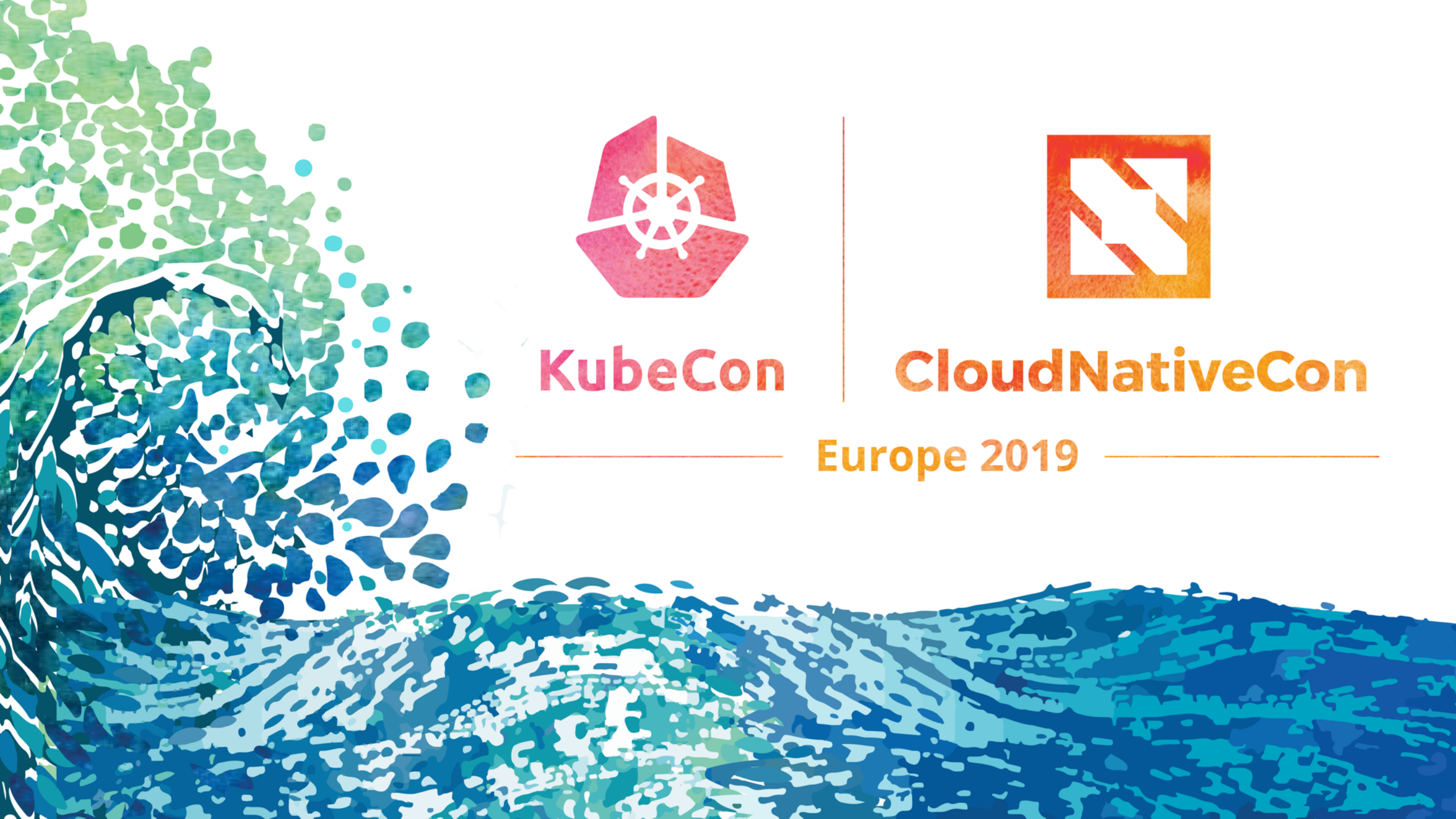

KubeCon
CloudNativeCon
Europe 2019

KubeCon | CloudNativeCon Europe 2019

# From Snowflake Servers to Snowflake Clusters

## Our GitOps Journey

Allison Richardet & Fabio Giannetti

# Topics



- Security
- Common workloads
- GitOps

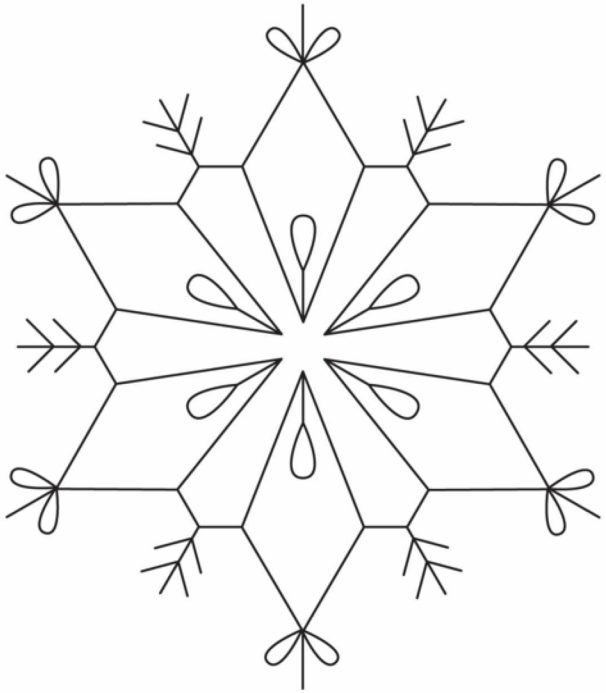
# Patterns & Snowflakes



Difficult to Reproduce

Hard to debug & test

Lack of audit trail

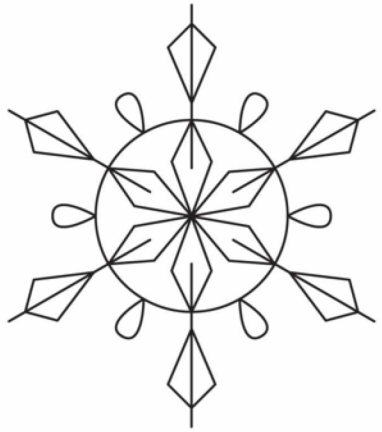


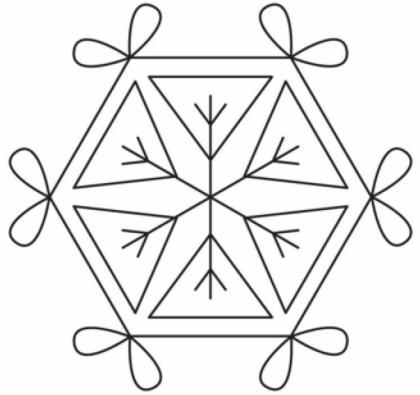
© Mollie Johanson

Change/upgrades problematic

Instances out of sync

Environment mismatch





# Problem

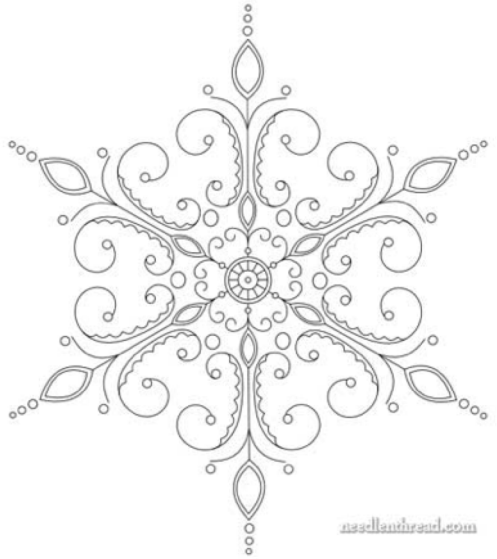


- Application teams need to move legacy applications to containerized workloads
- Constraints
  - Region requirements
  - Security concerns
- Developer and Operator experience

# Vision



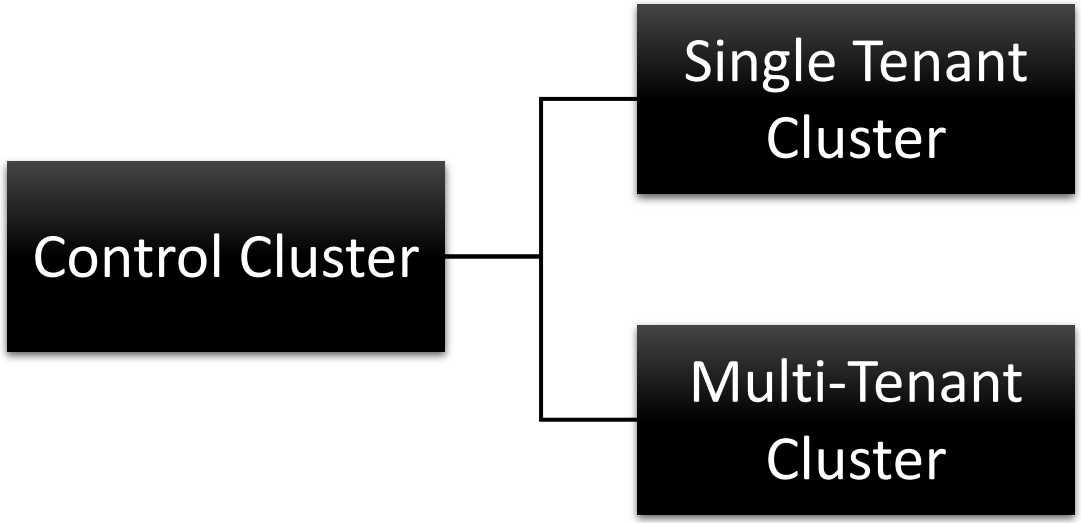
- Security
  - Multi-tenancy
- Common services based on patterns
- Structured onboarding for tenants



# How



- Manage different types of clusters
- Automated deployments & base services
- Tenant Workloads – options & customizations



# Timeline

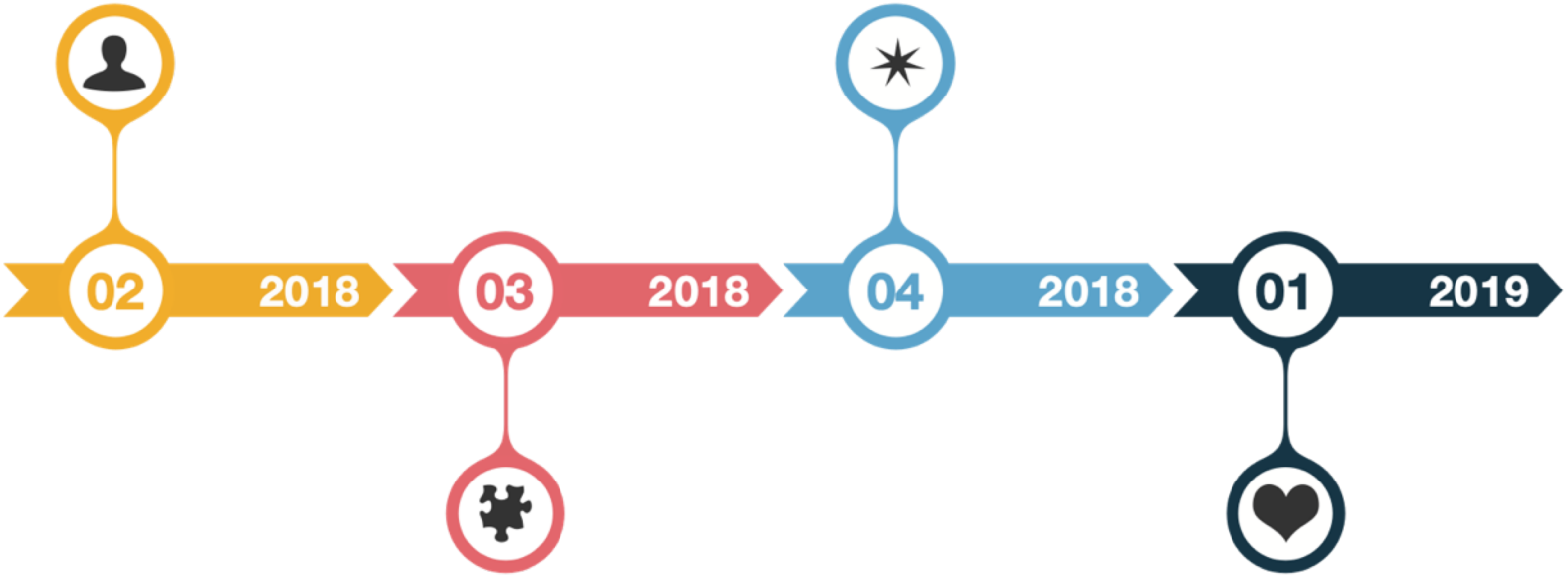


## Introduce Kubernetes

Introduction to application teams
Excitement in technology &
Ability to control deployments

## Snowflake Prevention

Consolidate base services
Automation
Scalable, Redundant & Secure




## Complexity

Application teams overwhelmed
Difficulty navigating technology

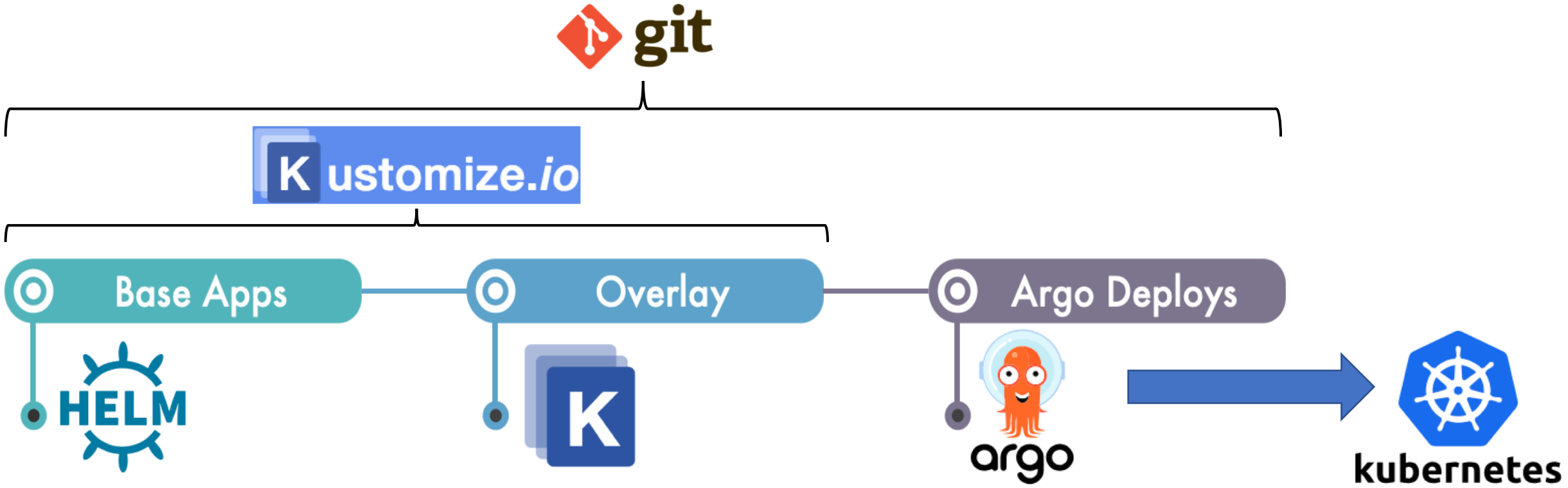
## Tenant Management

Tenant Isolation
Extend base services
Custom dashboards

# GitOps

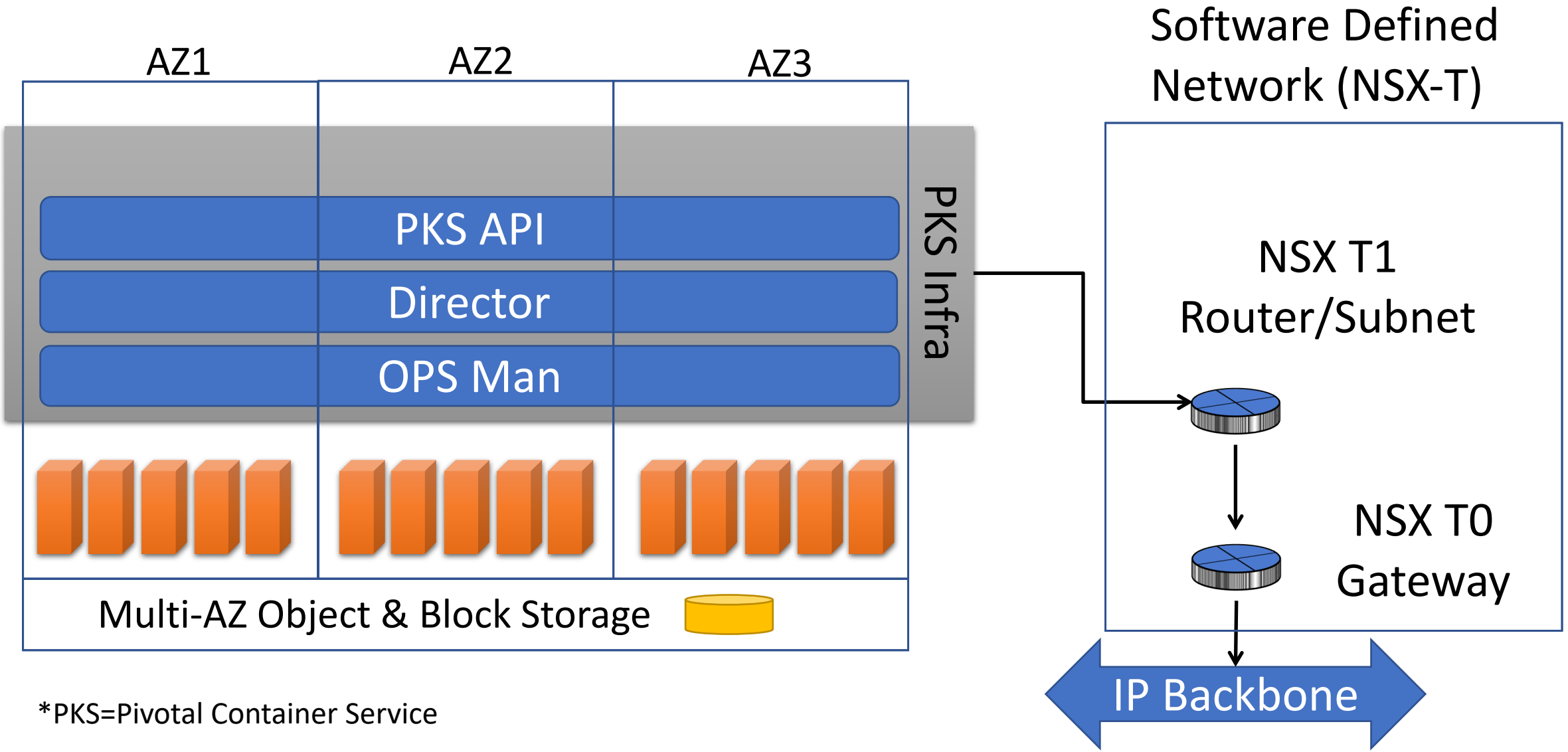


- Store state in Git – source of truth
- Manage deployments from Git
- Argo CD ensures the cluster state matches Git



# On-Prem Infrastructure

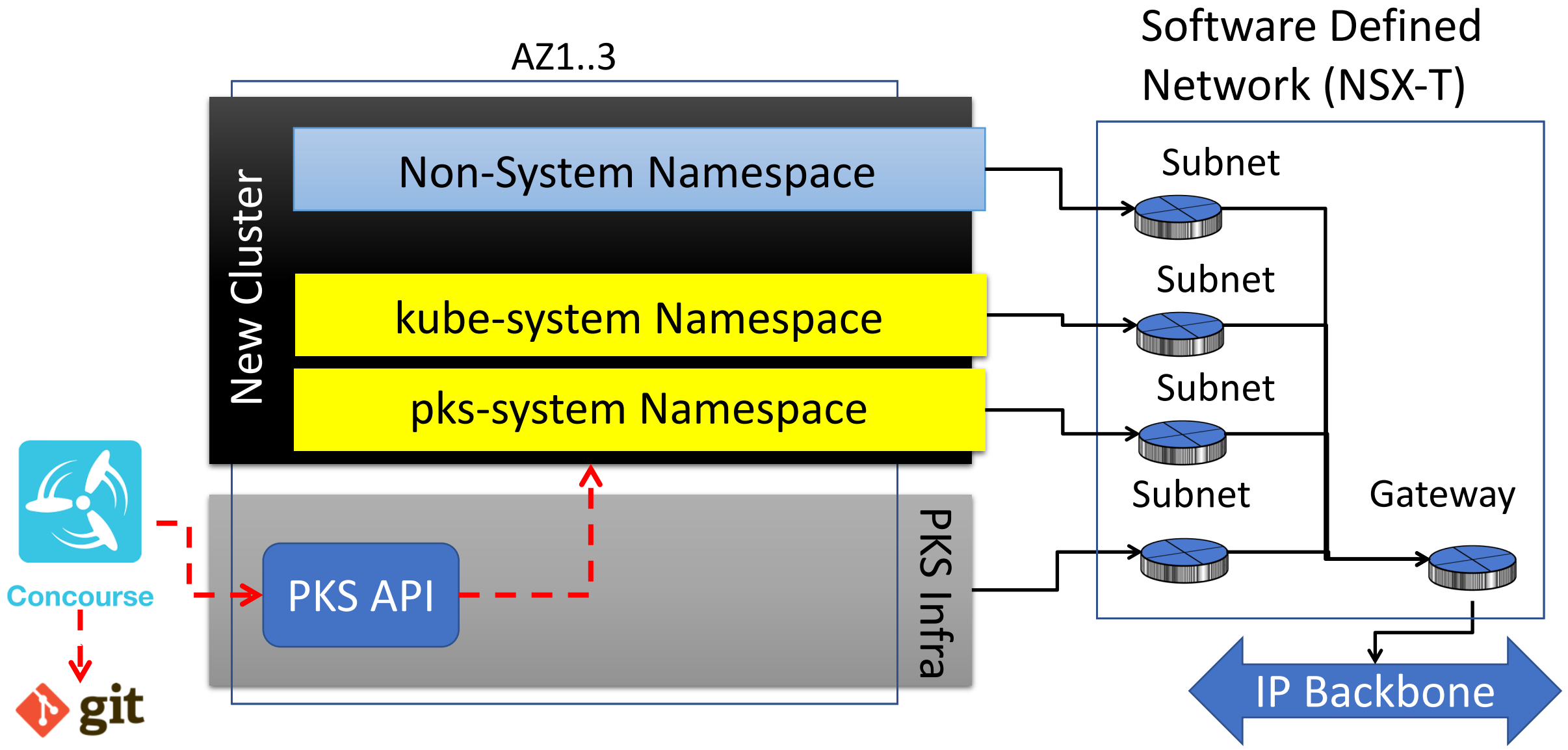





*PKS=Pivotal Container Service

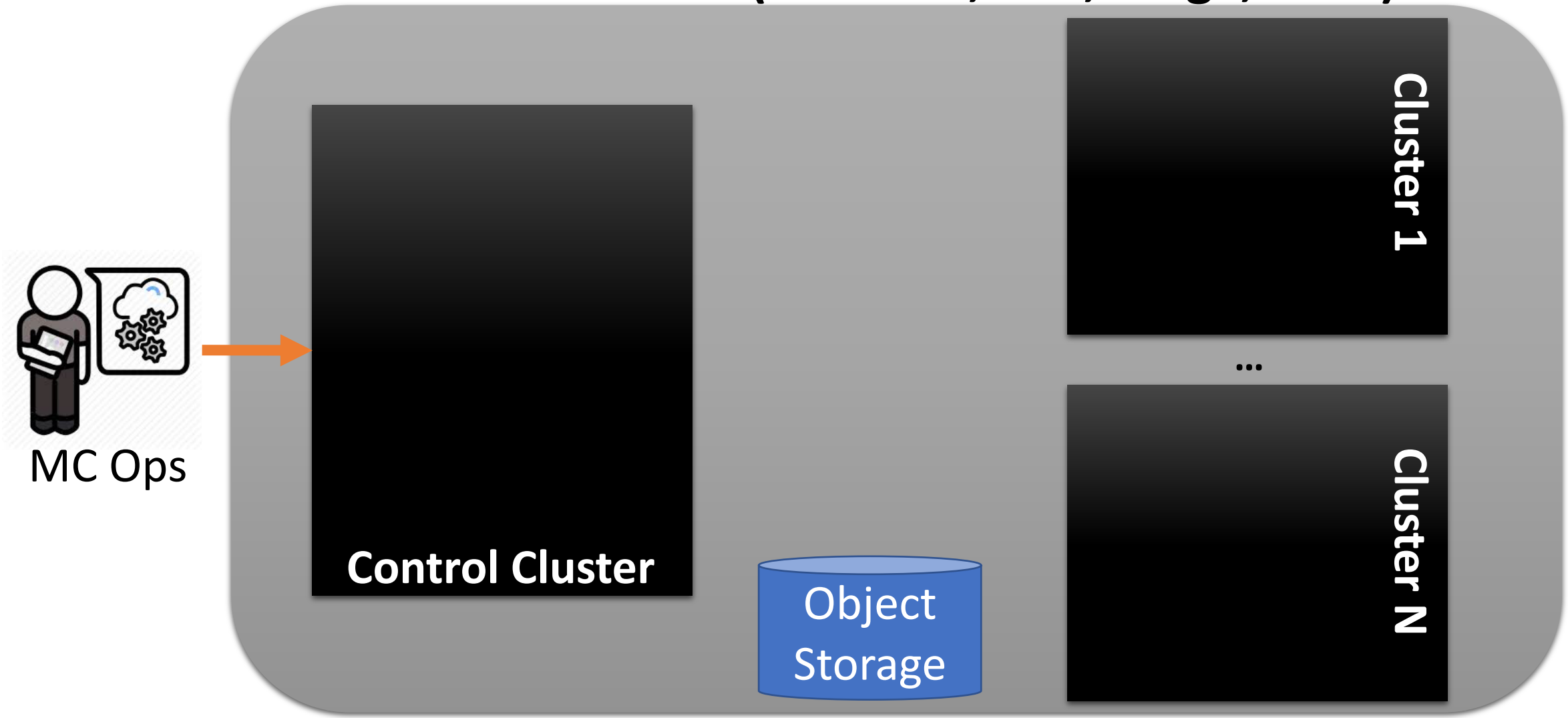
# Creating New K8s Clusters





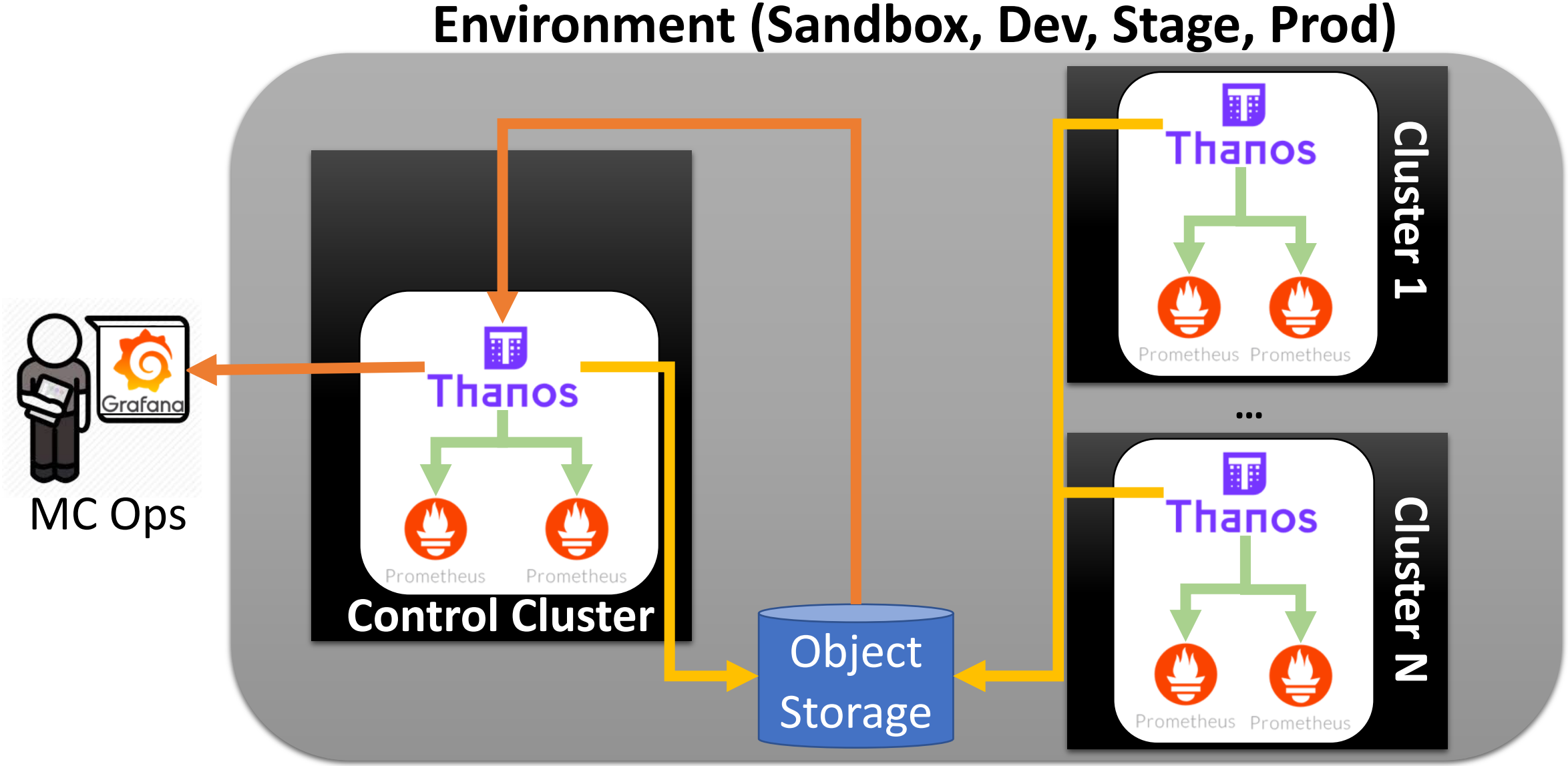
# Control Cluster





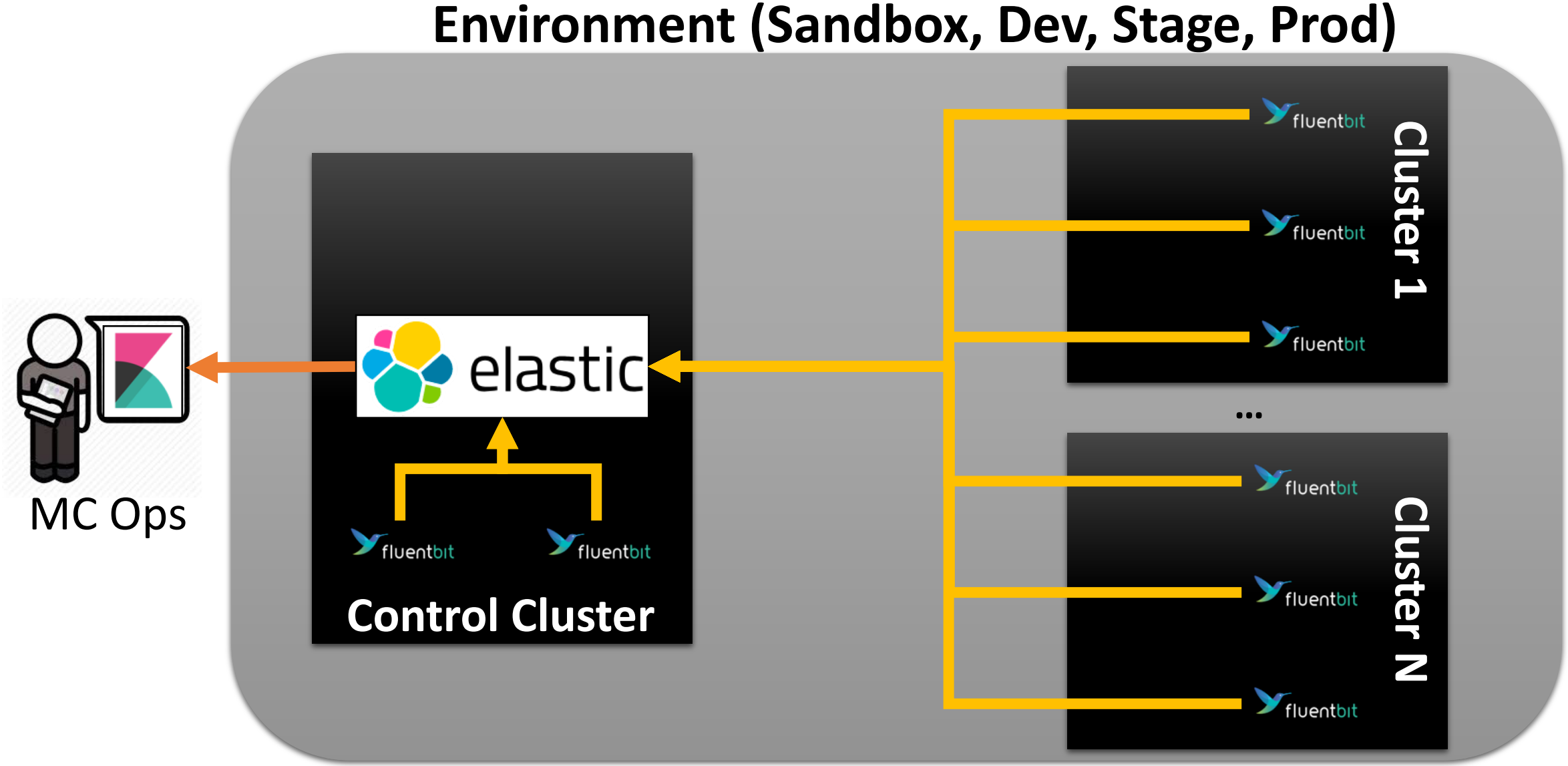
# Single Pane of Glass - Monitoring





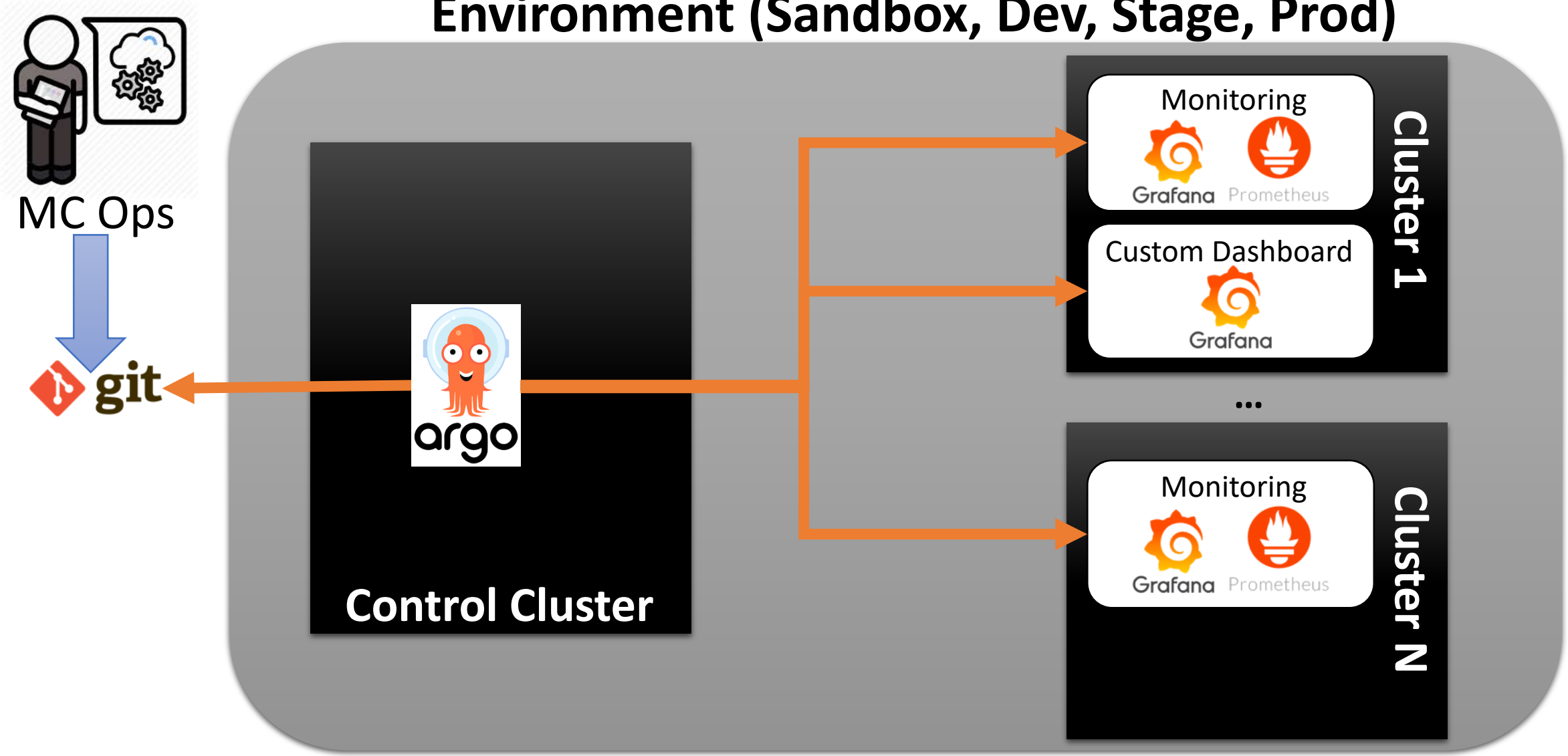
# Single Pane of Glass - Logging





# Unified CD Strategy





# Kustomize Overview

```
apiVersion: v1beta1
kind: Ingress
...
name: kibana
spec:
tls:
- hosts:
  - kibana
rules:
- host: kibana
...
```

```
- op: replace
path: /spec/tls/0/hosts/0
value: kibana.kubecon.mc.com
- op: replace
path: /spec/rules/0/host
value: kibana.kubecon.mc.com
```

```
apiVersion: v1beta1
kind: Ingress
...
name: kibana
spec:
tls:
- hosts:
  - kibana.kubecon.mc.com
rules:
- host: kibana.kubecon.mc.com
...
```

# Cluster Creation and Provisioning

Concourse

PKS API

Cluster Request Commit

MC Cluster CRD

MC A-la-Carte SVCs CRD

MC Cluster Mapping CRD

App Definitions

Kustomize Overlays

Kustomize Deployments

Argo Applications

git

JOB

argo

Provisioning

Control Cluster

New Cluster

Core Service

POD

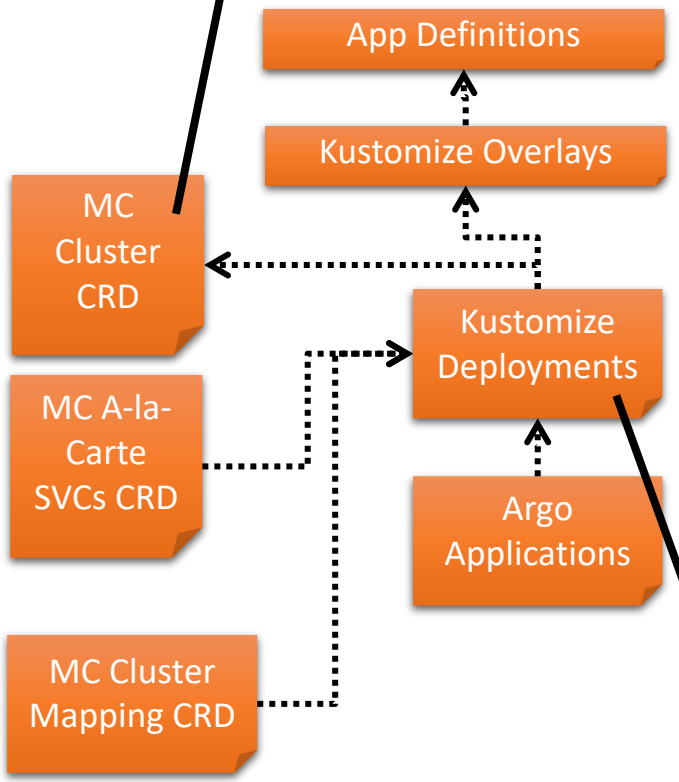
POD

A-La-Carte Service

POD

# CRD – Cluster Spec



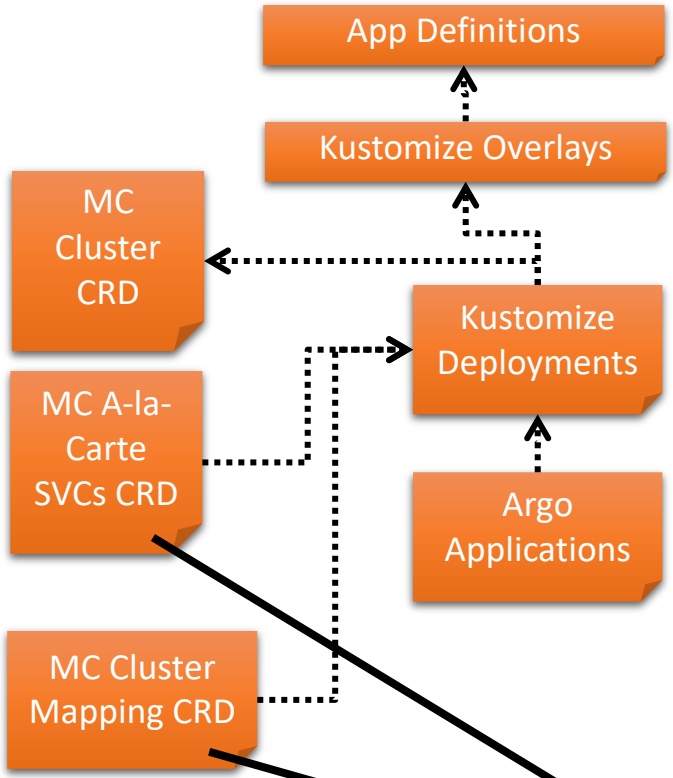



```
apiVersion: kubernetes.mc.com/v1beta1
kind: ClusterSpec
metadata:
  name: cluster-specificat
spec:
  clusterURL: https://clust
  clusterName: card-loyalt
  baseFQDN: dev.example
  clusterType: cardLoyalty
  inheritFromTypes:
    - singleTenant
    - piiData
    - pciCompliant
  clusterNodes: 10
  clusterPlan: medium
```

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
- cluster-spec.yaml
vars:
  - name: CLUSTER_NAME
    objref:
      kind: ClusterSpec
      name: cluster-specification
      apiVersion: kubernetes.mc.com/v1beta1
      fieldref:
        fieldpath: spec.clusterName
  - name: CLUSTER_FQDN
    ...
  - name: CLUSTER_URL
    ...
```

# CRD – Mapping Spec



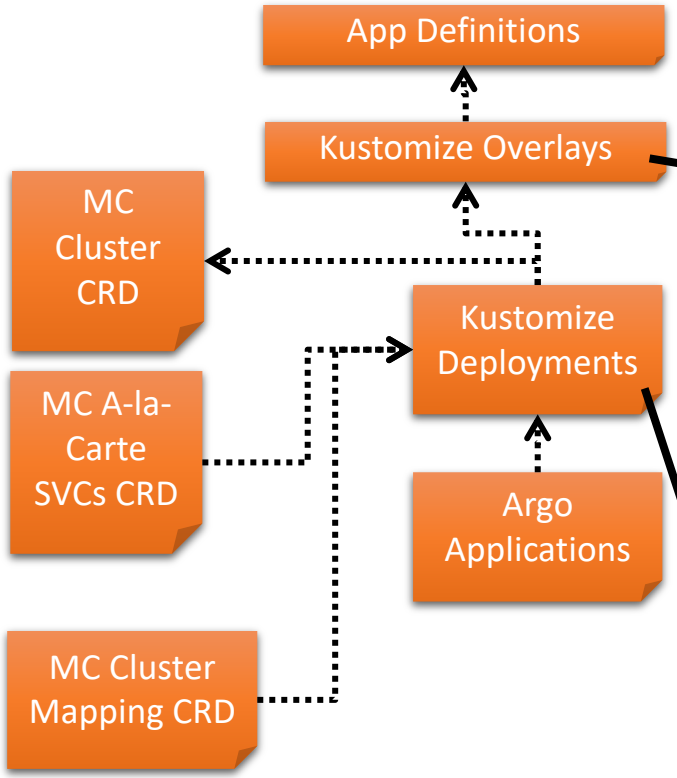



```
apiVersion: kubernetes.mc.com
kind: MappingSpec
metadata:
   name: a-la-carte-specificatio
   app-name: mc-loyalty
spec:
   cardLoyalty :
      project: card-loyalty-servi
      apps:
        - name: storage-service
          folderName: storage-s
          baseURL: ../../../../../a-
          automatedSync: true
        - name: queue-service
          folderName: queue-se
          baseURL: ../../../../../a-
          automatedSync: true
```

```
apiVersion: kubernetes.mc.com/v1beta1
kind: MappingSpec
metadata:
   name: mapping-specification
spec:
   core :
      project: core-services
      apps:
        - name: monitoring …
        - name: logging …
   singleTenant:
        …
   piiData:
        project: pii-services
        apps: …
          - name: pii-logging
   pciCompliant:
        project: pci-services
        apps: …
```

# Kustomize






```
- op: replace
  path: /spec/rules/0/host
  value: kibana.$(APP_NAME).$(CLUSTER_NAME).$(CLUSTER_FQDN)
- op: replace
  path: /spec/tls/0/hosts/0
  value: kibana.$(APP_NAME).$(CLUSTER_NAME).$(CLUSTER_FQDN)
```

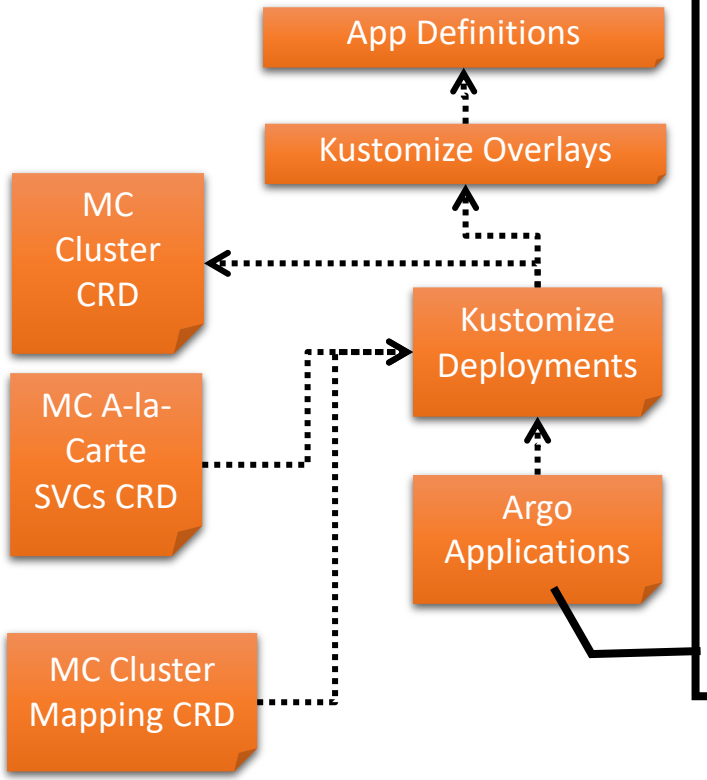
```
/pii-log
  kustomization.yaml
  patch-kibana-deployment.yaml
  patch-kibana-ingress-host.yaml
  patch-kibana-storage.yaml
```

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization

bases:
- ../../../../../pii-deployments/pii-logging
- ../../../specs/clusters/dev
```

# Argo CD Application






```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
name: $(CLUSTER_NAME)-$(APPLICATION_NAME)
namespace: argocd
spec:
  destination:
     namespace: $(APPLICATION_NAMESPACE)
     server: $(CLUSTER_URL)
     project: $(PROJECT_NAME)
   source:
     path: environments/dev/deployments/$(CLUSTER_NAME)/$(APPLICATION_NAME)
     repoURL: https://some-git-repo.com/kube_environments.git
     targetRevision: HEAD
```

# Future Plans

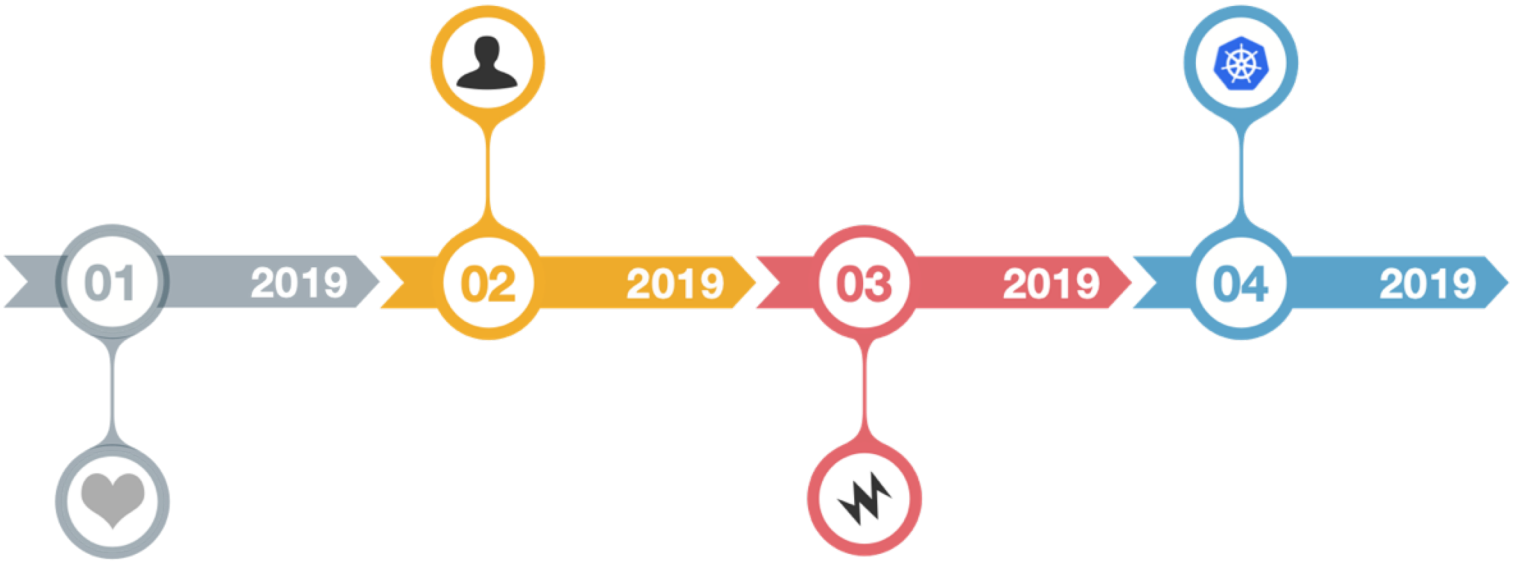


## Improve Onboarding

Improve tenant experience
Automation enhancements

## KubeCon US

Present updates
Share implemented tool




## Tenant Management

Tenant Isolation
Extend base services
Custom dashboards

## Application Rollout

UI for tenant on boarding
Simplify a la carte selection

# Takeaways



- Security
- Pattern from common needs
- GitOps
- Leverage CNCF upcoming technologies
  - Cluster API
  - Multi-tenancy SIG

# Thank you

@arichardet @fabi0g

@arichardet @fabgia

richardeta@objectcomputing.com

fabio.giannetti@mastercard.com

# References

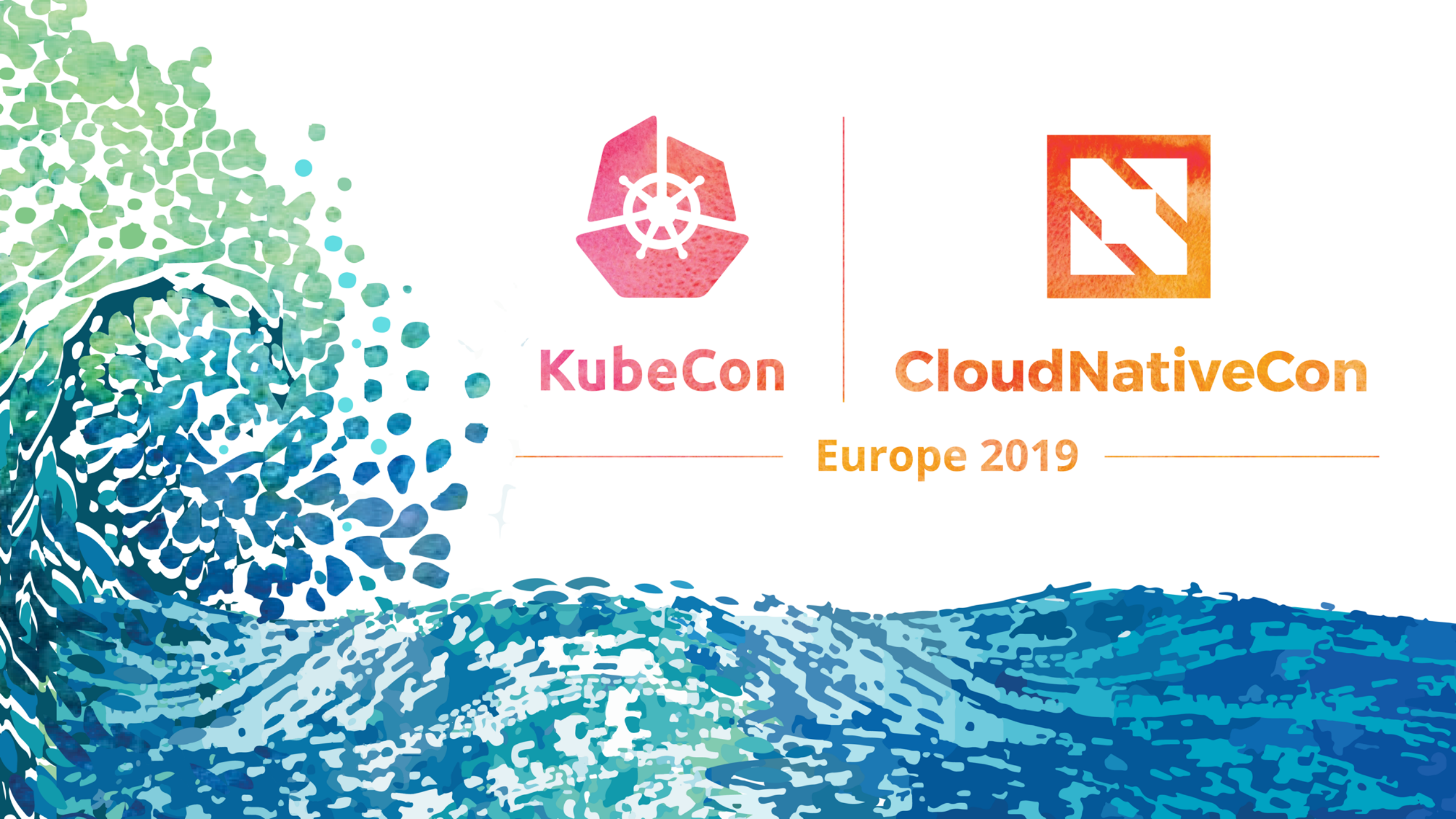
https://landscape.cncf.io/

https://concourse-ci.org/

https://pivotal.io/platform/pivotal-container-service

https://kustomize.io/

https://argoproj.github.io/argo-cd/


KubeCon
CloudNativeCon
Europe 2019