KubeCon | CloudNativeCon

Europe 2020

Virtual

Managing Multi-Cluster/Multi-Tenant Kubernetes with GitOps

Chris Carty, CKA/CKAD

JFrog

KubeCon | CloudNativeCon

Europe 2020

Virtual

GitOps Intro

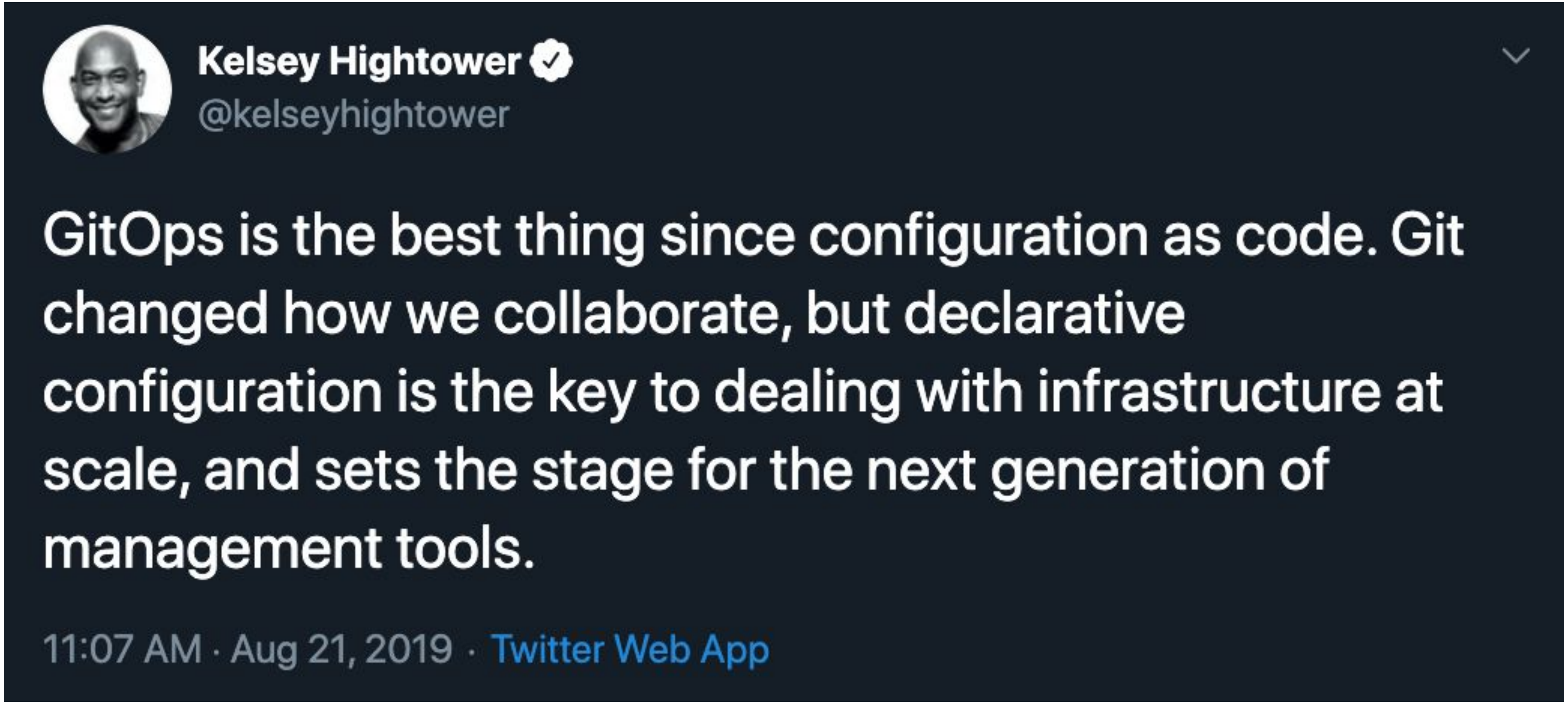
GitOps Intro

git

GitOps Intro

GitOps Intro

GitOps Intro

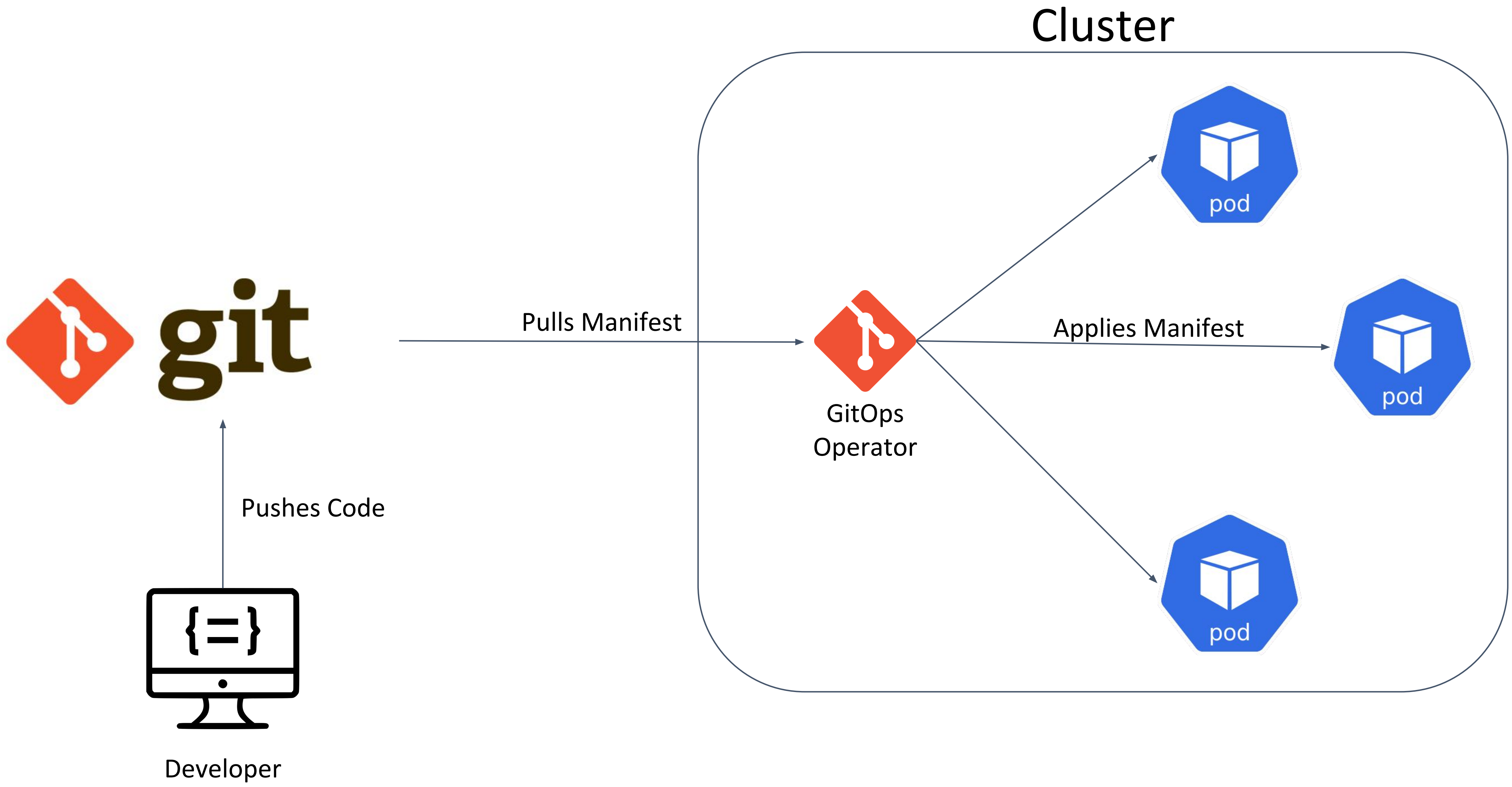


Kelsey Hightower ✓
@kelseyhightower

GitOps is the best thing since configuration as code. Git changed how we collaborate, but declarative configuration is the key to dealing with infrastructure at scale, and sets the stage for the next generation of management tools.

11:07 AM · Aug 21, 2019 · Twitter Web App

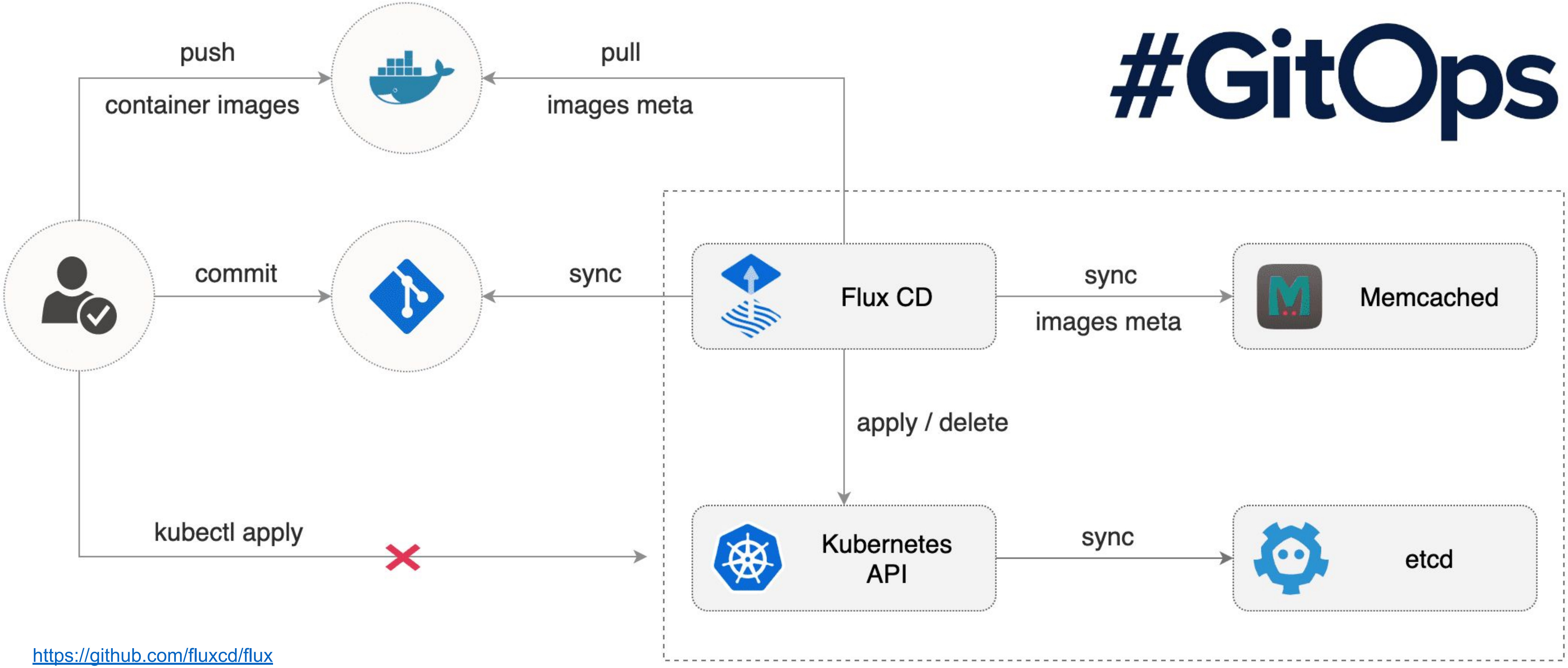
GitOps Intro



GitOps Intro

CNCF GitOps Operator Projects

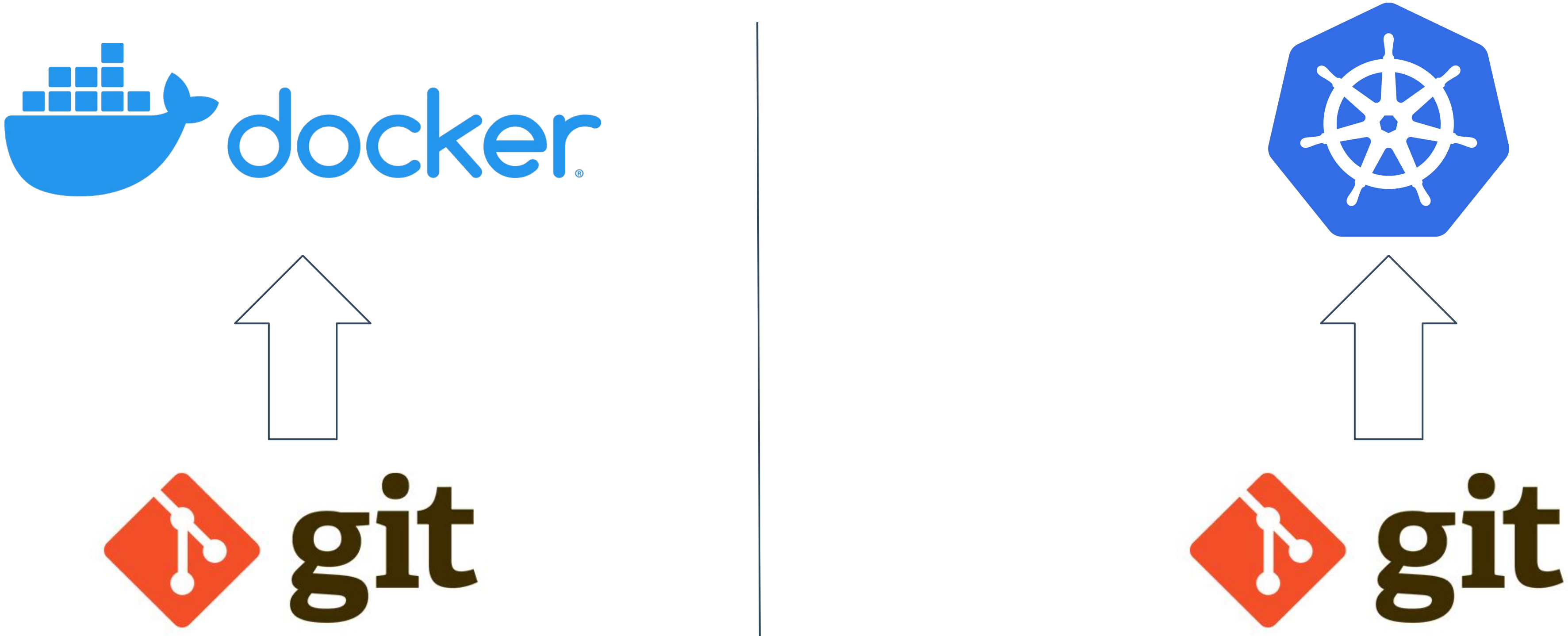
GitOps Intro



https://github.com/fluxcd/flux

Project Structure

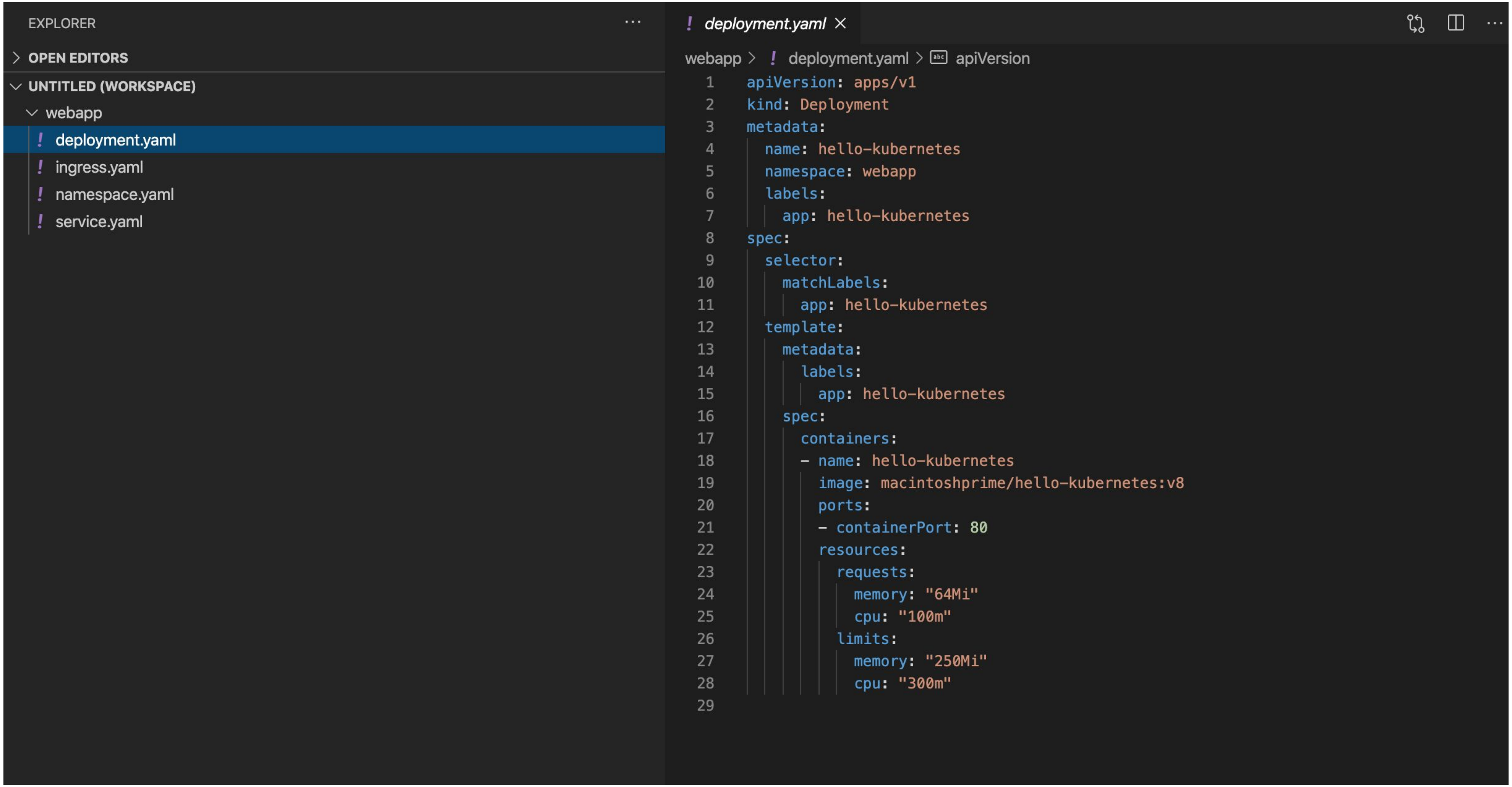
Project Structure



App Developer

App Operator

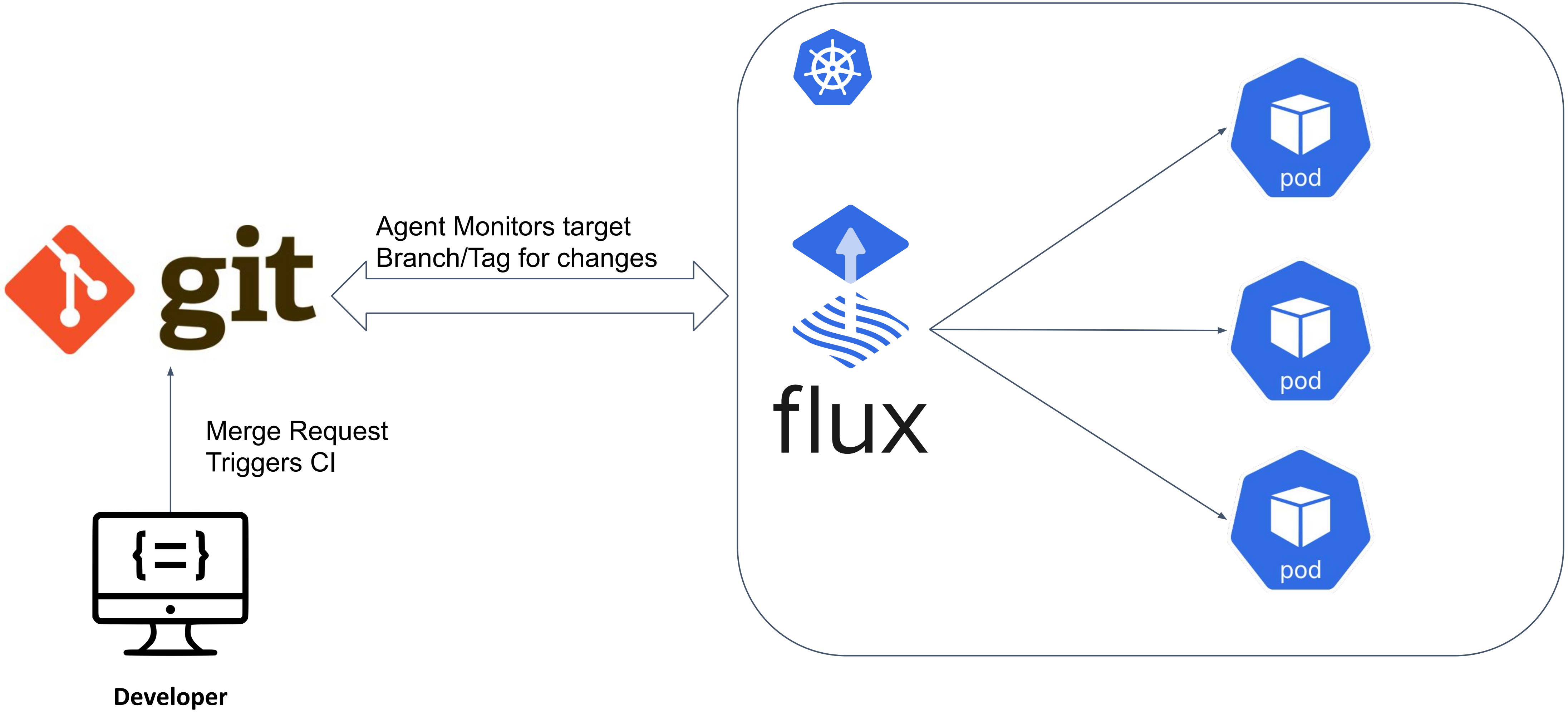
Project Structure



```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-kubernetes
  namespace: webapp
  labels:
    app: hello-kubernetes
spec:
  selector:
    matchLabels:
      app: hello-kubernetes
  template:
    metadata:
      labels:
        app: hello-kubernetes
    spec:
      containers:
      - name: hello-kubernetes
        image: macintoshprime/hello-kubernetes:v8
        ports:
        - containerPort: 80
        resources:
          requests:
            memory: "64Mi"
            cpu: "100m"
          limits:
            memory: "250Mi"
            cpu: "300m"

```

Project Structure


git
Agent Monitors target Branch/Tag for changes
Merge Request Triggers CI
Developer
flux
pod
pod
pod

Project Structure

Open Policy Agent

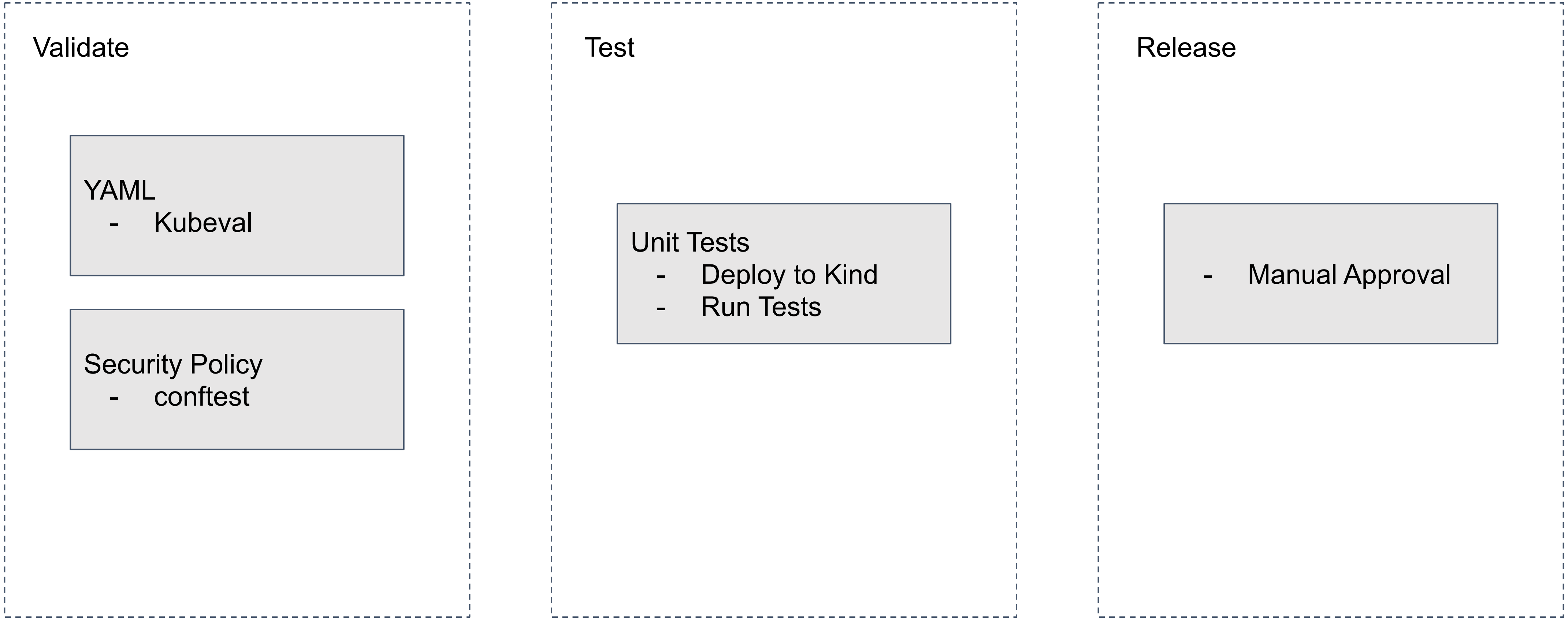
Conftest

kind

Kubeval

https://github.com/fluxcd/multi-tenancy

Project Structure



Validate

YAML
- Kubeval

Security Policy
- conftest

Test

Unit Tests
- Deploy to Kind
- Run Tests

Release

- Manual Approval

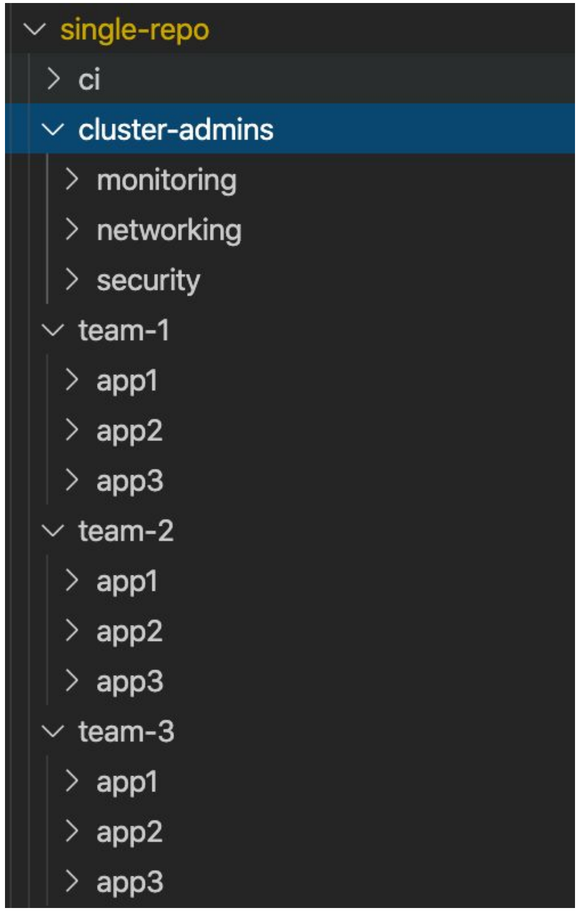
Project Structure

Single Repo

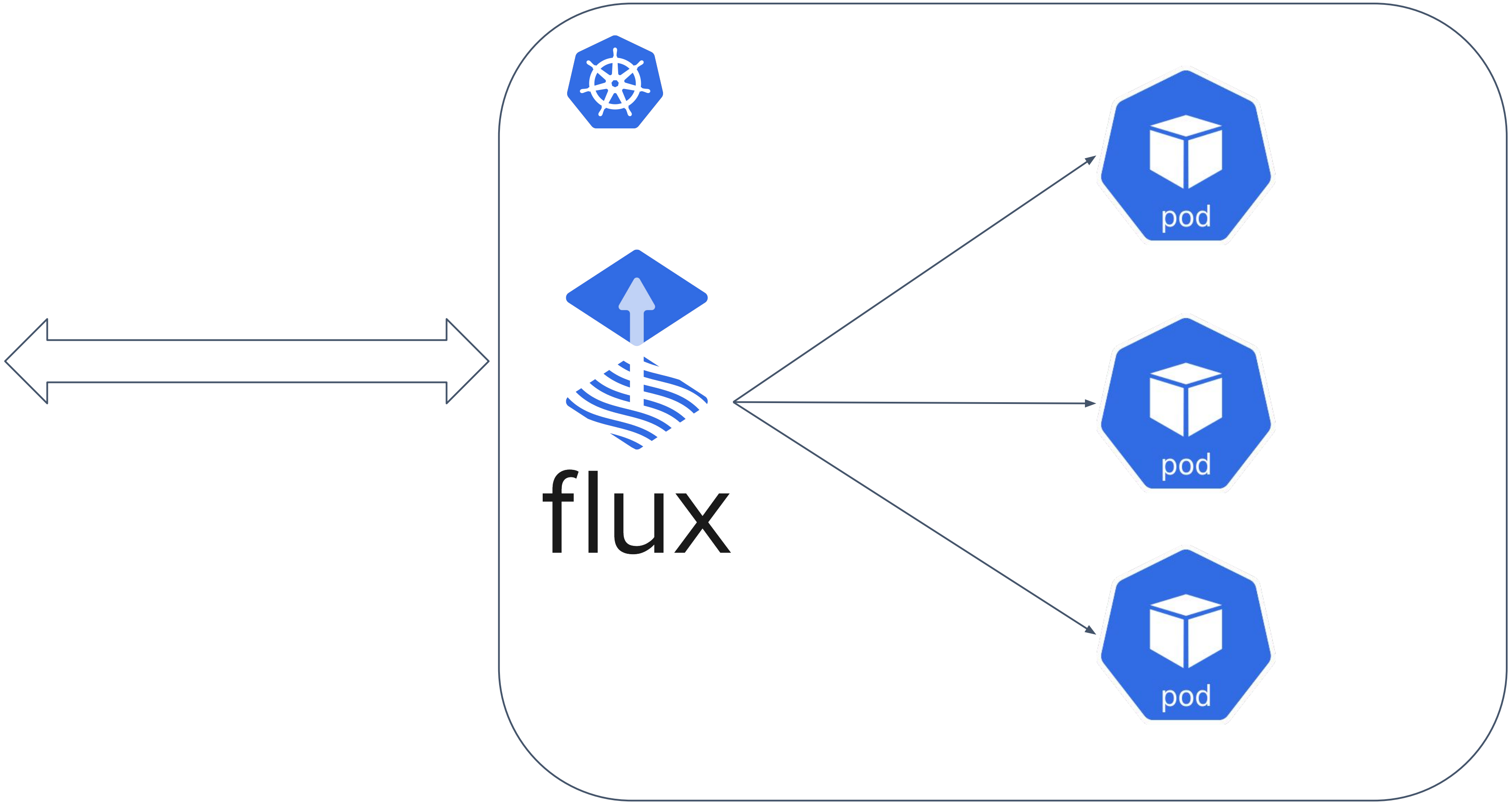
Multi-Repo

Single Repository

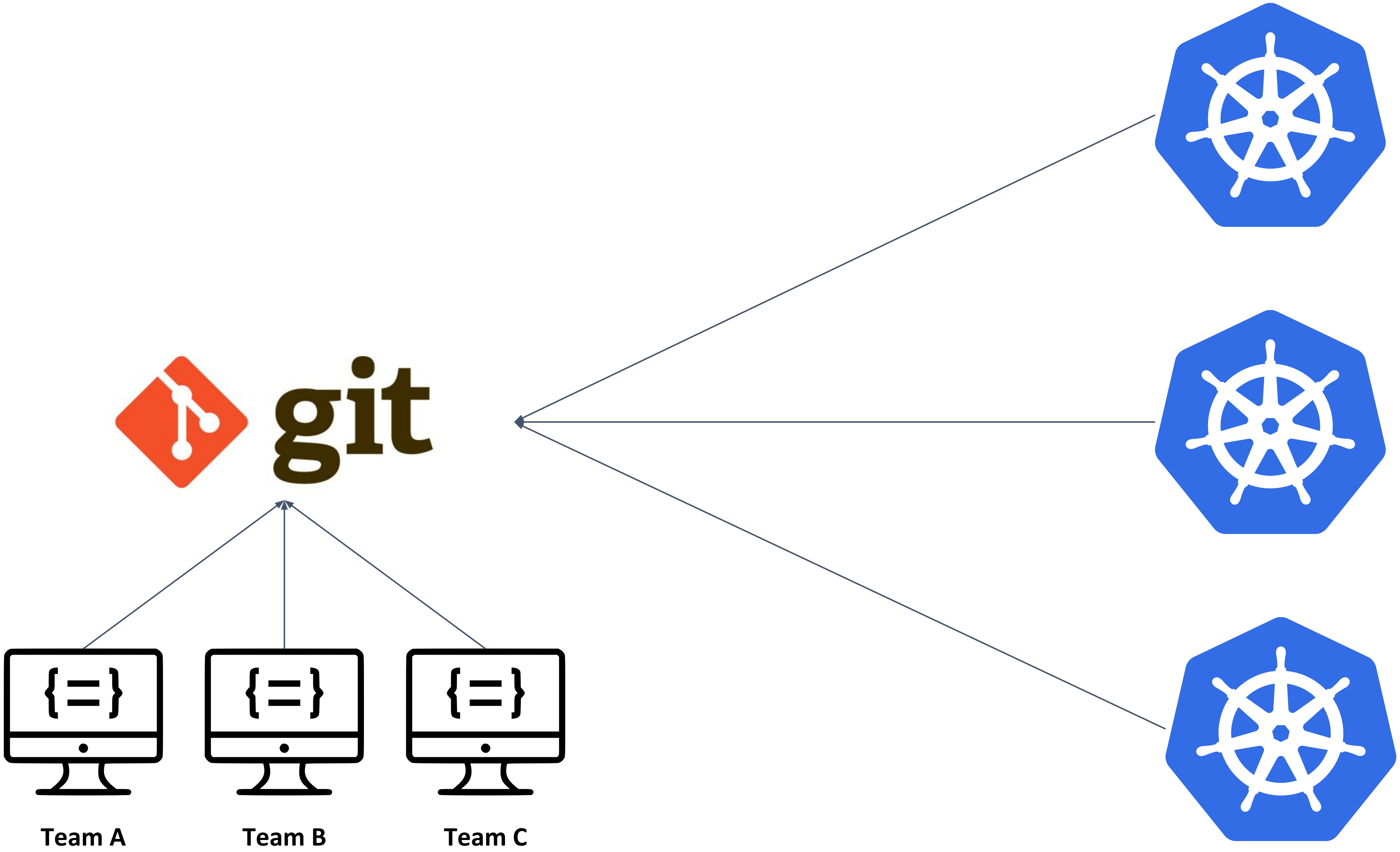
Single Repository



```
single-repo
  ci
  cluster-admins
    monitoring
    networking
    security
  team-1
    app1
    app2
    app3
  team-2
    app1
    app2
    app3
  team-3
    app1
    app2
    app3
```



Single Repository



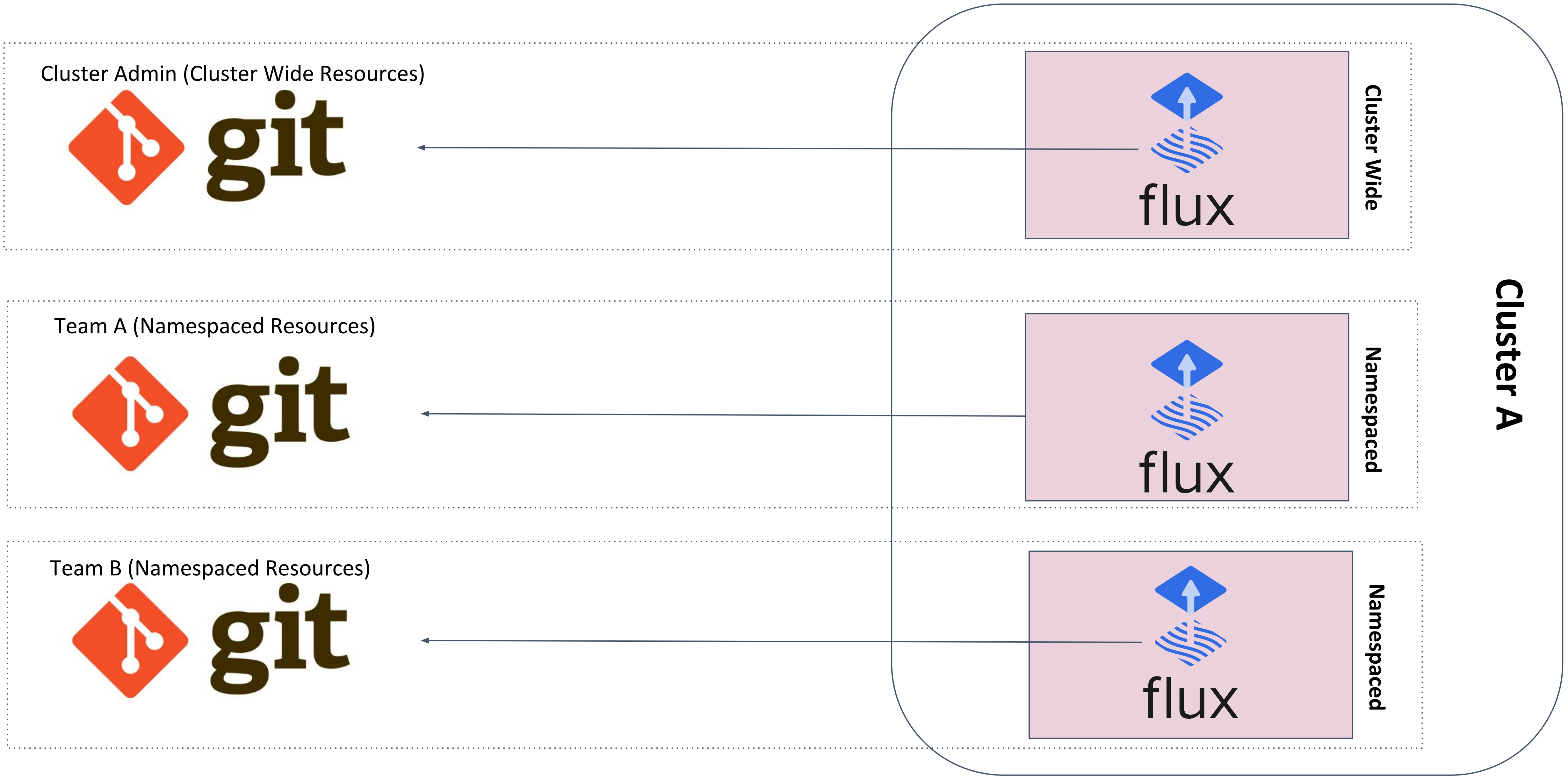
Dev
Sync's with Dev Branch
or Tag

QA
Sync's with QA
Branch or Tag

Prod
Sync's with Main
Branch or Tag

Multi-Repo Structure

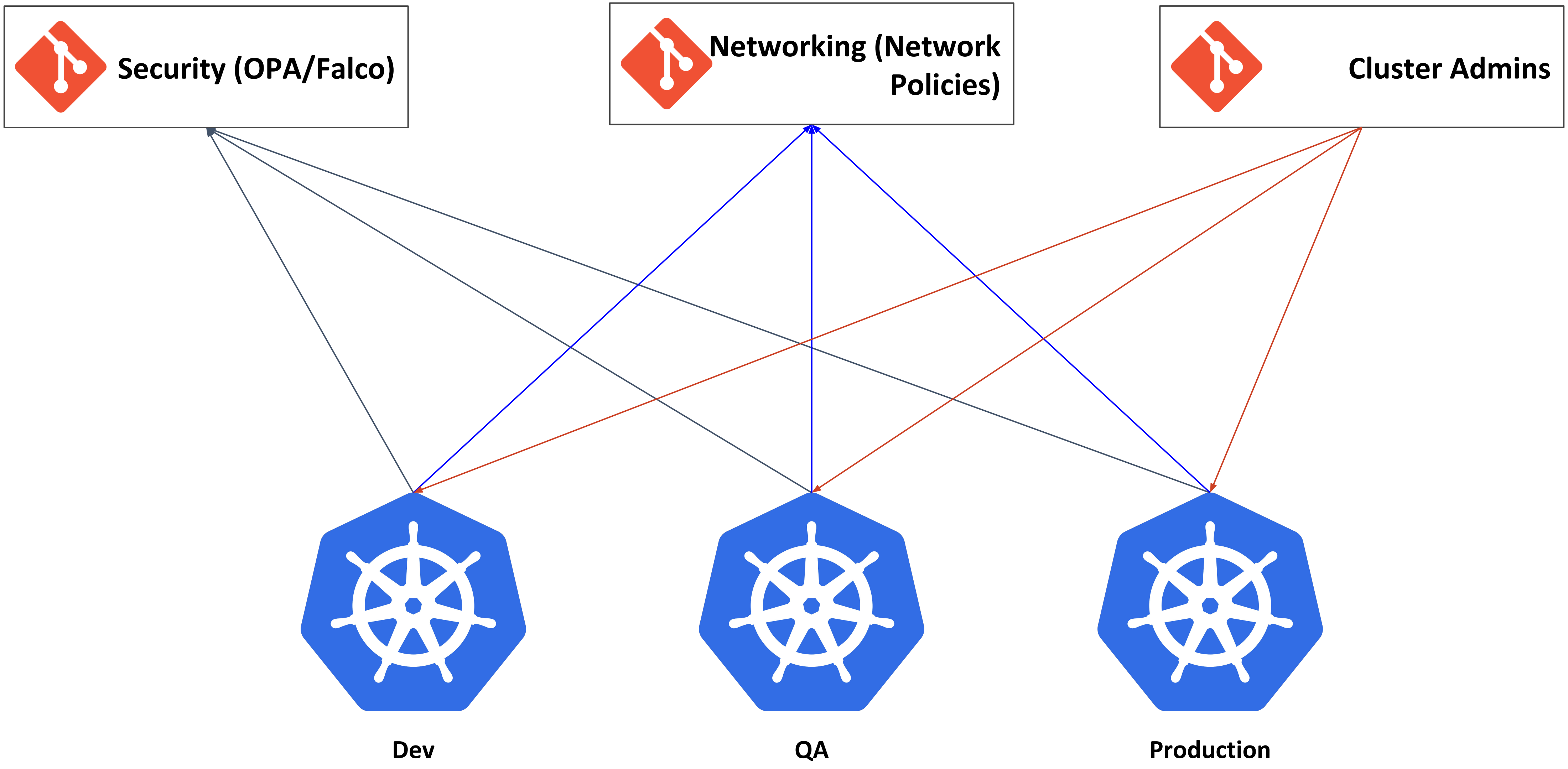
Multi-Repo Structure


Cluster Admin (Cluster Wide Resources)
git
flux
Cluster Wide
Team A (Namespaced Resources)
git
flux
Namespaced
Team B (Namespaced Resources)
git
flux
Namespaced
Cluster A

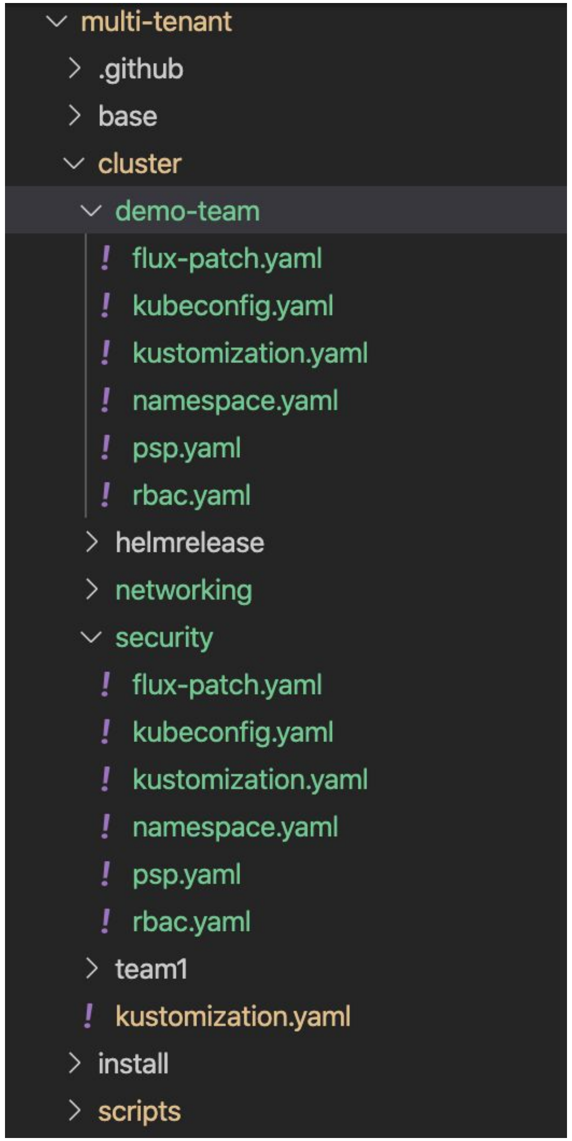
Multi-Tenant Structure

Branch/tag = Grouping/Environment/Region

Multi-Tenant Structure



Multi-Tenant Structure

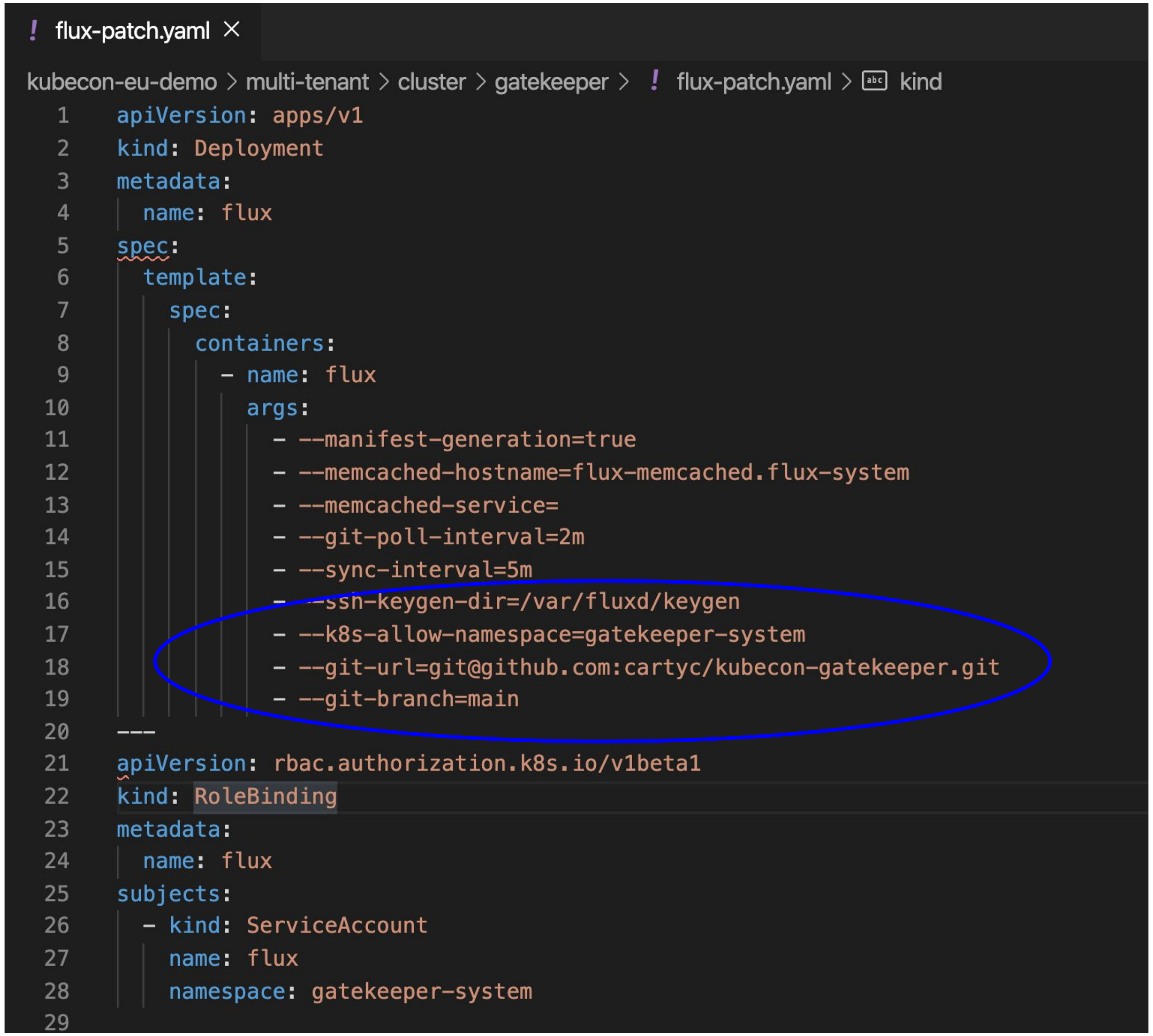


```
multi-tenant
  .github
  base
  cluster
    demo-team
      ! flux-patch.yaml
      ! kubeconfig.yaml
      ! kustomization.yaml
      ! namespace.yaml
      ! psp.yaml
      ! rbac.yaml
    helmrelease
    networking
    security
      ! flux-patch.yaml
      ! kubeconfig.yaml
      ! kustomization.yaml
      ! namespace.yaml
      ! psp.yaml
      ! rbac.yaml
    team1
    ! kustomization.yaml
  install
  scripts
```

- Leverages kustomize
- Permissions access repo (Read or Write)
- Base contains main Flux deployment configs
- Each team has its own agent

https://github.com/fluxcd/multi-tenancy

Multi-Tenant Structure


! flux-patch.yaml ×
kubecon-eu-demo > multi-tenant > cluster > gatekeeper > ! flux-patch.yaml > kind

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: flux
spec:
  template:
    spec:
      containers:
        - name: flux
          args:
            - --manifest-generation=true
            - --memcached-hostname=flux-memcached.flux-system
            - --memcached-service=
            - --git-poll-interval=2m
            - --sync-interval=5m
            - --ssh-keygen-dir=/var/fluxd/keygen
            - --k8s-allow-namespace=gatekeeper-system
            - --git-url=git@github.com:cartyc/kubecon-gatekeeper.git
            - --git-branch=main
---
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: RoleBinding
metadata:
  name: flux
subjects:
  - kind: ServiceAccount
    name: flux
    namespace: gatekeeper-system

```

https://github.com/fluxcd/multi-tenancy

Demo

Resources

Contact

- @macintoshprime (Twitter, Kubernetes Slack)

Resources

- Gitops.tech
- itnext.io/how-we-do-gitops-mettle-4cc771a6c029
- argoproj.github.io
- fluxcd.io

KubeCon | CloudNativeCon

Europe 2020

Virtual

KEEP CLOUD NATIVE CONNECTED