Running trusted payloads with Nomad and Waypoint

Bram Vogelaar
@attachmentgenie
$ whoami

- Used to be a Molecular Biologist
- Then became a Dev
- Now an Ops
- Currently Cloud Engineer @ The Factory
Monday Morning: Standup time!

“The intern “solved” the problem with $product by “fixing” the database connection”
Wait! What?
#nocontext

DEPLOYMENTS ON FRIDAY

WE DON'T DO THAT HERE
problems++?
Access Security
CI/CD is in place to provide trust

The discipline of experimenting on a distributed system in order to build confidence in the system’s capability to withstand turbulent conditions in production

Chaos Engineering Definition
Testing Pyramid

- E2E
- System Integration Tests
- Integration Tests
- Unit Tests
Shared Responsibility

Two-man, Four-eyes Principle

I’ve looked at it twice

By Lorraine
Waypoint

- Modern workflow to release across platforms.
- Pipelines written in (H)ashiCorp (C)onfiguration (L)anguage
- Extendable by with (self-written) plugins

https://www.waypointproject.io/
Common nomenclature for pipeline steps

project = "lorem-ipsum"
app "lorem-ipsum" {
  build {}  
  deploy {}  
  release {}  
}
Vault

- Open Source tool to do secrets management
- Secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.
- Certificate management
- Supports Password as a Service for tools like SSH and MySQL

https://www.vaultproject.io/
Supply Chain Attack Vectors

A Bypassed code review
B Compromised source control system
C Modified code after source control
D Compromised build platform
E Using a bad dependency
F Bypassed CI/CD
G Compromised package repo
H Using a bad package

https://slsa.dev/
Don’t trust the internet

Standing on the shoulders of giants, has pro’s and con’s

- Npm
- Maven
- Composer
- Rubygems
Be Self Sufficient!

- Build from local ensure continuity
  - OS repositories
  - Image repositories
  - Code packages
- Create a Software Bill of Materials (SBOM)
  - What is included in the first place?
  - Unwanted Licenses
  - Vulnerable Packages / Images
Vulnerability Scanning

clair

snyk
Garbage in, garbage out?

```yaml
app "lorem-ipsum" {
  build {
    hook {
      when = "before"
      command = ["./snyk_scan.sh", "build starting"]
    }
    hook {
      when = "after"
      command = ["./artifact_fingerprint.sh", "build finished"]
    }
  }
}
```
Don’t promote code, but promote artifacts
Nomad

- Open Source tool for dynamic workload scheduling
- Batch, containerized, and non-containerized applications.
- Has native Consul and Vault integrations.
- Has token based access setup.
- Jobs written in (H)ashiCorp (C)onfiguration (L)anguage

https://www.nomadproject.io/
Nomad Job Structure

```yaml
job "lorem-ipsum" {
  group "frontend" {
    network {
      port "http" { static = "8080" }
    }
  }
  task "server" {
    driver = "docker"
    config {
      image = "cicero/lorem-ipsum"
      ports = ["http"]
    }
  }
}
```
Docker Content Trust

$ docker trust key generate bram
$ docker trust key load key.pem --name bram
$ docker trust signer add --key cert.pem jeff registry.example.com/cicero/lorem-ipsum
$ docker trust sign registry.example.com/cicero/lorem-ipsum:1
$ export DOCKER_CONTENT_TRUST=1
$ docker push registry.example.com/cicero/lorem-ipsum:1
$ docker trust inspect --pretty registry.example.com/admin/demo:1

$ docker trust revoke registry.example.com/admin/demo:1

$ export DOCKER_CONTENT_TRUST=1
$ docker pull registry.example.com/user/image:1
Q.E.D?

https://slsa.dev/
Contact

bram@attachmentgenie.com

@attachmentgenie

https://www.slideshare.net/attachmentgenie