Let Your Software Supply Chain Ride with Kubernetes CI/CD

Ricardo Aravena

@raravena80

LISA 19

Who Am I?

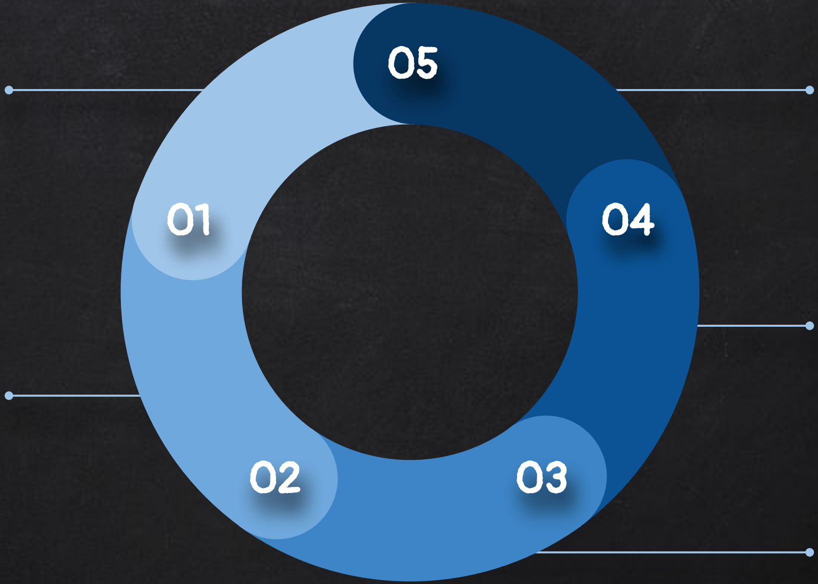
Ricardo Aravena (rico)

Work @Rakuten

Cloud Operations & Kubernetes

Kata Containers Contributor

K8s & CI/CD & GitOps @ Rakuten



Where?
Almost everywhere

K8s in prod
~1 year
Multiple services

CI/CD
Jenkins

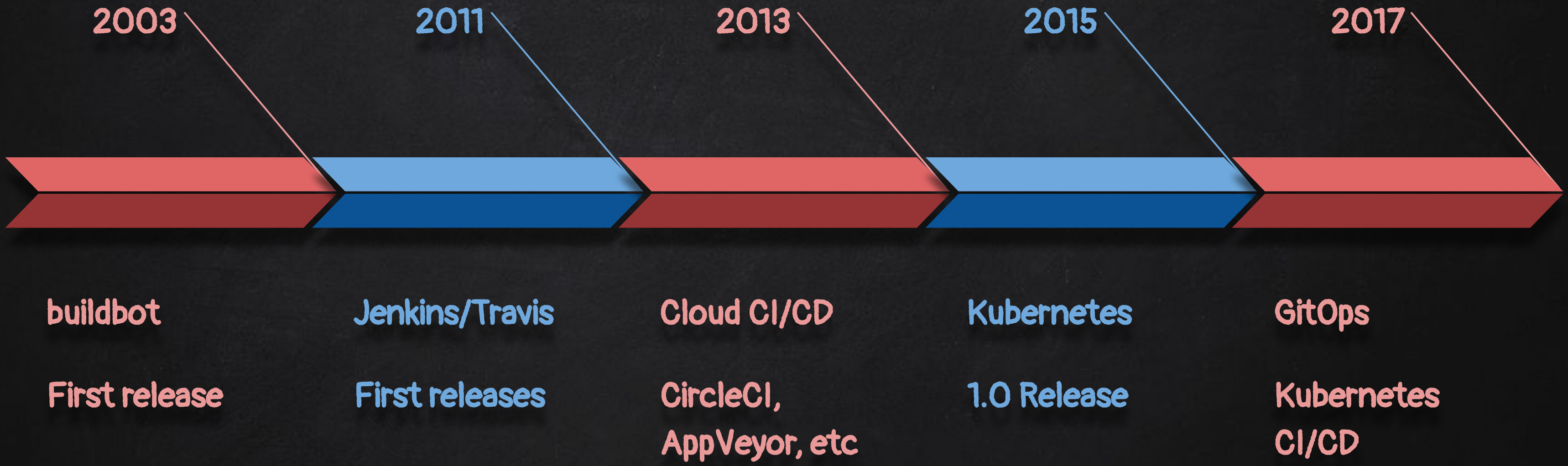
Tools
Flux/Helm
Terraform

DBs and Big Data
Standalone

Outline

- ✗ CI/CD History and Why GitOps?
- ✗ Tools and Security
  - ✗ Developer -> Draft, Flux, Others
  - ✗ Image Building -> Buildkit, Bazel
  - ✗ Templating -> Helm, Kustomize
  - ✗ Specifically Sec -> Notary, TUF, Trivy
- ✗ CI/CD -> JenkinsX, Tekton
- ✗ GitOps Future
- ✗ Takeaways

CI/CD History



2003

buildbot

First release

2011

Jenkins/Travis

First releases

2013

Cloud CI/CD

CircleCI,
AppVeyor, etc

2015

Kubernetes

1.0 Release

2017

GitOps

Kubernetes
CI/CD

Why GitOps?

Version Control

Both Infra & Code

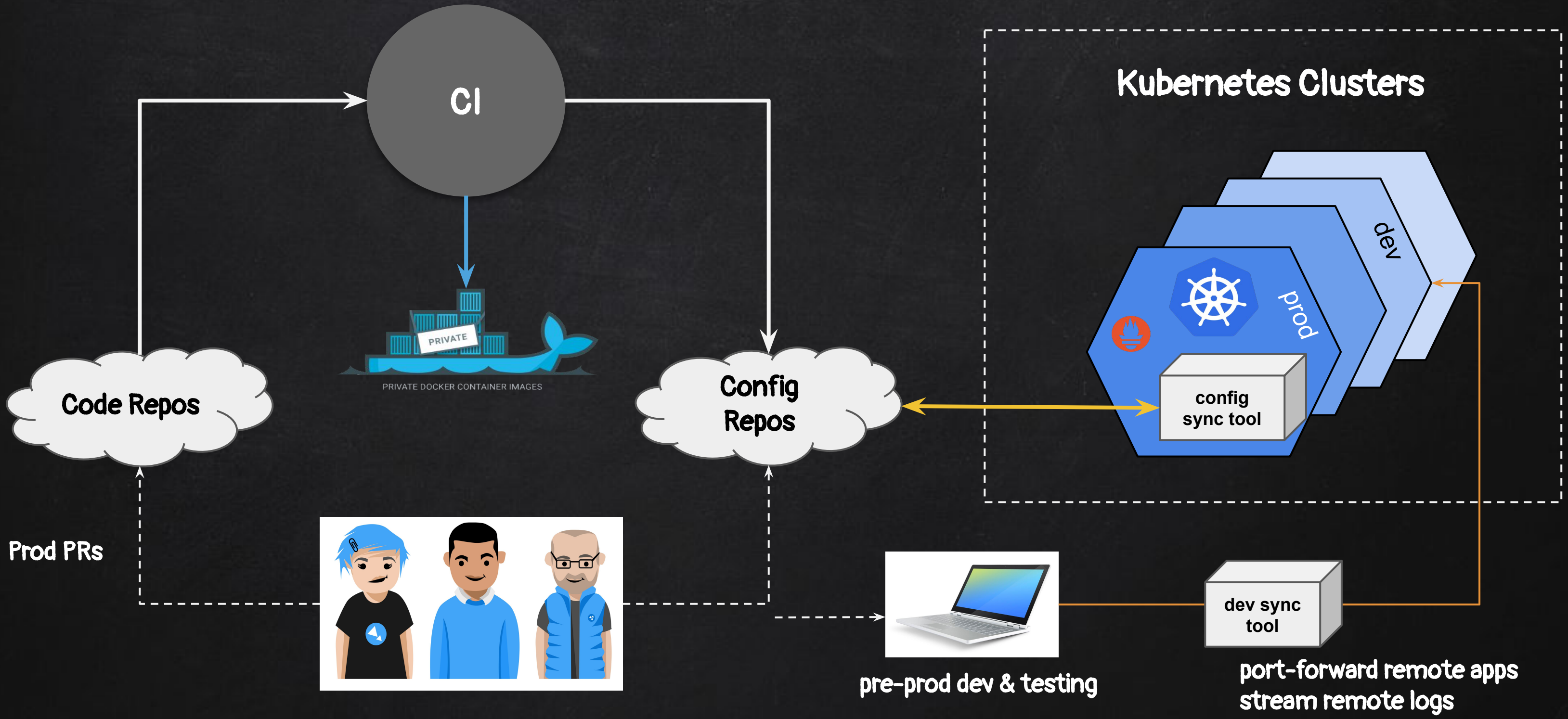
Use a tool

Compare current state to desired state

Automate Deployments

Gain reversibility, have an audit trail and transparency

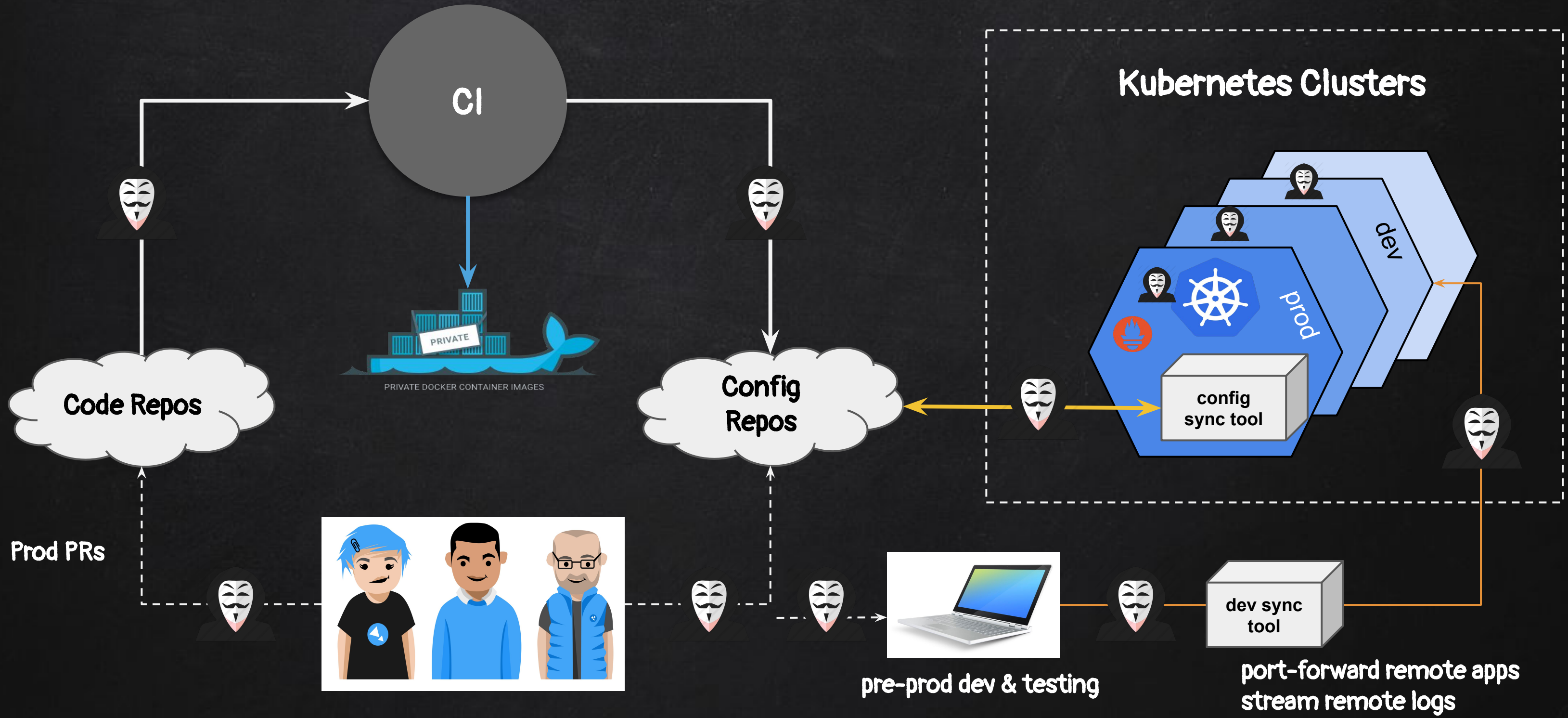
GitOps Infra



Why Care About Security?

@raravena80

GitOps Infra &



CI

PRIVATE

PRIVATE DOCKER CONTAINER IMAGES

Code Repos

Config Repos

Kubernetes Clusters

dev

prod

config sync tool

Prod PRs

pre-prod dev & testing

dev sync tool

port-forward remote apps
stream remote logs

@raravena80

GitOps Vulnerabilities

- ✗ Package dependencies in OSS
  - ✗ Glibc, Bash -> Shellshock
- ✗ Container backdoors
  - ✗ CVE-2019-5736: runc container breakout
- ✗ Fake downloads or typosquatting
  - ✗ Trojans
- ✗ Kubernetes
  - ✗ CVE-2018-1002105 - Privilege escalation
- ✗ Tools
  - ✗ Developer, image building, CI/CD

GitOps Developer Tools & Security

@raravena80

Draft

Who?	✗	MS Open Source
What?	✗	App development and deployment
How?	✗	Draft packs/cli
Local and Remote mgmt	✗	Yes – 'draft up/connect'

Draft Languages

- Clojure
- C#
- Erlang
- Go
- Java
- Python
- Gradle
- Javascript
- PHP
- Ruby
- Rust
- Swift

Draft Languages &

Draft

Pros

- Local development
- Uses git and its auth model
- Integrated docker image builder
- Support: active community

Cons

- Supports many languages
  - Security con
- Requires tiller -- Helm v2
- 0.16.x experimental release
- No native RBAC

Flux

Who?	✗ Weaveworks
What?	✗ App Deployment
How?	✗ git push ✗ fluxctl cmd
Local and remote mgmt	✗ git for local ✗ fluxctl for remote

Flux

Pros

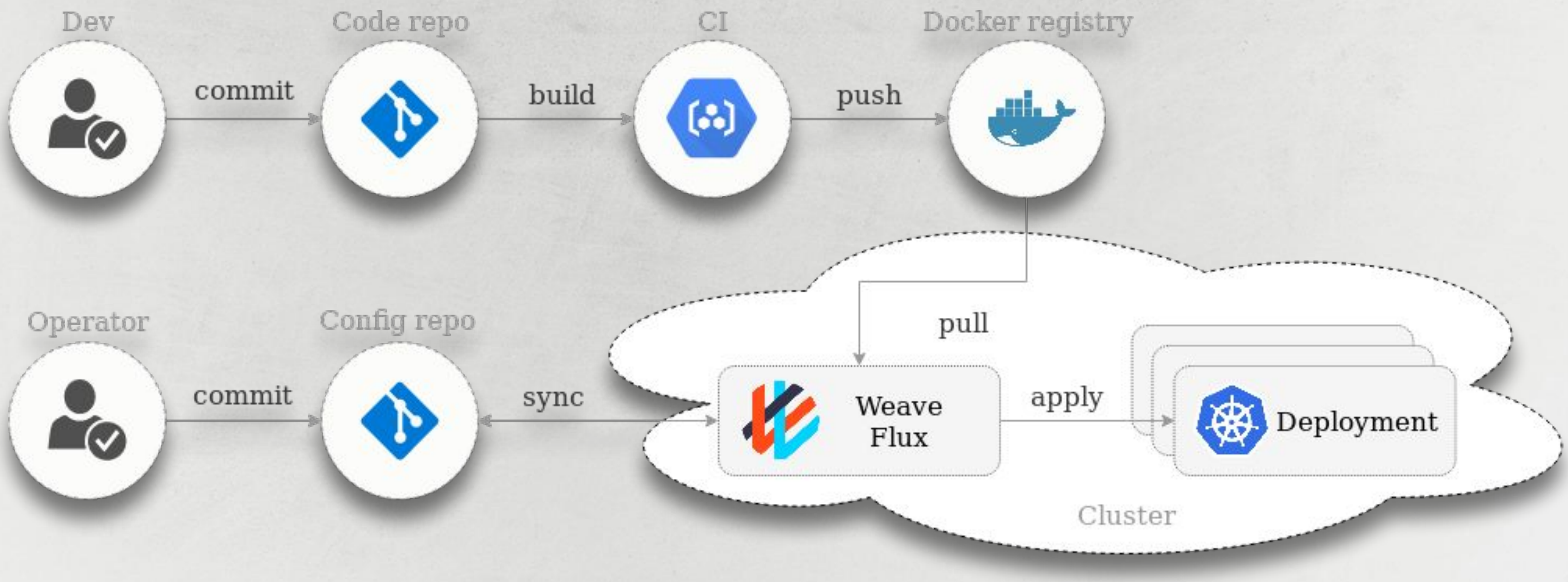
- ✗ Has its own controller and CRD
- ✗ Leverages git auth
- ✗ Mature 1.15.x release
- ✗ Support: active community

Cons

- ✗ No native RBAC
- ✗ Flux container image needs signing
- ✗ Automatic sync could be exposed to MIM
- ✗ No local development

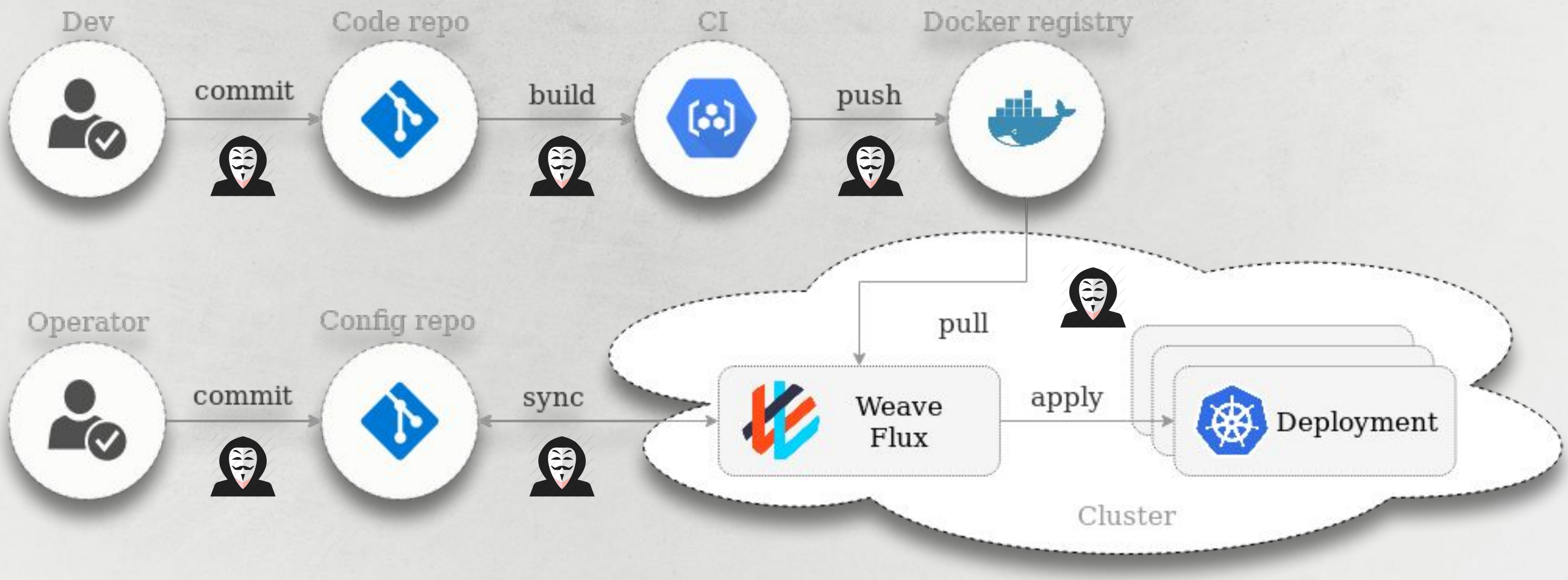
https://github.com/fluxcd/flux

Flux



https://github.com/fluxcd/flux

Flux &



@raravena80

https://github.com/fluxcd/flux

Other GitOps Developer Tools

- Skaffold
- garden
- gitkube
- DevSpace
- Tilt

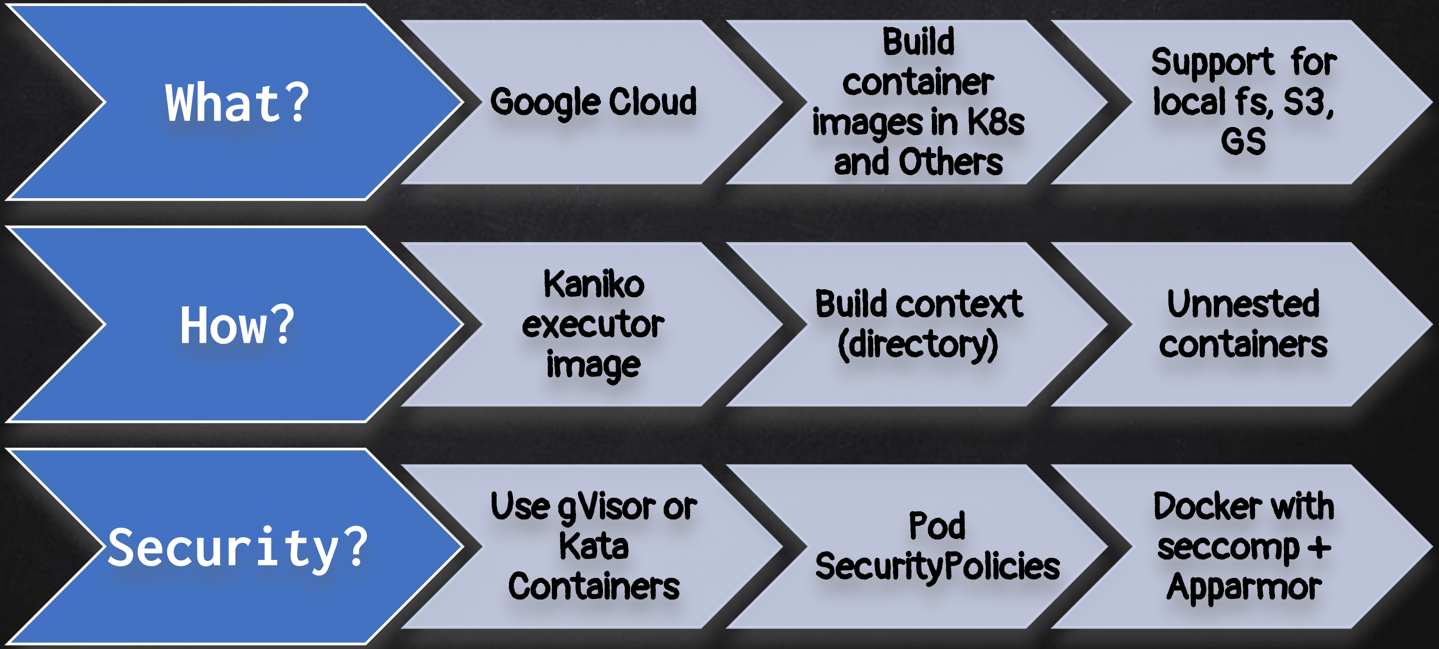
https://github.com/ramitsurana/awesome-kubernetes#developer-platform

Help!

@raravena80

Image Building Tools

Kaniko

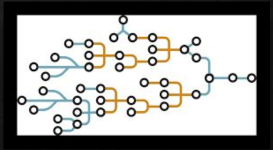


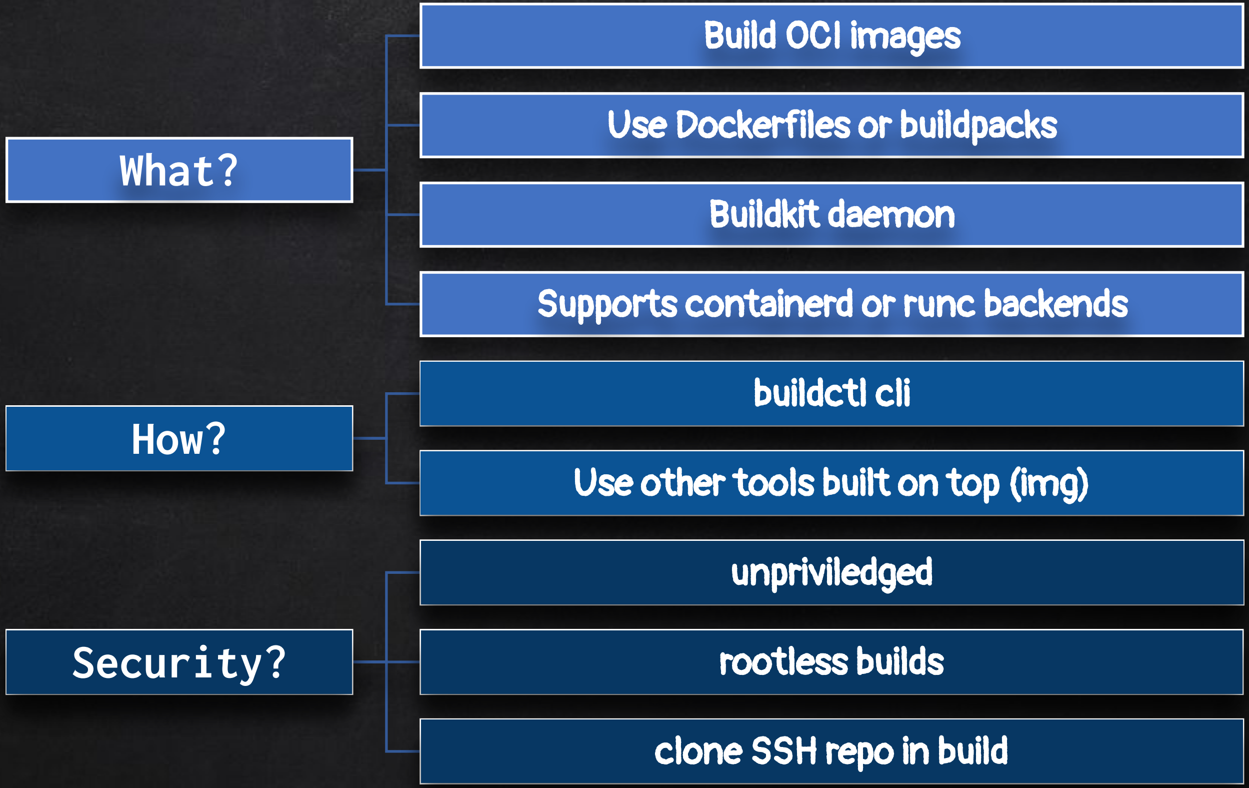
What? → Google Cloud → Build container images in K8s and Others → Support for local fs, S3, GS

How? → Kaniko executor image → Build context (directory) → Unnested containers

Security? → Use gVisor or Kata Containers → Pod SecurityPolicies → Docker with seccomp + Apparmor

BuildKit





What?

- Build OCI images
- Use Dockerfiles or buildpacks
- Buildkit daemon
- Supports containerd or runc backends

How?

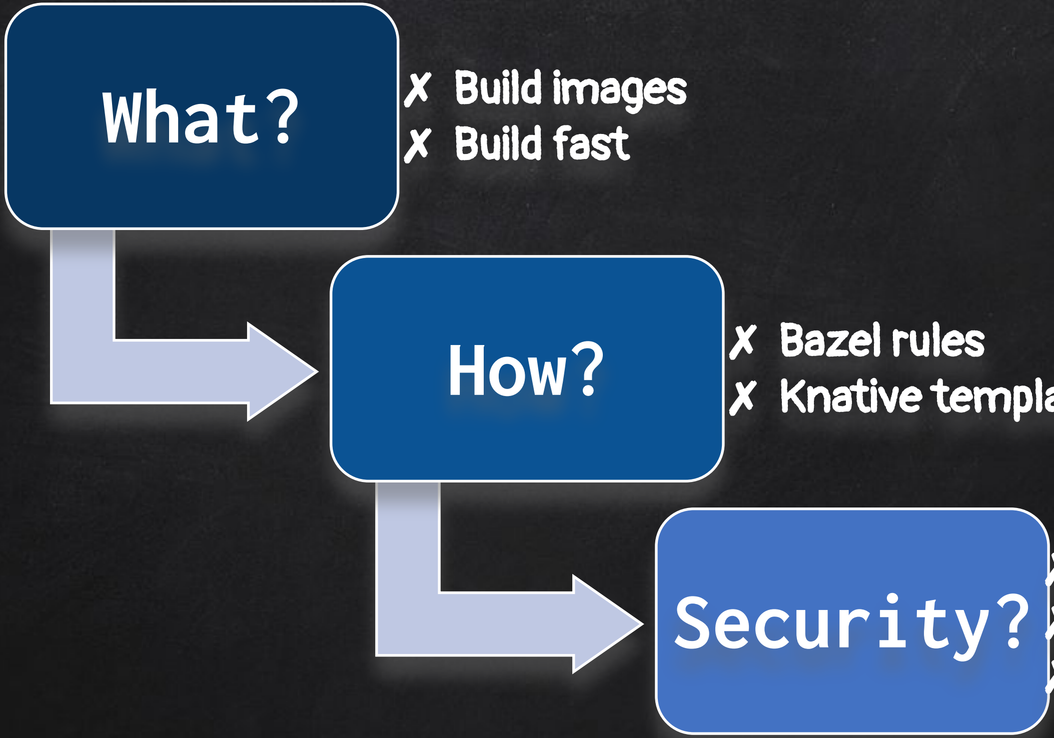
- buildctl cli
- Use other tools built on top (img)

Security?

- unpriviledged
- rootless builds
- clone SSH repo in build

https://github.com/moby/buildkit

Bazel



✗ Build images
✗ Build fast

✗ Bazel rules
✗ Knative templates

✗ Deterministic
✗ Reproducible
✗ Unprivileged

Other Build Tools

- kpack/buildpacks
- buildah
- img
- Knative Build
- Umoci/Orca

Templating tools

Helm

HELM

What?

✗ Manage packages for K8s clusters
✗ Go templating
✗ Extendable w/Lua (v3)

How?

✗ Helm CLI
✗ Tiller (v2) Going away with v3
✗ Helm charts

Security?

✗ SSL
✗ Other mechanism for secrets
✗ No security per se (helps with workflow)
✗ Tie together with other tools

Kustomize

What?	Change existing k8s manifests
	Leaves original YAML untouched
How?	kustomize.yaml
	kustomize cli
	Many fields to change k8s manifests
	Supported by Flux
Security?	Leverages kubectl v1.14 security
	Provides secret generator

Security Tools

@raravena80

TUF/Notary

- ✗ Moby/Docker

Who?

- ✗ TUF
  - ✗ Standard
- ✗ Notary
  - ✗ Metadata signatures
- ✗ Allows delegation

What?

- ✗ Client/Server
- ✗ Signer service
- ✗ Add to CI/CD
- ✗ Publishers can sign content offline

How?

Trivy

Who?

- ✗ Aqua Security

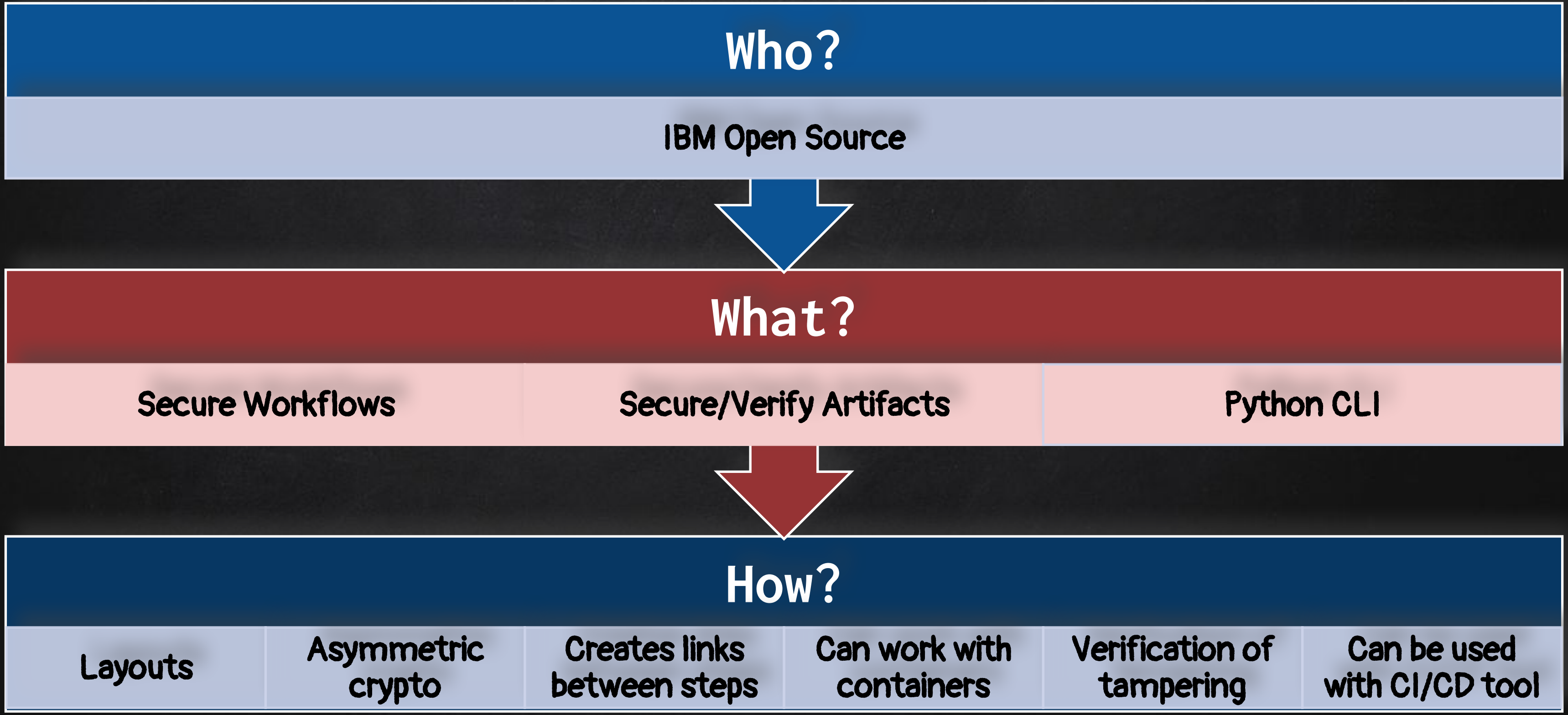
What?

- ✗ Container image scanning
- ✗ Application audit
- ✗ Policy enforcement

How?

- ✗ Trivy cli
- ✗ Using tar or local docker container
- ✗ Using CI/CD tool

IN-TOTO



Who?

IBM Open Source

What?

Secure Workflows	Secure/Verify Artifacts	Python CLI

How?

Layouts	Asymmetric crypto	Creates links between steps	Can work with containers	Verification of tampering	Can be used with CI/CD tool

Other Security Tools

- Falco - Container Activity Monitor
- Harbor - Secure registry (Notary)
- Anchore, Aqua, Clair, Dagda - Image scanning
- Grafeas - Signing
- Kritis, Portieris - Admission Controller
- Kube hunter - K8s Vulnerabilities
- Open Policy Agent - Config enforcer
- Trireme - Netpol mgmt
- Image encryption - Encrypt cont imgs
- Tern, Snyk - Package Compliance

CI/CD Tools

@raravena80

JenkinsX

What?

- Jenkins
- Nexus
- Draft
- ChartMuseum (Helm)
- Monocular (Chart disc)
- Skaffold

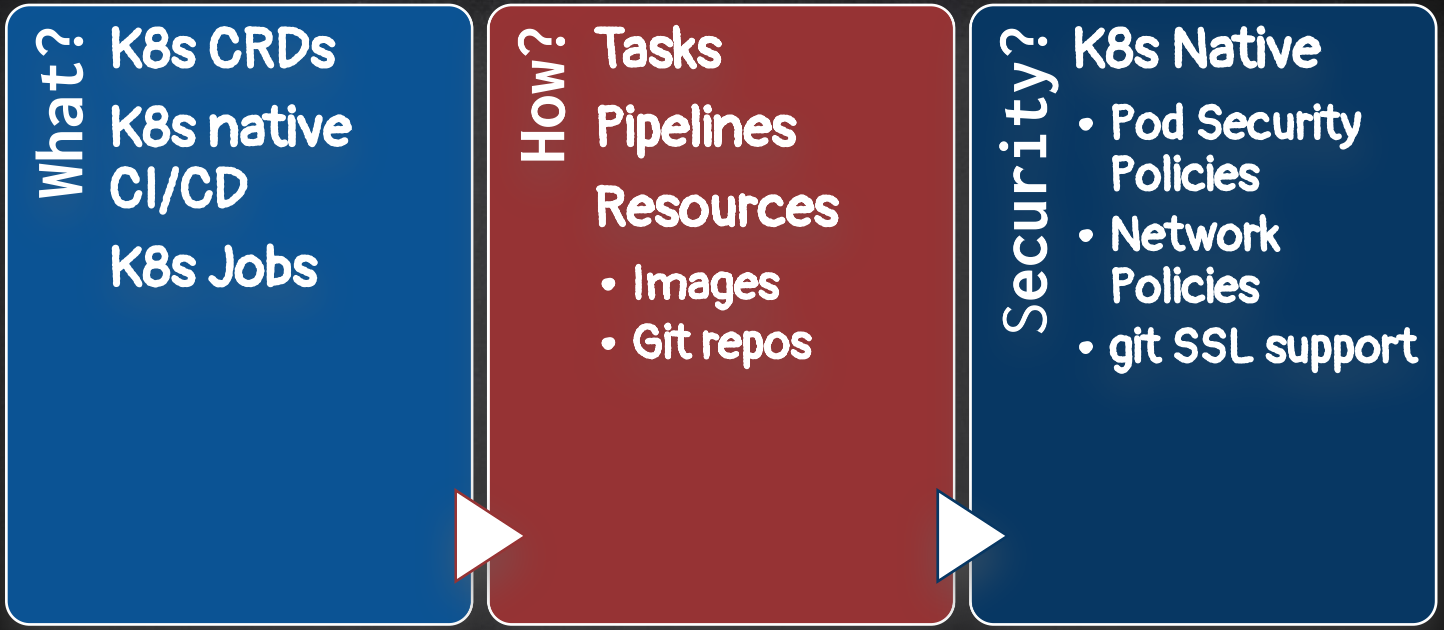
How?

- jx command line
- jenkins-x.yml file for pipelines
- Leverages draft to manage code
- Skaffold to build and push images

Security?

- Auto upgrade w/GitOps and Tekton
- Jenkins built in sec

Tekton



What?

K8s CRDs

K8s native CI/CD

K8s Jobs

How?

Tasks

Pipelines

Resources

- Images
- Git repos

Security?

K8s Native

- Pod Security Policies
- Network Policies
- git SSL support

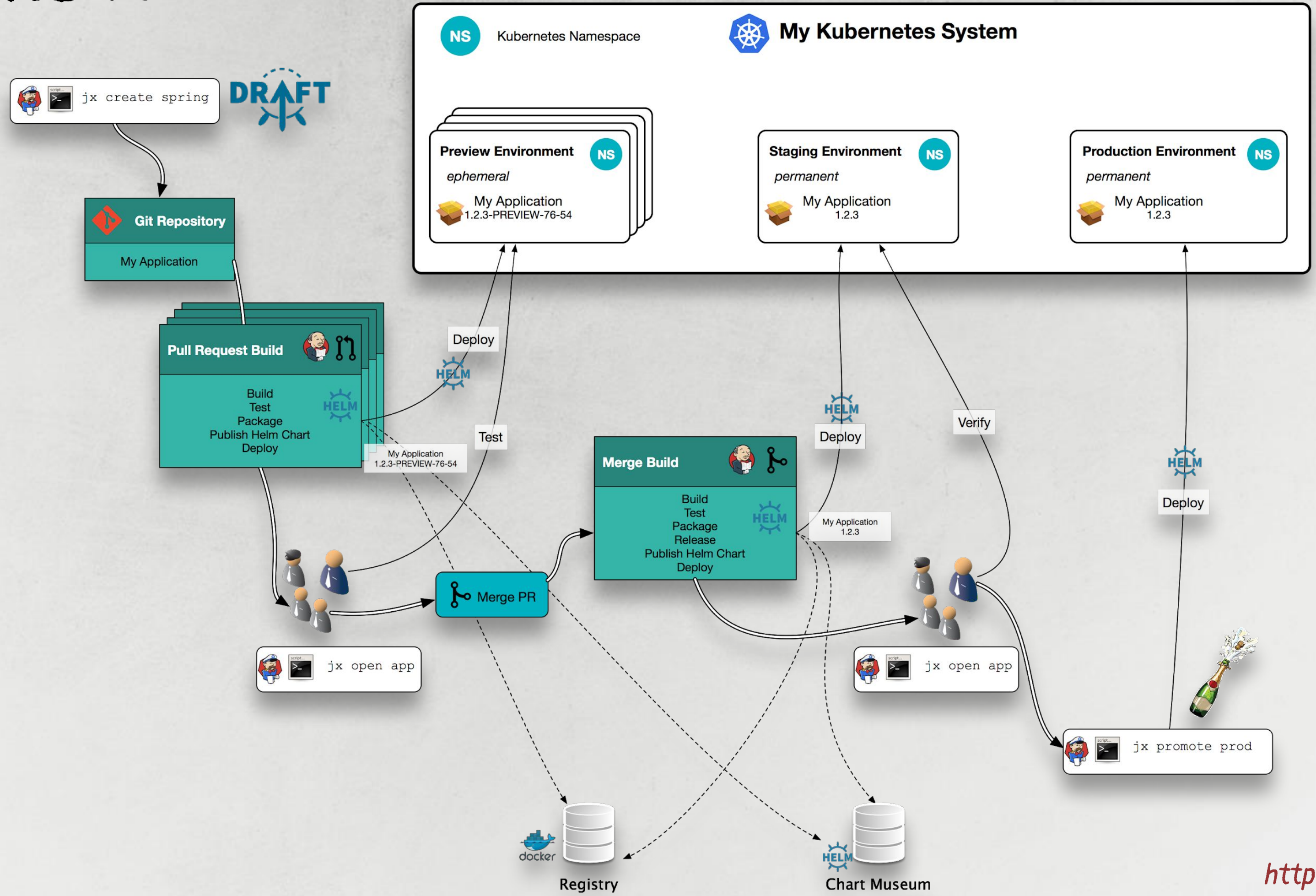
Other CI/CD Tools

- Spinnaker
- Argo CD
- Drone CI
- GoCD
- Gitlab
- TeamCity
- Screwdriver CD
- Rundeck
- Habitat

Secure Software Supply Chain

@raravena80

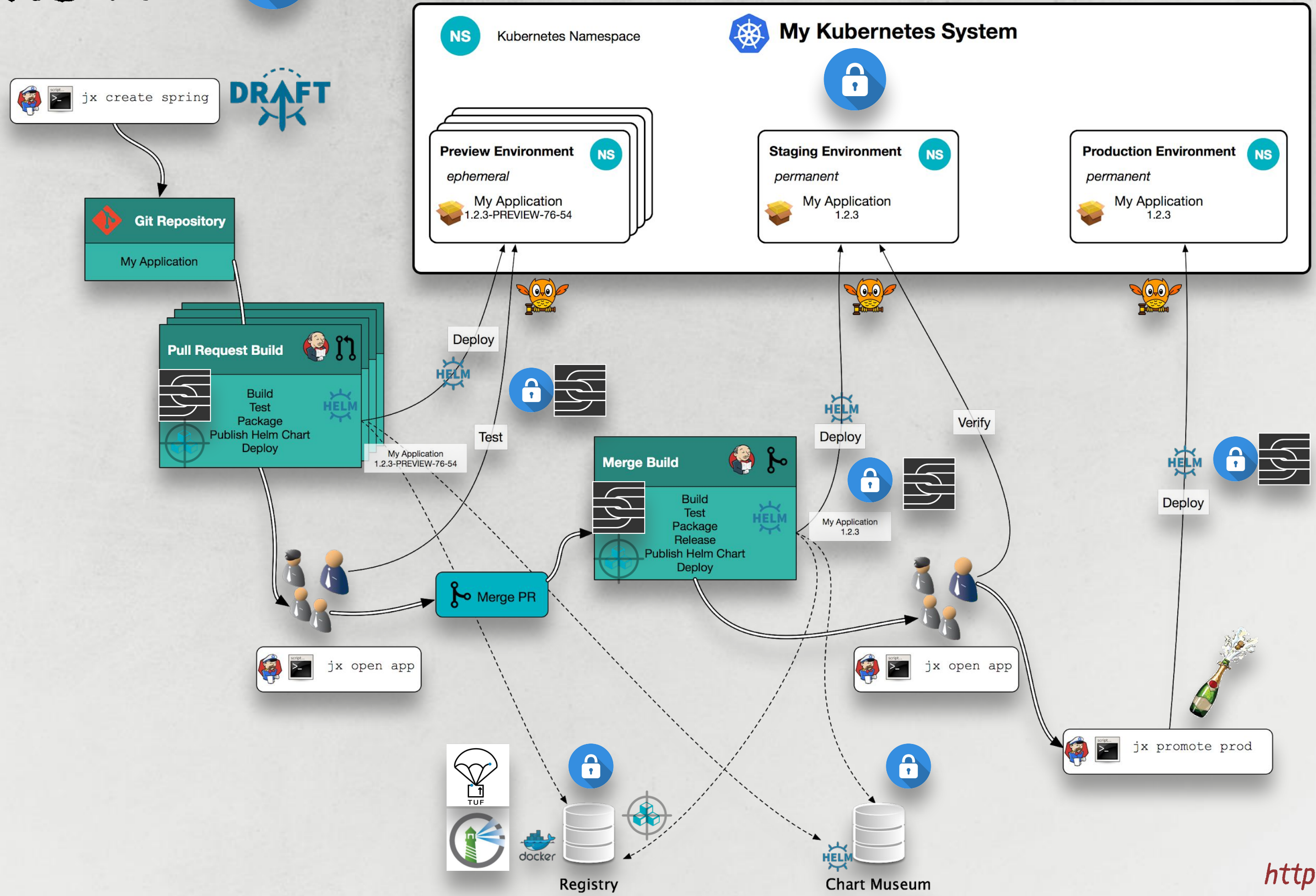
Jenkins X



@raravena80

https://jenkins-x.io/

Jenkins X +



@raravena80

https://jenkins-x.io/

GitOps Future

GitOps Future…

- ✗ GitOps tools self updates
  - ✗ Ie. Devs can't build if Draft/Flux not up to date
- ✗ Container runtime support
  - ✗ Kata, gVisor for GitOps and image building
  - ✗ GitOps with Ignite and VMs
- ✗ New configuration languages. I.e Dhall, Cue
- ✗ Integration with Open Policy Agent
  - ✗ K8s admission (Gatekeeper) + Uniform configs
- ✗ GitOps for Kubernetes cluster management
- ✗ Integrations, integrations and integrations

Takeaways

Takeaways...

□ **Separate environments**

- ✗ Dev, QA, Stage, Prod

□ **Security first!**

□ **runc**

- ✗ Patch regularly!!
- ✗ Use seccomp profiles

□ **Alternatively use Kata, or gVisor for pipelines**

- ✗ Check performance and compatibilities

□ **Always use unprivileged to build cont. images**

- ✗ Use rootless with BuildKit for extra security

https://sysdig.com/blog/33-kubernetes-security-tools/

Takeaways...

- □ Use GitOps CI/CD Tool to upgrade packages
  - ✗ Container packages and tools themselves
- □ Leverage in-toto (or Grafeas, Notary)
- □ Scan your images - Trivy/Anchore/Claire/Dagda
- □ Use K8s mechanisms
  - ✗ Admission ctrl (Kritis/Portieris), Authentication w/RBAC
- □ Configure Network Policies in K8s
  - ✗ Trireme, or overlay

https://sysdig.com/blog/33-kubernetes-security-tools/

Resources

- GitOps
  - https://www.weave.works/technologies/gitops/
- Security
  - K8s Sec Tools
    https://sysdig.com/blog/33-kubernetes-security-tools/
  - Harbor https://github.com/goharbor/harbor
  - In-toto https://in-toto.github.io/
  - Trivy https://github.com/aquasecurity/trivy
- CI/CD
  - JenkinsX https://jenkins.io/projects/jenkins-x/
  - Tekton https://tekton.dev/
  - Spinnaker https://www.spinnaker.io/

Thanks!

You can find me at:

✘ @raravena80

✘ https://blog.serverbooter.com