

Managing Helm Deployments with GitOPS at CERN

Ricardo Rocha

CERN IT-CM-RPS

Why

Single source of truth

Reusability

Automation of deployment and upgrades

Multi cluster configuration

Monday, November 18

9:00am ● Your Path to Production Ready Kubernetes hosted by Weaveworks (Additional Registration + Fee Required) (Description: gitops)

Tuesday, November 19

11:50am ● Intro: Flux - Stefan Prodan & Alexis Richardson, Weaveworks (Description: gitops)

2:25pm ● Managing Helm Deployments with Gitops at CERN - Ricardo Rocha, CERN

Wednesday, November 20

11:50am ● Deep Dive: Flux the GitOps Operator for Kubernetes - Stefan Prodan, Weaveworks

● From Brownfield to Greenfield: Istio Service Mesh Journey at Freddie Mac - Shriram Rajagopalan, Tetrade & Lixun Qi, Freddie Mac (Description: gitops)

2:25pm ● Fidelity's Move to "Finance Grade" Kubernetes with GitOps - Alexis Richardson, Weaveworks & Rajarajan Pudupatti SJ, Fidelity Investments

3:20pm ● Panel: GitOps User Stories - Tamao Nakahara, Weaveworks; Javeria Khan, Palo Alto Networks; Hubert Chen, Branch; Stefan Prodan, Weaveworks; & Edward Lee, Intuit

5:00pm ● Open Source Workshop: The GitOps Way - Meet Experts, Weaveworks

● Tutorial: Everything You Need To Become a GitOps Ninja - Alex Collins & Alexander Matyushentsev, Intuit (Limited Available Seating; First-Come, First-Served Basis)

And also ...

Transition to kubernetes is not trivial ...

*“ How do i retrieve my application’s logs? And
how to log rotate? “*

“ How do i access the node running container X ? “

“ How do i install package X on the nodes? “

*“ Seems like one of the cluster node’s filesystem went
read-only... “*

*“ Docker, Kubernetes, Ingress ... now Helm ... this is
a lot of new stuff! “*

Significant change in mindset and a steep learning curve

Making it easier...

Container Trainings, Workshops, Office Hours

One thing is similar ... what is now called GitOps

We've used git for years to store and manage configuration

Maybe that can help onboarding more service managers

Puppet to Helm

Manifests vs Golang, YAML config for both

Much faster turn-around

What is Helm

The Kubernetes package manager

A **Chart** manages the deployment and configuration of an application

- Reusable, shareable units

- Includes all required manifests, plus any required libraries for lifecycle

- Separate **values** definitions for instance configuration

Template

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: eosxd-config
  labels:
    app: {{ template "eosxd.name" . }}
    chart: {{ template "eosxd.chart" . }}
    release: {{ .Release.Name }}
    heritage: {{ .Release.Service }}
...
{{- range $area, $mountpoints := .Values.mounts }}
  {{- range $mountpoint, $letters := $mountpoints }}

  fuse.{{ $mountpoint }}.conf: |+
    {"name": "{{ $mountpoint }}", "hostport": "eos{{
$mountpoint }}.cern.ch", "localmountdir": "/eos/{{
$mountpoint }}/", "remotemountdir": "/eos/{{ $area }}/",
"bind": "{{ $letters }}"

    {{- end }}
  {{- end }}
```

Template

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: eosxd-config
  labels:
    app: {{ template "eosxd.name" . }}
    chart: {{ template "eosxd.chart" . }}
    release: {{ .Release.Name }}
    heritage: {{ .Release.Service }}
...
{{- range $area, $mountpoints := .Values.mounts }}
  {{- range $mountpoint, $letters := $mountpoints }}

  fuse.{{ $mountpoint }}.conf: |+
    {"name": "{{ $mountpoint }}", "hostport": "eos{{
$mountpoint }}.cern.ch", "localmountdir": "/eos/{{
$mountpoint }}/", "remotemountdir": "/eos/{{ $area }}/",
"bind": "{{ $letters }}"

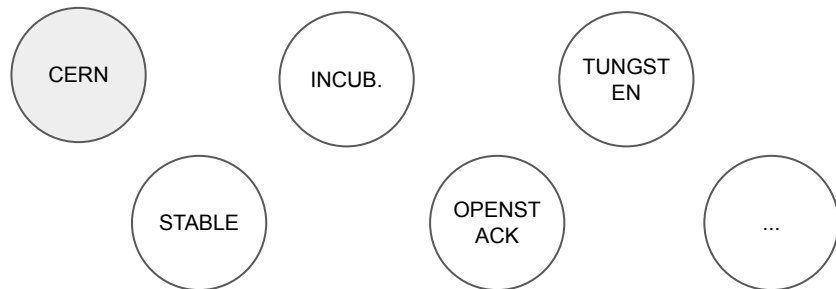
    {{- end }}
  {{- end }}
```

Values

```
image:
  repository: gitlab-registry.../eosd
  tag: 0.4.0
  pullPolicy: IfNotPresent
mounts:
  ams:
  atlas:
  cms:
  experiment:
  lhcb:
  project:
    project-i00: "a e j g v k q y"
    project-i01: "l h b p s f w n o"
    project-i02: "d c i r m t u x z"
  theory:
  user:
    home-i00: "l n t z"
    home-i01: "a g j k w"
    home-i02: "h o r s y"
    home-i03: "b e m v x"
    home-i04: "c f i p q"
  workspace:
```


Charts Repository

CERN instance: <https://registry.cern.ch/chartrepo>



A central catalog: the Helm Hub

Quite recent but already points to most popular charts

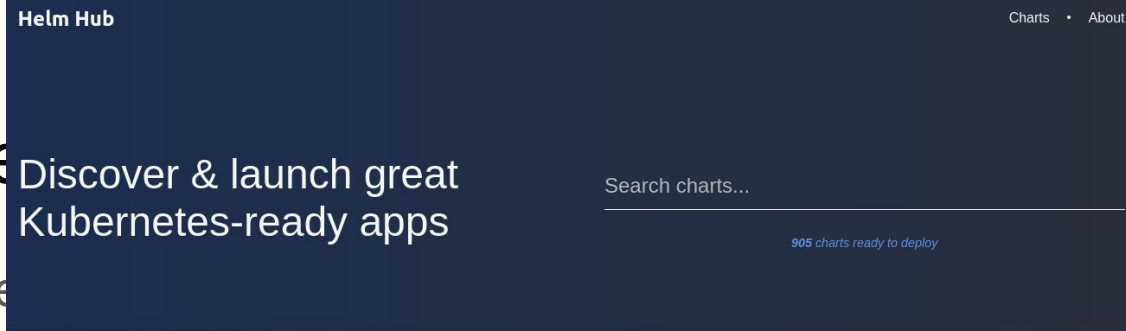
Does not host the charts, acts like a catalog

<https://hub.helm.sh>

Charts Re

Discover & launch great
Kubernetes-ready apps

CERN instance



A central catalog

Quite recent bu

Does not host t

<https://hub.helm.sh>

















| | | | |
|--|--|--|---|
|  mogaal/adminer 4.7.3 |  stable/aerospike v4.5.0.5 |  aerospike/aerospike 4.7.0.3 |  aerospike/aerospike-enterprise 4.7.0.3 |
|  buildkite/agent 3.12.0 |  choerodon/agile-service 0.19.3 |  agones/agones 1.1.0 |  bitnami/airflow 1.10.6 |
|  stable/airflow 1.10.4 |  stable/ambassador 0.85.0 |  stable/anchore-engine 0.5.2 |  banzaicloud-stable/anchore-policy-validator 0.3.6 |
|  kiwigrd/any-resource |  bitnami/apache |  pfisterer-knox/apache-knox-bootstrap |  choerodon/api-gateway |

Chart charts

CERN ir

Repository

all

stable

incubator

jfrog

kremers

linkerd2

linkerd2-edge

rimusz

buildkite

keel

appscore

gitlab

bitnami

fluxcd

jetstack

ibm-charts

kanister

flagger

zammad

agones

banzaicloud-

stable



A centra

Quite re

Does no

<https://h>

Q cern



cern/base



cern/condor-startd
1.0



cern/eosxd
0.4.0



cern/jupyterhub
1.0.0



cern/kube-monkey
0.3.0



cern/nftpd
1.0



cern/nvidia-gpu



cern/prometheus-cern
5.12.4



cern/squid



cern/sssd
1.0

Umbrella Charts

Charts are reusable deployments units

Most applications have multiple dependencies

Umbrella charts wrap all the required charts into a single deployment unit

With any additional manifests required

```
$ dependencies:  
- name: mysql  
  version: 5.3  
  repository: https://kubernetes-charts.storage.googleapis.com/  
- name: nginx  
  version: 1.16.1  
  repository: https://kubernetes-charts.storage.googleapis.com/
```

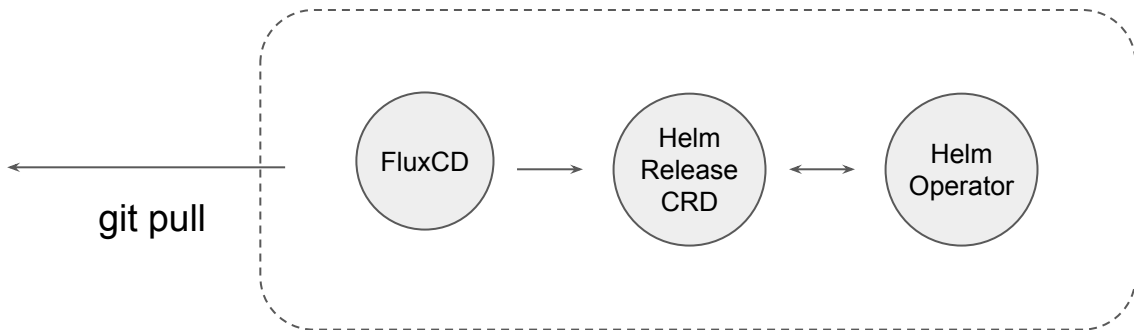
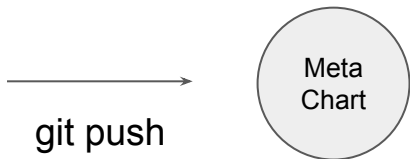
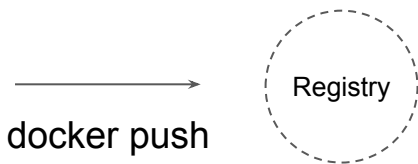
Flux and GitOps

Our end goal from the start

Relying on chart updates only

```
$ helm install fluxcd/flux \  
  --namespace flux --name flux --values flux-values.yaml  
  --set git.pollInterval=1m  
  --set git.url=https://gitlab.cern.ch/.../hub
```

```
$ cat flux-values.yaml  
rbac:  
  create: true  
helmOperator:  
  create: true  
  chartsSyncInterval: 5m  
  configureRepositories:  
    enable: true  
    repositories:  
      - name: jupyterhub  
        url: https://charts.cern.ch/jupyterhub  
  ...
```



Flux and GitOps

What's in a Helm Release?

```
apiVersion: flux.weave.works/v1beta1
kind: HelmRelease
metadata:
  name: hub
  namespace: prod
spec:
  releaseName: hub
  chart:
    git: https://gitlab.cern.ch/.../hub.git
    path: charts/hub
    ref: master
  valuesFrom:
  - secretKeyRef:
      name: hub-secrets
      key: values.yaml
  values:
    binderhub:
      ...
```

```
|-- charts
  |-- hub
    Chart.yaml requirements.yaml values.yaml
  |-- templates
    custom-manifest.yaml
|-- namespaces
  prod.yaml stg.yaml
|-- releases
  |-- prod
    hub.yaml
  |-- stg
    hub.yaml
|-- secrets
  |-- prod
    secrets.yaml
  |-- stg
    secrets.yaml
```



This is how we plug our encrypted values data

A Barbican Secret Plugin for Helm

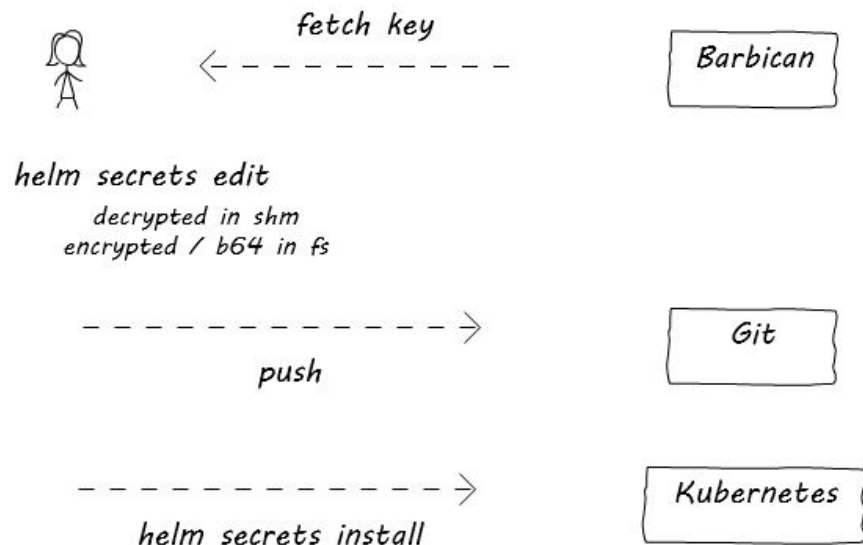
Similar interface to futuresimple helm-secrets

Builds on existing identity scheme to access and manage encryption keys

```
$ helm --name <release> secrets  
  view secrets.yaml  
  edit secrets.yaml  
  install stable/nginx --values secrets.yaml  
  upgrade stable/nginx --values secrets.yaml  
  lint --values secrets.yaml
```

Similar wrapper for kubectl

<https://github.com/cernops/helm-barbican>



Demo

Deployment Model

1 → 1: This is currently our most common model

Kubernetes clusters live in the end user's project

Any service aggregation and consolidation is done at that level

1 → *: Replicate the same application in multiple clusters

HA, Blast Radius, Blue / Green style

*** → ***: Workloads also share the underlying resources

Nice separation between service managers and infrastructure

Stronger requirements on multi-tenancy, quotas at cluster level

Ongoing: GitOps for Cluster Lifecycle

Currently validating this solution to centrally manage upgrades

Reduce the scope of the cluster orchestration tool to base components

Let a single Flux HelmRelease manage all add-ons (staging, prod)

```
dependencies:  
  - name: eosxd  
    version: 0.3.1-cern-0.1.0-7+ba5e81  
    repository: http://charts.cern.ch/cern  
  - name: fluentd  
    version: 2.2.1-cern-0.1.0-3+1c551a1  
    repository: http://charts.cern.ch/stable  
  - name: prometheus  
    version: 9.3.1-cern-0.1.0-3+1c551a1  
    repository: http://charts.cern.ch/stable  
  - name: traefik  
    version: 1.79.0-cern-0.1.0-3+1c551a1  
    repository: http://charts.cern.ch/stable  
  ...
```

NOVEMBER 14, 2019

Announcement

Introducing Argo Flux - A Weaveworks-Intuit-AWS Collaboration

The new “Argo Flux” provides a single tool chain for continuous deployment and fleet using GitOps.

November 14, 2019 - Today Weaveworks announces a partnership with Intuit to create Argo Flux, a major application delivery for Kubernetes via an industry-wide community. Argo Flux combines the [Argo CD project](#) driven by Weaveworks, two well known open source tools with strong community support. AWS contributor and BlackRock as a first enterprise user. AWS has endorsed and supported GitOps tooling t as in Flagger for AWS App Mesh. A starting point for this new collaboration is the [GitOps Engine](#) (more

Argo Flux - Kubernetes automation with GitOps

Flux CD and Argo CD have paved the way as the top open source projects for GitOps solutions. GitOps manage Kubernetes applications. In a GitOps model, users describe the applications and services they the running clusters to a correct application state and if the system drifts from the correct state, alerts a bespoke scripted and ad hoc UI-based management. Those may lead to incorrect system states and ca

🔍 SIGN IN [SIGN UP FOR TRIAL](#)

intuit quickbooks turbotax mint proconnect.

intuit Blog

Customers

Technology

Life at Intuit

News & Social

Partners

Company Information



Sign In

Intuit®: Official Blog > Technology > Engineering > Introducing Argo Flux

Introducing Argo Flux

ENGINEERING, TECHNOLOGY

November 14, 2019 / Pratik Wadher



At Intuit, proud maker of TurboTax, QuickBooks, and Mint, we believe that everyone deserves the opportunity to prosper. We're dedicated to providing the tools, skills, and insights that empower people around the world to take control of their finances and live the lives they want.

Nearly two years ago, Intuit [acquired](#) Applatix to accelerate Intuit's cloud journey by leveraging cloud native technologies to greatly increase development velocity. Applatix's focus was to provide the essential building blocks based on containers and public cloud to enable enterprises to quickly and continuously develop and deploy software and services. It wasn't easy. We were shepherding a new way of software development, changing the way developers create software and ship code. We knew there was a better way and so we set out to create [Argo](#), a container-native workflow engine for Kubernetes, and open sourced it to the cloud native developer community.

Tags

A Giant Story [AI](#) [Artificial Intelligence](#)
 Awards [Best Places to Work](#) [Blockchain](#) [Brad Smith](#) [CEO](#)
 Cloud [Data Science](#) [Design](#) [Diversity and Inclusion](#) [early career](#) [Earnings](#)
 entrepreneur [Finance](#) [Girl on Fire](#) [Growth](#) [Innovation](#)
 intern [Interns](#) [Intuit](#) [Intuit India](#) [IRS](#) [Leadership](#) [LGBTQ](#)
[Machine Learning](#) [Mint](#) [Open Source](#)
 Powering [Prosperity](#) [Quickbooks](#)
[QuickBooks](#) [Connect](#) [Sasan Goodarzi](#) [Self-Employed](#)
[Small Business](#) [Tax Deadline](#) [TAXES](#) [tax filing](#)
 Tech [Technology](#) [Turbo](#) [TurboTax](#) [Volunteer We](#)
 Care & Give Back [Women in Tech](#)

Intuit Blogs

- [TurboTax](#)
- [Quickbooks](#)
- [Mint](#)

Search

Search ...

Conclusion & Next Steps

Helm and (Argo) Flux give us a familiar toolset for containerized applications

Git as the source of truth

After our own tools, working on dissemination

Hack a Day Helm GitOps: <https://indico.cern.ch/event/867677/>

Experimenting with the best model to distribute workloads

Likely a mix in the end

Cattle clusters, Blue / Green, Canary with Service Mesh

? Should there be a WLCG repository for common reusable charts