Container deployments – useful tools

Michael Schuh
European XFEL, Data Analysis
PhD Researcher

Schenefeld, 25. February 2025

GitLab CI – DIND or Kaniko

- https://docs.gitlab.com/ci/docker/using_kaniko/

kaniko is a tool to build container images from a Dockerfile, inside a container or Kubernetes cluster.

- Docker-in-Docker requires privileged mode to function, which is a significant security concern.

```
build:
  extends: .base_build
  stage: build
  script:
    - echo "Building and pushing image"
    - /kaniko/executor
      --context "${CI_PROJECT_DIR}"
      --dockerfile "${CI_PROJECT_DIR}/Containerfile"
      --destination "${CI_REGISTRY_IMAGE}:${CI_COMMIT_SHORT_SHA}"
```

GitLab CI – Crane

- https://github.com/google/go-containerregistry/blob/main/cmd/crane/doc/crane.md

Crane is a tool for managing container images

Example: Validate and re-tag remote image without downloading it.

```yaml
release_image:
  stage: release
  image:
    name: gcr.io/go-containerregistry/crane:debug
    entrypoint: [""]
  variables:
    # Do not clone the repository
    GIT_STRATEGY: none
  script:
    - crane auth login -u "$CI_REGISTRY_USER" -p "$CI_REGISTRY_PASSWORD" "$CI_REGISTRY"
    - crane validate --remote "${CI_REGISTRY_IMAGE}:${CI_COMMIT_SHORT_SHA}"
    - crane tag "${CI_REGISTRY_IMAGE}:${CI_COMMIT_SHORT_SHA}" "${CI_COMMIT_REF_NAME}"
```

GitLab CI – Helm Repository

- https://helm.sh
  - Helm is a package manager for Kubernetes applications
  - Helm Charts define, install, and upgrade from simple to the most complex Kubernetes application

- https://docs.gitlab.com/user/packages/helm_repository/
  - Publish Helm packages in Gitlab's project package registry.
  - Then install the packages using this as a OCI Helm repository.

```
- cd k8s/helm/container-demo
- helm dependency update
- helm package .
- ls
- chart_file=$(ls -l container-demo*.tgz | head -n 1 | awk '{print $NF}')
- curl -v --request POST
  --user gitlab-ci-token:$CI_JOB_TOKEN
  --form "chart=@${chart_file}"
  "${CI_API_V4_URL}/projects/${CI_PROJECT_ID}/packages/helm/api/${CHANNEL}/charts"
```

Nested Helm Charts

Helm Chart.yaml - The Chart.yaml file is required for a chart (chart.json)

```yaml
apiVersion: v2
appVersion: 0.1.0
dependencies:
- condition: not database.external
  name: postgresql
  repository: https://charts.bitnami.com/bitnami
  version: 16.4.14
description: A Helm chart for container-demo on Kubernetes
name: container-demo
type: application
version: 0.1.0
```

Helm Chart.yaml - The Chart.yaml file is required for a chart (chart.json)

```yaml
apiVersion: v2
appVersion: "2.11"
description: Visa portal
name: panosc-visa
type: application
version: 3.11.0
dependencies:
  - name: redis
    version: "20.1.0" # Use the appropriate version
    repository: "https://charts.bitnami.com/bitnami"
    condition: redis.enabled
  - name: postgresql
    version: "15.5.15" # Use the appropriate version
    repository: "https://charts.bitnami.com/bitnami"
    condition: not database.external
```

Kompose

- Conversion tool for Docker Compose to container orchestrators such as Kubernetes (or OpenShift).
- https://kompose.io/conversion/

Flux GitOps

- Keep Kubernetes clusters in sync with sources of configuration (like Git repositories).
  - Git as Single Source of Truth
- Automate updates to deployments
  - and configuration
    - Nginx ingress
    - Certmanager
    - Sealed secrets

Sealed secrets - one-way encrypted Secrets

- Do not push (base64 encoded) clear text secrets to Gitlab, use human readable encrypted secrets.

```yaml
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  creationTimestamp: null
  name: visa-credentials
  namespace: flux-system
spec:
  encryptedData:
    password: AgA8wdIGMGh6kEuEdC/XUybAOZU9JBBl7TOFgqerkocnm7I7Z25TVE
    username: AgBRkkceKWDfS8YxKgGY0/uoQLgMG9abQrIdjFA//sPgxEY+yXOvb8
  template:
    metadata:
      creationTimestamp: null
      name: visa-credentials
      namespace: flux-system
```