It’s Time to Jump on The Secure GitOps Bandwagon

Ricardo Aravena
@raravena80
Open Source Summit North America
Who Am I?

Ricardo Aravena (rico)

Work @Rakuten
Cloud Operations & Kubernetes
Kata Containers Contributor
K8s & GitOps @ Rakuten

Where?
Almost everywhere

K8s in prod
~1 year
Multiple services

01
02
03
04
05

DBs and Big Data
Standalone

Tools
Flux/Helm/Terraform

CI/CD
Jenkins
Outline

✗ History and Why GitOps?
✗ Tools and Security
✗ Developer -> Draft, Flux, Others
✗ Image Building -> Buildkit, Bazel
✗ Templating -> Helm, Kustomize
✗ Specifically Sec -> Notary, TUF, Anchore
✗ CI/CD -> JenkinsX, Tekton, Spinnaker
✗ GitOps Security 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
  - Deploy to K8s
Version Control
Both Infra & Code

Use a tool
Compare current state to desired state

Why GitOps?

Automate Deployments
Gain reversibility, have an audit trail and transparency
GitOps Infra

- **Code Repos**
- **Config Repos**
- **CI**
- **Kubernetes Clusters**
  - prod
  - dev
- **Prod PRs**
- **pre-prod dev & testing**
- **prod sync tool**
- **dev sync tool**
- **port-forward remote apps stream remote logs**

- Prod sync tool
- Dev sync tool
GitOps Infra & Code Repos

CI

Kubernetes Clusters

Config Repos

Prod PRs

Config sync tool

pre-prod dev & testing

port-forward remote apps stream remote logs

dev sync tool
GitOps Vulnerabilities

✗ Package dependencies in OSS
✗ Shellshock
✗ Glibc
✗ Container backdoors
✗ CVE-2019-5736: runc container breakout
✗ Fake downloads or typosquatting
✗ Trojans
✗ CVE-2019-12735: Vim priv escalation
GitOps Vulnerabilities

✗ Kubernetes
  ✗ CVE-2018-1002105 - Privilege escalation
  ✗ CVE-2018-18264 - Dashboard vulnerability

✗ Tools
  ✗ Developer, image building, CI/CD
  ✗ CVE-2019-1003049 - Jenkins auth
GitOps Developer Tools
# Draft

<table>
<thead>
<tr>
<th>Who?</th>
<th>Who?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Open Source</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What?</th>
<th>What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>App development and deployment</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How?</th>
<th>How?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft packs/cli</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local and Remote mgmt</th>
<th>Local and Remote mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Draft Languages

<table>
<thead>
<tr>
<th>Clojure</th>
<th>Gradle</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td>Javascript</td>
</tr>
<tr>
<td>Erlang</td>
<td>PHP</td>
</tr>
<tr>
<td>Go</td>
<td>Ruby</td>
</tr>
<tr>
<td>Java</td>
<td>Rust</td>
</tr>
<tr>
<td>Python</td>
<td>Swift</td>
</tr>
</tbody>
</table>

[https://github.com/Azure/draft](https://github.com/Azure/draft)
Draft Languages &

C++
C#
Python
Java
JavaScript

@raravena80
https://github.com/Azure/draft
Security Pros
- Local development
- Uses git and its auth model
- Integrated docker image builder
- **Support**: active community

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

Draft

https://github.com/Azure/draft
## Flux

<table>
<thead>
<tr>
<th>Who?</th>
<th>✗ Weaveworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>What?</td>
<td>✗ App Deployment</td>
</tr>
<tr>
<td>How?</td>
<td>✗ git push</td>
</tr>
<tr>
<td></td>
<td>✗ fluxctl cmd</td>
</tr>
<tr>
<td>Local and remote mgmt</td>
<td>✗ git for local</td>
</tr>
<tr>
<td></td>
<td>✗ fluxctl for remote</td>
</tr>
</tbody>
</table>
Flux

Security Pros
- Has its own controller and CRD
- Leverages git auth
- Mature 1.13.x release
- **Support**: active community

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

https://github.com/fluxcd/flux
Other GitOps Developer Tools

- Skaffold
- garden
- gitkube
- DevSpace
- Tilt

https://github.com/ramitsurana/awesome-kubernetes#developer-platform
Help!
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 Security Policies
- Docker with seccomp + Apparmor

https://github.com/GoogleContainerTools/kaniko
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)
- unprivileged
- rootless builds
- clone SSH repo in build

Security?

https://github.com/moby/buildkit
Bazel

* What?
  - Build images
  - Build fast

* How?
  - Bazel rules
  - Knative templates

* Security?
  - Deterministic
  - Reproducible
  - Unprivileged

https://bazel.build
Templating Tools
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

https://helm.sh/
**Kustomize**

<table>
<thead>
<tr>
<th>What?</th>
<th>Change existing k8s manifests</th>
<th>Leaves original YAML untouched</th>
</tr>
</thead>
<tbody>
<tr>
<td>How?</td>
<td>kustomize.yaml</td>
<td>kustomize cli</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Many fields to change k8s manifests</td>
</tr>
<tr>
<td>Security?</td>
<td>Works with kubectl v1.14 or later</td>
<td>Leverages kubectl security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides secret generator</td>
</tr>
</tbody>
</table>

[https://github.com/kubernetes-sigs/kustomize/](https://github.com/kubernetes-sigs/kustomize/)
Security Tools
TUF/Notary

Who?

✗ Moby/Docker

What?

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

How?

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

Who?
- Anchore

What?
- Container image scanning
- Application audit
- Policy enforcement

How?
- Anchore engine
- Anchore image scanning worker
- Anchore cli

https://github.com/anchore/anchore-engine
in-toto

Who?
IBM Open Source

What?
Secure Workflows
Secure/Verify Artifacts
Python CLI

How?
<table>
<thead>
<tr>
<th>Layouts</th>
<th>Asymmetric crypto</th>
<th>Creates links between steps</th>
<th>Can work with containers</th>
<th>Verification of tampering</th>
<th>Can be used with CI/CD tool</th>
</tr>
</thead>
</table>

@raravena80
Other Security Tools

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

https://jenkins-x.io/
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

https://tekton.dev
Spinnaker

What?
- Igor (integ. w/Jenkins)
- Echo (event bus)
- Orca (orch engine)
- Front50 (metadata)
- Rosco -> Packer
- Kayenta -> Canary
- Clouddriver (AWS)
- Gate (API gate)

How?
- Run in K8s cluster
- Or Separately
- w/Halyard

Security?
- Built in SSL
- Use in-toto, image scanning, etc
- Fiat (auth)
- Built in public cloud interface

https://spinnaker.io
Other CI/CD Tools

- Argo CD
- Drone CI
- GoCD
- Gitlab
- TeamCity
- Screwdriver CD
- Rundeck
- Habitat
Secure Software Supply Chain
GitOps Sec Future
Security GitOps Future...

- GitOps tools self updates
- I.e. Devs can’t build if Draft/Flux not up to date
- Container runtime support
- Kata, gVisor for GitOps and image building
- Integration with Open Policy Agent
- Uniform configs
- Kubernetes admission
Takeaways
Takeaways...

- **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

- **Use GitOps CI/CD Tool to upgrade packages**
  - ✗ Container packages and tools themselves

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

- Leverage in-toto (or Grafeas, Notary)
- Scan your images - Aqua/Anchore/Claire/Dagda
- Sign your image metadata - in-toto, Notary, etc
- 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/
  ✗ Anchore https://github.com/anchore/anchore-engine

✗ 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.serverboooter.com
We are hiring!
Questions?