

GOVTECH  
SINGAPORE

# SHIP-HATS 2.0

## Docker Pipeline

### Webinar

Learning Events | Level 200 Tech



CLOUD | DEVOPS  
MACHINE LEARNING

Implementation and training  
services

CLOUD ENABLED

ENABLED BY CLOUD | DELIVERING CLOUD  
CLOUD ENABLED PTE LTD



SINCE  
**2013**

INDIA | SINGAPORE | DUBAI

PHONE +65 -81320344

EMAIL

reach@thecloudenabled.com

WEBSITE

[www.thecloudenabled.com](http://www.thecloudenabled.com)

## ABOUT US

**ANIL BIDARI**  
CEO @ CLOUD ENABLED



# Understanding Docker Pipeline



# Pipeline Templates

SHIP-HATS 2.0 offers a library of CI/CD pipeline templates that simplifies configuration efforts.

## E2E templates

- Main ci file to build your pipeline
- Build→Test→Deploy .yml files with all variable keys defined (only values you need to add)

## Modular templates

- Leverage these if Anything specific task in pipeline required
- Example – check webapp is ready or not

# Review E2E Templates

1. Go to Developer Portal: [SHIP-HATS Pipeline Templates](#)
2. Check for E2E Templates
3. Let's review SHIP-HATS Webapp E2E Template

[Access E2E templates in GitLab here](#)



E2E templates		
Template	Description	Template Type
<a href="#">SHIP-HATS Docker Image CI Pipeline Templates</a>	This template allows you to deliver a compliant CI pipeline for a standard docker application (regardless of language) considering best practices as well as security aspects.	End to end Template
<a href="#">SHIP-HATS Docker Multi Services App E2E Templates</a>	This template allows you to deliver a compliant CI/CD pipeline for a standard docker application (regardless of language) considering best practices as well as security aspects.	End to end Template
<a href="#">SHIP-HATS Docker Single Service App E2E Templates</a>	This template allows you to deliver a compliant CI/CD pipeline for a standard docker application (regardless of language) considering best practices as well as security aspects.	End to end Template
<a href="#">SHIP-HATS Webapp E2E Templates</a>	This template allows you to deliver a compliant CI/CD pipeline for a standard web application (regardless of language) considering best practices as well as security aspects.	End to end Template

# End-to-end Pipeline Template

## Your project pipeline plan

SHIP-HATS Webapp Pipeline  
Template

Your project specific variables



## End-to-End Pipeline Template From GovTech

E.g. SHIP-HATS Webapp Pipeline Template

# Modular Pipeline Templates

## Your project pipeline plan

Your project specific scripts

⋮  
⋮  
⋮  
⋮

Modular Testing Template

Modular Repo Template

Your project specific variables



## Modular Templates from GovTech

Build & Release Templates

QA & Security Templates

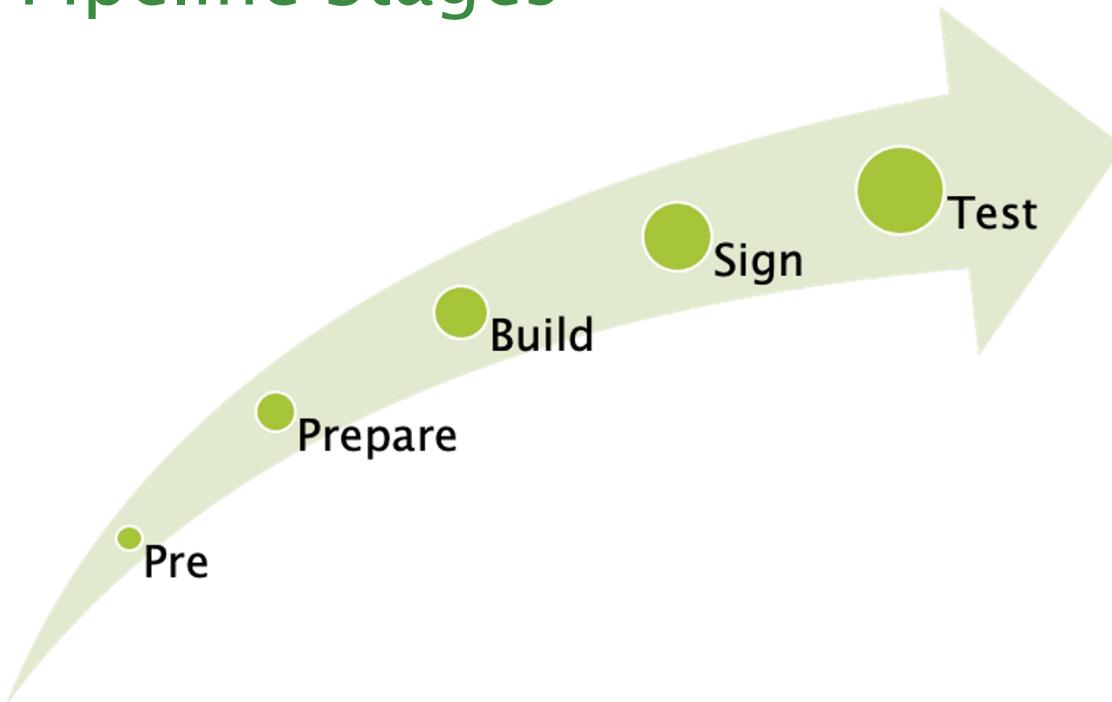
Artifact Repository Templates

⋮  
⋮  
⋮  
⋮

# Sample Docker Pipeline walkthrough

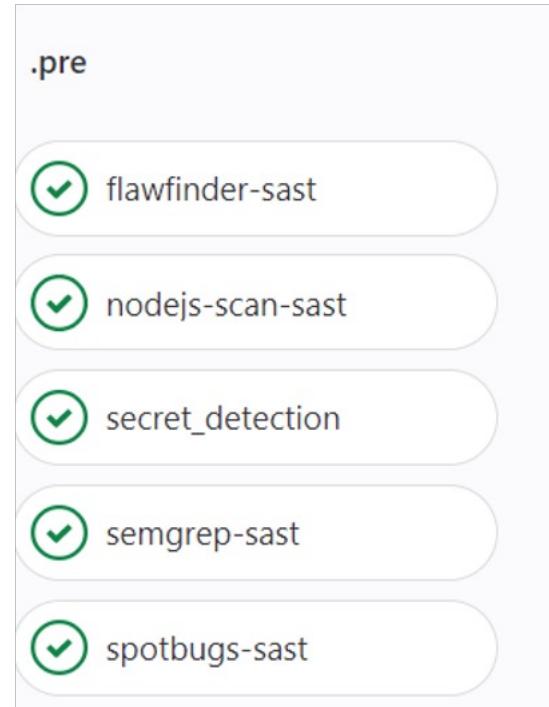


# Docker Pipeline Stages



We are using a nodejs app in this tutorial

# Pre-Stage



# Pre-Stage

```
15 Initialized empty Git repository in /builds/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-3/.git/
16 Created fresh repository.
17 Checking out 70bacb43 as main...
18 Skipping Git submodules setup
19 Executing "step_script" stage of the job script
20 Using docker image sha256:f53dd3cfe140639d05f587913865f0e6cbab5f3441d7f73cf8752df516433fec for registry.gitlab.com/security-products/gemnasiu
st registry.gitlab.com/security-products/gemnasium@sha256:d73db9517813851fd82758a23f59ba34cb5250d07a474ae8c1300eca300899d5 ...
21 $ ./analyzer run
22 [INFO] [Gemnasium] [2022-11-07T04:14:34Z] ► GitLab Gemnasium analyzer v3.10.5
23 [INFO] [Gemnasium] [2022-11-07T04:14:34Z] ► Using commit e0e4718d4e9dc8a00a87a0e103035bfea896cb6f
24 of vulnerability database
25 [INFO] [Gemnasium] [2022-11-07T04:14:39Z] ► using schema model 14
26 [INFO] [Gemnasium] [2022-11-07T04:14:39Z] ► Cannot auto-remediate dependency file, not supported: package-lock.json
27 [INFO] [Gemnasium] [2022-11-07T04:14:39Z] ► Cannot auto-remediate dependency file, not supported: views/angular.min.js
28 Executing "script" stage of the job script
29 Uploading artifacts for successful job
30 Uploading artifacts...
31 Uploading artifacts...
32 **/gl-sbom-*.cdx.json: found 1 matching files and directories
33 Uploading artifacts as "archive" to coordinator... 201 Created id=393142 responseStatus=201 Created token=noAmgtkH
```

# Pre-Stage

```
87 Initialized empty Git repository in /tmp/mog8yc/ShipStack-deployer-9823-trainee-group-0/result/testing-778+
88 Created fresh repository.
89 Checking out 70bacb43 as main...
90 Skipping Git submodules setup
▼ 92 Executing "step_script" stage of the job script
93 $ /analyzer run
94 [INFO] [NodeJsScan] [2022-11-07T04:15:20Z] ► GitLab NodeJsScan analyzer v3.3.2
95 [INFO] [NodeJsScan] [2022-11-07T04:15:20Z] ► Detecting project
96 [INFO] [NodeJsScan] [2022-11-07T04:15:20Z] ► Analyzer will attempt to analyze all projects in the repository
97 [INFO] [NodeJsScan] [2022-11-07T04:15:20Z] ► Running analyzer
98 [INFO] [NodeJsScan] [2022-11-07T04:15:48Z] ► Creating report
▼ 100 Uploading artifacts for successful job
```

# Pre-Stage

```
50 Skipping Git submodules setup
✓ 92 Executing "step_script" stage of the job script
  93 $ /analyzer run
  94 [INFO] [secrets] [2022-11-07T04:15:20Z] ► GitLab secrets analyzer v4.5.0
  95 [INFO] [secrets] [2022-11-07T04:15:20Z] ► Detecting project
  96 [INFO] [secrets] [2022-11-07T04:15:20Z] ► Analyzer will attempt to analyze all projects in the repository
  97 [INFO] [secrets] [2022-11-07T04:15:20Z] ► Running analyzer
  98 [INFO] [secrets] [2022-11-07T04:15:20Z] ►
  99 [INFO] [secrets] [2022-11-07T04:15:20Z] ►   o
 100 [INFO] [secrets] [2022-11-07T04:15:20Z] ►   |\ 
 101 [INFO] [secrets] [2022-11-07T04:15:20Z] ►   | o
 102 [INFO] [secrets] [2022-11-07T04:15:20Z] ►   o
 103 [INFO] [secrets] [2022-11-07T04:15:20Z] ►     gitleaks
 104 [INFO] [secrets] [2022-11-07T04:15:20Z] ►
 105 [INFO] [secrets] [2022-11-07T04:15:24Z] ► 4:15AM INF scan completed in 4.16s
 106 [INFO] [secrets] [2022-11-07T04:15:24Z] ► 4:15AM WRN leaks found: 8
 107 [INFO] [secrets] [2022-11-07T04:15:24Z] ► Creating report
✓ 109 Uploading artifacts for successful job
```

# Pre-Stage

```
87 SKIPPING GIT SUBMODULES SETUP
88
89 Executing "step_script" stage of the job script
90 $ ./analyzer run
91 [INFO] [Semgrep] [2022-11-07T04:15:18Z] ► GitLab Semgrep analyzer v3.8.0
92 [INFO] [Semgrep] [2022-11-07T04:15:18Z] ► Detecting project
93 [INFO] [Semgrep] [2022-11-07T04:15:18Z] ► Analyzer will attempt to analyze all projects in the repository
94 [INFO] [Semgrep] [2022-11-07T04:15:18Z] ► Running analyzer
95 [INFO] [Semgrep] [2022-11-07T04:15:41Z] ► Creating report
96 [INFO] [Semgrep] [2022-11-07T04:15:41Z] ► /tmp/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-3/gl-sast-report-post.json written
98 Uploading artifacts for successful job
```

```
95 [INFO] [Spotbugs] [2022-11-07T04:15:21Z] ► GitLab Spotbugs analyzer v3.3.0
96 [INFO] [Spotbugs] [2022-11-07T04:15:21Z] ► Detecting project
97 [WARN] [Spotbugs] [2022-11-07T04:15:21Z] ► No match in /tmp/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/resul
98 /tmp/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-3/gl-sast-report-post.json
```

# Prepare-Stage

prepare



prepare-job: [\$CI\_PROJECT\_NAME, \$WORKING\_DI...

```
39 Skipping Git submodules setup
41 Downloading artifacts
42 Downloading artifacts for gemnasium-dependency_scanning (393142)...
43 Downloading artifacts from coordinator... ok          id=393142 responseStatus=200 OK token=o_dR2ee
44 WARNING: gl-sbom-npm-npm.cdx.json: lchown gl-sbom-npm-npm.cdx.json: operation not permitted (suppressing repeats)
46 Executing "step_script" stage of the job script
47 $ export VARIABLE_NAME=ROLE_ARN
48 $ if [ -z "$($eval echo $$VARIABLE_NAME)" ]; then echo "$VARIABLE_NAME must be set. $CUSTOM_MSG" && exit 1; fi
49 $ STS=$(aws sts assume-role-with-web-identity \ # collapsed multi-line command
50 $ export VARIABLE_NAME=AGENCY
51 $ if [ -z "$($eval echo $$VARIABLE_NAME)" ]; then echo "$VARIABLE_NAME must be set. $CUSTOM_MSG" && exit 1; fi
52 $ export VARIABLE_NAME=PROJECT
53 $ if [ -z "$($eval echo $$VARIABLE_NAME)" ]; then echo "$VARIABLE_NAME must be set. $CUSTOM_MSG" && exit 1; fi
54 $ echo -e "section_start:`date +%s`:init_ecr[collapsed=true]\r\ne[0KInitialise AWS ECR Repository"
> 55 Initialise AWS ECR Repository
```

00:01

00:05

00:02

# Build-Stage

build



build-job: [\$CI\_PROJECT\_NAME, \$WORKING\_DIR, ...

```
302 70bacb435c26ae3cebb902b34f7130a523ee8d0c-53010: digest: sha256:60ee601d47c8cee5070f8d34da92dc6ab687e71b79d6215eae60a9c40b4e7e6  
6 size: 3042  
303 $ docker save $DOCKER_TARGET_REGISTRY/$DOCKER_TARGET_IMAGE > $OUTPUT_IMAGE_ARTEFACT  
304 $ mkdir -p ./build-image-job/  
305 $ echo "OUTPUT_IMAGE_ARTEFACT=$OUTPUT_IMAGE_ARTEFACT;" > ./build-image-job/env_$PRODUCT_IMAGE_NAME.sh  
306 $ chmod +x ./build-image-job/env_$PRODUCT_IMAGE_NAME.sh  
308 Uploading artifacts for successful job  
309 Uploading artifacts...  
310 result-testing-3.tar: found 1 matching files and directories  
311 ./build-image-job/env_result-testing-3.sh: found 1 matching files and directories  
312 Uploading artifacts as "archive" to coordinator... 201 Created id=393146 ntoken=K5CT_H-z Using Custom Setup token=K5CT_H-z
```

00:10

# Sign-Stage

sign

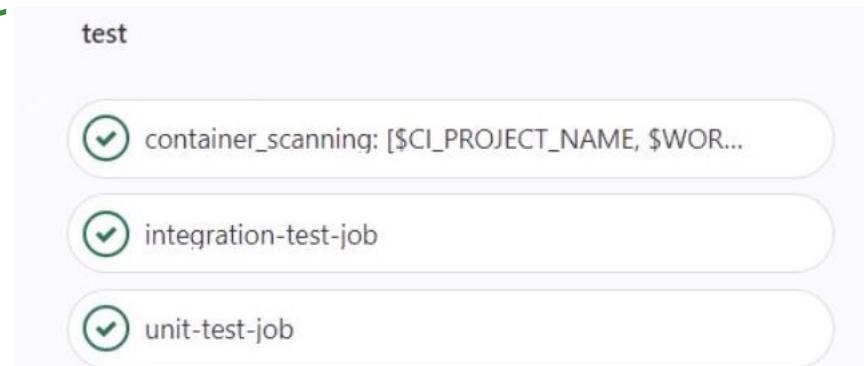


sign-container-job: [\$CI\_PROJECT\_NAME, \$WORK...

```
53 $ if [ -n "$COSIGN_KEY" ]; then # collapsed multi-line command
54 Private key written to cosign.key
55 Public key written to cosign.pub
56 WARNING: Image reference registry.sgts.gitlab-dedicated.com/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-
3:7bacb435c26ae3cebb902b34f7130a523ee8d0c-53010 uses a tag, not a digest, to identify the image to sign.
57 This can lead you to sign a different image than the intended one. Please use a
58 digest (example.com/ubuntu@sha256:abc123...) rather than tag
59 (example.com/ubuntu:latest) for the input to cosign. The ability to refer to
60 images by tag will be removed in a future release.
61 Pushing signature to: registry.sgts.gitlab-dedicated.com/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-3
62
63 Uploading artifacts for successful job
```

00:01

# Test-Stage



```
18 Skipping Git submodules setup
✓ 20 Executing "step_script" stage of the job script 00:11
21 Using docker image sha256:f89e06552ceb36788979a8240f7ae34410cfcc5edd5e82b8a46e491cc84373b2 for registry.gitlab.com/security-products/container-scanning/grype:5 with digest registry.gitlab.com/security-products/container-scanning/grype@sha256:92b026c24b82abce1513a9d544358404ca86bd4ee4d4de708311051d1242c25b ...
2 $ gtcs scan
23 [INFO] [2022-11-07 04:20:28 +0000] [container-scanning] > Scanning container from registry registry.sgts.gitlab-dedicated.com/wog/gvt/ship/stack-attendees/sgts-trainee-group-0/result-testing-3:70bacb435c26ae3cebb902b34f7130a523ee8d0c-53010 for vulnerabilities with severity level UNKNOWN or higher, with gcs 5.2.4 and Grype Version: 0.59.2 advisories updated at 2022-11-06T08:18:58+00:00
```

Using Custom Setup

# Test-Stage

```
-----+
882 | Unapproved | Critical GHSA-qm95-pgcg-qqfq | socket.io-parser | 3.4.1 | Insufficient validation when
decoding a Socket.IO packet |
883 +-----+-----+-----+
-----+
885 Uploading artifacts for successful job 00:03
886 Unloading artifacts
887 gl-container-scanning-report.json: found 1 matching files and directories
888 gl-dependency-scanning-report.json: found 1 matching files and directories
889 Uploading artifacts as "archive" to coordinator... 201 Created id=393148 responseStatus=201 Created token=P-smpBEW
890 Uploading artifacts...
891 gl-container-scanning-report.json: found 1 matching files and directories
892 Uploading artifacts as "container_scanning" to coordinator... 201 Created id=393148 responseStatus=201 Created token=P-smpBEW
893 Uploading artifacts...
894 gl-dependency-scanning-report.json: found 1 matching files and directories
895 Uploading artifacts as "dependency_scanning" to coordinator... 201 Created id=393148 responseStatus=201 Created token=P-smpBEW
```

# Test-Stage | Integration-test

```
22 Skipping Git submodules setup
✓ 24 Downloading artifacts 00:04
25 Downloading artifacts for build-job: [$CI_PROJECT_NAME, $WORKING_DIR, $CI_COMMIT_SHA-$CI_PIPELINE_ID, Dockerfile] (393146)...
26 Downloading artifacts from coordinator... ok      id=393146 responseStatus=200 OK token=HdtYxxnH
27 WARNING: build-image-job/env_result-testing-3.sh: lchown build-image-job/env_result-testing-3.sh: operation not permitted (sup
    pressing repeats)
✓ 29 Executing step_script stage of the job script 00:01
30 $ echo "Integration test"
31 Integration test
✓ 33 Cleaning up project directory and file based variables 00:00
```

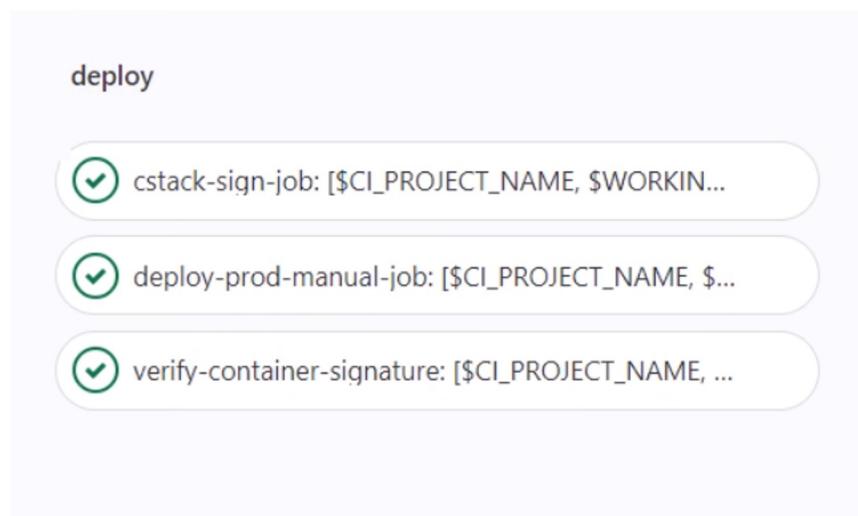
Using Custom Setup

# Test-Stage | Unit-test

```
25 Downloading artifacts for build-job: [$CI_PROJECT_NAME, $WORKING_DIR, $CI_COMMIT_SHA-$CI_PIPELINE_ID, Dockerfile] (393146)...
26 Downloading artifacts from coordinator... ok      id=393146 responseStatus=200 OK token=MXFBSzet
27 WARNING: build-image-job/env_result-testing-3.sh: lchown build-image-job/env_result-testing-3.sh: operation not permitted (sup
     pressing repeats)
29 Executing "step script" stage of the job script
30 $ echo "Unit test"
31 Unit test
33 Cleaning up project directory and file based variables
```

Using Custom Setup

# Deploy-Stage



# Deploy-Stage

```
17 DOCKER_PASSWORD: $AWS_ECR_TOKEN
18
19 build-and-push-docker-image:
20   image:
21     name: gcr.io/kaniko-project/executor:debug
22     entrypoint: []
23   tags:
24     - ship_docker
25   variables:
26     DOCKERFILE_PATH: "./"
27     DOCKERFILE_NAME: "Dockerfile"
28     DIGESTFILE_NAME: "$CI_PROJECT_DIR/digest"
29     OPTS: ""
30   script:
31     - export VARIABLE_NAME=DOCKER_TARGET_REGISTRY
32     - !reference [.check-variable-sh, script]
33     - export VARIABLE_NAME=DOCKER_TARGET_IMAGE
34     - !reference [.check-variable-sh, script]
35     - !reference [.check-docker-auth-config-sh, script]
36     - export DOCKER_CONFIG=~/.docker/
37     - /kaniko/executor --context "$DOCKERFILE_PATH" --dockerfile "$DOCKERFILE_PATH/$DOCKERFILE_NAME" --destination "$DOCKER_TARGET_REGISTRY/$DOC
38 artifacts:
39   paths:
40     - $DIGESTFILE_NAME
41   expire_in: 1 week
42
```

# Deploy-Stage

```
35 $ if [ -f "$HOME/.docker/config.json" ]; then # collapsed multi-line command
36   # cosign verify --key cosign.pub $DOCKER_REGISTRY/$IMAGE_NAME:$IMAGE_VERSION
37   # verification for Registry.sgts.gvttech.dedicated.com:40443/sgts-trainee-group-0/result-testing-3:70bacb4
38   # 35c26ae3cebb902b34f7130a523ee8d0c-53010 --
39   # The following checks were performed on each of these signatures:
40   #
```

# Post-Stage

.post



delete-testing-image-job: [\$CI\_PROJECT\_NAME, \$...



```
delete-testing-image-job: # delete image for testing from TEST_REGISTRY
  stage: .post
  extends: .delete-gitlab-cr-image
  variables:
    IMAGE_NAME: ""
    IMAGE_VERSION: $VERSION
  when: always
  allow_failure: true
  parallel:
    -
```

# Post-Stage

```

48 $ if [ -z "$(eval echo \$${VARIABLE_NAME})" ]; then echo "Expected $VARIABLE_NAME but not found in json. Unable to proceed. $CUSTOM_MSG" && exit 1; fi
49 $ DIGEST=$( curl --header "PRIVATE-TOKEN:$API_TOKEN" "https://$CI_SERVER_HOST/api/v4/projects/$CI_PROJECT_ID/registry/repositories/$REPOSITORY_ID/tags/$IMAGE_VERSION" | jq -r --arg VALUE "$IMAGE_VERSION" '. | select(.name | contains($VALUE)) | .digest' )
50 % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
51                                         Dload  Upload  Total  Spent   Left  Speed
52 0      0      0      0      0      0      0      0 --::--- --::--- --::--- 0
53 100  599  100  599  0      0      1035  0 --::--- --::--- --::--- 1034
54 $ curl --request DELETE --header "PRIVATE-TOKEN:$API_TOKEN" "https://$CI_SERVER_HOST/api/v4/projects/$CI_PROJECT_ID/registry/repositories/$REPOSITORY_ID/tags/$IMAGE_VERSION"
55 % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
56                                         Dload  Upload  Total  Spent   Left  Speed
57 100      3  100      3  0      0      16  0 --::--- --::--- --::--- 16
58 200$ CHECK_MESSAGE=$( curl --header "PRIVATE-TOKEN:$API_TOKEN" "https://$CI_SERVER_HOST/api/v4/projects/$CI_PROJECT_ID/registry/repositories/$REPOSITORY_ID/tags/$IMAGE_VERSION" | jq '. | select(.message != null) | .message' )
59 % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
60                                         Dload  Upload  Total  Spent   Left  Speed
61 0      0      0      0      0      0      0      0 --::--- --::--- --::--- 0
62 100  31  100  31  0      0      180  0 --::--- --::--- --::--- 181
63 $ if [ -z "$(eval echo \$${CHECK_MESSAGE})" ]; then echo "Failed to delete image." && exit 1; fi
64 $ curl --request DELETE --header "PRIVATE-TOKEN:$API_TOKEN" "https://$CI_SERVER_HOST/api/v4/projects/$CI_PROJECT_ID/registry/repositories/$REPOSITORY_ID/tags/${DIGEST/:/-}.sig"
65 % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
66                                         Dload  Upload  Total  Spent   Left  Speed

```

# Dependency Findings

	Project information
	Repository
	Issues 0
	Merge requests 0
	CI/CD
	Security & Compliance
	Security dashboard
	Vulnerability report
	On-demand scans
	Dependency list
	License compliance
	Policies
	Audit events
	Configuration
	Deployments
	Packages and registries

## Dependencies

Software Bill of Materials (SBOM) based on the [latest successful scan](#) • 3 months ago

Severity ▾

Component	Packager	Location	License
libtasn1-6 4.13-3		...e3cebb902b34f7130a523ee8d0c-53123	2 vulnerabilities detected
libdb5.3 5.3.28+dfsg1-0.5		...e3cebb902b34f7130a523ee8d0c-53123	1 vulnerability detected
socket.io-parser 3.3.2		...e3cebb902b34f7130a523ee8d0c-53123	1 vulnerability detected
libudev1 241-7~deb10u8		...e3cebb902b34f7130a523ee8d0c-53123	7 vulnerabilities detected
opener 1.5.2		...e3cebb902b34f7130a523ee8d0c-53123	4 vulnerabilities detected
libsystemd0 241-7~deb10u8		...e3cebb902b34f7130a523ee8d0c-53123	7 vulnerabilities detected
libtinfo6 6.1+20181013-2+deb10u2		...e3cebb902b34f7130a523ee8d0c-53123	2 vulnerabilities detected

# Security Findings

Last updated 3 months ago #53123

 1 failed security job



Status	Severity	Tool	Activity
Needs triage +1 more	All severities	All tools	All activity
Detected	Status	Severity	Description
<input type="checkbox"/>	2022-11-07	Needs Triage	 Critical Password in URL detected; please remove and revoke it if this is a leak. <a href="#">node_modules/pino/docs/transport.md:256</a>
<input type="checkbox"/>	2022-11-07	Needs Triage	 Critical Password in URL detected; please remove and revoke it if this is a leak. <a href="#">node_modules/pg-connection-string/README.md:20</a>
<input type="checkbox"/>	2022-11-07	Needs Triage	 Critical Password in URL detected; please remove and revoke it if this is a leak. <a href="#">node_modules/pg-pool/README.md:72</a>

# Compliance Framework

Automate adopting DevSecOps best practices based on industry pipeline security & IM8

Examples:

- SCA including Dependency scanning
- SAST / DAST / Container scanning
- Gating before deployment to high stake environments
- Reports generation as part of provenance
- Signing and verification of signature on artefacts
- Checksum verification of artefacts
- Use of artifactory

We will iteratively improve these to help you meet DevSecOps policy.

Highly recommended

# Compliance Framework

## Benefits

Set up CI/CD pipeline faster

Leverage GitLab's OTS security tools and reporting tools

Flexibility to change to **non-GitLab Alternative Tools** in 2.0

Better quality by achieving compliance to industry standards.

# Know your Resources: Activity

Bookmark [Learning Events](#) for past and upcoming events

Technical Documentation  
<https://go.gov.sg/ship-hats-docs>

Reach out to us at <https://go.gov.sg/she> for feedback, feature requests - we priorities based on demand!

# Thank You

