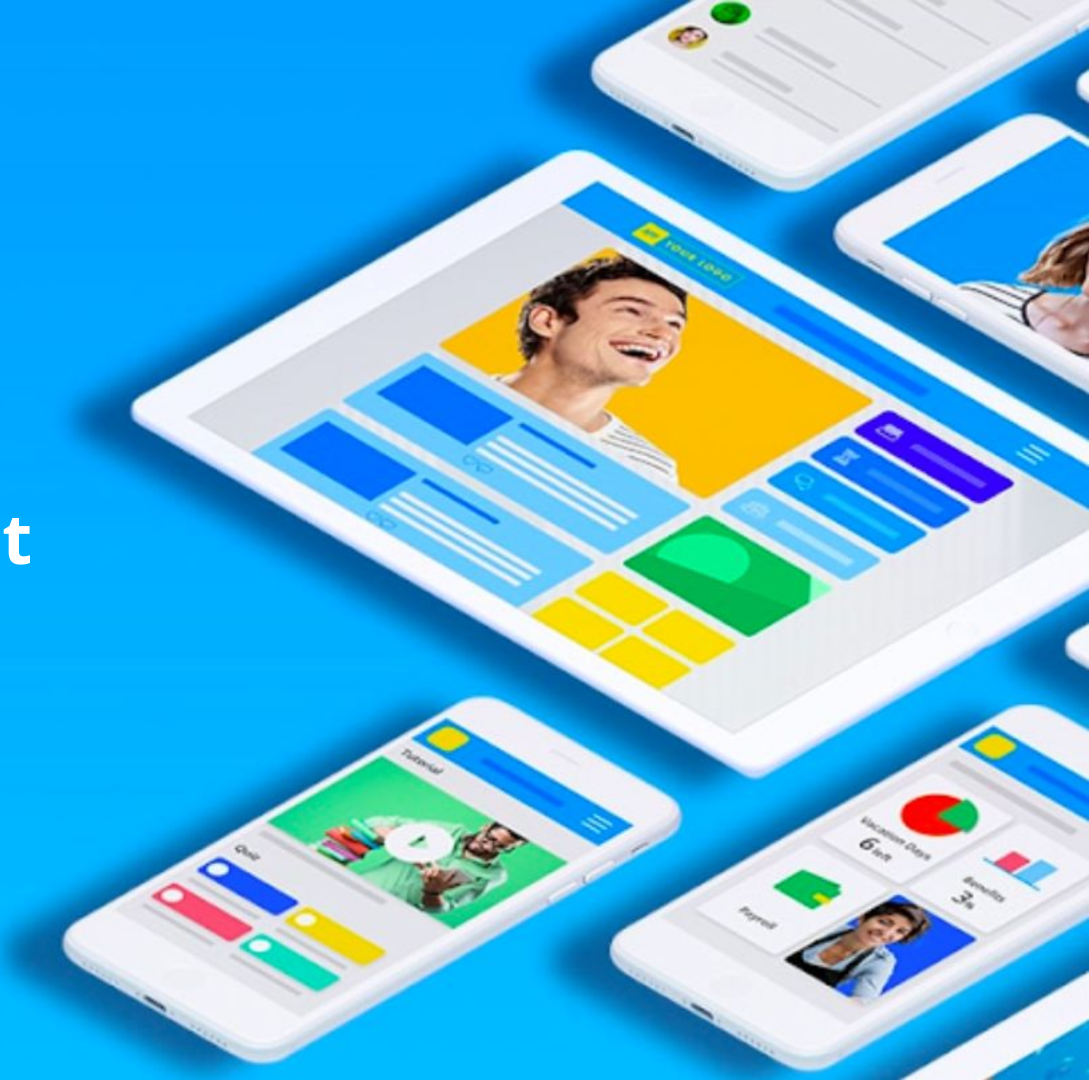
Staffbase

GitOps using Flux: How we manage Kubernetes Clusters at Staffbase

Rico Berger



Rico Berger

Site Reliability Engineer at Staffbase

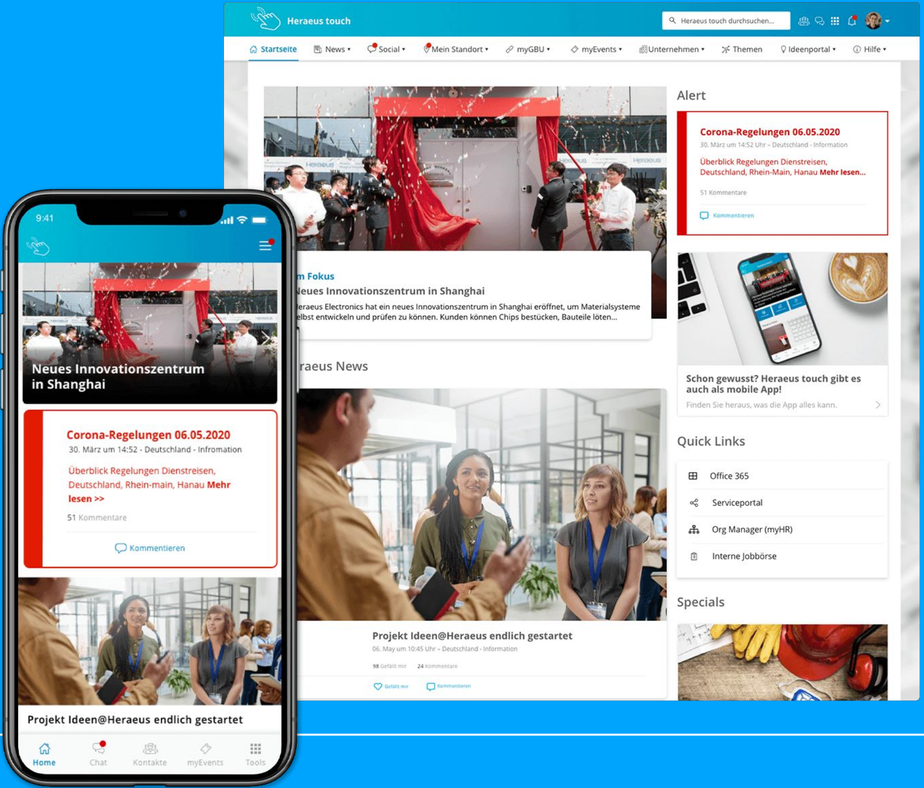
Responsible for the Infrastructure (Kubernetes) and Observability Topics at Staffbase

Open Source Contributor and Author of kubenav, kobs and the Vault Secrets Operator

You can follow me on Twitter: @rico_berger and GitHub: @ricoberger

Staffbase

An Internal Communications Platform



m Fokus

Neues Innovationszentrum in Shanghai

eraeus Electronics hat ein neues Innovationszentrum in Shanghai eröffnet, um Materialsysteme elbst entwickeln und prüfen zu können. Kunden können Chips bestücken, Bauteile löten...

raeus News

Projekt Ideen@Heraeus endlich gestartet

06. May um 10:45 Uhr – Deutschland - Information

98 Gefällt mir 24 Kommentare

Gefällt mir Kommentieren

Alert

Corona-Regelungen 06.05.2020

30. März um 14:52 Uhr – Deutschland - Information

Überblick Regelungen Dienstreisen, Deutschland, Rhein-Main, Hanau **Mehr lesen...**

51 Kommentare

Kommentieren

Schon gewusst? Heraeus touch gibt es auch als mobile App!

Finden Sie heraus, was die App alles kann.

Quick Links

- Office 365
- Serviceportal
- Org Manager (myHR)
- Interne Jobbörse

Specials

Neues Innovationszentrum in Shanghai

Corona-Regelungen 06.05.2020

30. März um 14:52 - Deutschland - Infromation

Überblick Regelungen Dienstreisen, Deutschland, Rhein-main, Hanau **Mehr lesen >>**

51 Kommentare

Kommentieren

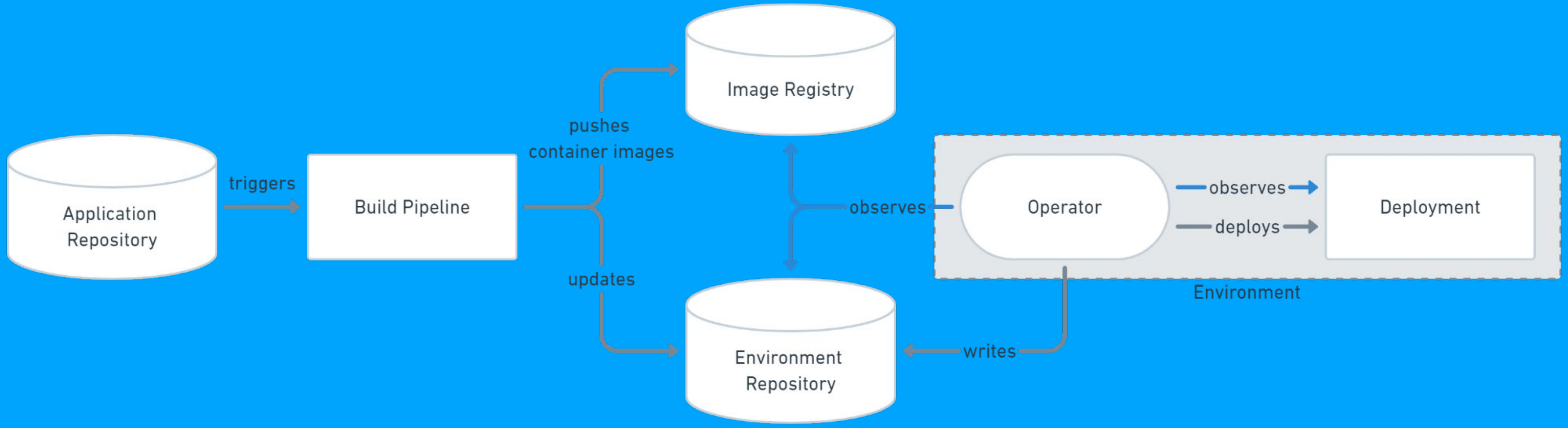
Projekt Ideen@Heraeus endlich gestartet

Staffbase

Why we are using GitOps?

- Multiple Kubernetes Clusters
- Cluster configuration should be stored in Git to have an audit log and rollback changes
- Each developer should be able to deploy new services
- New versions of our service should be automatically deployed

GitOps using Flux



GitOps using Flux

- Source Controller
  - Validate sources
  - Detect changes
  - Fetch resources

- Kustomize Controller
  - Reconcile the cluster state for multiple sources
  - Generate manifests with Kustomize
  - Validate and apply manifests

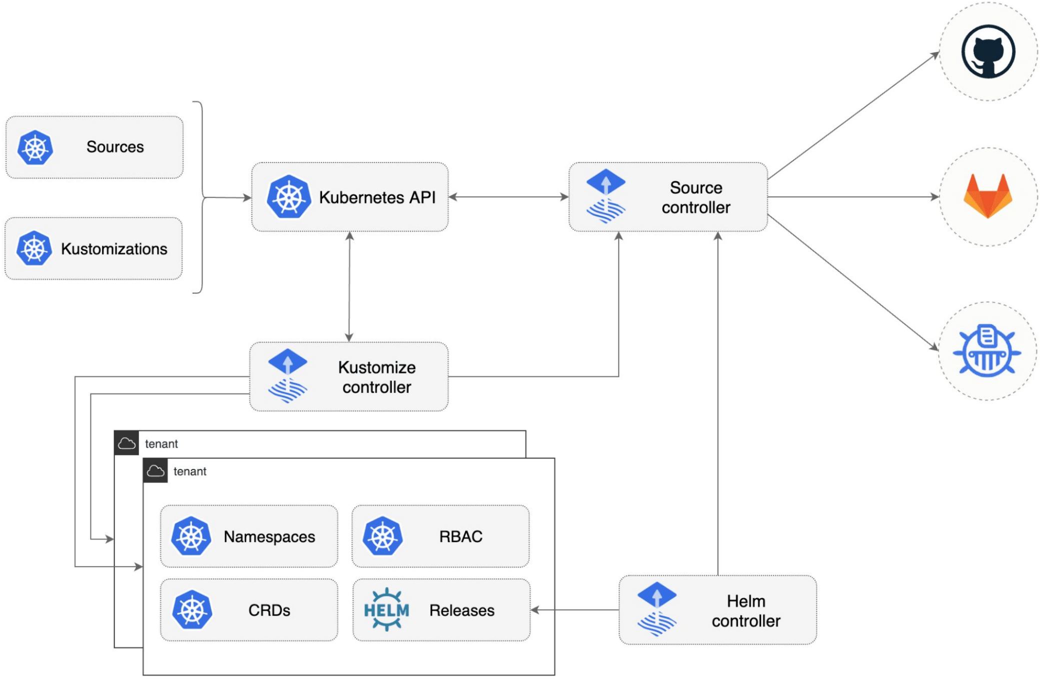
GitOps using Flux

- Helm Controller:
    - Declarative management of Helm chart releases with Kubernetes manifests

- Notifications Controller:
    - Handle inbound and outbound events

- Image Reflector and Automation Controllers:
    - Scan image repositories and reflect image metadata in Kubernetes resources
    - Update YAML files based on the latest image scan
    - Commit changes to Git repository

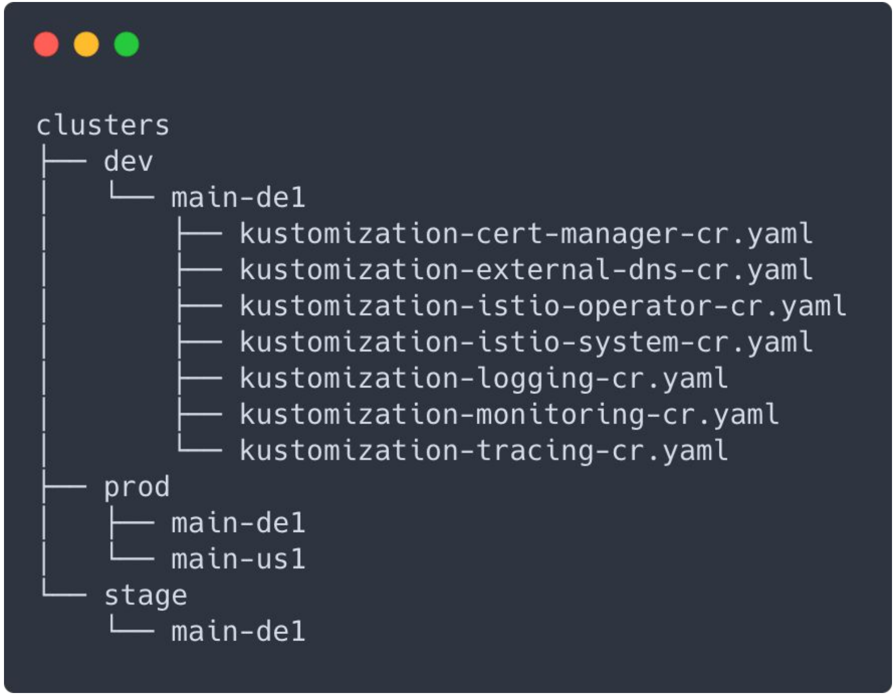
GitOps using Flux



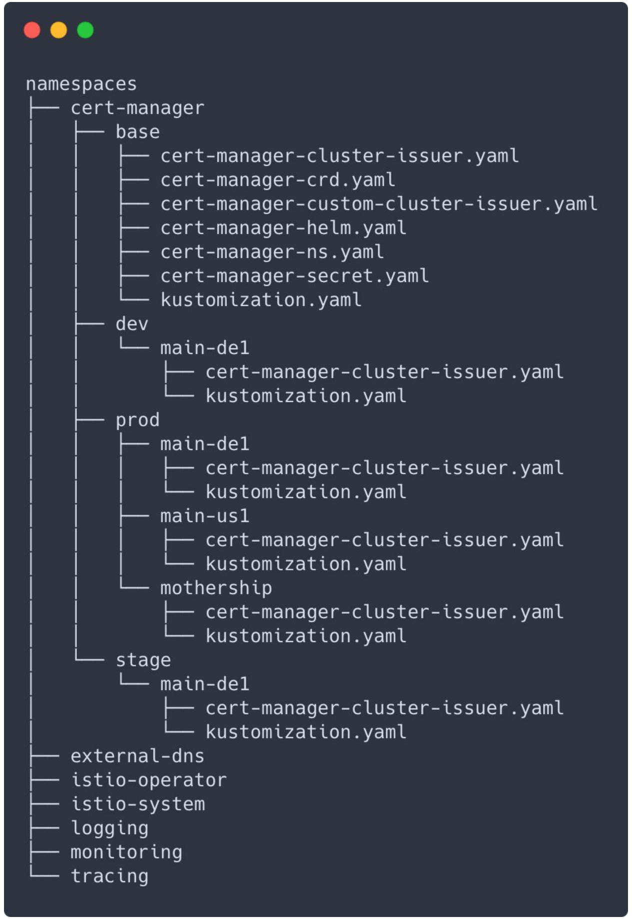
Demo

Best Practices

Repository Structure



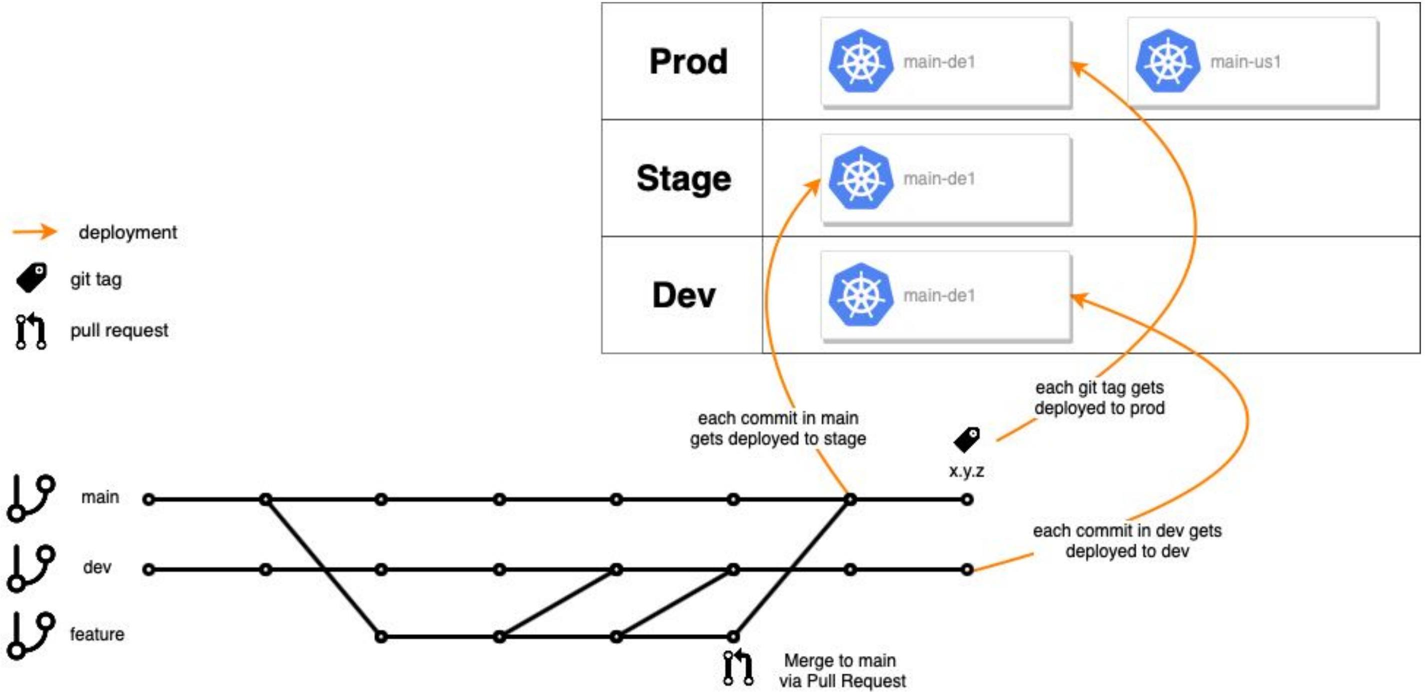
```
clusters
├── dev
│   └── main-de1
│       ├── kustomization-cert-manager-cr.yaml
│       ├── kustomization-external-dns-cr.yaml
│       ├── kustomization-istio-operator-cr.yaml
│       ├── kustomization-istio-system-cr.yaml
│       ├── kustomization-logging-cr.yaml
│       ├── kustomization-monitoring-cr.yaml
│       └── kustomization-tracing-cr.yaml
├── prod
│   ├── main-de1
│   └── main-us1
└── stage
    └── main-de1
```



```
namespaces
├── cert-manager
│   ├── base
│   │   ├── cert-manager-cluster-issuer.yaml
│   │   ├── cert-manager-crd.yaml
│   │   ├── cert-manager-custom-cluster-issuer.yaml
│   │   ├── cert-manager-helm.yaml
│   │   ├── cert-manager-ns.yaml
│   │   ├── cert-manager-secret.yaml
│   │   └── kustomization.yaml
│   ├── dev
│   │   └── main-de1
│   │       ├── cert-manager-cluster-issuer.yaml
│   │       └── kustomization.yaml
│   ├── prod
│   │   ├── main-de1
│   │   │   ├── cert-manager-cluster-issuer.yaml
│   │   │   └── kustomization.yaml
│   │   ├── main-us1
│   │   │   ├── cert-manager-cluster-issuer.yaml
│   │   │   └── kustomization.yaml
│   │   └── mothership
│   │       ├── cert-manager-cluster-issuer.yaml
│   │       └── kustomization.yaml
│   └── stage
│       └── main-de1
│           ├── cert-manager-cluster-issuer.yaml
│           └── kustomization.yaml
├── external-dns
├── istio-operator
├── istio-system
├── logging
├── monitoring
└── tracing
```

Best Practices

Image Updates

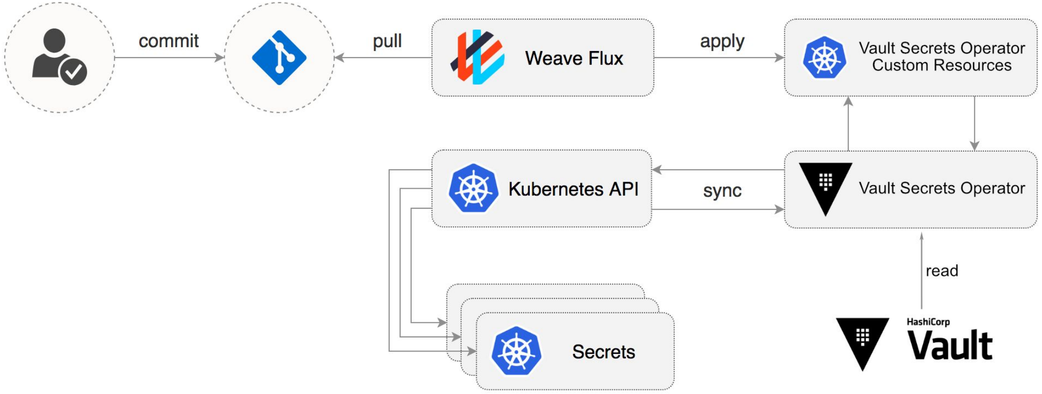


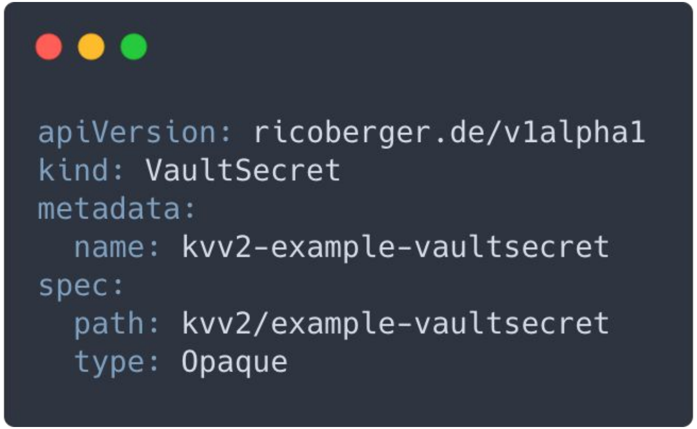
Prod
main-de1
main-us1
Stage
main-de1
Dev
main-de1
deployment
git tag
pull request
each commit in main gets deployed to stage
each git tag gets deployed to prod
x.y.z
main
dev
feature
each commit in dev gets deployed to dev
Merge to main via Pull Request

Best Practices

Secrets

Do not store Kubernetes secrets in Git, use a solution like Sealed Secrets or Vault and the Vault Secrets Operator (ricoberger/vault-secrets-operator)



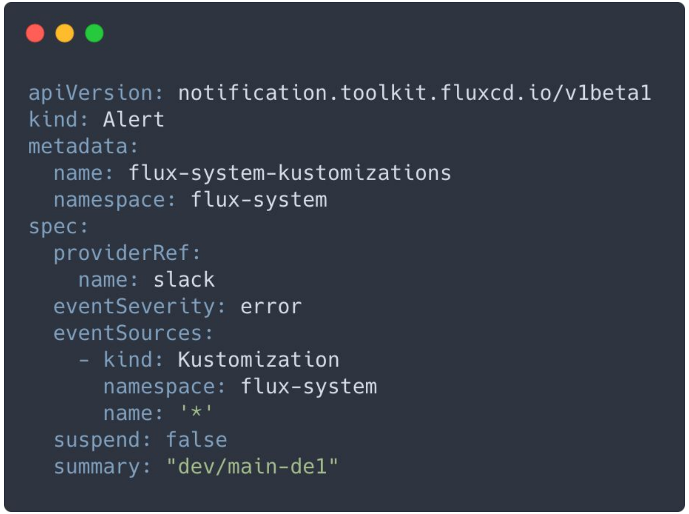


```yaml
apiVersion: ricoberger.de/v1alpha1
kind: VaultSecret
metadata:
  name: kvv2-example-vaultsecret
spec:
  path: kvv2/example-vaultsecret
  type: Opaque
```

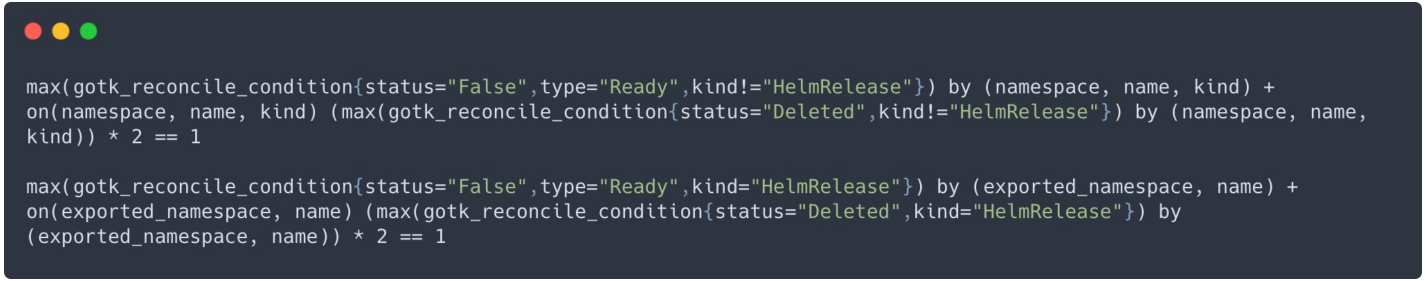
Best Practices

Notifications

Use the Notification controller to create an alert for failed reconciliations or use Prometheus and Alertmanager.



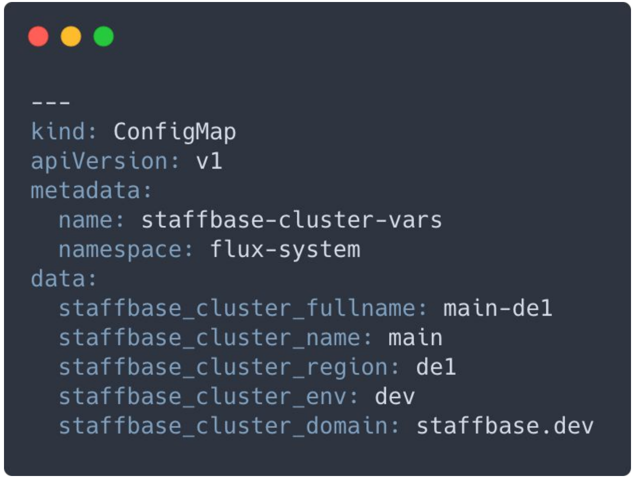
```yaml
apiVersion: notification.toolkit.fluxcd.io/v1beta1
kind: Alert
metadata:
  name: flux-system-kustomizations
  namespace: flux-system
spec:
  providerRef:
    name: slack
  eventSeverity: error
  eventSources:
    - kind: Kustomization
      namespace: flux-system
      name: '*'
  suspend: false
  summary: "dev/main-de1"
```



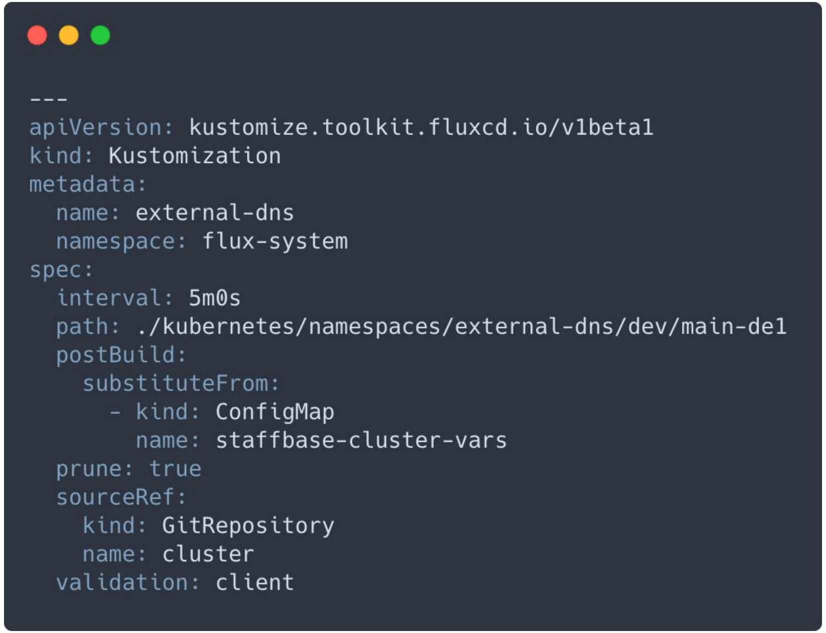
```
max(gotk_reconcile_condition{status="False",type="Ready",kind!="HelmRelease"}) by (namespace, name, kind) +
on(namespace, name, kind) (max(gotk_reconcile_condition{status="Deleted",kind!="HelmRelease"}) by (namespace, name,
kind)) * 2 == 1

max(gotk_reconcile_condition{status="False",type="Ready",kind="HelmRelease"}) by (exported_namespace, name) +
on(exported_namespace, name) (max(gotk_reconcile_condition{status="Deleted",kind="HelmRelease"}) by
(exported_namespace, name)) * 2 == 1
```

Best Practices

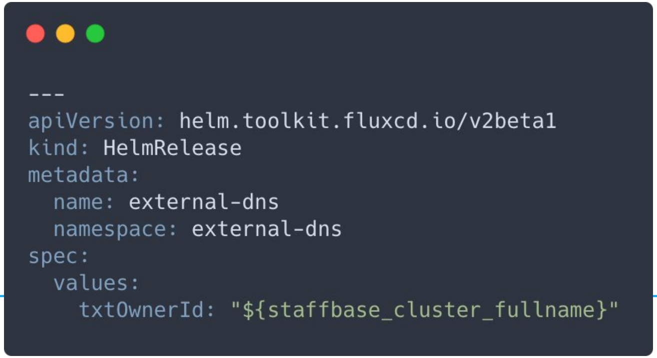
Environment Variables



```yaml
---
kind: ConfigMap
apiVersion: v1
metadata:
  name: staffbase-cluster-vars
  namespace: flux-system
data:
  staffbase_cluster_fullname: main-de1
  staffbase_cluster_name: main
  staffbase_cluster_region: de1
  staffbase_cluster_env: dev
  staffbase_cluster_domain: staffbase.dev
```



```yaml
---
apiVersion: kustomize.toolkit.fluxcd.io/v1beta1
kind: Kustomization
metadata:
  name: external-dns
  namespace: flux-system
spec:
  interval: 5m0s
  path: ./kubernetes/namespaces/external-dns/dev/main-de1
  postBuild:
    substituteFrom:
      - kind: ConfigMap
        name: staffbase-cluster-vars
  prune: true
  sourceRef:
    kind: GitRepository
    name: cluster
  validation: client
```



```yaml
---
apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: external-dns
  namespace: external-dns
spec:
  values:
    txtOwnerId: "${staffbase_cluster_fullname}"
```

We are hiring!

jobs.staffbase.com

Staffbase

www.staffbase.com