OVHcloud

KubeCon | CloudNativeCon

Europe 2020

Virtual

From Minikube to Production

Never Miss a Step in Getting Your K8s Ready

Kevin Georges

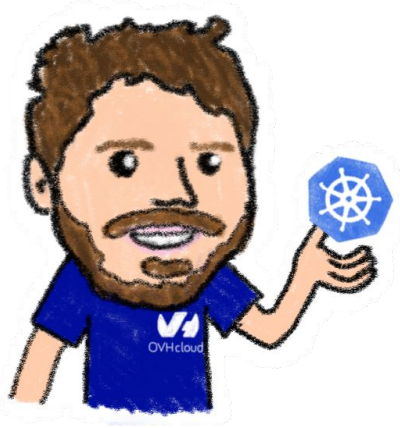
@ 0xD33D33

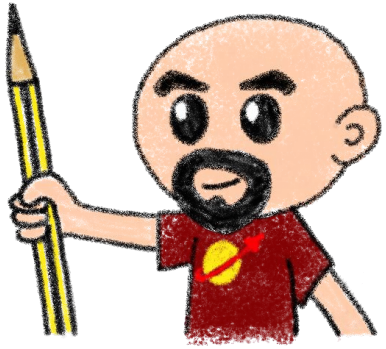
Horacio Gonzalez

@LostInBrittany

Who are we?

Introducing ourselves and introducing OVHcloud





@LostInBrittany

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

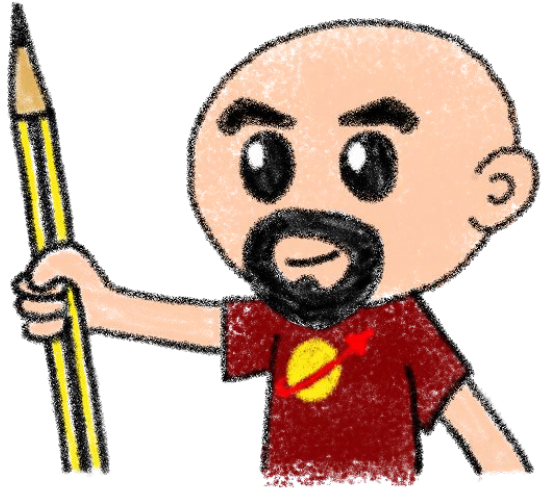
DevFest du
Bout du Monde

Finist Devs

Google Developers Experts 2019
Web Technologies
GDE
Flutter

OVHcloud

DevRel Leader

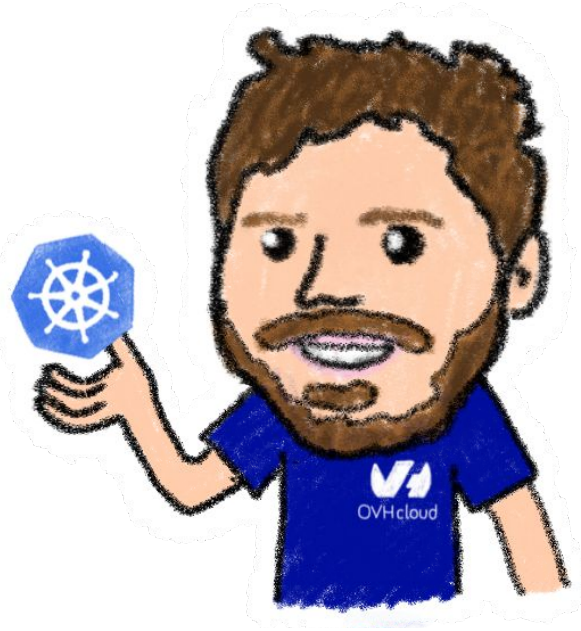


Kevin Georges

@0xd33d33

Kubernetes Engineering Manager

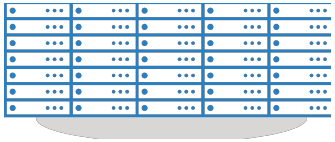
OVHcloud

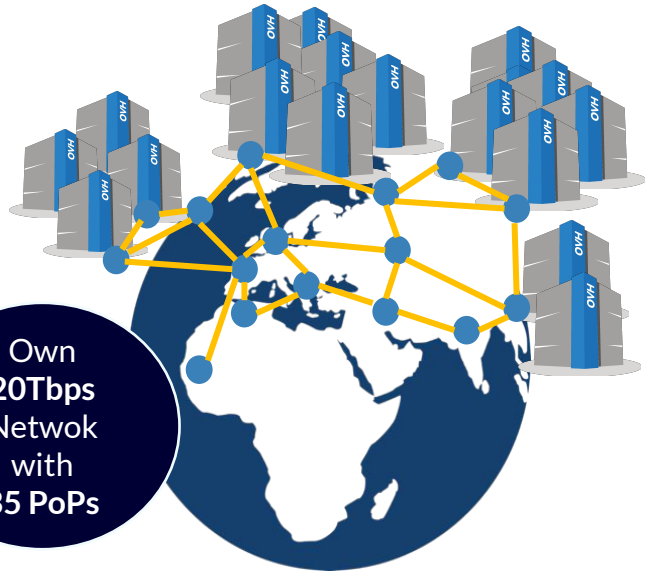


OVHcloud: A Global Leader

200k Private cloud VMs running

1 **Dedicated IaaS Europe**





30 Datacenters

Hosting capacity :
1.3M Physical Servers

360k
Servers already deployed

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

OVHcloud: 4 Universes of Products

KubeCon | CloudNativeCon Europe 2020 Virtual

WebCloud

Domain / Email
Domain names, DNS, SSL, Redirect

Email, Open-Xchange, Exchange

Collaborative Tools, NextCloud

PaaS for Web
Mutu, CloudWeb

Plesk, CPanel

PaaS with Platform.sh

Virtual servers
VPS, Dedicated Server

SaaS
Wordpress, Magento, Prestashop

CRM, Billing, Payment, Stats

MarketPlace

Support, Managed
Support Basic

Support thought Partners

Managed services

Baremetal Cloud

Standalone, Cluster
General Purpose
SuperPlan
Game
Virtualization
Storage
Database
Bigdata
HCI
AI
VDI Cloud Game
Network

T2 >20e
T3 >80e
T4 >300e
T5 >600e
12KVA /32KVA

VPS aaS
pCC DC

Virtuozzo Cloud

Wholesales
IT Integrators, Cloud Storage,

CDN, Database, ISV, WebHosting

High Intensive CPU/GPU,

Encrypt
KMS, HSM

Encrypt (SGX, Network, Storage)

Public Cloud

Compute
VM
Baremetal
K8S, IA IaaS
PaaS for DevOps

Storage
File, Block, Object, Archive

Databases
SQL, noSQL, Messaging,

Dashboard

Network
IP FO, NAT, LB, VPN, Router,

DNS, DHCP, TCP/SSL Offload

Security
IAM, MFA, Encrypt, KMS

IA, DL
Standard Tools for AI, AI Studio,

IA IaaS, Hosting API AI

Bigdata, ML, Analytics
Datalake, ML, Dashboard

Hosted Private Cloud

Hosted Private Cloud

VMware
SDDC, vSAN 1AZ / 2AZ
vCD, Tanzu, Horizon, DBaaS,
DRaaS

Nutanix
HCI 1AZ / 2AZ, Databases,
DRaaS, VDI

OpenStack
IAM, Compute (VM, K8S)
Stortage, Network, Databases

Storage
Ontap Select, Nutanix File
OpenIO, MinIO, CEPH
Zerto, Veeam, Atempo

AI
ElementAI, HuggingFace,
Deepopmatic, Systran,
EarthCube

Bigdata / Analitics / ML
Cloudera over S3, Dataiku,
Saagie, Tableau,

Hybrid Cloud
vRack Connect, Edge-DC, Private DC

Dell, HP, Cisco, OCP, MultiCloud

Secured Cloud
GOV, FinTech, Retail, HealtCare

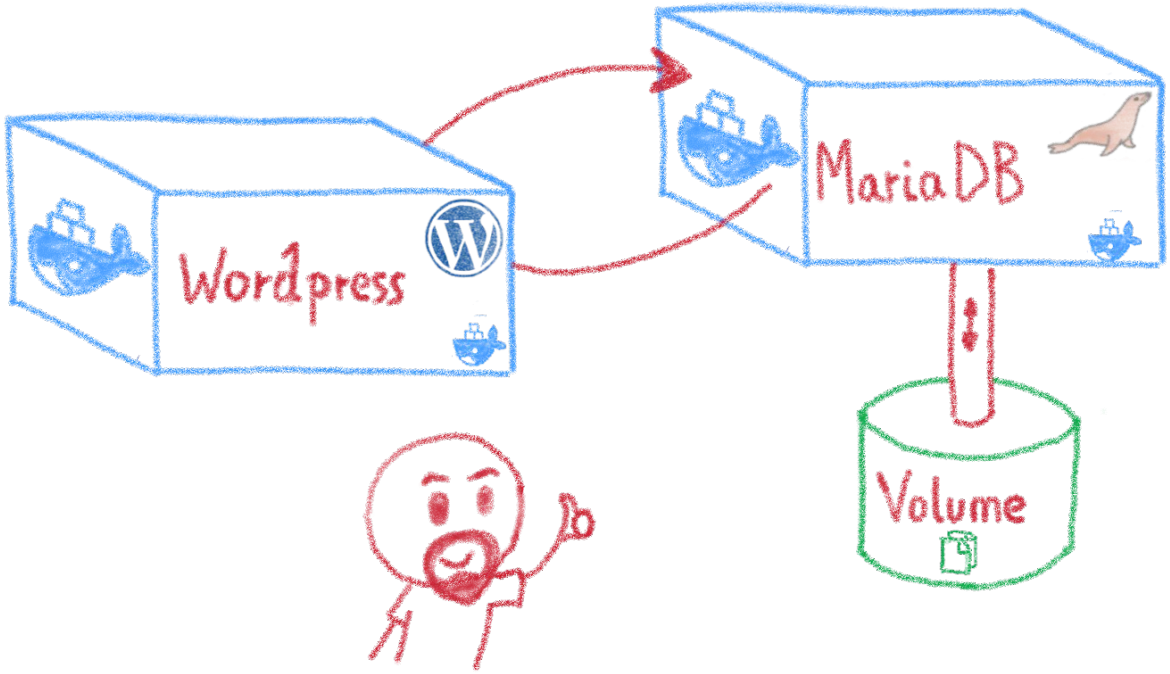
Orchestrating containers

Like herding cats… but in hard mode!

From bare metal to containers

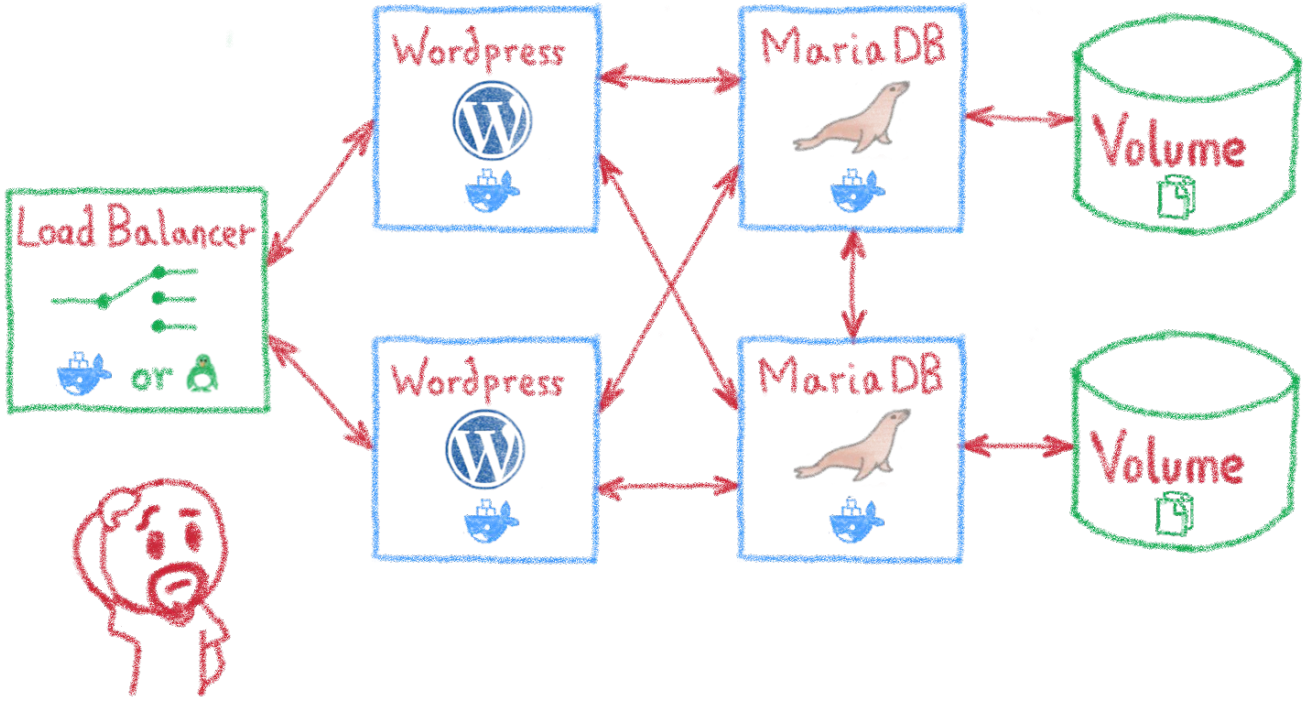
Another paradigm shift

Containers are easy...



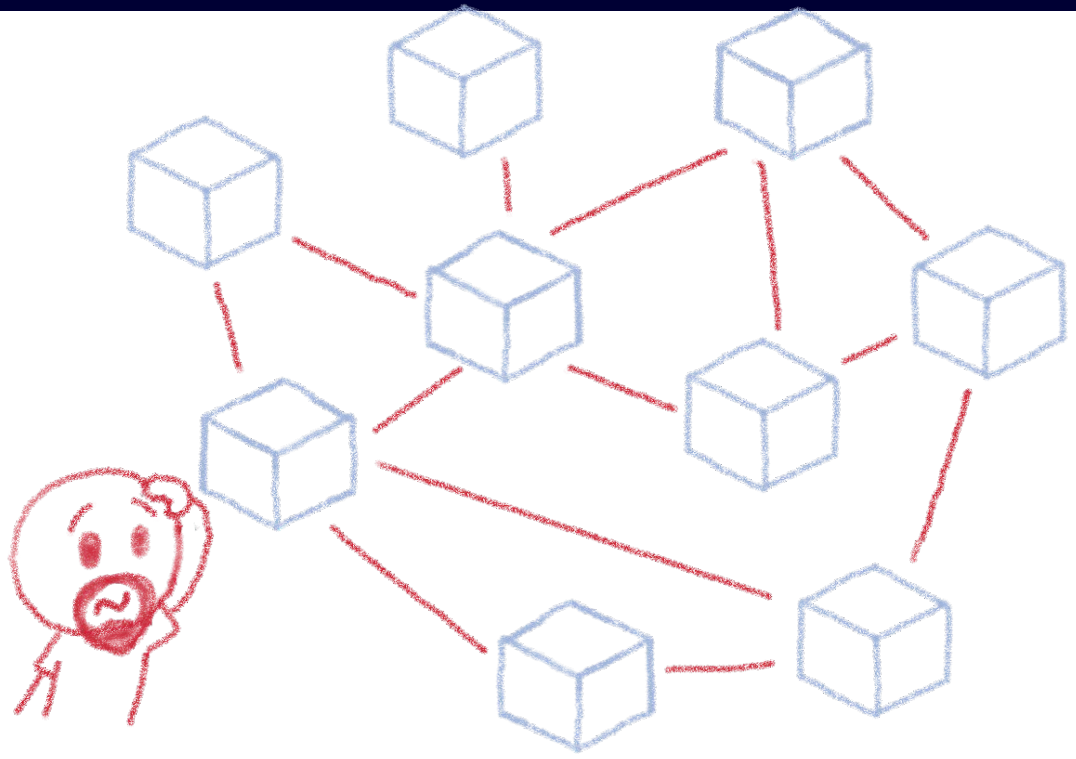
For developers

Less simple if you must operate them



Like in a production context

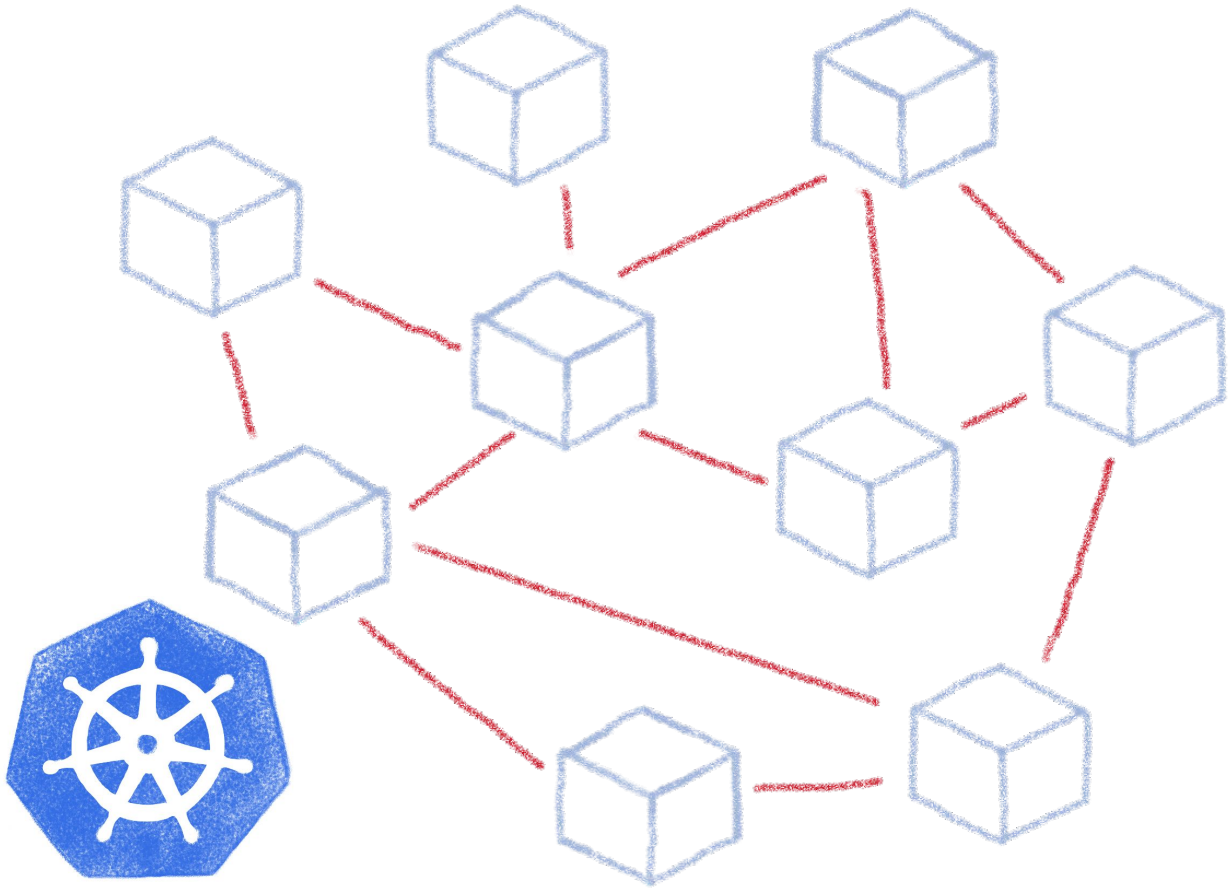
And what about microservices?



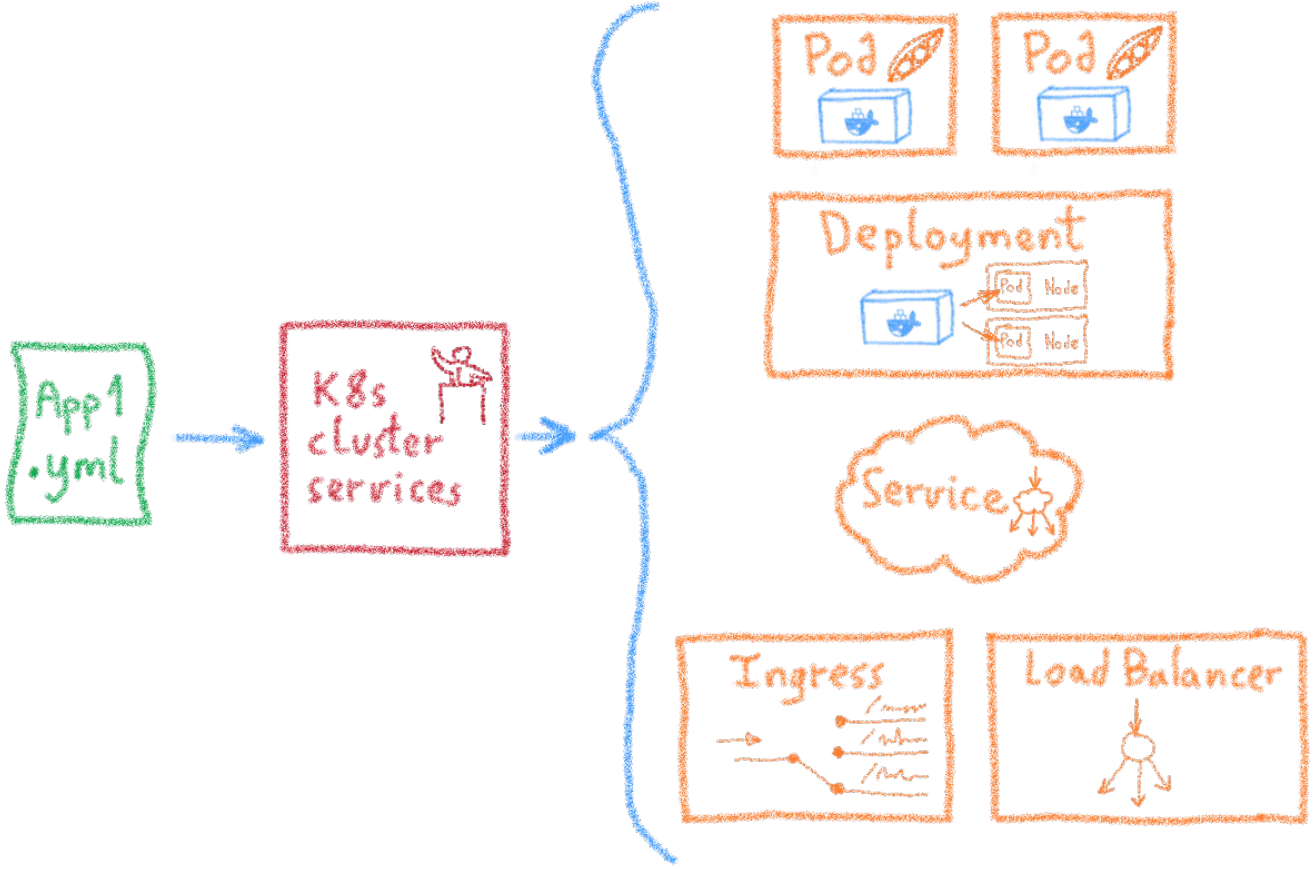
Are you sure you want to operate them by hand?

Taming microservices with Kubernetes

KubeCon CloudNativeCon Europe 2020 Virtual



Desired State Management



Ingress

Services

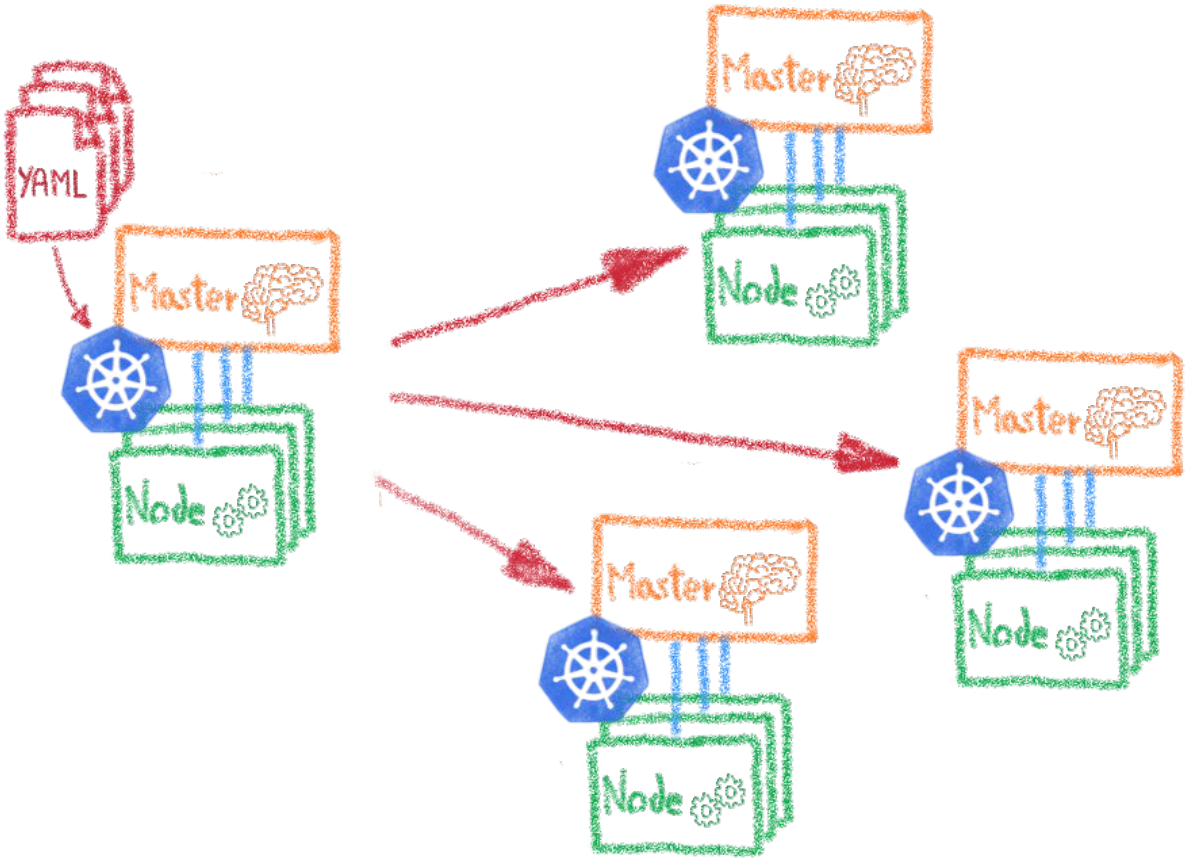
Deployments

Pods

Sidecars

Replica Sets

Having identical, software defined environments



Dev envs

Staging

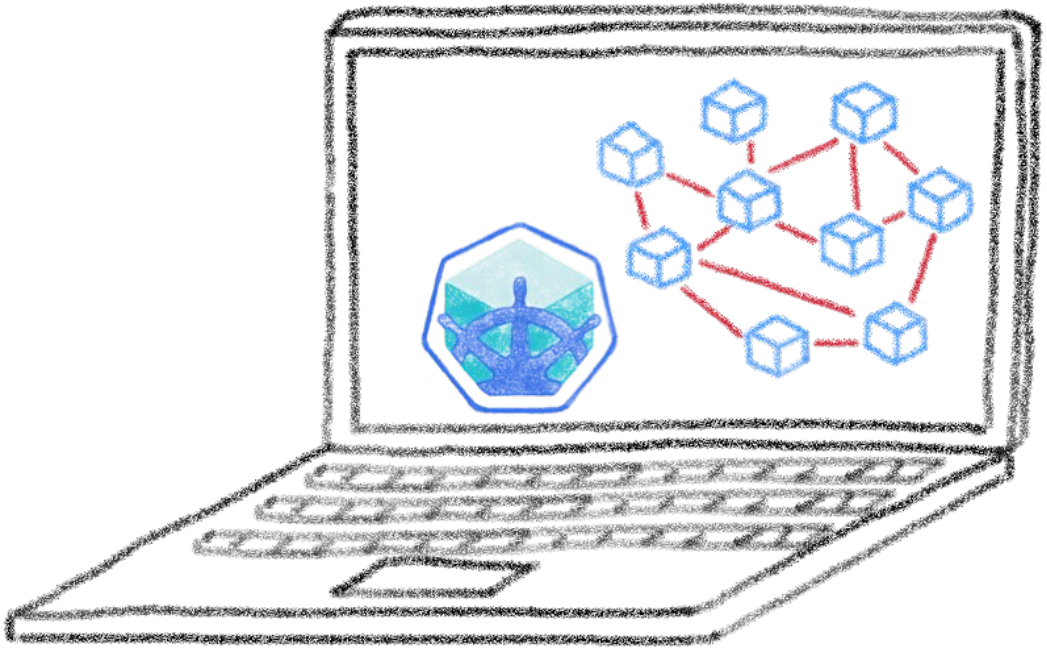
Multi-cluster

Multi-cloud

I have deployed on Minikube, woah!

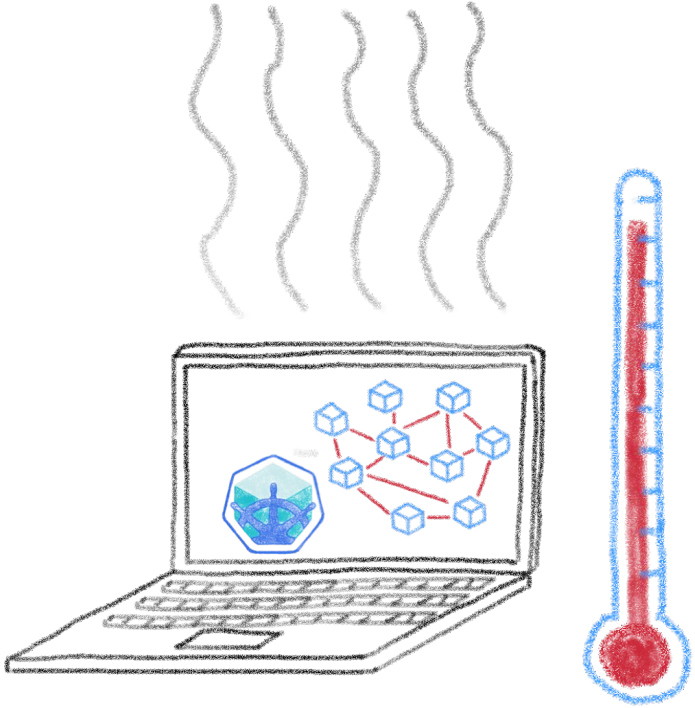
A great fastlane into Kubernetes

Running a full K8s in your laptop



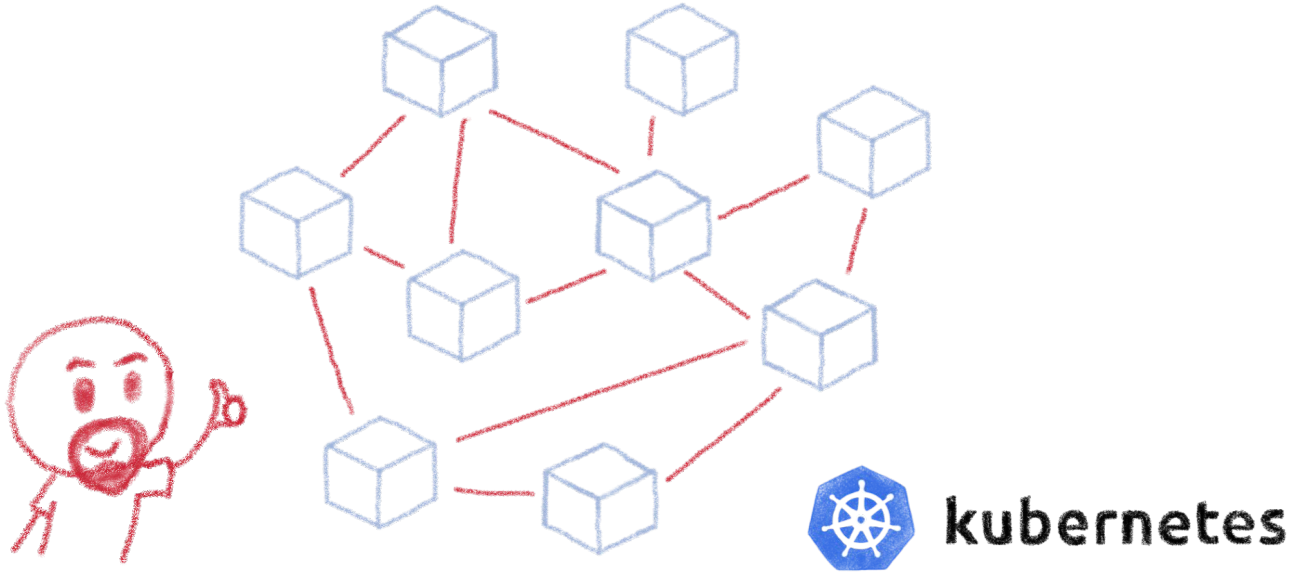
A great learning tool

Your laptop isn't a true cluster



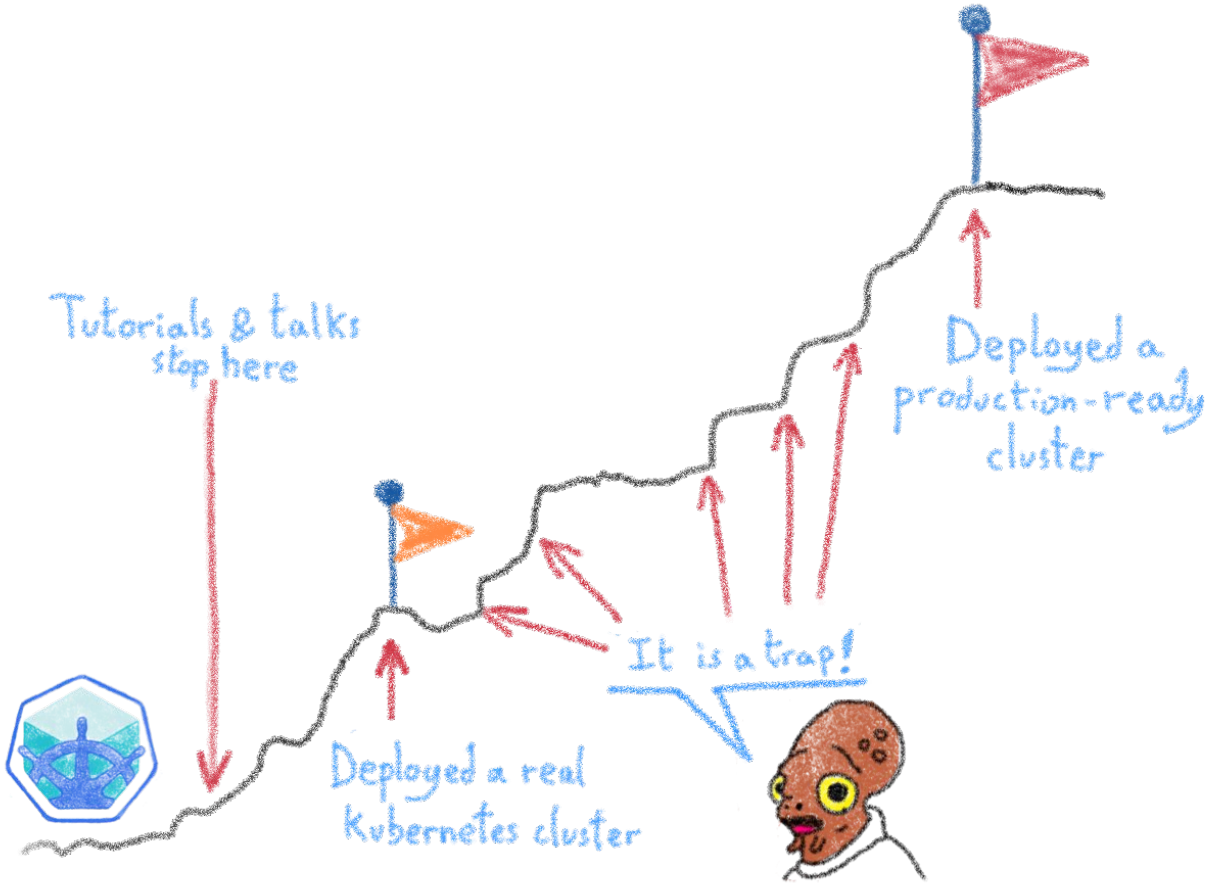
Don't expect real performances

Beyond the first deployment



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

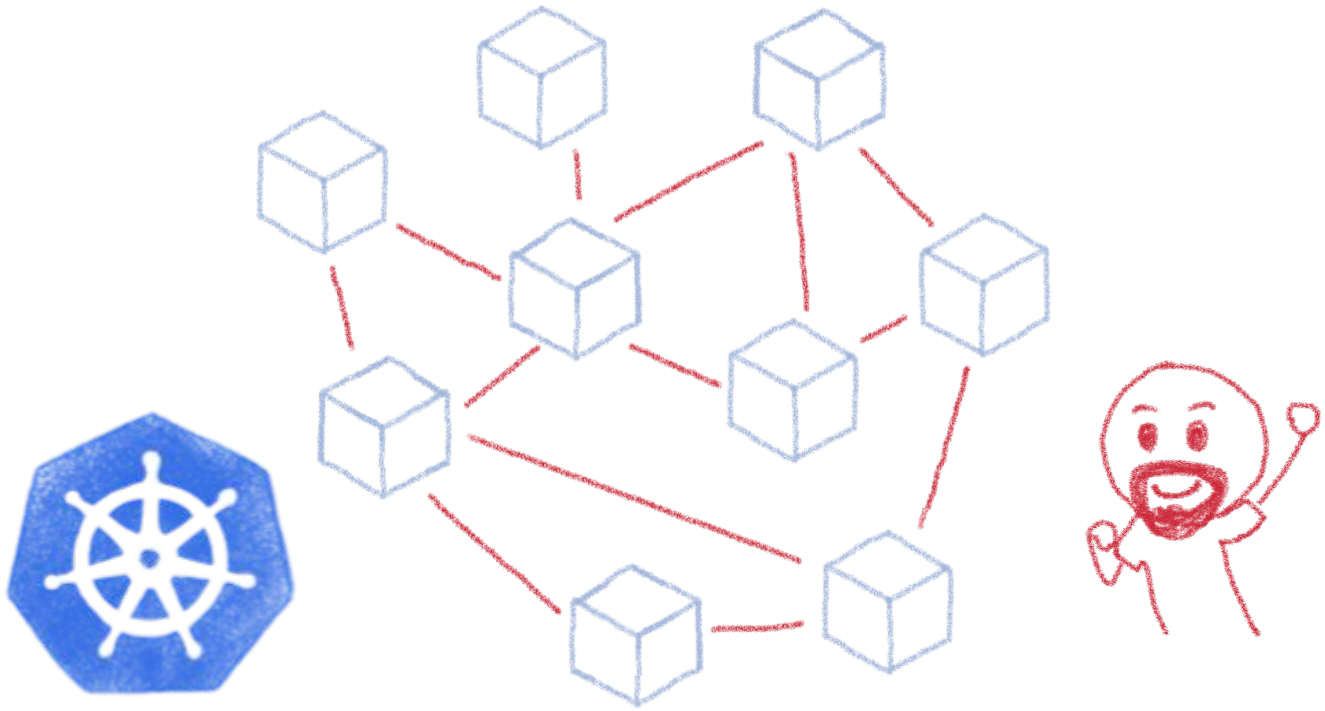
Minikube is only the beginning



From Minikube to prod

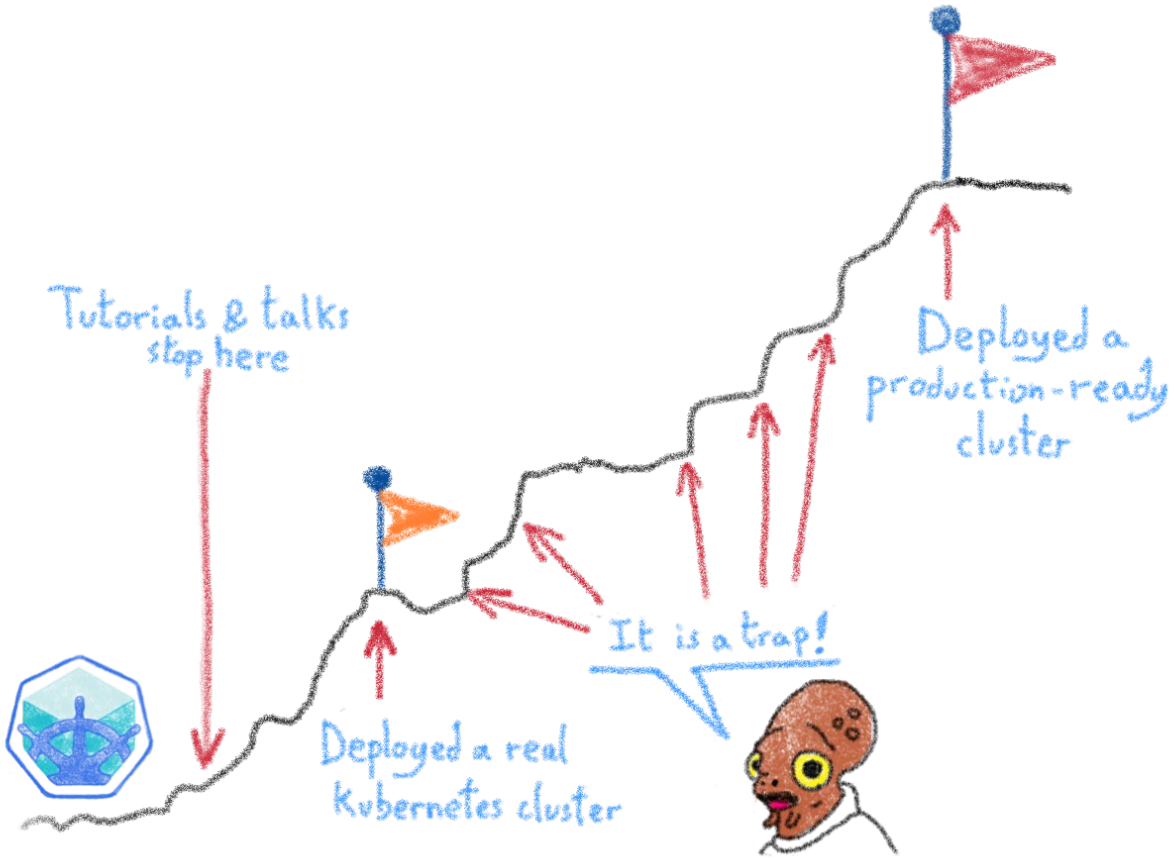
A journey not for the faint of heart

Kubernetes can be wonderful

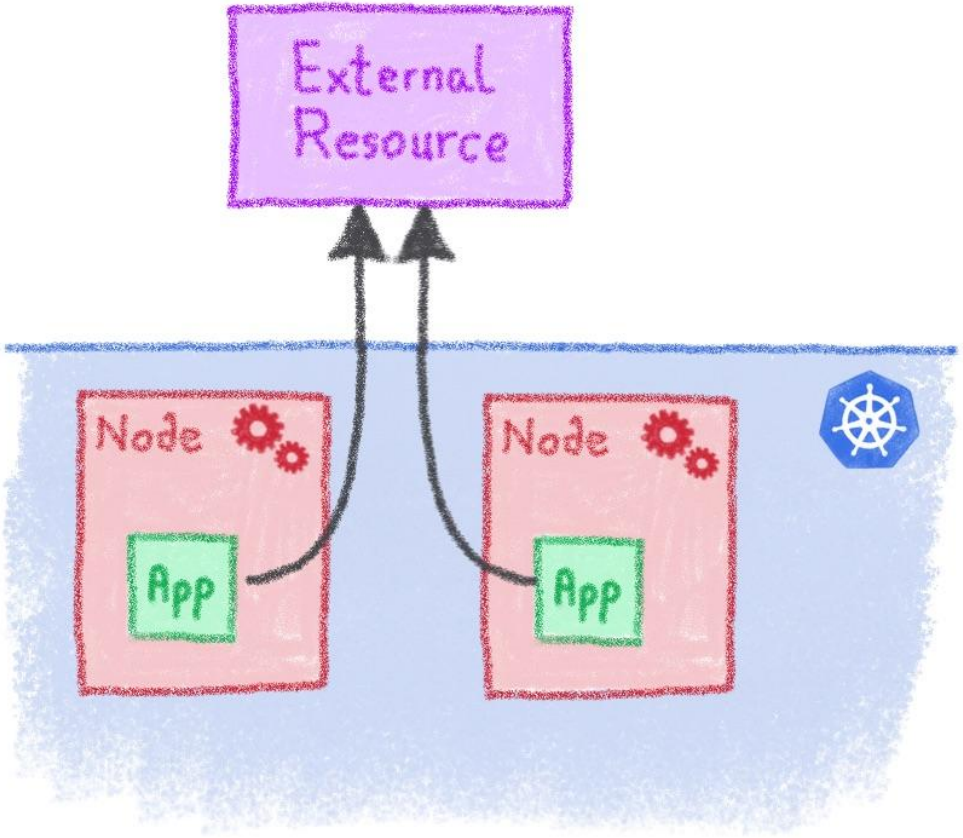


For both developers and devops

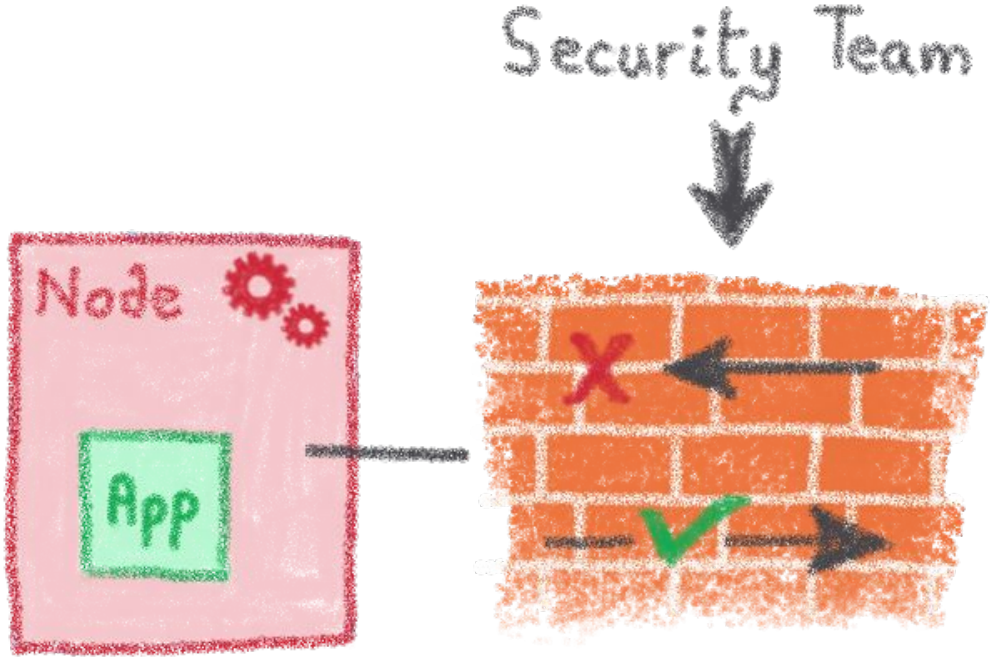
But it comes with a price...



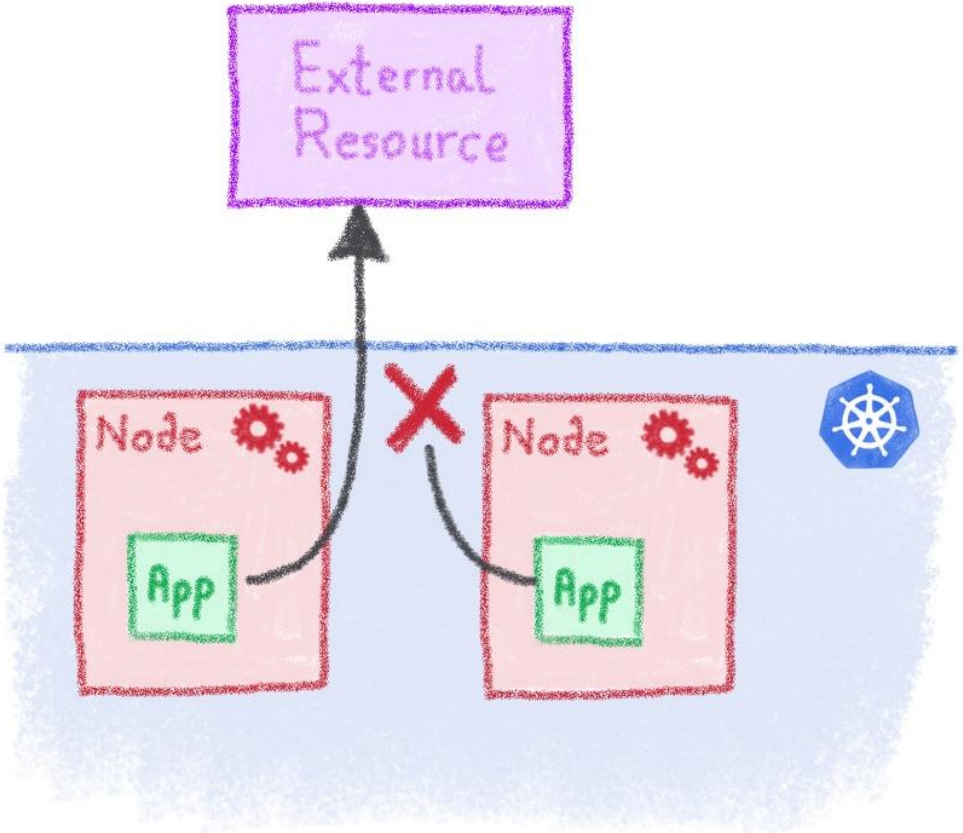
An example among many others



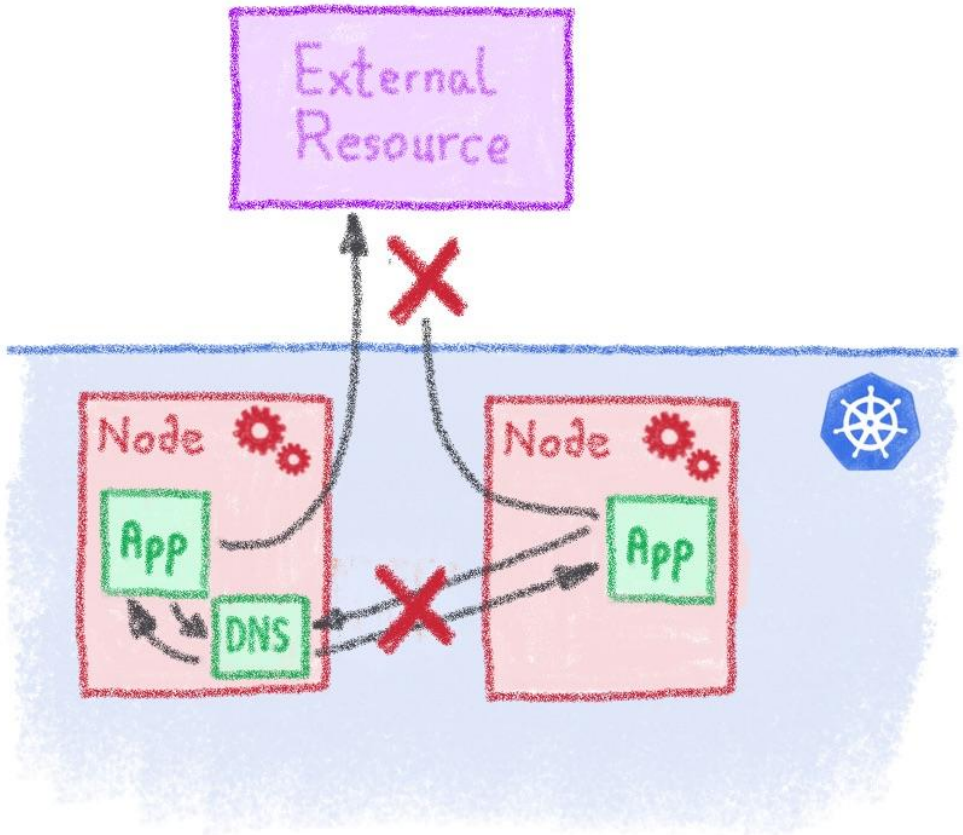
An example among many others



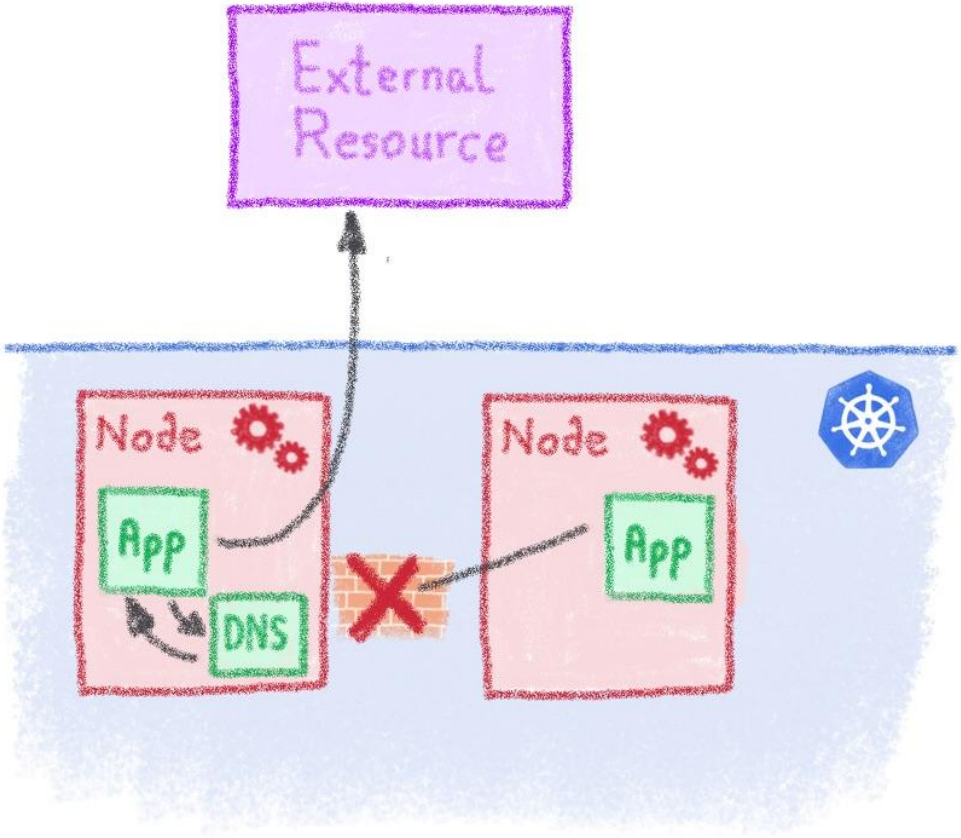
An example among many others



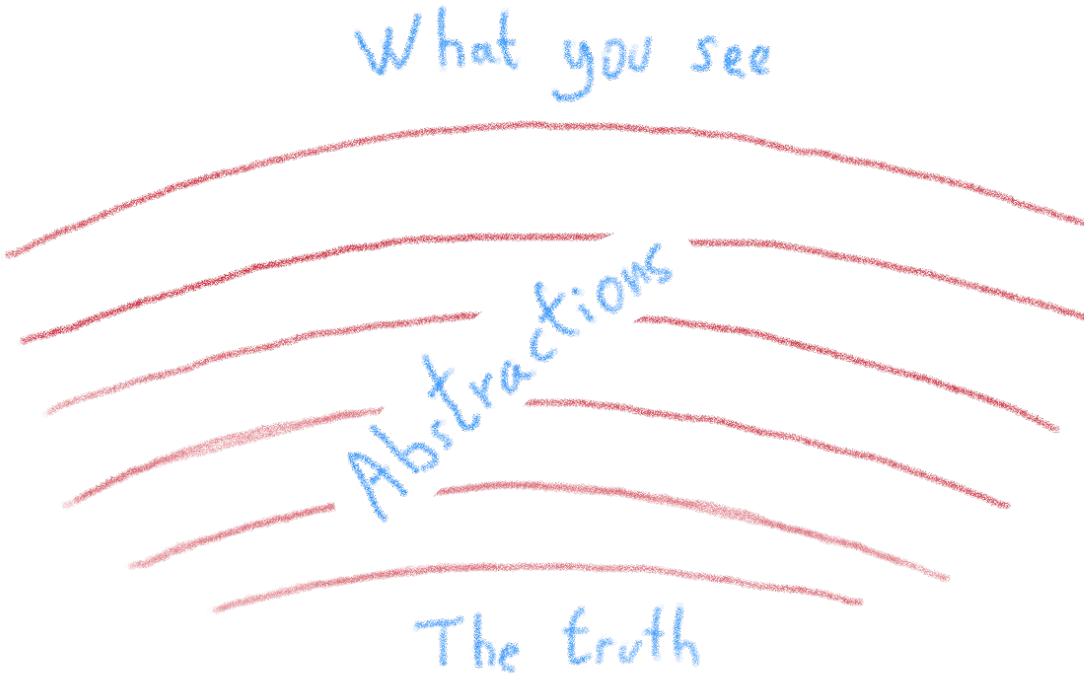
An example among many others



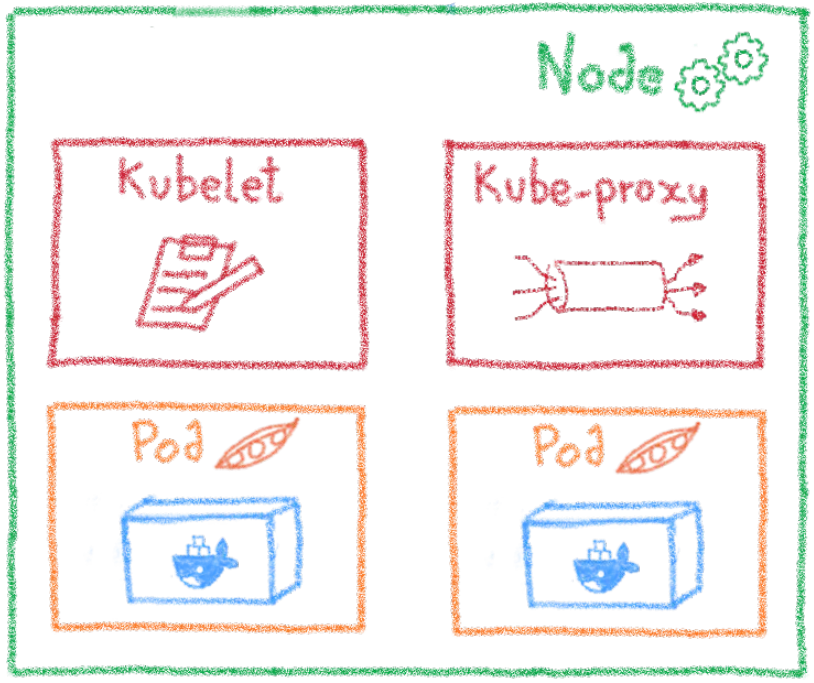
An example among many others



The truth is somewhere inside...



A network example: KubeProxy



KubeProxy: 3 proxy modes

- Userspace
- IPTables
- IPVS

A network example: KubeProxy

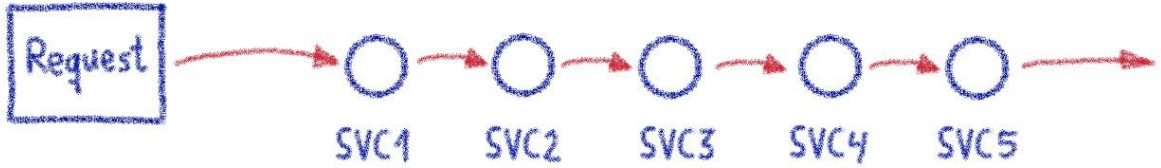
--proxy-mode ProxyMode

Which proxy mode to use: 'userspace' (older) or 'iptables' (faster) or 'ipvs'. If blank, use the best-available proxy (currently iptables). If the iptables proxy is selected, regardless of how, but the system's kernel or iptables versions are insufficient, this always falls back to the userspace proxy.

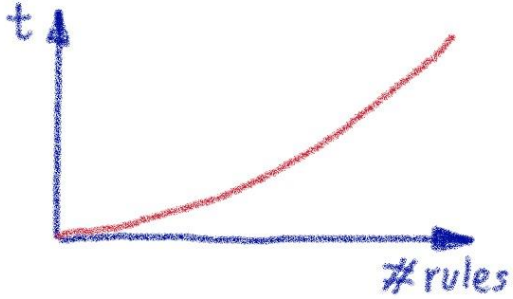
iptables by default

A network example: KubeProxy

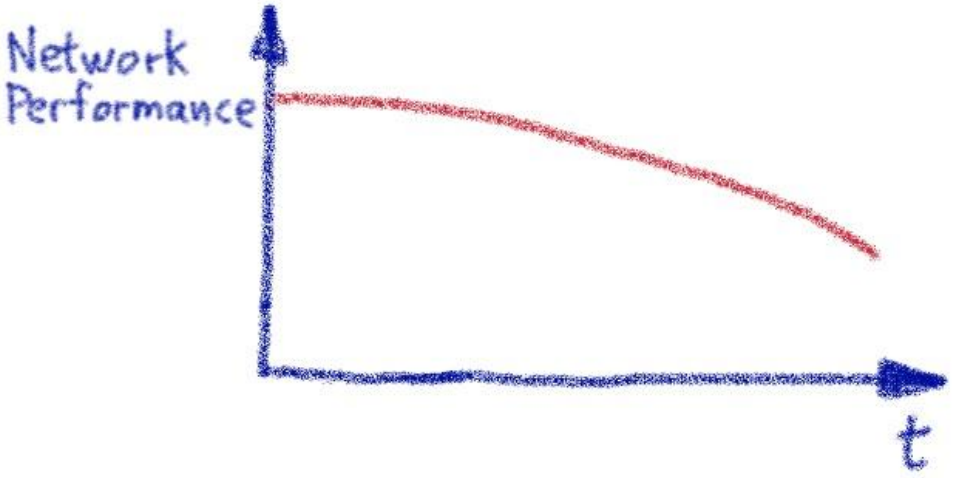
IPtables are based on rule chains



More rules → More time to insert or evaluate them



A network example: KubeProxy

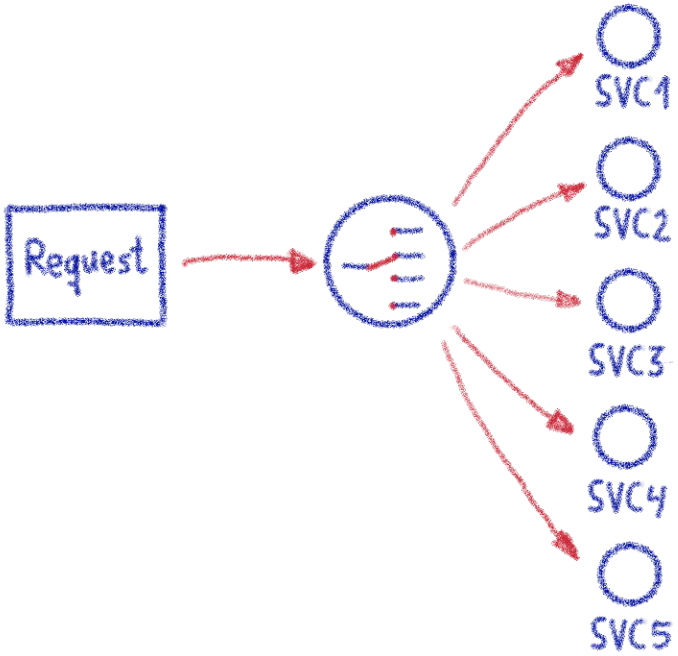


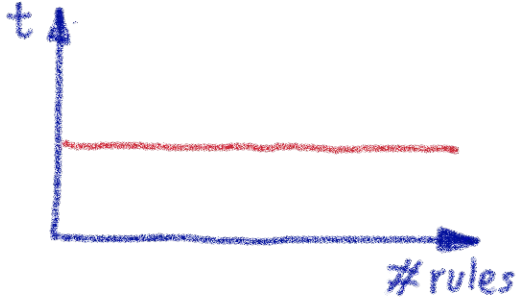
Cluster networking will be slower and slower

A network example: KubeProxy

IPVS is based on hash tables

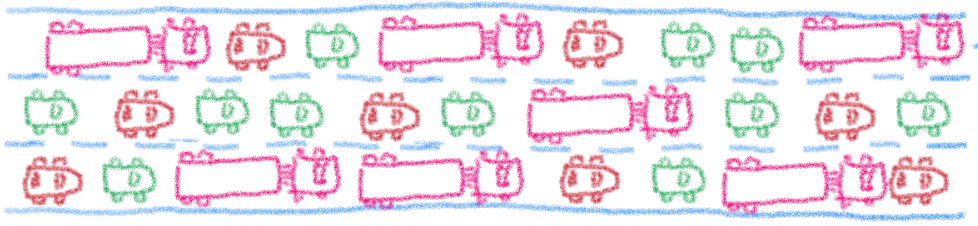
Constant time to insert or evaluate them





IPVS to the rescue!

Kubernetes networking is complex...



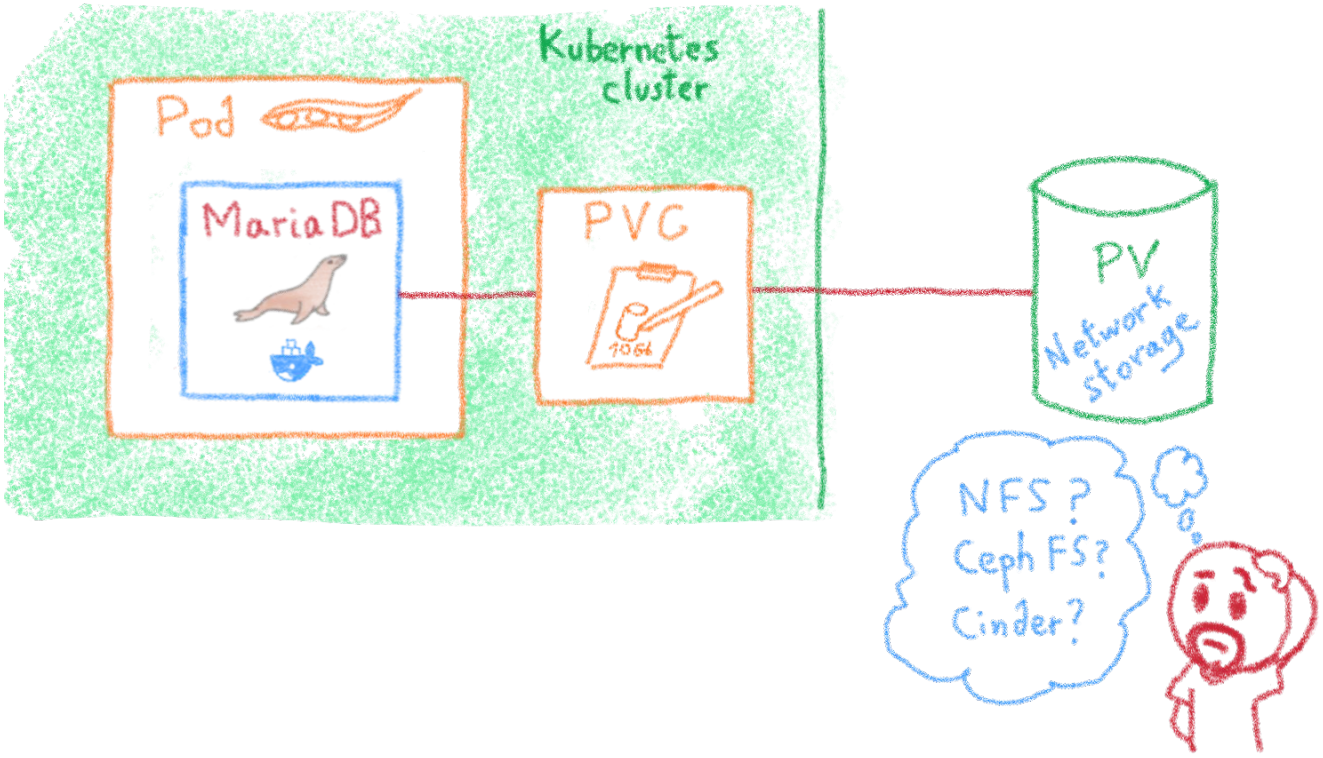
Network plugins (Flannel, Calico, Weave...)

- IPAM
- routing
- iptables
- crossnode networking

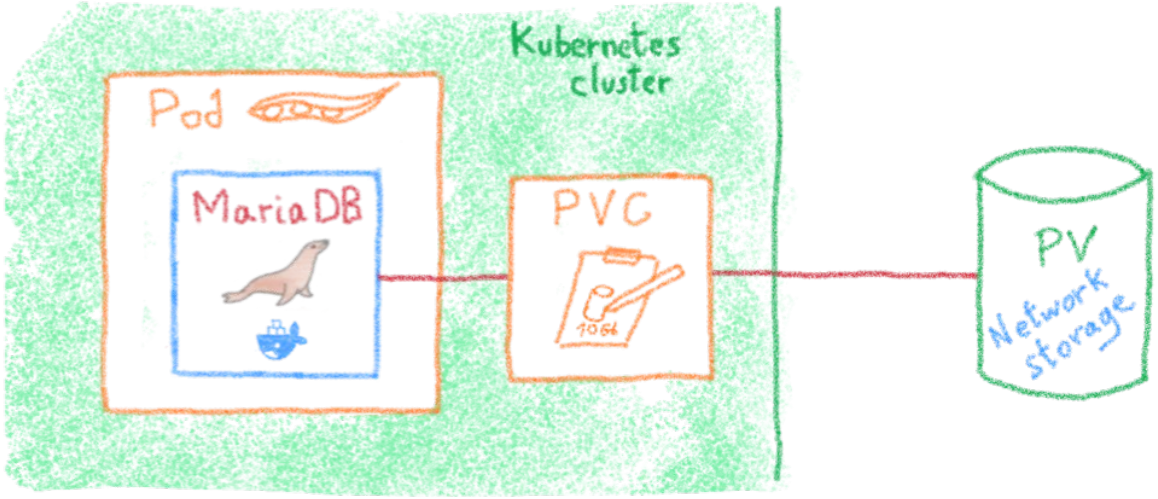
Cluster IP, NodePort, Ingress

Service Meshes, Istio

The storage dilemma



The storage dilemma

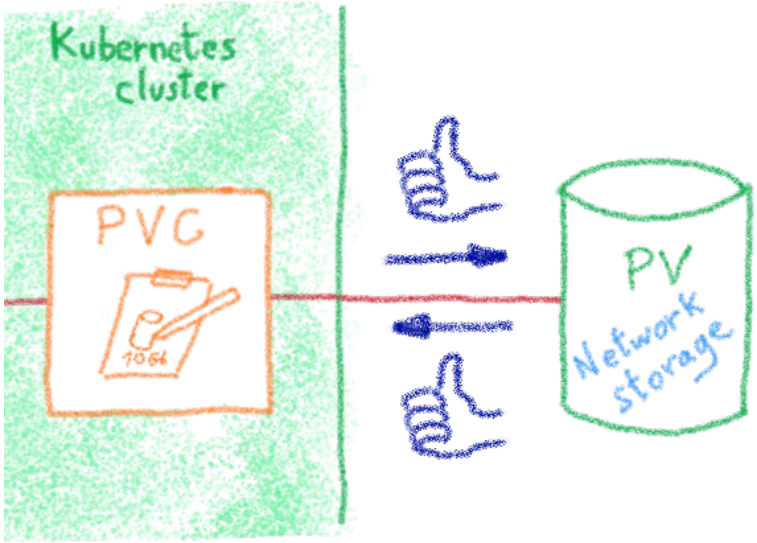


Volumes are handle through CSI

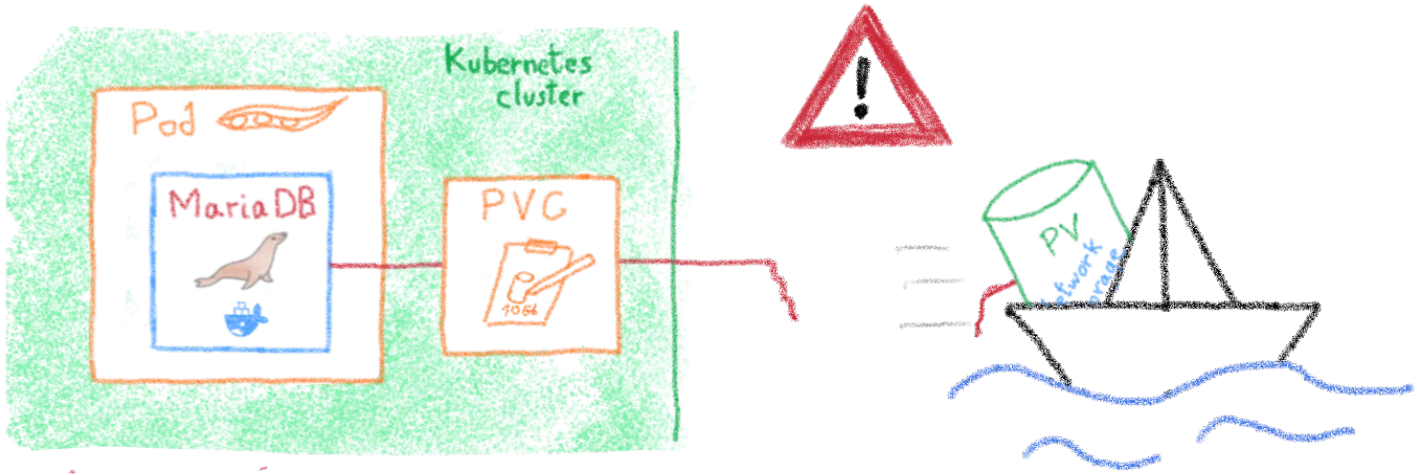
CSI provide an interface between Kubernetes and storage technologie

The storage dilemma

Most CSI assume
perfect sync
between Kubernetes and
the storage backend



The storage dilemma



Storage backend are subject to errors or maintenance

Potential state shifts between storage and Kubernetes

The storage dilemma

I0724 13:03:20.853645 1 csi_handler.go:100] Error processing "csi-afcb533080943": failed to attach: rpc error: code = NotFound desc = ControllerPublishVolume Volume not found

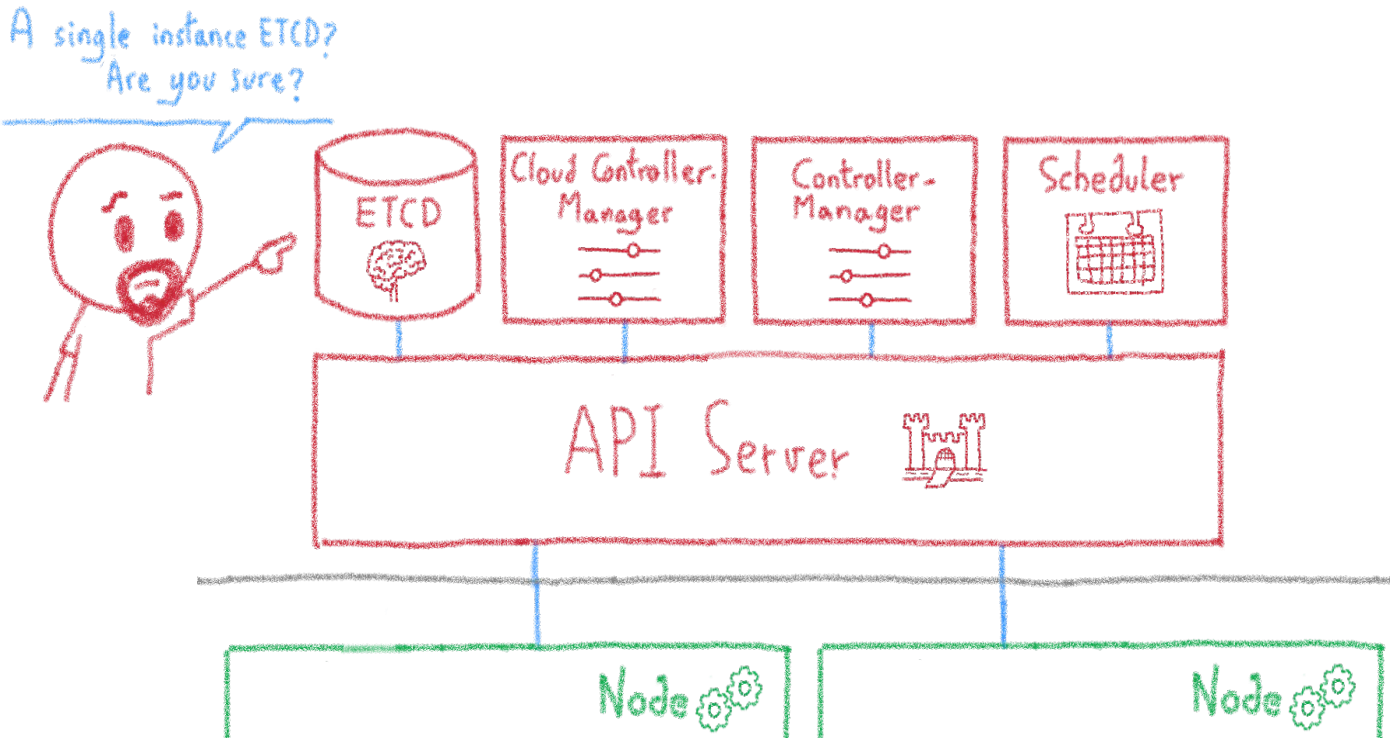
The storage dilemma

I0724 13:03:19.012008 1 csi_handler.go:100] Error processing "csi-2259b290c": failed to attach: rpc error: code = Internal desc = ControllerPublishVolume Attach Volume failed with error failed to attach 9aa1b78d-503d-49ec-8e51-11e7c7a2dee7 volume to ea295f86-9fa8-497a-aeb9-4ad27a99a8ce compute: Bad request with: [POST https://compute.cloud.net/v2.1/327b346ae2034427b84dd/servers/ea295f86-9fa8-497a-aeb9-4ad27a99b76de/os-volume_attachments], error message: {"badRequest": {"message": "Invalid input received: Invalid volume: Volume status must be available to reserve. (HTTP 400) (Request-ID: req-8c41d48a-9a32-4225-b423-8e84131a3db8)", "code": 400}}

The storage dilemma

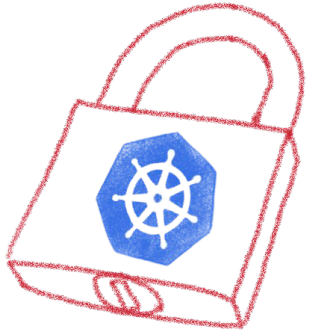
I0724 13:03:15.997499 1 csi_handler.go:100] Error processing "csi-69164e184900": failed to attach: rpc error: code = Internal desc = ControllerPublishVolume Attach Volume failed with error disk 57dbca1b-9611-4496-a960-ab13e355g23a is attached to a different instance (1621db21-b4af-4bd8-9419-954ed70gh892)

The ETCD vulnerability



Security

Hardening your Kubernetes



The security journey

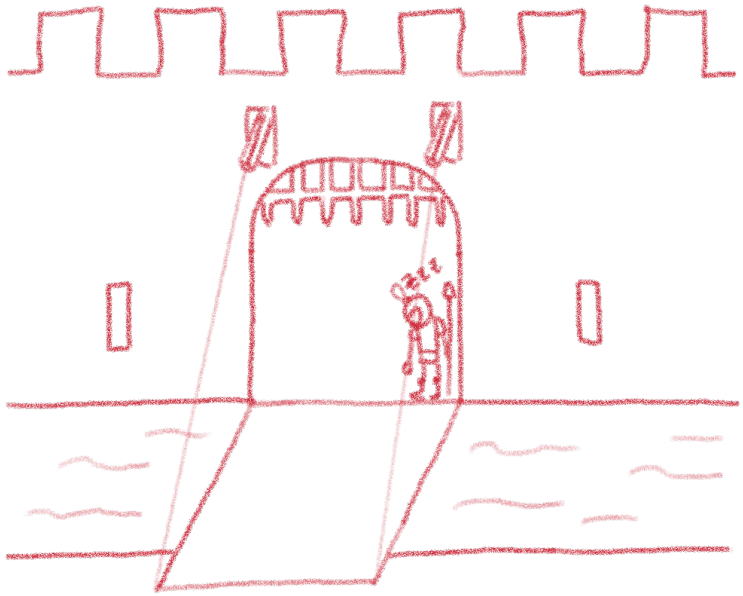
Mattias Gees
@MattiasGees

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)

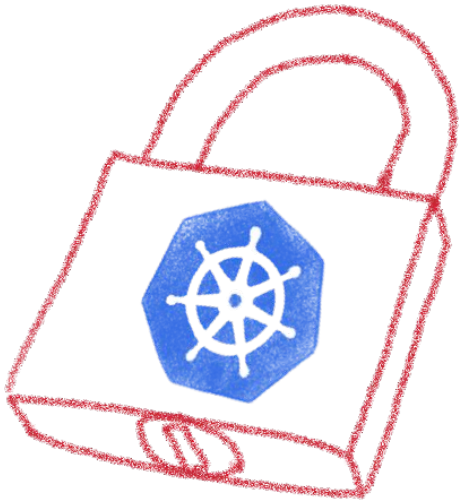
Kubernetes is insecure by design*



It's a feature, not a bug.
Up to K8s admin to secure it according to needs

Not everybody has the same security needs

Kubernetes allows to enforce security practices as needed



Listing some good practices

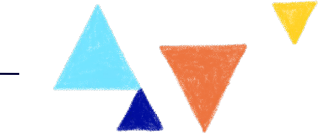
- Close open access
- Define and implement RBAC
- Define and implement Network Policies
- Isolate sensitive workloads

Security defaults

Kubernetes is insecure by default:

```
--anonymous-auth     Default: true
```

> Enables anonymous requests to the secure port of the API server. Requests that are not rejected by another authentication method are treated as anonymous requests. Anonymous requests have a username of system:anonymous, and a group name of system:unauthenticated.



Security defaults

Kubernetes is insecure by default:

```
--authorization-mode stringSlice     Default: [AlwaysAllow]
```

Ordered list of plug-ins to do authorization on secure port. Comma-delimited list of: AlwaysAllow,AlwaysDeny,ABAC,Webhook,RBAC,Node.

Close open access

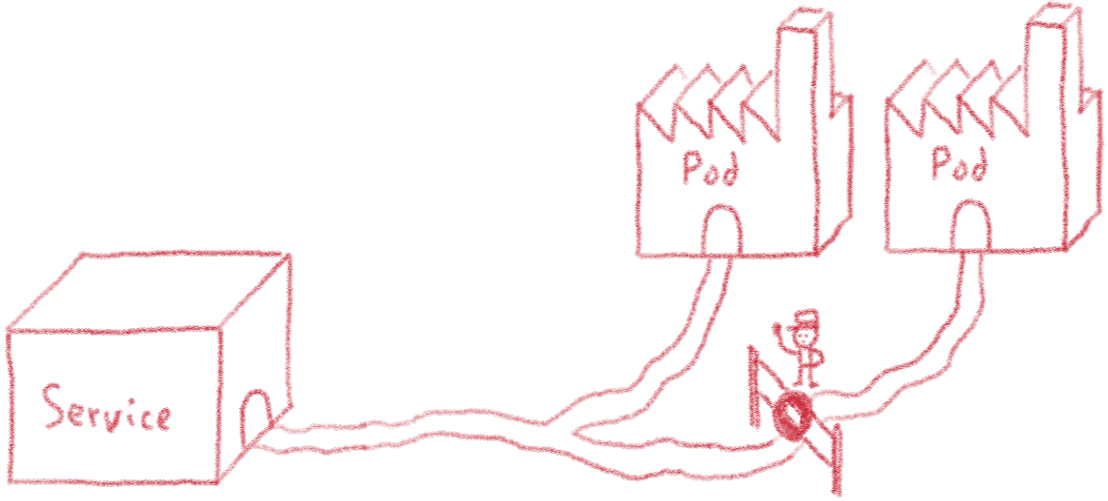
Close all by default, open only the needed ports

Follow the least privileged principle

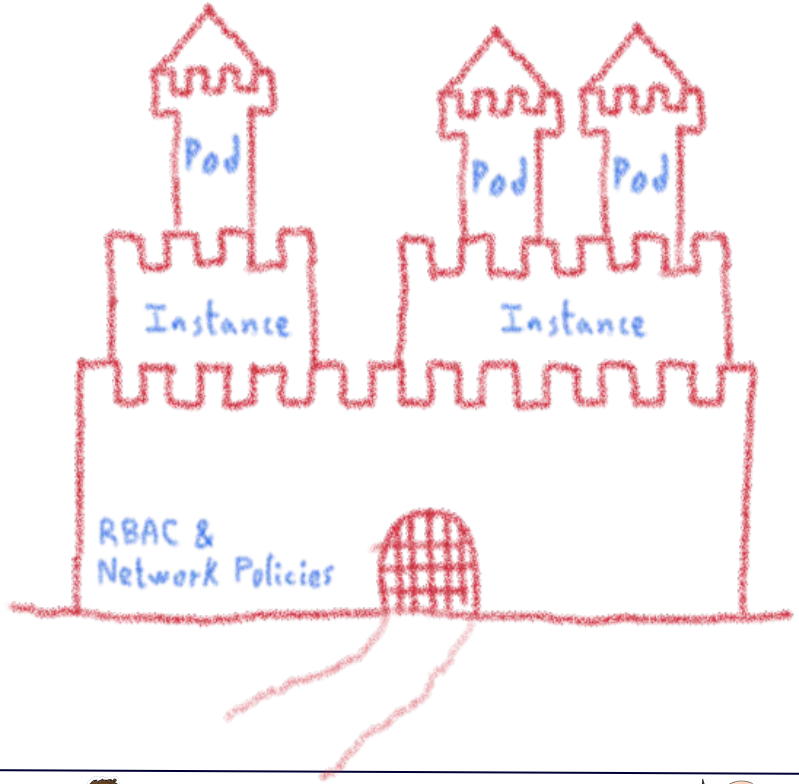
Define and implement RBAC

According to your needs

Define and implement network policies



Use RBAC and Network Policies to isolate your sensitive workload



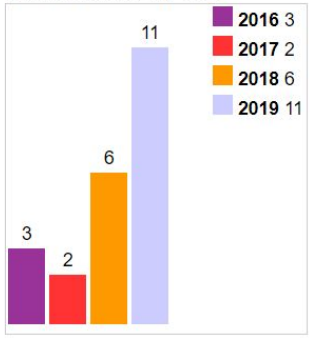
Always keep up to date

Both Kubernetes and plugins

Because Kubernetes is a big target

KubeCon CloudNativeCon Europe 2020 Virtual

Vulnerabilities By Year



Kubernetes » Kubernetes : Vulnerability Statistics

Vulnerabilities (22) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (0) Inventory Definitions (0) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2016	3										1	1			
2017	2										1				
2018	6									1					
2019	11	2									1				
Total	22	2								1	3	1			
% Of All		9.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.5	13.6	4.5	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not b years.)

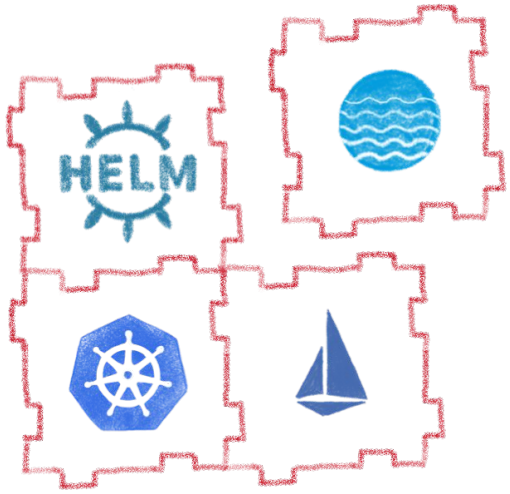
And remember, even the best can get hacked

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

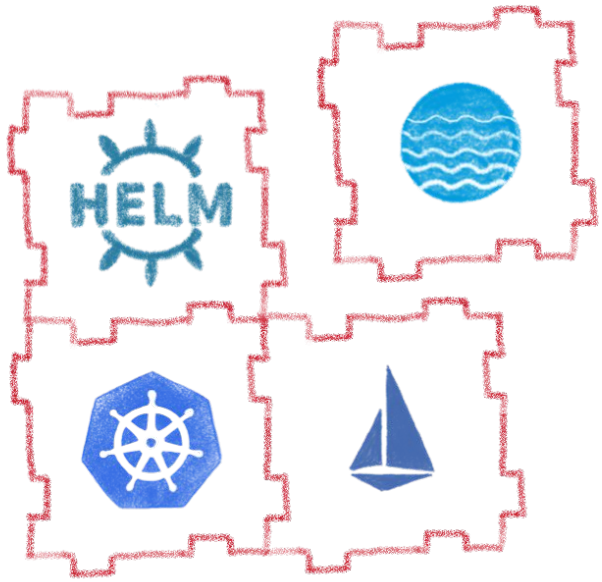
Remain attentive, don't get too confident

Extensibility

Enhance your Kubernetes



Kubernetes is modular



Fully extensible

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

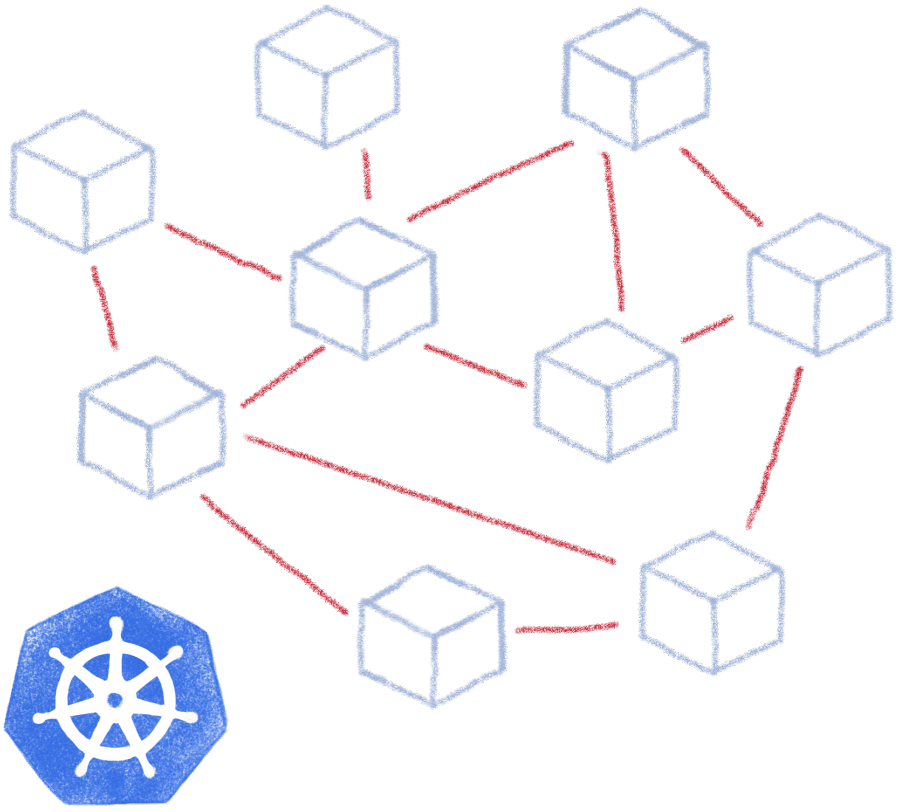
Operators

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

Helm

A package management for K8s

Complex deployments



Ingress

Services

Deployments

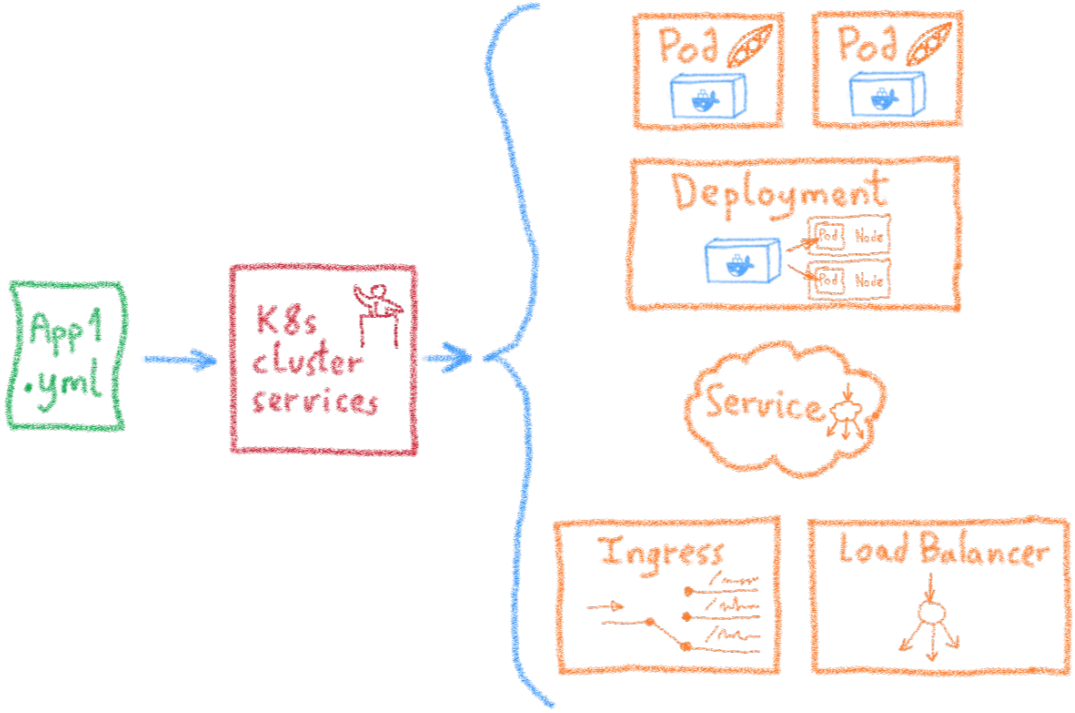
Pods

Sidecars

Replica Sets

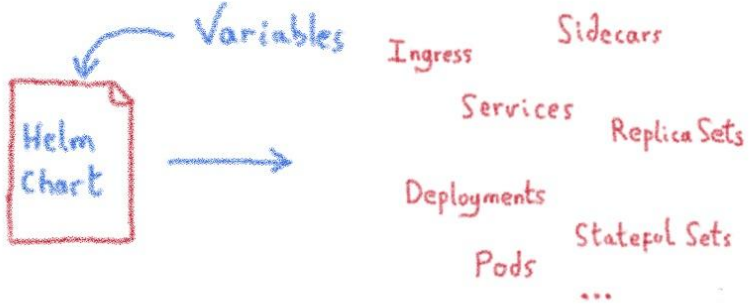
Statepul Sets

Using static YAML files



Complex deployments

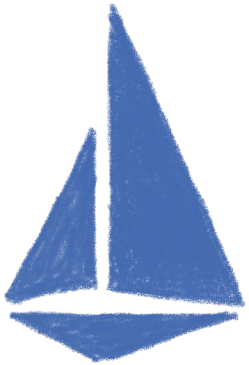
A package manager for Kubernetes



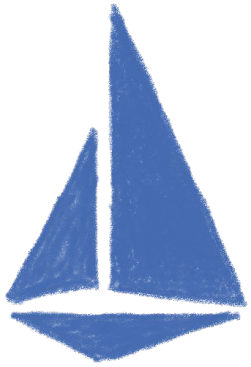
- Manage complexity
- Simple sharing
- Easy upgrades
- Easy rollbacks

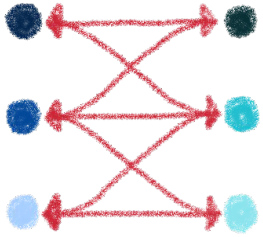
Istio

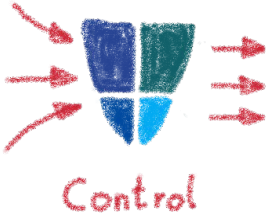
A service mesh for Kubernetes…
and much more!

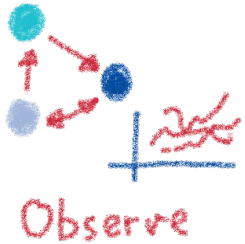


Istio: A service mesh…
but not only









Rolling upgrades

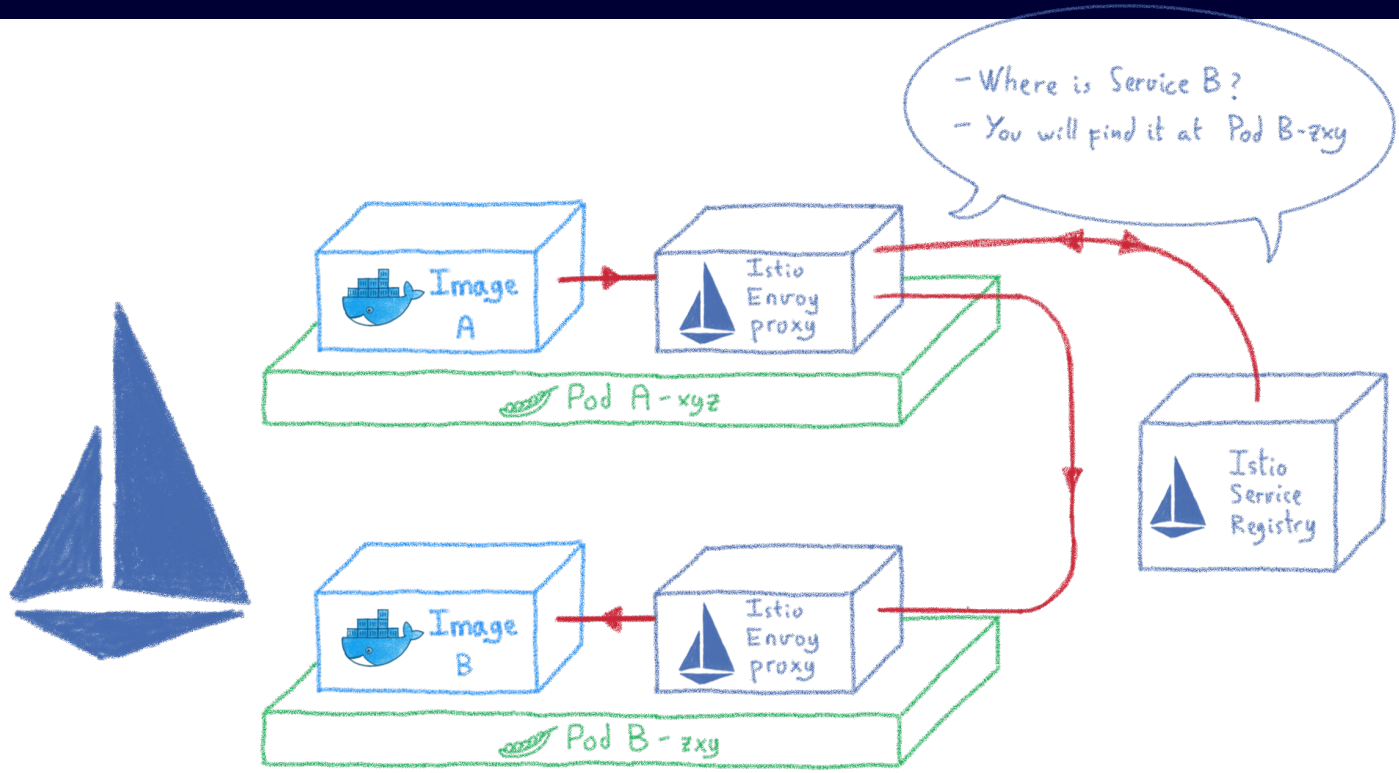
A/B Testing

Canary Testing

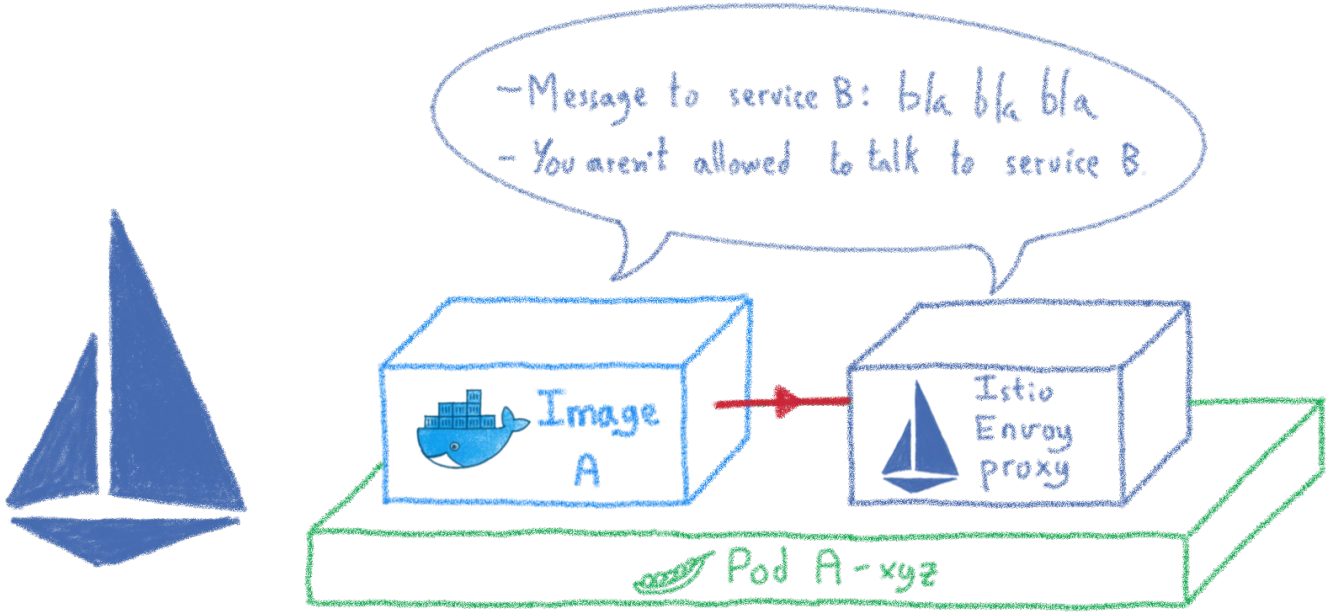
Edge traffic management

Multicluster service mesh

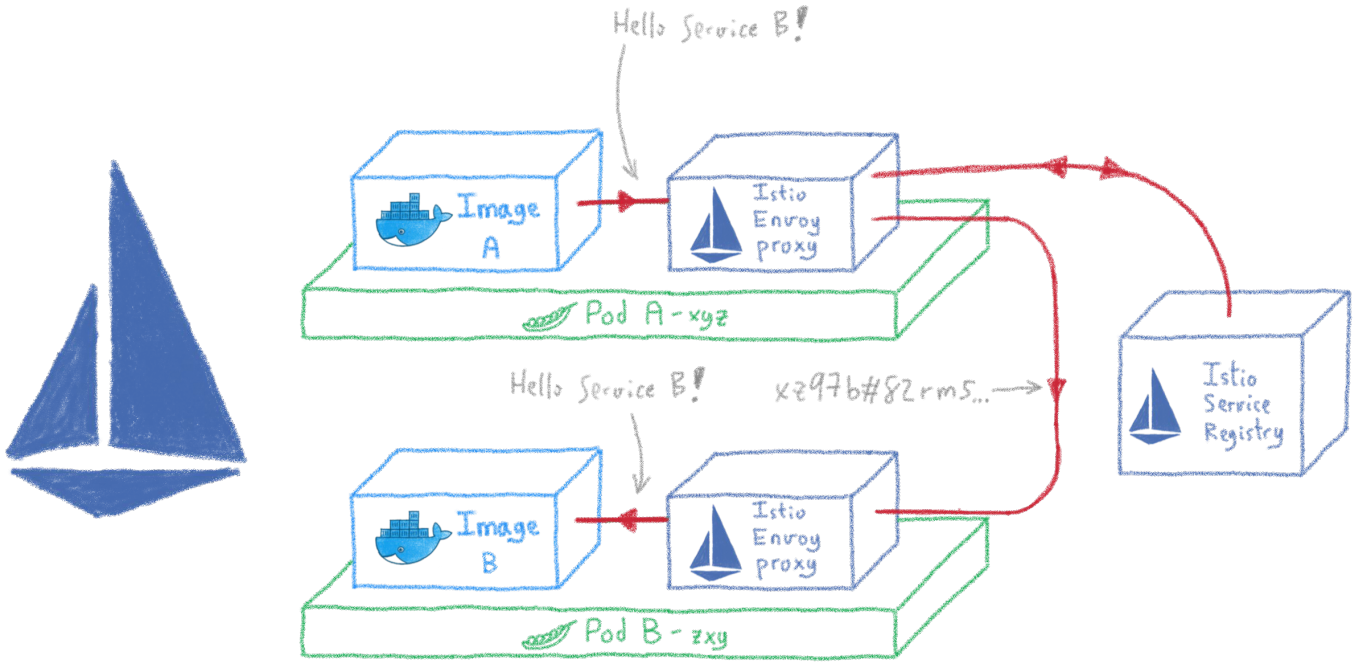
Service discovery



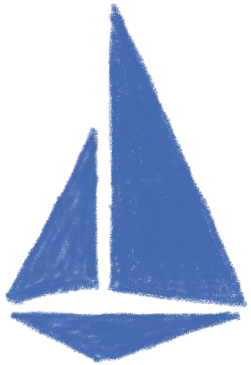
Traffic control

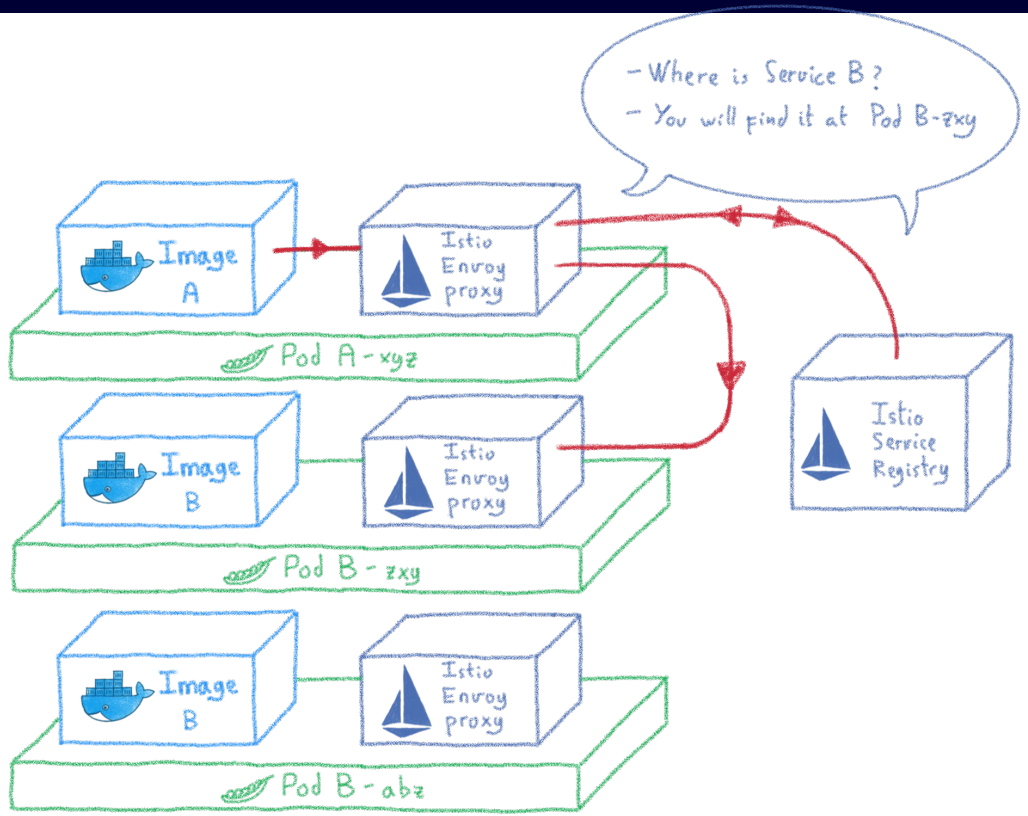


Encrypting internal communications

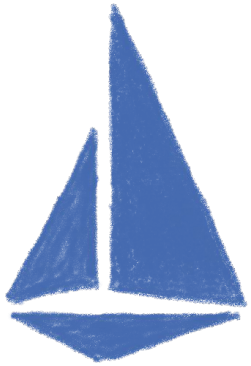


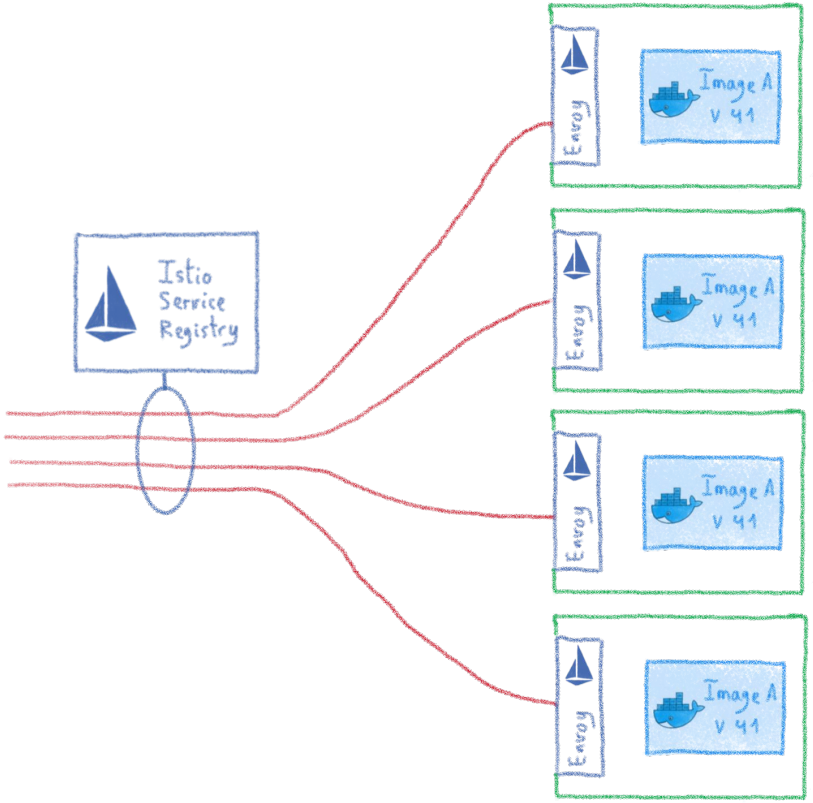
Routing and load balancing



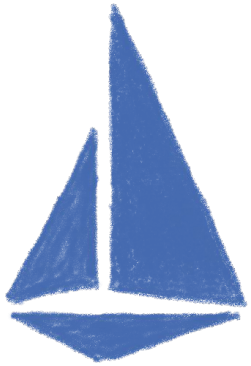


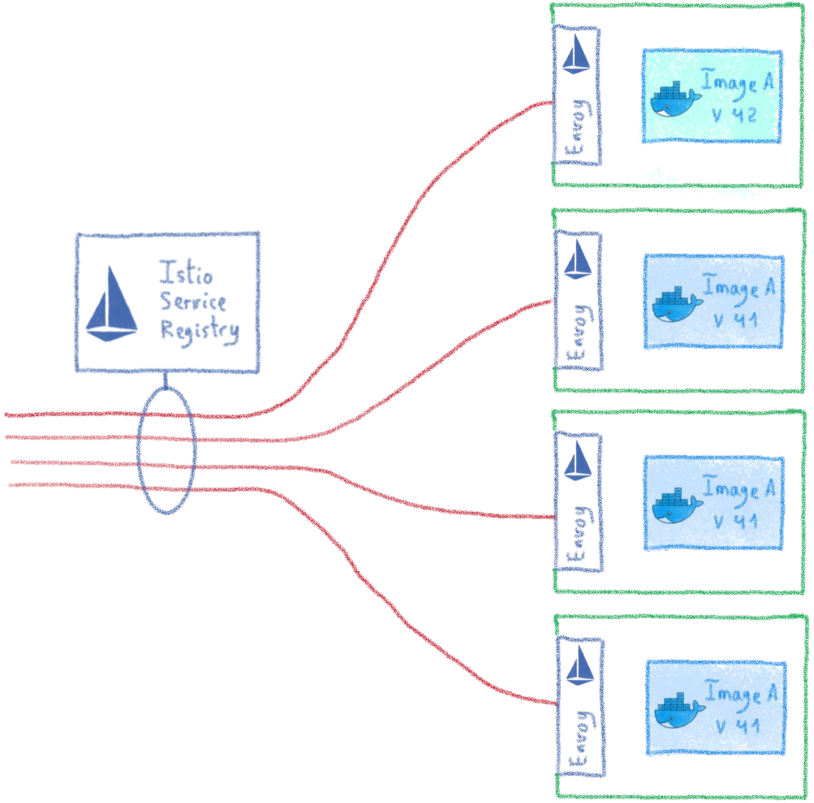
Rolling upgrades



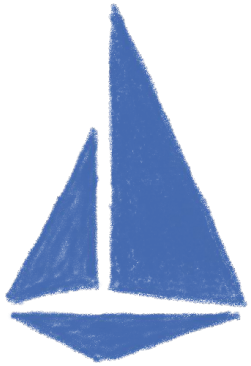


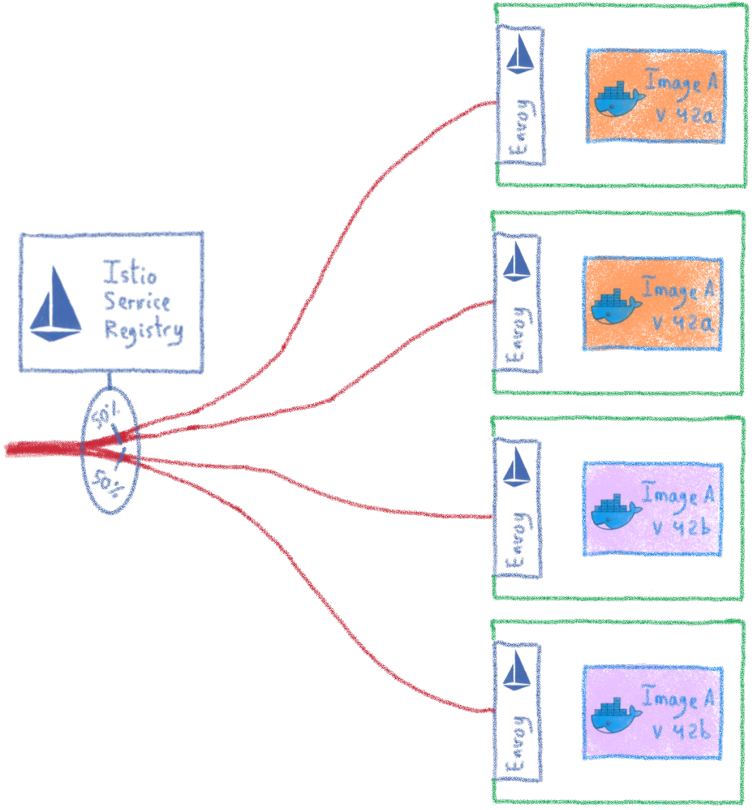
Rolling upgrades



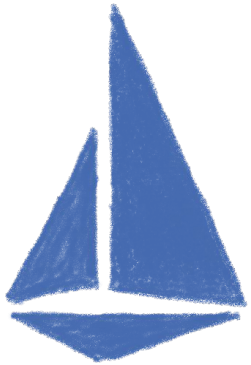


A/B testing




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

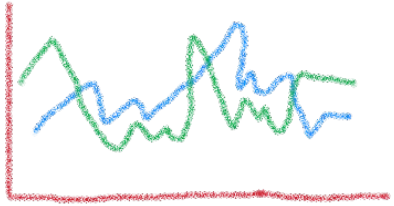
Monitoring your cluster



- Metrics
- Logs
- Tracing

} at {

- Envoy level
- Control plane level

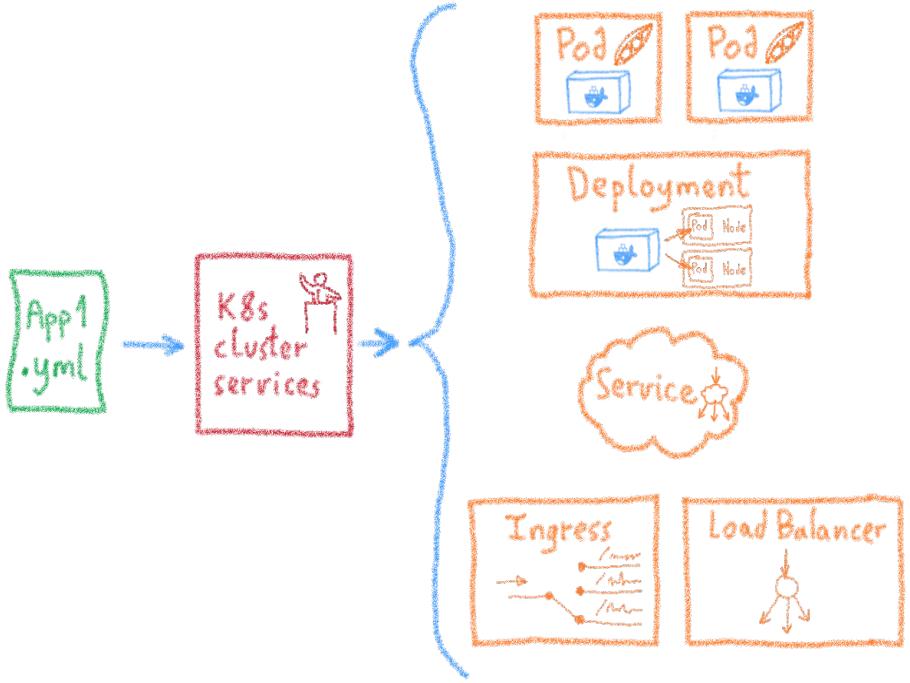


Dashboards

Velero

Backing up your Kubernetes

Kubernetes:
Desired State Management



Ingress

Services

Deployments

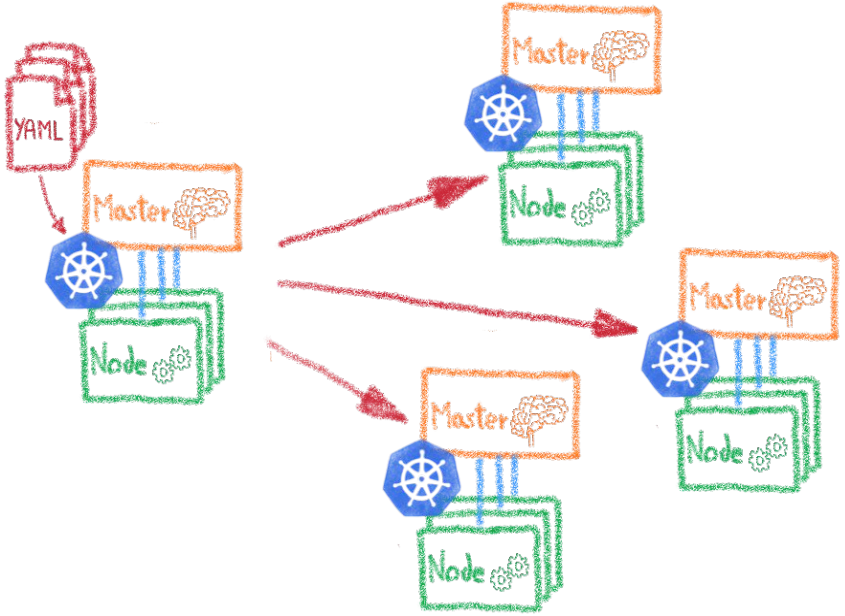
Pods

Sidecars

Replica Sets

Statepul Sets

YAML files allows to clone a cluster



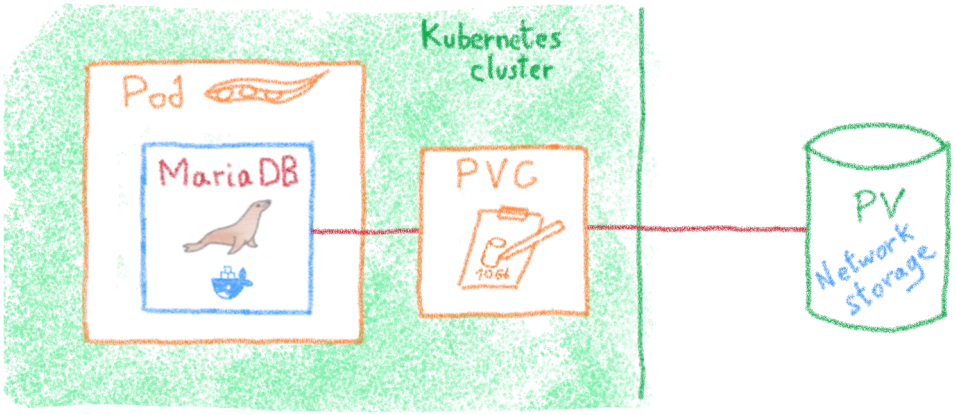
Dev envs

Staging

Multi-cluster

Multi-cloud

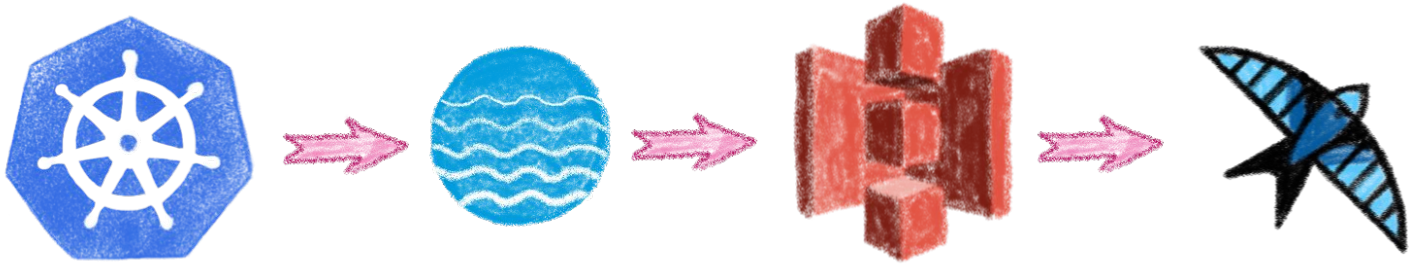
But what about the data?



Velero

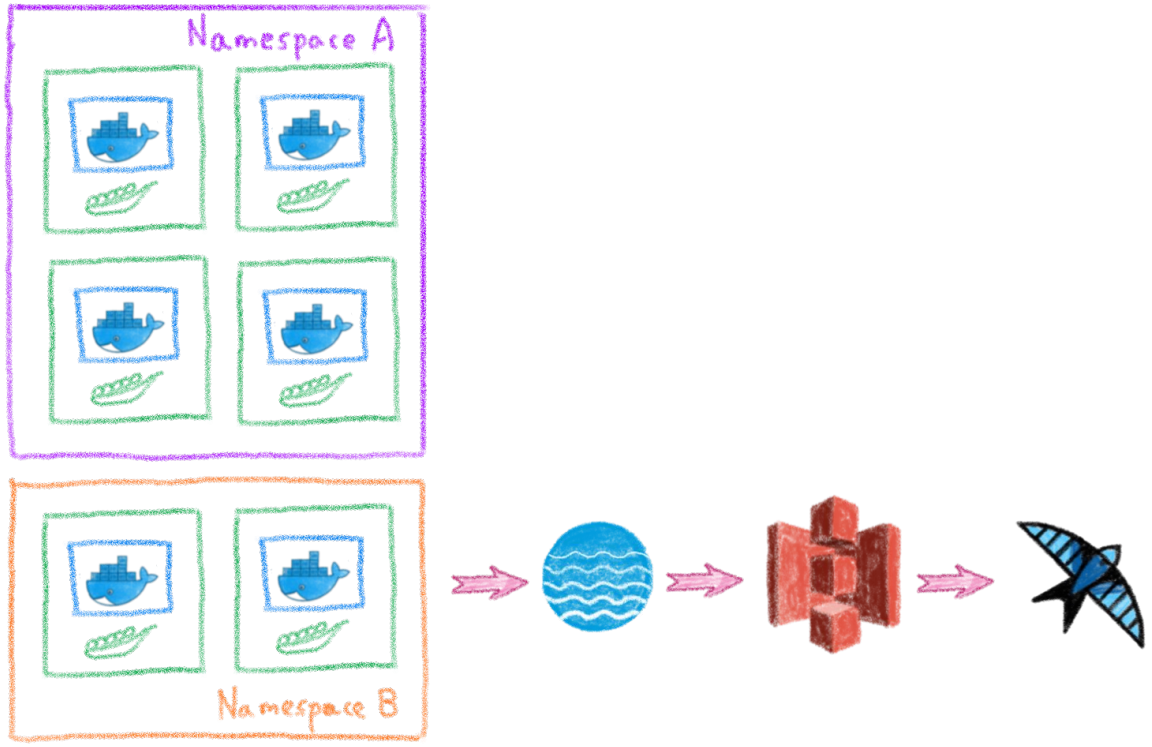
Backup and migrate Kubernetes applications and their persistent volumes

S3 based backup

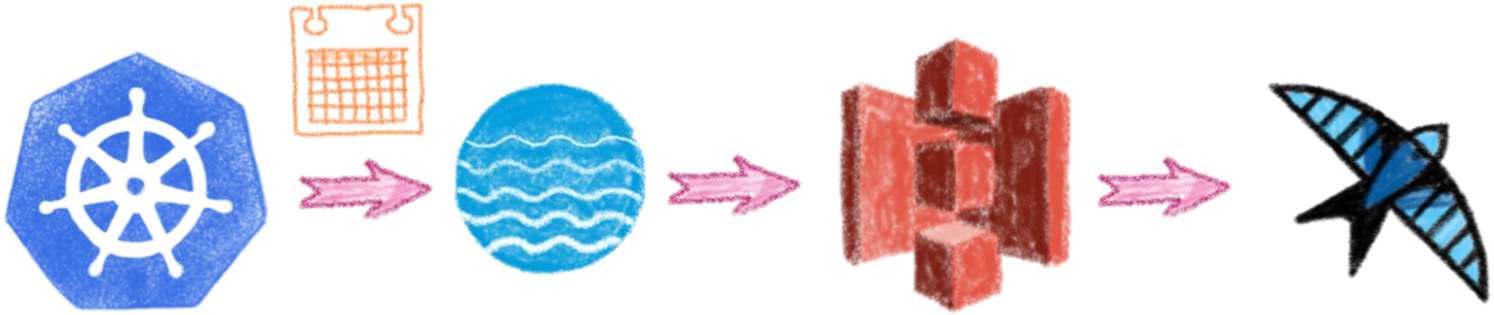


On any S3 protocol compatible store

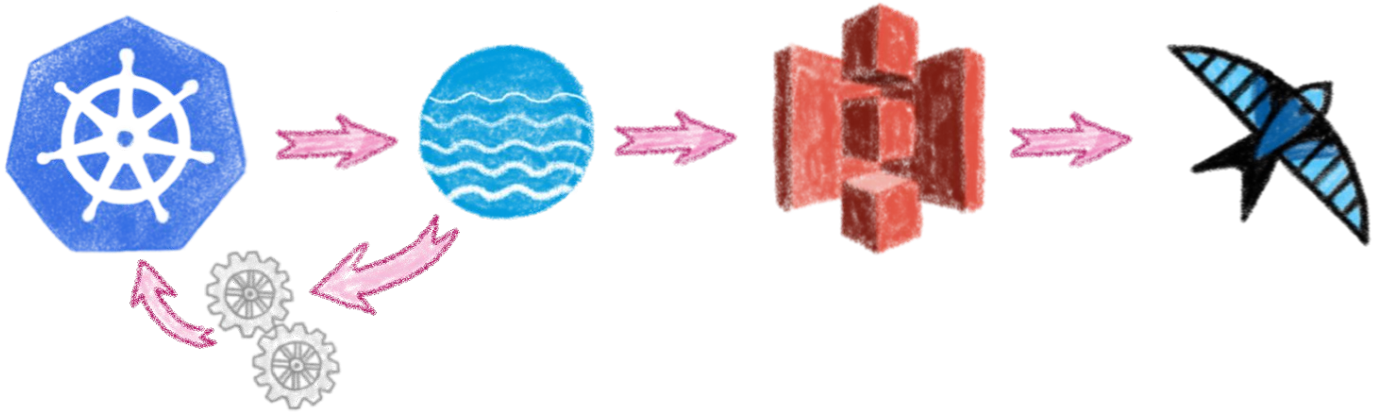
Backup all or part of a cluster



Schedule backups



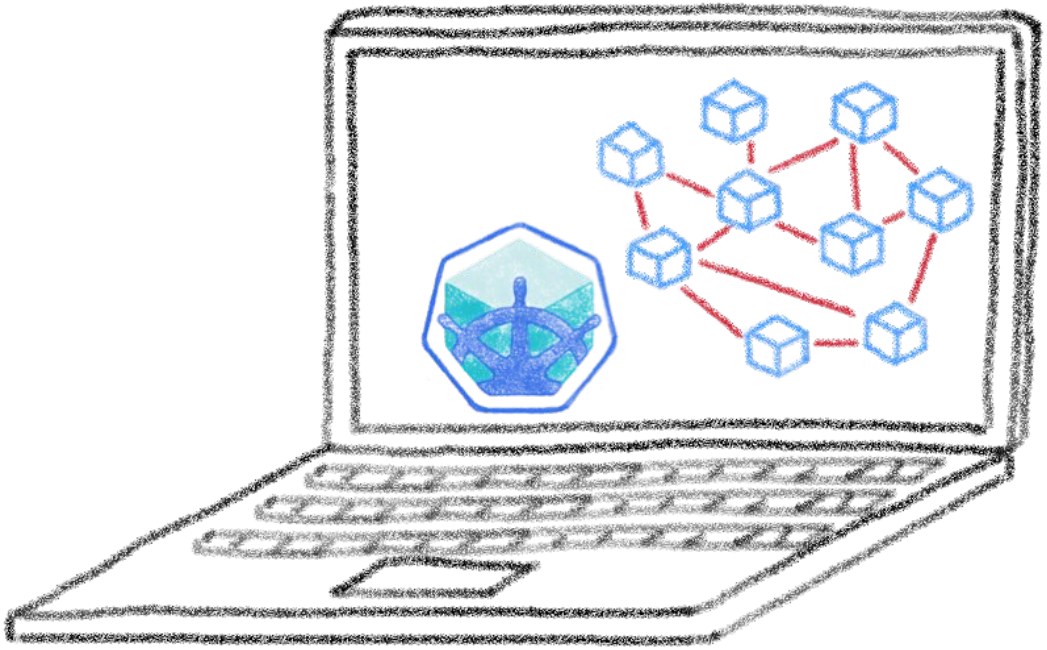
Backups hooks



Conclusion

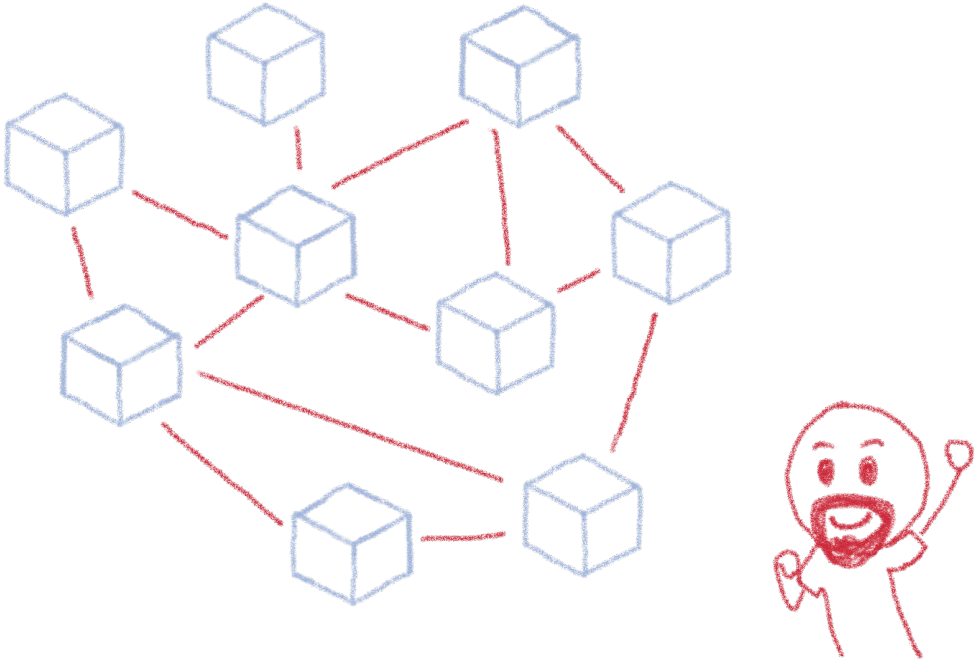
And one more thing...

Kubernetes is easy to begin with



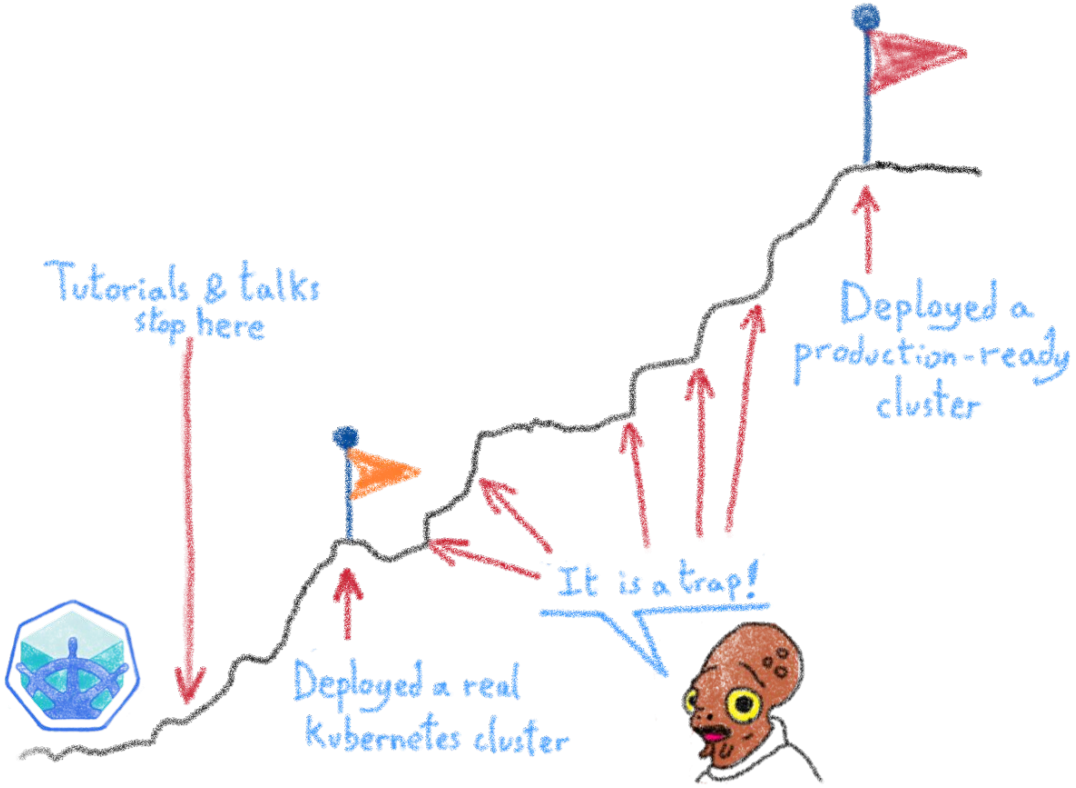
Minikube, K3s...

Kubernetes is powerful



It can make Developers' and DevOps' lives easier

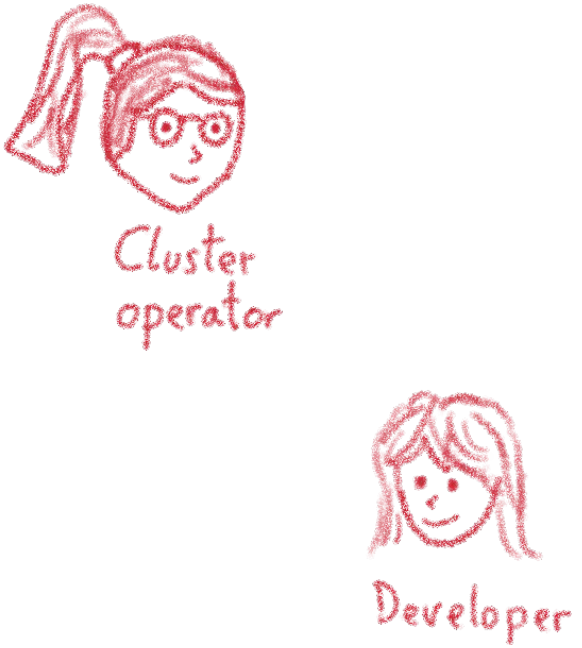
But there is a price: operating it



Lot of things to think about

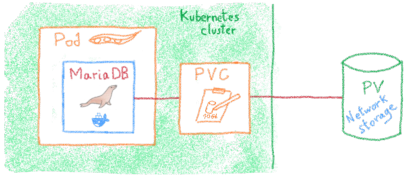
We have seen some of them

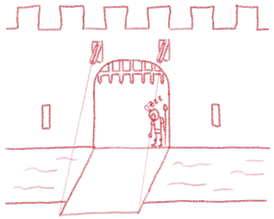
Different roles

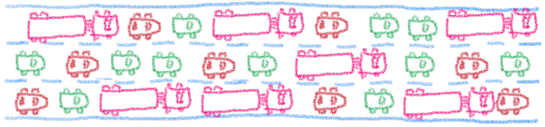


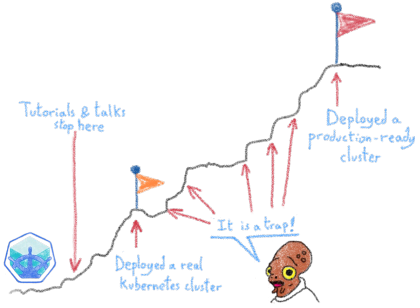
Each role asks for very different knowledge and skill sets

Operating a Kubernetes cluster is hard



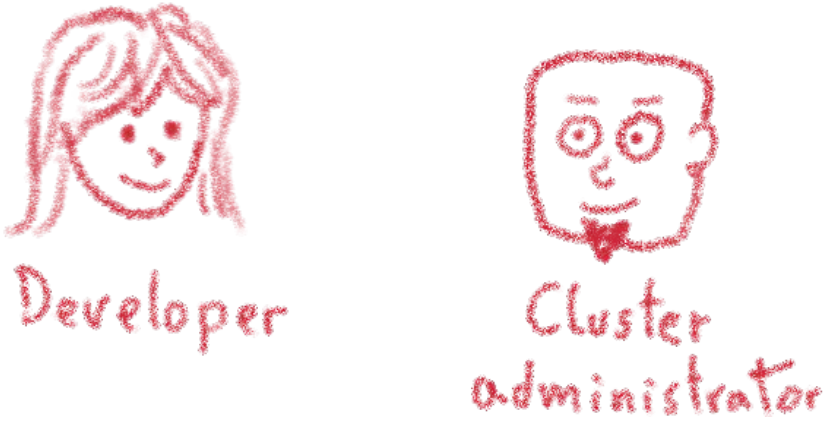






But we have a good news...

Most companies don't need to do it!



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

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

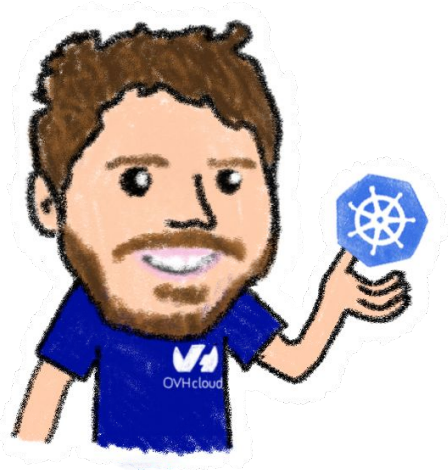
You get the cluster, the operator get the problems

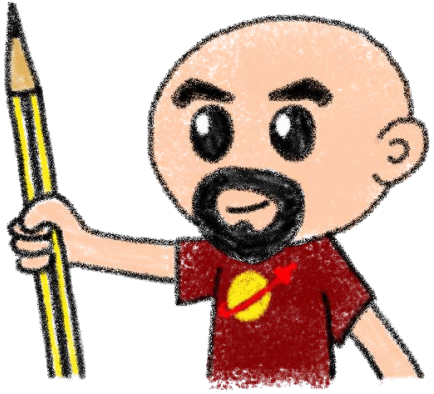
Like our OVH Managed Kubernetes

OVHcloud

Made with ❤ by the Platform team

Do you want to try?





Come to our (virtual) booth!

OVHcloud

Thank you for listening