To integrate **#1 (Trivy image scanning)** and **#2 (Checkov for IaC scanning)** into your existing .gitlab-ci.ymlpipeline, you'll want to add **security scanning stages** before the Terraform stages. Here's the **updated version** with both tools integrated while preserving your original structure:

image:

name: registry.gitlab.com/gitlab-org/gitlab-build-images:terraform

entrypoint:

- '/usr/bin/env'

- 'PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin'

variables:

TF\_VAR\_gitlab\_token: ${GITLAB\_ACCESS\_TOKEN}

AWS\_ACCESS\_KEY\_ID: ${MY\_AWS\_KEY}

AWS\_SECRET\_ACCESS\_KEY: ${MY\_AWS\_ACCESS\_KEY}

AWS\_DEFAULT\_REGION: "us-east-1"

cache:

paths:

- .terraform

before\_script:

- terraform --version

- terraform init -backend-config="tfstate.config"

stages:

- security\_scan

- validate

- plan

- apply

- destroy

*# 1. Trivy Image Scan*

trivy\_scan:

stage: security\_scan

image: aquasec/trivy:latest

script:

- trivy image registry.gitlab.com/gitlab-org/gitlab-build-images:terraform

allow\_failure: true

tags:

- docker

*# 2. Checkov IaC Scan*

checkov\_scan:

stage: security\_scan

image: bridgecrew/checkov:latest

script:

- checkov -d .

allow\_failure: false

tags:

- docker

*# 3. TFSec IaC Scan*

tfsec\_scan:

stage: security\_scan

image: aquasec/tfsec:latest

script:

- tfsec .

allow\_failure: false

tags:

- docker

validate:

stage: validate

script:

- terraform validate

plan:

stage: plan

script:

- terraform plan -out="planfile"

dependencies:

- validate

artifacts:

paths:

- planfile

apply:

stage: apply

script:

- terraform apply -input=false "planfile"

dependencies:

- plan

when: manual

destroy:

stage: destroy

script:

- terraform destroy --auto-approve

when: manual

**🔍 Key Notes:**

* **trivy\_scan** scans the base image for vulnerabilities.
* **checkov\_scan** scans your Terraform code directory for security misconfigurations.
* Both are added as a new stage: security\_scan.
* allow\_failure: true for Trivy allows CI to continue even if it finds CVEs (optional).
* Ensure Docker runners are available (tags: [docker]) for container execution.