

# Platform Perseverance

## Taming 1,000 Kubernetes Clusters

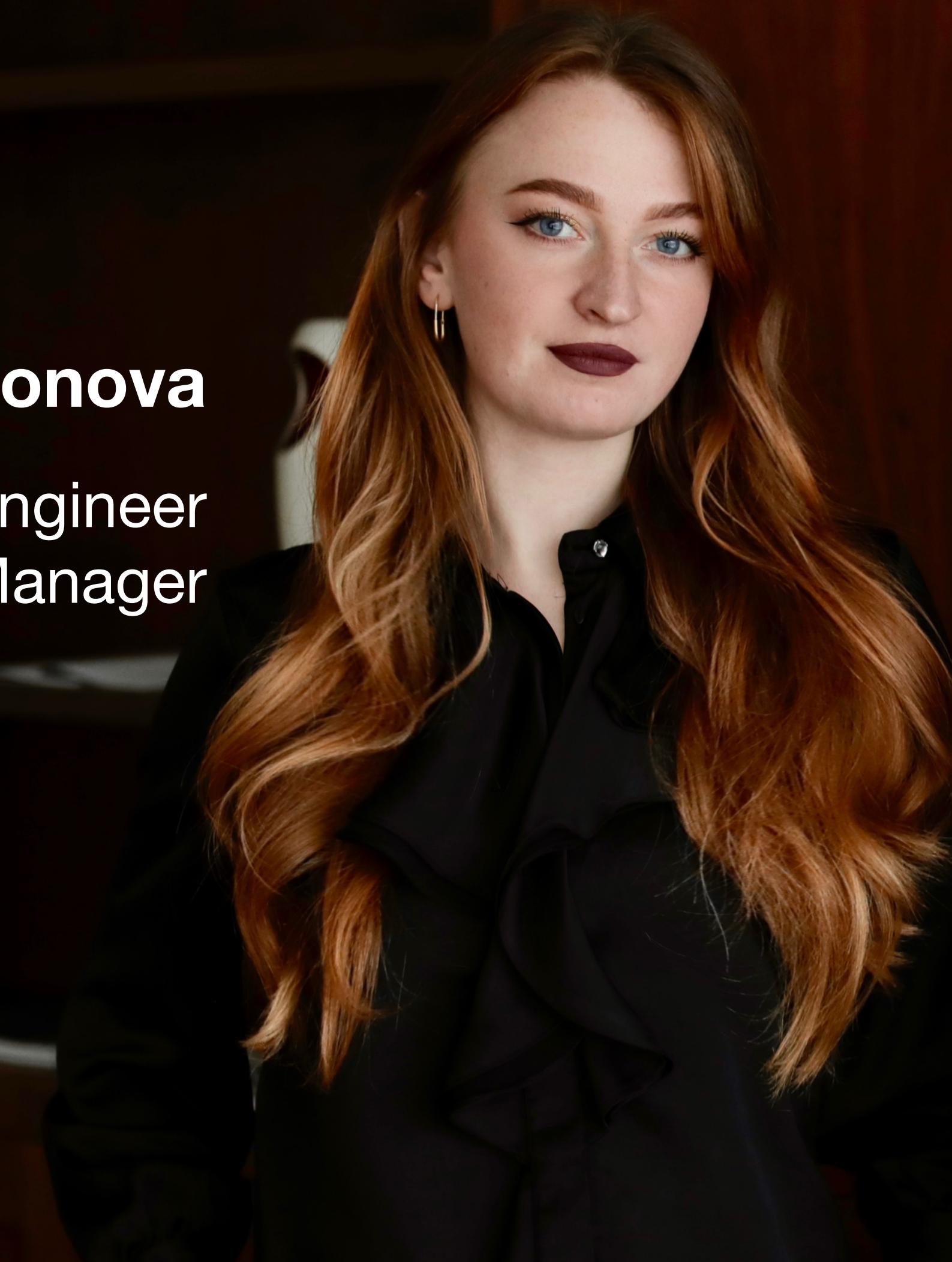
Marcy Paramonova & Stéphane Cusin

Banque Pictet & Cie SA

# Who are we?

**Marcy Paramonova**

DevOps Engineer  
IT Portfolio Manager



**Stéphane Cusin**

Software Engineer Architect  
Product Manager of Kubernetes  
Technical Lead



# Banking at Scale

## People & Infrastructure

### Swiss Private Bank: Pictet & Cie SA

- 5k employees
- 30 offices
- 650 developers

### Infrastructure

- 15 datacenters
- 10k virtual servers
- 1k physical servers



# Kubernetes at Pictet

## The Early Days

- 🚀 Started in 2018
- 📦 Bare metal deployment
- 🔧 Kubernetes 1.10
- 📦 Upstream only, no vendor
- 📚 Followed “K8s the Hard Way”

Kubernetes the Hard Way (2018)

```
...  
openssl genrsa -out ca.key  
etcd --peer-client-cert-auth  
kubelet --kubeconfig=...  
kubectl apply -f ...
```

No kubeadm. No vendor.  
Just YAML, certificates, and pain.

# Growing Pains

## From 1 App to 200

2018: First production app

2022: 200+ production apps

All apps on a single production cluster

Platform maintenance was deprioritized

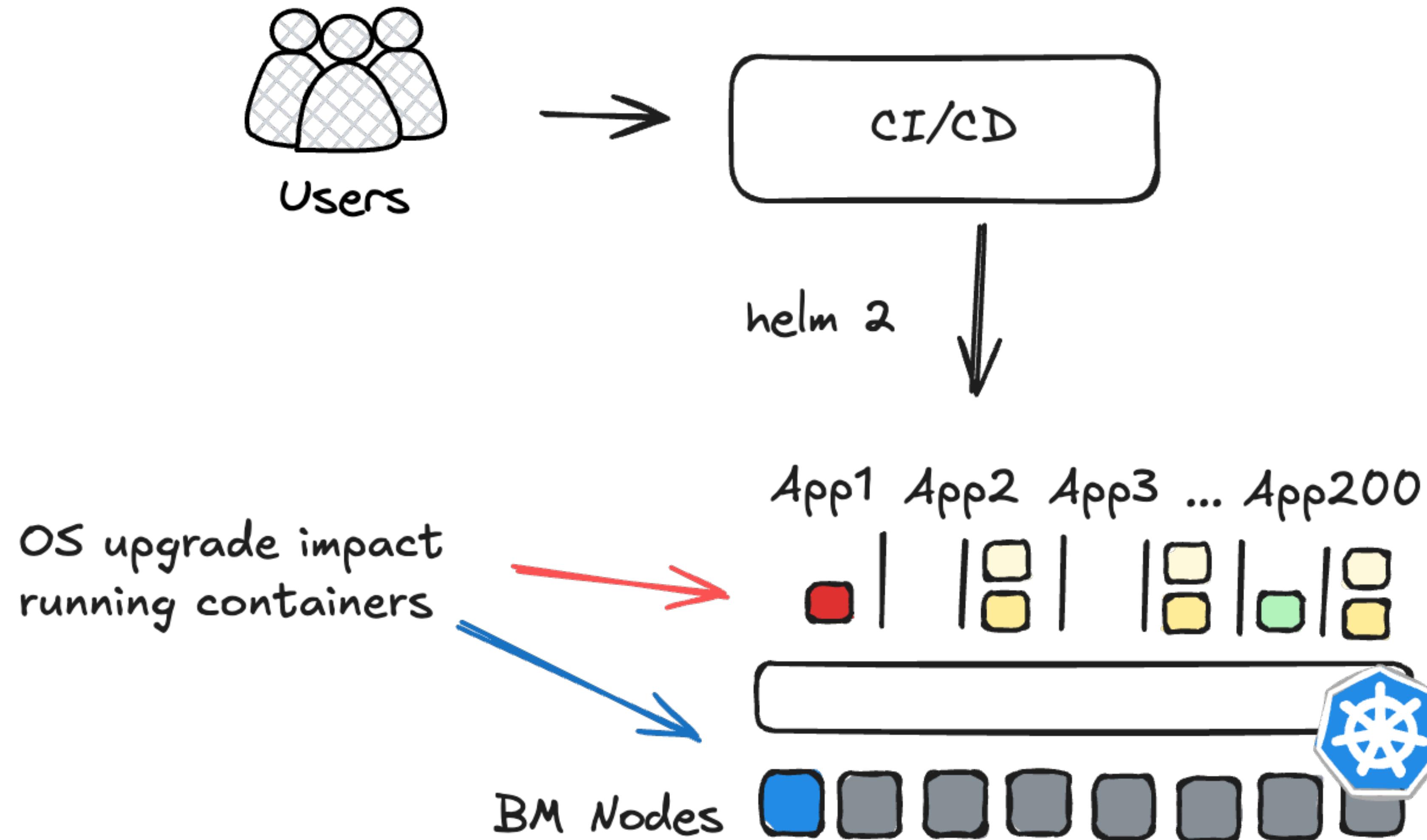
Kubernetes 1.12

Underestimated release management complexity

Each major change required full testing campaign



# Single Cluster = Single Point of Complexity



# Assumptions That Didn't Hold

- Kubernetes upgrades would be easy
- One cluster was enough for everyone
- Teams could safely share operators in namespaces
- Stability means we can delay maintenance
- New projects won't slow platform evolution

# What Worked Well

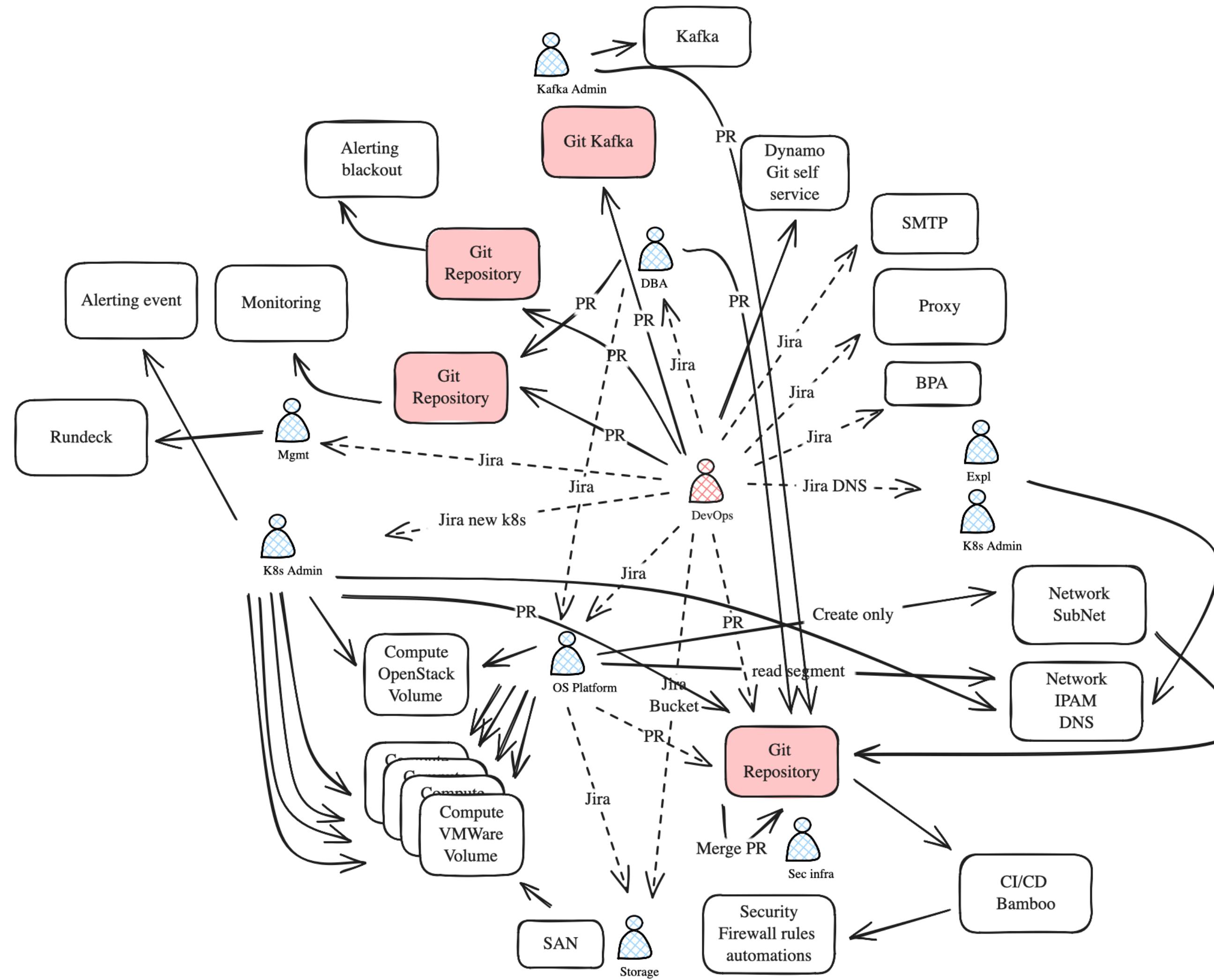
- ✓ Strong adoption by developers
- ✓ Developer autonomy & productivity
- ✓ Vendor-free, upstream Kubernetes installation

# Challenge 1

Tenancy per cluster



# Our reality





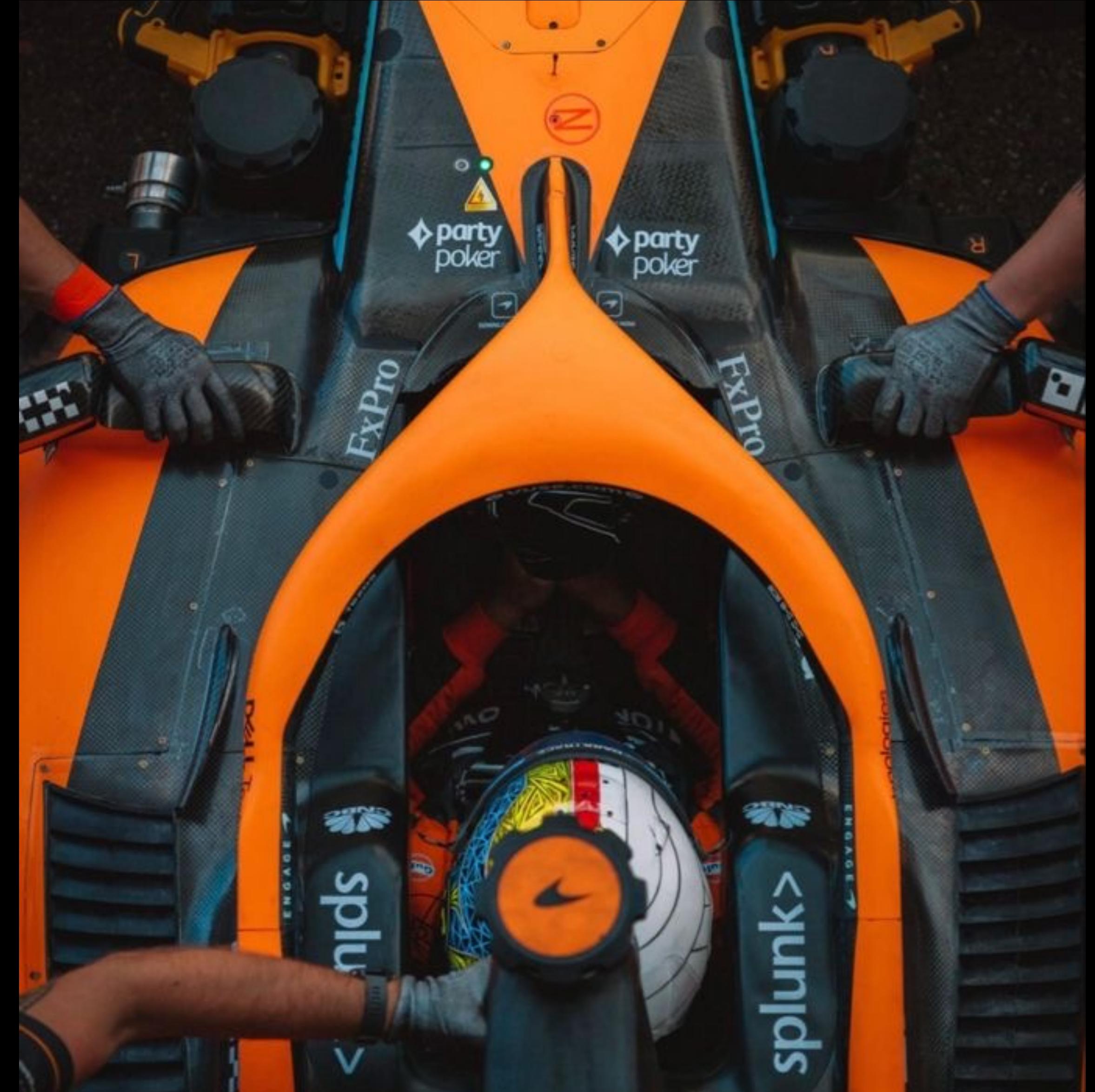
# Challenge 2

## Release management

# Guiding Principles of Our Internal Developer Platform

# Platform as a Product

- Productivity, UX
- User-Centric approach
- Build what your users need



# Stable & standard platform

- Stability == trust
- Standardisation == scalability
- Easy Inter Team Collaboration



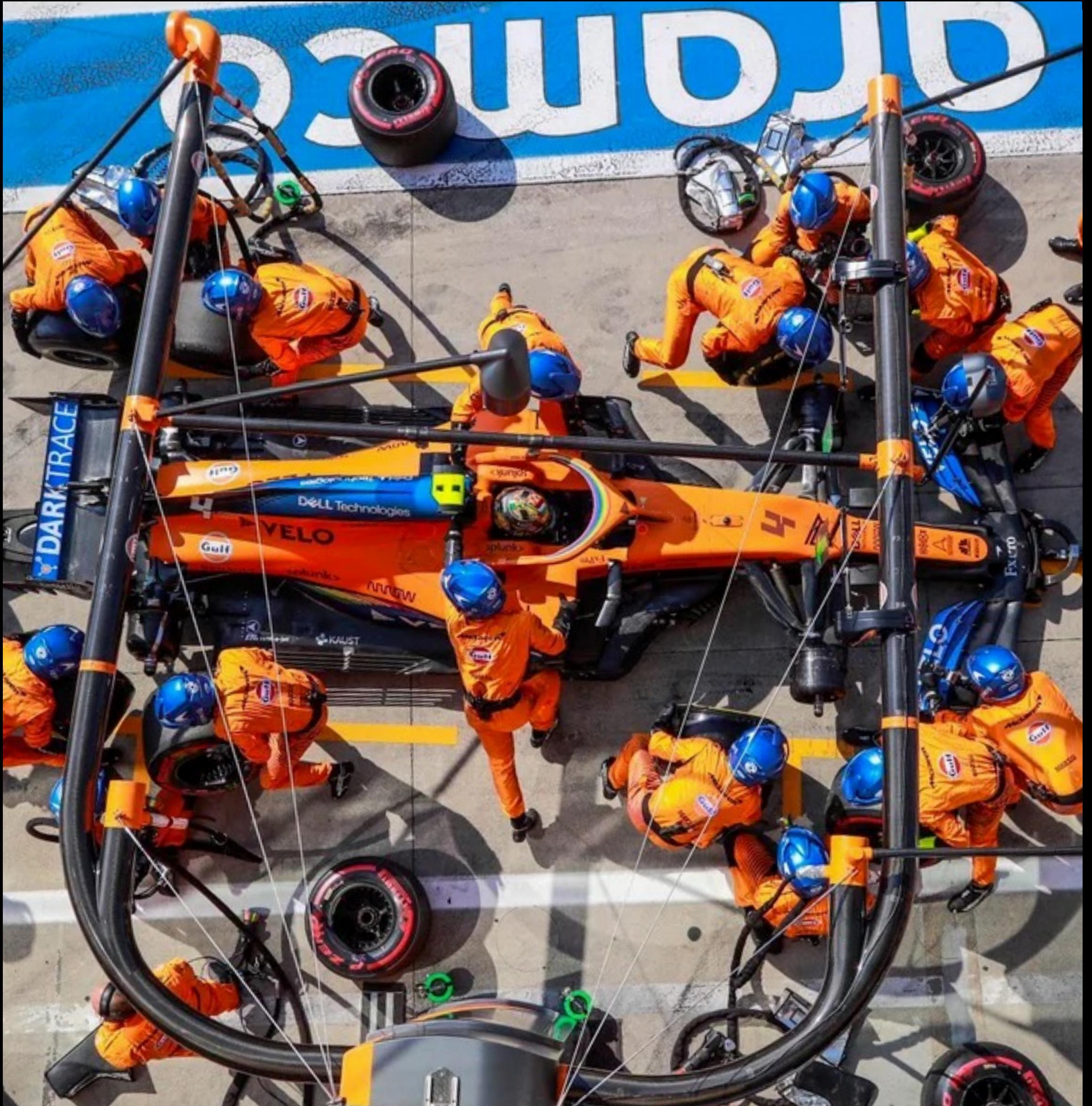
# Build platform for Day 2

- Stable, secure & continuously improved
- No one-and-done
- Automated and painless



# Eat your own dog food

- We trust our own workflows
- Sharp UX
- No disconnect with users



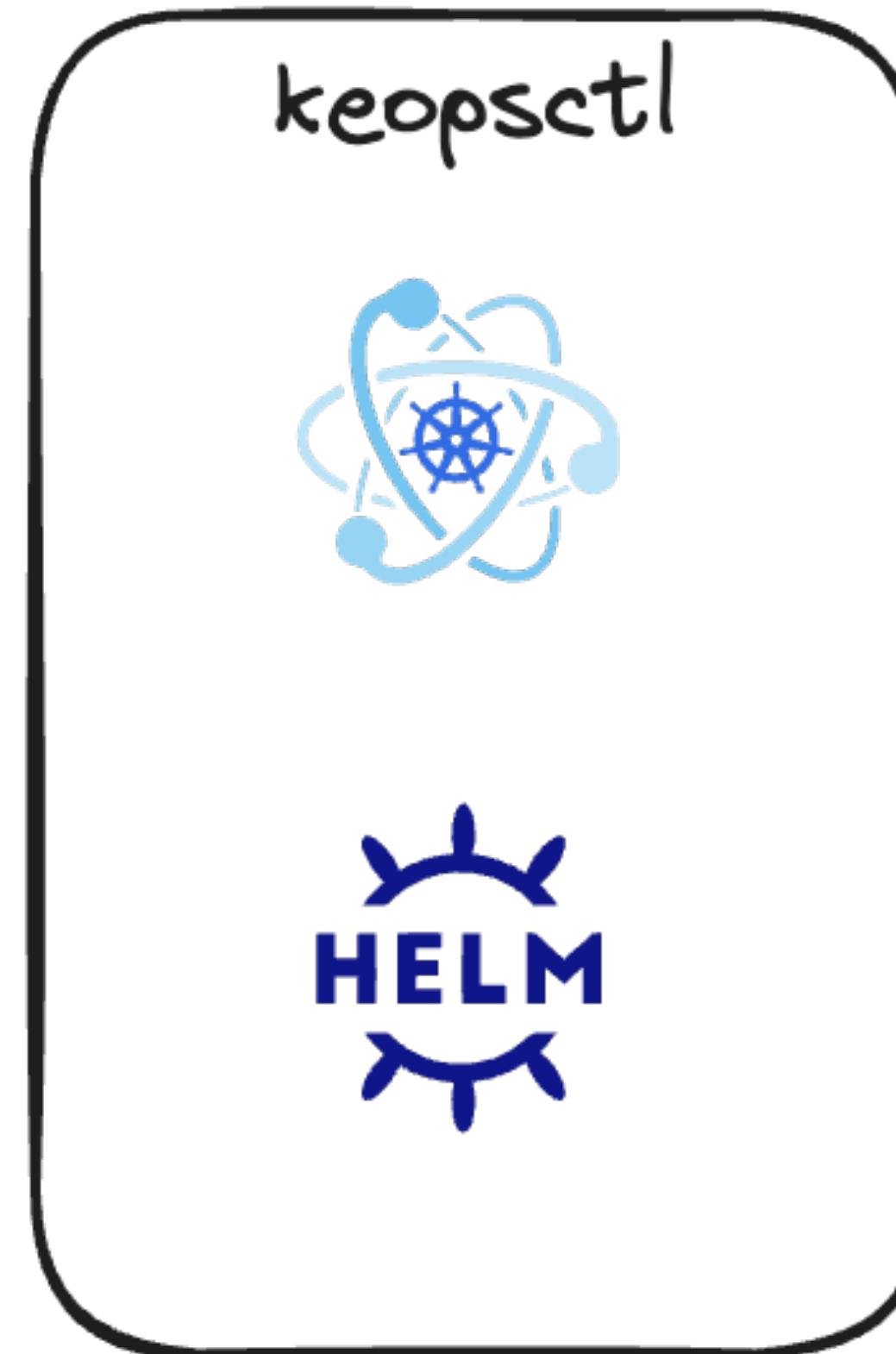
# Rethinking Tenancy

- ✓ One cluster per product
- ✓ Strong isolation = better reliability
- ✓ Easier upgrades, less coordination

# Building the New Platform

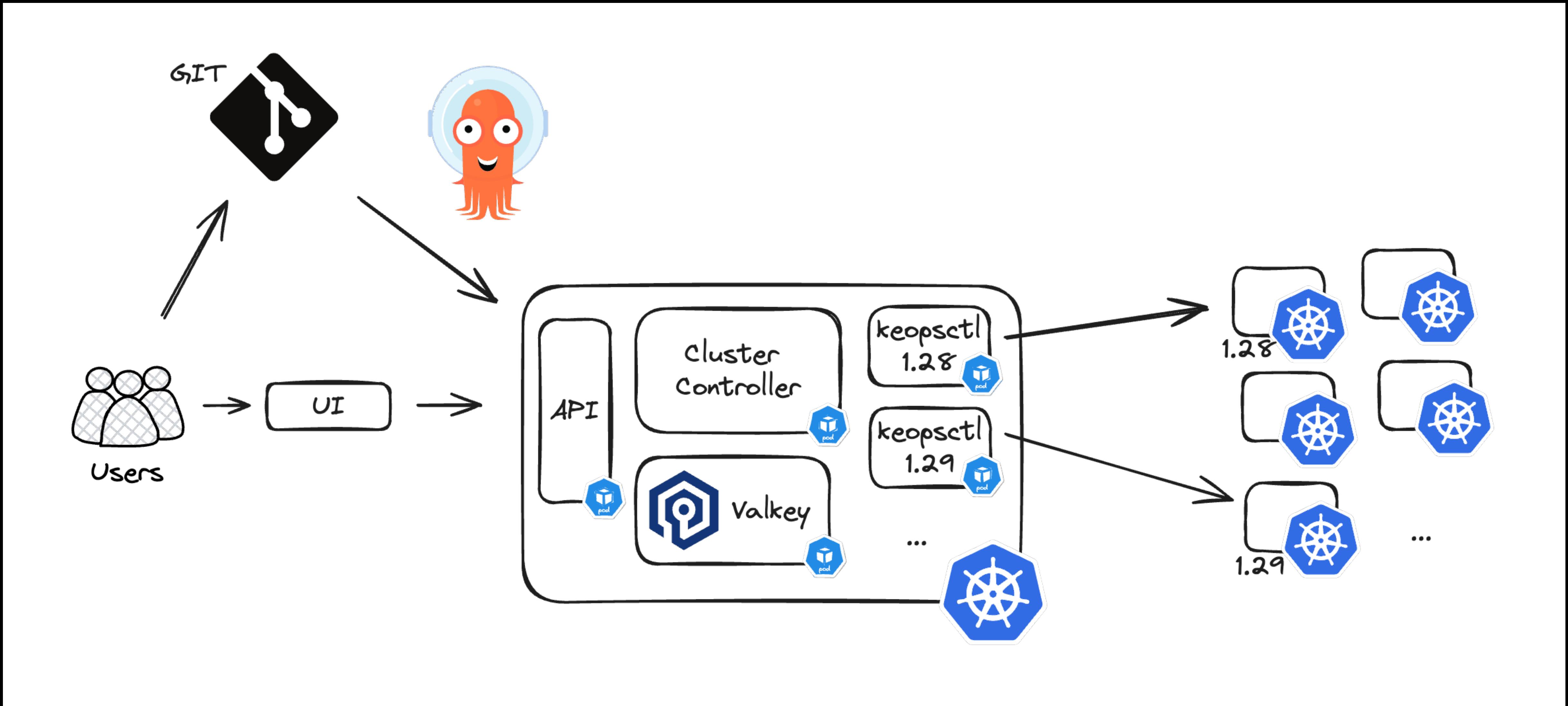
- ✓ Still based on upstream Kubernetes
- ✓ Built our own CLI to manage cluster lifecycle
- ✓ Custom operator + CRD to describe clusters
- ✓ 1,000 clusters managed like any other resource

# Platform Stack Overview



In house Kubernetes distribution that ships pure upstream Kubernetes

# How Our Cluster Operator Works



# Cluster Custom Resource Example

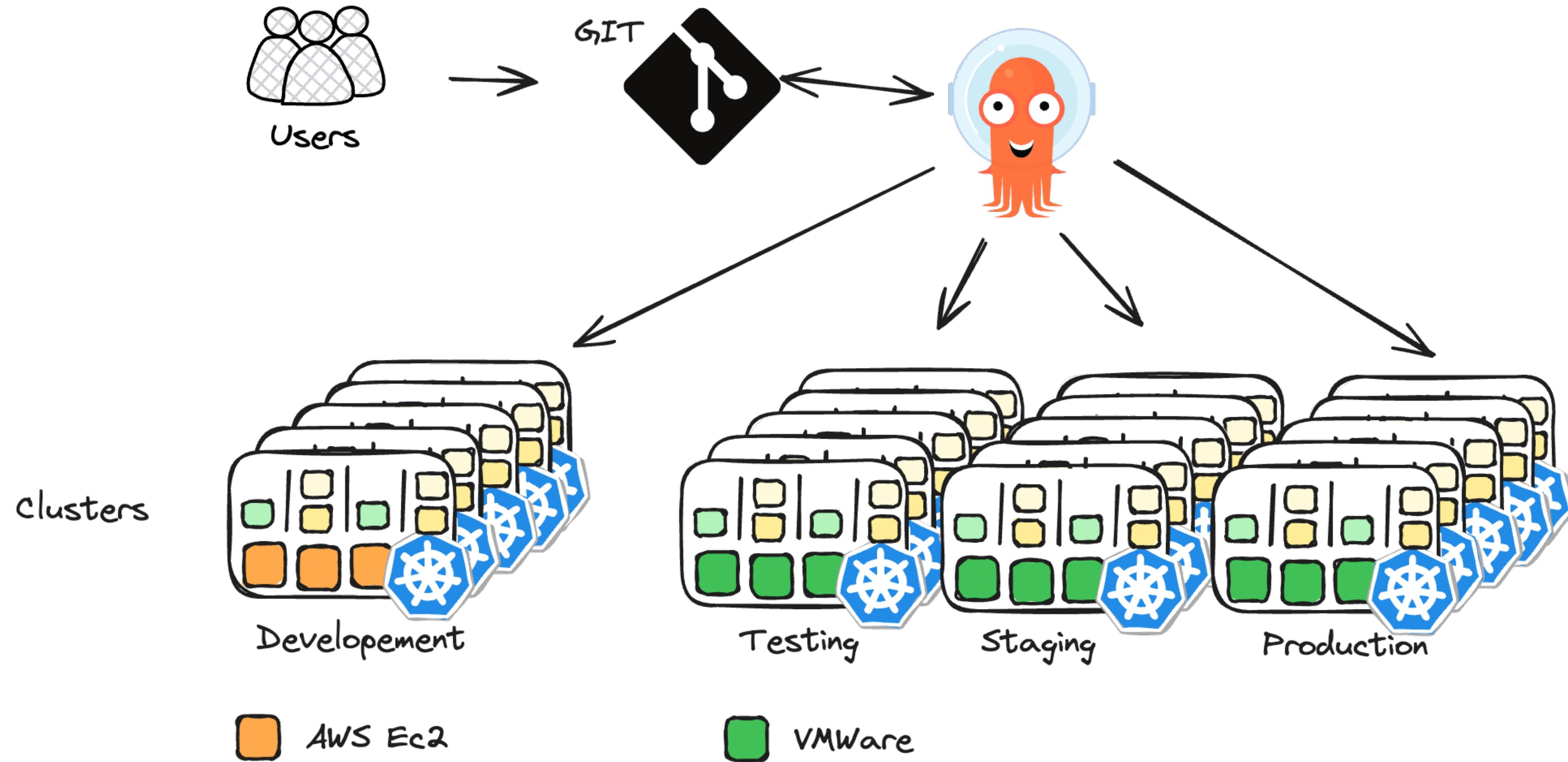
```
---
```

```
apiVersion: run.hosting.pictet.io/v1beta1
kind: KubernetesCluster
metadata:
  name: cncf-prod-demo
  annotations:
    ct.run.hosting.pictet.io/batch-sync-disabled: "true"
spec:
  identification:
    product: cncf
    environment: prod
    function: demo
  topology:
    controlPlane:
      count: 1
  settings:
    runtime:
      target: aws-eu-common-devext
    network:
      subnet: aws-eu-common-devext-sn-11
  flags:
    - key: CICD_ARGOCD_MANAGED
      enabled: false
  nodes:
    - id: 4
      instanceType: t3a.xlarge
```

# Enabling a Smooth Migration

1. Build trust with developers
2. Support change: Genius Bar, docs, onboarding
3. Co-create with devs, without sacrificing Day 2
  - Enhancement request process
  - Feature flags for safe rollout

# The Developer Experience



# Key Benefits of the New Platform

- ✓ Faster Kubernetes upgrades
- ✓ Better isolation and reliability
- ✓ Scalable platform: 1,000+ clusters
- ✓ Developer autonomy preserved
- ✓ Secure, repeatable, observable by design

# Lesson learned

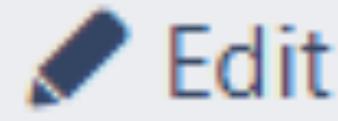
- ✓ One cluster doesn't scale forever
- ✓ Tenancy at the cluster level brings clarity
- ✓ Treat clusters as declarative resources
- ✓ Co-building with developers is key
- ✓ Invest in platform UX, not just infra

# Our simple change request



ITSM - Change Management / CHG-80902

## Release Management 1000 clusters on a Saturday



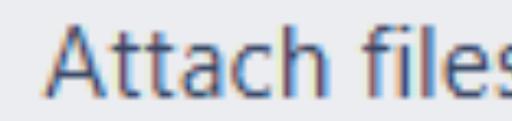
Edit



Add comment



Log work



Attach files



More



In Preparation

### Details

Type:



Generic Change

# Gradual rollout with no impact

200/1000 : OK

500/1000 : OK

700/1000 : OK



# We can do it

1000/1000



# Takeaways

1. Be perseverant.
2. Break the silos in infra teams.
3. Don't impact developer.

# Thank You!

- Thank you for your attention
- We're happy to take your questions!