



Hands-on Gitops

Weaveworks – <https://weave.works> – @weaveworks
Kubecon Seattle – December 2018

Brice Fernandes – brice@weave.works – @fractallambda

Hi

I'm Brice

I work for Weaveworks as a **customer success engineer**

You can find **Weaveworks** at <https://www.weave.works> or [@weaveworks](#)

The team at Weaveworks is behind the GitOps model

You can find me online at [@fractallambda](#) and email me at brice@weave.works



Everything available at

tinyurl.com/gitops-tutorial

What is Gitops?

GitOps is...

An operation model

Derived from CS and operation knowledge

Technology agnostic (name notwithstanding)

A set of principles (Why instead of How)

A way to speed up your team



- 1 The entire system is described declaratively.
- 2 The canonical desired system state is versioned (with Git)
- 3 Approved changes to the desired state are automatically applied to the system
- 4 Software agents ensure correctness and alert on divergence

- 1 The entire system is described declaratively.

1 The entire system is described declaratively.

Beyond code, data ⇒

Implementation independent

Easy to abstract in simple ways

Easy to validate for correctness

Easy to generate & manipulate from code

1 The entire system is described declaratively.

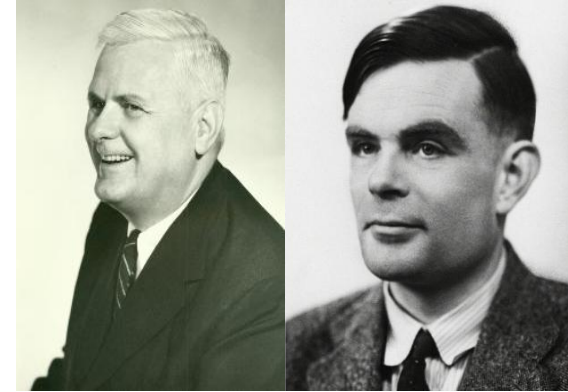
Beyond code, data ⇒

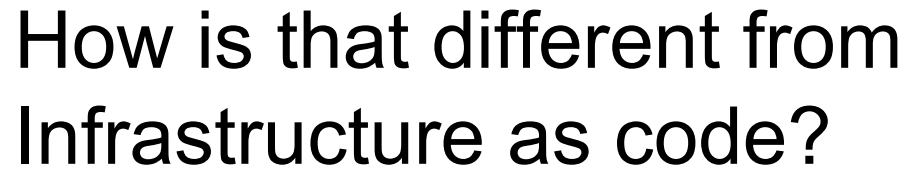
Implementation independent

Easy to abstract in simple ways

Easy to validate for correctness

Easy to generate & manipulate from code



A white speech bubble with a black outline and a tail pointing towards the bottom-left. It contains the text "How is that different from Infrastructure as code?".

How is that different from
Infrastructure as code?

How is that different from
Infrastructure as code?

It's about consistency in the
failure case.

It's about consistency in the failure case.

When imperative systems fail, the system ends up in an **unknown, inconsistent state**.

an **unknown, inconsistent state.**

Declarative changes let you think of changes as transactions.

Declarative changes let you think of changes as transactions.

This is a very good thing.

2

The canonical desired system state is versioned
(with Git)

2 The canonical desired system state is versioned (with Git)

Canonical Source of Truth (DRY)

With declarative definition, trivialises rollbacks

Excellent security guarantees for auditing

Sophisticated approval processes (& existing workflows)

Great Software ↔ Human collaboration point

3

Changes to the desired state are automatically applied to the system

3 Approved changes to the desired state are automatically applied to the system

Significant velocity gains

Privileged operators don't cross security boundaries

Separates **What** and **How**.

4

Software agents ensure correctness and alert on divergence



4

Software agents ensure correctness and alert on divergence

Continuously checking that desired state is met

System can self heal

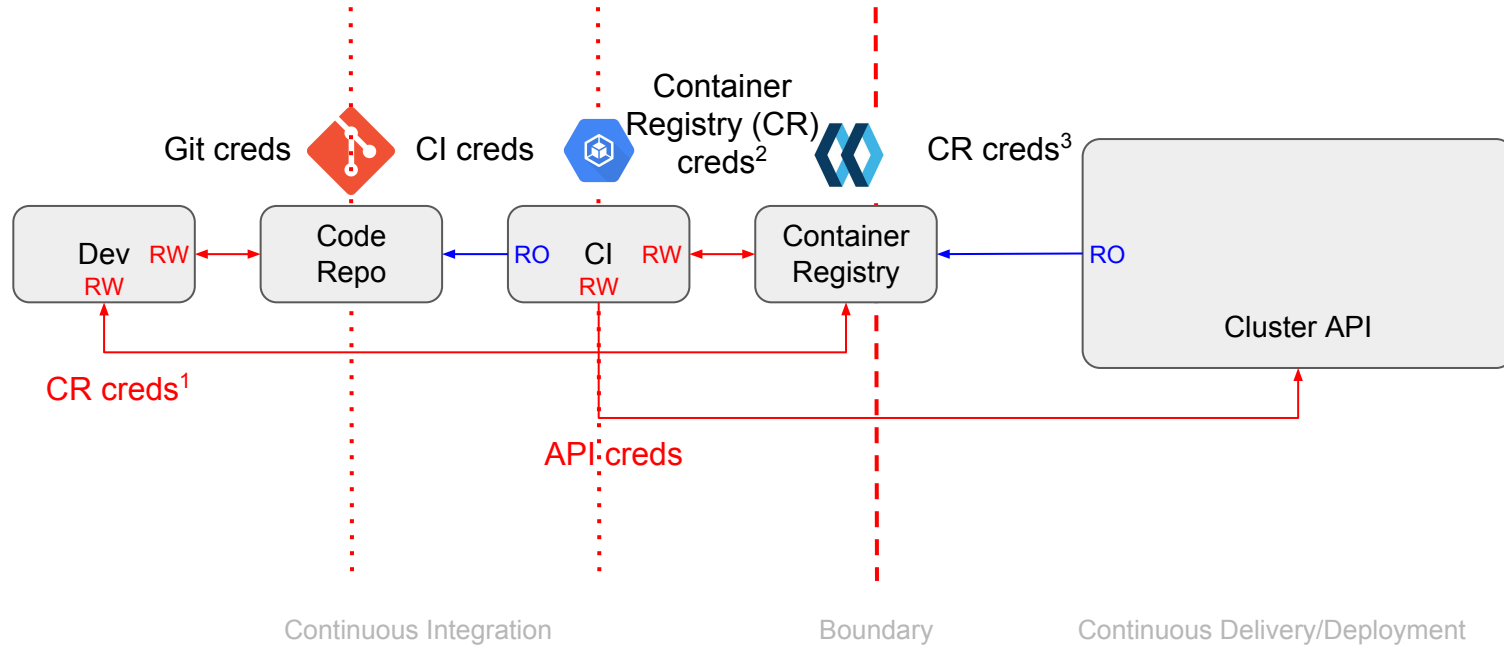
Recovers from errors without intervention (PEBKAC)

It's the control loop for your operations

- 1 The entire system is described declaratively.
- 2 The canonical desired system state is versioned (with Git)
- 3 Approved changes to the desired state are automatically applied to the system
- 4 Software agents ensure correctness and alert on divergence

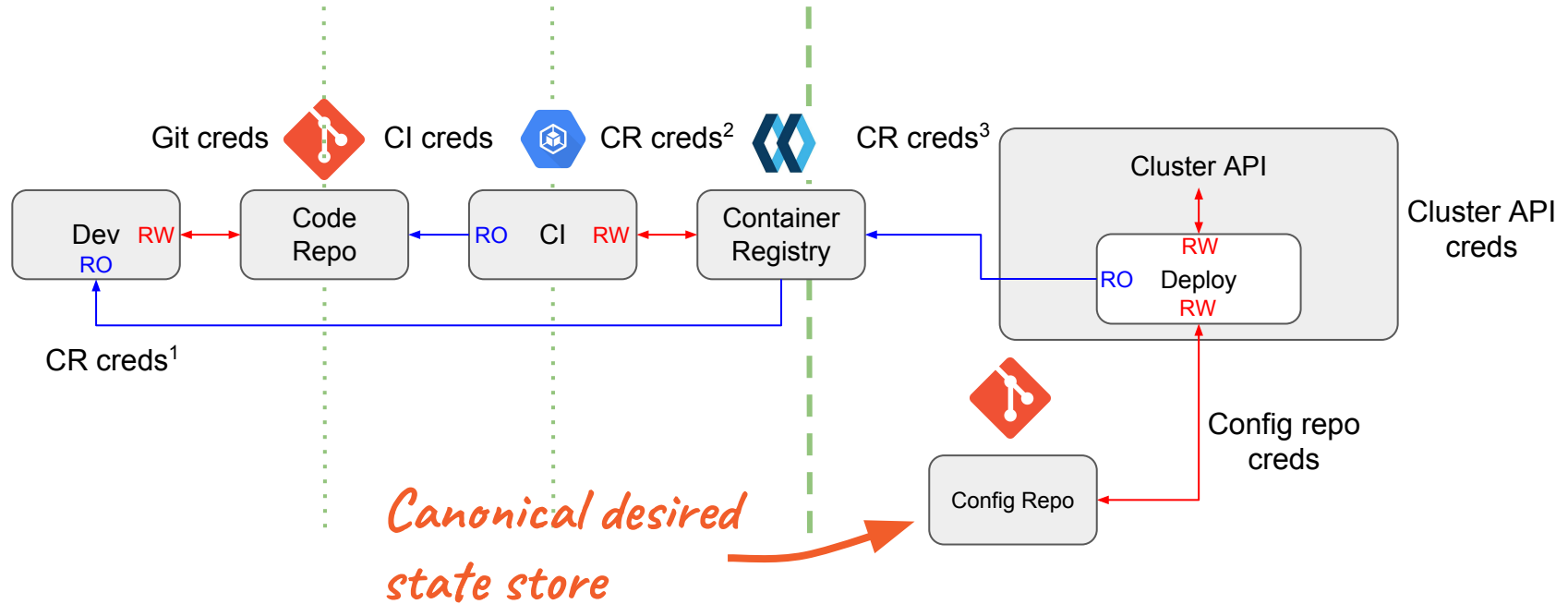
Typical CICD pipeline

Shares credentials cross several logical security boundaries.



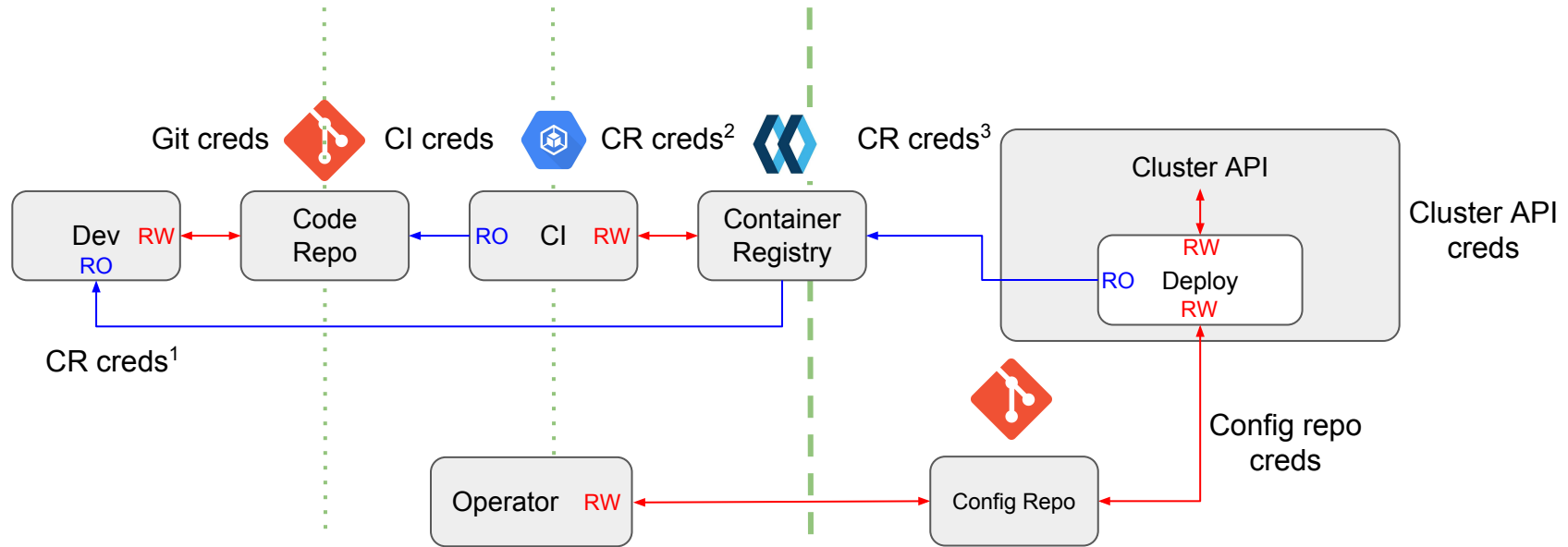
GitOps pipeline

Credentials are never shared across a logical security boundary.



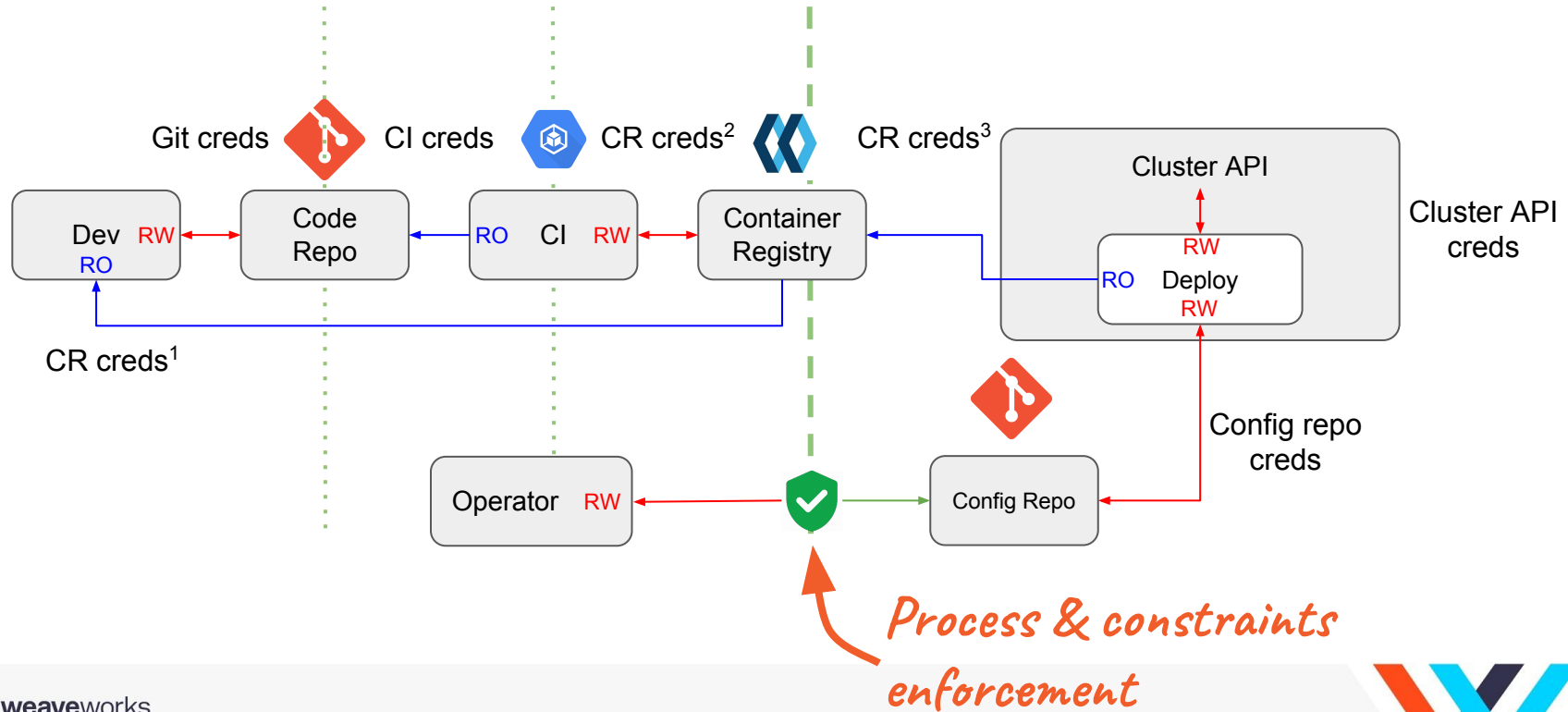
GitOps pipeline

Credentials are never shared across a logical security boundary.



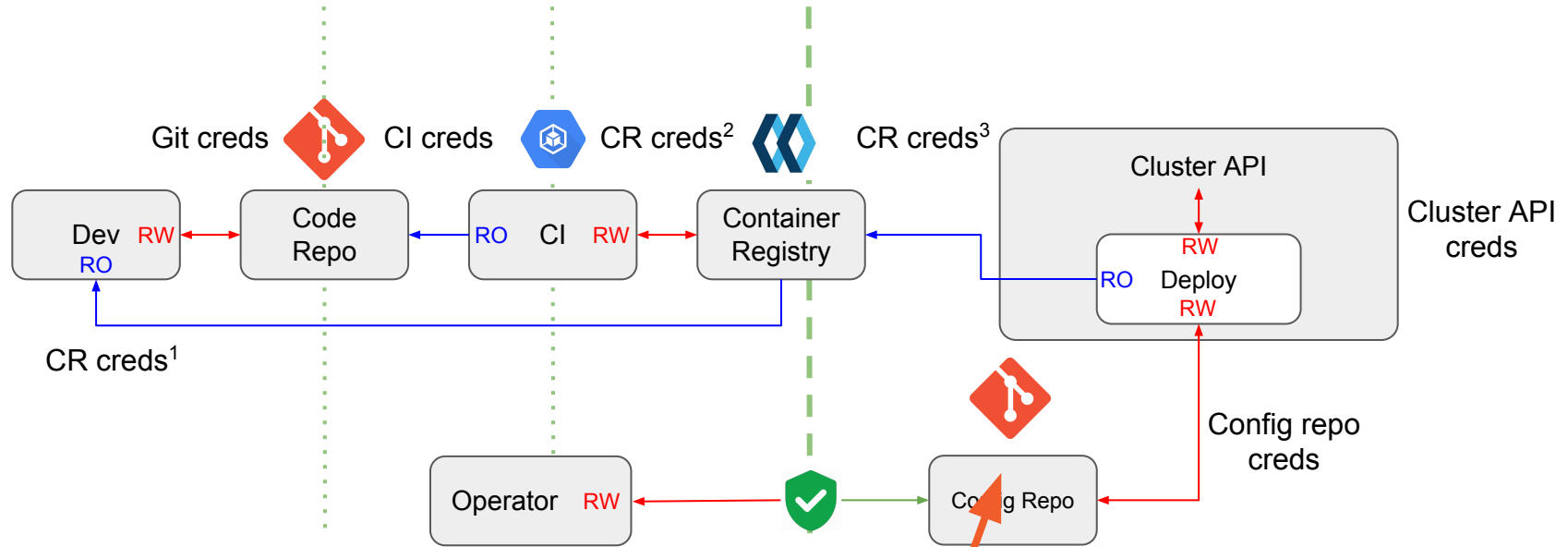
GitOps pipeline

Credentials are never shared across a logical security boundary.



GitOps pipeline

Credentials are never shared across a logical security boundary.



*Exceptional auditing
and attribution*



Gitops is Functional Reactive Programming...

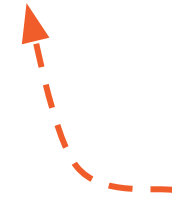
...for your infrastructure.

Like React, but for servers and applications.



What should be GitOps'ed?

What should be GitOps'ed?



*I'm so very
sorry*



?



Kubernetes Manifests

Dashboards

Application checklists

Application configuration

Alerts

Recording Rules

Provisioning scripts

Playbook

Sealed Secrets



 jml Fix corp alert rules

488f056 on 2 Aug

[1 contributor](#)

36 lines (32 sloc) | 1.15 KB

Raw

Blame

History



```
1 # Rules for alerting on stuff related to corporate IT.
2 #
3 # All of these alerts must have 'team = "corp"' in their labels. This routes
4 # them to the #corporate-it channel and away from the production on-call.
5
6 # Alert when our terradiff for corp doesn't match the environment.
7 ALERT CorpTerradiff
8     IF max(terradiff_plan_exit_code) == 2
9     FOR 1h
10    LABELS {
11        severity = "warning",
12        team = "corp",
13    }
14    ANNOTATIONS {
15        summary = "weaveworks/corp terraform config differs from reality",
16        impact = "Someone has lost access to something, or someone has access without approval",
17        dashboardURL = "${base_url}/admin/corp-terradiff",
18        containerName = "terradiff",
19    }
```

279

280 **resource** "github_membership" "bricef" {

281 username = "bricef"

282 role = "admin"

283 }

284

14:30 **AlertManager** APP

[CorpTerradiff - weaveworks/corp terraform config differs from reality](#)

Someone has lost access to something, or someone has access without approval

[Dashboard](#)

Gitops Hands-on

Everything available at

tinyurl.com/gitops-tutorial



**KEEP
CALM
IT'S
DEMO
TIME**

*Installing
and using
OSS Flux*



cloud.weave.works/fluxv2/little-meadow-46/services

Socket Shop (socks.weave.w...)

Deploy Explore Monitor

ilya@weave.works

RESOURCES HISTORY

search Filters UPDATE ALL

<input type="checkbox"/> Workload ▲	Image	Current Tag	Behind	Latest Tag	🔒	🚚	Update
<input type="checkbox"/> loadtest:deployment/load-test	weaveworksdemos/load-test	master-57a...	5mo				UP TO DATE
<input type="checkbox"/> sock-shop:deployment/carts	weaveworksdemos/carts	master-1c6...	5mo				UP TO DATE
<input type="checkbox"/> sock-shop:deployment/carts-db	mongo	No tag specified				🚚	
<input type="checkbox"/> sock-shop:deployment/catalogue	weaveworksdemos/catalogue	master-bf5...	5mo				UP TO DATE
<input type="checkbox"/> sock-shop:deployment/catalogue-db	weaveworksdemos/catalogue-db	master-bf5...	5mo				UP TO DATE
<input type="checkbox"/> sock-shop:deployment/front-end	weaveworksdemos/front-end	master-af3b...	6h Diverged				UPDATE
<input type="checkbox"/> sock-shop:deployment/orders	weaveworksdemos/orders	master-f89...	5mo			🚚	
<input type="checkbox"/> sock-shop:deployment/orders-db	mongo	No tag specified				🚚	
<input type="checkbox"/> sock-shop:deployment/payment	weaveworksdemos/payment	master-b64...	4mo			🚚	
<input type="checkbox"/> sock-shop:deployment/queue-master	weaveworksdemos/queue-master	master-b8b...	5mo			🚚	
<input type="checkbox"/> sock-shop:deployment/rabbitmq	rabbitmq	3.7-rc-man...	2mo	23 versions	3.6-manage... 1mo		UPDATE
<input type="checkbox"/> sock-shop:deployment/session-db	redis	32bit	1mo	4 versions	4-alpine 1mo		UPDATE
<input type="checkbox"/> sock-shop:deployment/shipping	weaveworksdemos/shipping	master-ba3...	5mo			🚚	



cloud.weave.works/fluxv2/little-meadow-46/history

Socket Shop (socks.weave.w...)


Deploy Explore Monitor

ilya@weave.works

RESOURCES HISTORY

History

- Manual deploy: weaveworksdemos/front-end:master-af3b817e to sock-shop:deployment/front-end
23 minutes ago
- Sync to cluster: sock-shop:deployment/front-end (20c187340bbe)
23 minutes ago
- Commit: sock-shop:deployment/front-end (20c187340bbe)
by matthias <matthias@weave.works>
23 minutes ago
- Sync to cluster: sock-shop:deployment/catalogue (f68ba0f8a507)
4 days ago
- Unlock: sock-shop:deployment/catalogue (f68ba0f8a507)
Demo
by brice <brice@weave.works>
4 days ago
- Sync to cluster: sock-shop:deployment/catalogue (2fd23dd6bd93)
4 days ago
- Lock: sock-shop:deployment/catalogue (2fd23dd6bd93)
Demo
by brice <brice@weave.works>
4 days ago
- Manual deploy: weaveworksdemos/catalogue:master-bf571e15 to sock-shop:deployment/catalogue
4 days ago



cloud.weave.works/app/little-meadow-46#!/state/?"gridSortedBy":"docker_memory...

Sock Shop (socks.weave.w... Deploy Explore Monitor ilya@weave.works

April 24th 14:45 15:00 15:15 15:30 15:45 16:00 16:15 16:30 16:45 17:00 17:15 17:30

2018-04-24T16:07:37Z UTC

SEARCH PROCESSES CONTAINERS PODS HOSTS

BY NAME BY DNS NAME CONTROLLERS WEAVE NET

BY IMAGE SERVICES

GRAPH TABLE RESOURCES

CPU Memory

shipping queue-master catalogue front-end

gke-sock-shop-default-p... gke-sock-shop-default-p... gke-sock-shop-default-p... gke-sock-shop-default-p...

11.6MB 109.1MB 290.6MB 14.6MB

front-end

gke-sock-shop-default-pool-9652982b-7pbs gke-sock-shop-default-pool-9652982b-7pbs gke-sock-shop-default-pool-9652982b-7pbs gke-sock-shop-default-pool-9652982b-7pbs

orders

gke-sock-shop-default-p...

16 NODES (101 FILTERED)

All System Containers Application Containers

Stopped containers Running containers Both

Show Uncontained Hide Uncontained

default kube-public kube-system loadtest sock-shop weave All Namespaces

front-end

[weaveworksdemos/fron... front-end-84dbb9c79c-c... gke-sock-shop-default-p...](#)

STATUS

CPU 11.06 %

MEMORY 109.1 MB

INFO

IMAGE: weaveworksdemos/front-end:master

command: /usr/local/bin/npm start

VERSION d19b0293 ON service PLUGINS: n/a



cloud.weave.works/prom/little-meadow-46/workloads/sock-shop%3Adeployment%2...

Sock Shop (socks.weave.w...)

Deploy Explore Monitor

ilya@weave.works

DASHBOARDS

- Workload Resources
- Node Resources
- Workloads
 - kube-system
 - fluentd-gcp-v2.0.10
 - nvidia-gpu-device-plugin
 - event-exporter-v0.1.7
 - heapster-v1.5.0
 - kube-dns
 - kube-dns-autoscaler
 - kubernetes-dashboard
 - l7-default-backend
 - metrics-server-v0.2.0
 - loadtest
 - load-test
 - sock-shop
 - carts
 - carts-db
 - catalogue
 - catalogue-db
 - front-end
 - orders
 - orders-db
 - payment
 - queue-master
 - rabbitmq
 - session-db
 - shipping
 - user
 - user-db
 - weave

April 24th

14:45 15:00 15:15 15:30 15:45 16:00 16:15 16:30 16:45 17:00 17:15 17:30

2018-04-24T16:08:26Z UTC 1h

sock-shop:deployment/catalogue

Workload Dashboard

Summary Resources Go

Concurrency

Number of Goroutines

Time	Number of Goroutines (Approximate)
15:15	10
15:30	10
15:45	10
16:00	10



**KEEP
CALM
IT'S
DEMO
TIME**

*Using
Weave Cloud*

Questions?



Weaveworks

<https://weave.works>

@weaveworks

@fractallambda

brice@weave.works

45 day trial



go.weave.works/extended