Kubernetes: beyond Minikube

Horacio Gonzalez

@LostInBrittany

OVH

openexpo europe

Horacio Gonzalez

@LostInBrittany

Spaniard lost in Brittany, developer, dreamer and all-around geek

DevFest du Bout du Monde

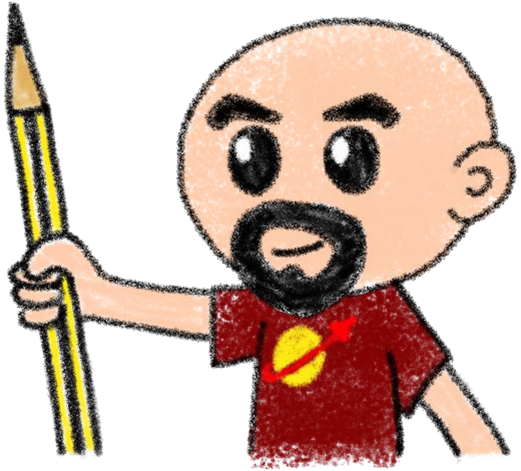
Finist Devs

Google Developers Experts 2019

Web Technologies GDE

OVH

Team DevRel



Summary

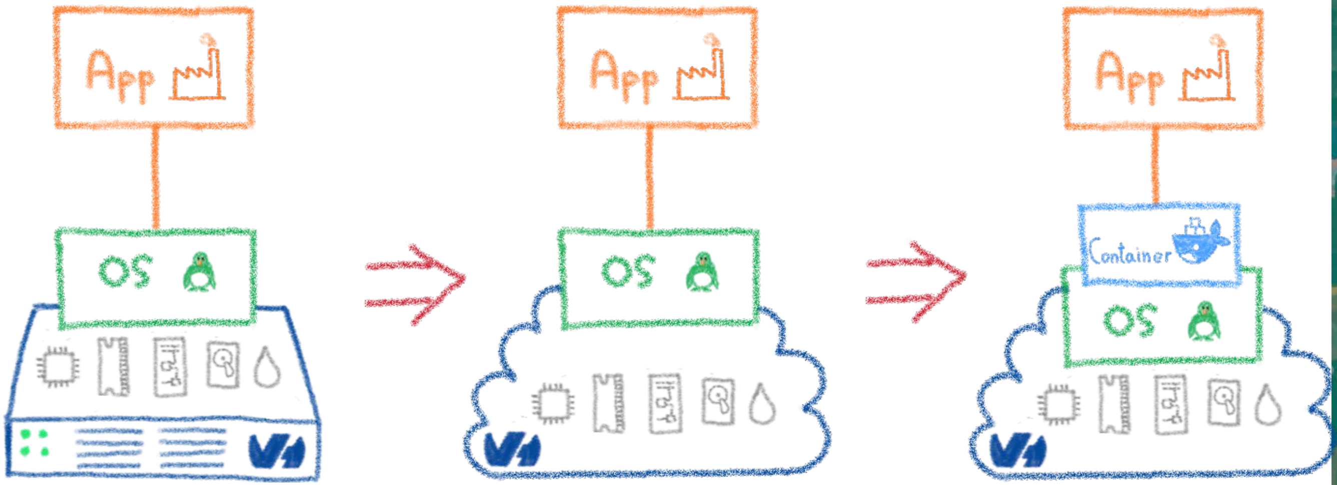
What I would like to speak about:

- Orchestrating containers
- Kubernetes: some concepts
- I have deployed on Minikube, woah!
- From Minikube to prod
- Building a managed Kubernetes service

Orchestrating containers

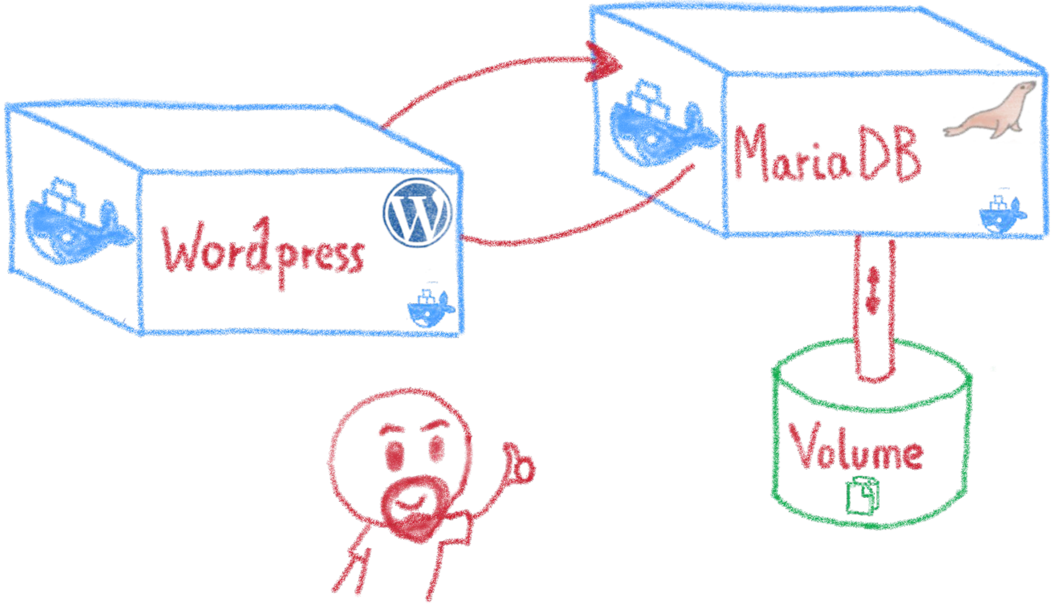
Like herding cats... but in hard mode!

From bare metal to containers



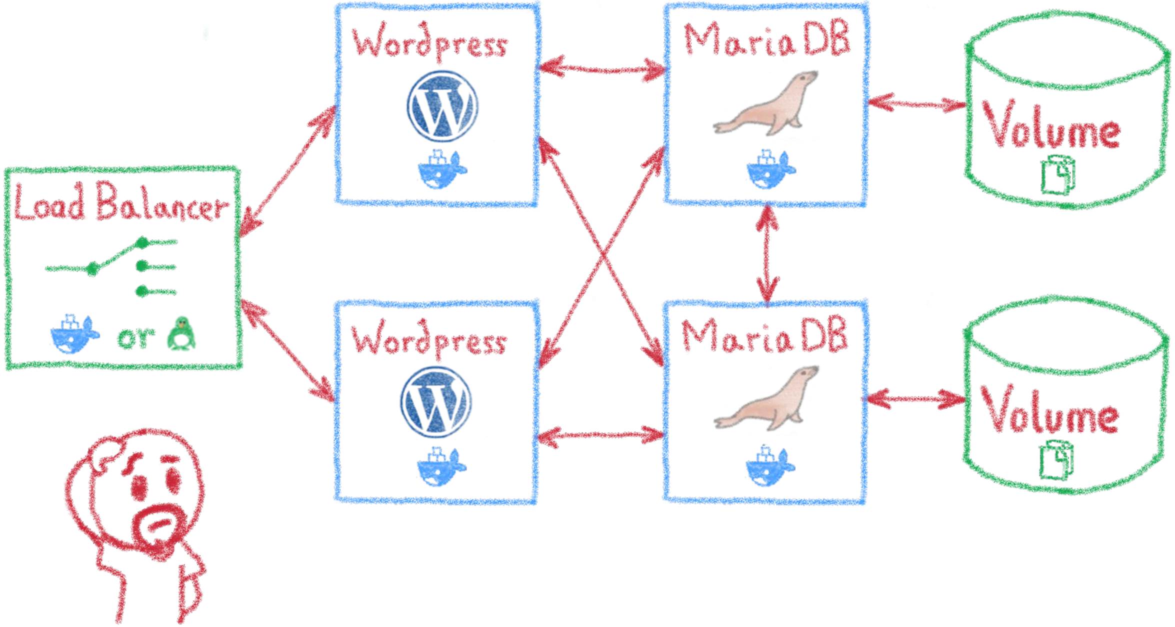
Another paradigm shift

Containers are easy…



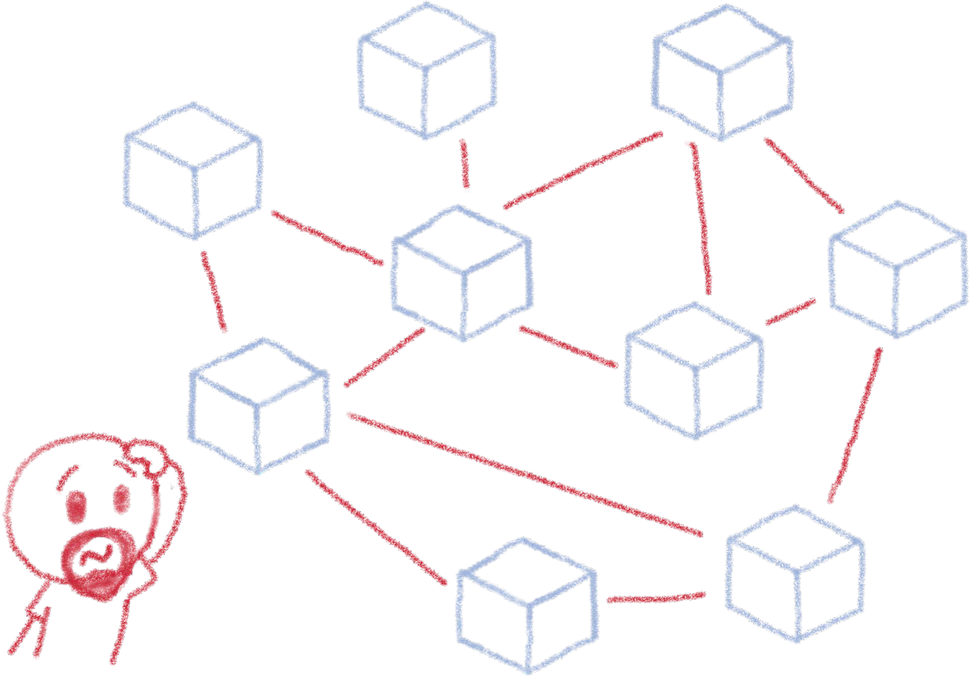
For developers

Less simple if you must operate them



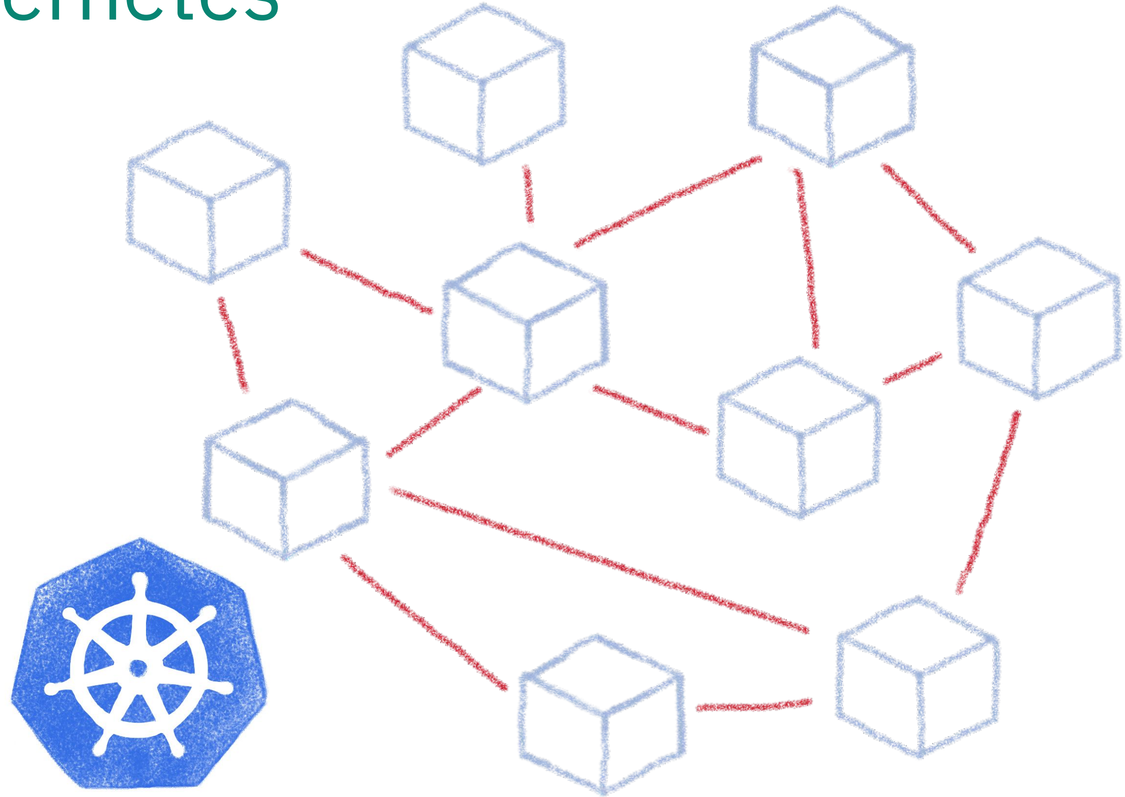
Like in a production context

And what about microservices?



Are you sure you want to operate them by hand?

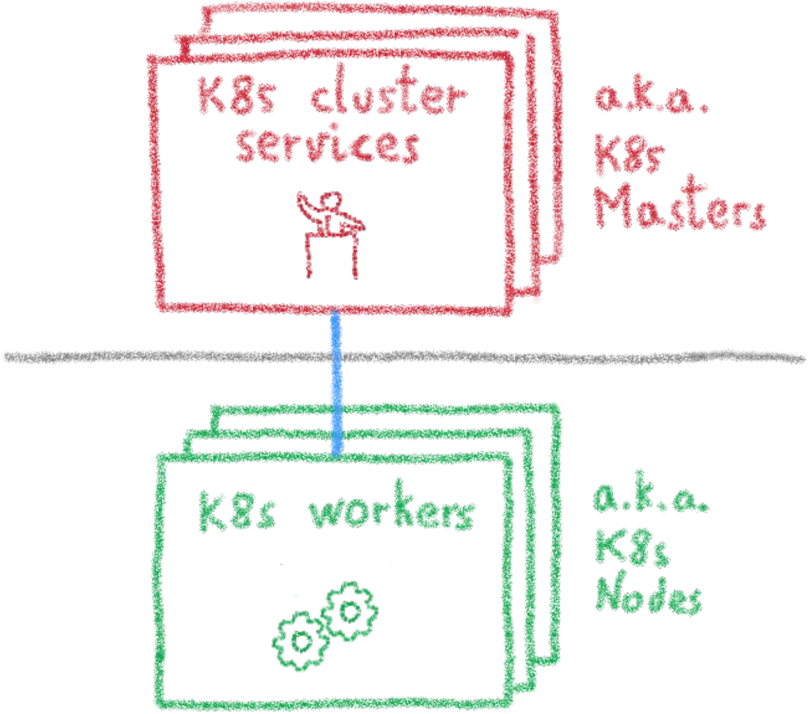
Taming microservices with Kubernetes



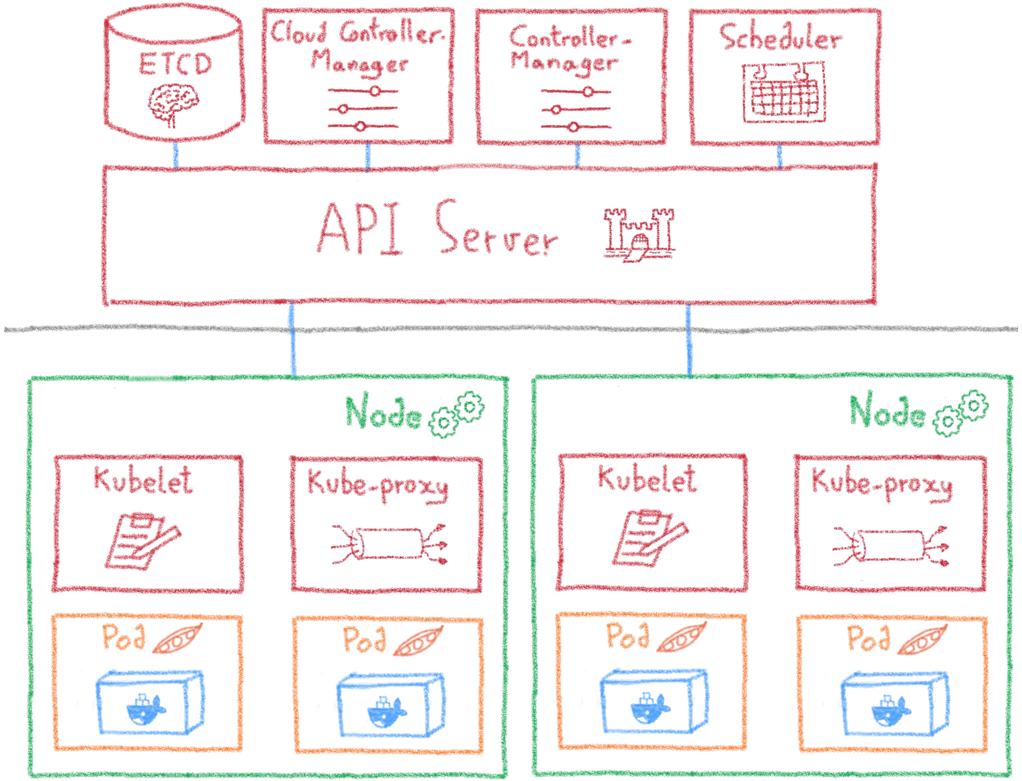
Kubernetes

Way more than a buzzword!

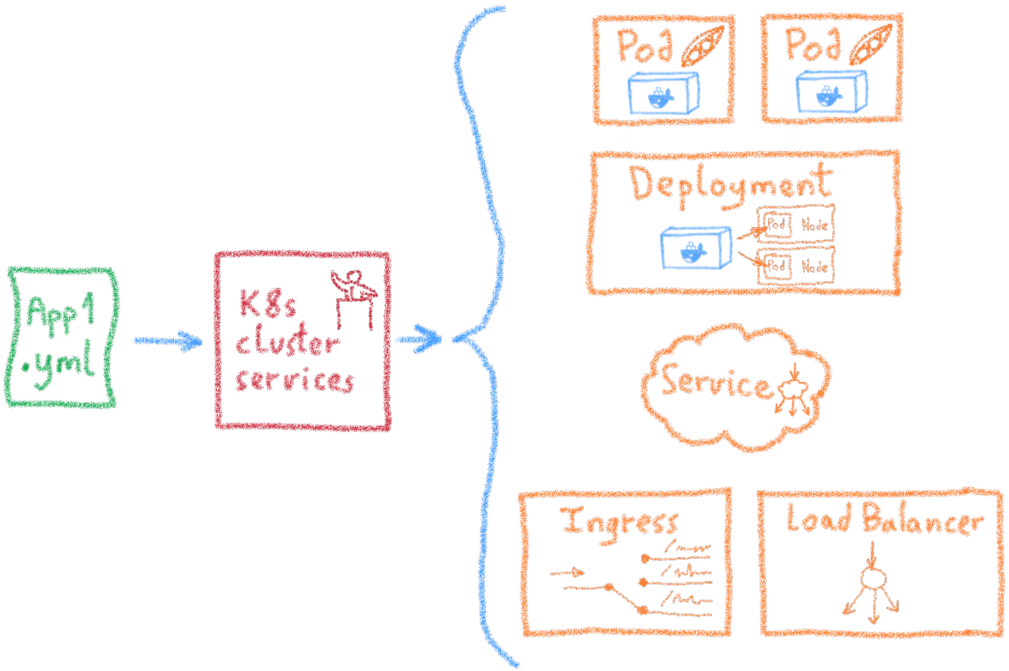
Masters and nodes



Some more details



Desired State Management



Ingress

Services

Deployments

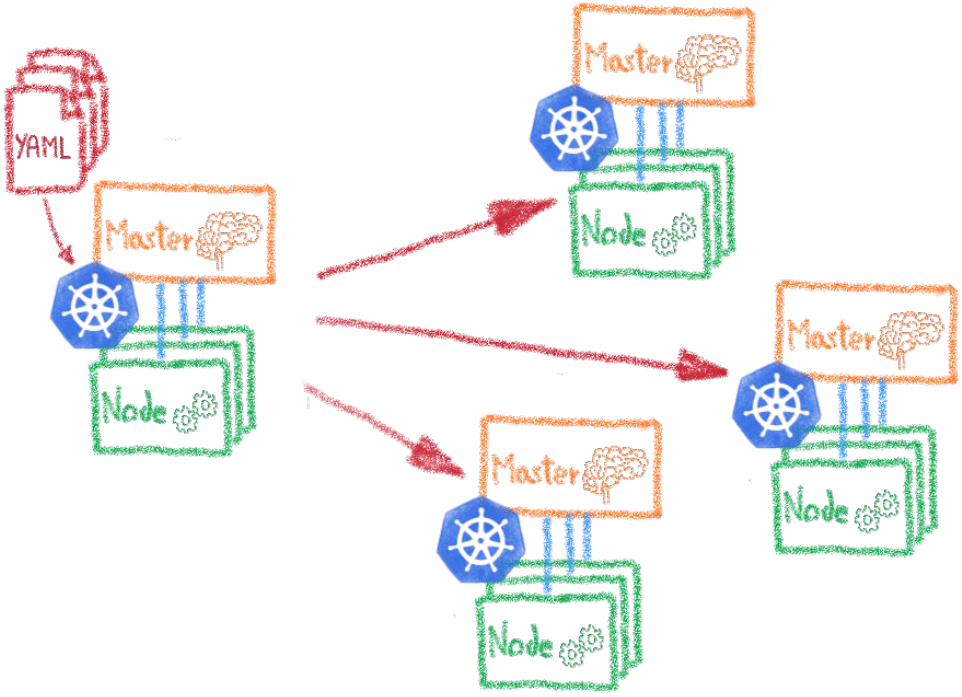
Pods

Sidecars

Replica Sets

Stateful Sets

Having identical, software defined environments

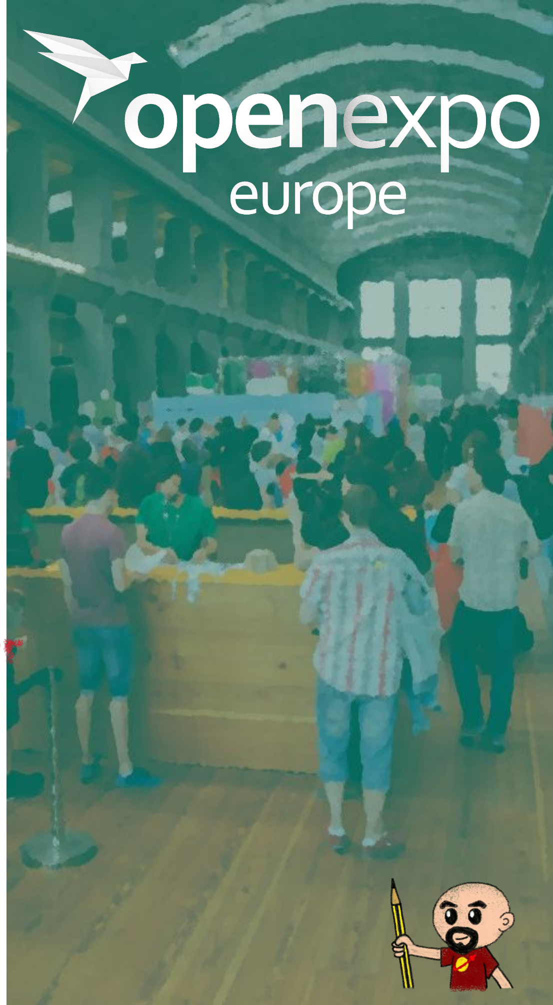


Dev envs

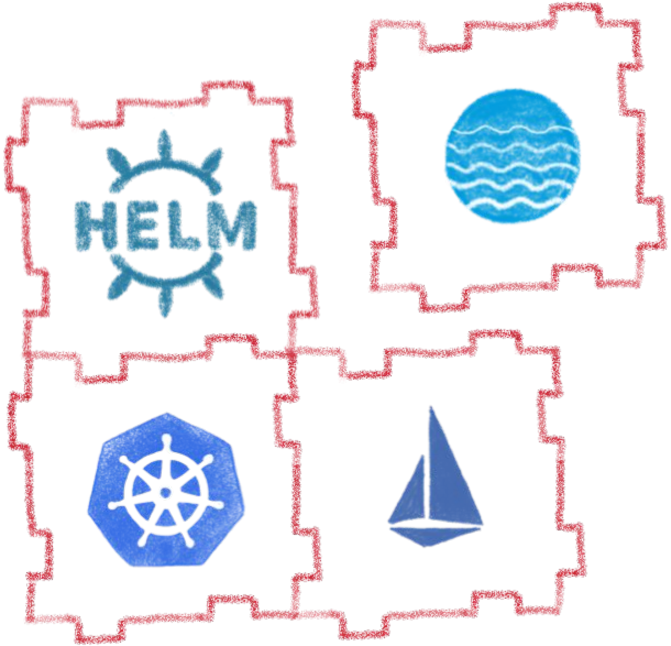
Staging

Multi-cluster

Multi-cloud



Extending Kubernetes

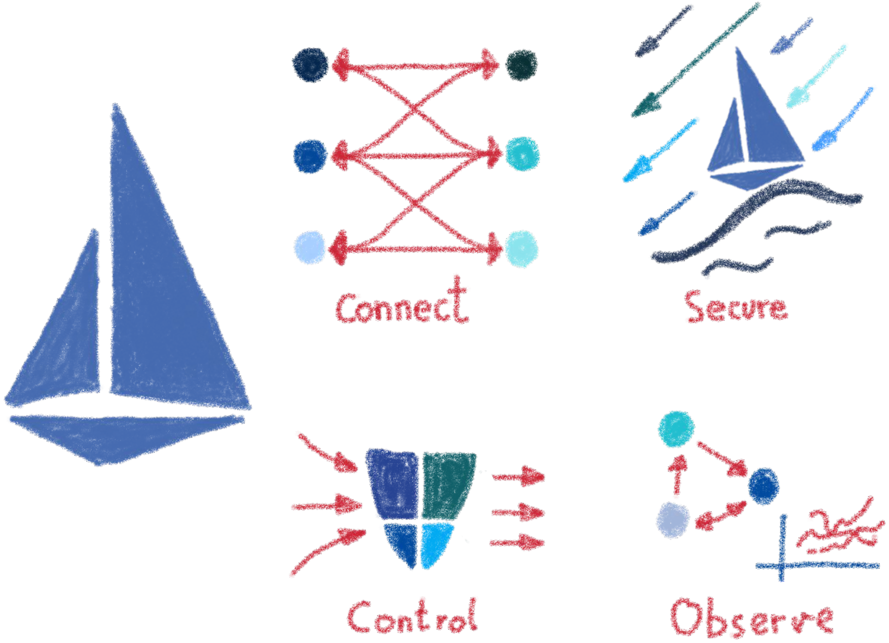


Fully extensible

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

Operators

Extension example: Istio, a service mesh for Kubernetes



Rolling upgrades

A/B Testing

Canary Testing

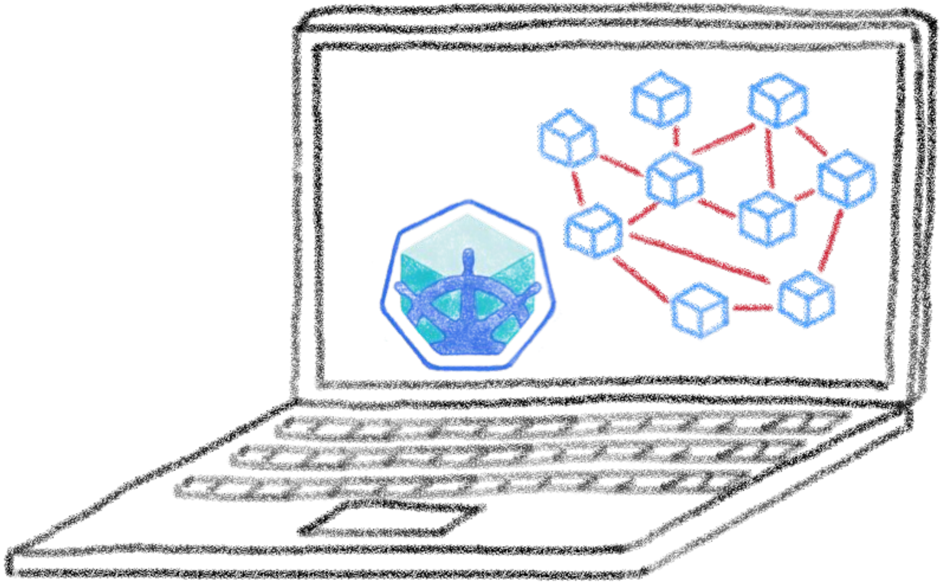
Edge traffic management

Multicluster service mesh

Minikube: K8s on my laptop

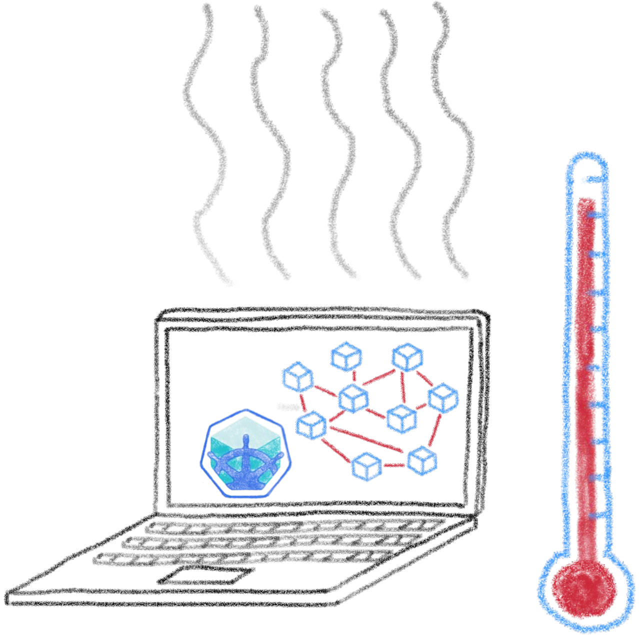
A great fastlane into Kubernetes

Running a full K8s in your laptop



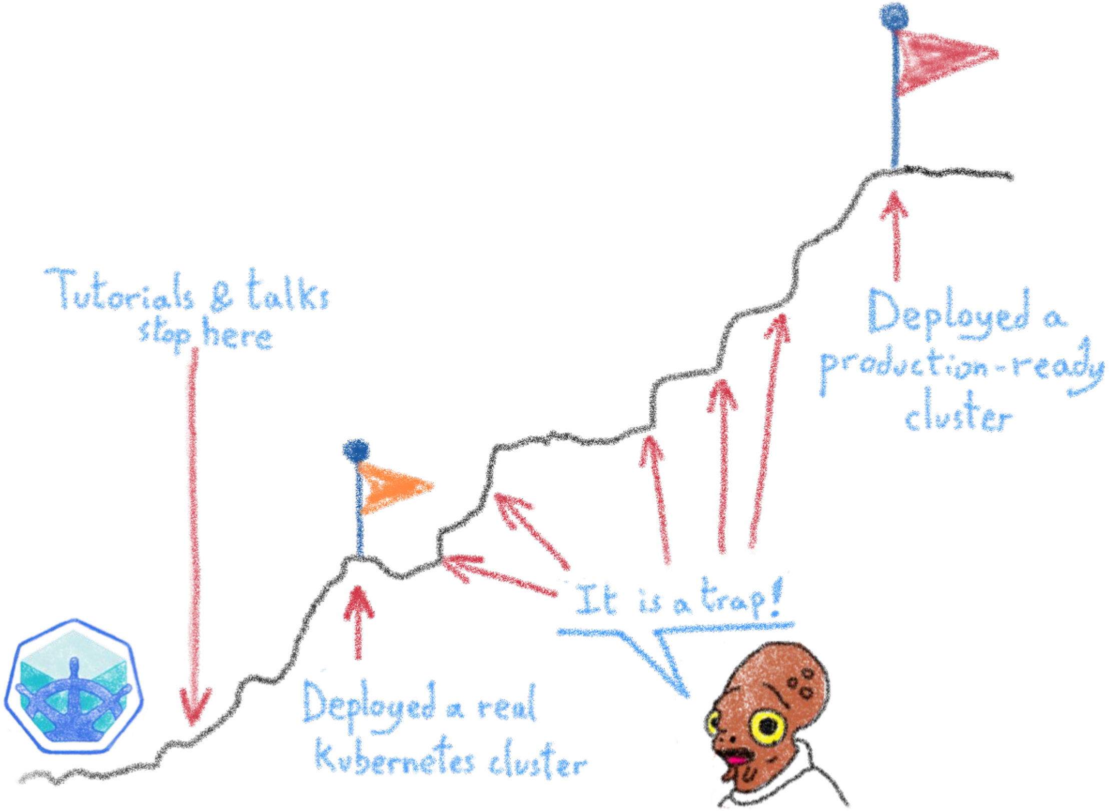
A great learning tool

Your laptop isn't a true cluster



Don't expect real performances

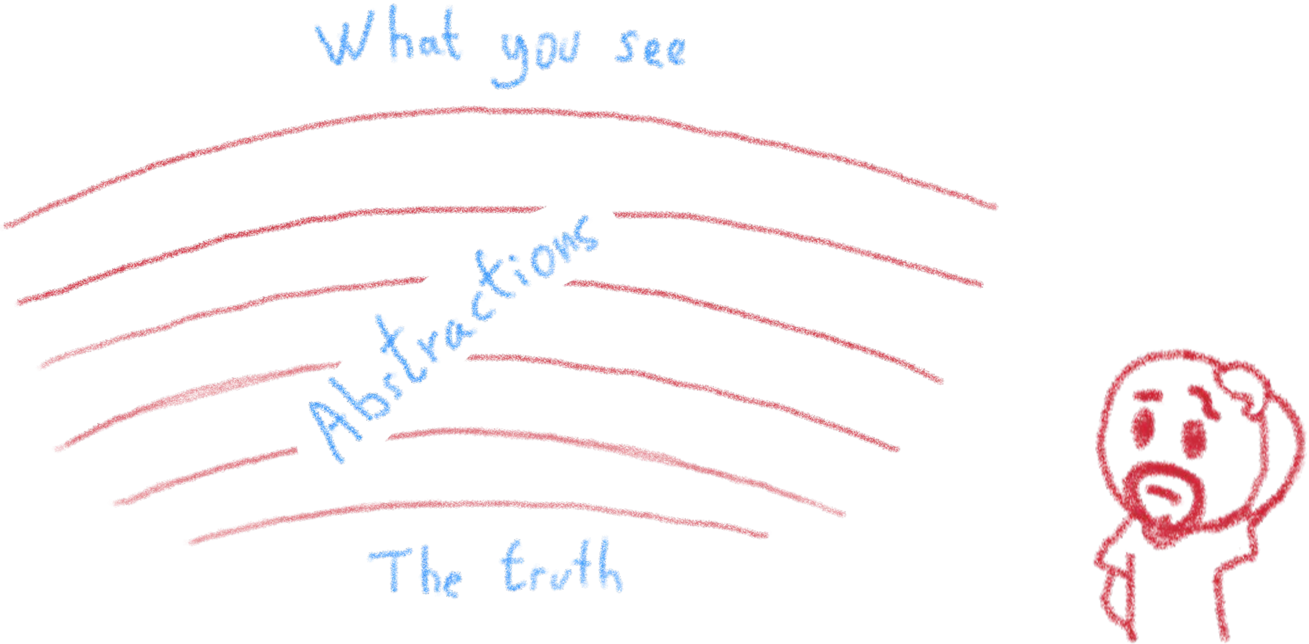
Minikube is only the beginning


Tutorials & talks stop here
Deployed a real kubernetes cluster
It is a trap!
Deployed a production-ready cluster

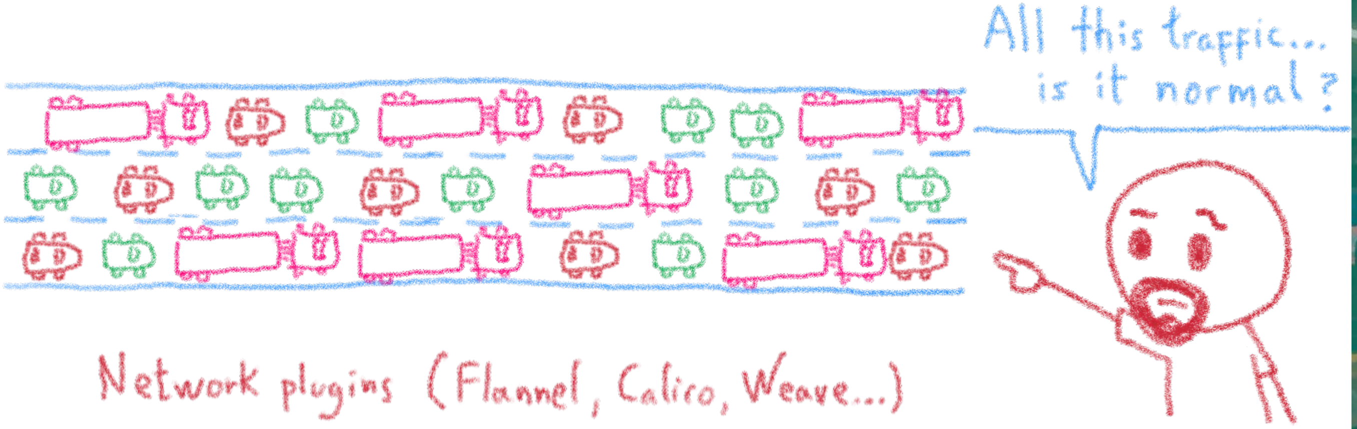
From Minikube to prod

A journey not for the faint of heart

The truth is somewhere inside...



The network is going to feel it...

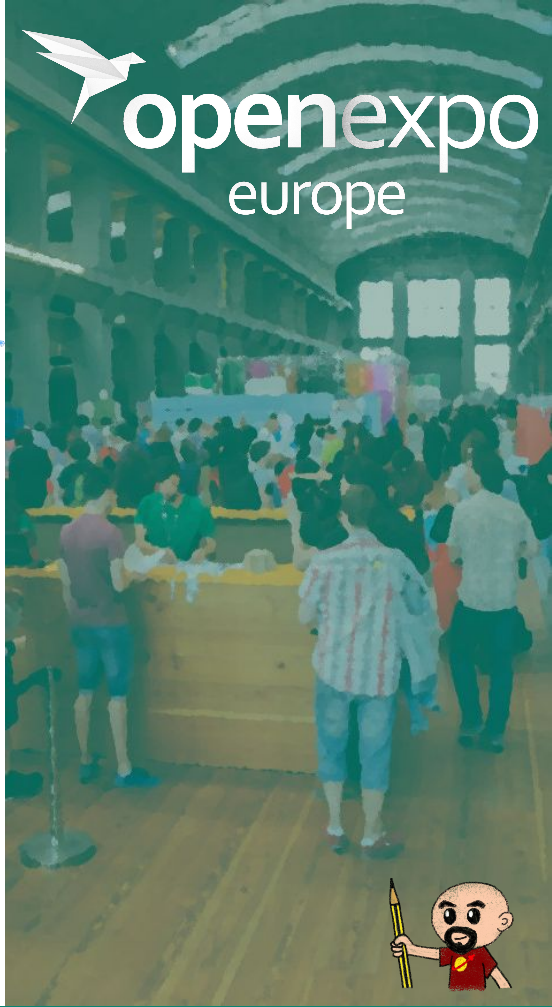


Network plugins (Flannel, Calico, Weave...)

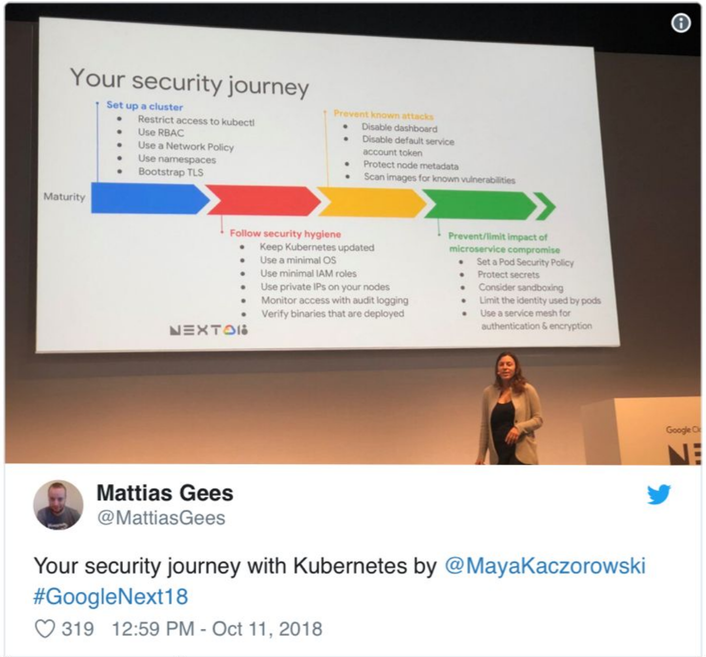
- IPAM
- routing
- iptables
- crossnode networking

Cluster IP, NodePort, Ingress

Service Meshes, Istio



The security journey



Your security journey

Maturity

Set up a cluster
- Restrict access to kubectl
- Use RBAC
- Use a Network Policy
- Use namespaces
- Bootstrap TLS

Follow security hygiene
- Keep Kubernetes updated
- Use a minimal OS
- Use minimal IAM roles
- Use private IPs on your nodes
- Monitor access with audit logging
- Verify binaries that are deployed

Prevent known attacks
- Disable dashboard
- Disable default service account token
- Protect node metadata
- Scan images for known vulnerabilities

Prevent/limit impact of microservice compromise
- Set a Pod Security Policy
- Protect secrets
- Consider sandboxing
- Limit the identity used by pods
- Use a service mesh for authentication & encryption

NEXT 18

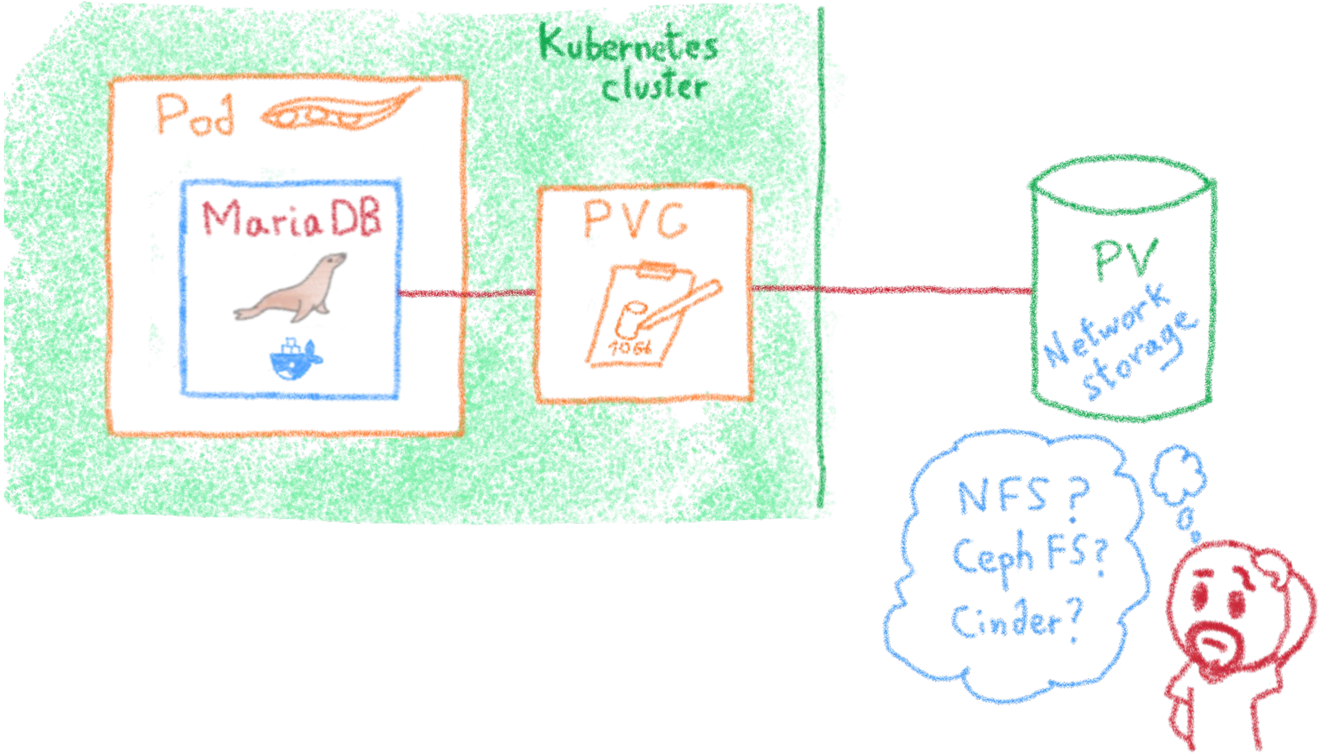
Mattias Gees
@MattiasGees

Your security journey with Kubernetes by @MayaKaczorowski #GoogleNext18

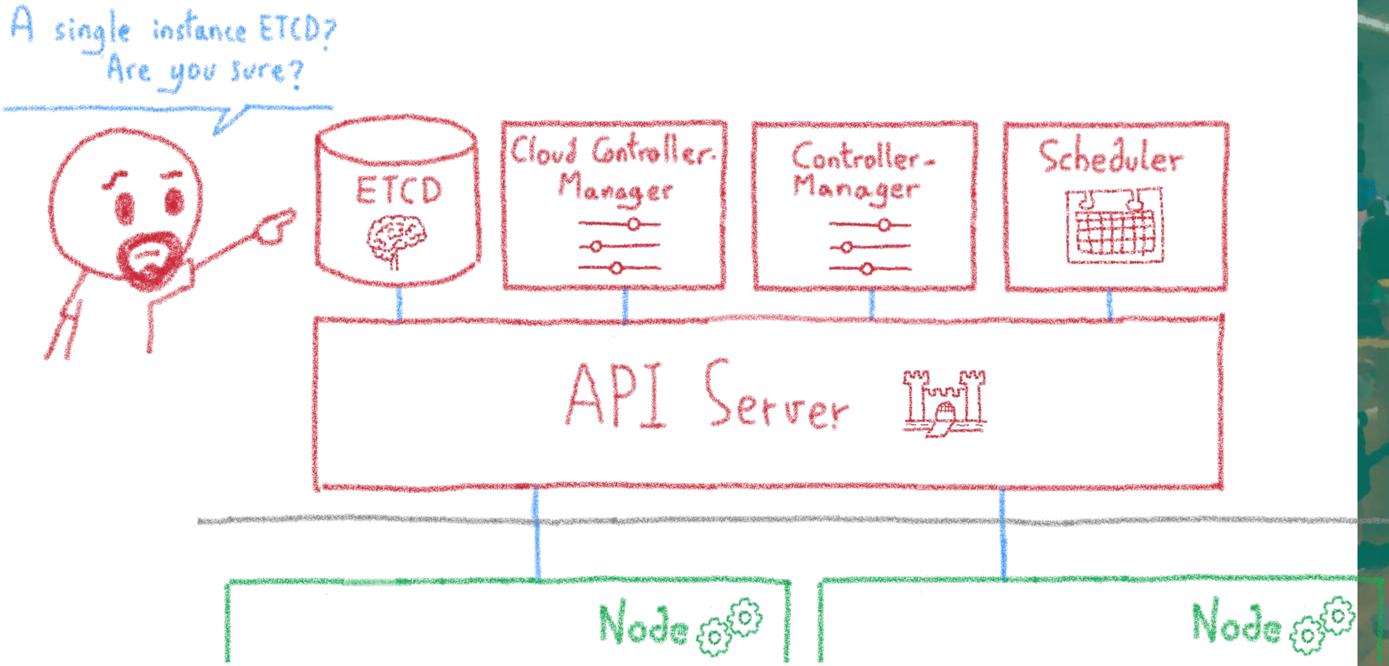
♡ 319 12:59 PM - Oct 11, 2018

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

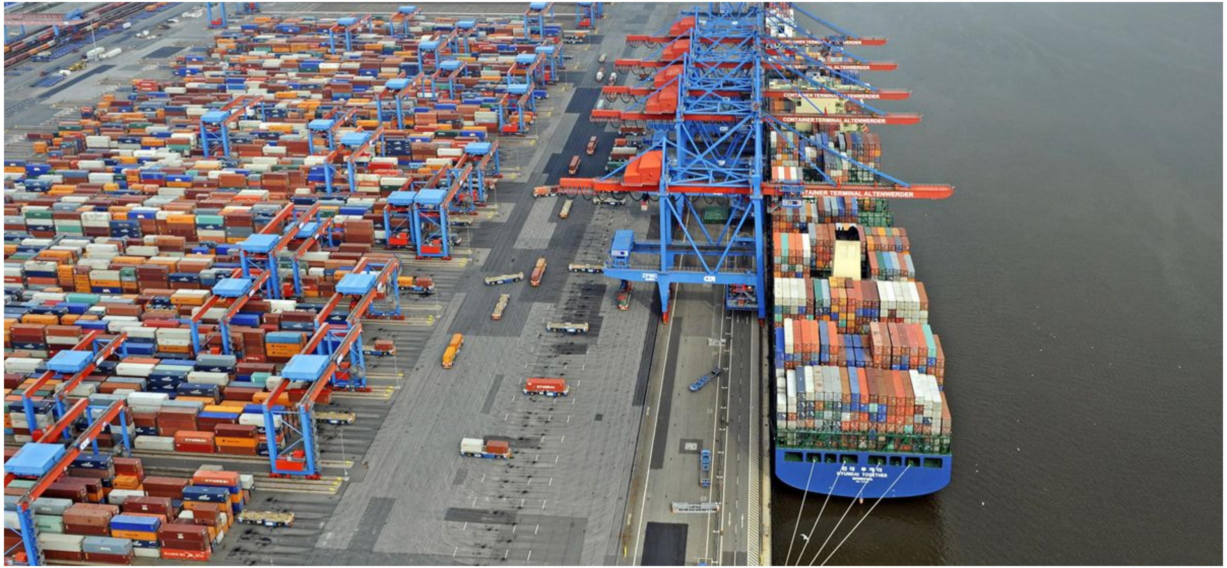


The ETCD vulnerability

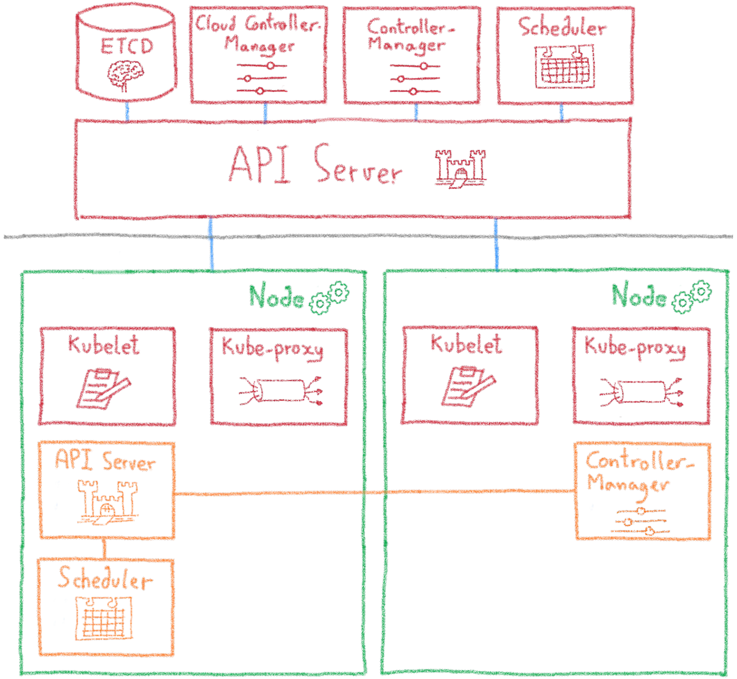


Managed Kubernetes

Don't try it at home, folks!

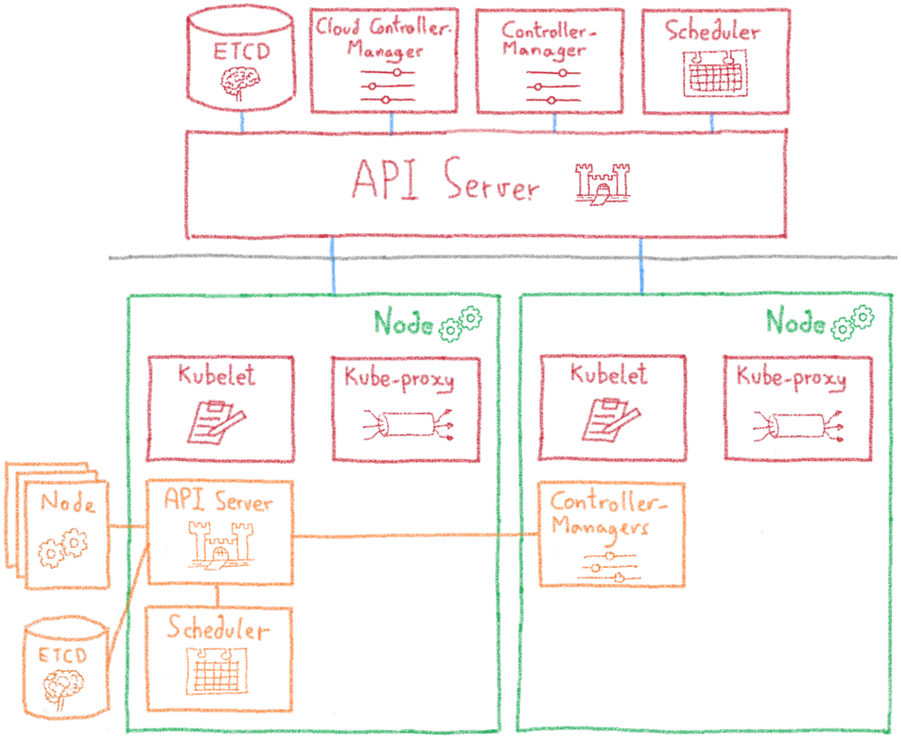


Kubinception: running K8s on K8s

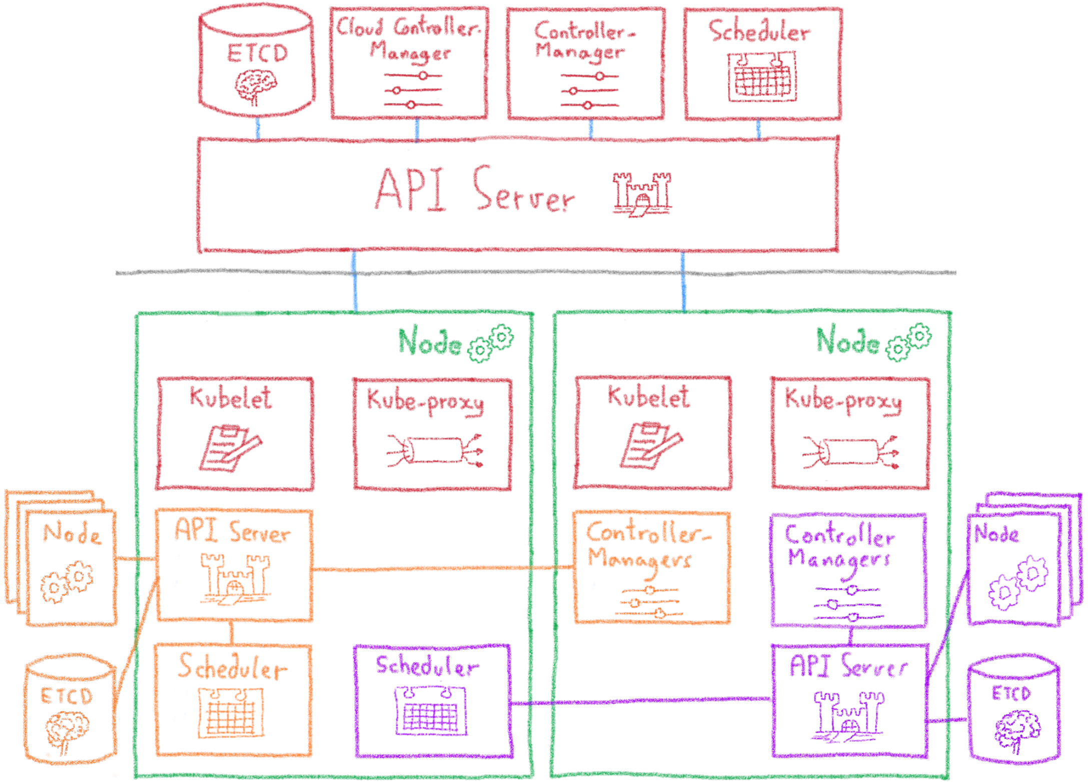


Using Kubernetes to run Kubernetes

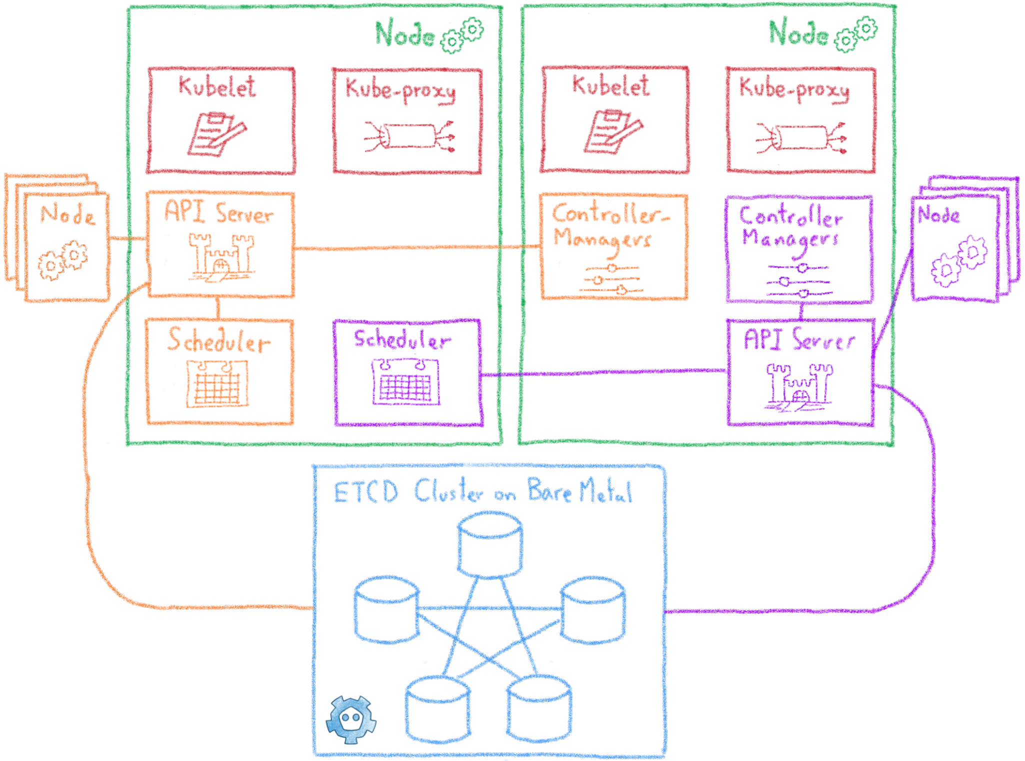
Kubinception: where are the nodes?



Kubinception with several customers



And the ETCD?



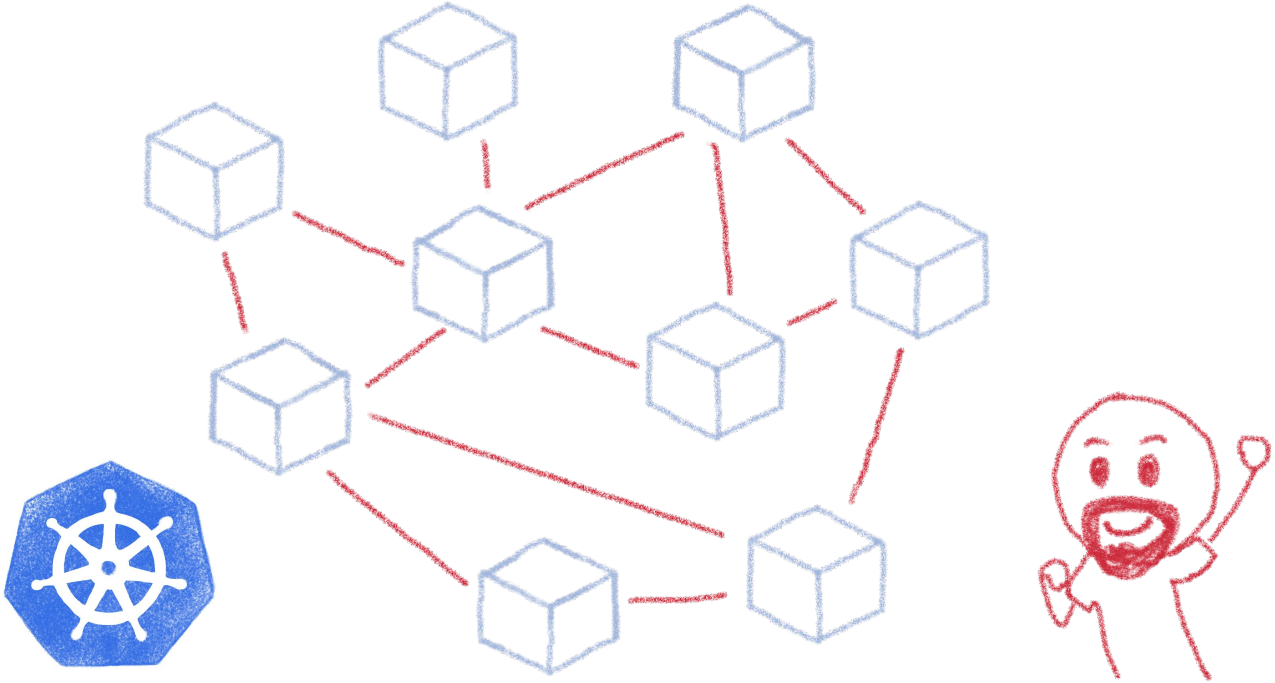
Node
Kubelet
Kube-proxy
Node
Kubelet
Kube-proxy
Node
API Server
Controller-Managers
Controller Managers
Node
Scheduler
Scheduler
API Server
ETCD Cluster on Bare Metal

openexpo
europe

Conclusions

And the point was?

Kubernetes is powerful



It can make Developers' and DevOps' lifes easier

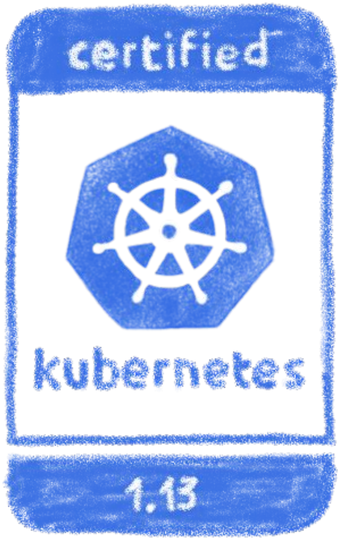
Different roles

Very different skill sets and knowledge needed

Most companies don't need to operate the clusters

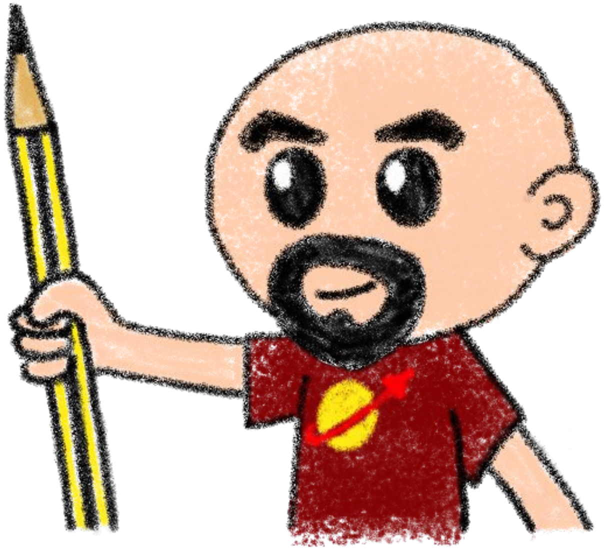
As they don't build and rack their own servers!

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



You get the cluster, the operator get the problems

Do you want to try?



Send me an email to get some vouchers...

horacio.gonzalez@corp.ovh.com