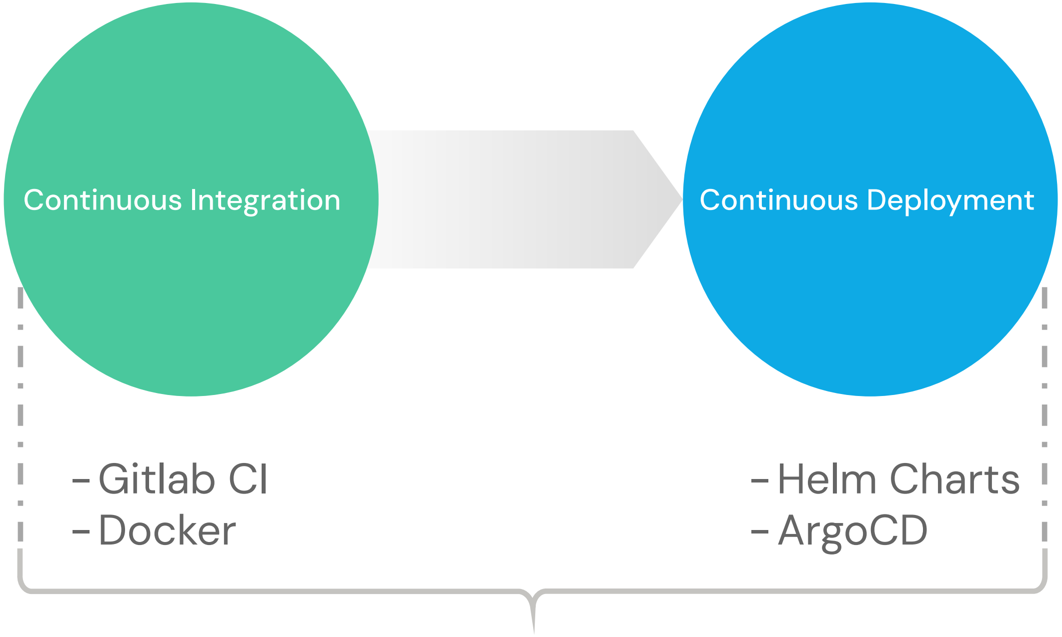
MOLDOVA
DEVOPS COMMUNITY

CI/CD Pipeline

Secrets Versioning

● ● ● ●



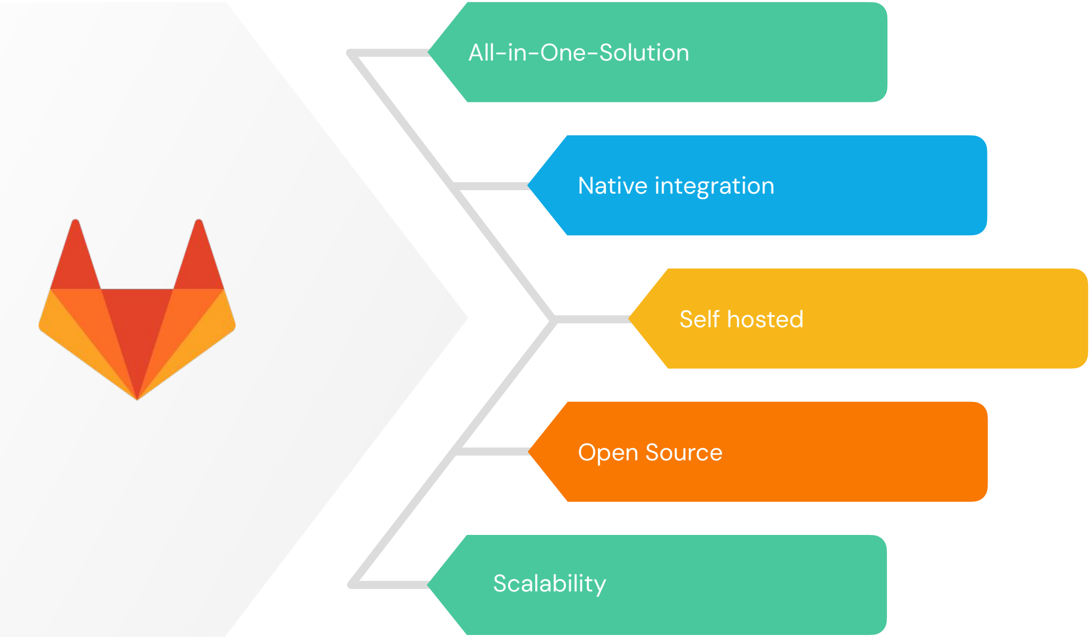
Continuous Integration

Continuous Deployment

- Gitlab CI
- Docker

- Helm Charts
- ArgoCD

SOPS: Secrets OPerationS



All-in-One-Solution

Native integration

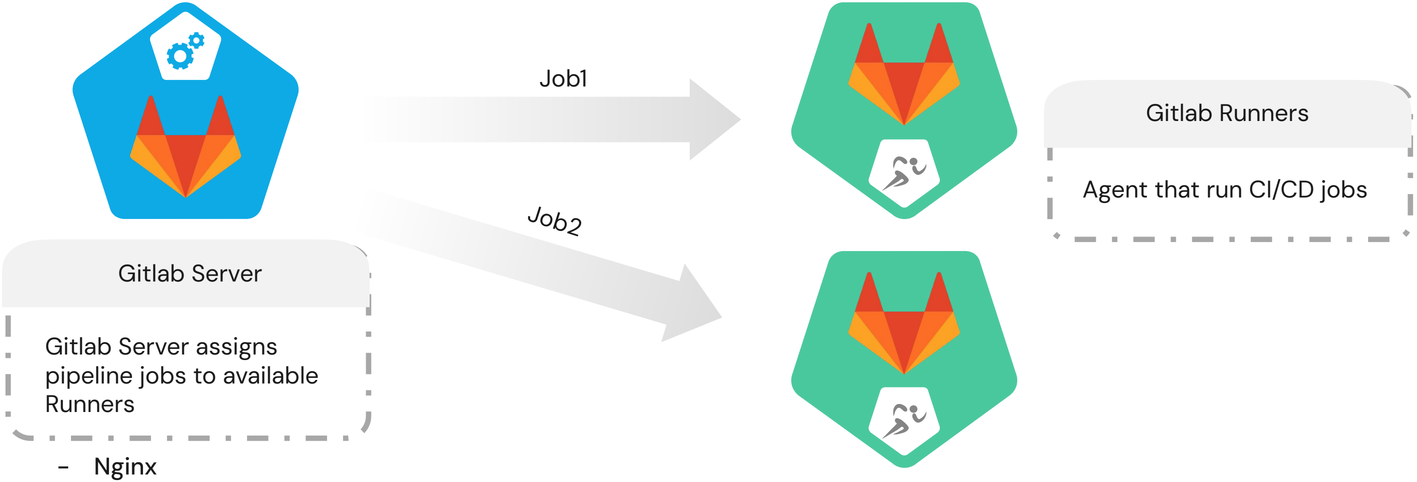
Self hosted

Open Source

Scalability

Gitlab-CI

It was launched in nov 2016 Ukrainian developer Dmytro Zaporozhets and Dutch developer Sytse Sijbrandij. As programing language for writing Gitlab-CI was used Ruby, GO, Vue JS and Javascript.



Gitlab Server

Gitlab Server assigns pipeline jobs to available Runners

Gitlab Runners

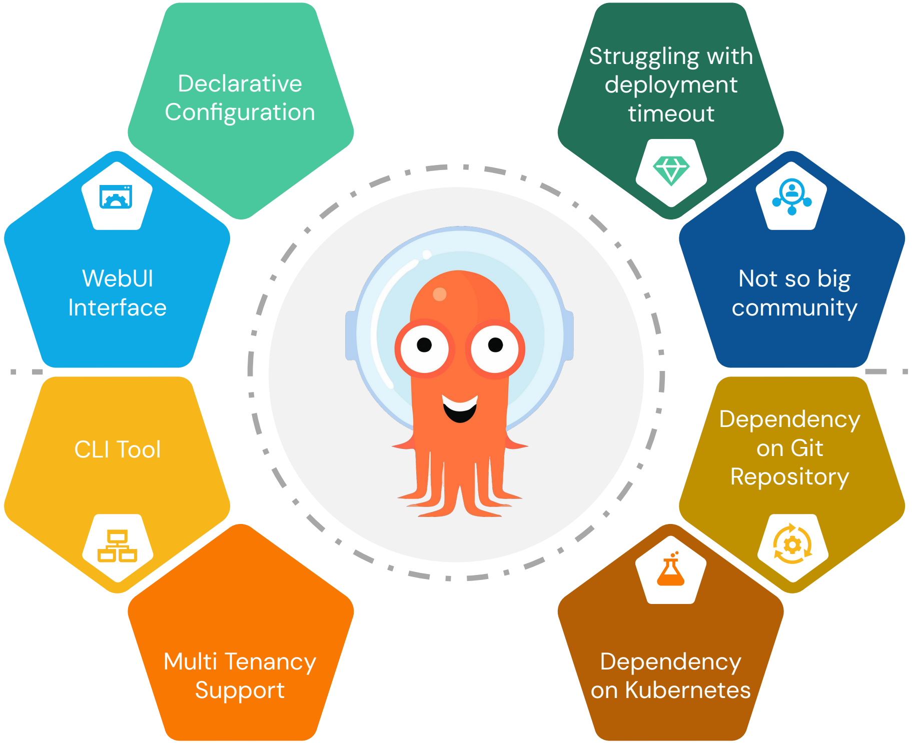
Agent that run CI/CD jobs

- Nginx
- Gitlab Pages
- Gitlab Workhorse
- Gitlab Shell
- Gitaly
- Puma
- PostgreSQL
- Redis
- Sidekiq

ArgoCD

- Live sync with GIT Repositories
- Integration with: HelmCharts, Kustomize, Simple Manifests, Custom solutions (Plugins)
- Deploy on multiple kubernetes clusters

- Multiple methods of authentication (LDAP, SAML, Oauth)
- Web Interface
- CLI tool



- Solution with custom timeout is not working well
- Comparing to other open source tools not have so big community

- Can manage only kubernetes applications
- It's working only with GIT

HelmCharts

- HelmCharts is a package manager for Kubernetes apps that simplifies deployment.
- It's a declarative form that provides many parametrization and templatization options for your application, allowing for improved reuse in various scenarios.
- They can be versioned for tracking purposes and rollback if necessary.

Artifact Hub is a platform that serves as a centralized repository for discovering, sharing, and collaborating on software packages and artifacts. It's particularly popular in the context of cloud-native applications and Kubernetes. Here's a breakdown of what Artifact Hub entails:

Chart.yaml

This file contains metadata about the Helm Chart, such as the name, version, description, maintainer, and dependencies.

values.yaml

This file defines default configuration values for the Helm Chart. Values specified in this file can be overridden during deployment to customize the behavior of the application.

Templates

This directory contains template files (usually with the .yaml or .tpl extension) that define Kubernetes manifest files. Each template file represents a Kubernetes resource, such as Deployment, Service, Ingress, ConfigMap, Secret, etc.

_helpers.tpl

Is a special template file that contains helper functions and utilities that can be used across multiple template files within the Chart.

Charts (optional)

This directory is used to store dependencies on other Helm Charts. If your Chart depends on other Charts, Helm automatically resolves and installs these dependencies when deploying your Chart.

SOPS: Secrets Operations SOPS

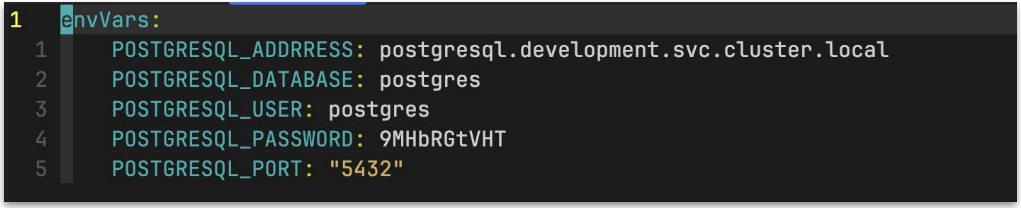
SOPS stands for Standard Operating Procedures. SOPS is used as a secret management tool within source control systems such as git, and is a popular solution in the context of Kubernetes and Helm charts. Essentially, he performs encryption and decryption on the basis of a key stored somewhere secure, with granular access controls over who and what has access.

ENCRYPTION AND DECRYPTION

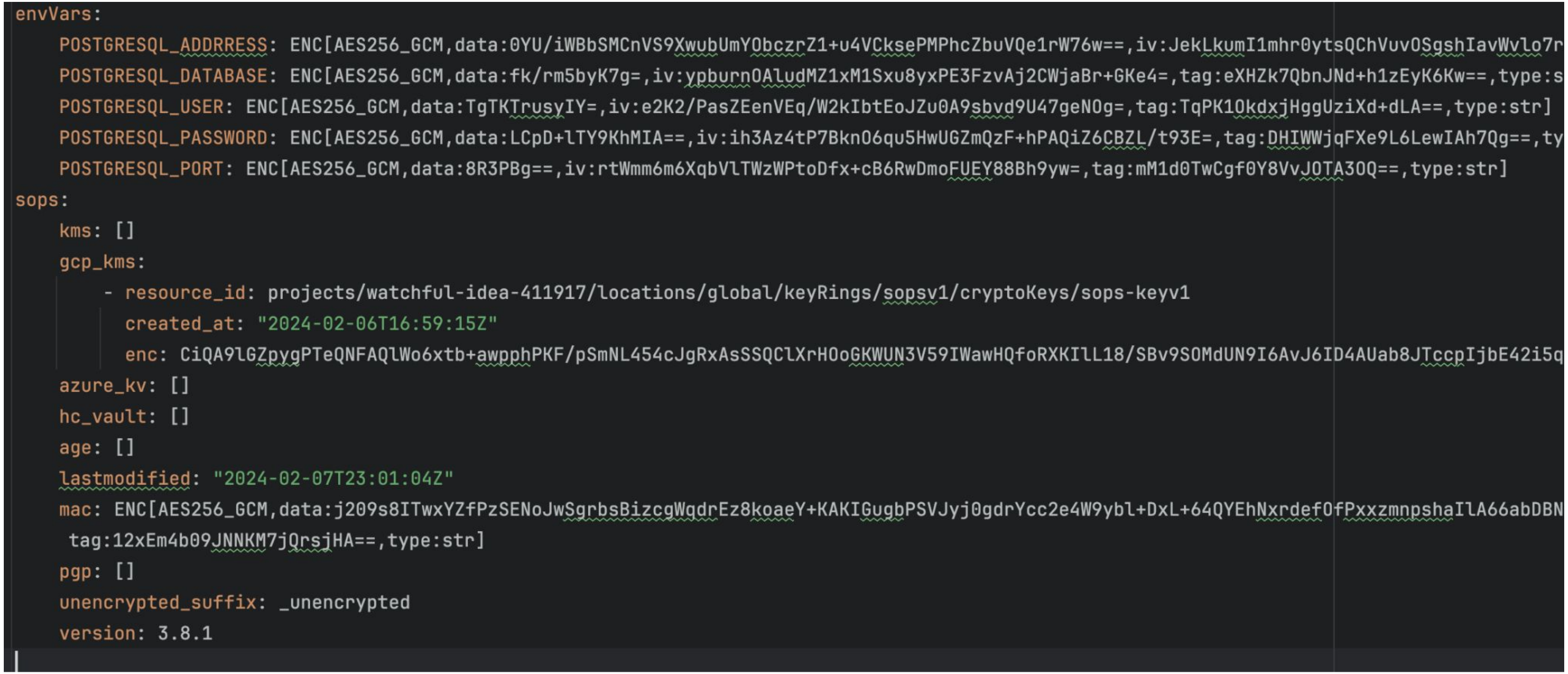
Integration with different text editors and IDE, starting with VIM and finishing for exemple with Intellij

You can version SOPS secrets with GIT that can offer changes tracking and rollback in case of unforeseen situations.

It’s support a big amount of key management systems such as: GPG or cloud based from (Azure, AWS or GCP)

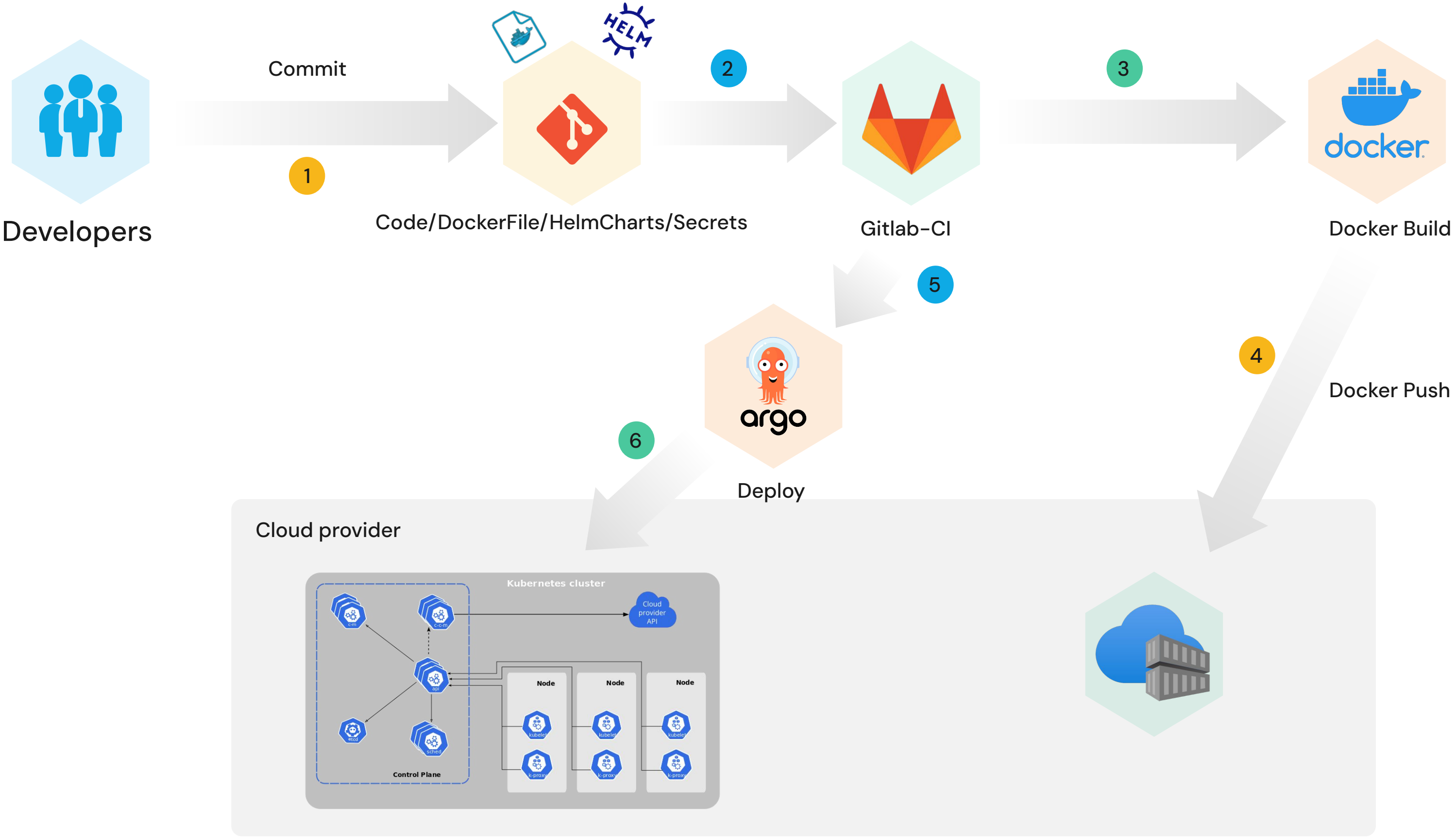


```yaml
envVars:
    POSTGRESQL_ADDRRESS: postgresql.development.svc.cluster.local
    POSTGRESQL_DATABASE: postgres
    POSTGRESQL_USER: postgres
    POSTGRESQL_PASSWORD: 9MHbRGtVHT
    POSTGRESQL_PORT: "5432"
```



```yaml
envVars:
    POSTGRESQL_ADDRRESS: ENC[AES256_GCM,data:0YU/iWBbSMCnVS9XwubUmYObczrZ1+u4VCksePMPhcZbuVQe1rW76w==,iv:JekLkumI1mhr0ytsQChVuvOSgshIavWvlo7r
    POSTGRESQL_DATABASE: ENC[AES256_GCM,data:fk/rm5byK7g=,iv:ypburnOAludMZ1xM1Sxu8yxPE3FzvAj2CWjaBr+GKe4=,tag:eXHZk7QbnJNd+h1zEyK6Kw==,type:s
    POSTGRESQL_USER: ENC[AES256_GCM,data:TgTKTrusyIY=,iv:e2K2/PasZEenVEq/W2kIbtEoJZu0A9sbvd9U47geNOg=,tag:TqPK1OkdxjHggUziXd+dLA==,type:str]
    POSTGRESQL_PASSWORD: ENC[AES256_GCM,data:LCpD+lTY9KhMIA==,iv:ih3Az4tP7BknO6qu5HwUGZmQzF+hPAQiZ6CBZL/t93E=,tag:DHIWWjqFXe9L6LewIAh7Qg==,ty
    POSTGRESQL_PORT: ENC[AES256_GCM,data:8R3PBg==,iv:rtWmm6m6XqbVlTWzWPtoDfx+cB6RwDmoFUEY88Bh9yw=,tag:mM1d0TwCgf0Y8VvJOTA3OQ==,type:str]
sops:
    kms: []
    gcp_kms:
        - resource_id: projects/watchful-idea-411917/locations/global/keyRings/sopsv1/cryptoKeys/sops-keyv1
          created_at: "2024-02-06T16:59:15Z"
          enc: CiQA9lGZpygPTeQNFAQlWo6xtb+awpphPKF/pSmNL454cJgRxAsSSQClXrHOoGKWUN3V59IWawHQfoRXKIlL18/SBv9SOMdUN9I6AvJ6ID4AUab8JTccpIjbE42i5q
    azure_kv: []
    hc_vault: []
    age: []
    lastmodified: "2024-02-07T23:01:04Z"
    mac: ENC[AES256_GCM,data:j209s8ITwxYZfPzSENoJwSgrbsBizcgWqdrEz8koaeY+KAKIGugbPSVJyj0gdrYcc2e4W9ybl+DxL+64QYEhNxrdefOfPxxzmnpshaIlA66abDBN
     tag:12xEm4b09JNNKM7jQrsjHA==,type:str]
    pgp: []
    unencrypted_suffix: _unencrypted
    version: 3.8.1
```

MOLDOVA DEVOPS COMMUNITY



Developers

1 Commit

Code/DockerFile/HelmCharts/Secrets

2

Gitlab-CI

3

Docker Build

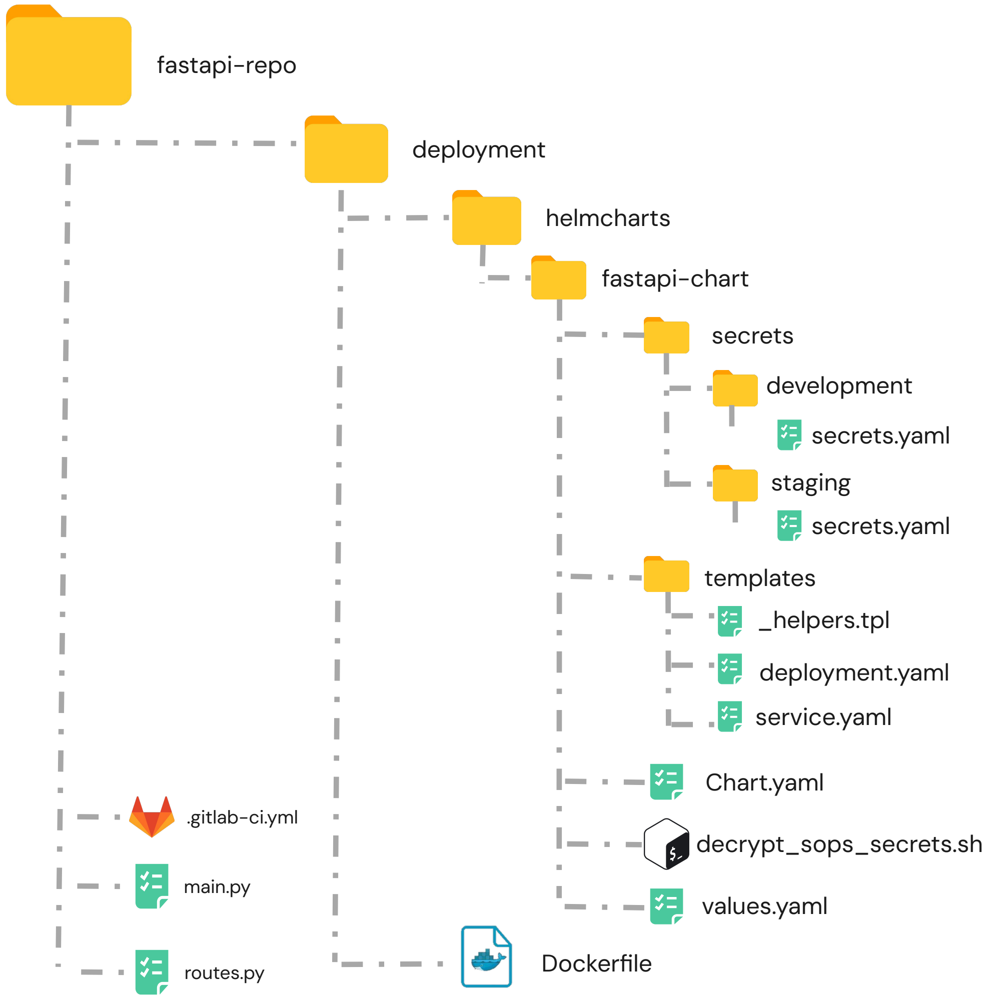
4 Docker Push

5

Deploy

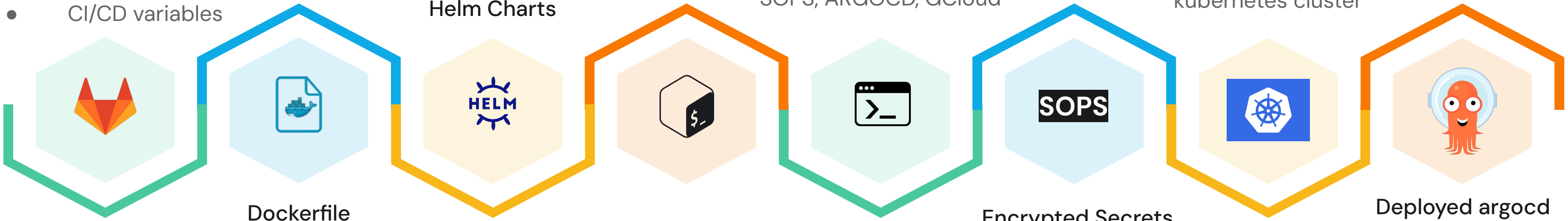
6

Cloud provider



- fastapi-repo
  - deployment
    - helmcharts
      - fastapi-chart
        - secrets
          - development
            - secrets.yaml
          - staging
            - secrets.yaml
        - templates
          - _helpers.tpl
          - deployment.yaml
          - service.yaml
        - Chart.yaml
        - decrypt_sops_secrets.sh
        - values.yaml
    - Dockerfile
  - .gitlab-ci.yml
  - main.py
  - routes.py

Pipeline Configuration



Configured gitlab-ci repo

- Repo structure
- .gitlab-ci.yaml
- CI/CD variables

Dockerfile

Helm Charts

Bash script for decrypt

This bash script will be used by ArgoCD pipeline to decrypt sops secret before apply helm chart.

Installed cli tools

SOPS, ARGOCD, GCloud

Encrypted Secrets

With Gcloud KMS key ring

Kubernetes

Already deployed kubernetes cluster

Deployed argocd

- Disabled tls for ArgoCD server
- Custom docker image for repo-server
- Added git repo to ArgoCD
- K8S Secret from SA Key
- SOPS Plugin ConfigMap
- Update argocd-repo-server with plugin as side car
- ArgoCD Application

ArgoCD
Repo Server

ConfigMap
SopsPlugin

DEMO

Q/A