



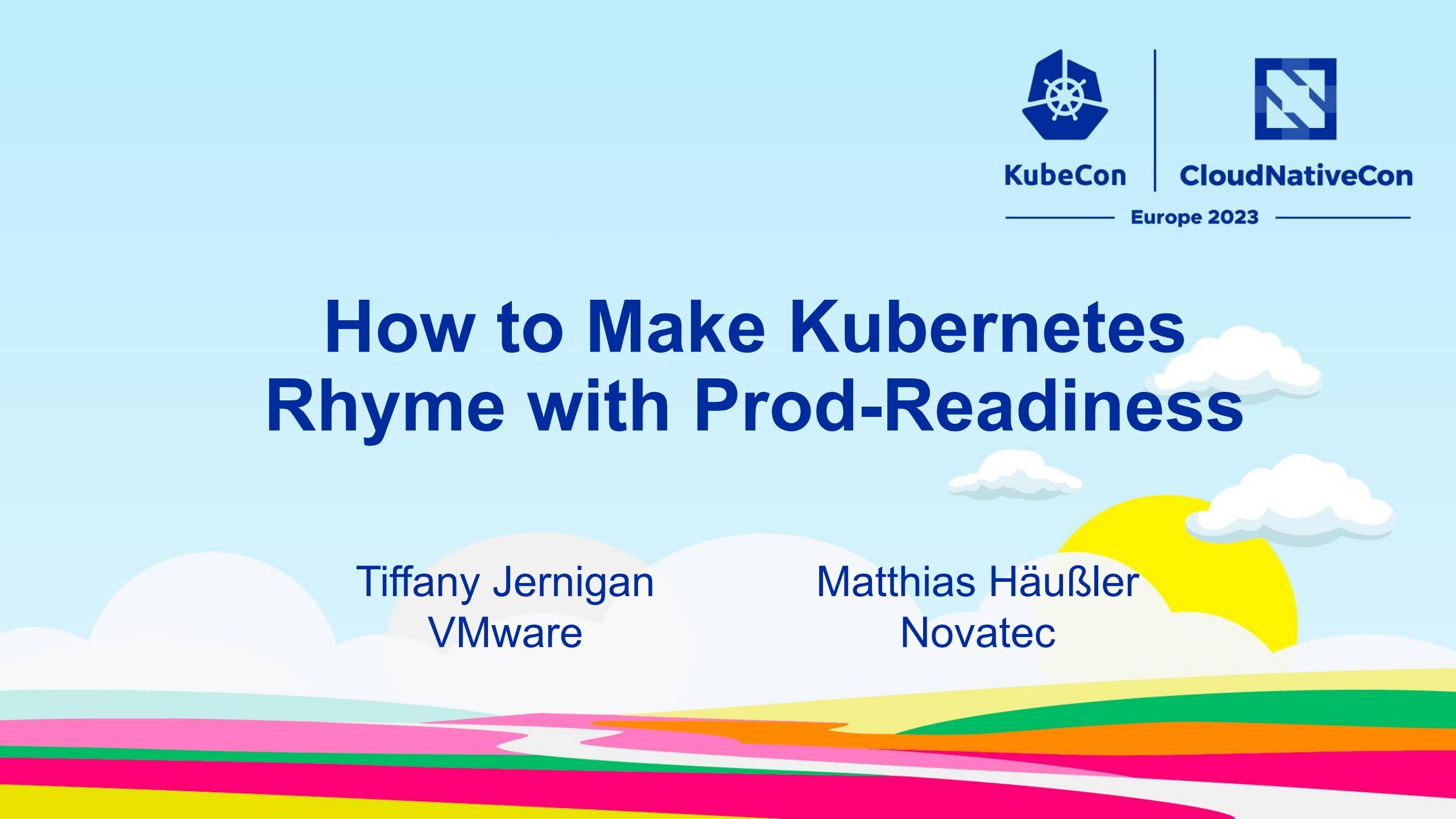
KubeCon



CloudNativeCon

Europe 2023

How to Make Kubernetes Rhyme with Prod-Readiness



Tiffany Jernigan
VMware

Matthias Häußler
Novatec

Who we are



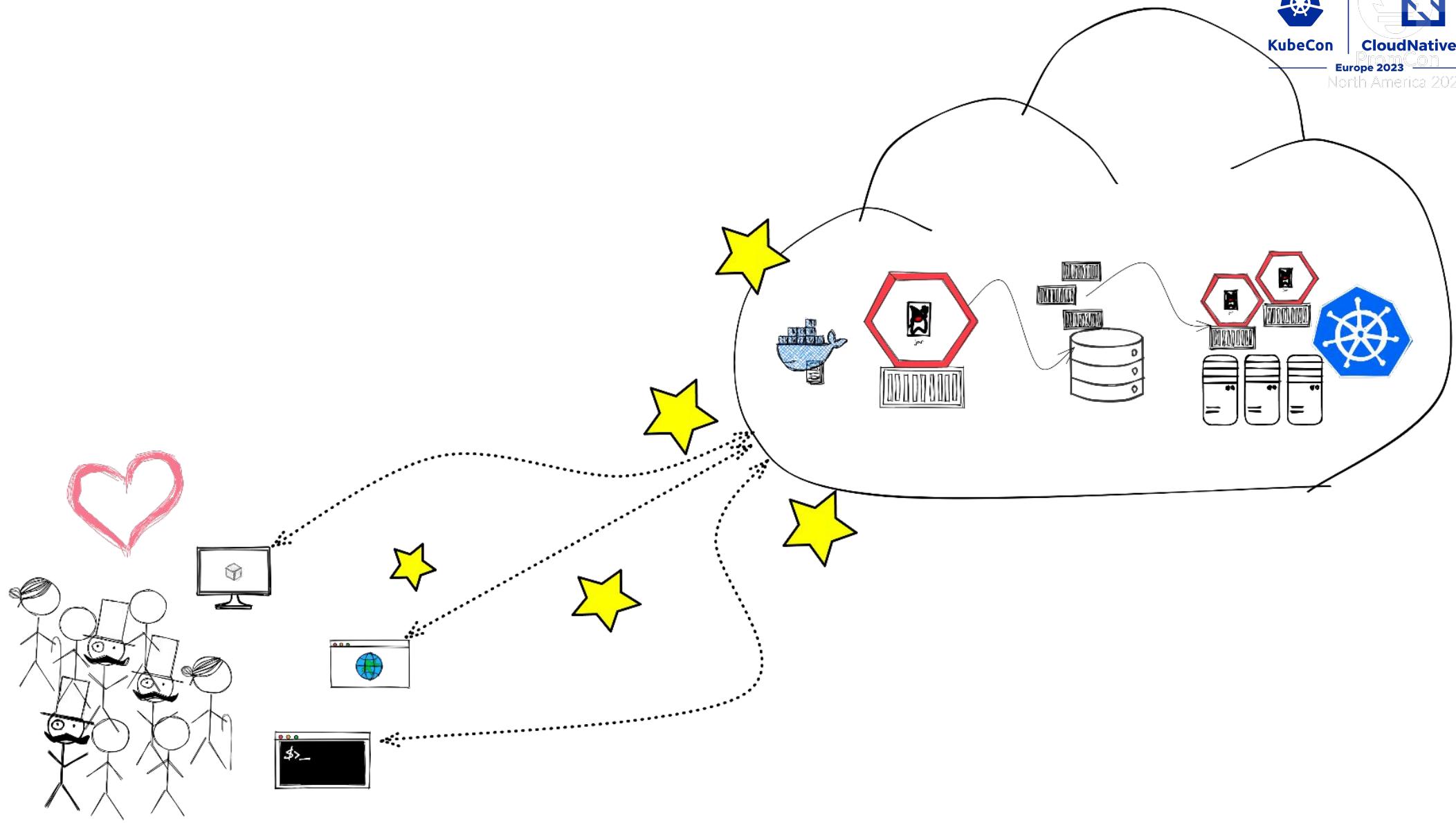
Tiffany Jernigan
Sr. Dev Advocate, VMware
@tiffanyfayj

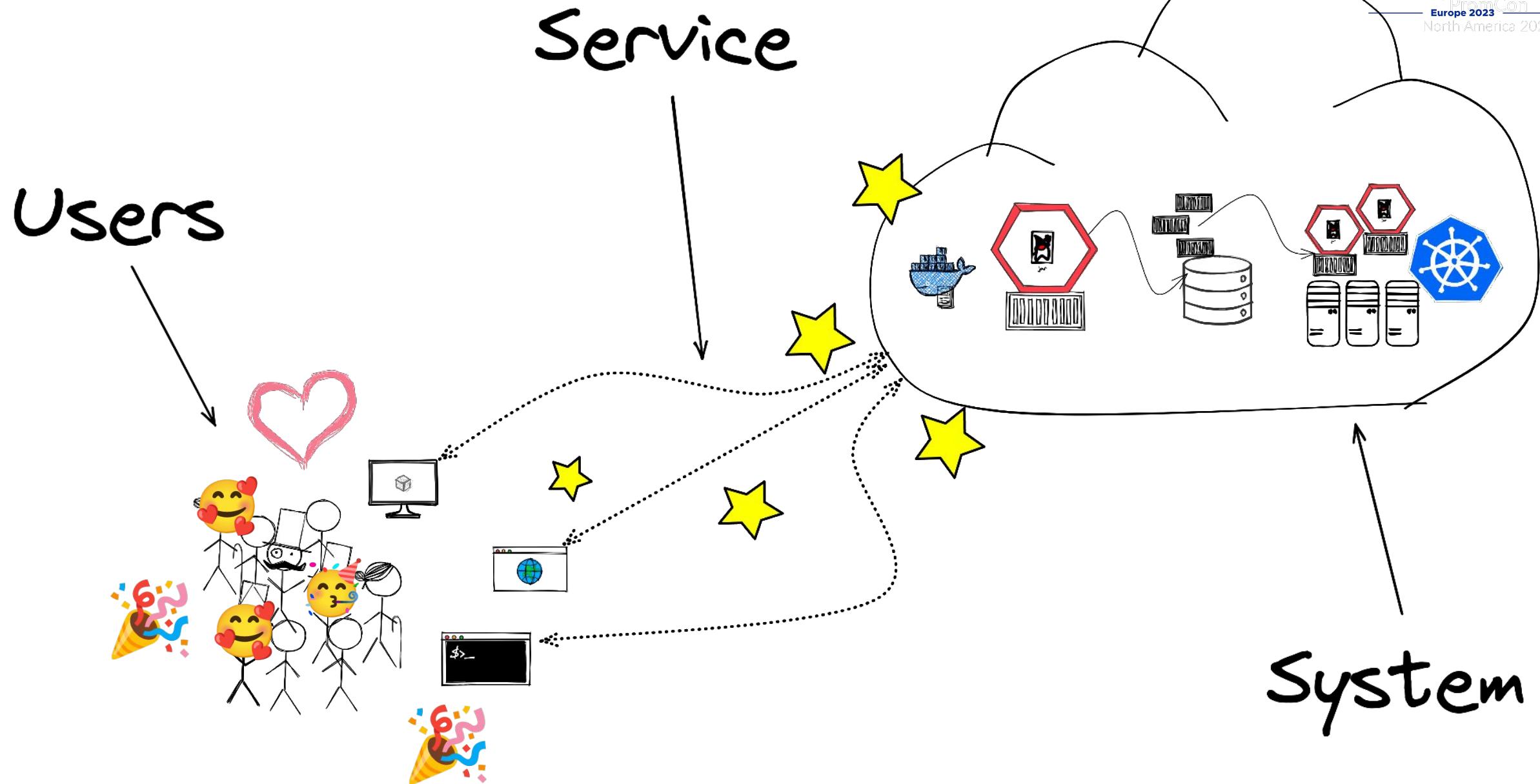
@maeddes @tiffanyfayj



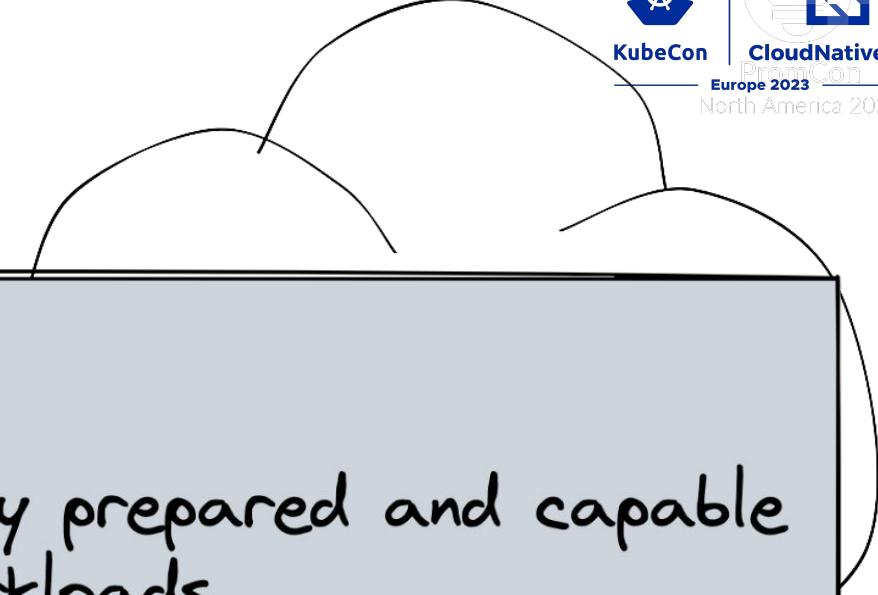
Matthias Häußler
Chief Technologist, Novatec
@maeddes

Why this talk?



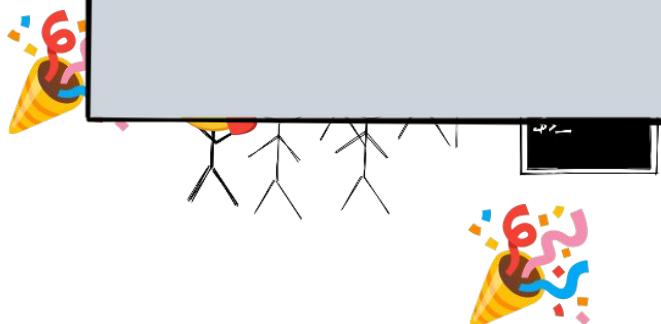


What is production readiness?



The state of a system which is fully prepared and capable of running prod workloads

Provides the level of service and performance required by its users



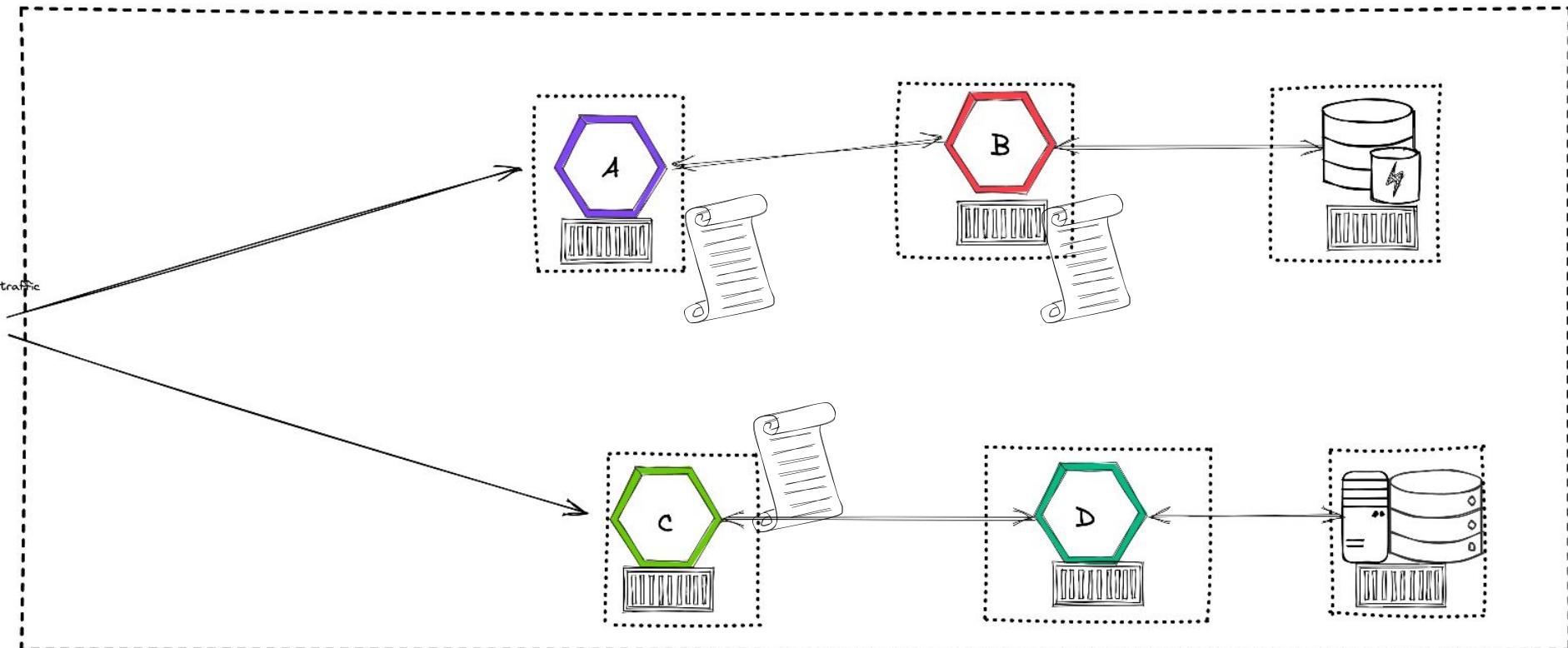
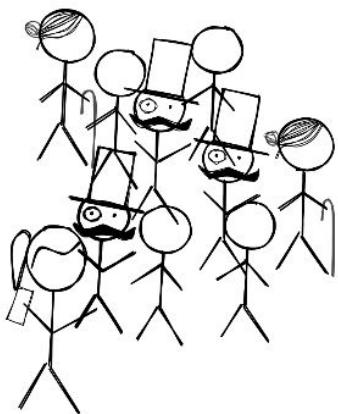
Prod readiness in detail

- Has undergone rigorous testing and quality assurance
- Ensured it's reliable, stable and secure
- Performs optimally under expected load and traffic conditions
- Adaptive to unexpected load/traffic conditions and failures
- Properly documented & described
- Consistently and repeatably buildable
- Monitored and Observable - Ability to identify and resolve issues quickly
- "Future-proofing": Being able to upgrade to patch security issues

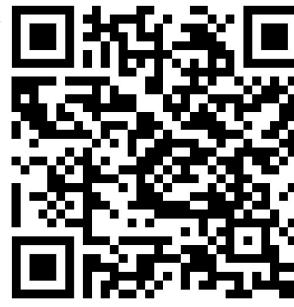
What does “vanilla” Kubernetes provide?



Kubernetes

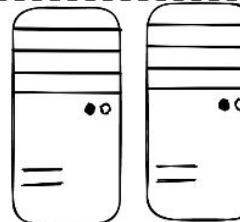
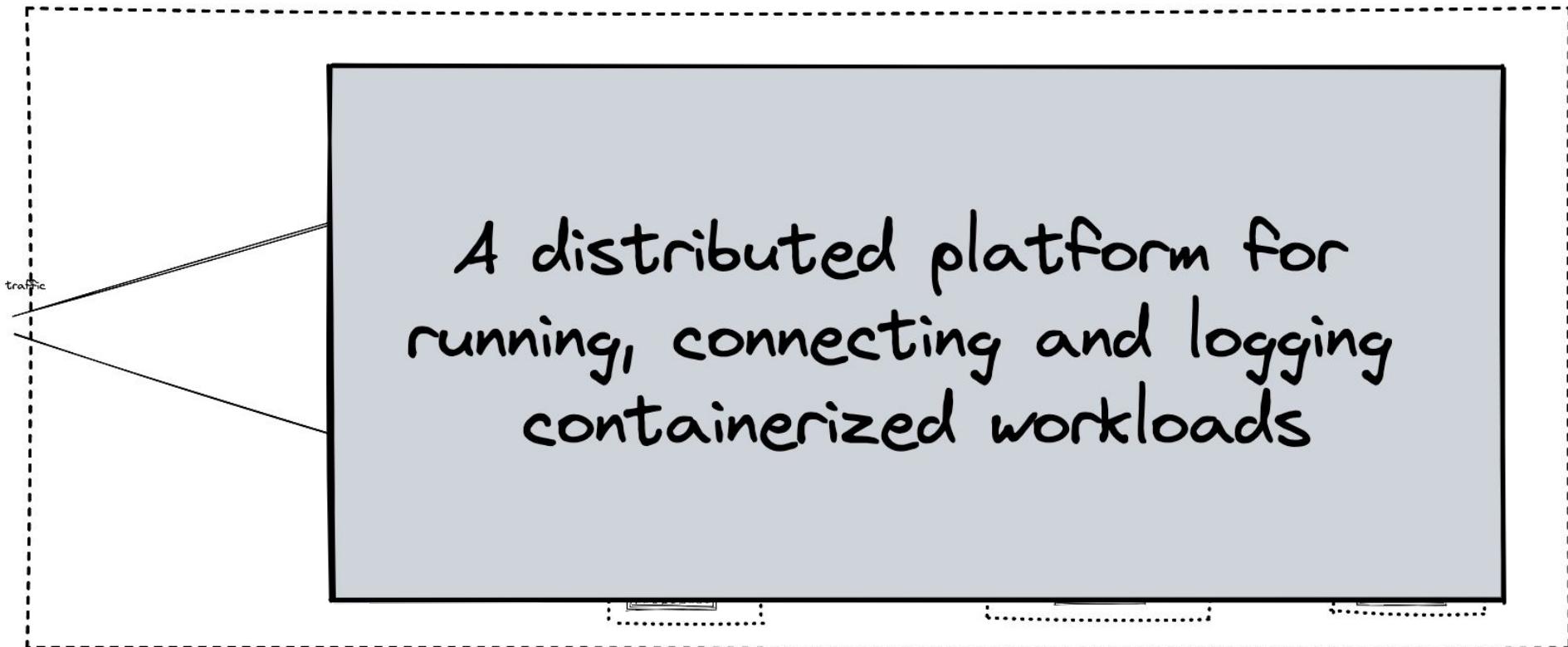
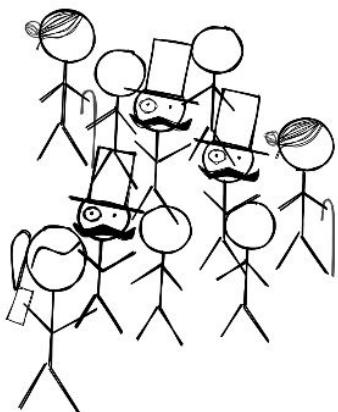


made by @maeddes with @excalidraw



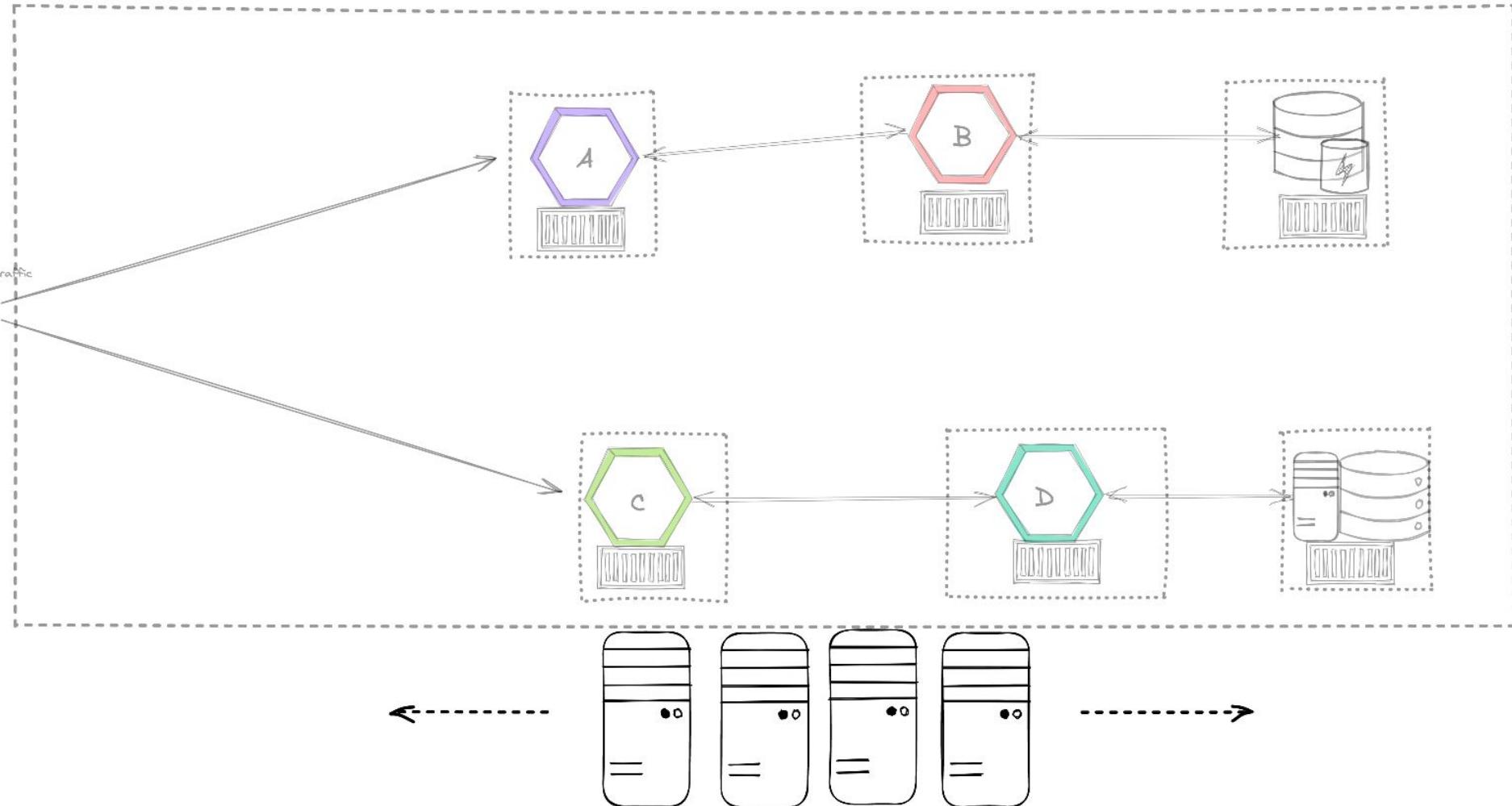
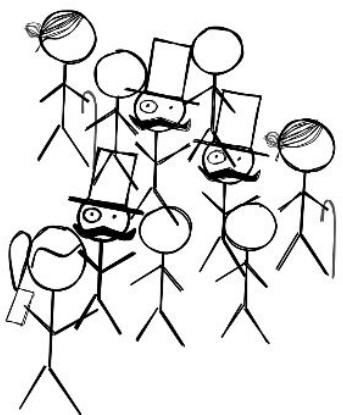


Kubernetes



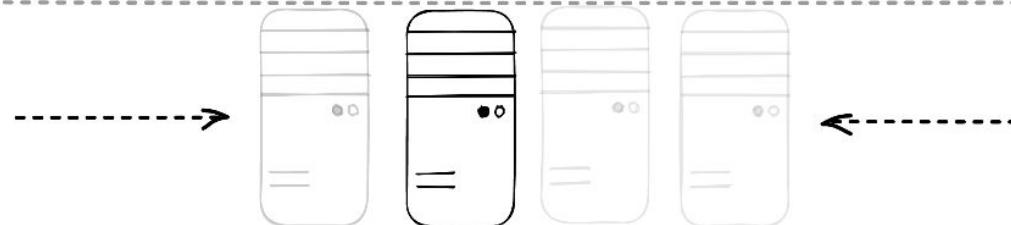
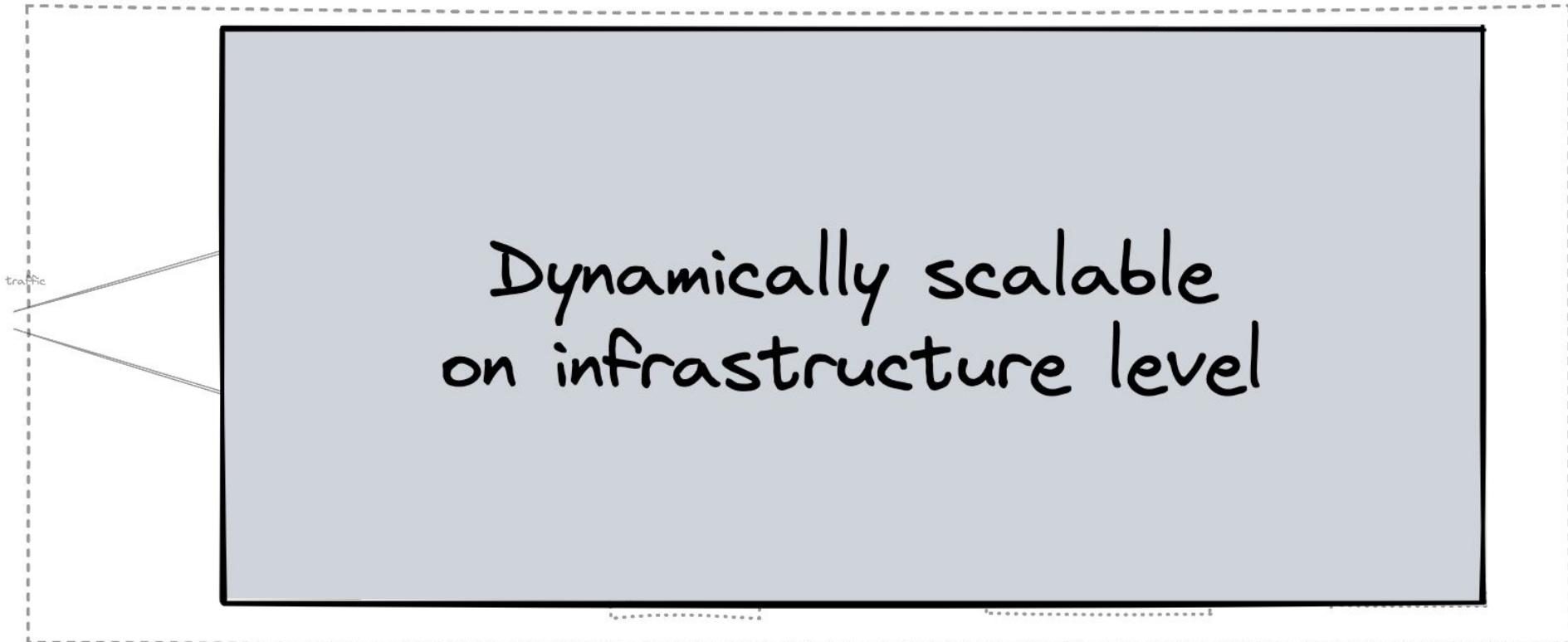
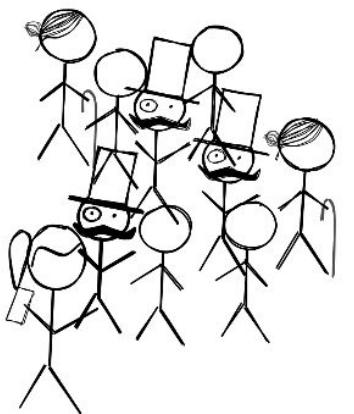


Kubernetes

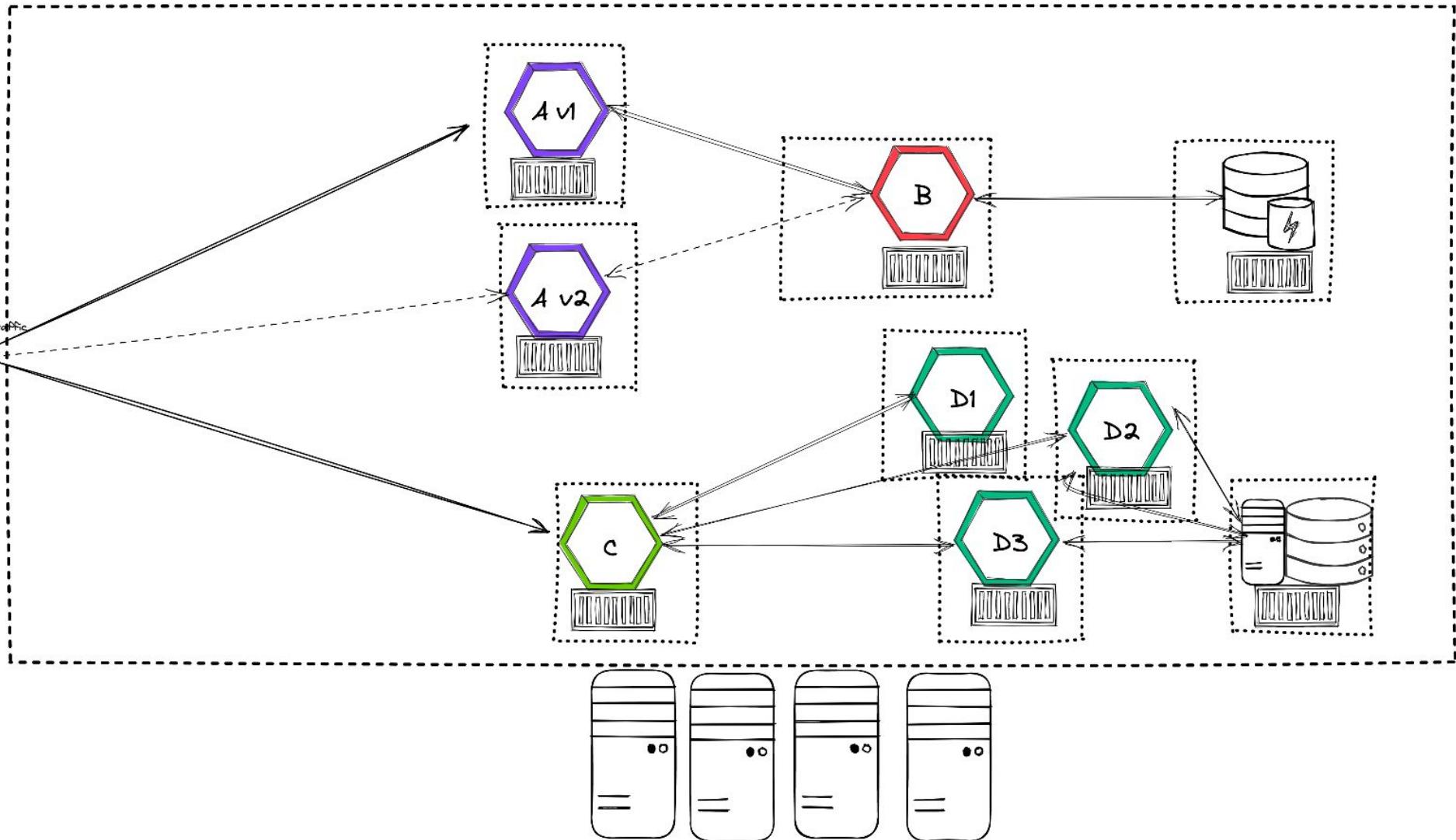
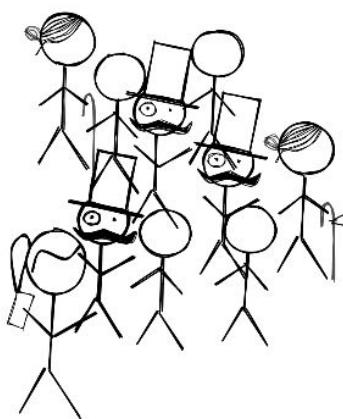




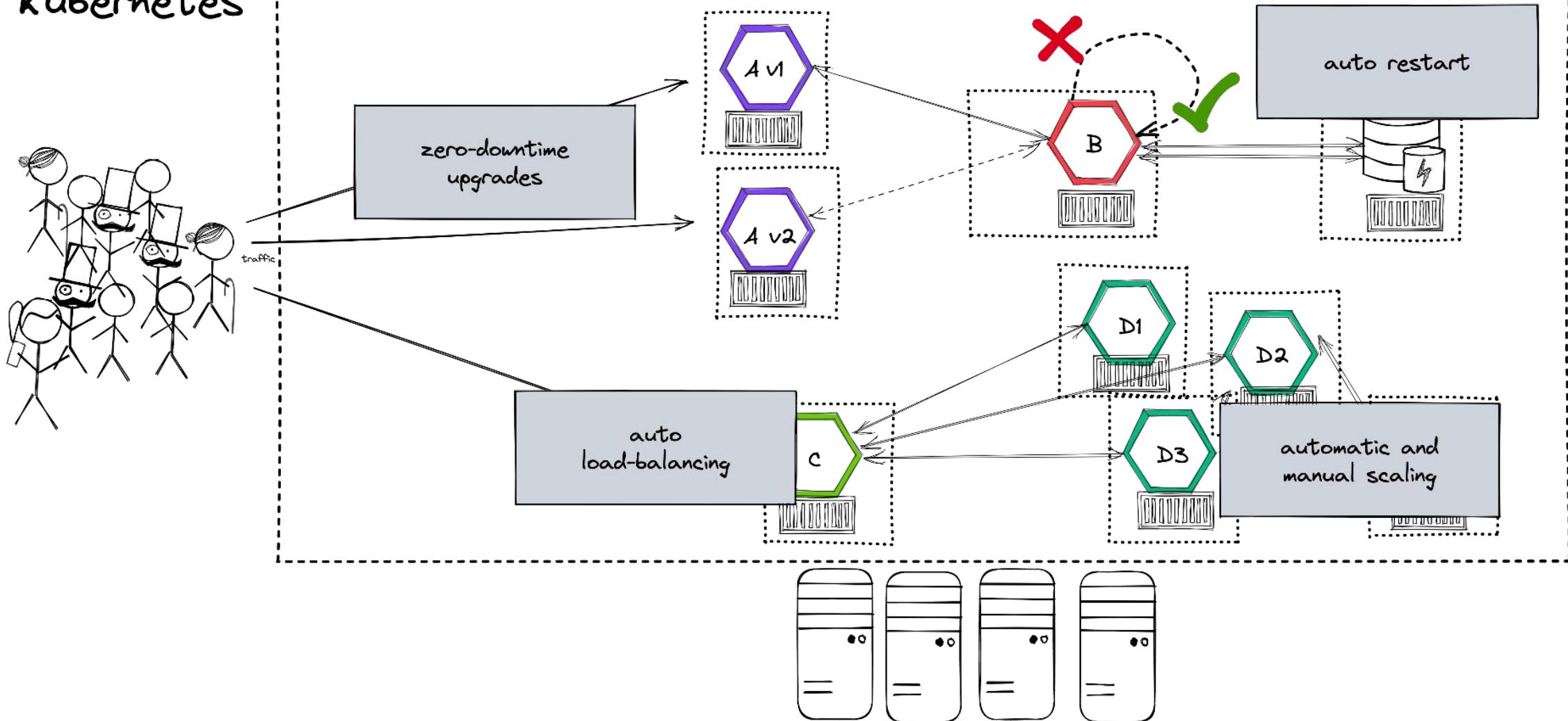
Kubernetes



Kubernetes



Kubernetes

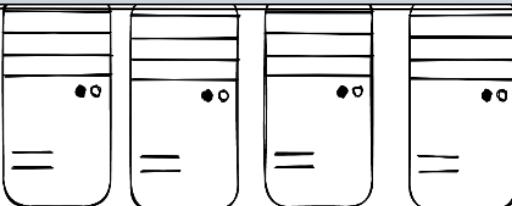


Kubernetes



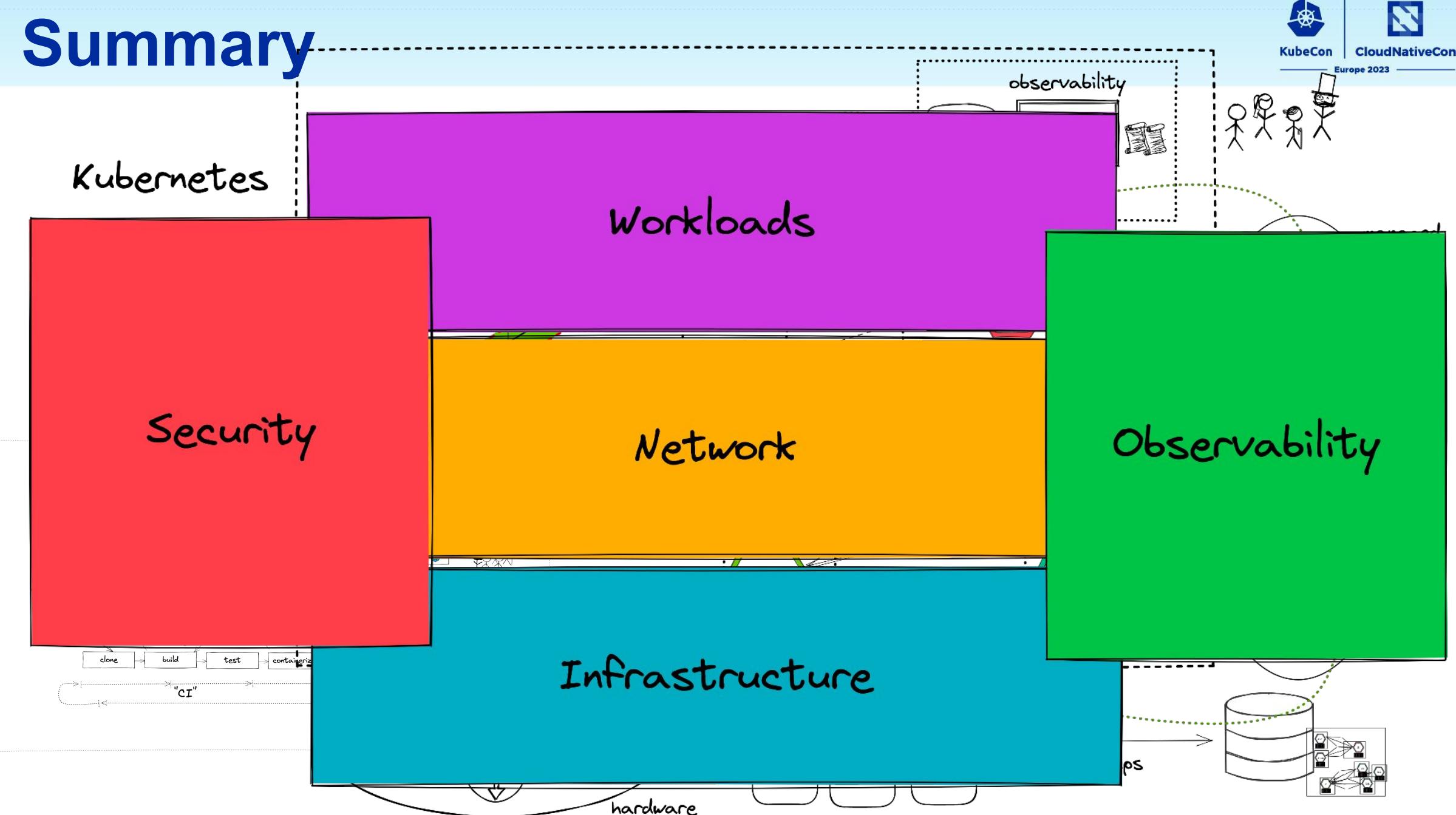
Summary of "core" Kubernetes - focus on:

- High-Availability and Resilience of workloads
- Fault tolerance
- Elasticity (infrastructure / workloads)
- Extensibility

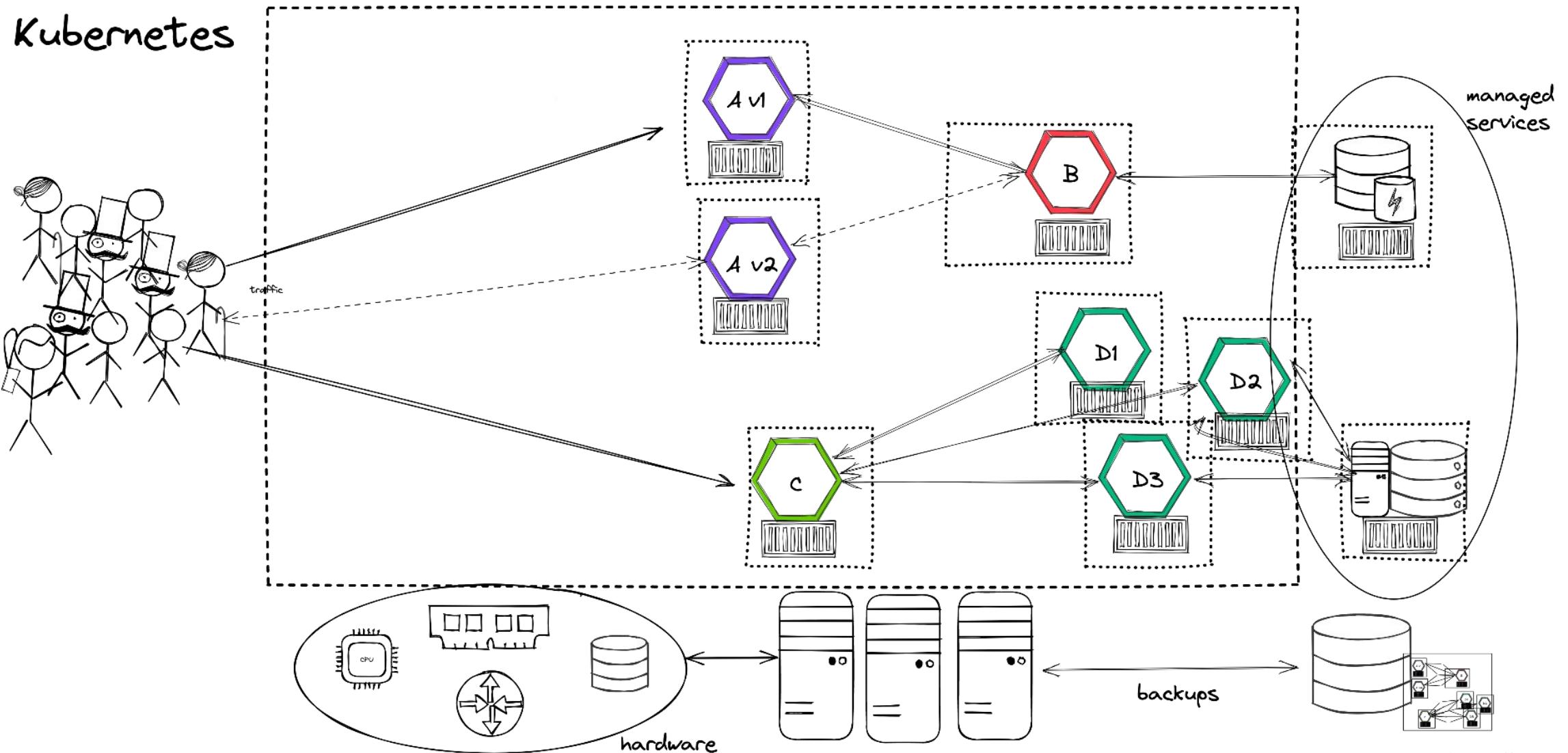


What is “vanilla” Kubernetes missing?

Summary

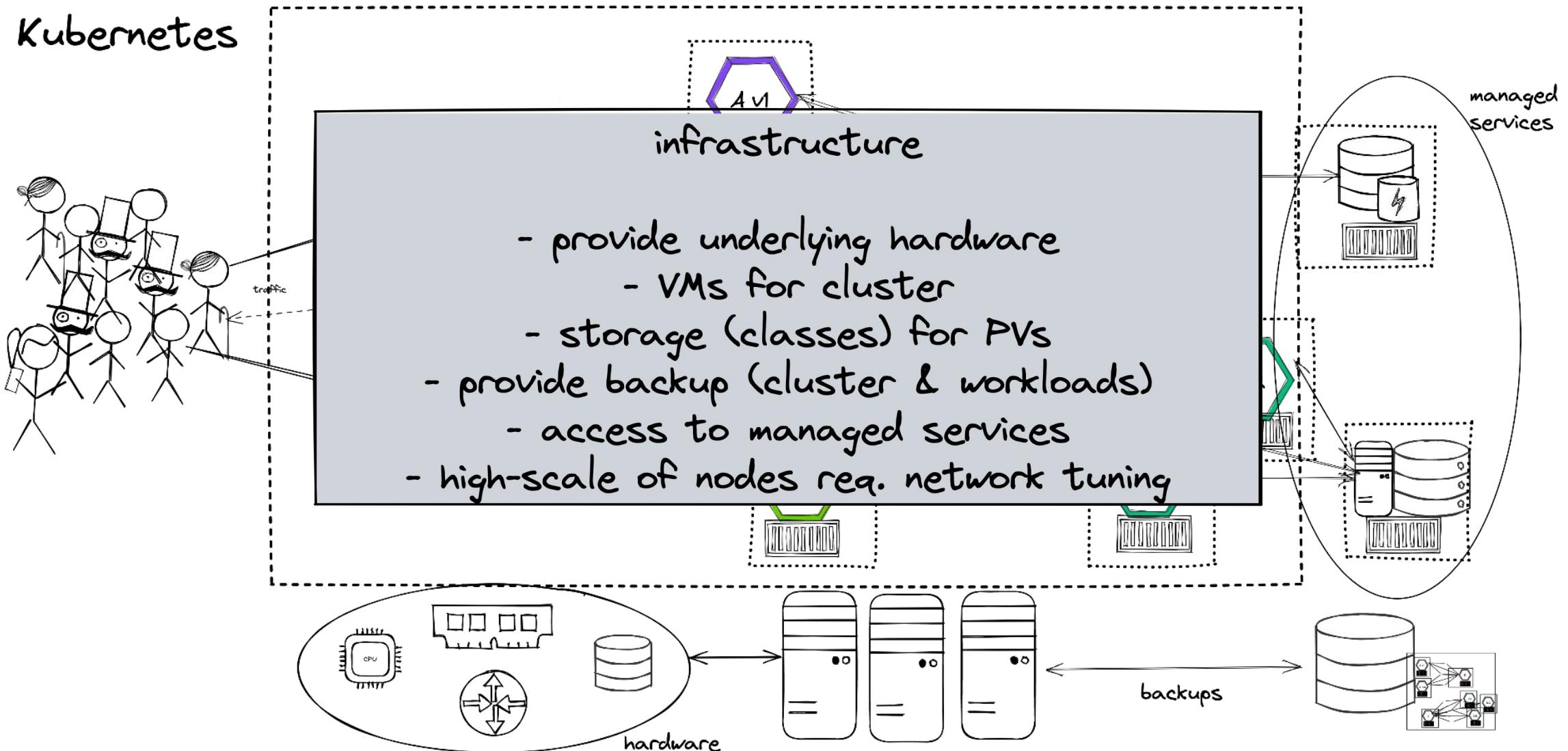


Infrastructure

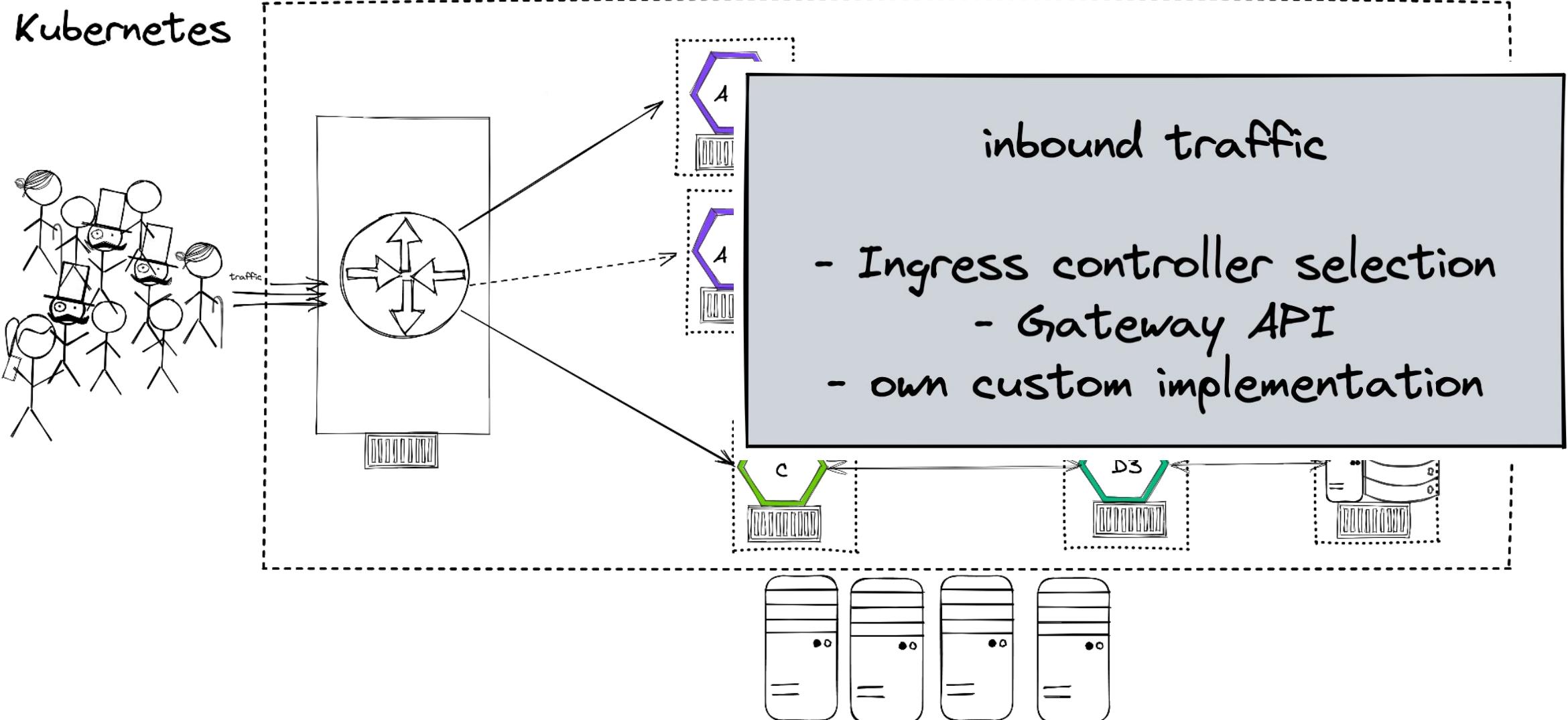


Infrastructure

Kubernetes

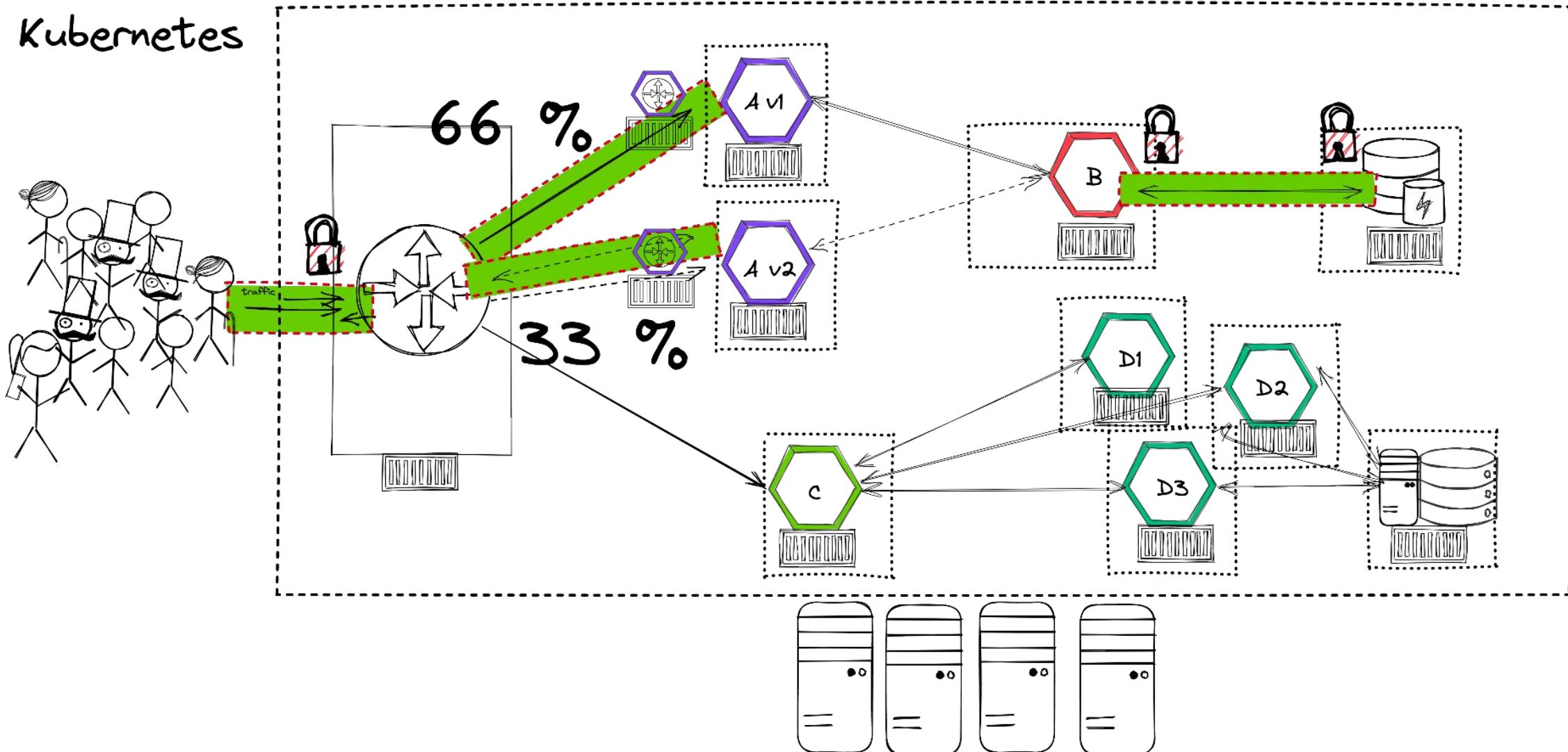


Networking - Inbound traffic



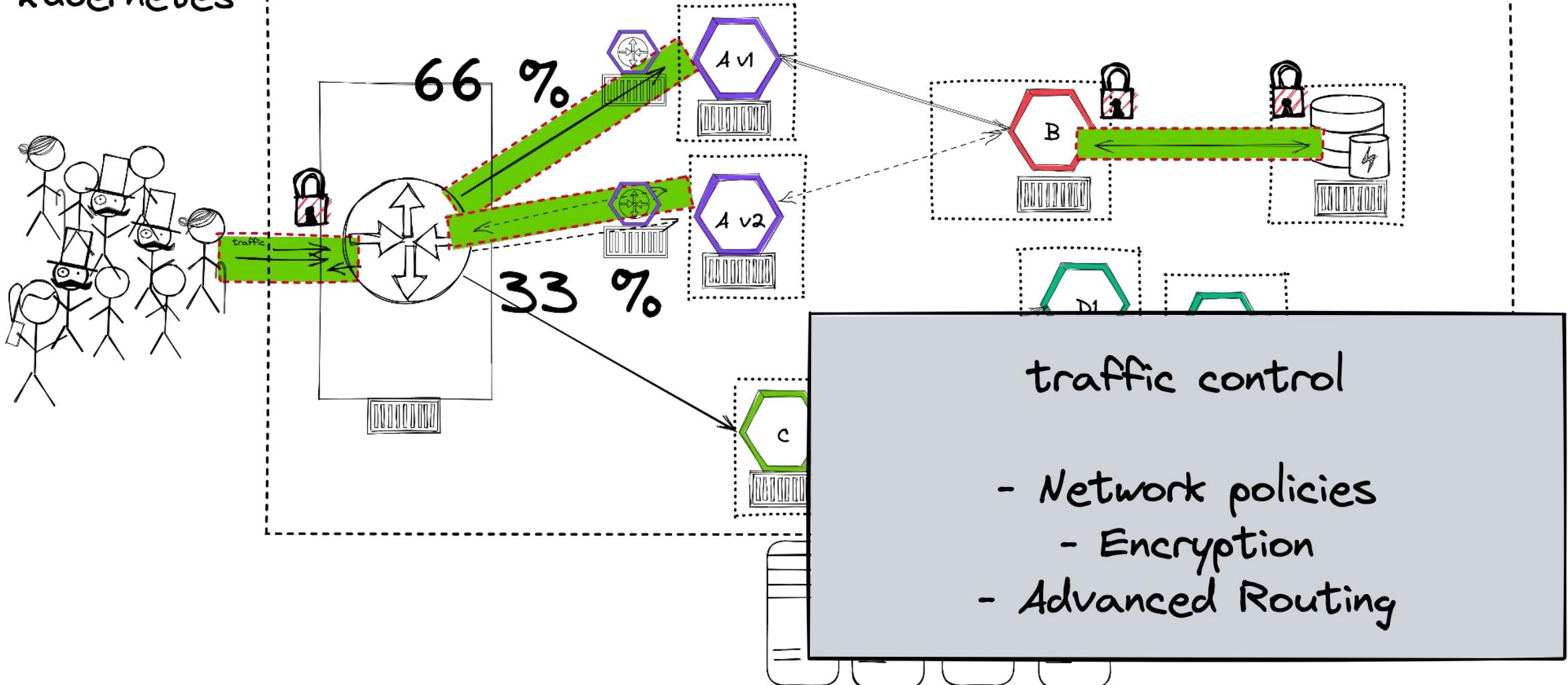
Networking - Traffic control

Kubernetes



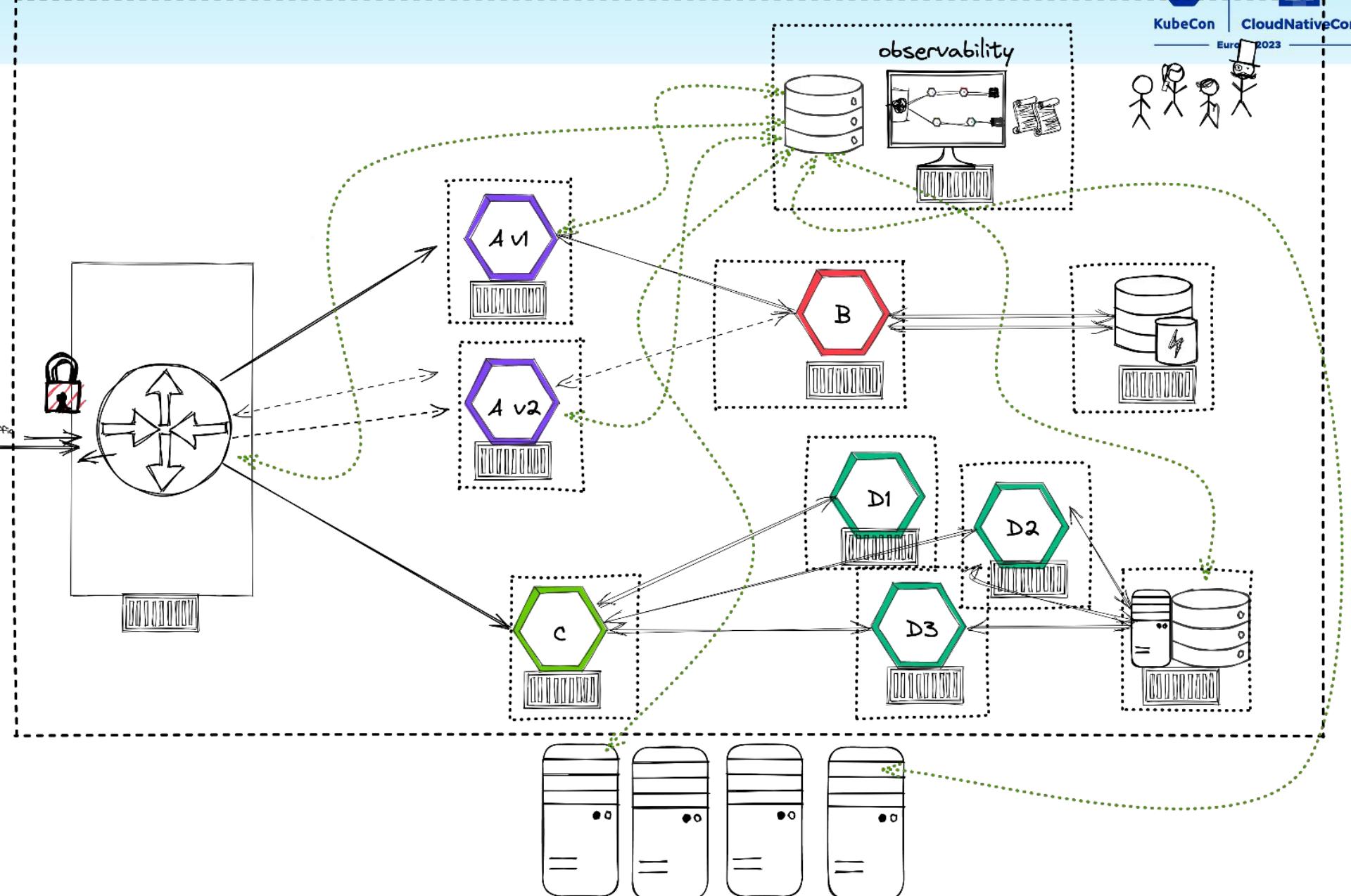
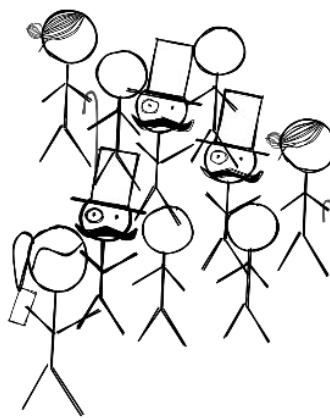
Networking - Traffic control

Kubernetes

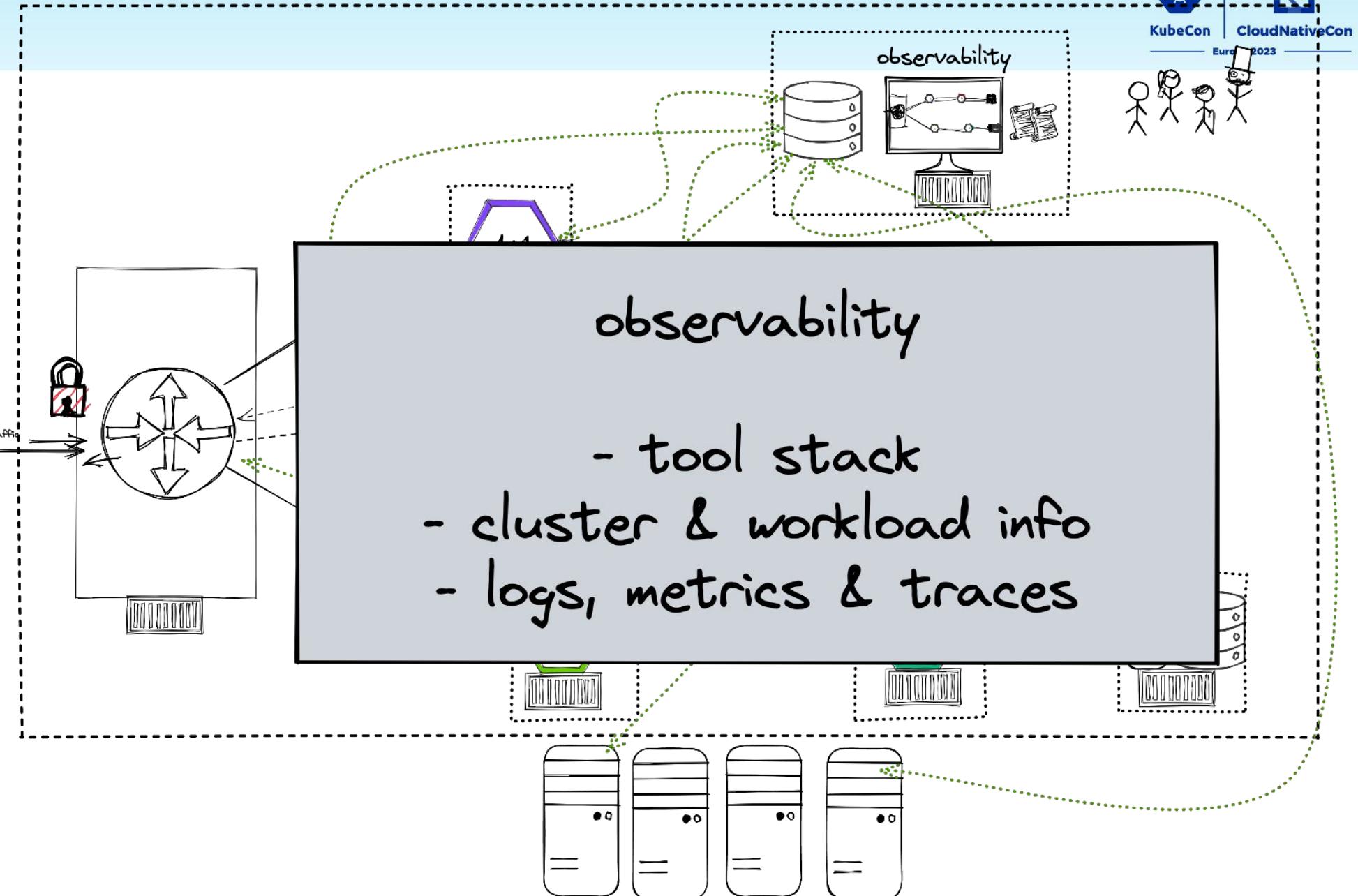
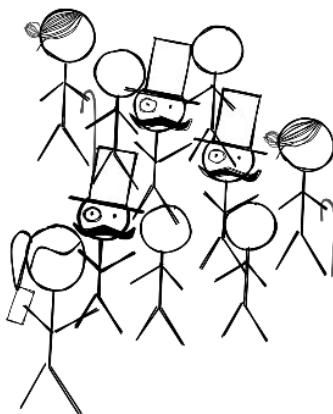


O11y

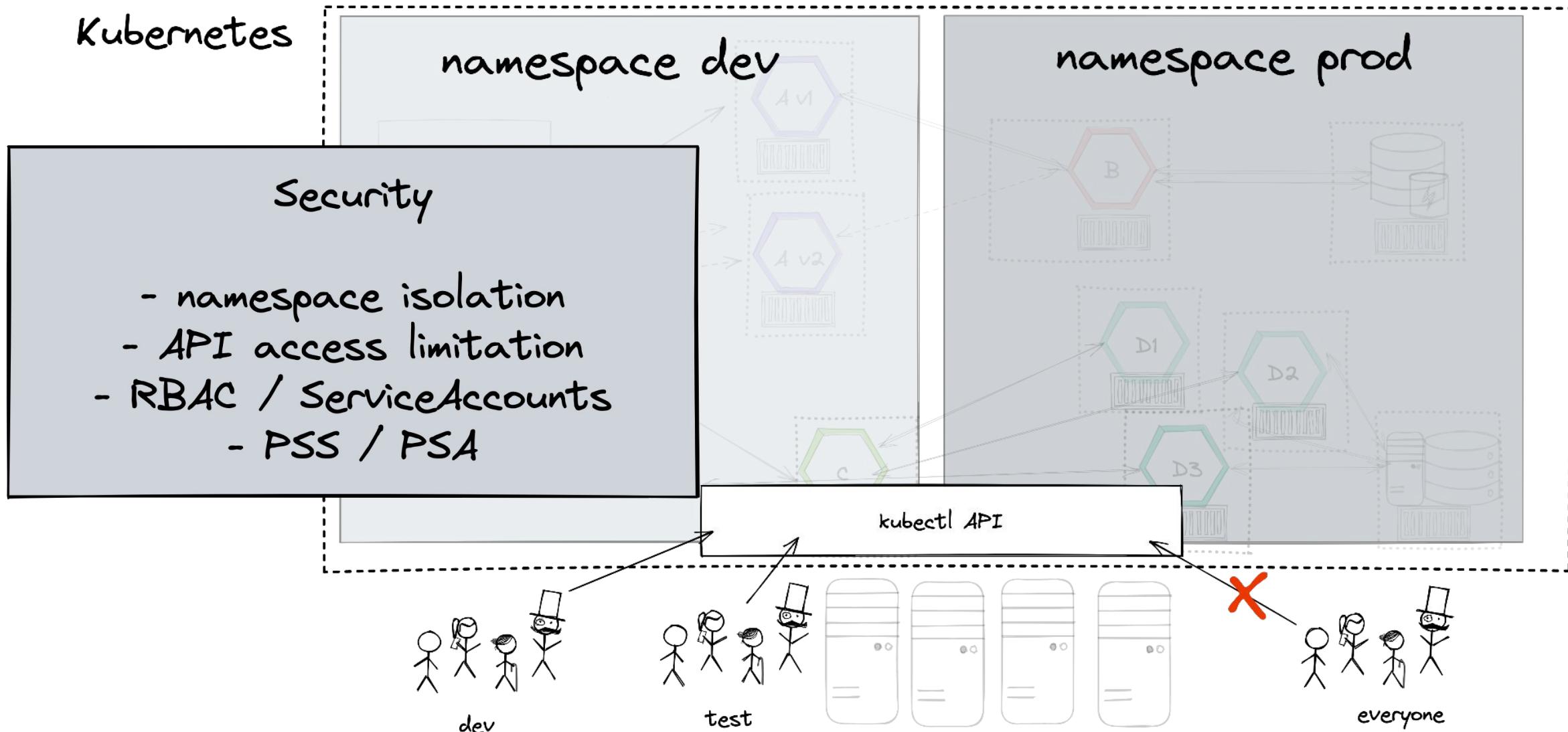
Kubernetes



Kubernetes

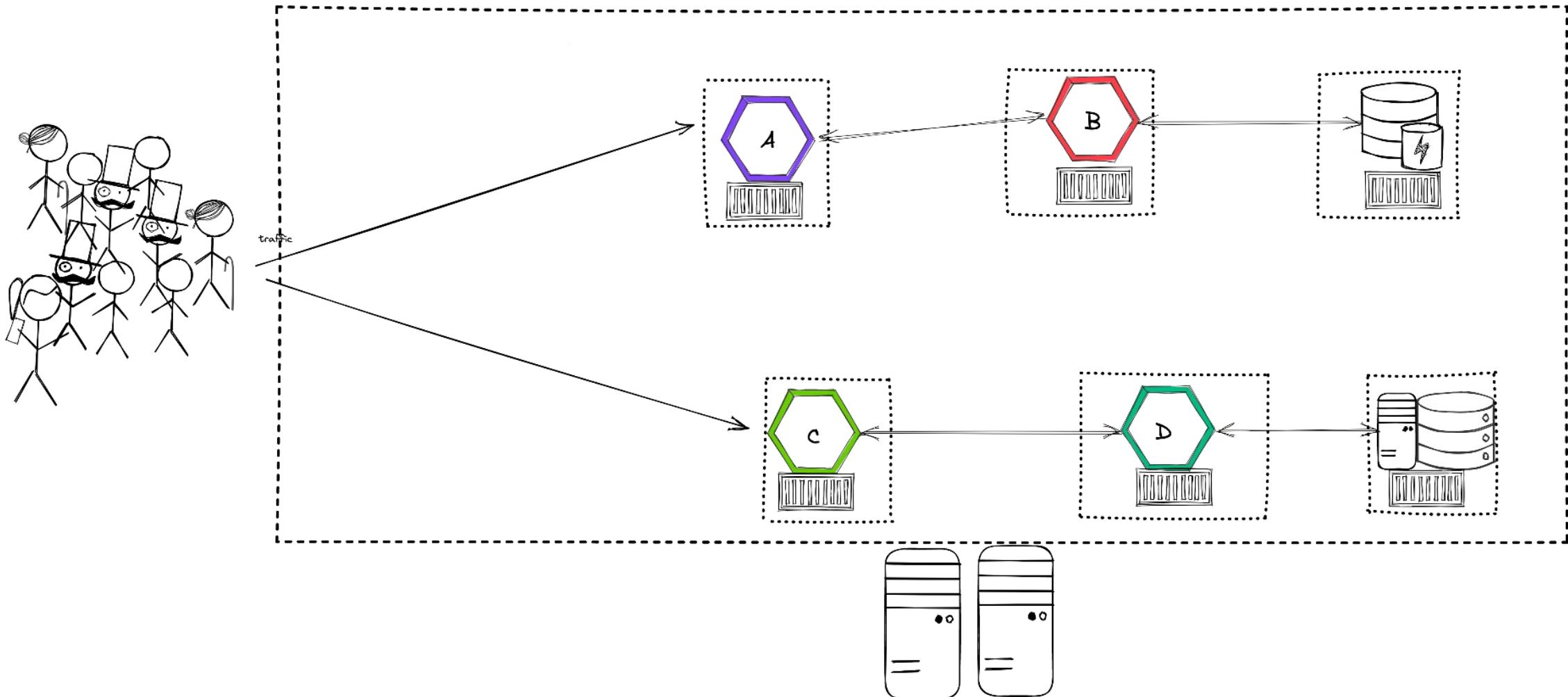


Security - API Access / RBAC



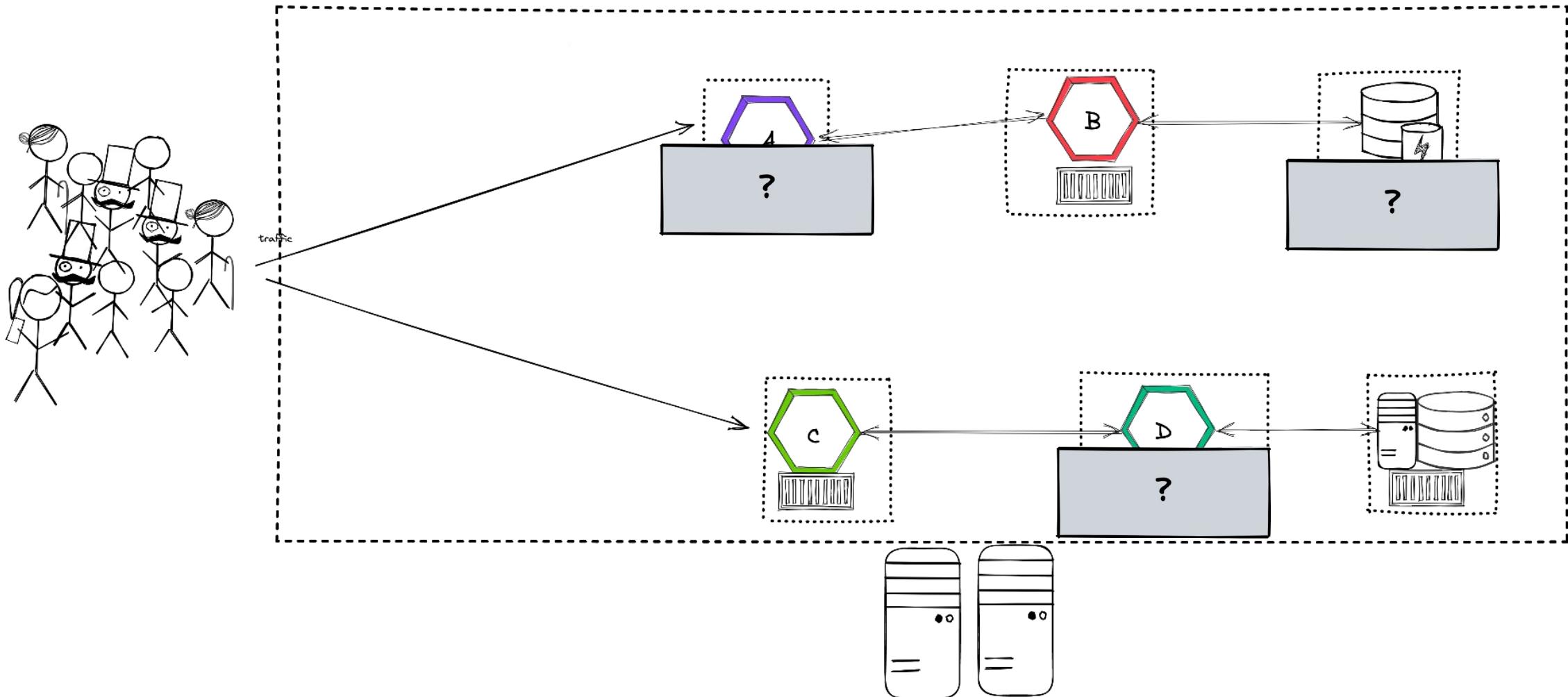
Workloads

Kubernetes



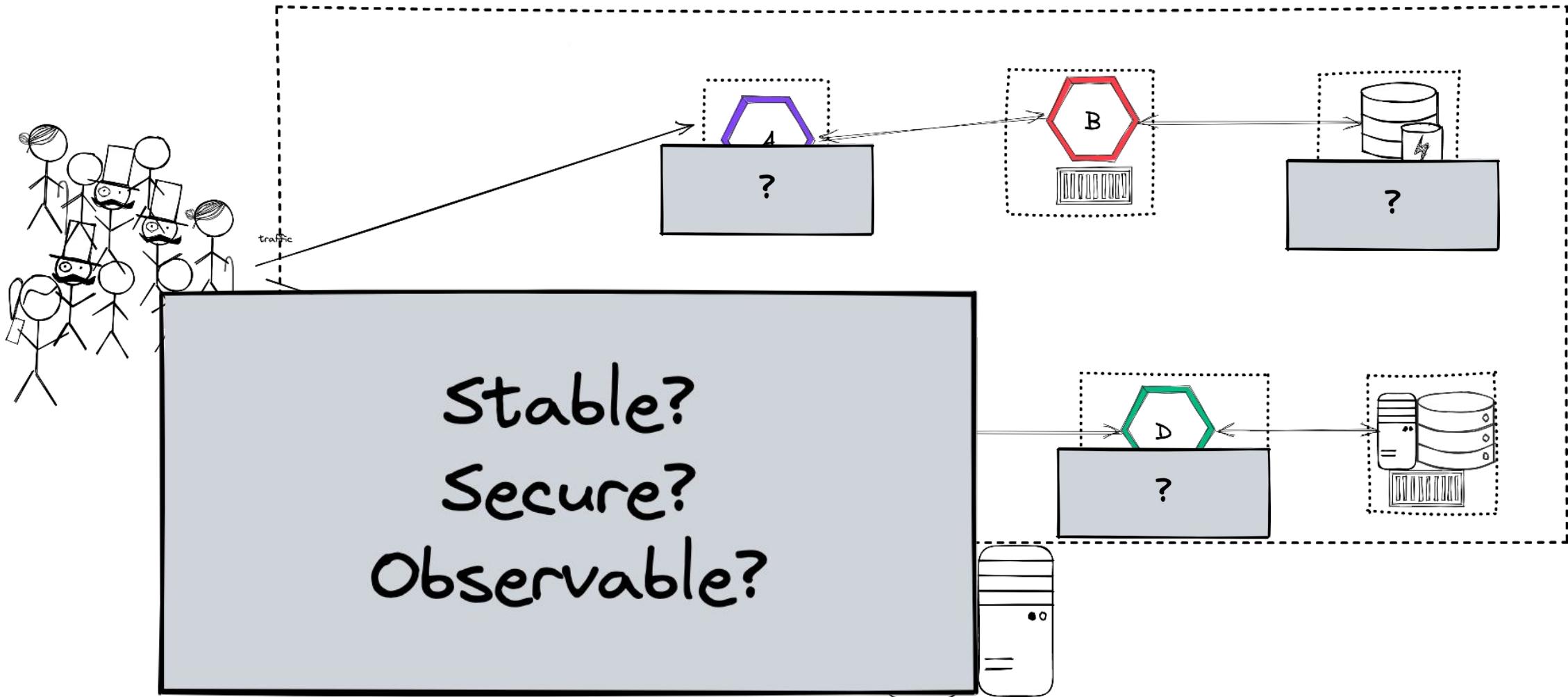
Workloads

Kubernetes

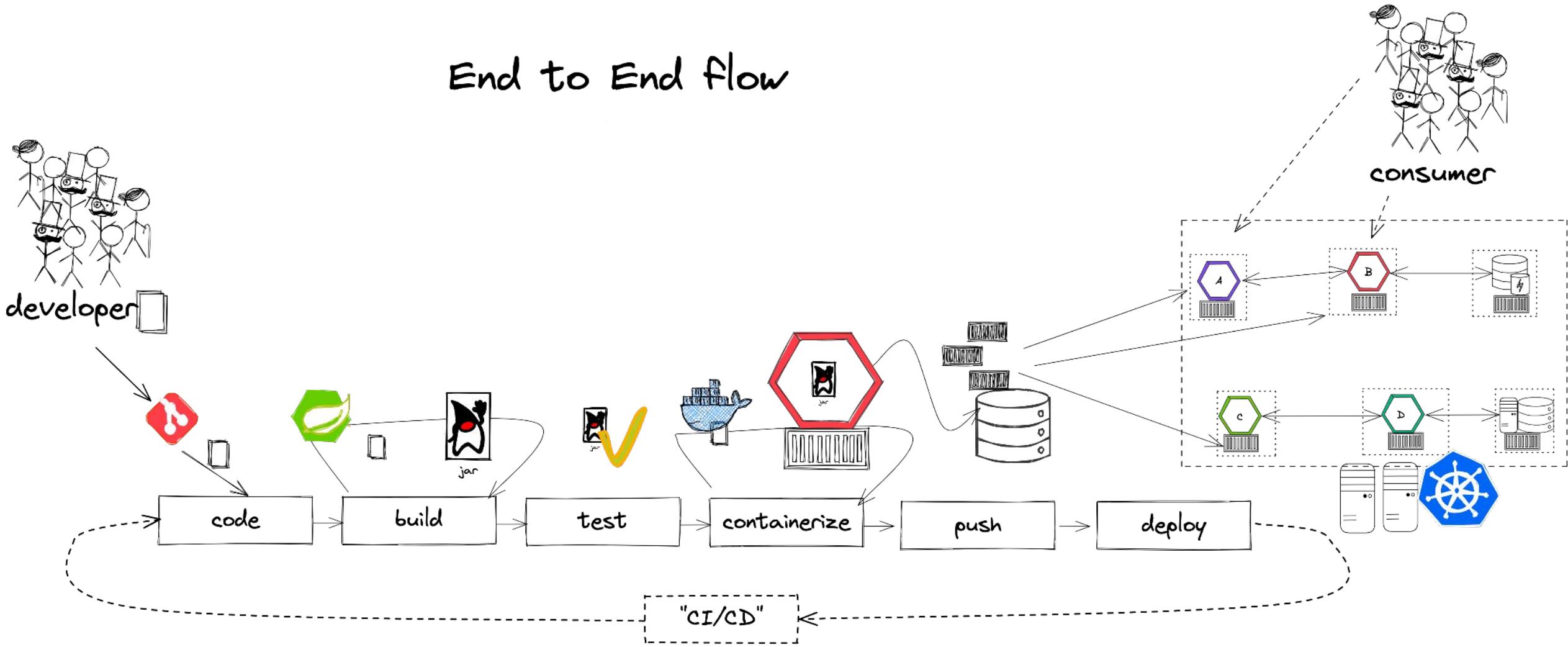


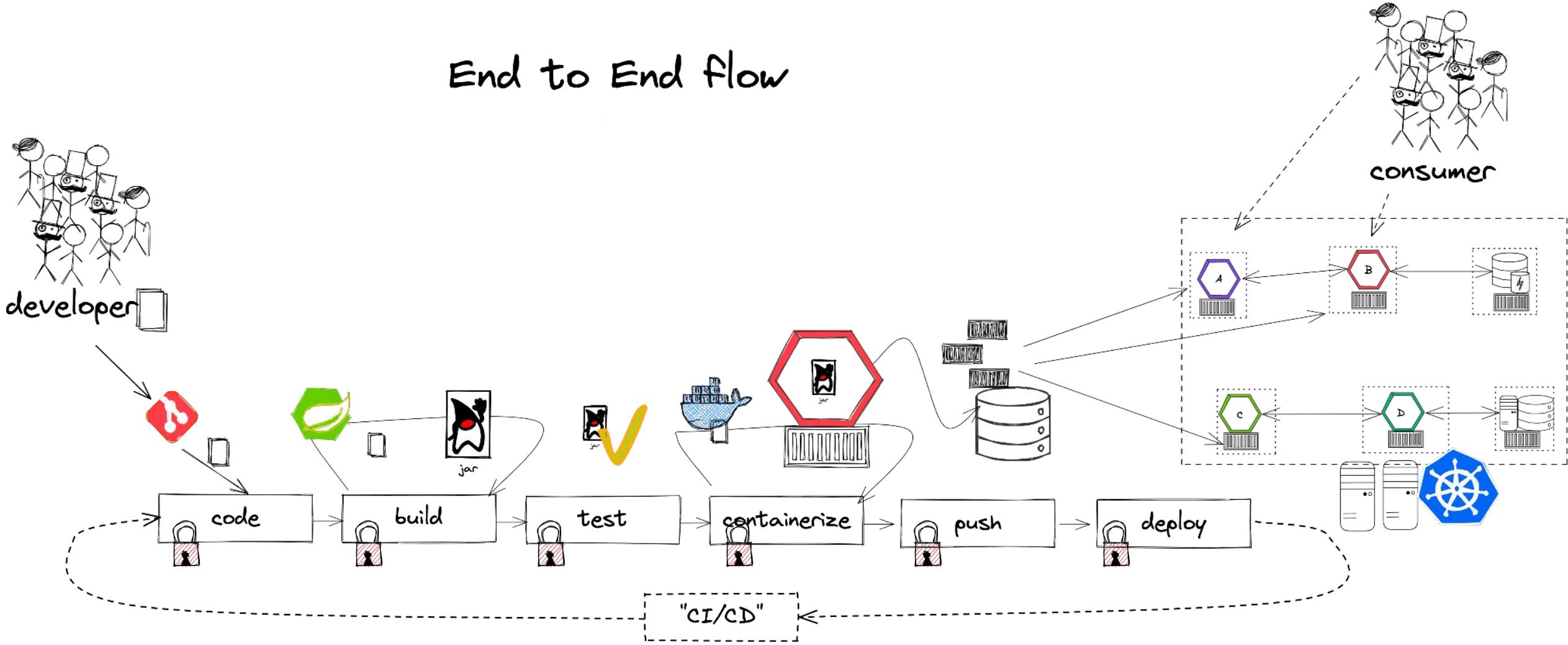
Workloads

Kubernetes



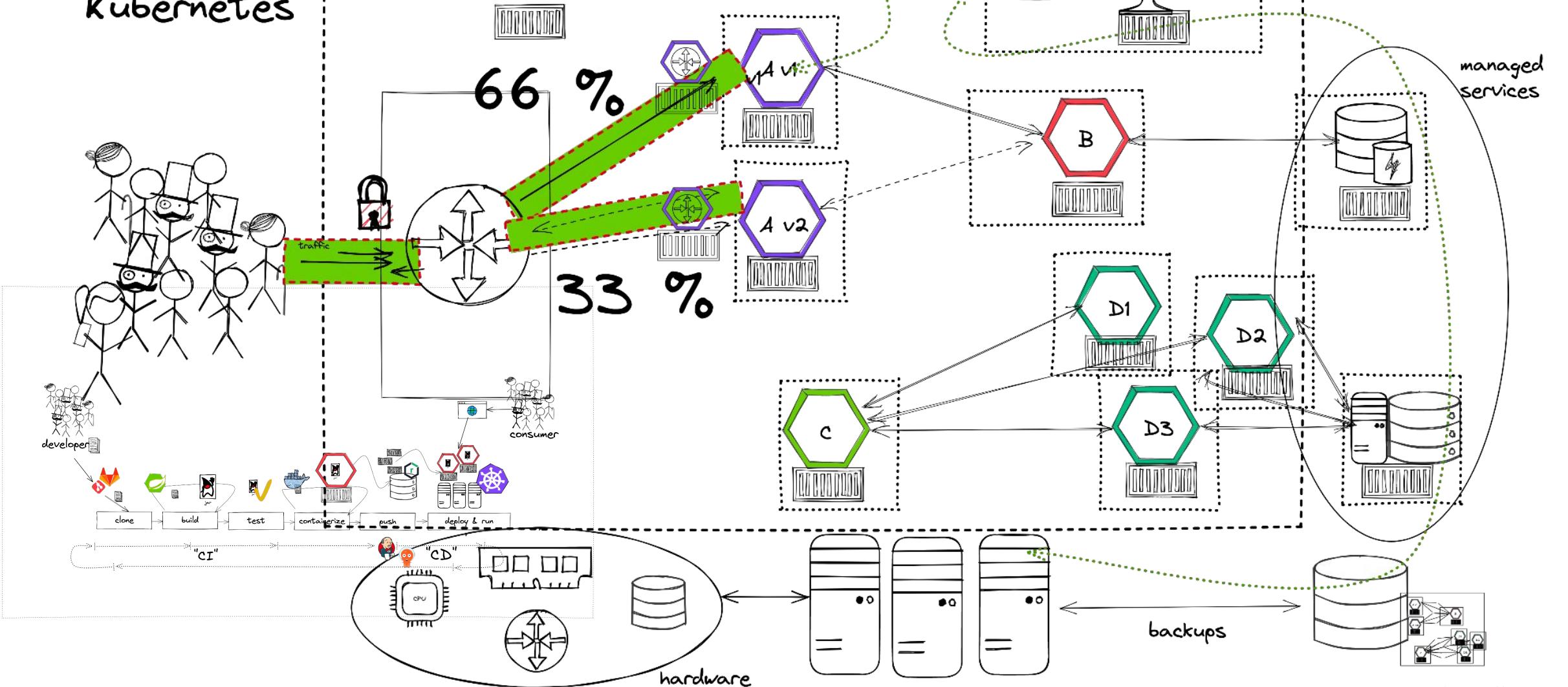
Workloads



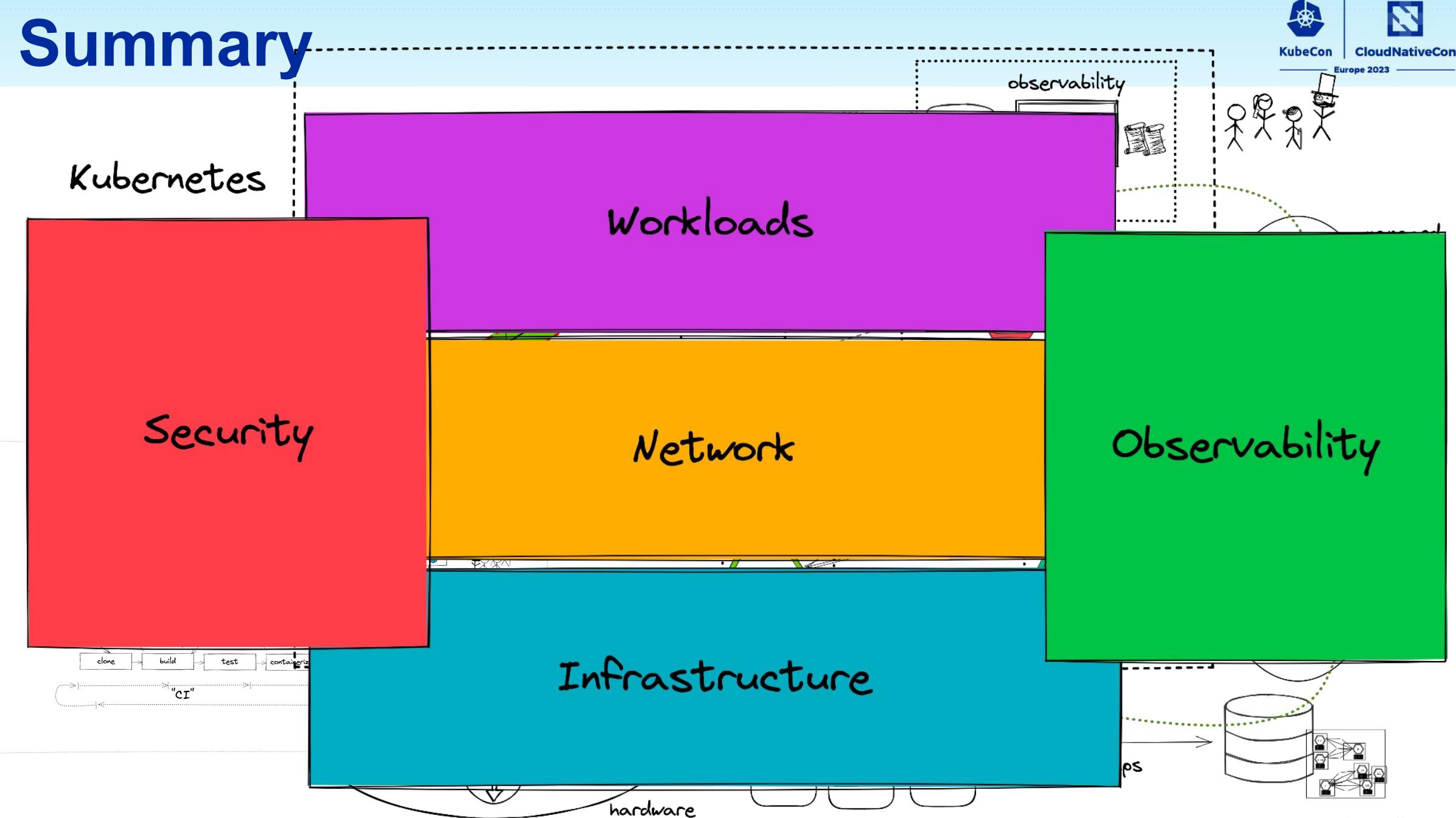


“Summary”

Kubernetes

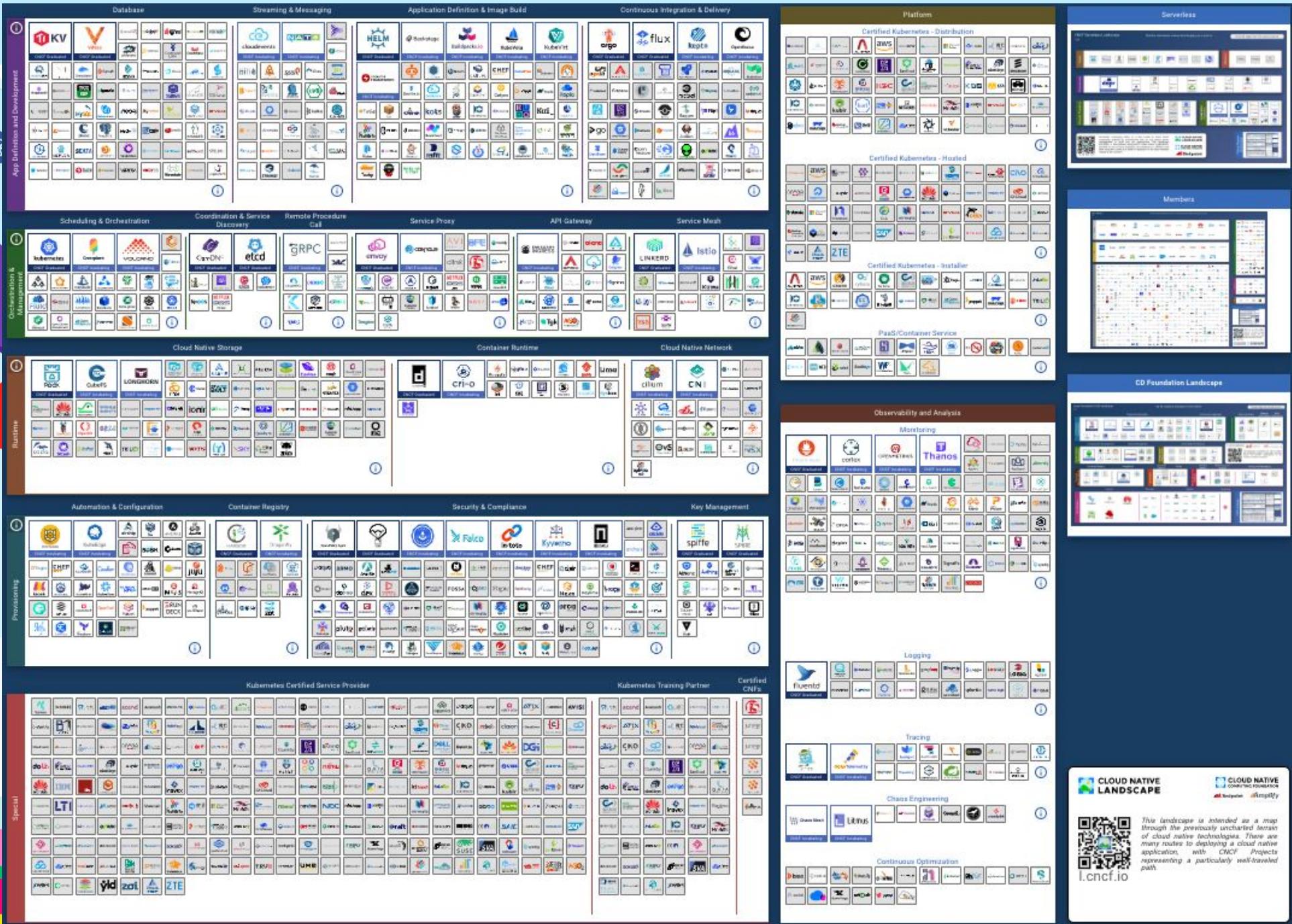


Summary



c h e c k l i s t

pod logs	logs	
kubelet logs		
control plane logs		
metrics-server	metrics	
time series database (Prom, etc)		observability
tracing	tracing	
ingress controller		networking
service mesh		
Gateway API		
network policies		security
secret manager		
PVC backups		infrastructure/ backups
control plane backups (if applicable)		
cluster autoscaler (when applicable)		



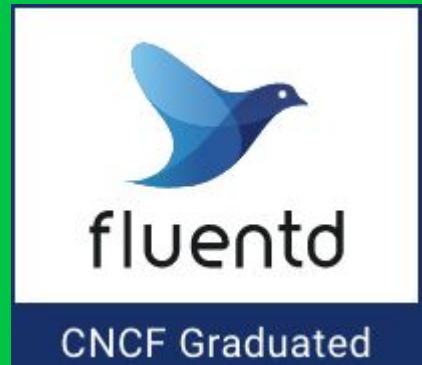
Infrastructure



Network



Observability



Security



Workloads



And now what?



Kelsey Hightower ✅ @kelseyhightower · Mar 11, 2019

...

Platform in a box solutions that are attempting to turn Kubernetes into a **PaaS** are missing the "as a service" part. It's more like PaaR: Platform as a Responsibility. Your responsibility to purchase, staff, patch, scale, and upgrade.

7

64

200



Management

un-managed

managed

*fully-managed

Apps / Workloads

Sec / Net / Obs

Kubernetes

Infrastructure / HW

■ you manage

Apps / Workloads

Sec / Net / Obs

Kubernetes

Infrastructure / HW

■ provider managed

Apps / Workloads

Sec / Net / Obs

Kubernetes

Infrastructure / HW



Tanzu Kubernetes Grid

Declarative API

Common Kubernetes Services*

IdP auth

Monitoring

Logging

Networking

Container registry

Ingress

HARBOR

VELERO

SONOBUOY

Grafana

ANTREA

Cluster API

CONTOUR

CARVEL

fluentbit

Prometheus

CALICO

Cluster Lifecycle Management



Supervisor Cluster / Management Cluster *



HYBRID CLOUD

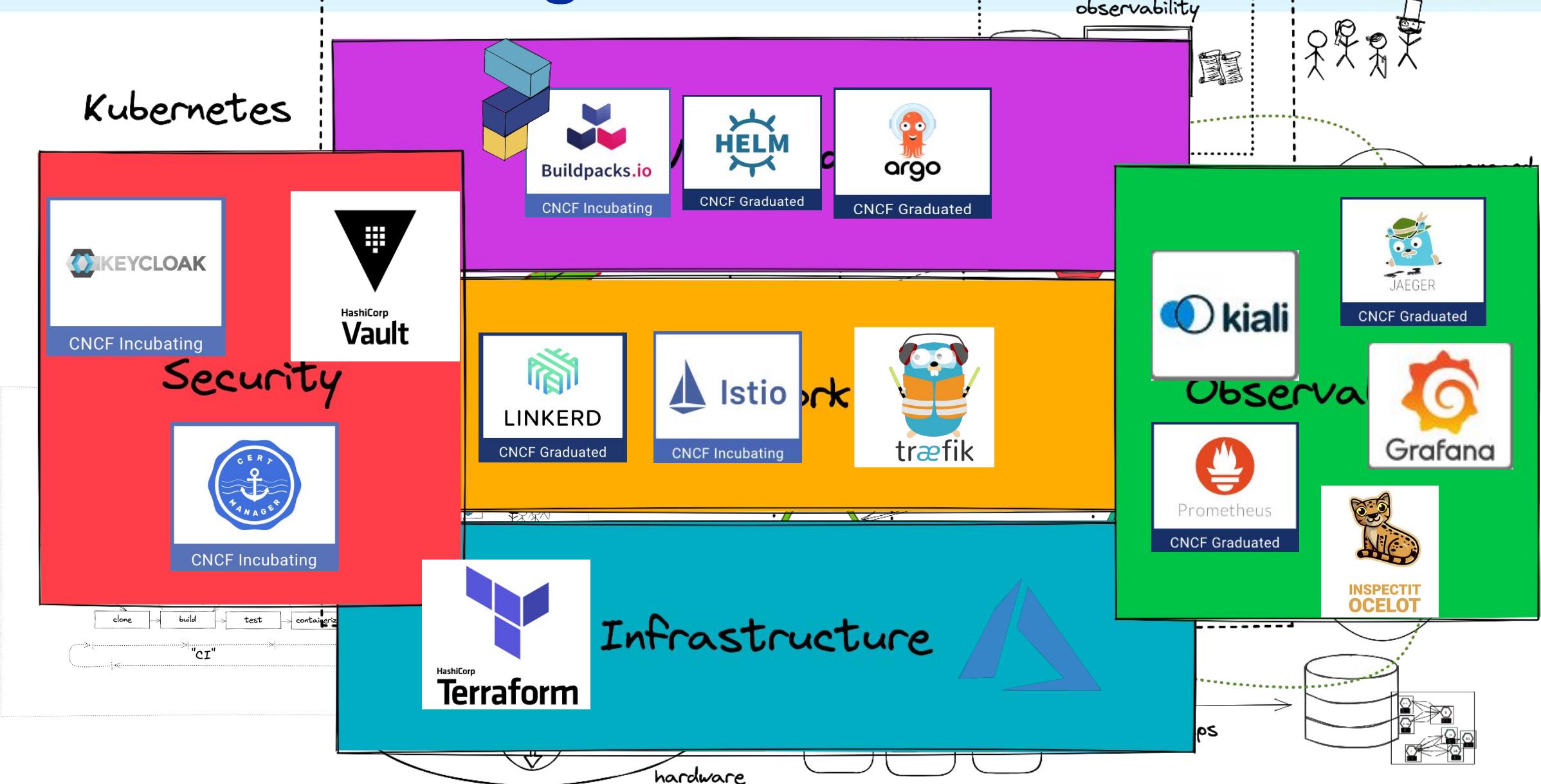


PUBLIC CLOUD



EDGE

Novatec Training Environment



| Application Code |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| Data Store |
| Runtime / Middleware |
| Containers | Containers | Containers | Containers | Containers |
| Operating System |
| Virtualization | Virtualization | Virtualization | Virtualization | Virtualization |
| Hardware | Hardware | Hardware | Hardware | Hardware |

Traditional IT

IaaS

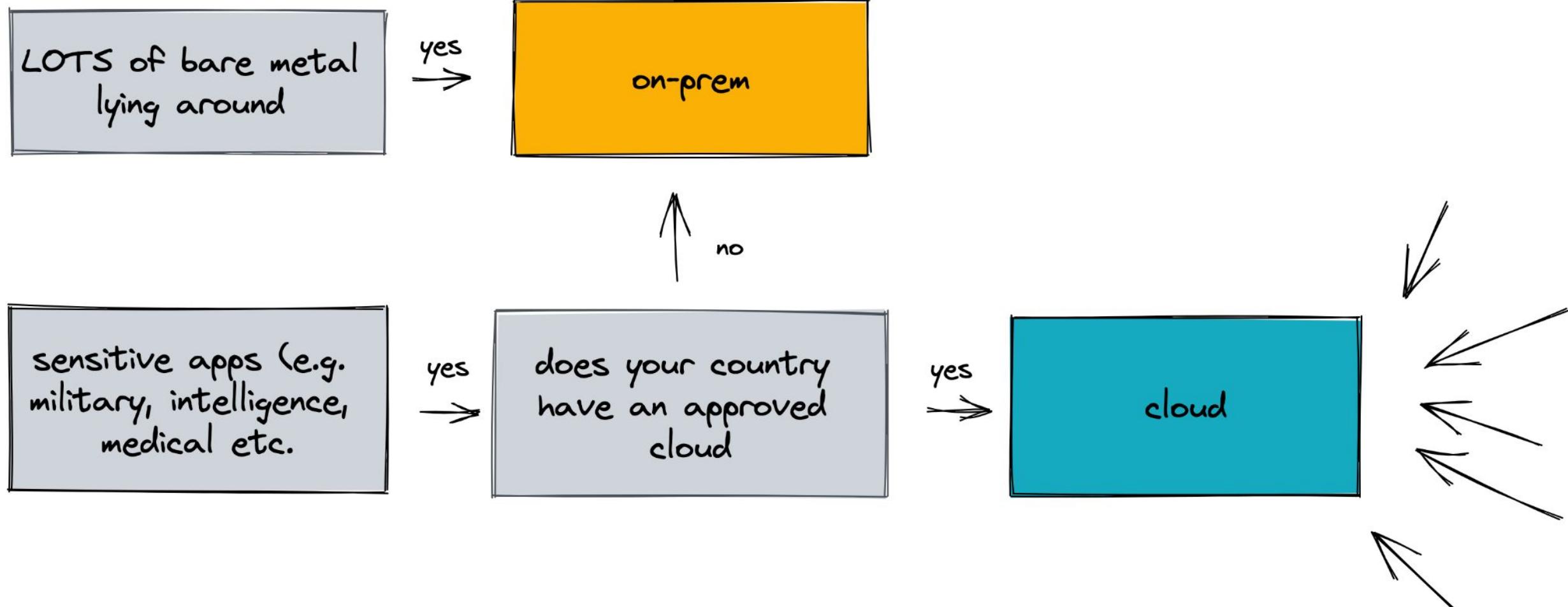
CaaS

PaaS

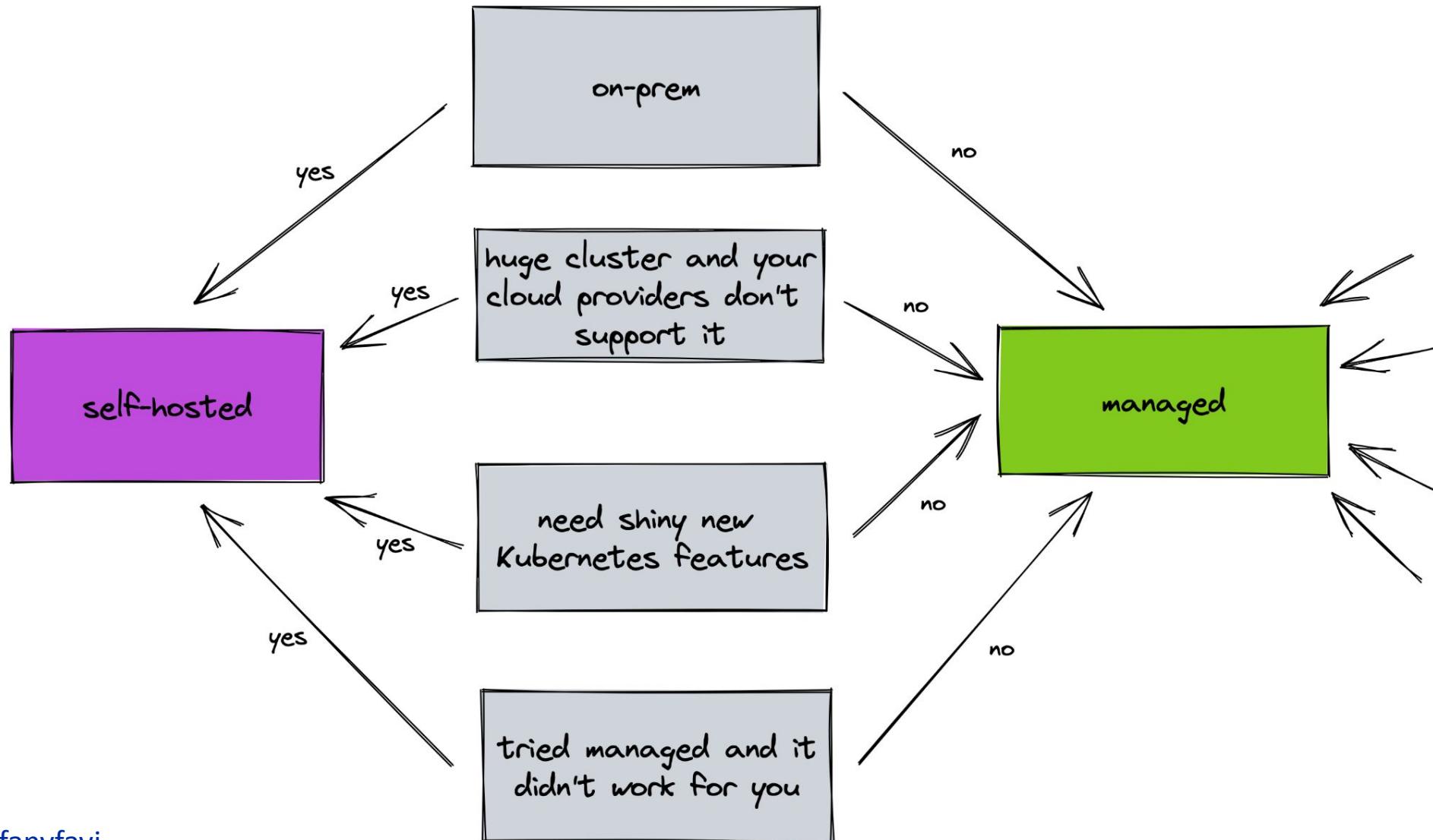
SaaS

- Managed by vendor
- You manage

Cloud vs On-Prem



Managed vs Self-Hosted





Jérôme Petazzoni @jpetazzo · Dec 11, 2018

...

The fastest, **easiest**, and cheapest way to run your **Kubernetes** cluster is to get someone else to do it for you. #kubecon

8

80

221



Summary

- In the end there is no right or wrong,
it is more about the decision where to invest the time and money
 - Maintain the stack yourself -> Invest in the skill and have it in-house
 - Have someone done it for you -> Invest in service providers
- In general we recommend to use the highest abstraction possible
Don't solve problems which have already been solved!
- Using and relying on a ready tested platform will let you focus more on higher abstractions -> your apps!
- If there is a managed solution that suits your needs -> use it!
- If you want to manage the stack yourself -> get enablement & consultancy

Please reach out to us!



Tiffany Jernigan
Sr. Dev Advocate, VMware
@tiffanyfayj

@maeddes @tiffanyfayj



Matthias Häußler
Chief Technologist, Novatec
@maeddes



Feedback :)



KubeCon



CloudNativeCon

Europe 2023



TiKV

Sponsor Shout-Out!

Thank you to our Session Recording
Sponsor:

uptycs

