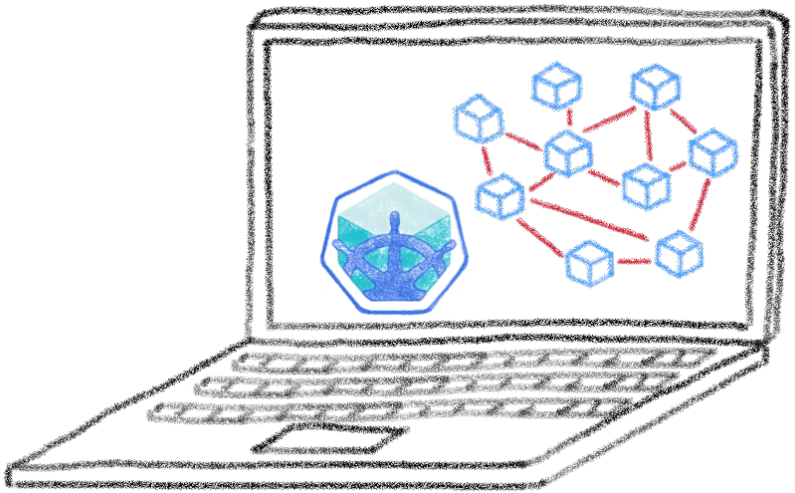


DEVOXX™

Minikube: K8s on my laptop

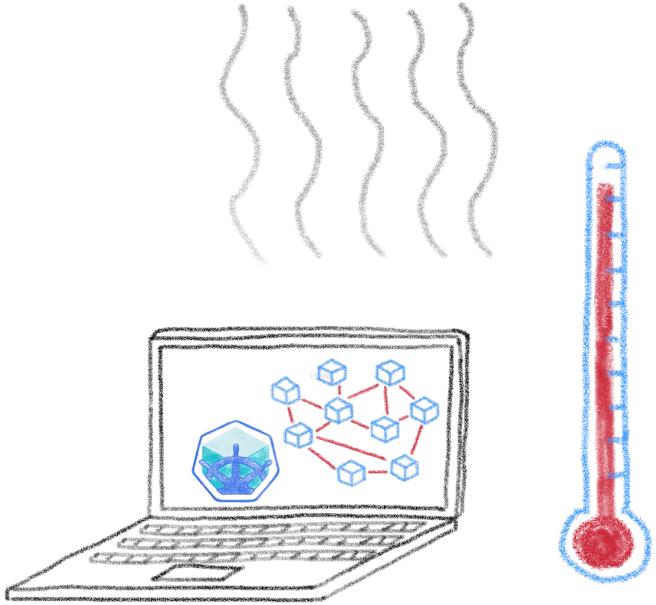
A great fastlane into Kubernetes

Running a full K8s in your laptop



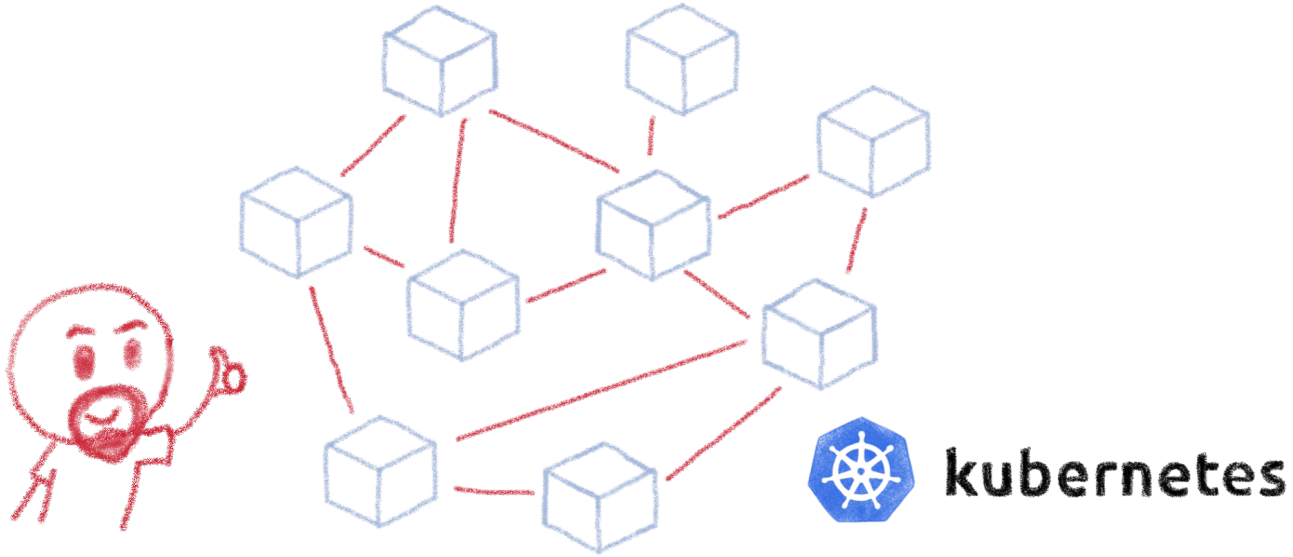
A great learning tool

Your laptop isn't a true cluster



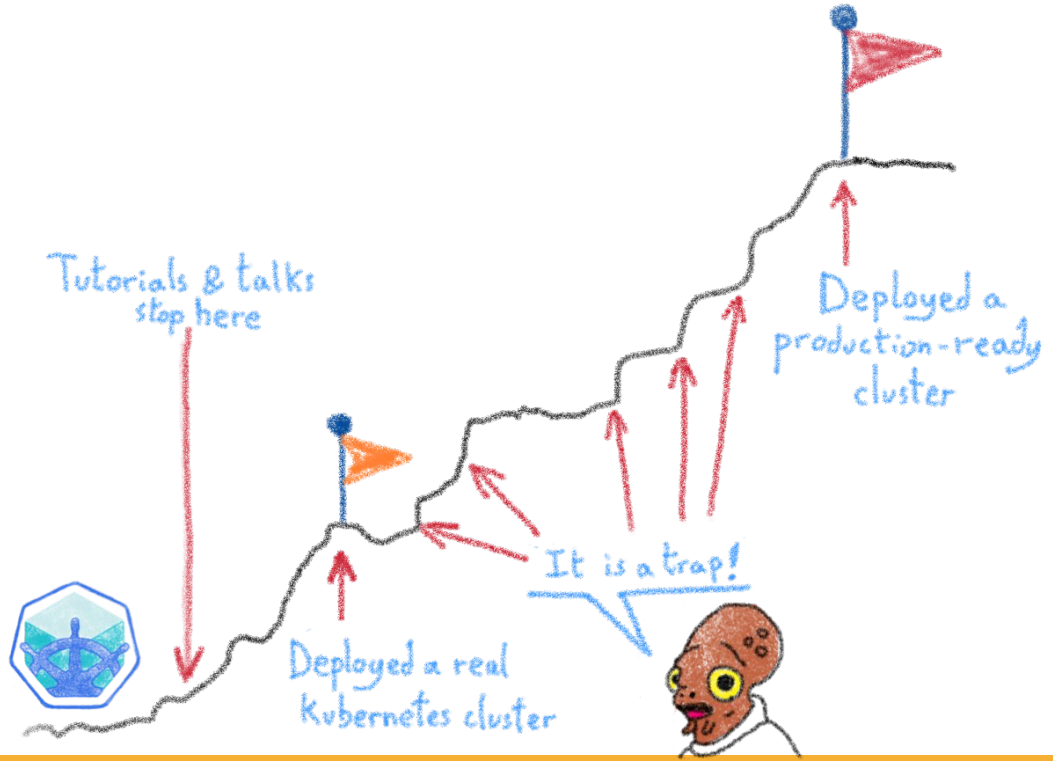
Don't expect real performances

Beyond the first deployment



So I have deployed my distributed architecture on K8s, everything is good now, isn't it?

The long path to production



DEVOXX™

From Minikube to prod

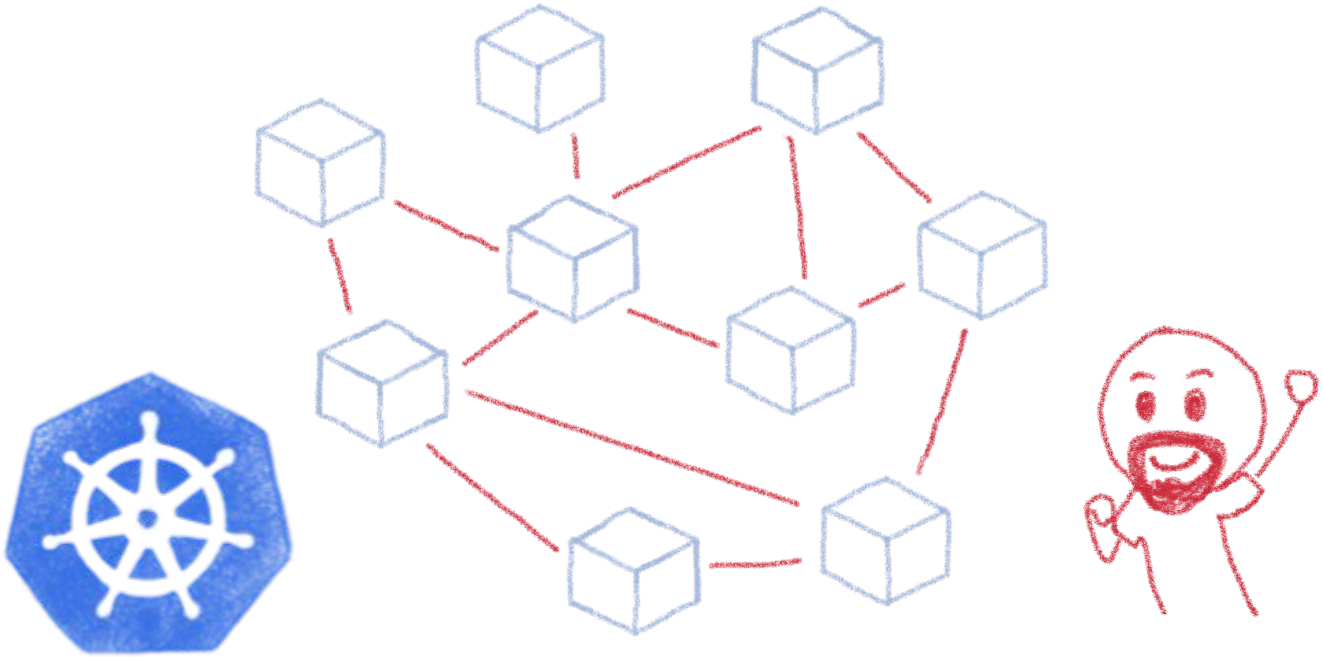
A journey not for the faint of heart

DEVOXX™

Technical Difficulties

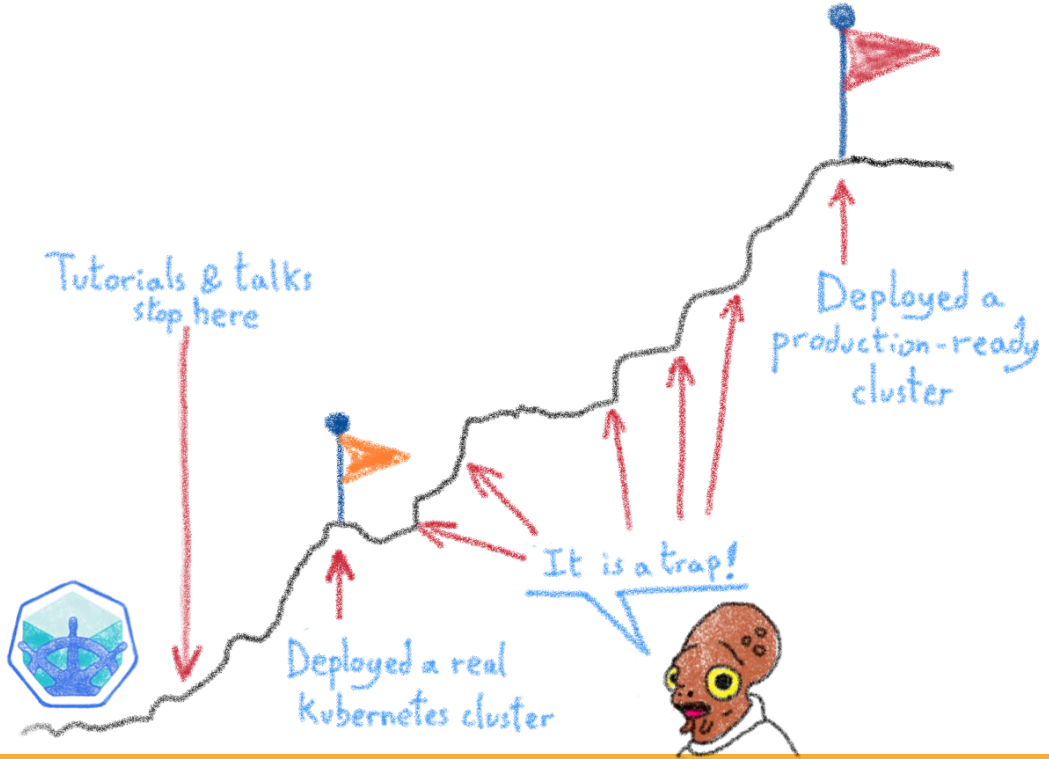
Because music has a price

Kubernetes can be wonderful

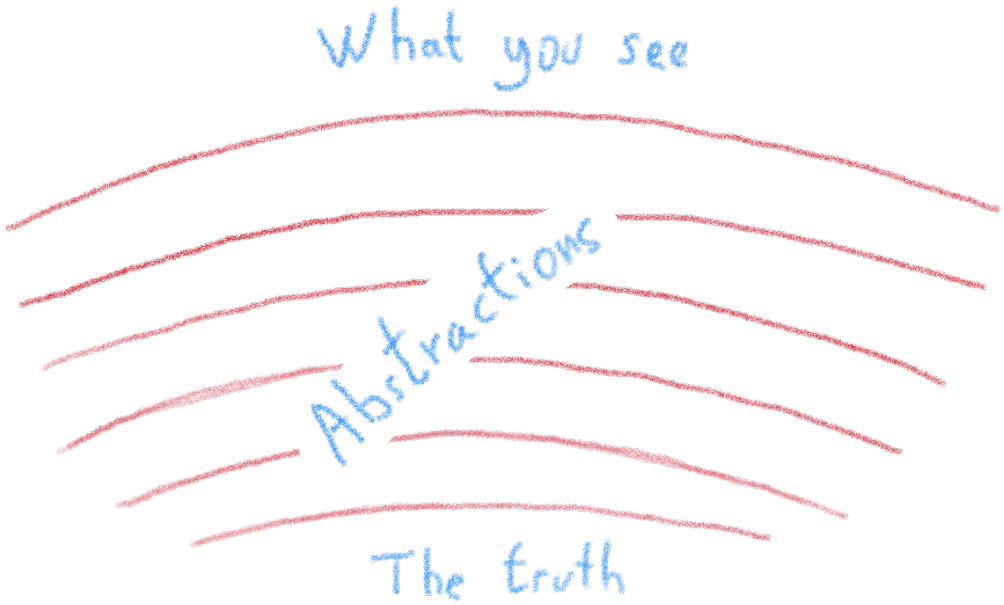


For both developers and devops

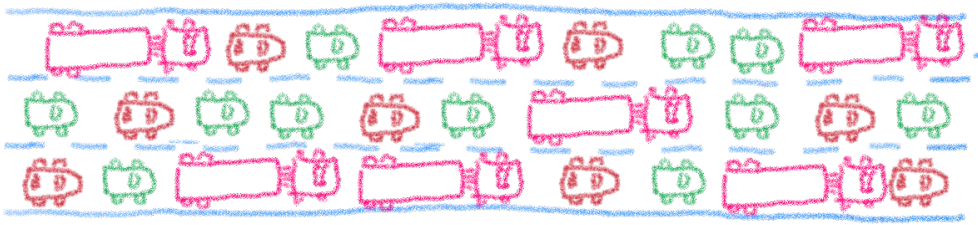
But it comes with a price...



The truth is somewhere inside...



The network is going to feel it...



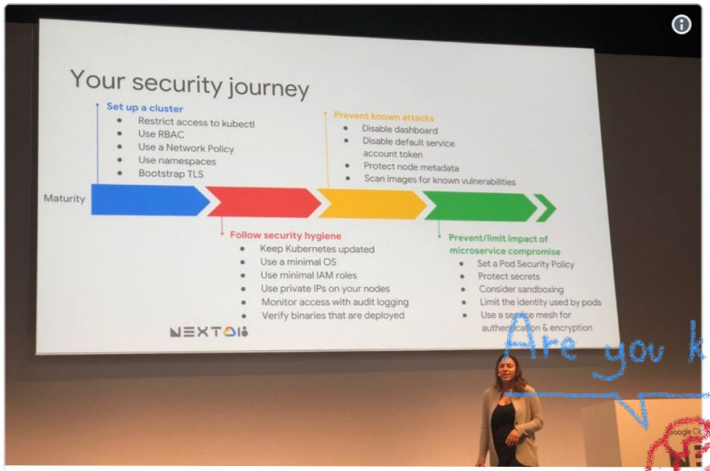
Network plugins (Flannel, Calico, Weave...)

- IPAM
- routing
- iptables
- crossnode networking

Cluster IP, NodePort, Ingress

Service Meshes, Istio

The security journey

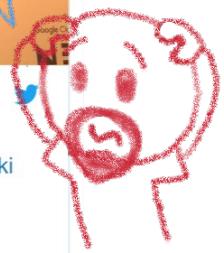


Mattias Gees
@MattiasGees

Your security journey with Kubernetes by @MayaKaczorowski #GoogleNext18

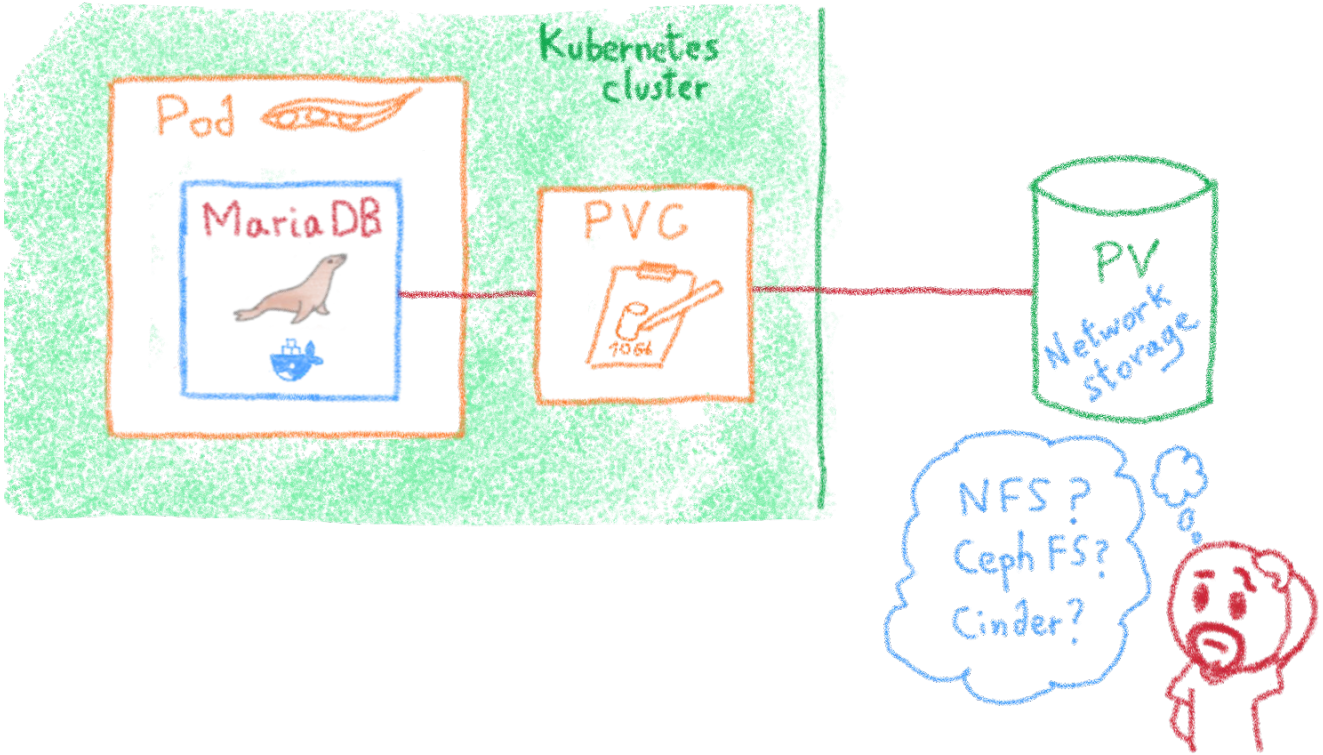
♡ 319 12:59 PM - Oct 11, 2018

Are you kidding me?

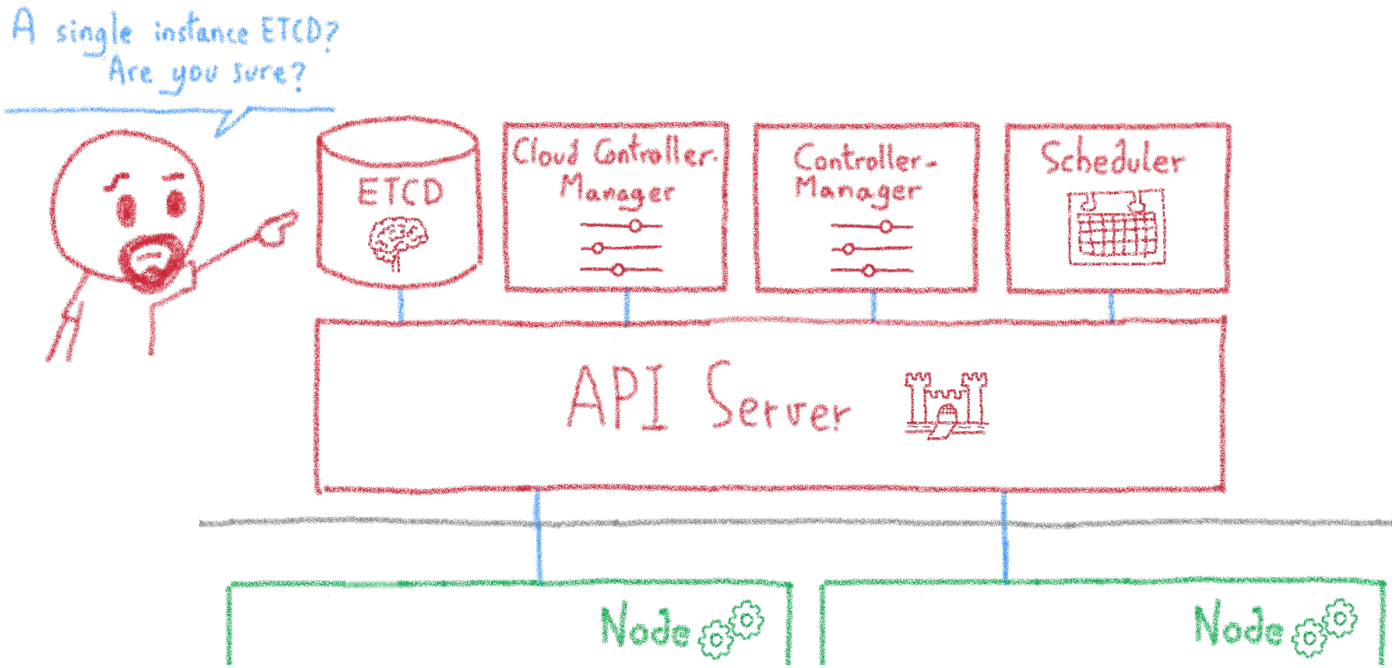


Open ports (e.g. etcd 2379/TCP)
Kubernetes API (e.g. Tesla hacking)
Exploits (lots of CVEs)
RBAC (e.g. badly defined roles)

The storage dilemma



The ETCD vulnerability



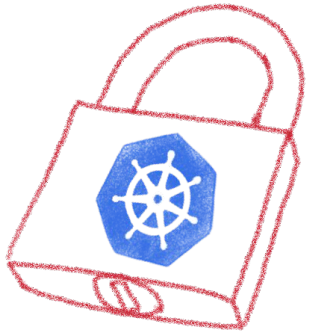
Describing some of those traps

To ease and empower your path to production

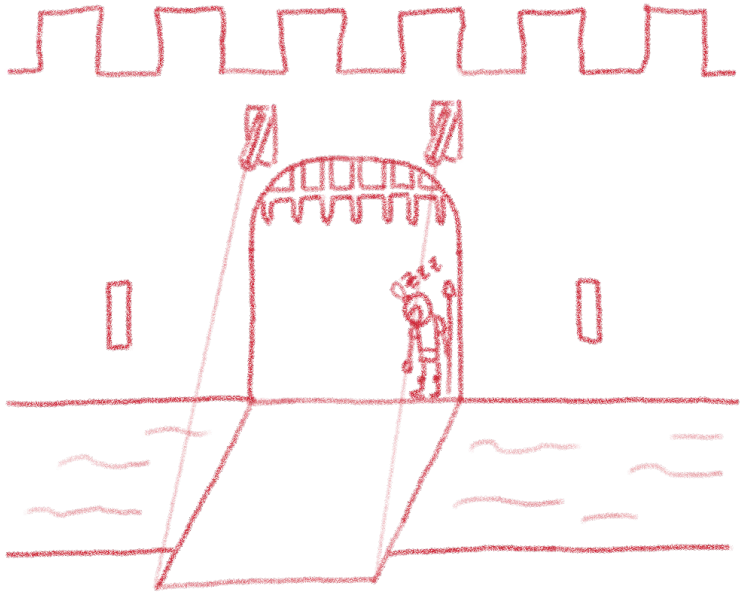
DEVOXX™

Security

Hardening your Kubernetes



Kubernetes is insecure by design

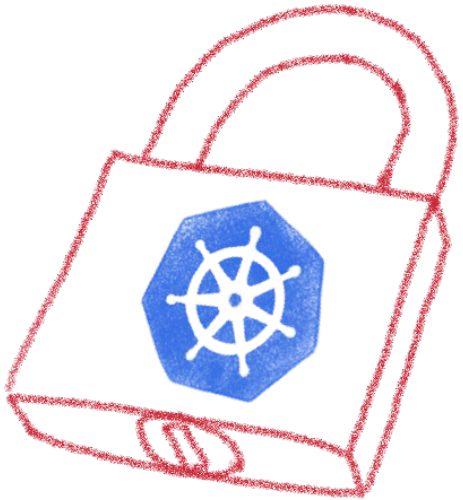


It's a feature, not a bug

It's up to the K8s admin to secure it according to their needs

Not everybody has the same security needs

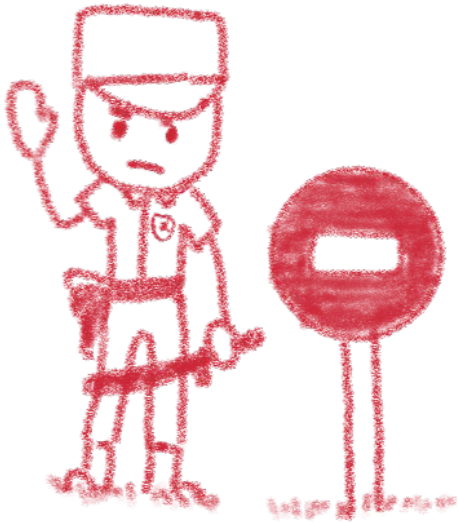
Kubernetes allows to enforce security practices as needed



Listing some good practices

- Close open access
- Define and implement RBAC
- Define and implement Network Policies
- Isolate sensitive workloads

Close open access

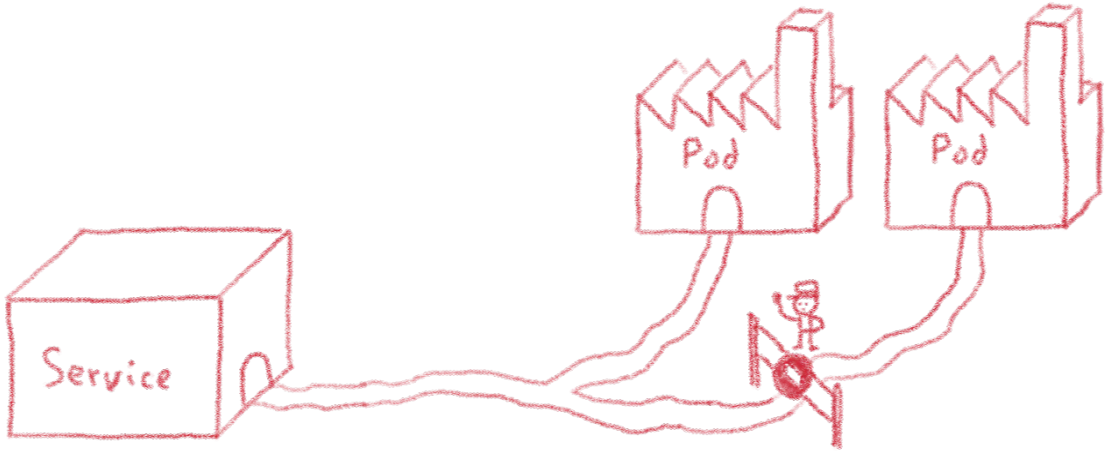


Close all by default, open only the needed ports
Follow the least privileged principle

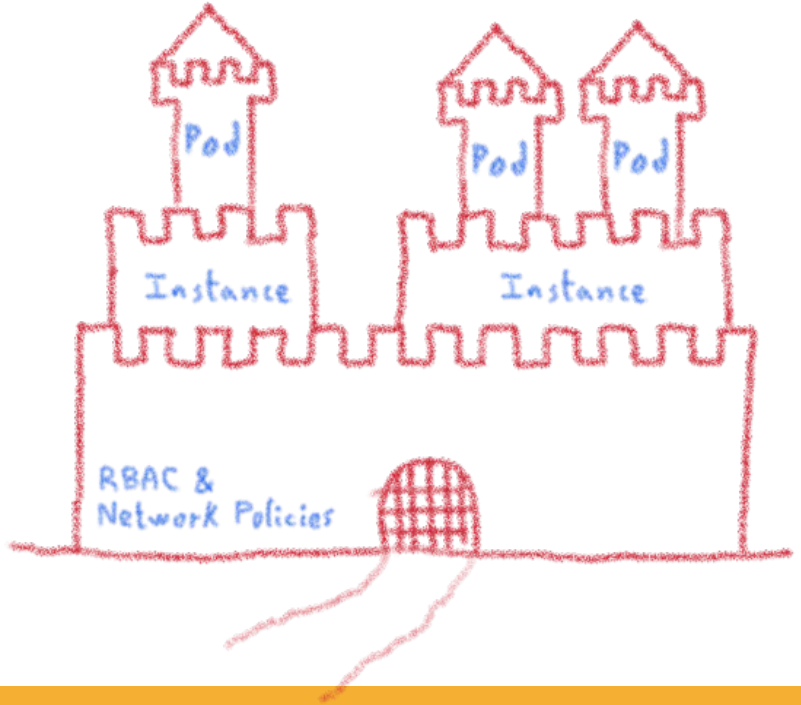
Define and implement RBAC

According to your needs

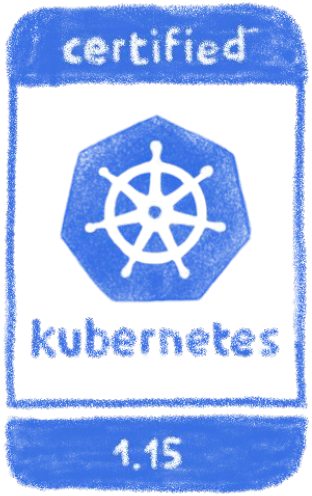
Define and implement network policies



Use RBAC and Network Policies to isolate your sensitive workload



Always keep up to date



Both Kubernetes and plugins

And remember, even the best can get hacked

One of Tesla's cluster got hacked
via an unprotected K8s API endpoint,
and was used to mine cryptocurrency...

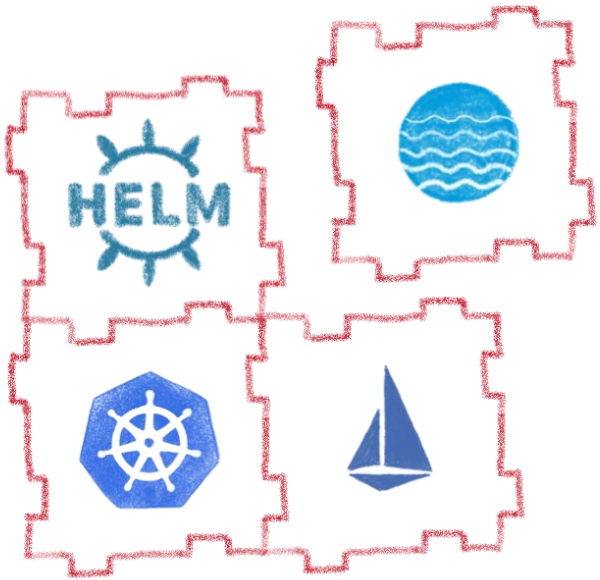
Remain attentive, don't get too confident

DEVOXX™

Extensibility

Enhance your Kubernetes

Kubernetes is modular



Fully extensible

- Kubernetes API
- Cluster demons
- Controllers
- Custom resources
- ...

Operators

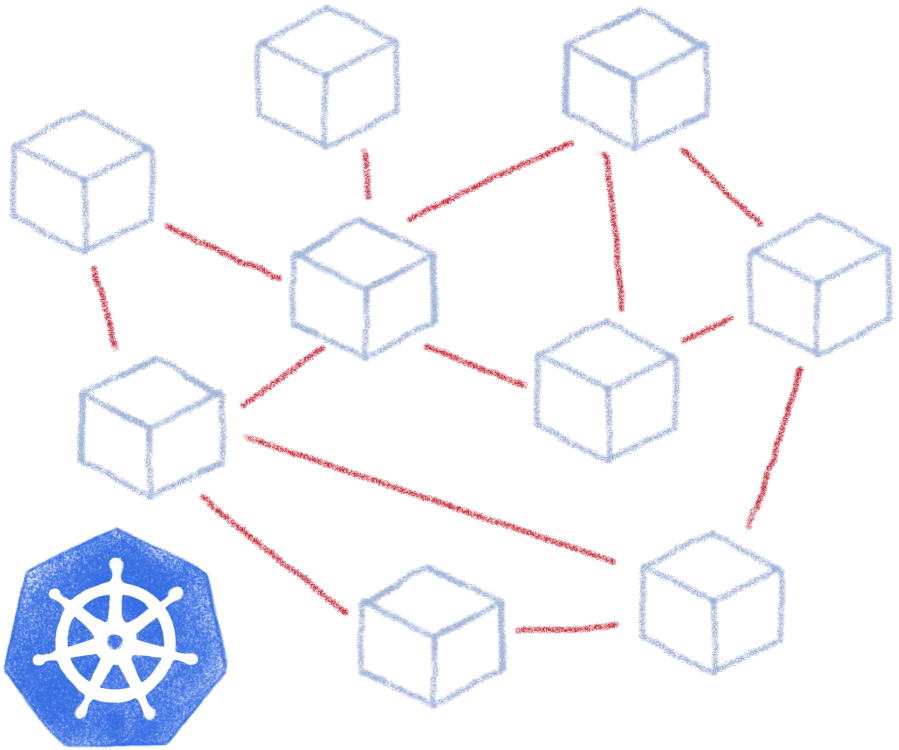
Let's see how some of those plugins can help you

DEVOXX™

Helm

A package management for K8s

Complex deployments



Ingress

Services

Deployments

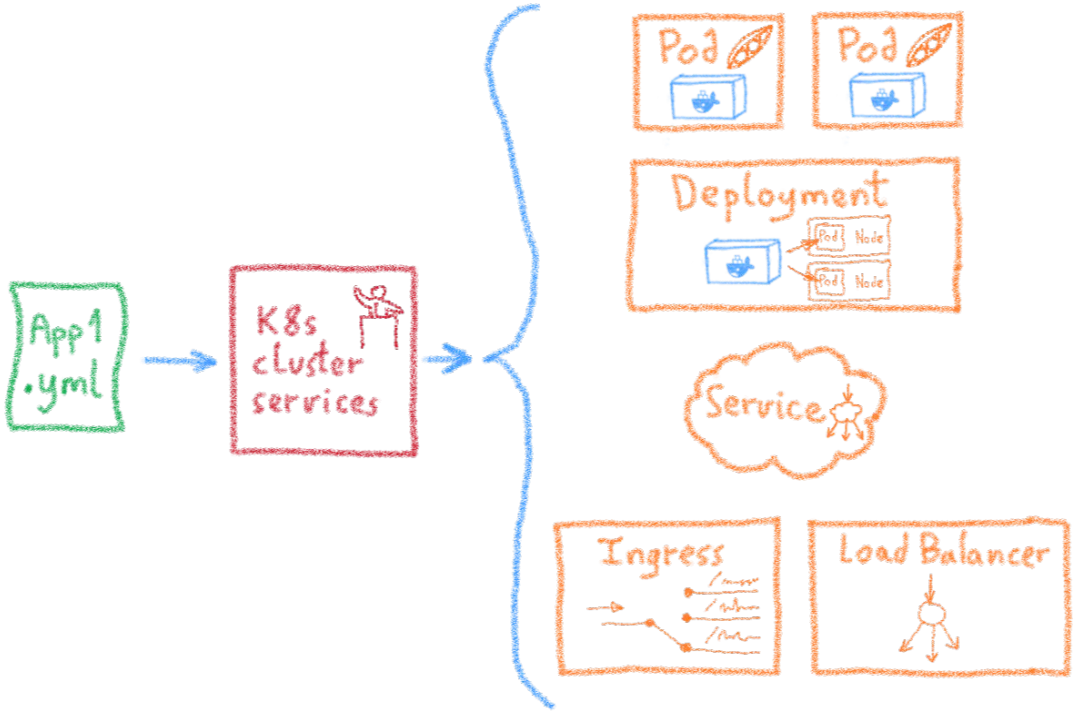
Pods

Sidecars

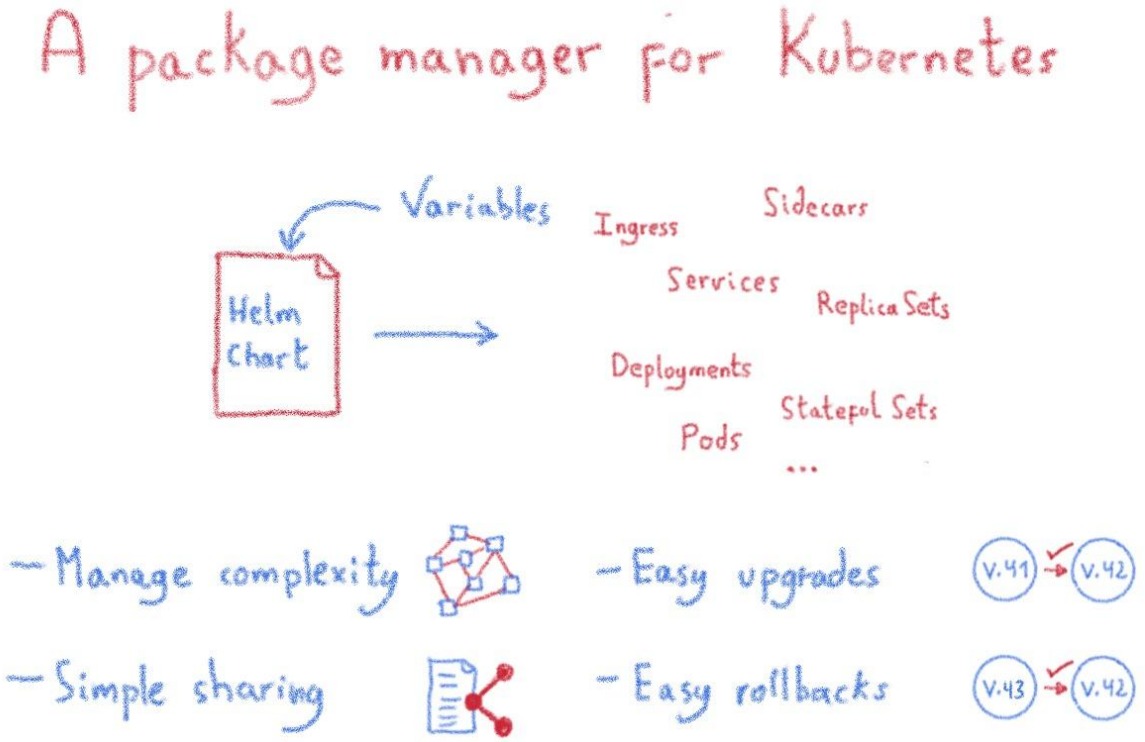
Replica Sets

Statepul Sets

Using static YAML files



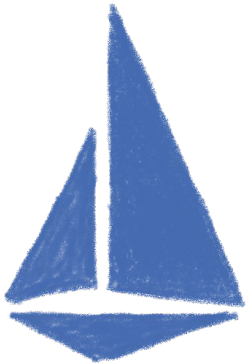
Complex deployments



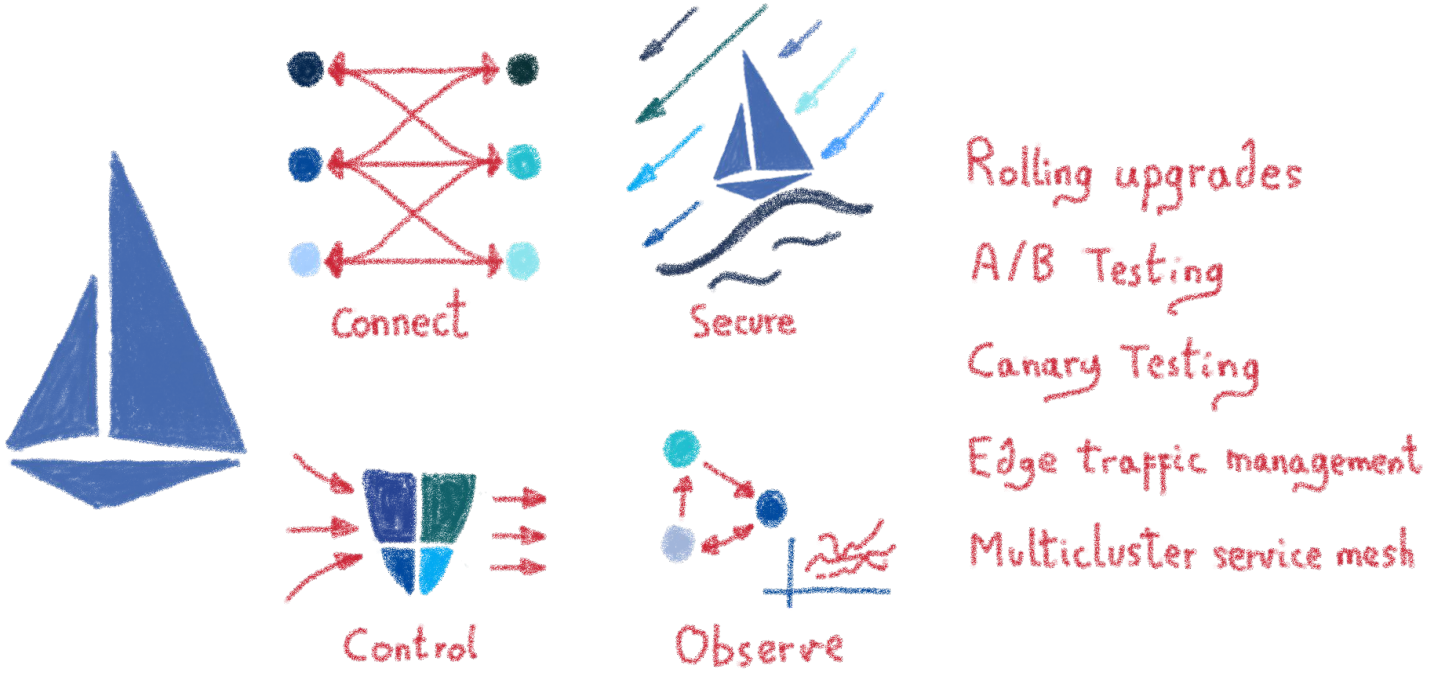
DEVOXX™

Istio

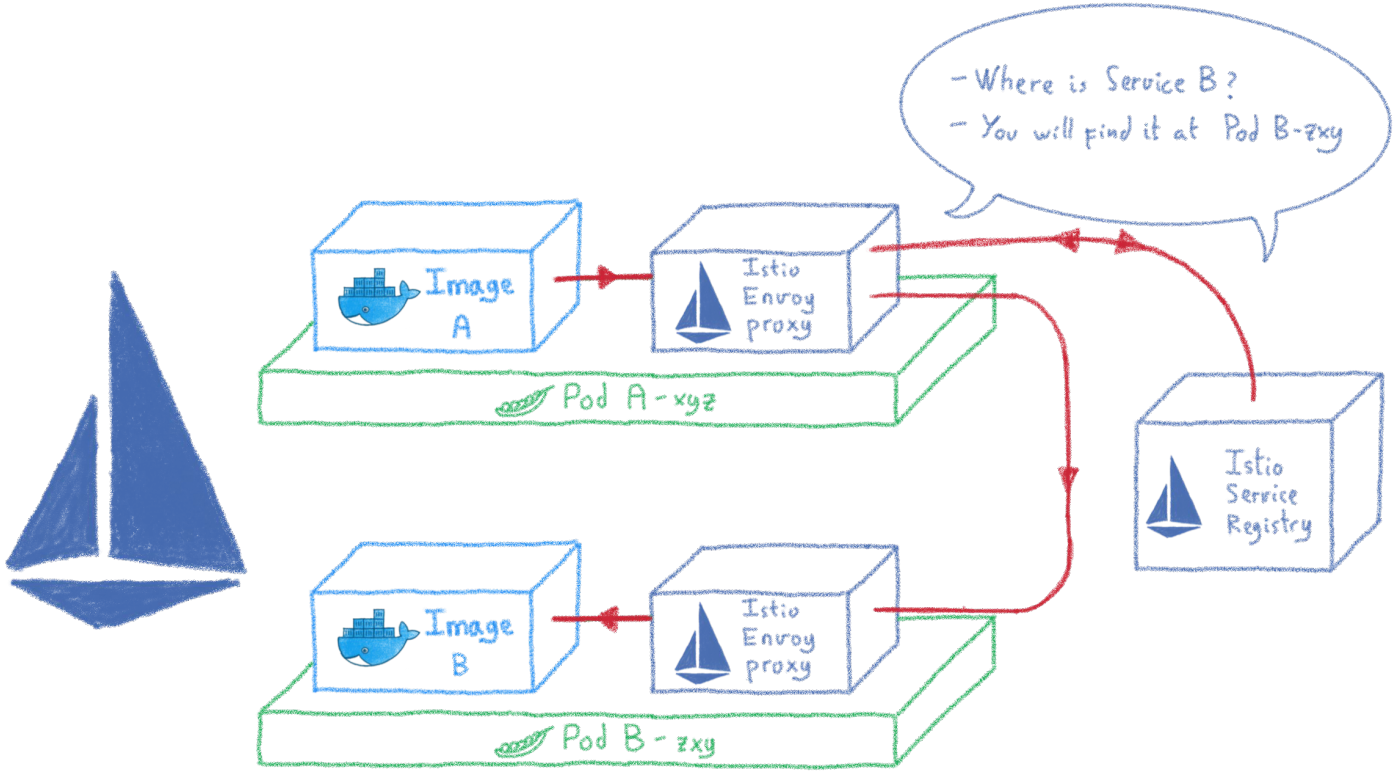
A service mesh for Kubernetes...
and much more!



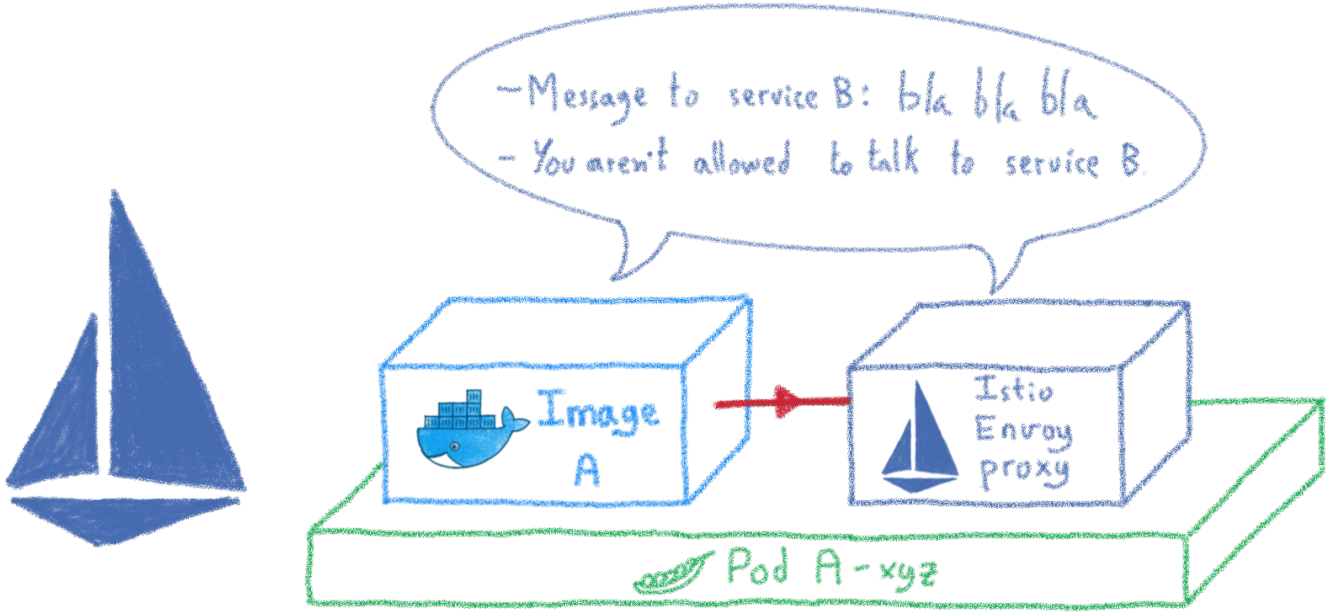
Istio: A service mesh but not only



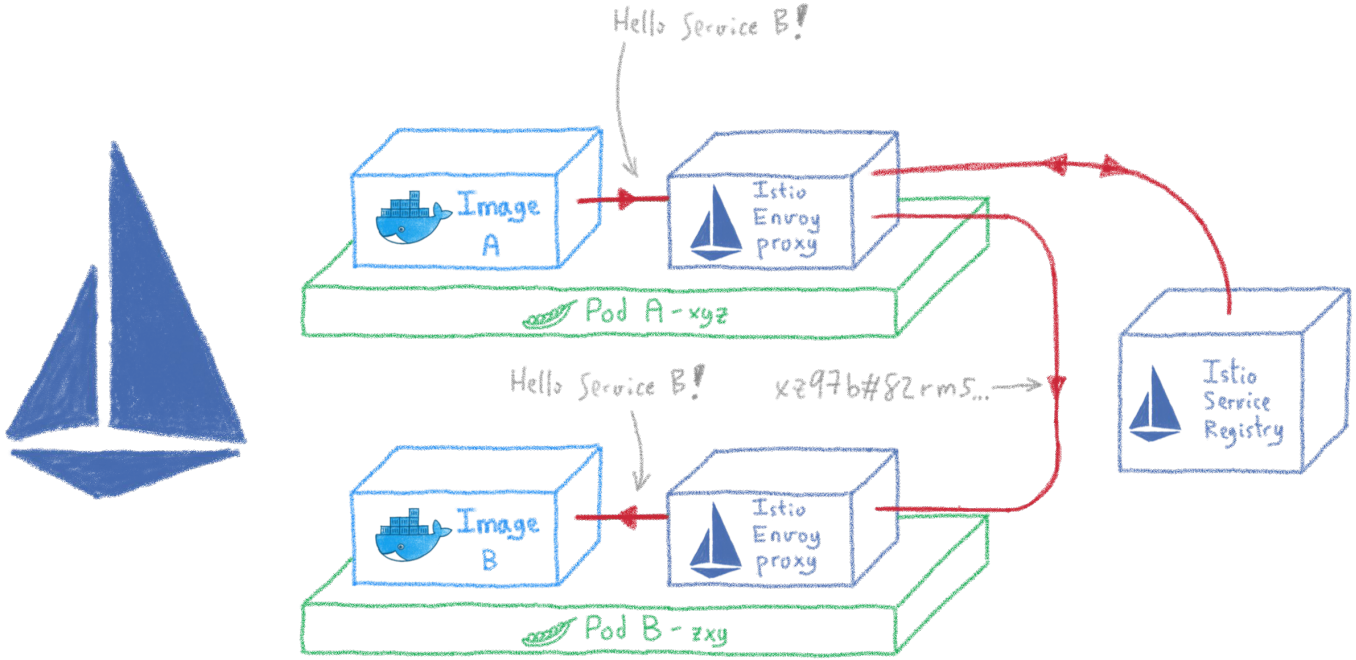
Service discovery



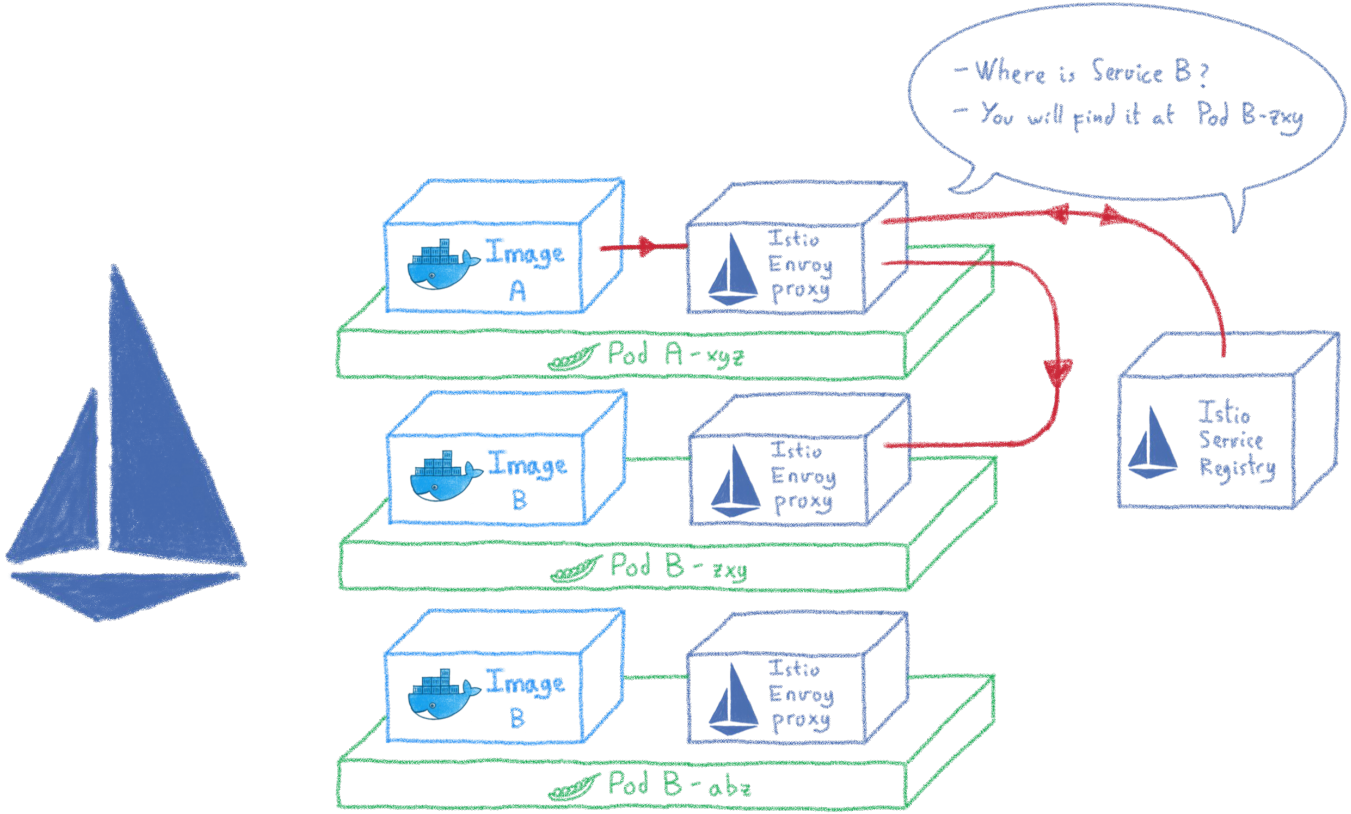
Traffic control



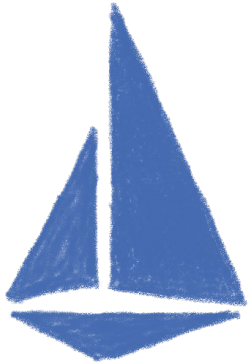
Encrypting internal communications

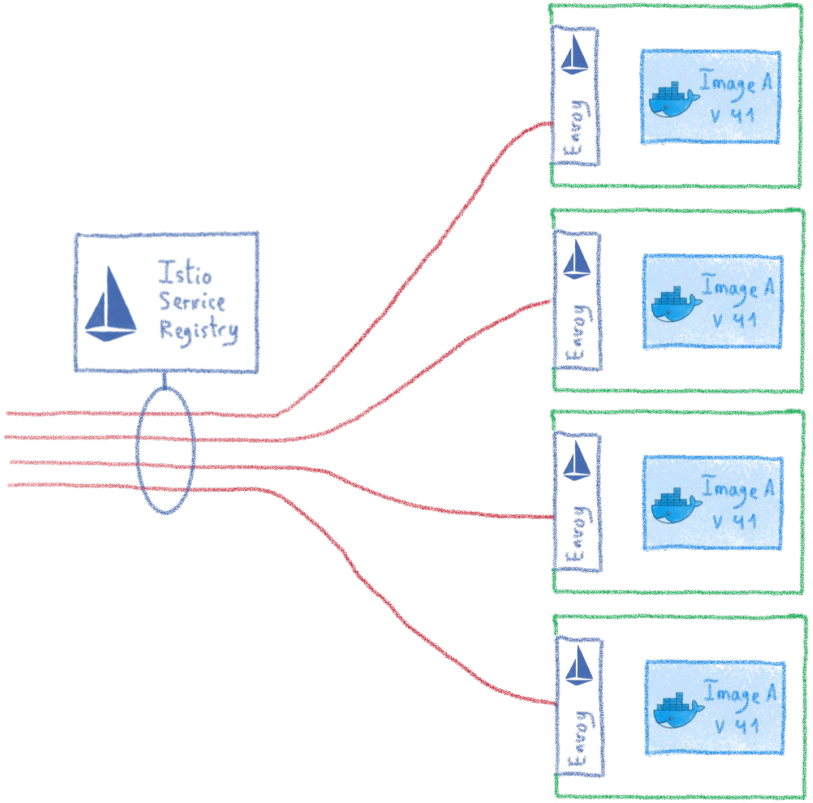


Routing and load balancing

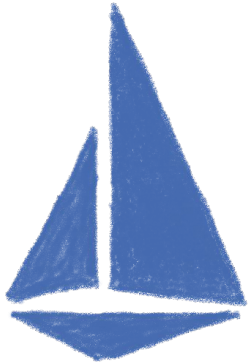


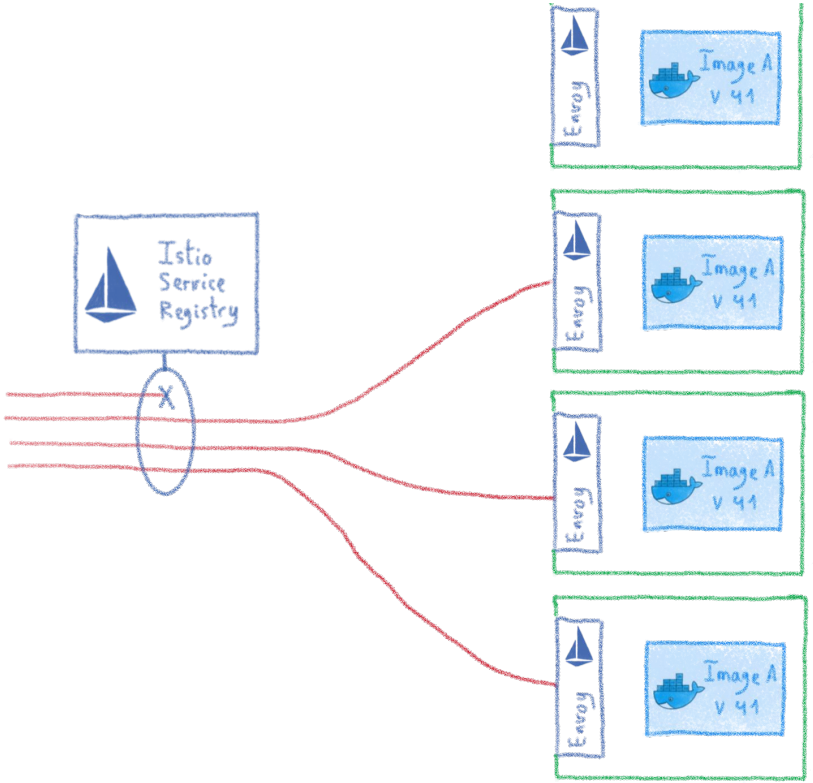
Rolling upgrades



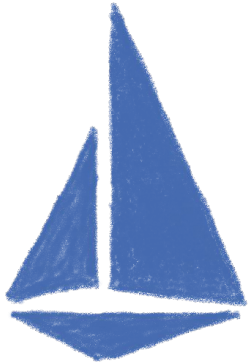


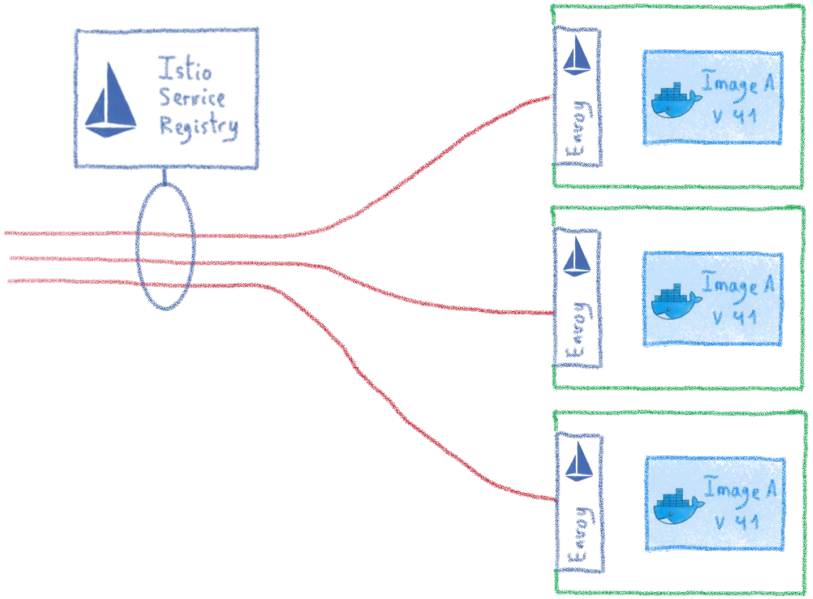
Rolling upgrades



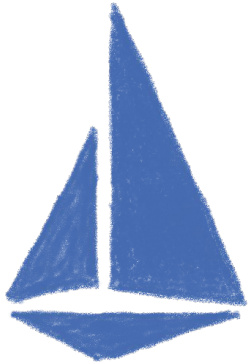


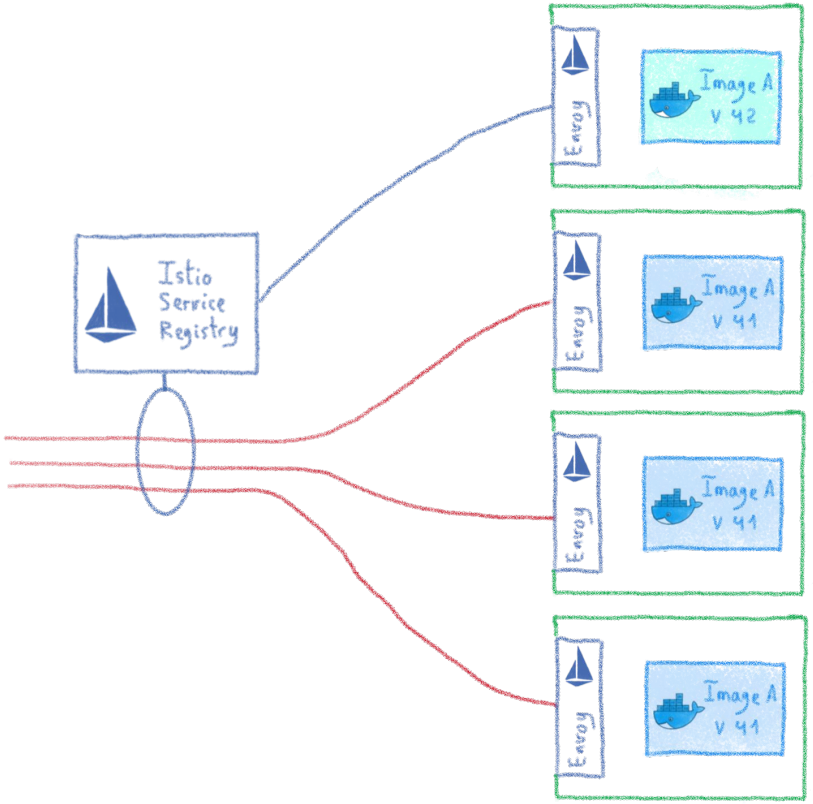
Rolling upgrades



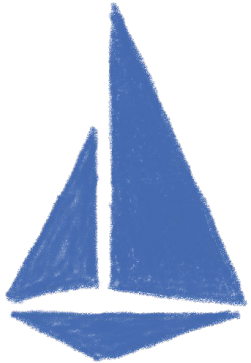


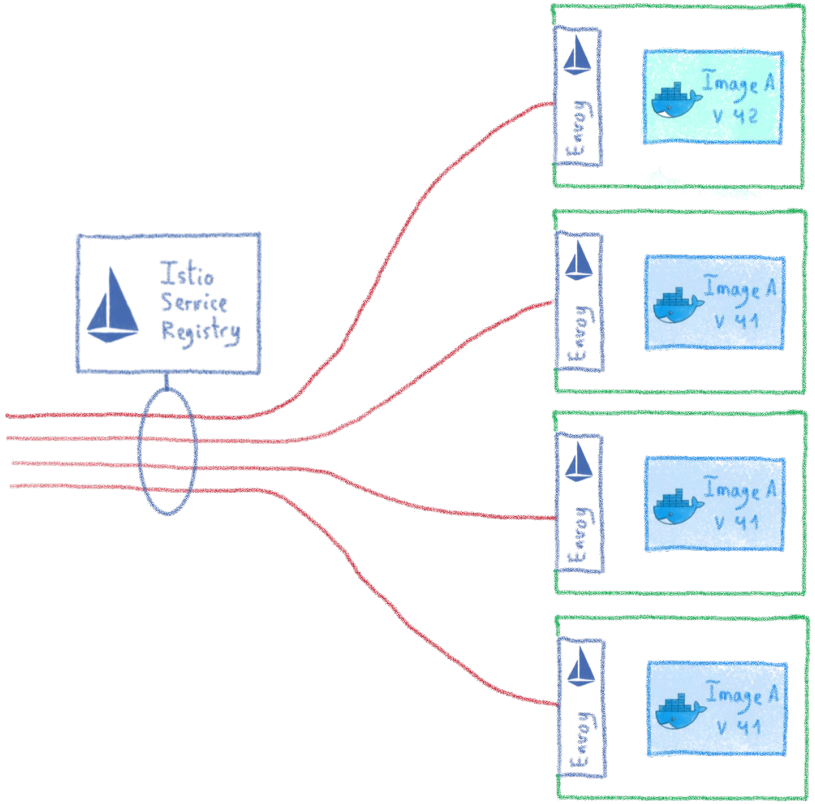
Rolling upgrades



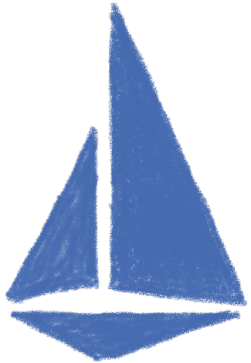


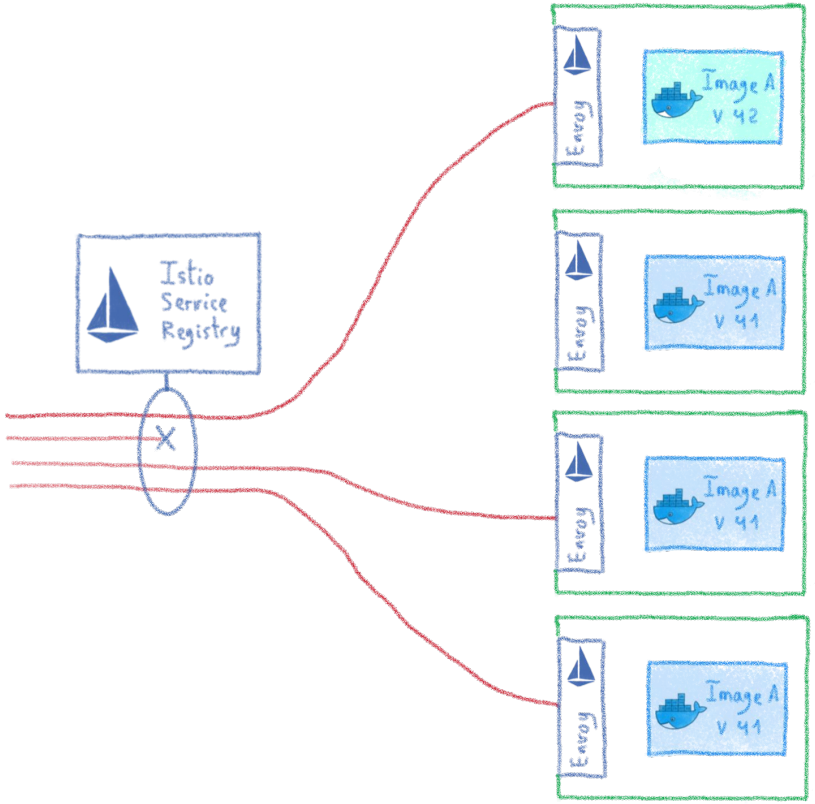
Rolling upgrades



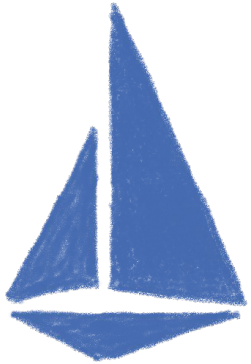


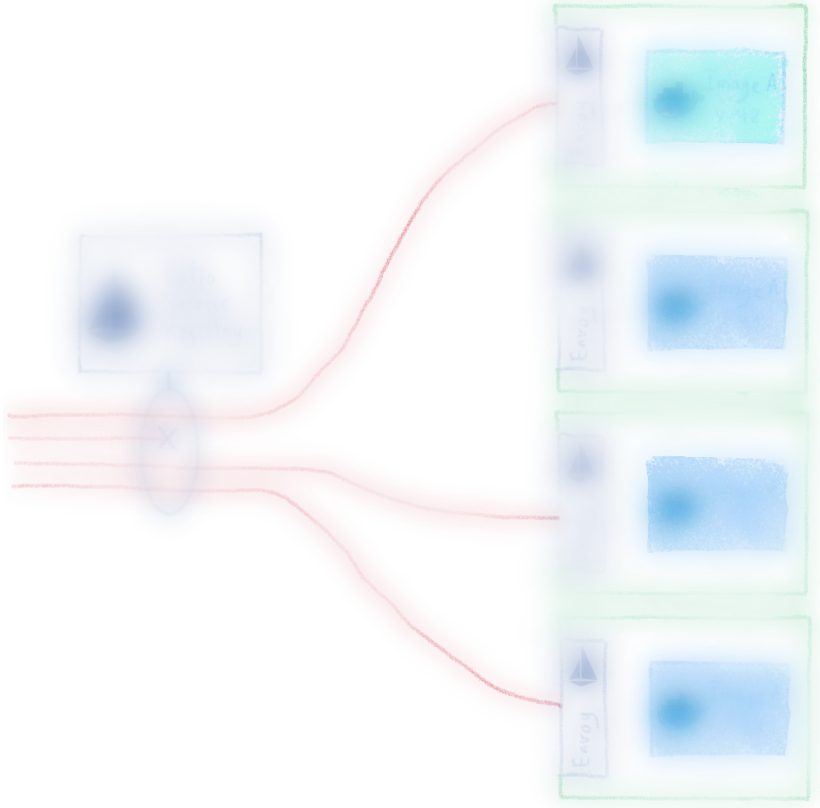
Rolling upgrades



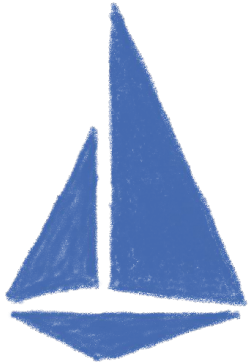


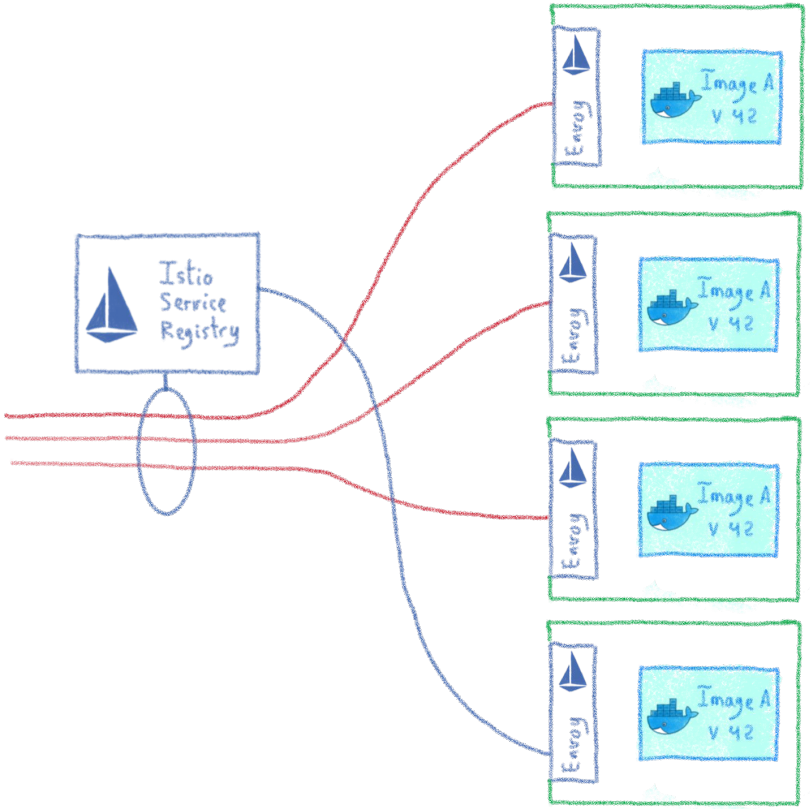
Rolling upgrades



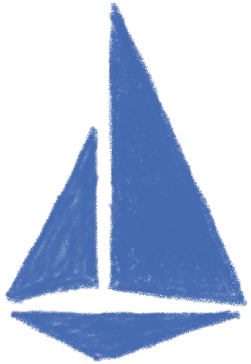


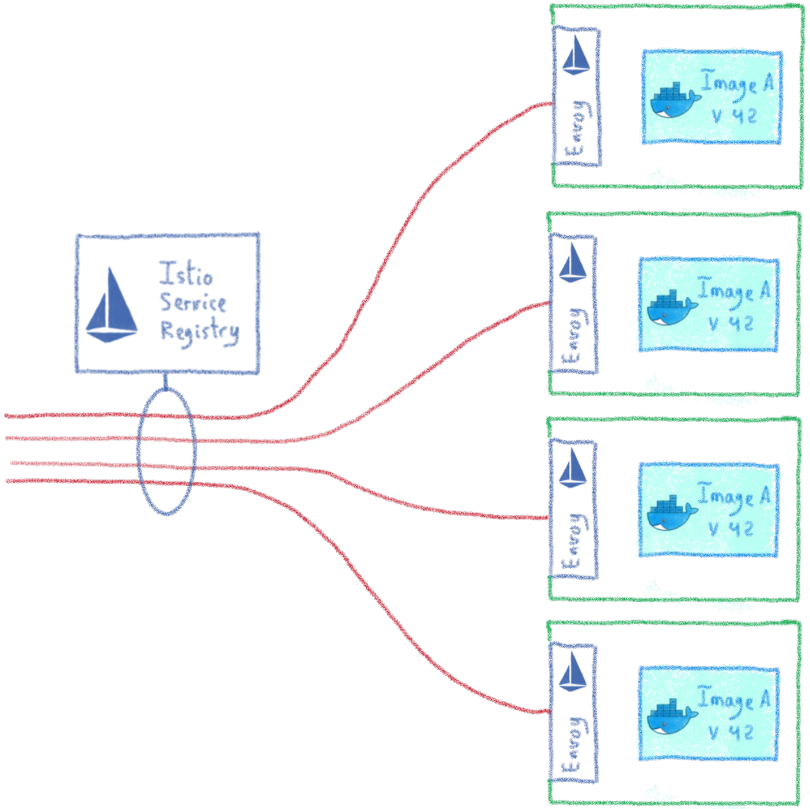
Rolling upgrades



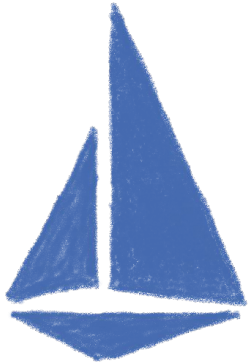


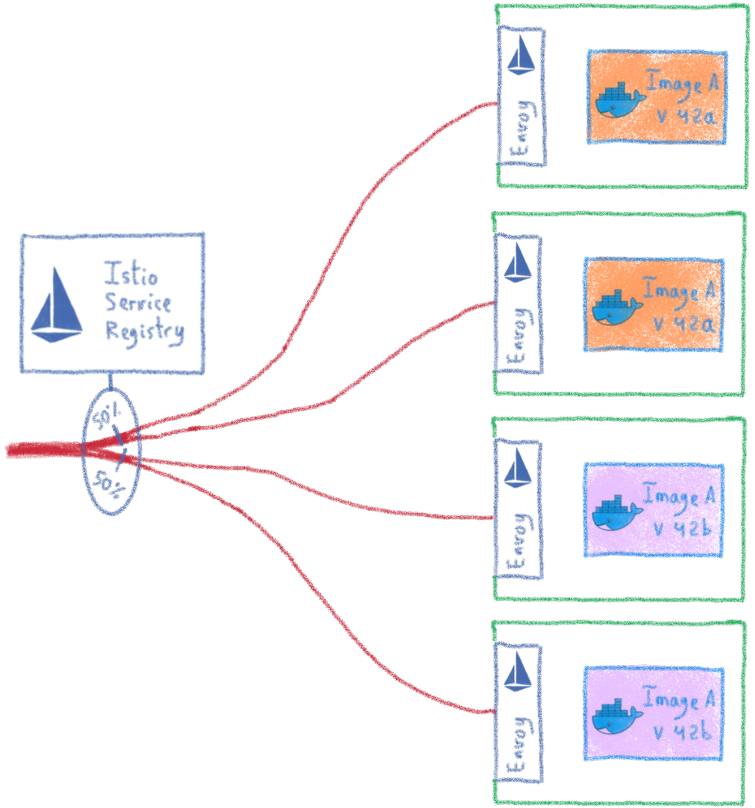
Rolling upgrades



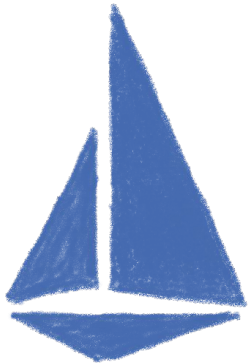


A/B testing




Istio
Service
Registry
50%
50%
Envoy
Image A
v 42a
Envoy
Image A
v 42a
Envoy
Image A
v 42b
Envoy
Image A
v 42b

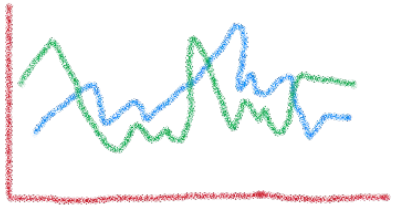
Monitoring your cluster



- Metrics
- Logs
- Tracing

} at {

- Envoy level
- Control plane level



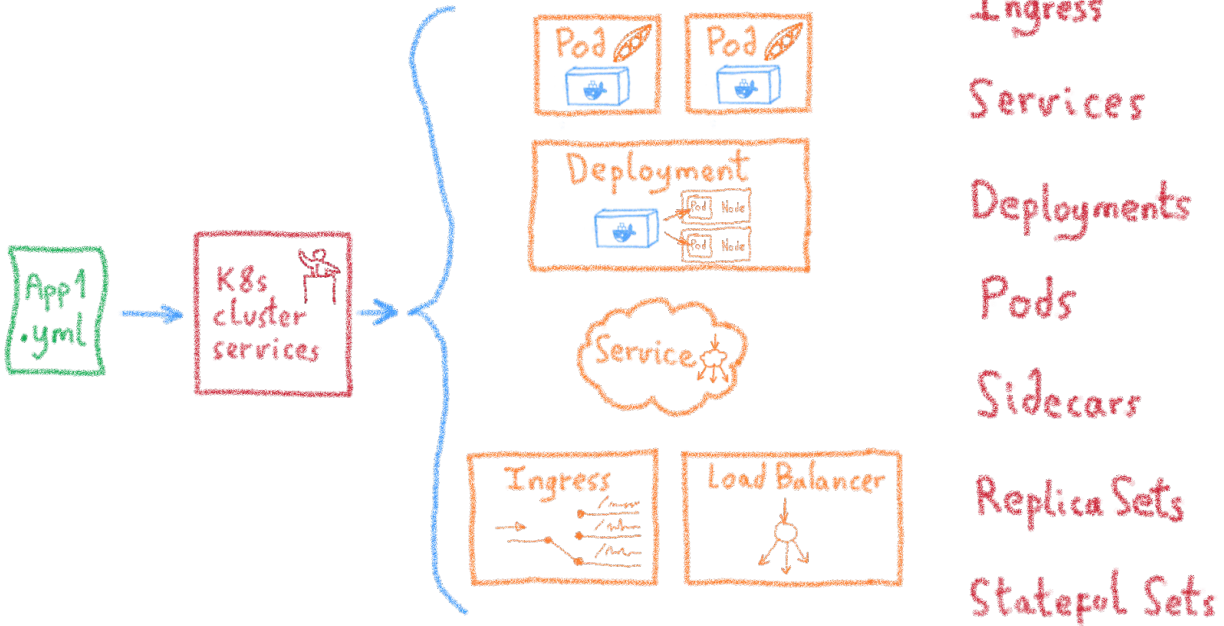
Dashboards

DEVOXX™

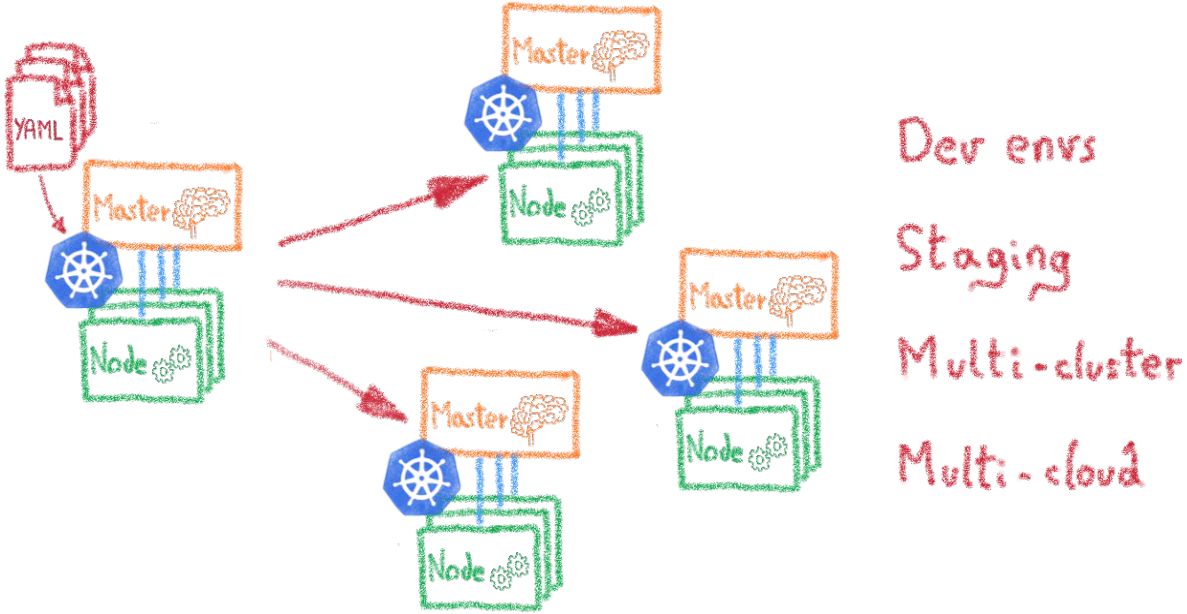
Velero

Backing up your Kubernetes

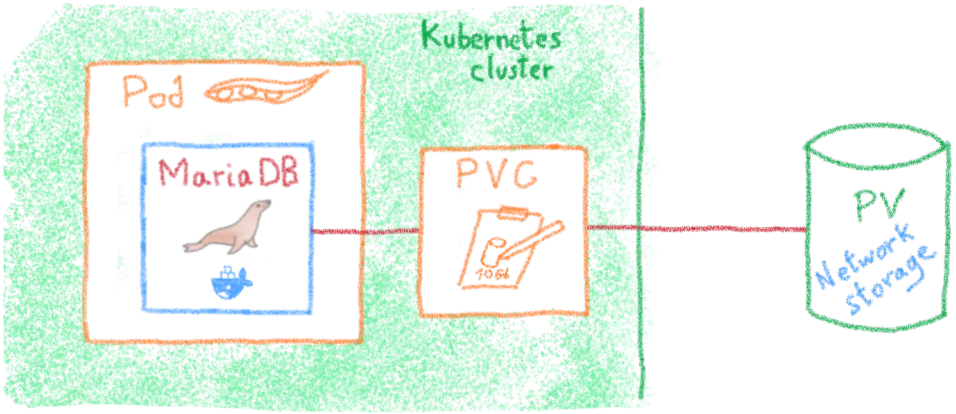
Kubernetes: Desired State Management



YAML files allows to clone a cluster



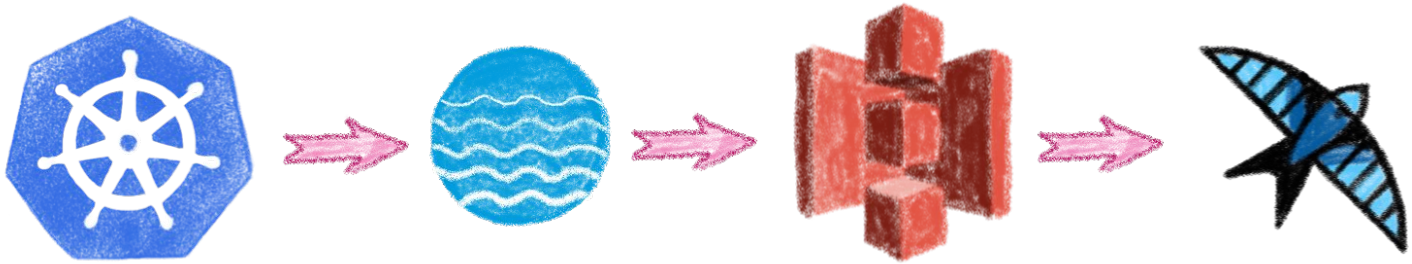
But what about the data?



Velero

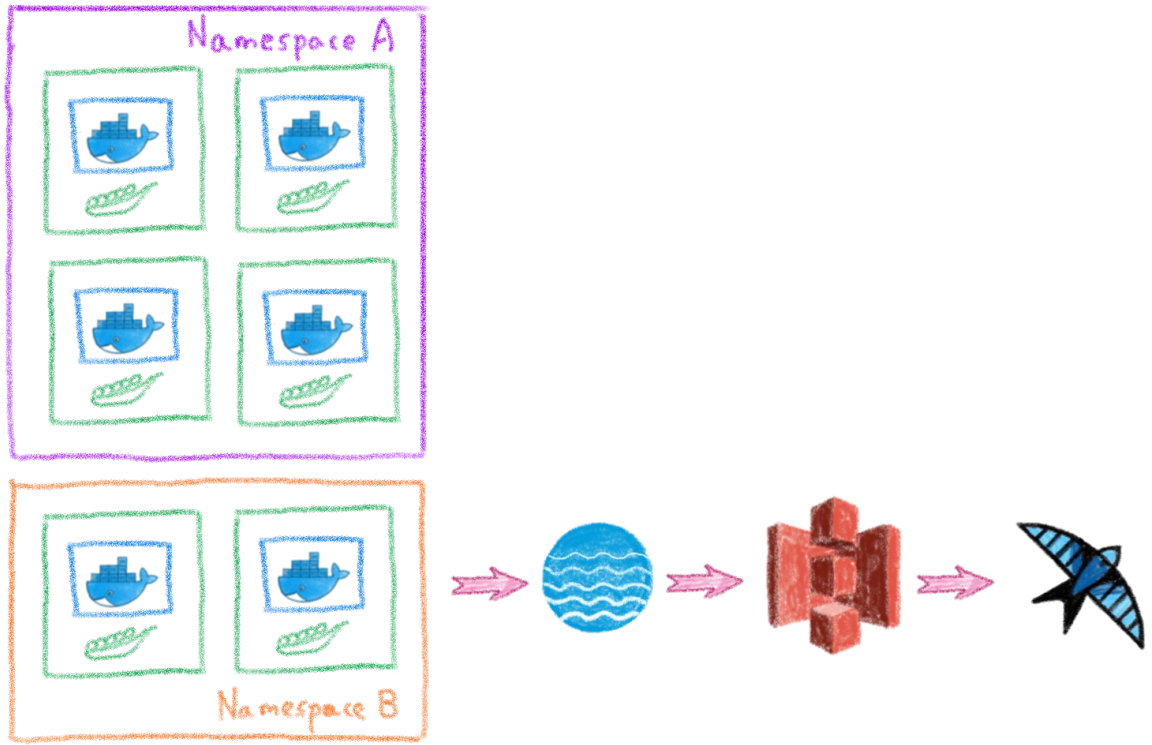
Backup and migrate Kubernetes applications
and their persistent volumes

S3 based backup

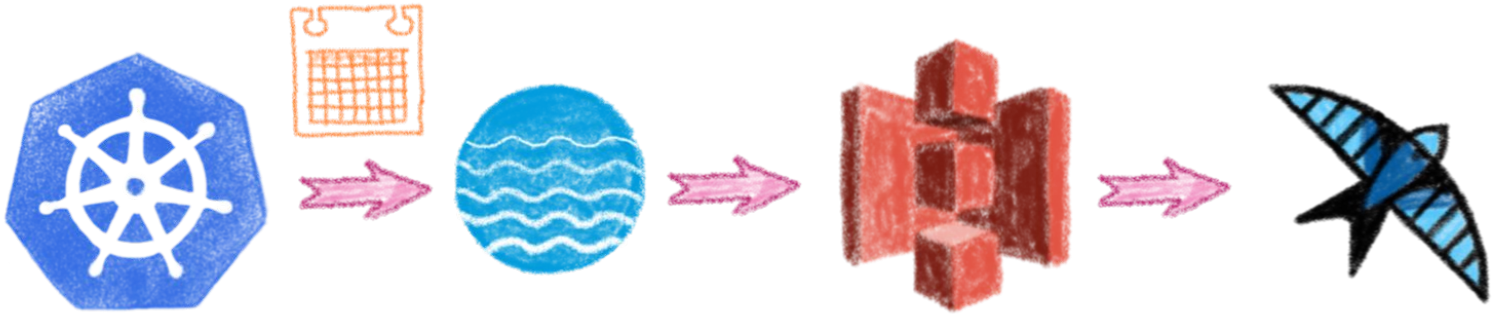


On any S3 protocol compatible store

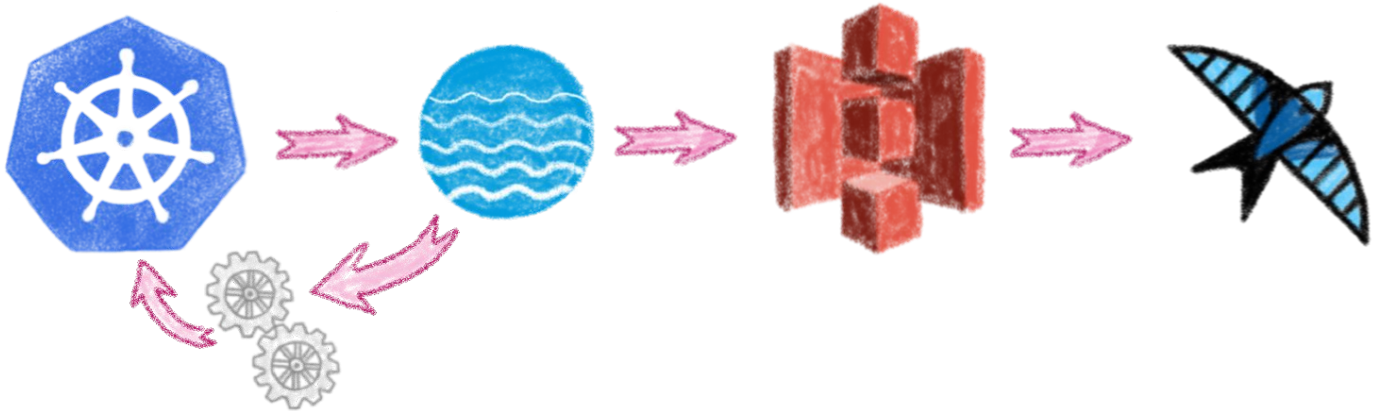
Backup all or part of a cluster



Schedule backups



Backups hooks

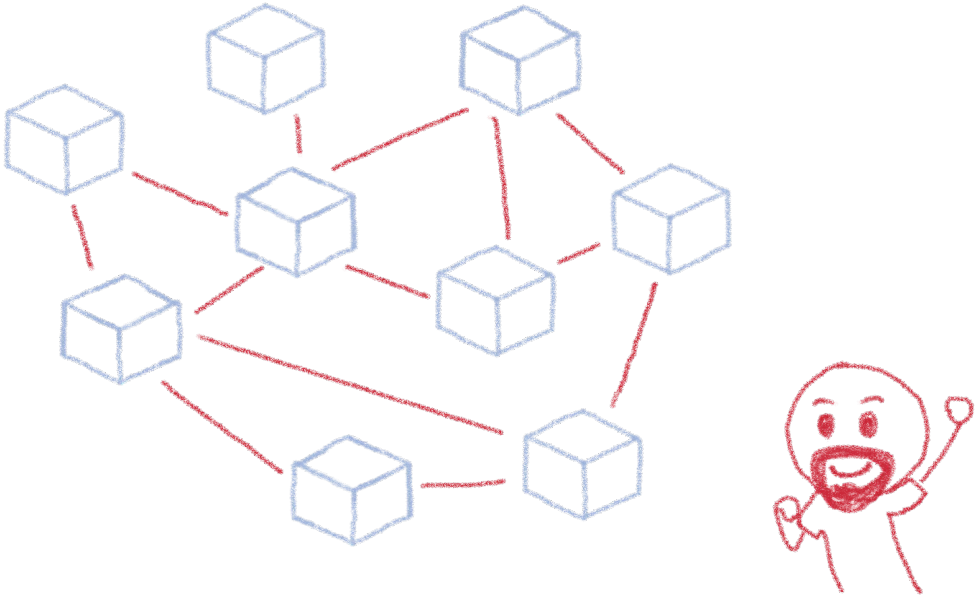


DEVOXX™

Conclusion

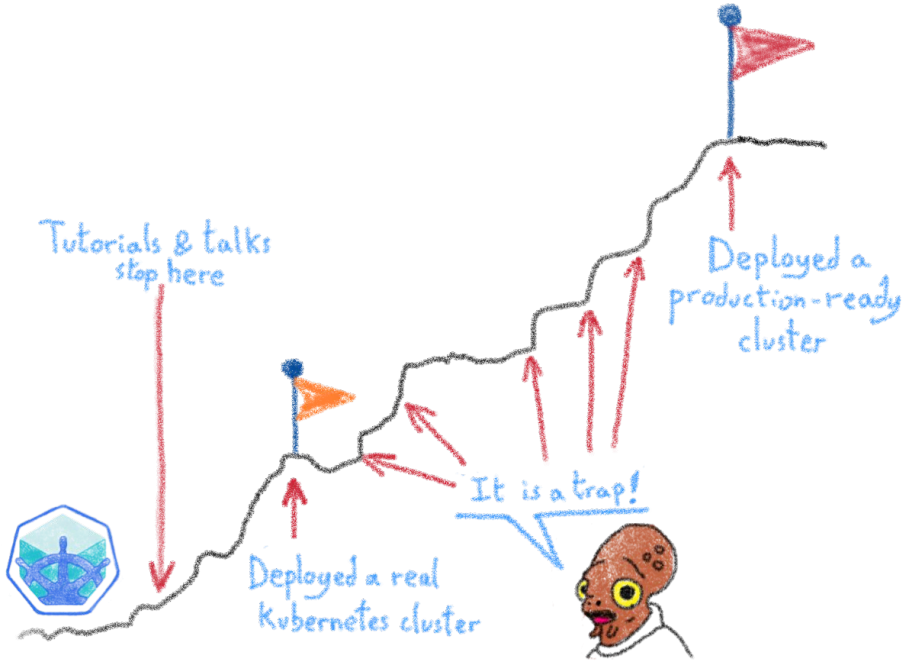
And one more thing...

Kubernetes is powerful



It can make Developers' and DevOps' lives easier

But there is a price: operating it

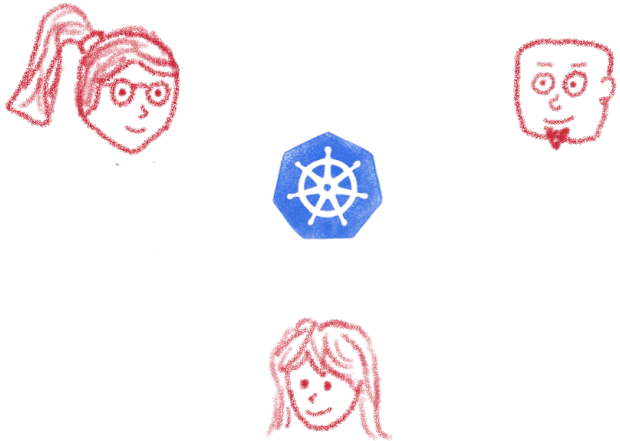


Lot of things to think about

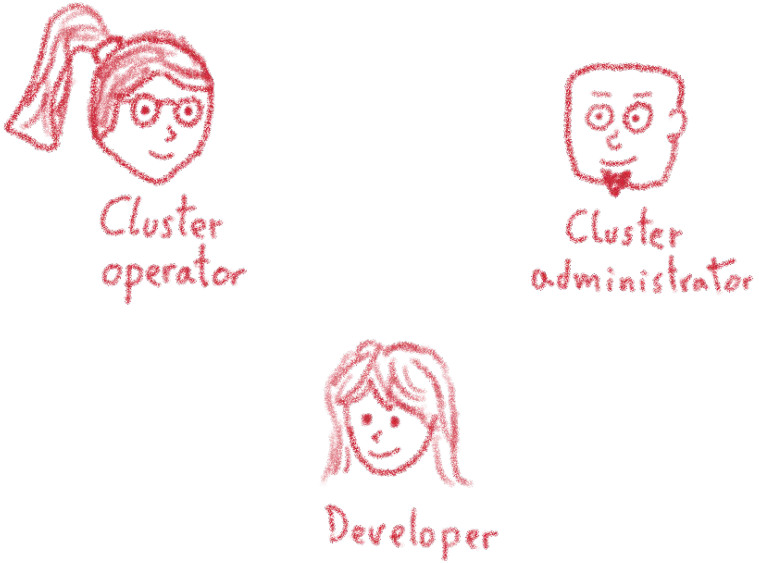
We have seen some of them

One more thing...

Who should do what?

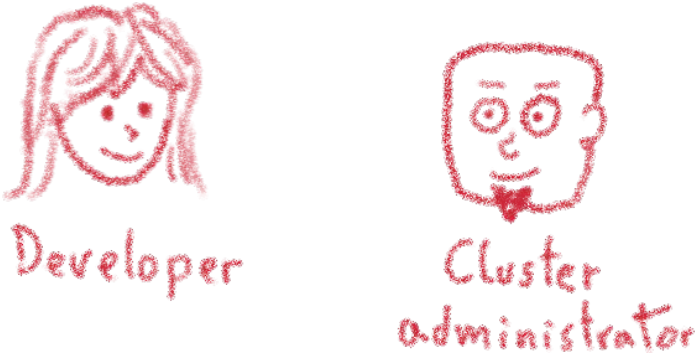


Different roles



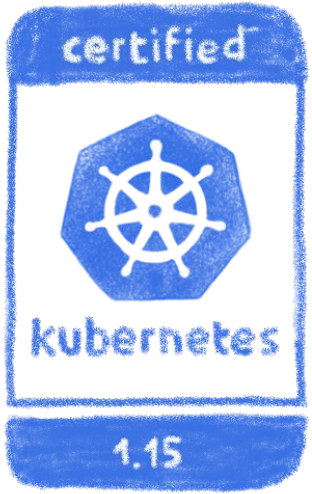
Each role asks for very different knowledge and skill sets

Most companies don't need to operate the clusters



As they don't build and rack their own servers!

If you don't need to build it, choose a certified managed solution

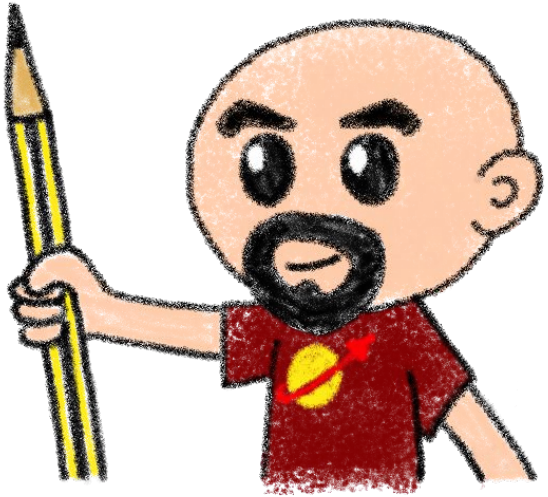


You get the cluster, the operator
get the problems

Like our OVH Managed Kubernetes

Made with ❤ by the Platform team

Do you want to try?



Send me an email to get some vouchers...

horacio.gonzalez@corp.ovh.com

Thank you for listening

That's all, folks!