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

DBs and Big Data
Standalone

Tools
Flux/Helm
Terraform

CI/CD
Jenkins
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
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**
  - **config sync tool**
  - **pre-prod dev & testing**
  - **port-forward remote apps**
  - **stream remote logs**
- **Prod PRs**

@raravena80
Why Care About Security?
GitOps Infra & Code Repos

CI

Kubernetes Clusters

Config Repos

Prod PRs

pre-prod dev & testing

port-forward remote apps

stream remote logs

config sync tool

dev sync tool

dev

prod

dev sync tool

config sync tool
**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
## Draft

<table>
<thead>
<tr>
<th>Who?</th>
<th>MS Open Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>What?</td>
<td>App development and deployment</td>
</tr>
<tr>
<td>How?</td>
<td>Draft packs/cli</td>
</tr>
<tr>
<td>Local and Remote mgmt</td>
<td>Yes - ‘draft up/connect’</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>

[@raravena80](https://github.com/Azure/draft)
Draft Languages &

- Go
- Groovy
- C#
- JS
- PL/SQL
- J
- PHP
- Ruby
- Python
- Groovy

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

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Local development</td>
<td>● Requires tiller -- Helm v2</td>
</tr>
<tr>
<td>● Uses git and its auth model</td>
<td>● 0.16.x experimental release</td>
</tr>
<tr>
<td>● Integrated docker image builder</td>
<td>● Support: active community</td>
</tr>
<tr>
<td>● <strong>Support:</strong> active community</td>
<td>● Security con</td>
</tr>
</tbody>
</table>

[https://github.com/Azure/draft](https://github.com/Azure/draft)
<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**

**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
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?
- unprivileged builds

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

What?
- Build images
- Build fast

How?
- Bazel rules
- Knative templates

Security?
- Deterministic
- Reproducible
- Unprivileged

https://bazel.build
Other Build Tools

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

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

https://github.com/theupdateframework
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

https://github.com/aquasecurity/trivy
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

@raravena80
### Other Security Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Falco</td>
<td>Container Activity Monitor</td>
</tr>
<tr>
<td>Harbor</td>
<td>Secure registry (Notary)</td>
</tr>
<tr>
<td>Anchore, Aqua, Clair, Dagda</td>
<td>Image scanning</td>
</tr>
<tr>
<td>Grafeas</td>
<td>Signing</td>
</tr>
<tr>
<td>Kritis, Portieris</td>
<td>Admission Controller</td>
</tr>
<tr>
<td>Kube hunter</td>
<td>K8s Vulnerabilities</td>
</tr>
<tr>
<td>Open Policy Agent</td>
<td>Config enforcer</td>
</tr>
<tr>
<td>Trireme</td>
<td>Netpol mgmt</td>
</tr>
<tr>
<td>Image encryption</td>
<td>Encrypt cont imgs</td>
</tr>
<tr>
<td>Tern, Snyk</td>
<td>Package Compliance</td>
</tr>
</tbody>
</table>
CI/CD Tools
## JenkinsX

<table>
<thead>
<tr>
<th>What?</th>
<th>How?</th>
<th>Security?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Jenkins</td>
<td>• jx command line</td>
<td>• Auto upgrade w/GitOps and Tekton</td>
</tr>
<tr>
<td>• Nexus</td>
<td>• jenkins-x.yml file for pipelines</td>
<td>• Jenkins built in sec</td>
</tr>
<tr>
<td>• Draft</td>
<td>• Leverages draft to manage code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Skaffold to build and push images</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ChartMuseum (Helm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monocular (Chart disc)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Skaffold</td>
<td></td>
</tr>
</tbody>
</table>
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
Other CI/CD Tools

- Spinnaker
- Argo CD
- Drone CI
- GoCD
- Gitlab
- TeamCity
- Screwdriver CD
- Rundeck
- Habitat
Secure Software Supply Chain
GitOps Future
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
- ✗ 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.serverboote.com