Gitless GitOps: Der Weg zu einer sicheren App-Umgebung mit Flux und OCI

Max Jonas Werner

Flux Core Maintainer

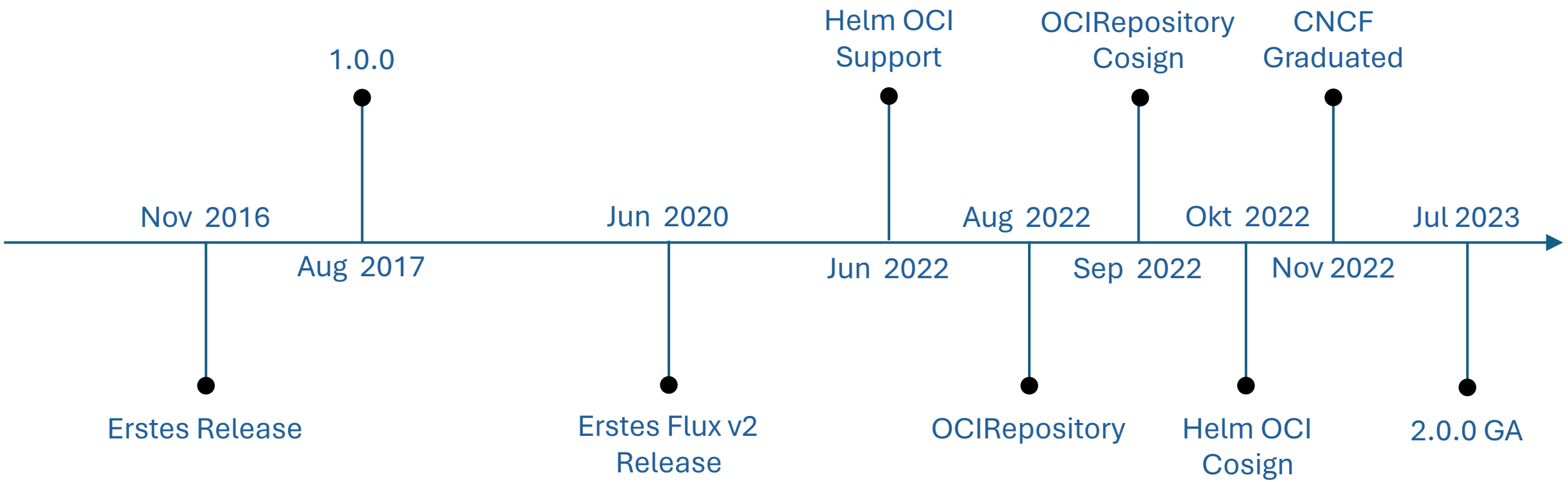
Consultant @ Associmates

Was ist Flux?

Basis von Continuous Delivery Plattformen

ΛSSOCIMΛTES

Meilensteine



ASSOCIMATES

Flux Mechanics

Workload Definition: Helm, Kustomize, Plain Kubernetes YAML

Desired State Acquisition: Git, OCI, S3, Helm Repository

Reconciliation: Drift detection and correction

Observability: Events, Metrics, Logs, Alerts, Traces

Kustomization
HelmRelease

GitRepository
OCIRepository
HelmRepository
HelmChart
Bucket

Flux API

13 CRDs, 6 Controller

Alert
Provider
Receiver

ImagePolicy
ImageRepository
ImageUpdateAutomation

ASSOCIMATES

fluxcd-kustomize-mutating-webhook

Azure Arc

GitLab

ControlPlane

aws-cloudformation-controller-for-flux

flux-kcl-controller

Flux Ecosystem

Gimlet

ocm-controller

EKS Anywhere

Nutanix DKP

jsonnet-controller

Giant Swarm

flux-kluctl-controller

tofu-controller

VMware Tanzu

ΛSSOCIMΛTES

Go SDK

github.com/fluxcd/pkg

ΛSSOCIMΛTES

Weaveworks Shutdown

ΛSSOCIMΛTES

OCI

ASSOCIMATES

OCI

Open Containers Initiative: https://opencontainers.org

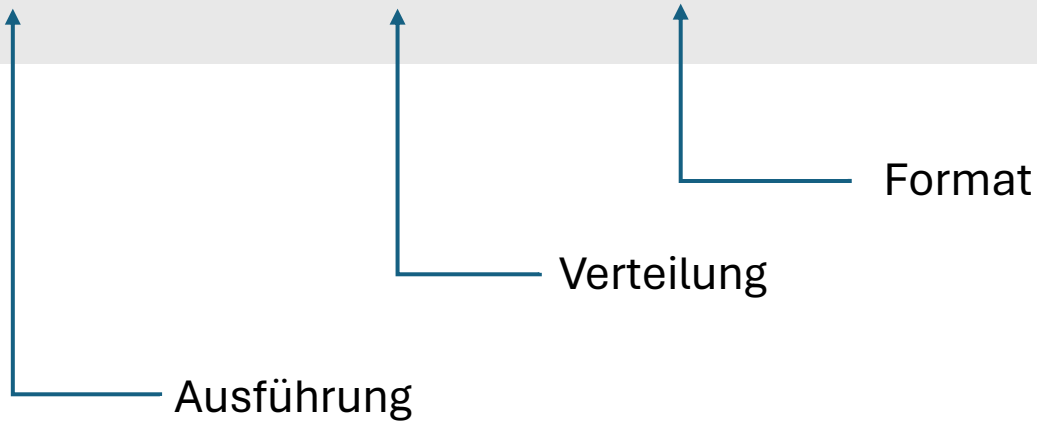
Gegründet 2015 von Docker und Weiteren

Teil der Linux Foundation

OCI

Die OCI entwickelt Spezifikationen für Image-Formate, -Verteilung und –Ausführung.
Zusammengenommen bilden sie einen mächtigen Baukasten:

```
$ docker run -it --rm docker.io/nginx
```



OCI

Ein OCI-Image ist nichts mehr als ein archiviertes Dateisystem

OCI: Beispiel

ghcr.io/stefanprodan/manifests/podinfo:6.6.2

OCI: Beispiel

ghcr.io/stefanprodan/manifests/podinfo:6.6.2

https://ghcr.io/v2/stefanprodan/manifests/podinfo/manifests/6.6.2

=

https://ghcr.io/v2/stefanprodan/manifests/podinfo/manifests/sha256:6ca1d018a562caa81bfee3c56c41d255b085bbdb30da79e09849559680df8675

OCI: Beispiel

https://ghcr.io/v2/stefanprodan/manifests/podinfo/manifests/6.6.2


```
{ "schemaVersion": 2,
  "mediaType": "application/vnd.oci.image.manifest.v1+json",
  "config": {
    "mediaType": "application/vnd.cncf.flux.config.v1+json",
    "size": 233,
    "digest": "sha256:d94773e55f310364bf3d51655b7cfdc5bcfab17f0f14f08ead84712728850a82"
  },

...
```


OCI: Beispiel

https://ghcr.io/v2/stefanprodan/manifests/podinfo/manifests/6.6.2

```
"layers": [{
      "mediaType": "application/vnd.cncf.flux.content.v1.tar+gzip",
      "size": 1115,
      "digest": "sha256:ac30c282a66c6a3fc076b8977670e75505c416a383846ba52e1005ba5d841acd"
    }],
  "annotations": {
    "org.opencontainers.image.created": "2024-04-10T11:07:54Z",
    "org.opencontainers.image.revision": "6.6.2/8d010c498e79f499d1b37480507ca1ffb81a3bf7",
    "org.opencontainers.image.source": "https://github.com/stefanprodan/podinfo"
  }}
```

OCI: Signaturen

ghcr.io/stefanprodan/manifests/podinfo@
sha256:6ca1d018a562caa81bfee3c56c41d255b085bbdb30da79e
09849559680df8675

ghcr.io/stefanprodan/manifests/podinfo:
sha256-
6ca1d018a562caa81bfee3c56c41d255b085bbdb30da79e0984955
9680df8675.sig

Flux + OCI = ♥

ASSOCIMATES

Flux + OCI

GitOps at Scale! (Alexis' Keynote vom letzten Jahr)

Images, Konfiguration und Signaturen an einem einzigen Ort

Registries haben oft eine bessere Verfügbarkeit

OCI Registries sind API-basiert, Git nicht wirklich

Regionaler Traffic spart dir Geld

Passwortlose Authentifizierung (Workload Identity, IAM)

Keyless Verification (OIDC)

Flux + OCI: Passwortlose Authentifizierung

Keine Schlüsselverwaltung mehr

Keine Generierung von SSH-Keys mehr

Keine proprietären APIs mehr für Token-Generierung

Gleicher Mechanismus/gleiche Credentials wie für das Pullen von Container-Images

Flux + OCI

Schlüssellose Integritätsprüfung mit Cosign und (bald) Notation

YAML-Generierung mit CUE oder Jsonnet

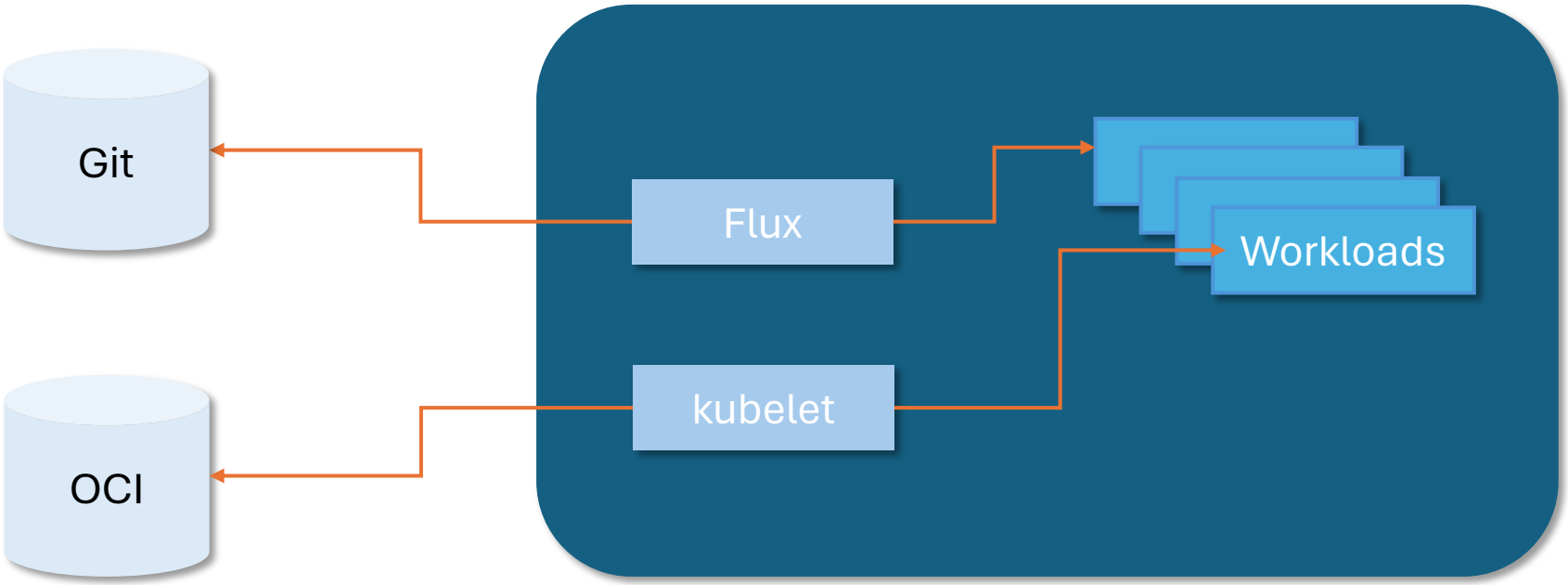
Lokale Entwicklung dank lokaler OCI-Registry (Demo)

Es ist immer noch GitOps!

ΛSSOCIMΛTES

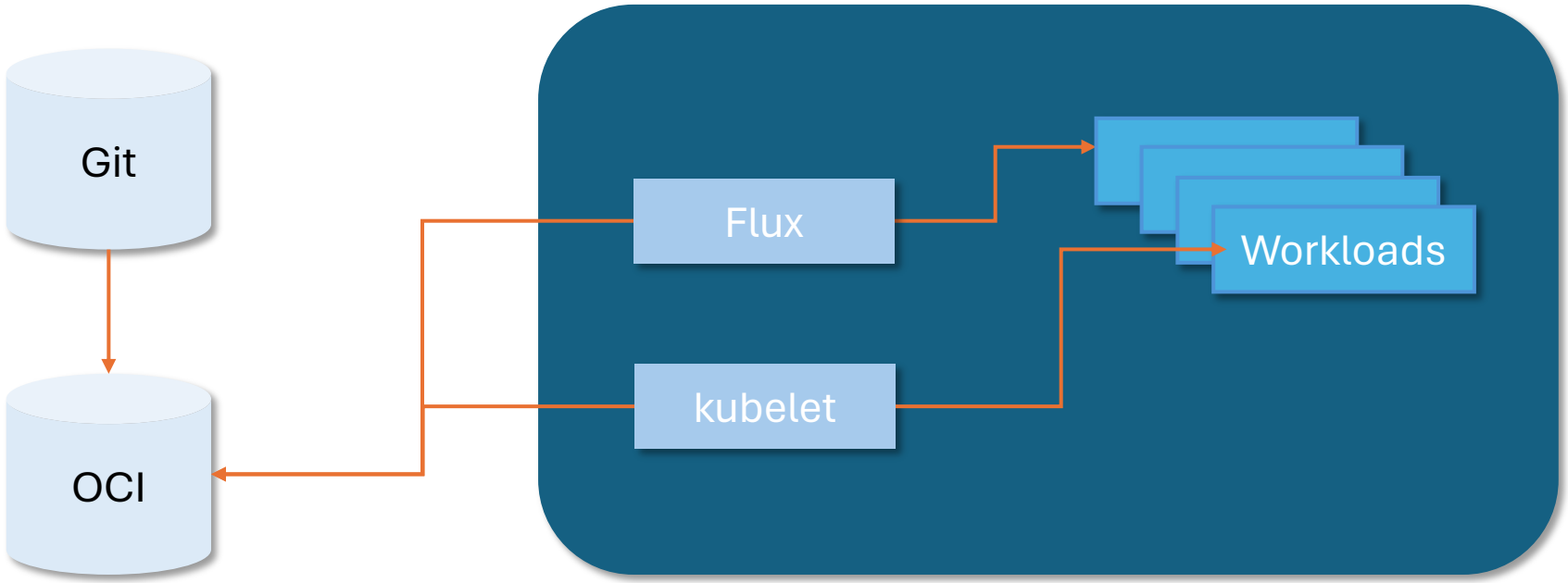
Es ist immer noch GitOps!

Git ist immer noch die Source of Truth



Es ist immer noch GitOps!

Git ist immer noch die Source of Truth



“GitOps is a transaction system with a Git backend and OCI cache”

ΛSSOCIMΛTES

Flux + OCI in der Praxis

`flux push artifact`

`flux trace`

Kubernetes-Manifeste

Terraform-Module

Push-based GitOps: Receiver + GitHub Actions Flux action: https://github.com/fluxcd/flux2/tree/main/action

Roadmap 2024+

ΛSSOCIMΛTES

Roadmap 2024+

Mehr **Diversität** (ControlPlane, GitLab, OpsMX, etc.)

#flux-ecosystem im CNCF-Slack

Notary Project: Verifikation von OCI-Signaturen mit Notation Trust Policies

CDEvents-Integration: Reconciliation mit CDEvents triggern

Helm OCI Verbesserungen: OCIRepositories als Helm Release Quellen

80% aller APIs GA