CNCF CLOUD NATIVE MEETUP MADRID - OCTOBER 2023

GitOps at Real Scale with Fleet Project

Juan Herrera Utande - SUSE

Agenda

CLOUD NATIVE COMMUNITY GROUPS IBERIA

1. Introduction to CI/CD
2. What is Fleet (and Rancher)
3. The architectural challenges of Continuous Delivery
4. Fleet design principles
5. Other features summary
6. Some project numbers

What is Continuous Delivery? Learn the jargon first

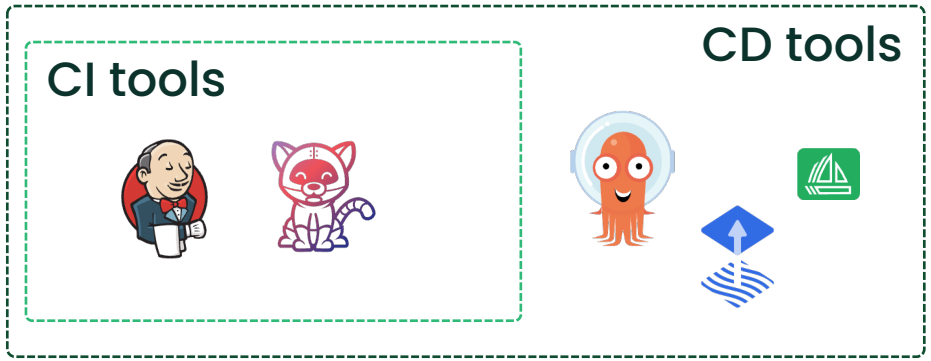
CLOUD NATIVE COMMUNITY GROUPS IBERIA

1. **Continuous Integration (CI)** is a software development approach where developers regularly merge their code in a central repository. Automated validations, builds, and tests are then triggered helping to surface any integration problem early in the process

2. **Continuous Delivery/Deployment (CD)** complements CI to cover the automated deployment of all those software artifacts produced by the CI process in a set of target environments

3. **DevOps** is a much broader practice that integrates the development best practices as defined on CI/CD to also cover the operational aspect of application management and life cycle. The name comes from the union of the Development and Operations worlds.

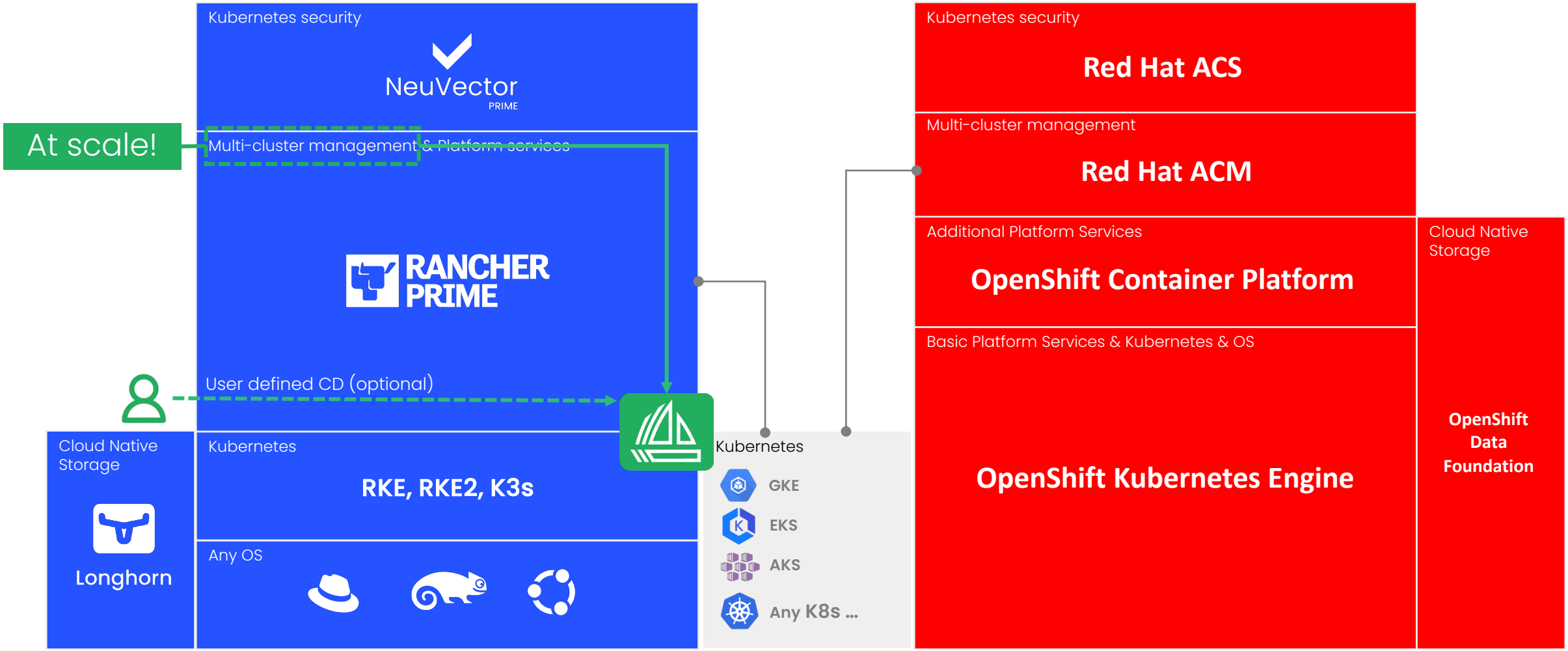
4. **GitOps** is an operations framework built around DevOps best practices that use Git as the source of truth for deployments and environment configuration management (e.g., Kubernetes), ensuring system state alignment and providing an audit trail with rollback capability



What is Fleet?

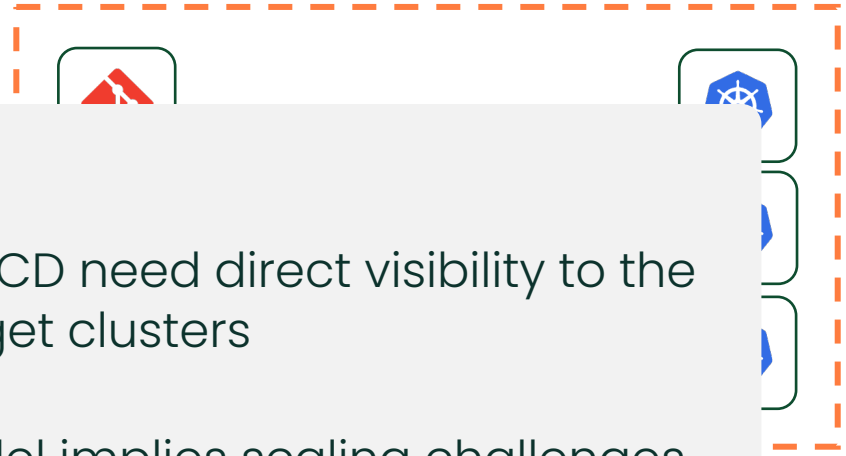
- Fleet is a Continuous Delivery/Deployment open-source tool.
- It's a Kubernetes-native application so it's API first and relies on CRDs and Operators.
- Created in 2020 by Rancher to offer CD capabilities more closely aligned to the Rancher Kubernetes management philosophy (Kubernetes at **scale**)
- Used internally by Rancher Management Application to manage downstream clusters, also available to end users to implement their own CD strategy
- It can work together and coexist with other CI/CD tools like ArgoCD and Flux
- Relevant links:
  - Website: https://fleet.rancher.io/
  - Git: https://github.com/rancher/fleet

What is Rancher?



ArgoCD (& Flux) architectural challenges

ArgoCD is great!



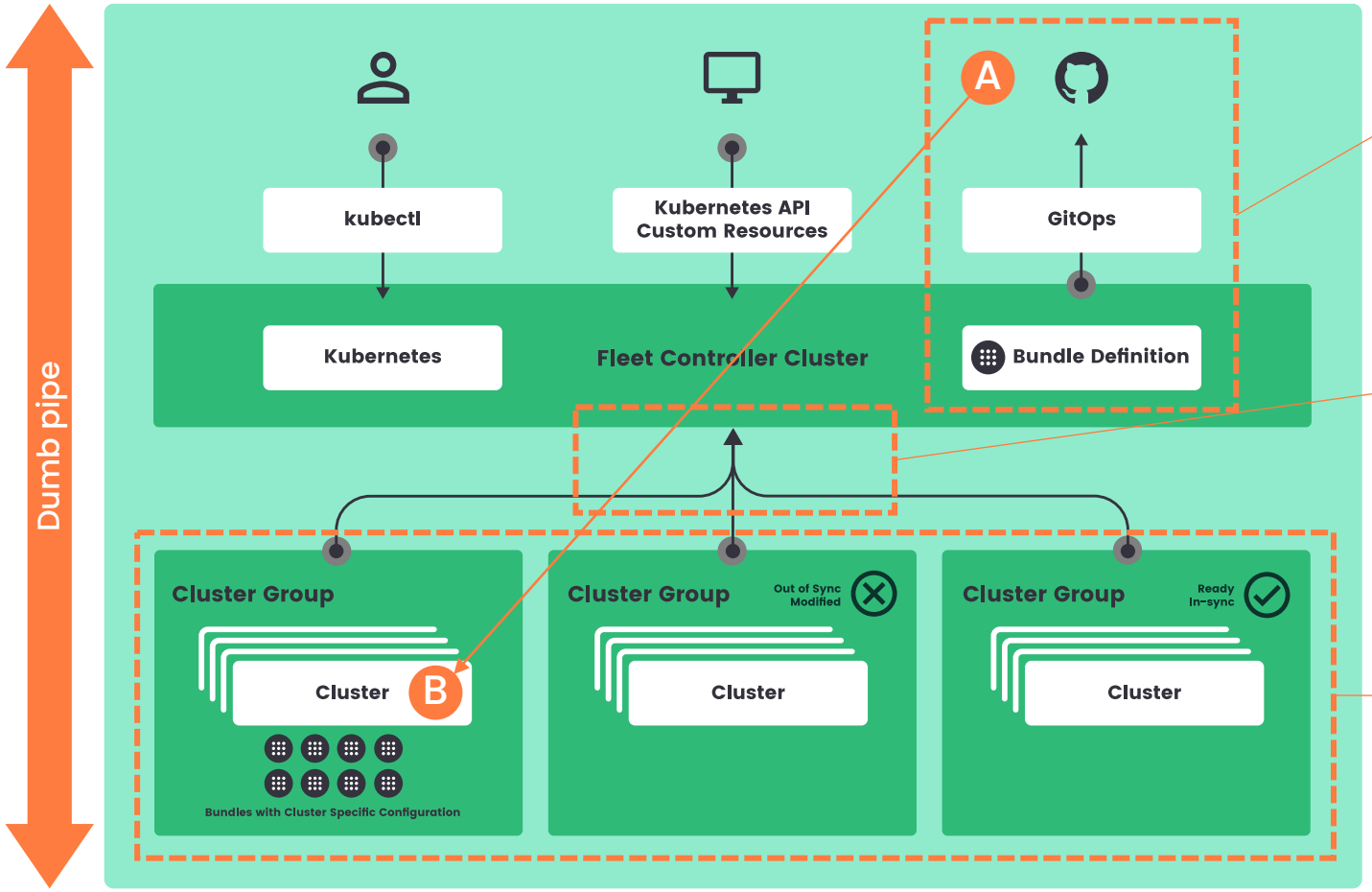
Some limitations:

- **Security**: ArgoCD need direct visibility to the K8s API of target clusters
- **Scale**:
  - Push model implies scaling challenges (usually just few tens of clusters)
  - Complex topologies or complex operational models needed to use it at scale

Fleet design principles

- Keep it simple: dumb pipe model
- ”Unlimited” scale
  - Pull vs Push
  - Advanced targeting
  - Bandwidth optimization
- How to allow secure and flexible topologies

How to scale better with Fleet: main pillars

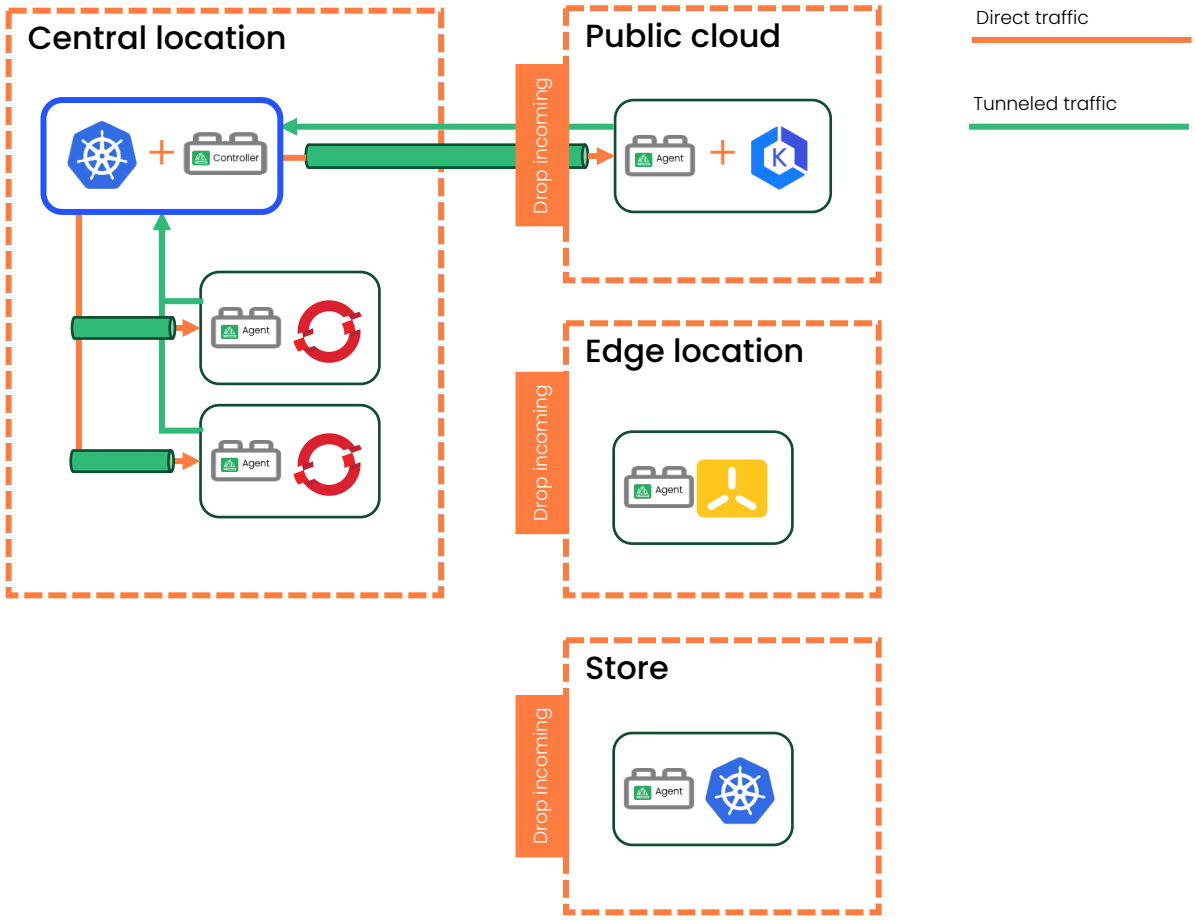


Network traffic optimization

Downstream clusters **PULL** Git repo status and definitions (bundles) from the main Fleet Controller Cluster or Rancher Management Cluster

Advanced targeting and variables: how to target hundreds of repos to thousands of Kubernetes clusters

Secure and flexible topologies



- The management layer doesn't need direct access to managed clusters. No exposed endpoints.
- Simplified FW and networking.
- Expiring registration tokens and restricted Service Account (only access to list bundles, and check bundle and cluster status)
- Direct traffic used for payload: get Bundles, check for repo changes, ...
- Tunneled traffic just used to check cluster/bundle state, ...
- Supports non persistent links and air gapped scenarios*

Other features summary

- Full support for Helm and Kustomize
- Git: Multi-repo and multi-branch
- Git: Both polling and web-hook modes
- Helm: support for dependency resolver
- Granularity: Cluster, Cluster Group and Evnironment
- Powerful Targeting Semantics
- Built-in RBAC*
- Store Fleet configuration (fleet.yaml) at managed Git repos
- ...

Some real world numbers

CLOUD NATIVE COMMUNITY GROUPS IBERIA

- Theoretical scale up to 1 million clusters (blame etcd!)
- QA works on the 10.000 mark
- Some real-world customer using Fleet:
  - Retail: +1000 K3s managed clusters
  - Surveillance cameras: 1 single node K3s cluster per camera. Avg. 50 cameras per venue, designed to scale up to 250
  - Industrial Edge: 120 factories with 2 clusters per factory. ~50 different source repos
  - Telco: network access platform with 900 locations (1x3 node K3s cluster per location)
- Remember: every cluster managed by Rancher uses Fleet underneath …

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Frankenstrasse 146

90461 Nürnberg

www.suse.com