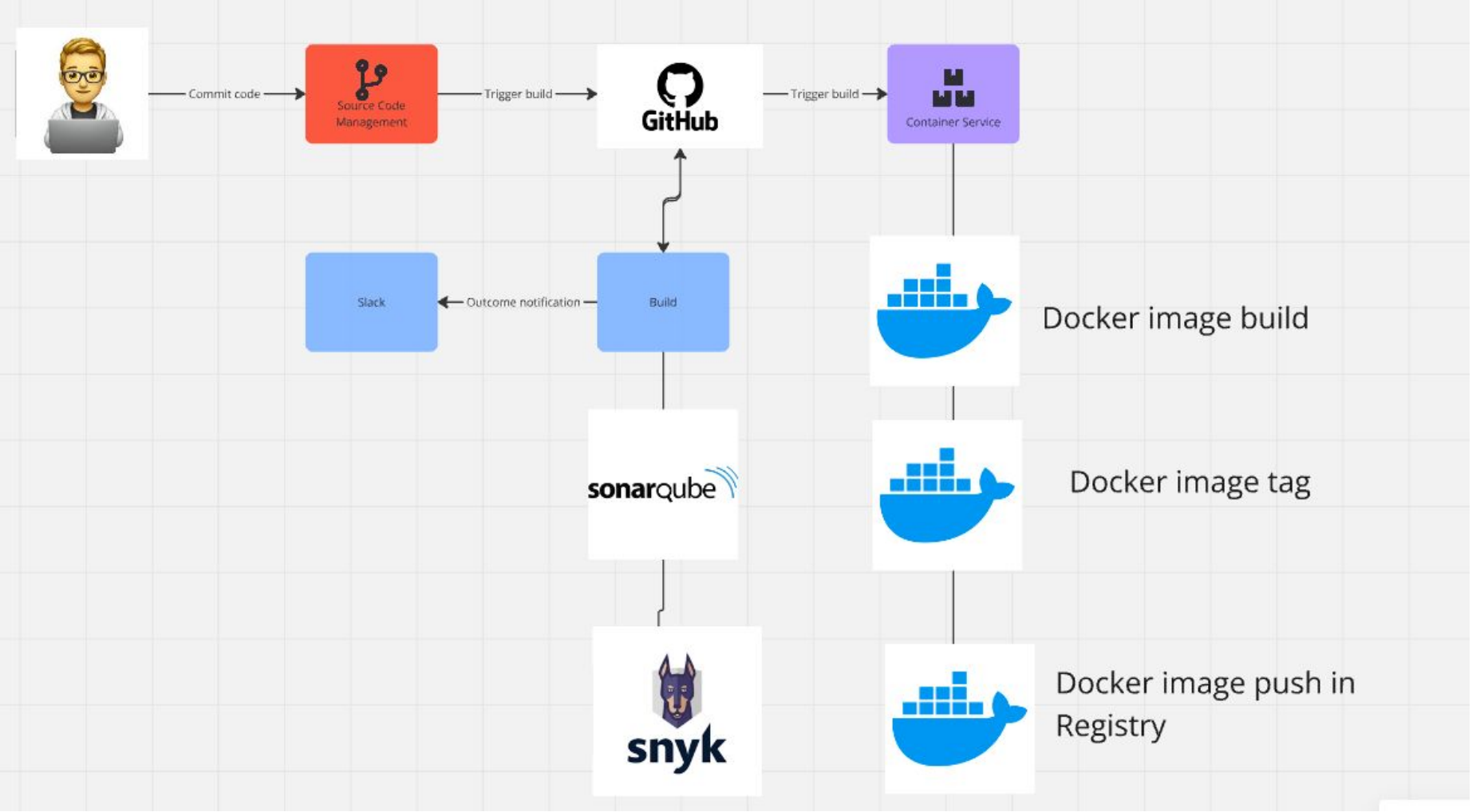
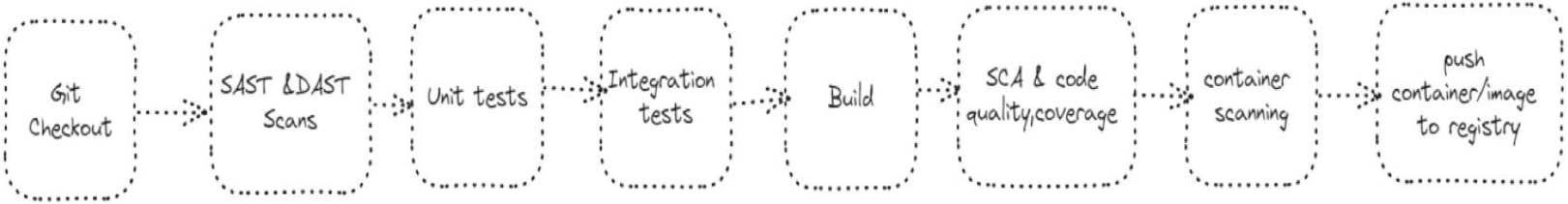
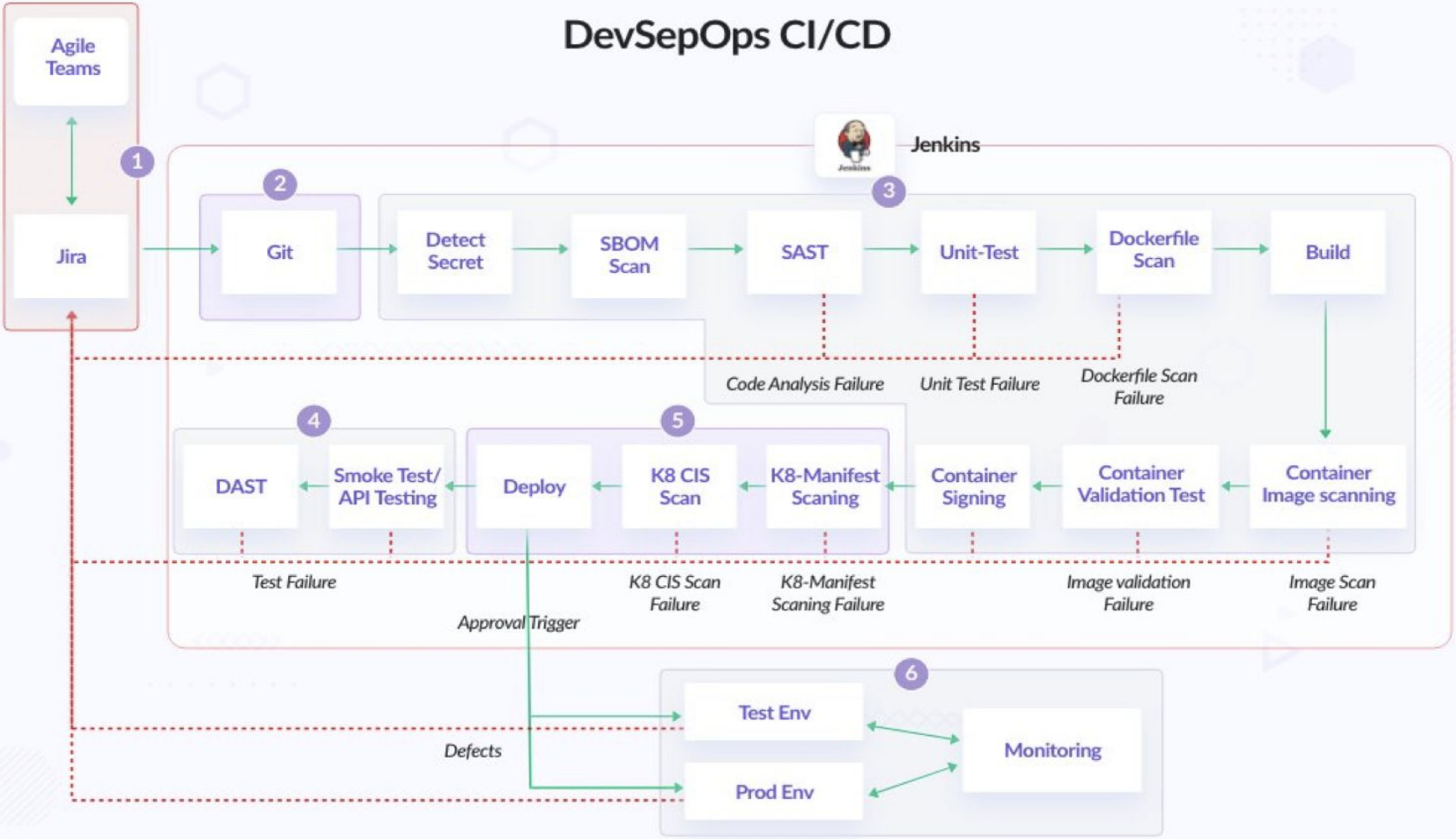
End to End DevSecOps CI Pipeline using Github Action.


Commit code
Source Code Management
Trigger build
GitHub
Trigger build
Container Service
Slack
Outcome notification
Build
Docker image build
sonarqube
Docker image tag
snyk
Docker image push in Registry

END TO END PIPELINE STAGES-



DevSepOps CI/CD



Snyk Vs Sonarcloud

- Snyk mostly works on security aspects like SAST(Static Application Security Testing) and SCA(Software Composition Analysis).
- Sonarcloud or Sonarqube focuses on Code coverage,Code quality , etc
- Both offer a range of services.
- We can even include DAST (Dynamic Application Security Testing) like OWASP Zed proxy Attack,Nikto etc

Key requirements for Application Build

1. Create A Build Server from your Cloud Account or you can use github provided runner
2. Add the cloud Server in github as a runner
3. Install the software which required to build the application (maven,java, docker)
4. Create Github Action for CI/CD pipelines.
5. Make sure the code is scanned using Sonar Cloud (Create a free account on https://sonarcloud.io)
6. The code needs to be scanned and built on every branch code commit.
7. Create a free account on **JFROG** **Artifactory** because this will be used to store JAR/Docker Image.

STEP1- got to github repo →Setting→Action→Runner and then download the tar in your server

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

General

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Rules

Actions

General

Runners

Webhooks

Environments

Codespaces

Pages

Security

Runners / Add new self-hosted runner · ankit20000/DevSecops_Pipeline

Adding a self-hosted runner requires that you download, configure, and execute the GitHub Actions Runner. By downloading and configuring the GitHub Actions Runner, you agree to the GitHub Terms of Service or GitHub Corporate Terms of Service, as applicable.

Runner image

macOS | Linux | Windows

Architecture

x64

Download

```
# Create a folder
$ mkdir actions-runner && cd actions-runner
# Download the latest runner package
$ curl -o actions-runner-linux-x64-2.320.0.tar.gz -L
https://github.com/actions/runner/releases/download/v2.320.0/actions-runner-linux-x64-
2.320.0.tar.gz
# Optional: Validate the hash
$ echo "93ac1b7ce743ee85b5d386f5c1787385ef07b3d7c728ff66ce0d3813d5f46900  actions-runner-linux-x64-
```

Step1: Clone/fork this spring petclinic repo

https://github.com/ankit20000/DevSecops_Pipeline.git

Step2: copy snyk api token snyk account

snyk

ORGANIZATION

DevSecOps pipeline

- Dashboard
- Projects
- Integrations
- Members
- Settings

Help

Deepak Reddy

- Usage
- Your plan and billing
- Plans and pricing
- Licenses
- Notifications
- Snyk Preview

INTEGRATIONS

- GitHub
- GitLab

Organization slug

The Organization slug is the canonical name for the Organization. It is required for use in the CLI, and also can be used for SSO user role assignment. See our user role management documentation for more details.

```
deepakreddyats1
```

Copy

Organization API key

Service accounts can be used to access this organization and its projects via the Snyk CLI and the Snyk API .

Manage service accounts

Organization ID

This ID uniquely identifies this organization. You'll need it if you're using the Snyk API. See our API documentation for more details.

```
0c423c1a-5805-4b22-a62a-38ec7fc8cd40
```

Copy

Ignores

Control how ignore policies are applied to projects within this organization.

Ability to ignore an issue, or edit the ignore settings on an issue through the Snyk app or API

- Admin users only

Step3: Add Sonar Url , sonartoken, jfrog url jfrog toke , docker username and docker password

Security

- Code security
- Deploy keys
- Secrets and variables
  - Actions
  - Codespaces
  - Dependabot

Integrations

- GitHub Apps
- Email notifications

Repository secrets

New repository secret

Name	Last updated
DEVSECOPS_PIPELINE_TOKEN	4 days ago
DOCKER_PASSWORD	4 days ago
DOCKER_USERNAME	4 days ago
JFROG_TOKEN	2 days ago
SONAR_HOST_URL	4 days ago
SONAR_PROJECT_KEY	4 days ago
SYNK_API_TOKEN	4 days ago

Step4- Create the pipeline

ankit20000 / DevSecops_Pipeline

Type / to search

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

Files

master

Go to file t

- .github/workflows
  - build.txt
  - feature.yml
  - imagepush.yml
  - javabuild.yml
  - sonar.yml
  - test.yml
- .gradle
- gradle
- src

DevSecops_Pipeline / .github / workflows /

Add file

ankit20000 added ✓ 1bc6529 · 2 days ago History

Name	Last commit message	Last commit date
..		
build.txt	added	2 days ago
feature.yml	added	2 days ago
imagepush.yml	added	2 days ago
javabuild.yml	added	2 days ago
sonar.yml	added	2 days ago
test.yml	added	2 days ago

STEP 5 – after adding variables run the pipeline or make any commit to execute.

ankit20000 / DevSecops_Pipeline

Type / to search

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

← CI Pipeline

added #10

Re-run all jobs

Summary

Jobs

- build
- sonar
- test
- imagepush

Run details

- Usage
- Workflow file

Triggered via push 2 days ago

ankit20000 pushed 1bc6529 master

Status	Total duration	Artifacts
Success	6m 24s	2

feature.yml

on: push

build / build 2m 20s → sonar / sonar 49s → test / test 41s → imagepush / image_push 2m 2s

SonarQube status

sonarcloud

My Projects | My Issues | Explore

Filters

Quality Gate

- Passed 1
- Failed 0

Reliability

- A 0
- B 0
- C 1
- D 0
- E 0

Security

- A 1
- B 0

Search for projects | Perspective: Overall Status | Sort by: Name | 1 projects

ankit shukla / petclinic NEW PUBLIC — Passed

Last analysis: 26/10/2024, 00:02 • 1.2k Lines of Code • Java, XML

A 0	C 1	A 25	A 100%	88.6%	0.0%
Security	Reliability	Maintainability	Hotspots Reviewed	Coverage	Duplications

1 of 1 shown

Jfrog Artifacts -

JFrog Platform | All Projects | Application | Administration | Search Artifacts

Artifactory > Artifacts

- Get Started
- Artifactory
  - Packages
  - Builds
  - Artifacts
  - Release Lifecycle
- Xray
- Integrations
- MyJFrog Portal

Happily serving 669 artifacts

Set Me Up | Deploy | Manage Repositories

Search Repositories | Clear | My Favorites | Tree View:

- java-libs-release
- java-libs-snapshot
- artifactory-build-info
- docker-trial
- java-libs-release-local
- java-libs-snapshot-local
- petjfrog-repo
  - target
    - spring-petclinic-3.2.0-SNAPSHOT
  - Dockerfile
- tf-trial

petjfrog-repo

General | Effective Permissions | Properties | Followers

Info

Name:	petjfrog-repo
Package Type:	Maven
Repository Path:	petjfrog-repo/
File URL:	https://trial42aeja.jfrog.io/artifactory/petjfrog-repo/

Docker Hub status-

dockerhub Explore Repositories Organizations Usage Search Docker Hub ⌘+K A

ankit1111 / Repositories / petapp / General

Using 1 of 1 private repositories.

General Tags Builds Collaborators Webhooks Settings

ankit1111/petapp

Last pushed 1 day ago

This repository does not have a description INCOMPLETE

This repository does not have a category INCOMPLETE

Docker commands

Public View

To push a new tag to this repository:

```
docker push ankit1111/petapp:tagname
```

Tags

This repository contains 3 tag(s).

Tag	OS	Type	Pulled	Pushed
1bc652921697b9253...		Image	---	2 days ago
2458b6477b3e8535b...		Image	2 days ago	2 days ago

Automated Builds

Manually pushing images to Hub? Connect your account to GitHub or Bitbucket to automatically build and tag new images whenever your code is updated, so you can focus your time on creating.

Available with Pro, Team and Business subscriptions. Read more about automated builds.