Status of the Common Platform

October 2020 Edition

The Team

Pranav Baitule

Chase Dooley

Michael Irwin

Brian Maloney

Nandan Sadineni

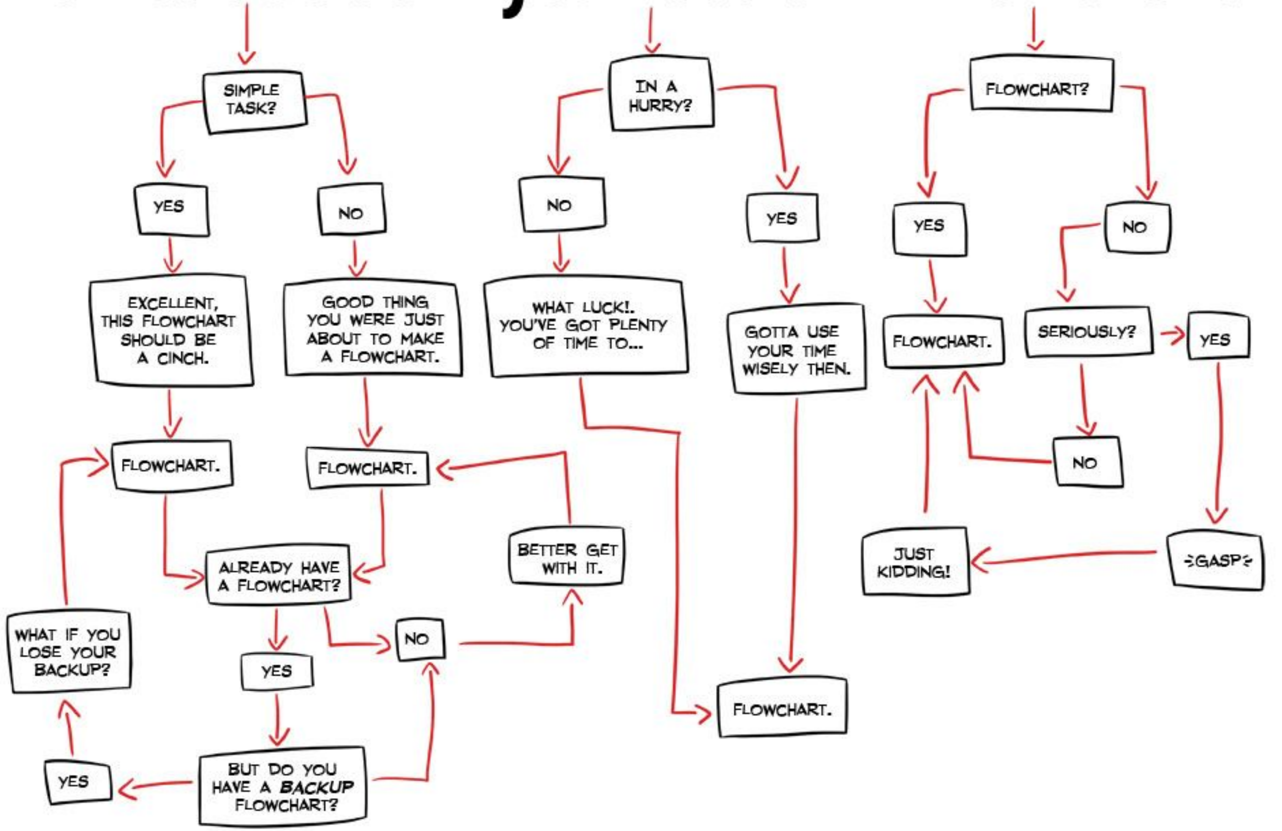
Mathew Mathai

Justin Strickland

AJ Yost

What problems are we trying to solve?

How to decide if you need a . . . flowchart.


SIMPLE TASK?
YES
NO
EXCELLENT, THIS FLOWCHART SHOULD BE A CINCH.
GOOD THING YOU WERE JUST ABOUT TO MAKE A FLOWCHART.
FLOWCHART.
FLOWCHART.
ALREADY HAVE A FLOWCHART?
YES
NO
BETTER GET WITH IT.
BUT DO YOU HAVE A BACKUP FLOWCHART?
YES
WHAT IF YOU LOSE YOUR BACKUP?
IN A HURRY?
NO
YES
WHAT LUCK!. YOU'VE GOT PLENTY OF TIME TO...
GOTTA USE YOUR TIME WISELY THEN.
FLOWCHART.
FLOWCHART?
YES
NO
FLOWCHART.
SERIOUSLY?
YES
NO
:GASP:
JUST KIDDING!

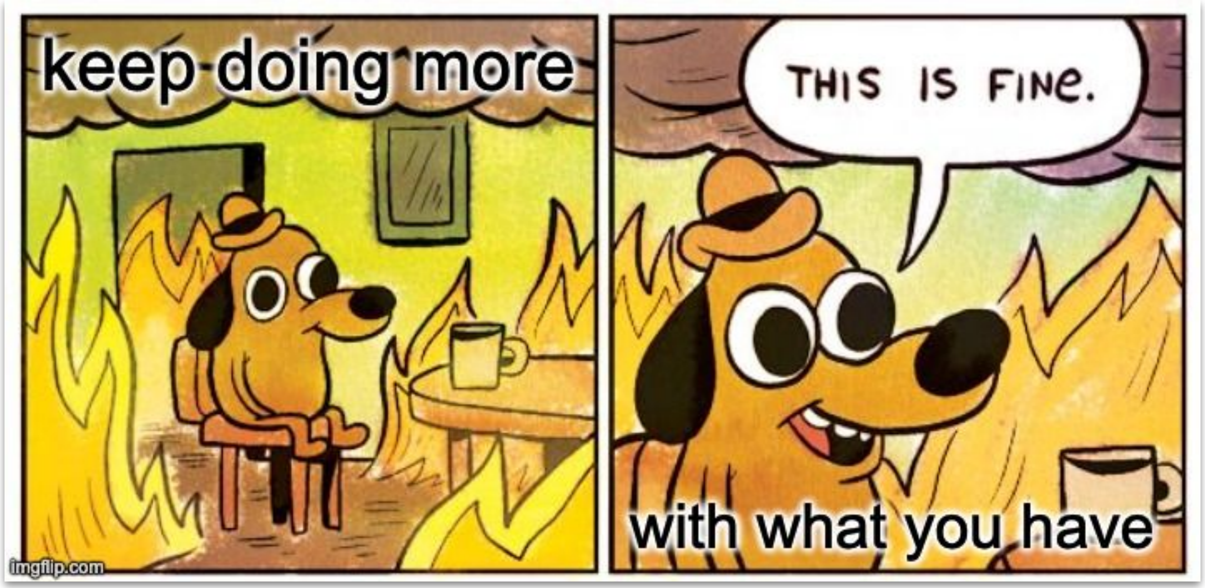
PAJAMAFOREST.COM

© 2011 EVAN DIAZ

There is no cloud
it's just someone else's computer

ONE DOES NOT SIMPLY
"GO TO THE CLOUD"
made on imgur

60% OF THE TIME
DEPLOYMENTS WORK EVERYTIME!


keep doing more
THIS IS FINE.
with what you have
imgflip.com

What is the industry doing to help?

The Rise of Declarative Frameworks

```
resource "aws_s3_bucket" "state_bucket" {
  bucket = "my-state-bucket"
  versioning {
    enabled = true
  }
  tags = {
    Environment = "Dev"
  }
}


resource "aws_iam_policy" "bucket_access" {
    name = "state_bucket_access"
    policy = <<POLICY
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [ "s3:ListBucket" ],
        "Resource": [ "${aws_s3_bucket.state_bucket.arn}" ]
      },
      {
        "Effect": "Allow",
        "Action": [ "s3:GetObject" ],
        "Resource": [ "${aws_s3_bucket.state_bucket.arn}/*" ]
      }
}
POLICY
}
```

```
version: "3.7"
services:
  app:
    build: ./
    ports:
     - "8080:8080"
    volumes:
       - ./:/code

  db:

    image: postgresql
```

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: example-cert
spec:
  commonName: my-app.example.com
  secretName: my-app-tls-cert
  issuerRef:
    kind: ClusterIssuer
    name: letsencrypt
```

The Rise of Containerized Applications

How’s the Common Platform solving these problems?

The Original Charge

Initiative

Establish an organizational unit that provides application technology infrastructure and shared services for all application development teams in the Division and as a service to all.

Outcomes

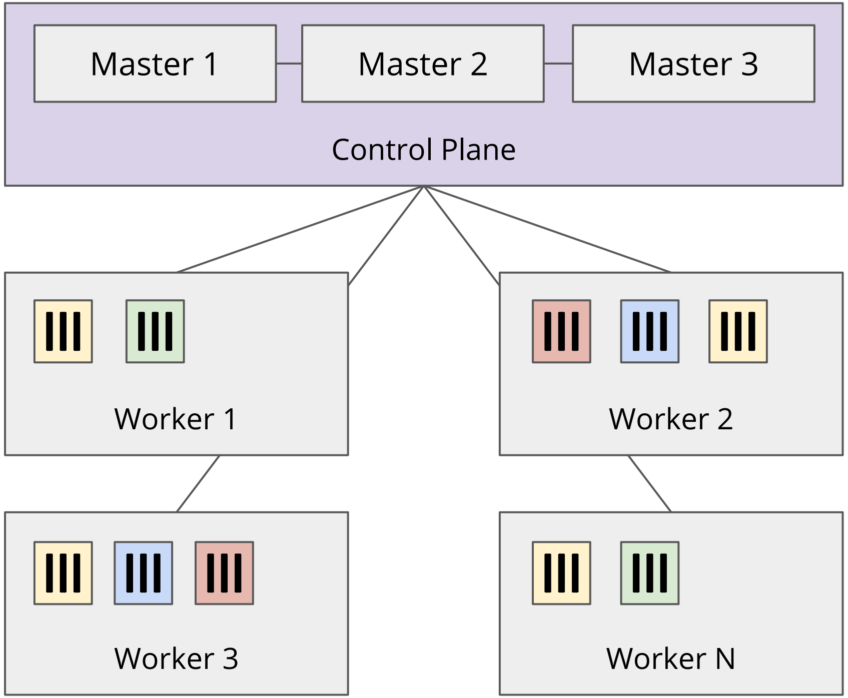
- Teams will leverage a single common platform on which to run applications.
- Shared application development and deployment services will be managed by a single team.

The Goal, tldr style

- If you can make a container image, we can run it
    - Means we can support any language, framework, or toolset
- We’ll provide tools/services to help build, configure, monitor, troubleshoot, and smoothly deploy updates
- You won’t have to worry about machines, certs, and more

Using Container Orchestration (Kubernetes)

- A declarative system that works to make **actual state** reflect **desired state**
- The framework uses event-driven mechanisms to respond to changes
- Supports many built-in types of resources, but highly extensible



A few guiding principles…

- Multi-tenancy by design, from the start
- Give as much control back to app teams as possible
- Make things as easy as possible to help adoption
- We will “dogfood” as much of the system and processes as possible
- *-as-code as much as possible
- Be as open and transparent as possible

What have we been doing lately?

In the past six months, we’ve...

- Learned *a lot* about Kubernetes
    - Completed courses for Certified Kubernetes Administrator and Certified Kubernetes Application Developer
- Spun up many, many Kubernetes clusters
    - Some to replace accidental breakages, some on purpose
- Learned to manage our clusters completely using Git
    - Changes are applied via automated build pipelines

We’ve also…

- Figured out DNS structure and direction
  - Both for the cluster, as well as apps that will be deployed on it
- Explored various deployment models
  - Deploy via pipelines vs gitops vs manual interactions
- Integrated automatic TLS cert management
  - No more requesting certs. No more expired certs. No more worries.

Even more, we’ve...

- Integrated the ability to safely auto-assume AWS roles
    - Leverage services in another AWS account (S3, SQS, etc.)
- Integrated Vault support
    - Store secrets in Vault and authorize k8s apps to have access to them
- Plugged in a policy framework to protect teams
    - Ensure teams only use resources they have access to

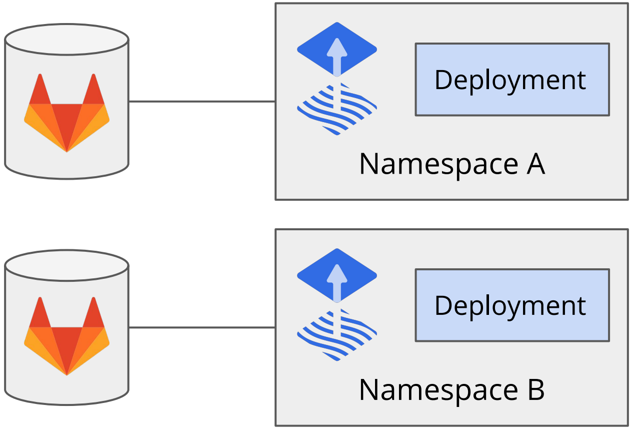
How’s it going to work?

Carving up the Cluster

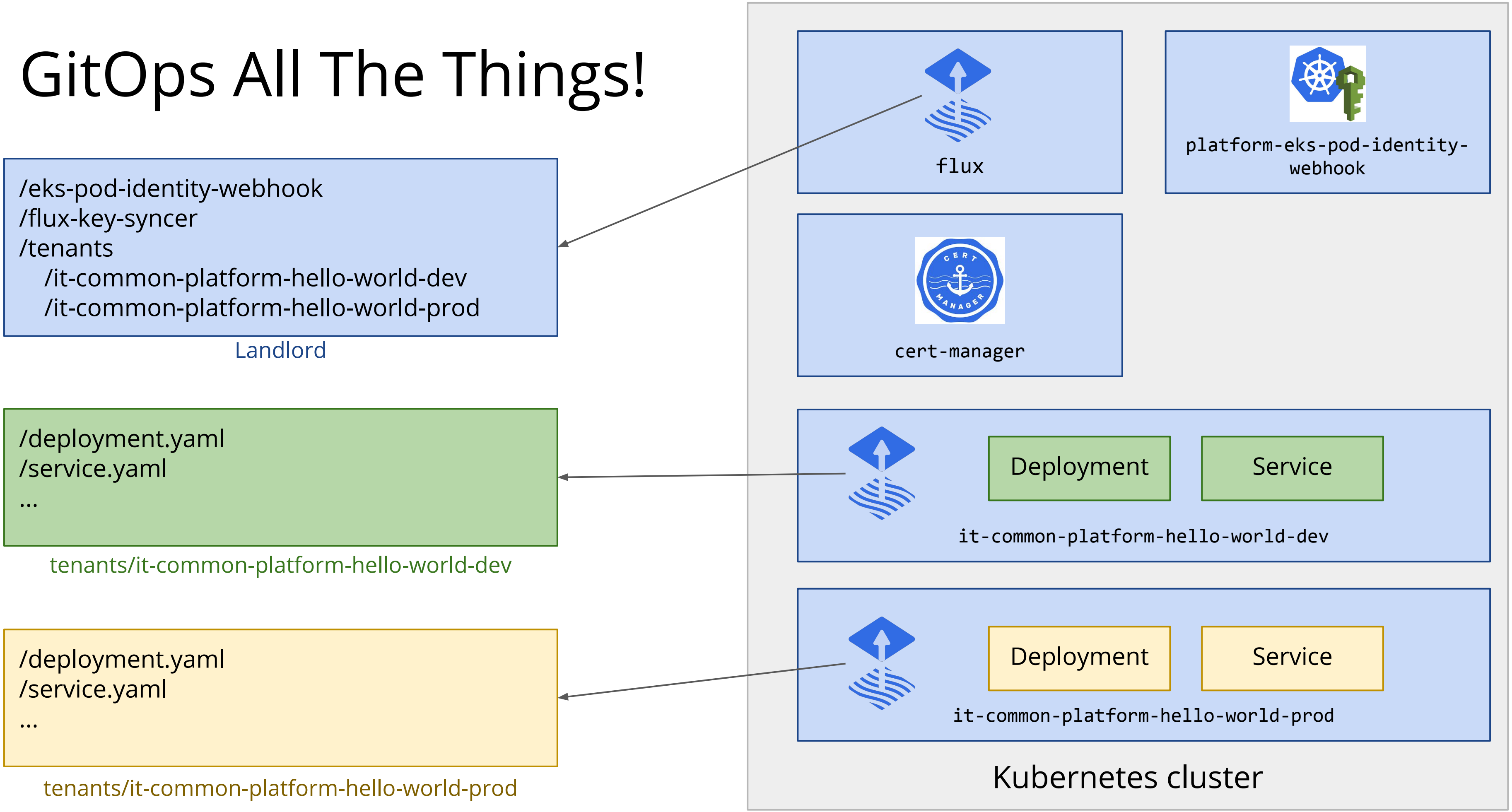
- Kubernetes supports the concept of **namespaces**
  - Provides the ability to create smaller “virtual clusters”
- When combined with RBAC, roles and users can be limited to operate on only specific resources within a specific namespace
- Each app will have its own namespace
  - Beyond that, each environment of an app will have its own

Making Changes in the Cluster

- Each app will have a repo that will contain YAML manifest files
- Changes to the manifests are automatically applied in the cluster
    - This is using a pull-model; pipelines and users will be read-only



GitOps All The Things!



/eks-pod-identity-webhook
/flux-key-syncer
/tenants
  /it-common-platform-hello-world-dev
  /it-common-platform-hello-world-prod

Landlord

/deployment.yaml
/service.yaml
…

tenants/it-common-platform-hello-world-dev

/deployment.yaml
/service.yaml
…

tenants/it-common-platform-hello-world-prod

flux

platform-eks-pod-identity-webhook

cert-manager

Deployment Service

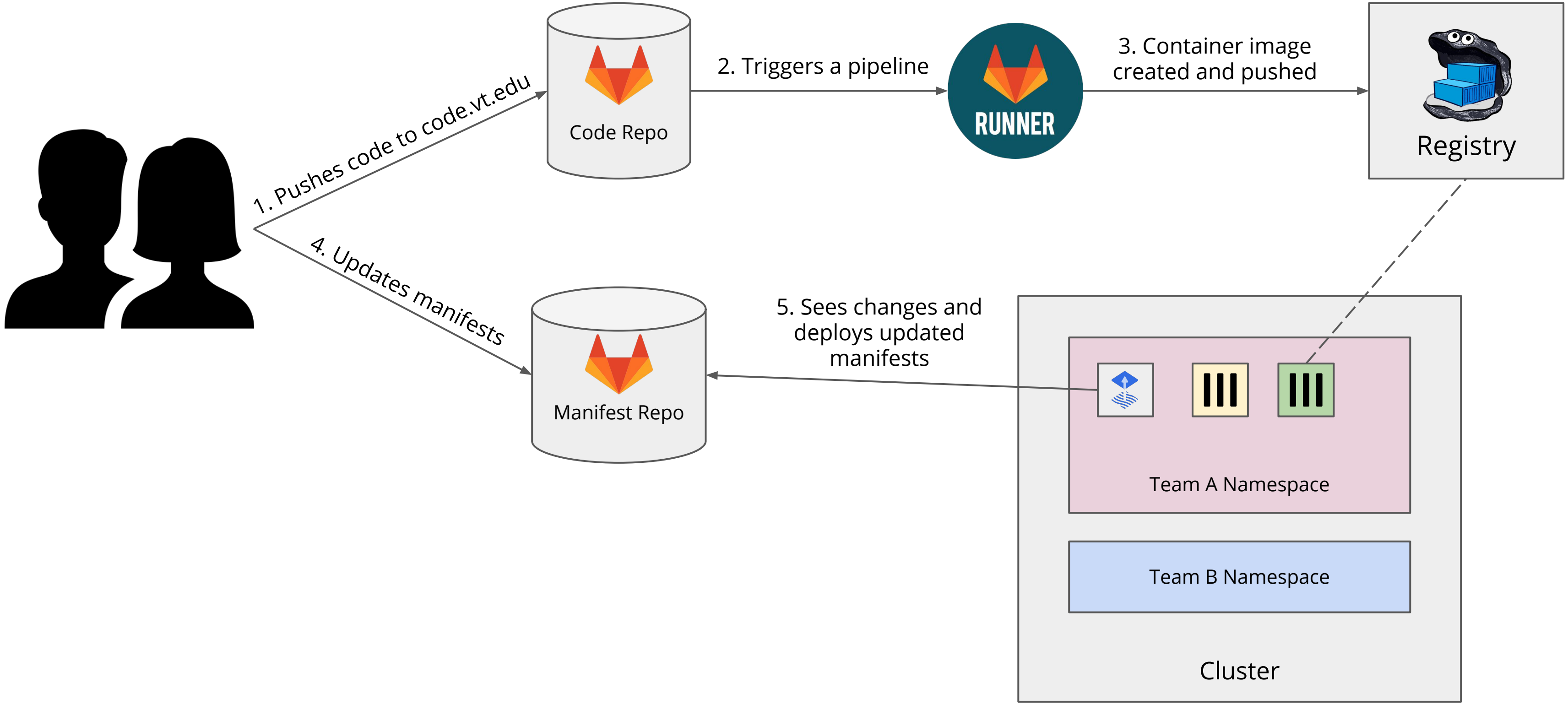
it-common-platform-hello-world-dev

Deployment Service

it-common-platform-hello-world-prod

Kubernetes cluster

A Typical App Update Journey



DEMO
ALL THE THINGS
imgflip.com

What’s coming up?

Pilot Users Wanted!

- We’re ready to start onboarding a few test apps!
- Expectations
  - Will be a highly collaborative effort
  - Looking only for non-mission critical apps
  - Will only have business hour support right now
  - Smaller scale apps (resource-wise) are preferred right now
- If interested, contact Michael Irwin, Justin Strickland, or AJ Yost

Want to keep up?

- Follow us on the `#it-common-platform` Slack channel
  - Get updates and ask questions
  - Links to bi-weekly sprint reviews and their recordings
- Join us for our next Sprint Review this afternoon at 1:30
  - Link is in the `#it-common-platform` Slack channel
- Reach out to Michael Irwin, Justin Strickland, or AJ Yost

Thanks! Questions?