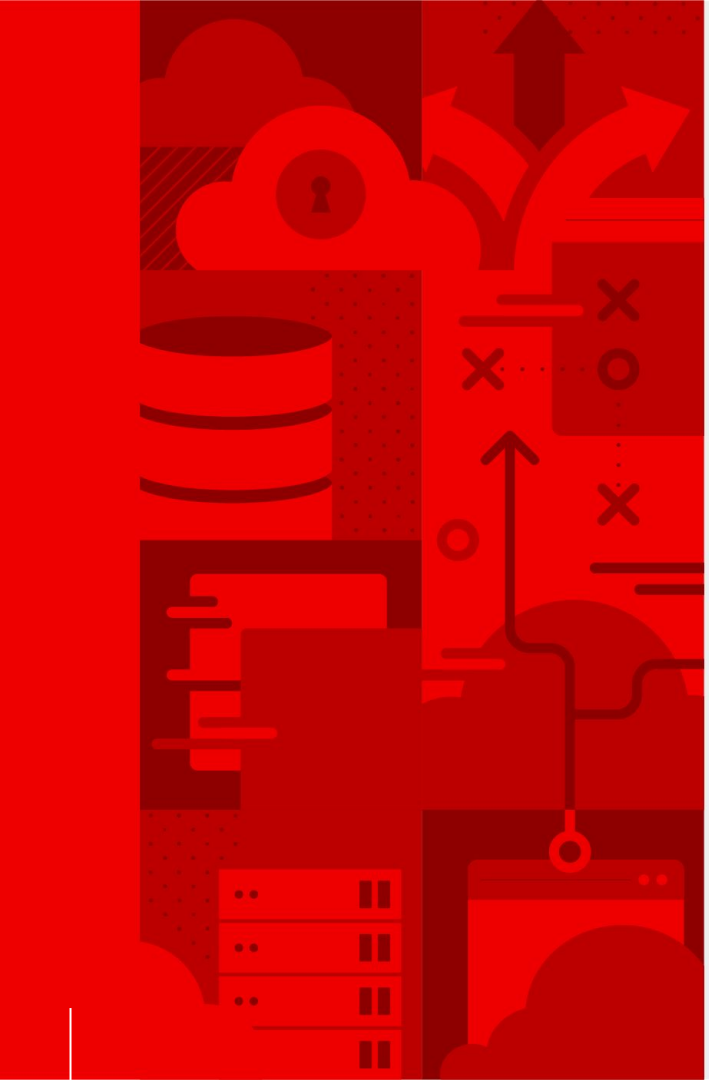


OpenShift Developer

Application Packaging

CI/CD

Self introduction

Name: Wanja Pernath

Email: wpernath@redhat.com

Base: Germany (very close to the Alps)

Role: EMEA Technical Partner Development Manager - OpenShift and MW

Experience: Years of Consulting, Training, PreSales at Red Hat and before

Agenda / etc.

Agenda

- Application Packaging with OpenShift
  - Basics
  - OpenShift Templates
  - kustomize.io
  - Helm Charts
  - Operators
  - Summary
- Demo

Helm Charts

What

- Helm originally invented 2015 and introduced later that year at KubeCon
- Helm moved as Kubernetes subproject in 2016 as Helm 2.0
- Helm 3.x is now (since 2020) an official CNCF project
- Helm is THE package manager for Kubernetes Applications
    - Helm is like RPM / APT for Linux
    - Or maven / npm for Java / node.js
- Helm Charts can easily be created, installed into a Kubernetes Cluster and also being upgraded
- With the Artifact Hub you have a huge repository of available community driven and maintained charts for every need

Can I use it?

- Short answer: Of course, but mainly for distributing your app!
- Longer answer: If you have an app release and you have to make it available for others, create a Helm Chart for it and make it easy for your customers (regardless of internal or external) to consume it
    - If you are just looking for a way to move your app from one stage to the other, have a look at Templates or kustomize.io
    - Helm and ArtifactHub are a great resource to look at for components you might need

Szenarios to use Helm Charts

- Well used for distribution of Applications
- Internal distribution & external
- Not so great for use within CI/CD (but possible, of course)

Drawbacks?

- Learning curve of Helm Charts is steep at the beginning
- It adds another complexity to your app development cycle
- Client is a templating engine with its own DSL and complexity
- Helm is intended for Day-1 Operations
- Helm is intended for stateless application distribution

Helm 2 vs 3

- Helm 2 required a server component called Tiller
  - Another app on top of kubernetes which had to be managed and maintained
  - Tiller had its own RBAC and its own audit trail
  - Tiller was storing sensitive data in ConfigMaps
  - → Loss of visibility
- Helm 3 does not need a server side component
  - It uses native kubernetes approach and only a client side tool

- **⇒ This is the reason why OpenShift did not natively support Helm prior V3**

Resources

- Helm.sh
- Spotlight on Helm
- To Helm or not?. Helm is becoming a very popular tool to… | by Stepan | FAUN
- From Templates to Openshift Helm Charts
- Working with Helm charts using the Developer perspective - Application life cycle management | Applications | OpenShift Container Platform 4.6
- How to make a Helm chart in 10 minutes
- Artifact Hub
- https://github.com/wpernath/helm-demo.git
- Automated Application Packaging And Distribution with OpenShift - Part 2/3 – Open Sourcerers

Helm DEMO

Operators

What

- Operators were originally invented 2018 by coreos as a way to extend kubernetes by adding new custom resources and controllers or to help human operators to operate and manage stateful applications on kubernetes
- Operators are part of the kubernetes project
- Operators are like Helm Charts a way to distribute your app
- Operators contain all the domain logic required to manage the app
    - It understands how to scale up / down a stateful app
    - It understands how to do backups
- Operators are packaged as a mix of yaml definitions and a standard language like Go, Java etc.
- OperatorHub.io contains a nice set of available operators
- OperatorSDK helps you to create an own operator

Wait… stateless / stateful?

- Stateless
  - Kubernetes can manage stateless apps easily
  - Scaling is just a matter of adding a new pod
- Stateful
  - Imagine a mysql database
  - Scaling that up, means kubernetes is creating copies of the data
  - In fact, you then would have 3 different DBs
  - You need to find a way to properly scale mysql
  - Every app handles that differently (mysql vs. postgres vs. redis)
  - That domain logic needs to be put into an Operator to automate those tasks

Can I use it?

- Short answer: Of course!
- Longer answer:
  - Whenever you need to find a way to tell kubernetes how to manage your stateful complex app, you have to use Operators.
  - If your app is stateless or does not need special treatment, don’t use Operators, think about Helm Charts then

Drawbacks?

- Quite complex
- You need to understand kubernetes properly

Resources

- OperatorHub.io | The registry for Kubernetes Operators
- Operators on Red Hat OpenShift
- Operator SDK
- An intro to Kubernetes operators
- Kubernetes Operator simply explained in 10 mins

Summary

Summary

- All 4 packaging mechanisms discussed are solving mainly 2 different use cases
  - Application Distribution
  - CI/CD
- Helm Charts, Kubernetes Operators and kustomize are standardized kubernetes or CNCF projects.
- Templates are OpenShift specific
- Unfortunately, you have to think about 2 different mechanisms in a typical project
  - You need CI/CD → kustomize or Templates
  - You might need app distribution → Helm or Operator

Summary - CI/CD

- Use OpenShift Templates if
  - You're purely on OpenShift
  - You need a quick and easy way to move your apps to other stages
  - You want to create special sample apps for developers
  - You want to be included in the developer perspective to choose from
  - You don't like the approach of kustomize (patch&merge)
- Use kustomize if
  - You just want to have a standard way of doing CI/CD
  - You don't like the template approach
  - You don't know if you're staying on OpenShift
  - You want to rely on kubernetes standards

Summary - Application Distribution

- Use Helm if
  - Your app is relatively easy and straight forward
  - Your app does not require special kubernetes configs
  - You app is mainly a stateless application
- Use Operators if
  - Your app requires special handling, special kubernetes custom resources (CRDs)
  - Is complex and requires a special backup strategy
  - Needs several Dependencies
  - Have a special need for Day 2 Operations
  - Is a stateful application
- Good: You can even create Operators out of a Helm Chart

Resources

- Kubernetes Operators and Helm — It takes Two to Tango
- Kubernetes Operators vs. Helm Charts: Which to Use and When
- Build Kubernetes Operators from Helm Charts in 5 steps
- Automated Application Packaging and Distribution with OpenShift – Part 1/2
- Automated Application Packaging And Distribution with OpenShift - Part 2/3

CI/CD with OpenShift

Basics

Wouldn't it be great, if everything could be automated?

Wouldn't it be great, if we simply do <insert hype here> and it solves all problems we have?

With DevOps we have a principle which solves most of the issues - but wait! The *DevOps Person* of the customer is currently on vacation


WE DO DEVOPS ALREADY
JUST WITHOUT AGILE, STANDUPS, CI, CODE OR ANY OF THAT OTHER HIPSTER STUFF
memes.com

Basics - Developer

- Important: Separation of code and config!
- Writes the code of the App
- Writes set of build files (maven, gradle, etc.)
- Writes all needed tests (unit, integration, load)
- Writes Pipeline files
- Writes kubernetes manifest files
- Stores everything auditable in Git
- Finds a way and tools to combine all of the above

Basics - Operations

- Gets images, configs, test descriptions from Devs
- Adds own kubernetes manifests to the soup
- Makes sure, everything gets deployed
- Makes sure every dependency is installed and ready
- Thinks about security
- Thinks about networking
- Thinks about storage
- Thinks about compute power
- Thinks about plumbing everything together

Basics

CI/CD

=

Automation of Software Delivery

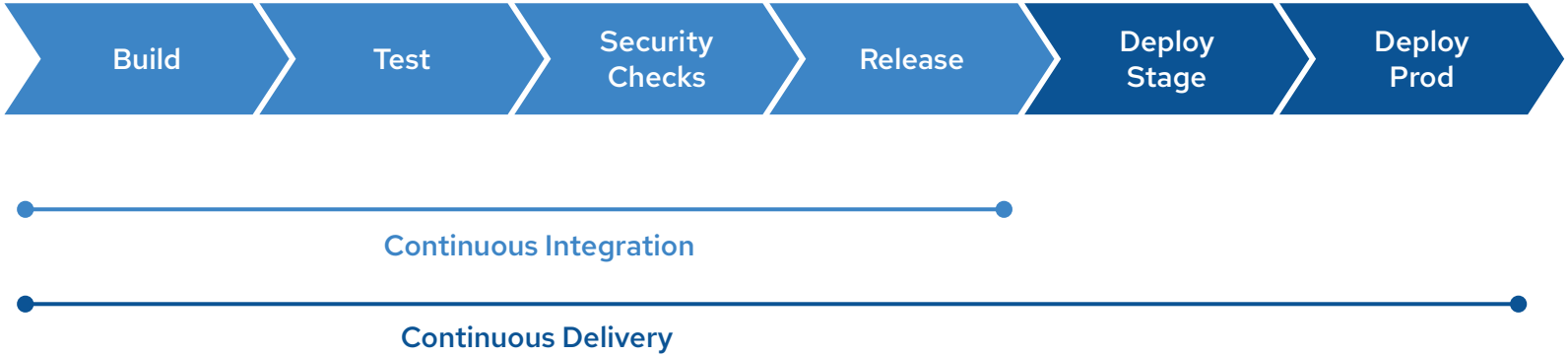
DevOps

=

Let’s have Dev and Ops TALK to each other

Continuous Integration(CI) & Continuous Delivery (CD)

A key DevOps principle for automation, consistency and reliability



Red Hat

OpenShift Builds

Automate building container images using Kubernetes tools

Red Hat

OpenShift Builds

Kubernatives-native image build

A Kubernative-native way to building container images on OpenShift which is portable across Kubernetes distros

Supports multiple build strategies

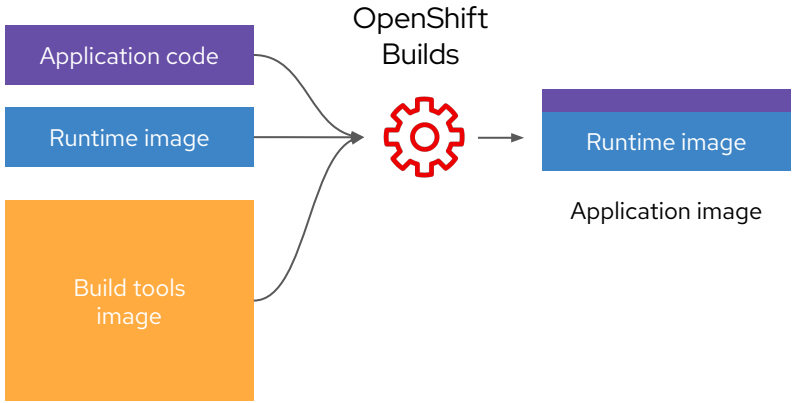
Choose the build strategy that fits best your applications and skills: source-to-image, Dockerfile, and Cloud-Native Buildpacks

Extend with additional build strategies

Extend to use community Kubernetes builds strategies or your own custom builds

OpenShift Builds

- Build images on OpenShift and Kubernetes
- Use Kubernetes builds tools
  - Source-to-Image
  - Buildpacks
  - Buildah
  - Kaniko
  - ...more
- Create lean application images
- Extend with your own build tools
- Based on Shipwright open-source project



OpenShift Builds

BuildStrategy

How to build images e.g. S2I, Buildpacks, etc

Build

What to build

BuildRun

Build execution details

OpenShift Builds

Cloud-Native Buildpacks

```
kind: Build
metadata:
  name: myapp-buildpack
spec:
  source:
    url: https://github.com/myorg/myapp
  strategy:
    name: buildpacks-v3
  builder:
    image: paketobuildpacks/builder:full
  output:
    image: quay.io/myorg/myapp:v1
```

Source-to-Image (S2I)

```
kind: Build
metadata:
 name: myapp-s2i
spec:
 source:
   url: https://github.com/myorg/myapp
 strategy:
   name: source-to-image
 builder:
   image:
registry.redhat.io/openjdk/openjdk-11-rhel8
 output:
   image: quay.io/myorg/myapp:v1
 runtime:
   image: docker.io/openjdk:11-jre-slim
```

Tekton / OpenShift Pipelines

Kubernetes native on demand delivery pipelines

Red Hat

What is Cloud-Native CI/CD?

Containers

Built for container apps and runs on Kubernetes

Serverless

Runs serverless with no CI/CD engine to manage and maintain

DevOps

Designed with microservices and distributed teams in mind

Why Cloud-Native CI/CD?

Traditional CI/CD	Cloud-Native CI/CD
Designed for Virtual Machines	Designed for Containers and Kubernetes
Require IT Ops for CI engine maintenance	Pipeline as a service with no Ops overhead
Plugins shared across CI engine	Pipelines fully isolated from each other
Plugin dependencies with undefined update cycles	Everything lifecycled as container images
No interoperability with Kubernetes resources	Native Kubernetes resources
Admin manages persistence	Platform manages persistence
Config baked into CI engine container	Configured via Kubernetes ConfigMaps

Why Cloud-Native CI/CD?

Traditional CI/CD	Cloud-Native CI/CD
Designed for Virtual Machines	Designed for Containers and Kubernetes
Require IT Ops for CI engine maintenance	Pipeline as a service with no Ops overheard
Plugins shared across CI engine	Pipelines fully isolated from each other
Plugin dependencies with undefined update cycles	Existing library of reusable images
No interoperability with Kubernetes resources	Native Kubernetes resources
Admin manages persistence	Platform manages persistence
Config baked into CI engine container	Configured via Kubernetes ConfigMaps

Jenkins

TEKTON

OpenShift Pipelines

Built for Kubernetes

Cloud-native pipelines taking advantage of Kubernetes execution and , operational model and concepts

Scale on-demand

Pipelines run and scale on-demand in isolated containers, with repeatable and predictable outcomes

Secure pipeline execution

Kubernetes RBAC and security model ensures security consistently across pipelines and workloads

Flexible and powerful

Granular control over pipeline execution details on Kubernetes, to support your exact requirements

Powered by TEKTON

Red Hat

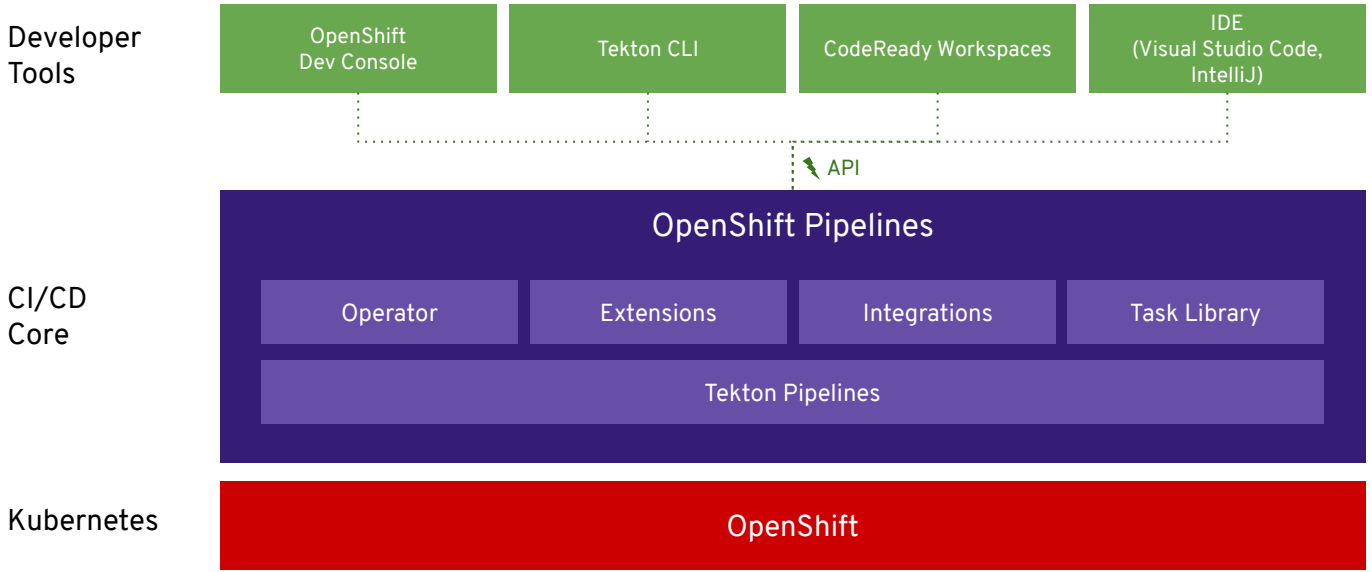
An open-source project for providing a set of shared and standard components for building Kubernetes-style CI/CD systems

Governed by the Continuous Delivery Foundation

Contributions from Google, Red Hat, Cloudbees, IBM, Pivotal and many more

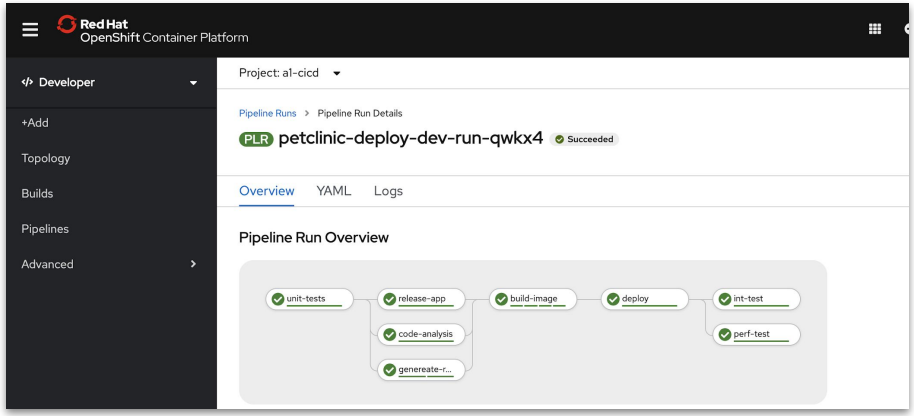
Red Hat

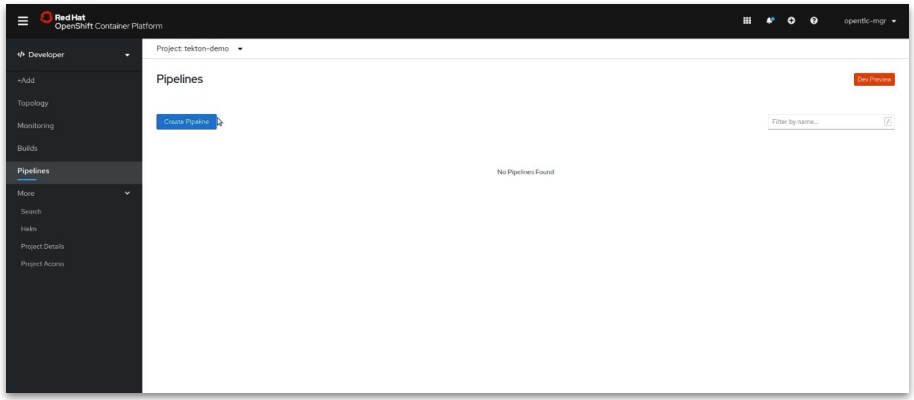
OpenShift Pipelines



OpenShift Pipelines

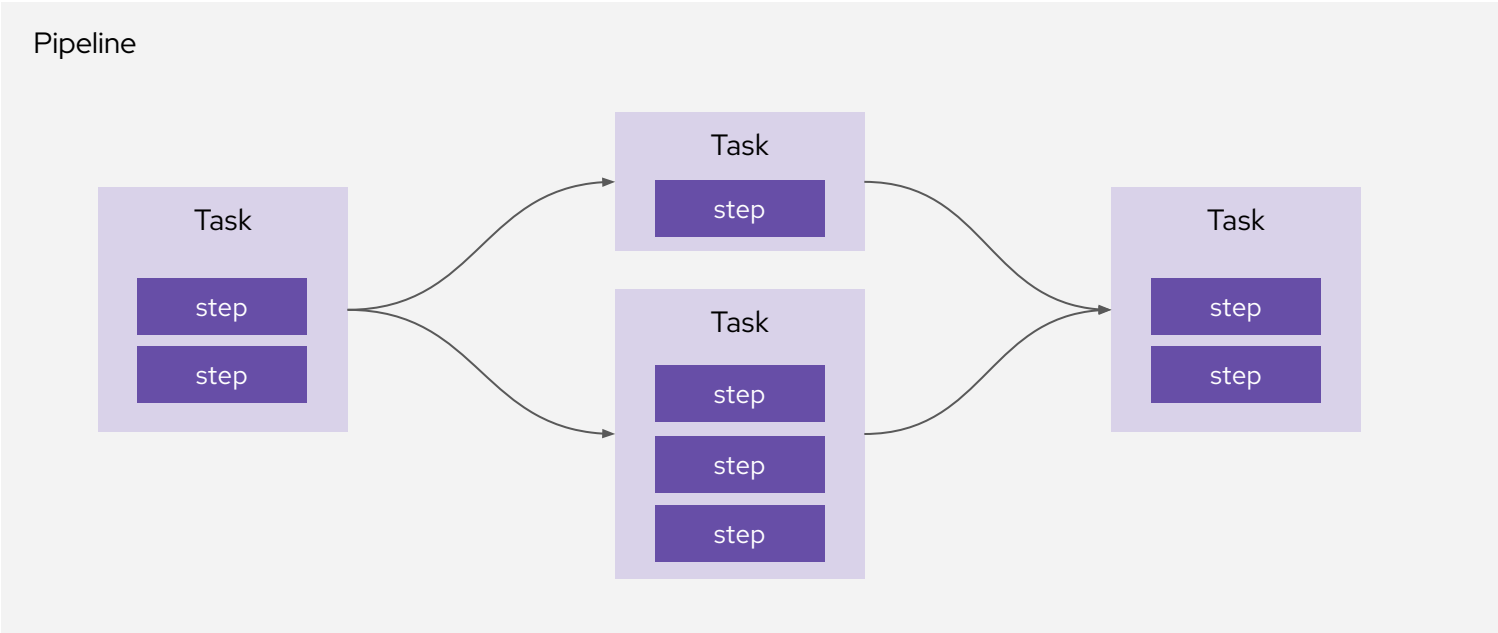
- Based on Tekton Pipelines
- Kubernetes-native declarative CI/CD
- Pipelines run on-demand in isolated containers
- No central server to maintain! No plugin conflicts!
- Task library and integration with Tekton Hub
- Secure pipelines aligned with Kubernetes RBAC
- Visual and IDE-based pipeline authoring
- Pipeline templates when importing apps
- Automated install and upgrades via OperatorHub
- CLI, Web, VS Code and IntelliJ plugins





Red Hat

Tekton Concepts



Tekton Concepts: `step`

- Run command or script in a container
- Kubernetes container spec
  - Env vars
  - Volumes
  - Config maps
  - Secrets

```yaml
- name: build
  image: maven:3.6.0-jdk-8-slim
  command: [“mvn”]
  args: [“install”]
```

```yaml
- name: parse-yaml
  image: python3
  script:|-
    #!/usr/bin/env python3
    ...
```

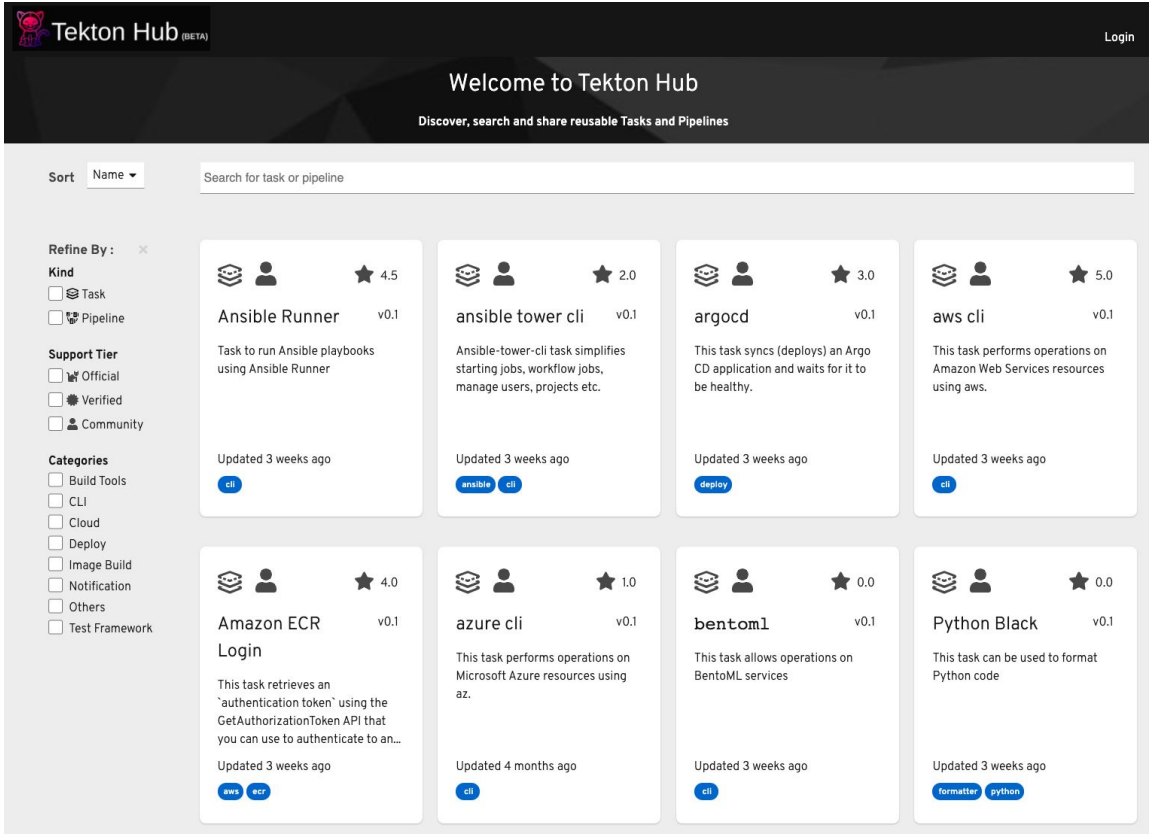
Tekton Concepts: Task

- Performs a specific task
- List of steps
- Steps run sequentially
- Reusable

```yaml
kind: Task
metadata:
 name: buildah
spec:
 params:
 - name: IMAGE
 steps:
 - name: build
   image: quay.io/buildah/stable:latest
   command: ["buildah"]
   args: ["bud", ".", "-t", "$(params.IMAGE)"]
 - name: push
   image: quay.io/buildah/stable:latest
   script: |
     buildah push $(params.IMAGE) docker://$(params.IMAGE)
```

Tekton Hub

Search, discover and install Tekton Tasks

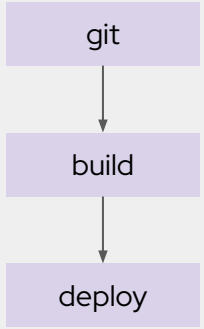


Red Hat

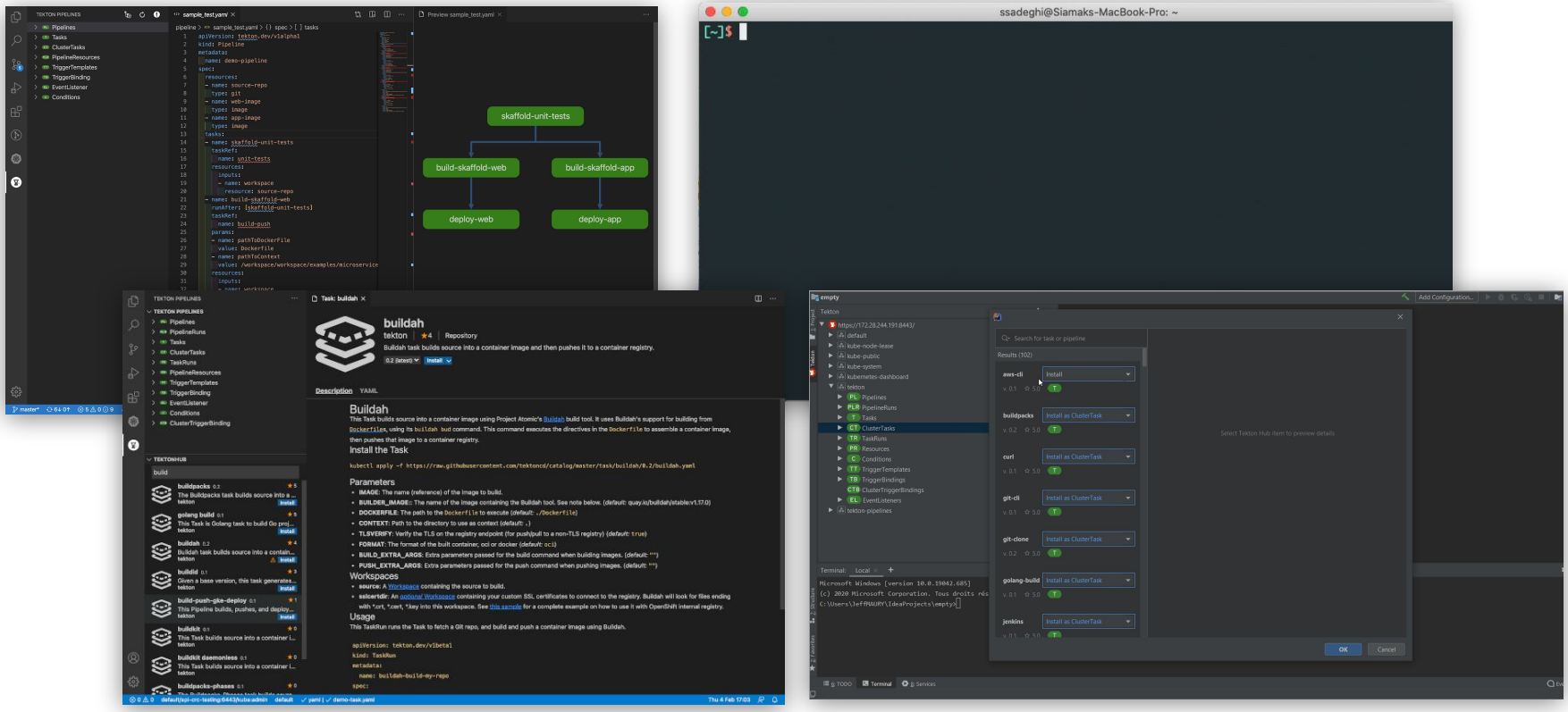
Tekton Concepts: `Pipeline`

- A graph of Tasks: concurrent & sequential
- Tasks run on different nodes
- Task execution logic
  - Conditional
  - Retries
- Share data between tasks

```yaml
kind: Pipeline
metadata:
 name: deploy-dev
spec:
 params:
   - name: IMAGE_TAG
 tasks:
   - name: git
     taskRef:
       name: git-clone
     params: [...]
   - name: build
     taskRef:
       name: maven
     params: [...]
     runAfter: ["git"]
   - name: deploy
     taskRef:
       name: knative-deploy
     params: [...]
     runAfter: ["build"]
```



Tekton CLI, Visual Studio Code, and IntelliJ



Red Hat

DEMO TIME

https://github.com/wpernath/openshift-cicd-demo

Red Hat

OpenShift GitOps

Declarative GitOps for multi-cluster continuous delivery

Red Hat

What is GitOps?

GitOps is when the infrastructure and / or application state is fully represented by the contents of a git repository. Any changes to the repository are reflected in the corresponding state of the associated infrastructure and applications through automation

GitOps is a natural evolution of Agile and DevOps (and Kubernetes) methodologies

Why GitOps

It takes too long to provision a new environment!

The app behaves different in prod than in test!

Environments are all manually configured!!!

Production deployments have a low success rate!

I have no visibility or record of config changes in deployments!

I can't audit config changes!!

I can't easily rollback changes to a specific version

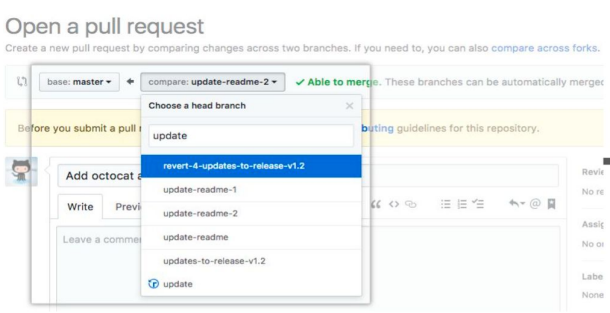
GitOps Benefits

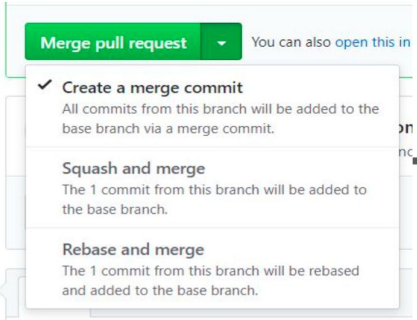
- All changes are auditable
- Standard roll-forward or backwards in the event of failure
- Disaster recovery is “reapply the current state of the manifests”
- Experience is “pushes and pull-requests”

OpenShift and GitOps - A great match

- OpenShift is a declarative environment
  - Cluster configuration is declared and Operators make it happen
  - Application deployments are declared and Kubernetes scheduler makes it happen
- GitOps in traditional environments requires automation/scripting, declarative environment minimizes or eliminates this need
- Declarations are yaml files which are easily stored and managed in git

Day 2 operations: All changes triggered from Git





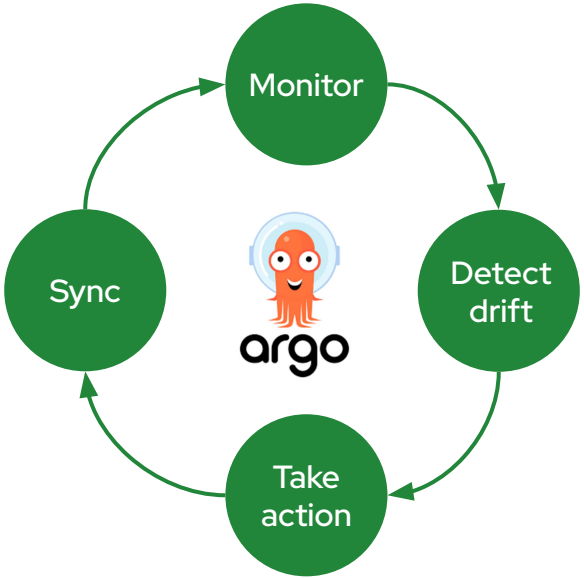

```
$ tkn pipelinerun logs update-from-master-run-g6s45

[run-kubectl] {"level":"info","ts":1580989837.3045664,"logger":"fallback-
logger","caller":"logging/config.go:69","msg":"Fetch GitHub commit ID from kodata failed:
\"KO_DATA_PATH\" does not exist or is empty"}
[run-kubectl] serviceaccount/demo-sa unchanged
[run-kubectl] clusterrolebinding.rbac.authorization.k8s.io/tekton-triggers-openshift-binding unchanged
[run-kubectl] eventlistener.tekton.dev/demo-event-listener configured
[run-kubectl] task.tekton.dev/deploy-from-source-task configured
[run-kubectl] triggerbinding.tekton.dev/update-from-master-binding unchanged
[run-kubectl] triggertemplate.tekton.dev/update-from-master-template unchanged
```

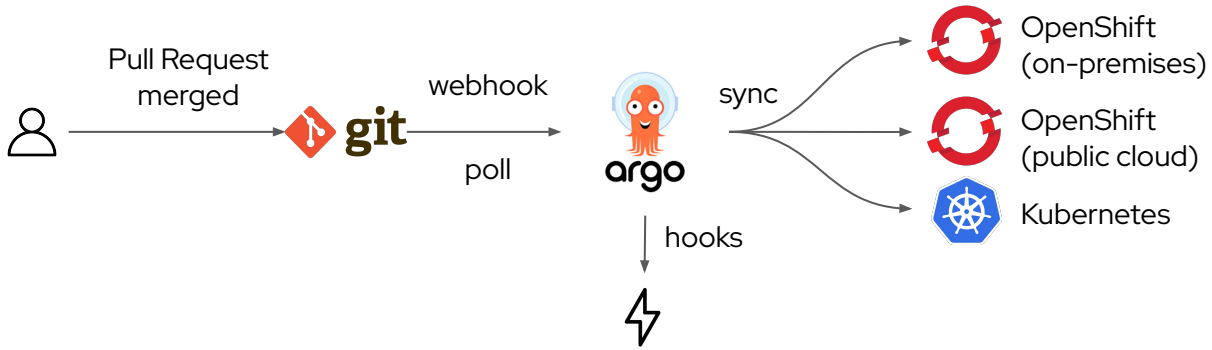
Red Hat

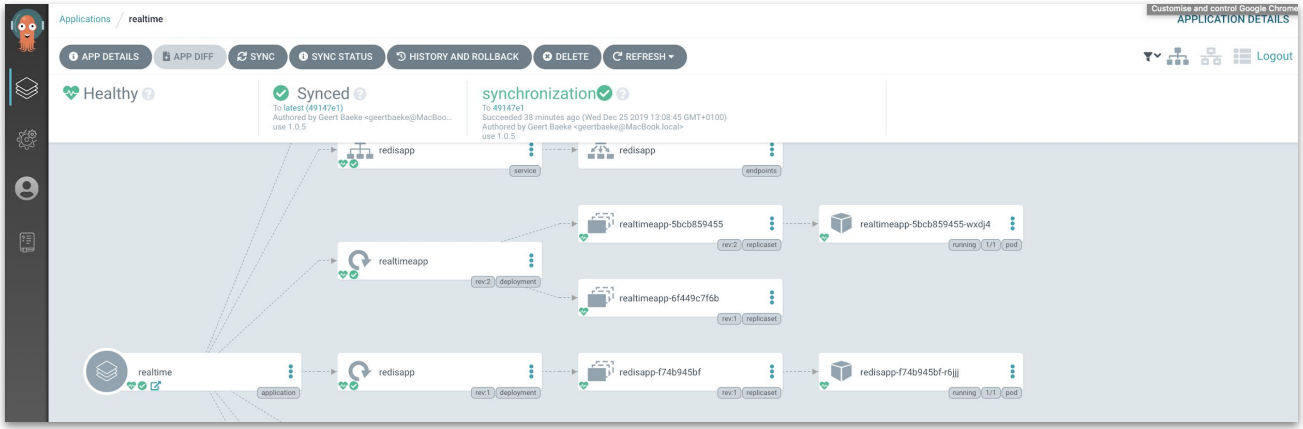
Argo CD

- Cluster and application configuration versioned in Git
- Automatically syncs configuration from Git to clusters
- Drift detection, visualization and correction
- Granular control over sync order for complex rollouts
- Rollback and rollforward to any Git commit
- Manifest templating support (Helm, Kustomize, etc)
- Visual insight into sync status and history



Argo CD

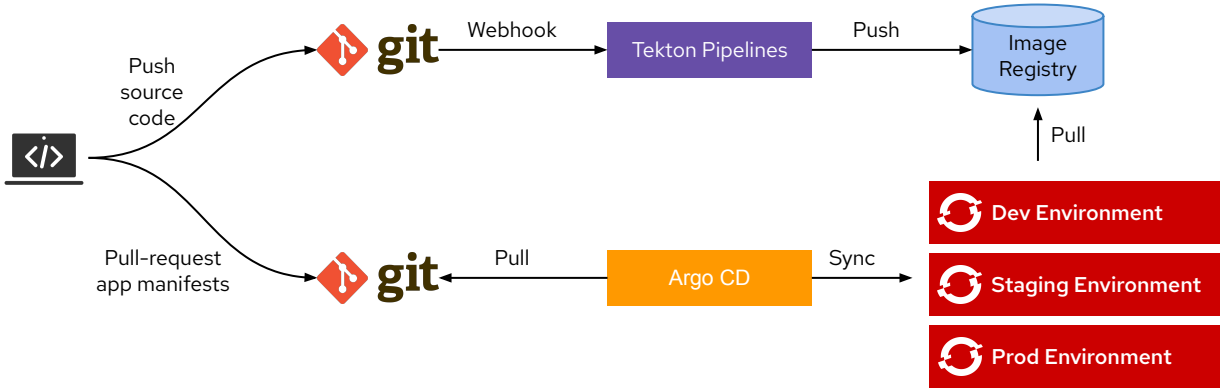




Red Hat

GitOps Application Manager CLI

```
$ kam bootstrap
```



Red Hat

OpenShift GitOps

Multi-cluster config management

Declaratively manage cluster and application configurations across multi-cluster OpenShift and Kubernetes infrastructure with Argo CD

Automated Argo CD install and upgrade

Automated install, configurations and upgrade of Argo CD through OperatorHub

Opinionated GitOps bootstrapping

Bootstrap end-to-end GitOps workflows for application delivery using Argo CD and Tekton with GitOps Application Manager CLI

Deployments and environments insights

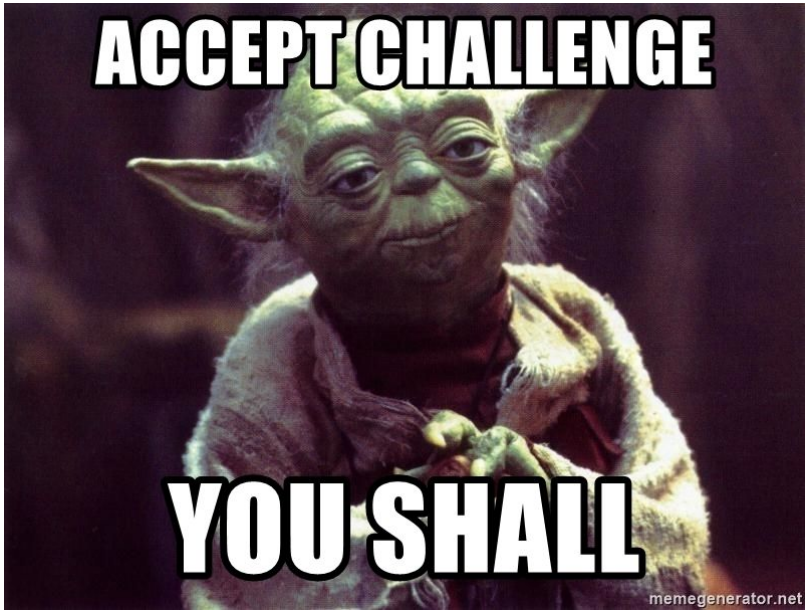
Visibility into application deployments across environments and the history of deployments in the OpenShift Console

Powered by argo

Red Hat

ArgoCD - Challenges

- Repo structure for manifests
  - One Repo or
  - Separate Repos for environments
- Order dependent deployments
- Non-declarative deployments
- Integration with CI/CD tools (Jenkins, Pipelines...)
  - Who does manage deployments?



Multiple repositories

/taxi.git

- deploy
- pipelines
- pkg/cmd/booktaxi
- web
- Dockerfile

/taxi-config-**stage**.git

- deploy
- pipelines
- README.md

/taxi-config-**prod**.git

- deploy
- pipelines
- README.md

/taxi-config-**test**.git

- deploy
- pipelines
- README.md

/taxi-config-**dev**.git

- deploy
- pipelines
- README.md

Single Repository

```
├── apps
│   └── app-1
│       ├── base
│       │   └── kustomization.yaml
│       └── dev
│           ├── deployment.yaml
│           └── kustomization.yaml
├── envs
│   ├── base
│   │   ├── 205-serviceaccount.yaml
│   │   └── kustomization.yaml
│   └── dev
│       └── kustomization.yaml
└── services
    └── service-a
        ├── base
        │   ├── config
        │   │   ├── 300-deployment.yaml
        │   │   ├── 310-service.yaml
        │   │   └── kustomization.yaml
        │   └── kustomization.yaml
        └── dev
            ├── dev-deployment.yaml
            ├── dev-service.yaml
            └── kustomization.yaml
```

```
├── base
│   ├── deployment.yaml
│   ├── kustomization.yaml
│   └── service.yaml
└── overlays
    ├── development
    │   ├── kustomization.yaml
    │   └── replicas.yaml
    ├── production
    │   ├── kustomization.yaml
    │   ├── replicas.yaml
    │   └── volumes.yaml
    └── staging
        ├── kustomization.yaml
        └── volumes.yaml
```

```
├── 00-tekton
│   ├── release.notags.yaml
│   └── release.yaml
├── 01-namespaces
│   ├── cicd-environment.yaml
│   ├── dev-environment.yaml
│   └── stage-environment.yaml
├── 02-serviceaccount
│   ├── demo-sa-admin-dev.rolebinding.yaml
│   ├── demo-sa-admin-stage.rolebinding.yaml
│   ├── role-binding.yaml
│   ├── role.yaml
│   └── serviceaccount.yaml
├── 03-tasks
│   ├── buildah-task.yaml
│   ├── create-github-status-task.yaml
│   ├── deploy-from-source-task.yaml
│   └── deploy-using-kubectl-task.yaml
├── 04-templatesandbindings
│   ├── dev-cd-deploy-from-master-binding.yaml
│   ├── dev-cd-deploy-from-master-template.yaml
│   ├── dev-ci-build-from-pr-binding.yaml
│   ├── dev-ci-build-from-pr-template.yaml
│   ├── stage-cd-deploy-from-push-binding.yaml
│   ├── stage-cd-deploy-from-push-template.yaml
│   ├── stage-ci-dryrun-from-pr-binding.yaml
│   └── stage-ci-dryrun-from-pr-template.yaml
├── 05-ci
│   ├── dev-ci-pipeline.yaml
│   └── stage-ci-pipeline.yaml
├── 06-cd
│   ├── dev-cd-pipeline.yaml
│   └── stage-cd-pipeline.yaml
├── 07-eventlisteners
│   └── cicd-event-listener.yaml
└── 08-routes
    └── github-webhook-event-listener.yaml
```

ArgoCD - Order Dependent Deployments

- Sometimes you have cases where you need to deploy things in a specific order
  - Subscribe Operator before deploying instance
  - Create namespace before deploying app into it
  - Deploy required infrastructure before application
- Tools like kustomize and Helm might help handling this in some cases
- ArgoCD provides Sync Phases and Waves to address other use cases
  - 3 sync phases - Pre-sync, sync, post-sync
  - Each phase can have multiple waves, next wave does not proceed until previous phase is healthy

ArgoCD - Non-declarative requirements

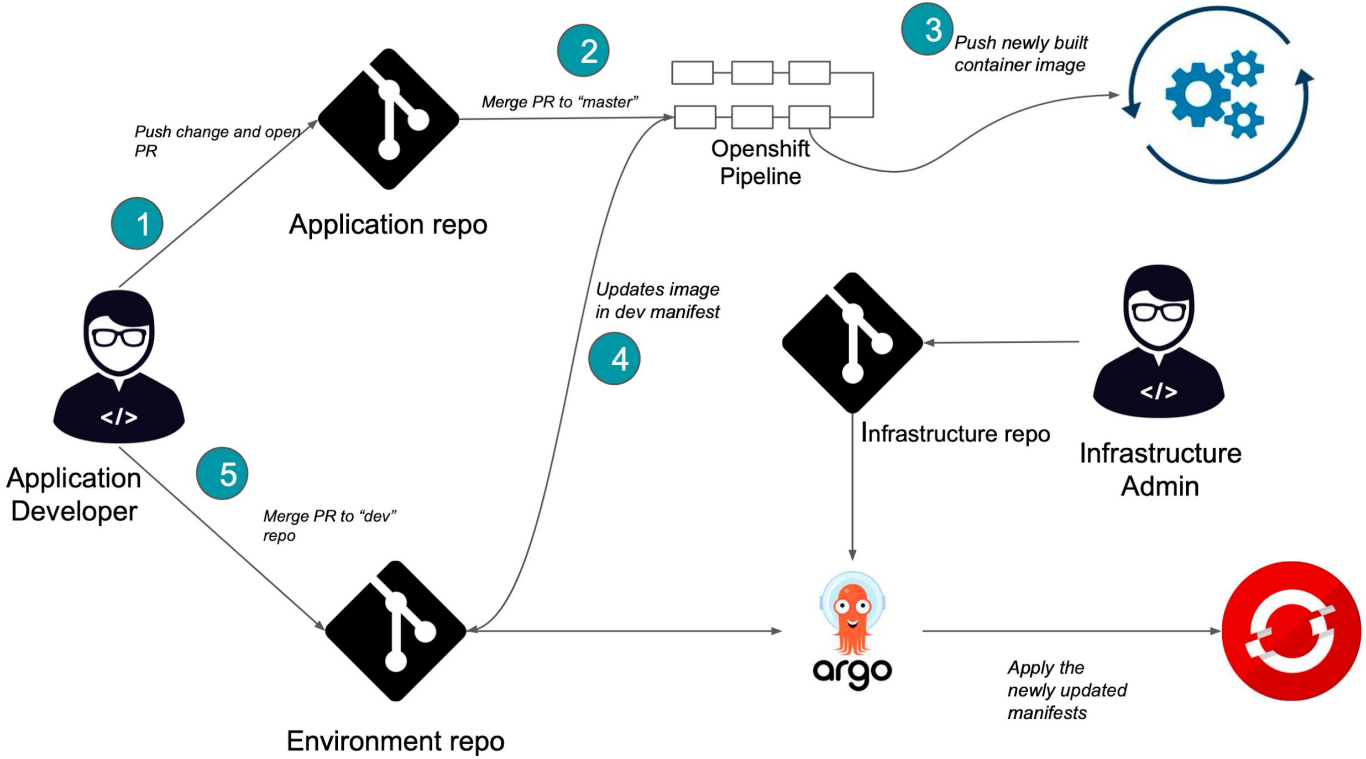
- There can be instances where you need to deploy something which cannot fully be done in a declarative way and it must be scripted
- Try minimizing this and leverage kubernetes primitives where possible
  - Init Containers
  - Jobs
  - Operators
- ArgoCD Resource Hooks
  - Hooks are ways to run scripts before, during and after a sync operation
  - Hooks can be run: PreSync, Sync, PostSync and SyncFail

ArgoCD - Integrating with CI/CD Tools

ArgoCD and NOT ArgoCI/CD

CI tools like Jenkins, Pipelines still required!

	ArgoCD Managed Deployment	Pipeline Managed Deployment
Pro	Consistent	Post-Test update of image reference
Con	Image reference updated in git before integration tests, manage rollback?	Inconsistent
Con	Pipeline tools must be able to wait for sync	


1
Push change and open PR
Application repo
2
Merge PR to "master"
Openshift Pipeline
3
Push newly built container image
Application Developer
5
Merge PR to "dev" repo
Environment repo
4
Updates image in dev manifest
Infrastructure repo
Infrastructure Admin
argo
Apply the newly updated manifests

DEMO TIME

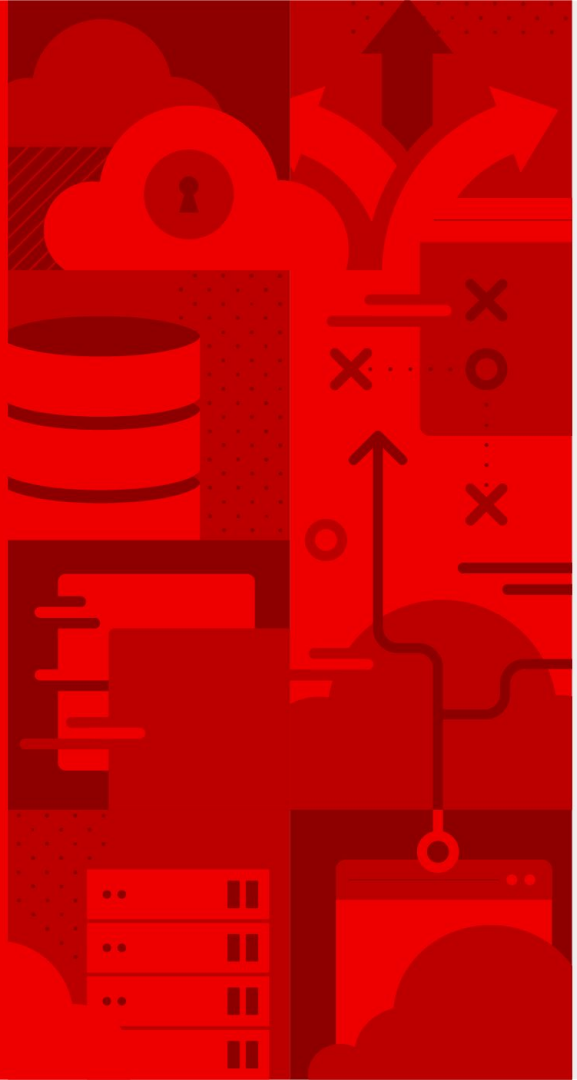
https://github.com/wpernath/openshift-cicd-demo

Red Hat

Summary

Summary

- You don’t have to change anything, if you don’t want
- You can use tools like Jenkins to do your CI
- OpenShift Builds is to integrate building your image in your existing pipeline
- OpenShift Pipelines (tekton) is a nice kubernetes-native way of pipelining
- GitOps and ArgoCD helps you to do a declarative approach
    - You as developer are used to use Git
    - You as admin are used to use Git
    - → Adoption of GitOps could be high



Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat