weaveworks

GitOps mit Flux

Vom Home-Cluster bis zum
Enterprise-Deployment

Max Jonas Werner

Senior Software Engineer

Flux Core Maintainer

@makkes@hachyderm.io

Was ist Flux?

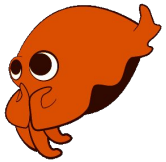
- Ein CNCF Graduated Open Source project (1 von 20)
- Ein Git-zentrierter Paket-Manager für deine Anwendungen
- Eine Sammlung von Continuous und Progressive Delivery Lösungen für Kubernetes

Nutzen von Flux

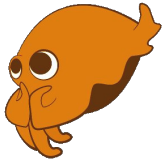
- Reduziert Last der Entwickler (“just push to git”)
- Modular & erweiterbar
- Unterstützt Kustomize und Helm von Haus aus
- Gemacht für Kubernetes, keine proprietären APIs, nur CRDs

Was Flux' Controller machen

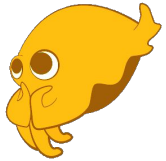
flux
fluxcd.io



Source Controller
- Resourcen abrufen und als Artefakte speichern



Kustomize Controller
- Manifeste anwenden, Manifest-Generierung mittels kustomize



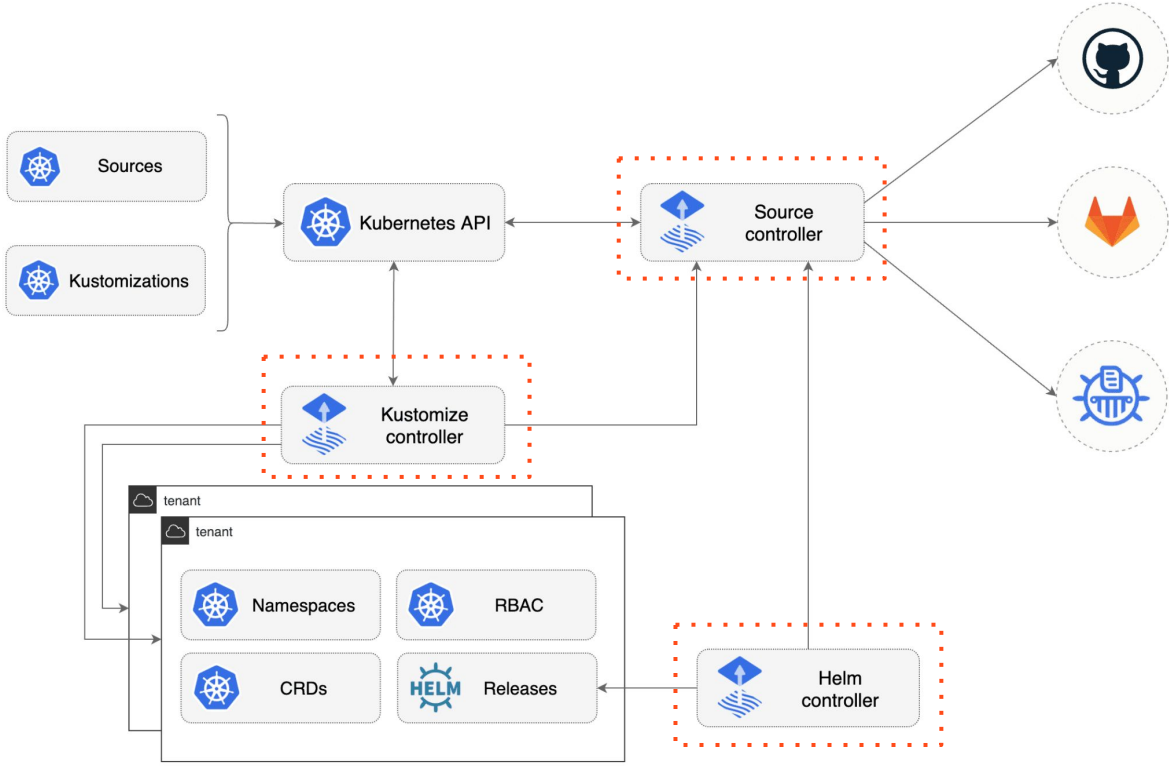
Helm Controller
- Deployment von Helm-Charts

Notification Controller
- Benachrichtigungen versenden

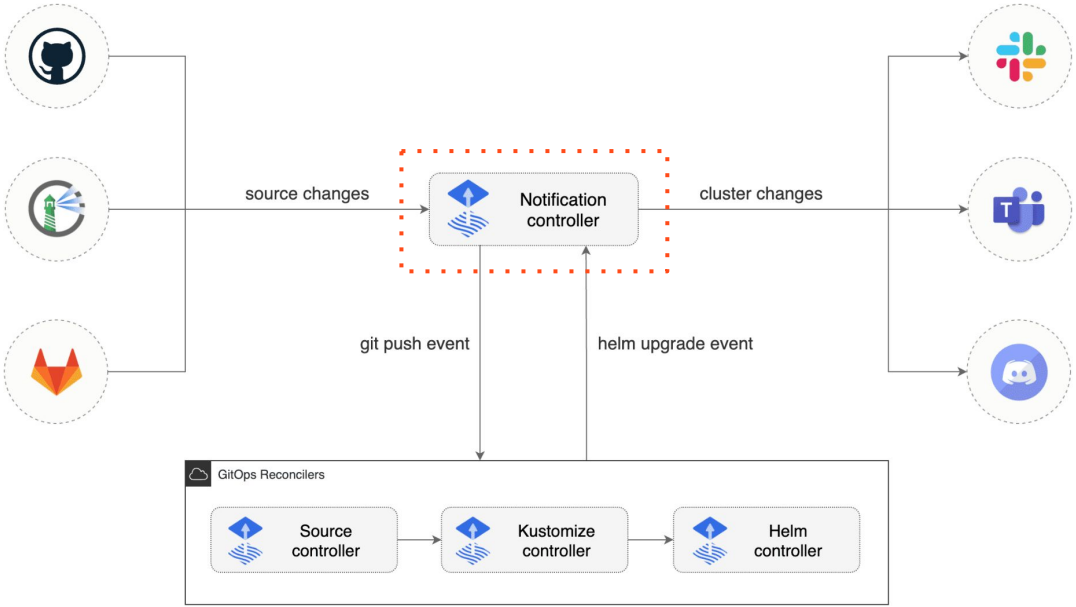
Image Reflector Controller
- Spiegelt Image-Metadaten für andere Controller

Image Automation Controller
- Aktualisiert YAML-Manifeste, wenn neue Images verfügbar sind

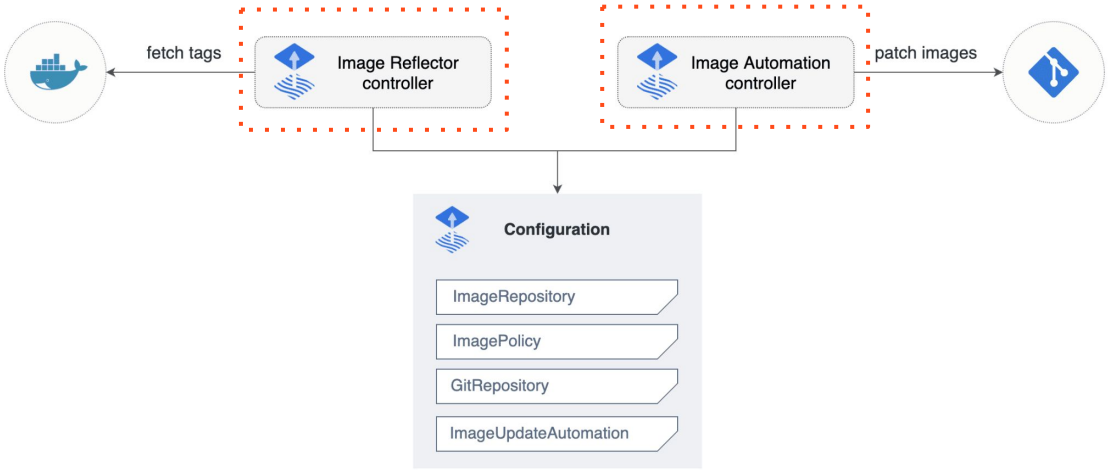
Flux Core Components



Flux Core Components



Flux Additional Components



Demo – Teil 1

- Einstieg/Installation
- Anwendungen deployen
- Web Interface
- Disaster Recovery

Demo – Teil 1

- Einstieg/Installation ✅
- Anwendungen deployen ✅
- Web Interface ✅
- Disaster Recovery ✅

Going Beyond: Security

- Supply Chain Security: Alle Flux-Images sind signiert

```
$ COSIGN_EXPERIMENTAL=1 cosign verify ghcr.io/fluxcd/source-controller:v0.34.0

Verification for ghcr.io/fluxcd/source-controller:v0.34.0 --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - Existence of the claims in the transparency log was verified offline
  - Any certificates were verified against the Fulcio roots.
```

Going Beyond: Security

- Supply Chain Security: Alle Flux-Images sind signiert
- Alle Flux-Images enthalten eine Software Bill of Materials

```
$ docker sbom fluxcd/source-controller:v0.34.0
```

Going Beyond: Security

- Supply Chain Security: Alle Flux-Images sind signiert
- Alle Flux-Images enthalten eine Software Bill of Materials
- Pod-Sicherheits-Standards: Alle Flux Controller-Deployments folgen der “restricted pod security policy”

Going Beyond: Security

- Supply Chain Security: Alle Flux-Images sind signiert
- Alle Flux-Images enthalten eine Software Bill of Materials
- Pod-Sicherheits-Standards: Alle Flux Controller-Deployments folgen der “restricted pod security policy”
    - alle Linux-Capabilities werden verworfen
    - Das Root-Filesystem ist read-only
    - Das Seccomp-Profil ist immer “RuntimeDefault”
    - Binaries laufen als non-root
    - Die Dateisystem-Gruppe ist 1337
    - User- und Group-ID sind 65534

Going Beyond: Security

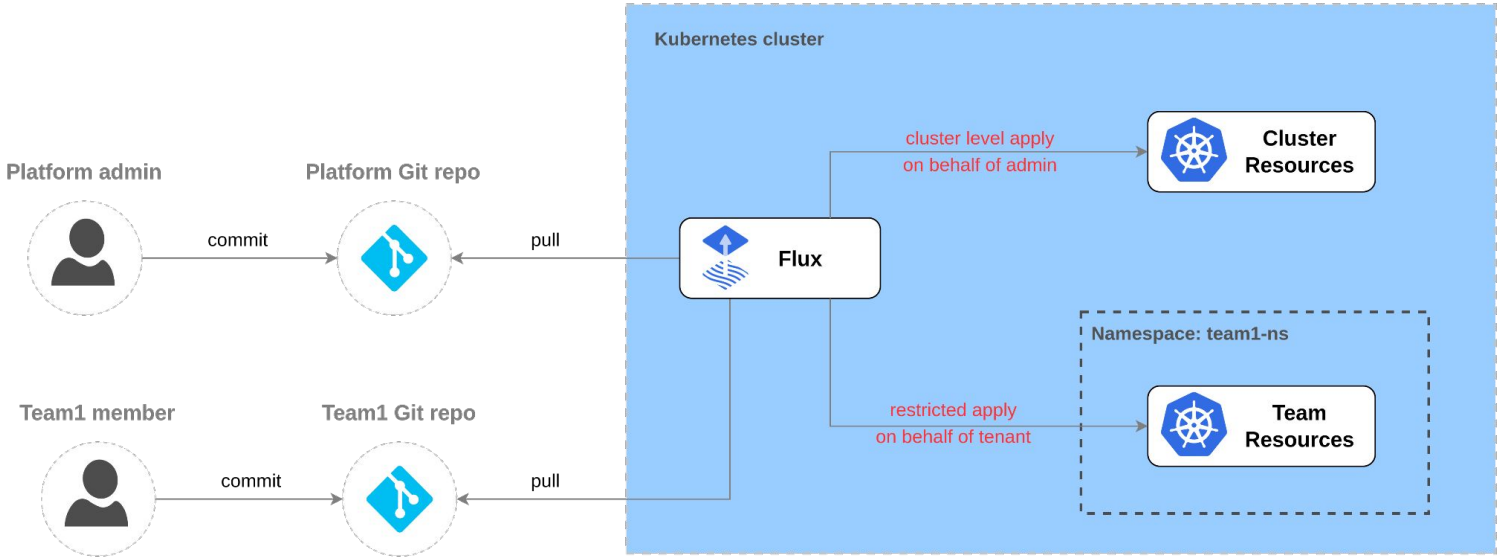
- Supply Chain Security: Alle Flux-Images sind signiert
- Alle Flux-Images enthalten eine Software Bill of Materials
- Pod-Sicherheits-Standards: Alle Flux Controller-Deployments folgen der “restricted pod security policy”
- Flux-Images werden kontinuierlich auf Schwachstellen gescannt (trivy)

Going Further: Multi-Tenancy

- Shared Cluster - Soft Multi-Tenancy
- Tenant Clusters - Hard Multi-Tenancy

Multi-tenancy: (a.k.a. “soft multi-tenancy”)

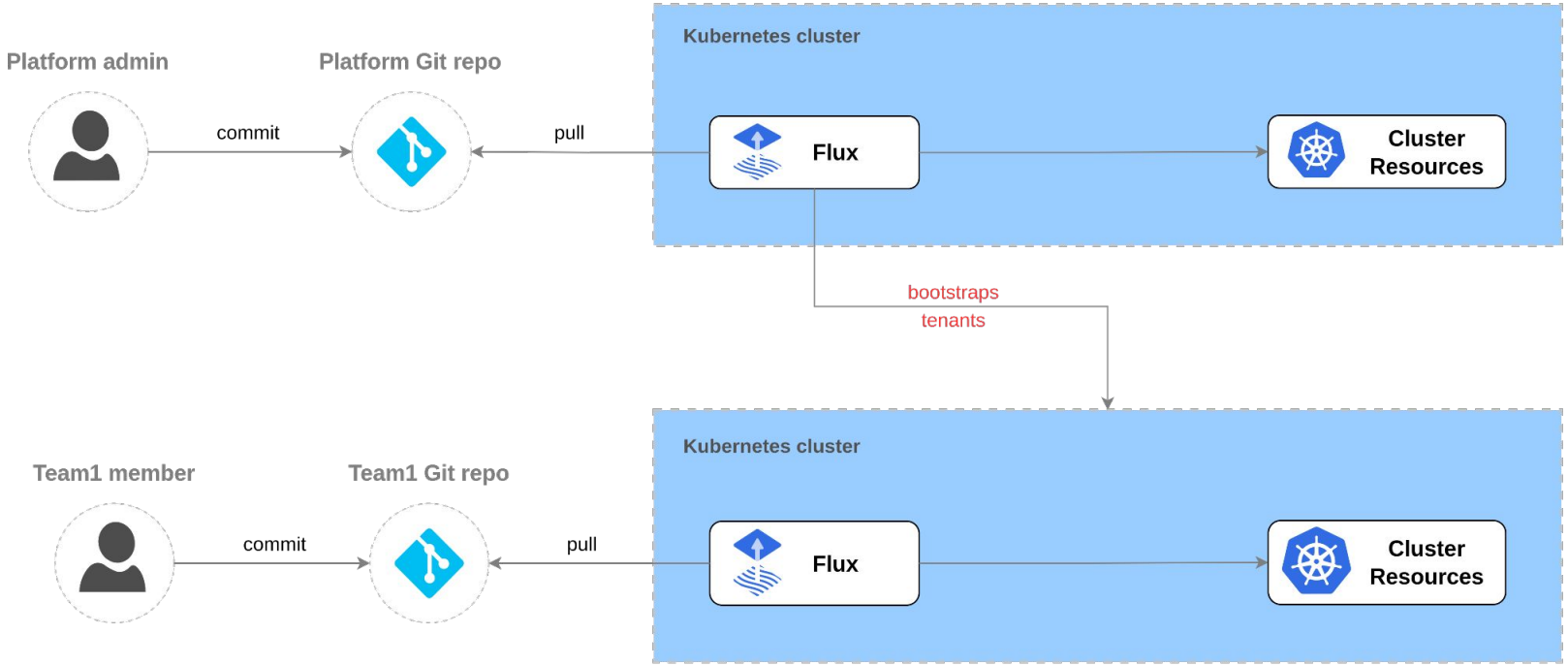
Single Cluster with Shared Flux Instance



Multi-tenancy:

(a.k.a. “hard multi-tenancy”)

Tenant-dedicated Cluster and Flux Instance



Going Further: Multi-Tenancy

- https://github.com/fluxcd/flux2-kustomize-helm-example
- https://github.com/fluxcd/flux2-multi-tenancy

Demo – Teil 2: Integration

- Deployments testen mit GitOps Run
- Multi-Cluster mit CAPI
- Secrets sicher verwalten mit SOPS

Demo – Teil 2

- Deployments testen mit GitOps Run ✅
- Multi-Cluster mit CAPI ✅
- Secrets sicher verwalten mit SOPS ✅

To the Moon

- OCI als Source of Truth (Git => CI => OCI => Cluster): `flux push artifact`
- Controller-Lockdown mit default ServiceAccounts
- Verhinderung von Cross-Namespace-Referenzen
- Weave GitOps Enterprise
  - Multi-Cluster UI
  - Cross-Cluster Deployment Pipelines
  - GitOps Templates
  - Policy

Die Flux-Community

- Try Flux! Follow our Getting Started guide
- Browse the docs at fluxcd.io/docs/
- Join #flux on the CNCF Slack
- Sign up for the Flux Mailing list for monthly updates, announcements, etc. (https://lists.cncf.io/g/cncf-flux-dev)
- Flux on GitHub: https://github.com/fluxcd/flux2
- Join the conversation in GitHub Discussions

weaveworks

max@weave.works

@makkes@hachyderm.io

weave.works