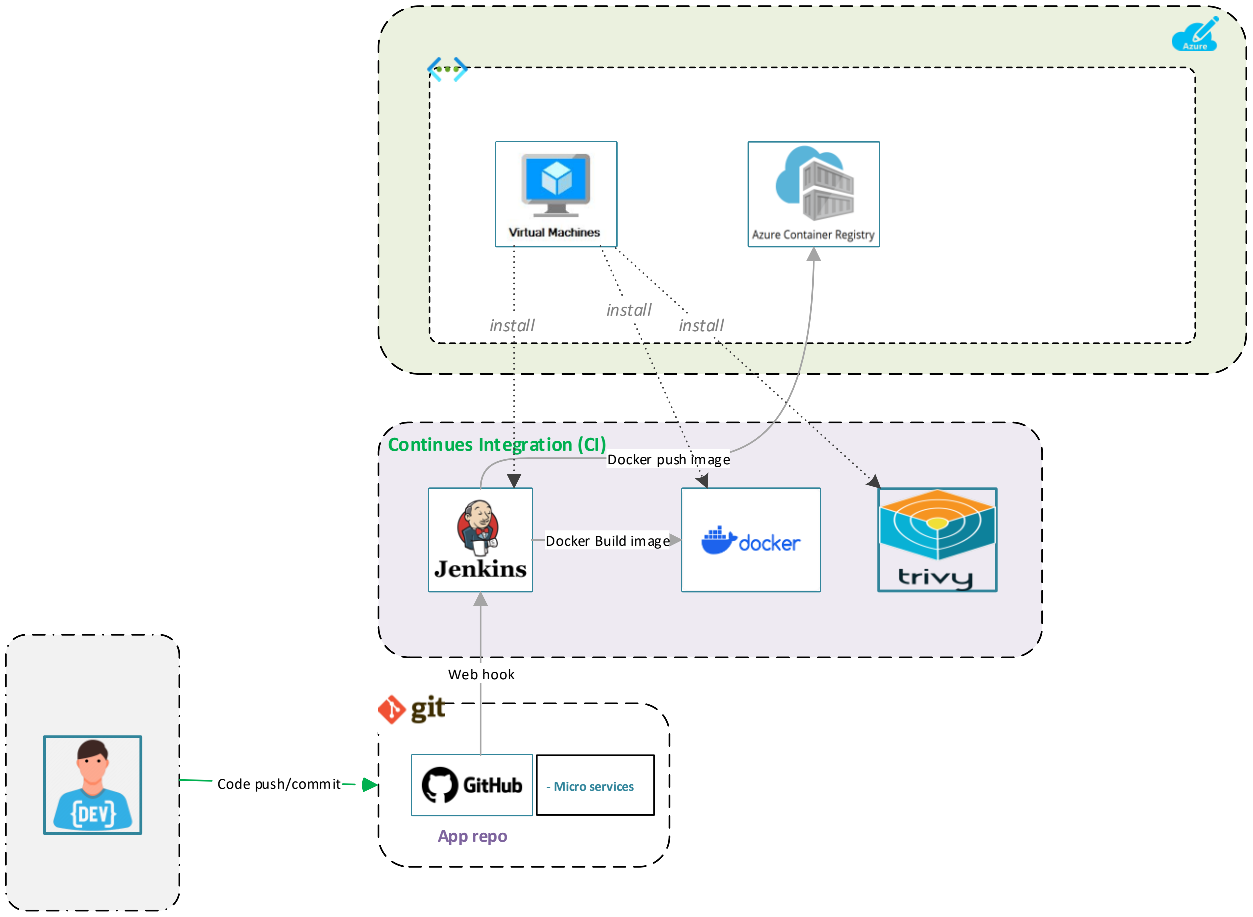
Overview

This document will help you to setup and demonstrate *Jenkins Groovy Pipeline* and use *Trivy* tool to scan for security as a part of the continues integration (CI).

This also demonstrates the CI flow (automatically trigger the CI flow when there is a code change is pushed to the Application code).



Prerequisites

- A virtual machine is provisioned with the Jenkins, Docker, Trivy installed from the ***2-PiSharpAssigment-SetupInfrastructure.docx***
- You are required to configure the Jenkins. Please refer to this guide https://www.cherryservers.com/blog/how-to-install-jenkins-on-ubuntu-22-04 *(starts from step #6: Set up Jenkins)*. While setup the Jenkins, please make sure the plugins below get installed:
    - Jenkins suggested plugins
    - Docker PipelineVersion
    - Pipeline Utility Steps
    - HTML Publisher
- An Azure Container Registry (ACR) is provided from the ***2-PiSharpAssigment-SetupInfrastructure.docx***
- Should clone or visit these source codes from GitHub for reference purposes.

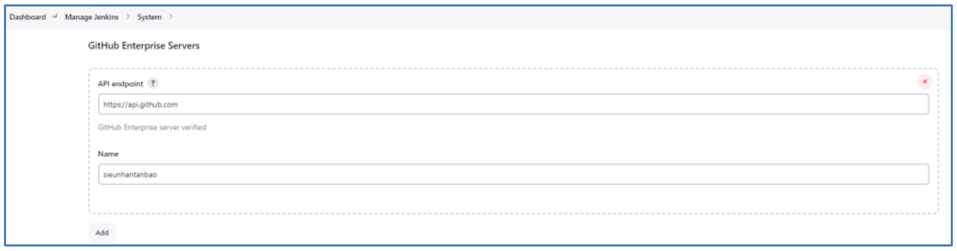
- DevOps CI with Jenkins Groovy: *git clone* *https://github.com/sieunhantanbao/sd2411-devops-ci.git*
- Application code: *git clone* *https://github.com/sieunhantanbao/sd2411_msa.git*

Works details

1. **Setup Jenkins Organization project**

   Login to the Jenkins (i.e. http://172.173.112.179:8080/)

- **Step 1**: Configure **GitHub Enterprise Servers**
  - Go to Manage Jenkins -> System -> GitHub Enterprise Servers
  - Add a new GitHub Enterprise Servers as below



Dashboard > Manage Jenkins > System >

GitHub Enterprise Servers

API endpoint ?

https://api.github.com

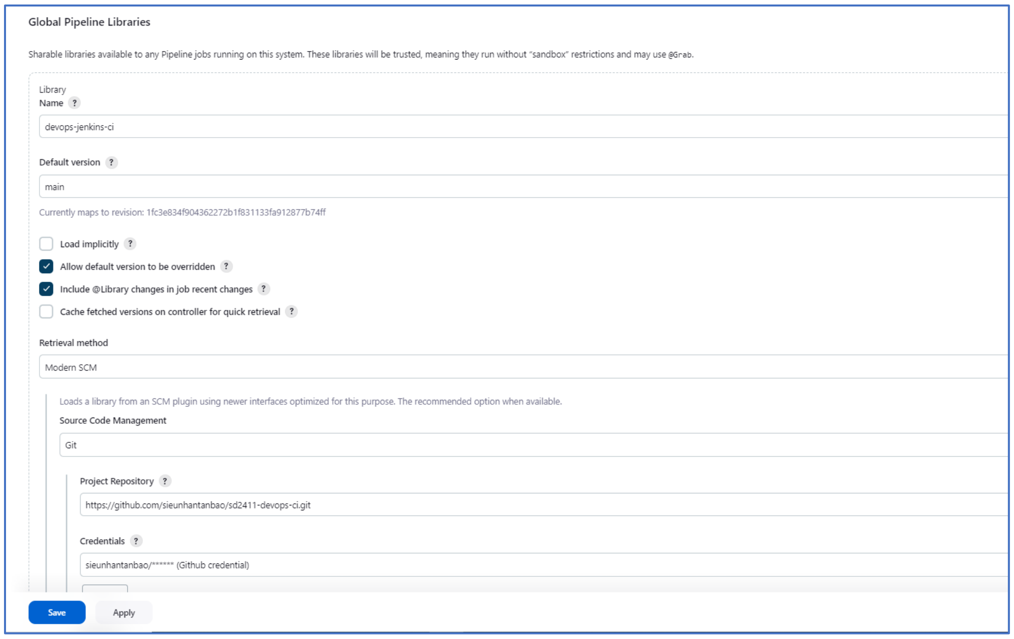
GitHub Enterprise server verified

Name

sieunhantanbao

    - API endpoint: https://api.github.com
    - Name: *<your GitHub account name>*

- **Step 2:** Configure **Global Pipeline Libraries**
  - Go to Manage Jenkins -> System -> Global Pipeline Libraries
  - Add a new Global Pipeline Libraries as below



Global Pipeline Libraries

Sharable libraries available to any Pipeline jobs running on this system. These libraries will be trusted, meaning they run without "sandbox" restrictions and may use @Grab.

Library

Name ?

devops-jenkins-ci

Default version ?

main

Currently maps to revision: 1fc3e834f904362272b1f831133fa912877b74ff

- ☐ Load implicitly ?
- ✓ Allow default version to be overridden ?
- ✓ Include @Library changes in job recent changes ?
- ☐ Cache fetched versions on controller for quick retrieval ?

Retrieval method

Modern SCM

Loads a library from an SCM plugin using newer interfaces optimized for this purpose. The recommended option when available.

Source Code Management

Git

Project Repository ?

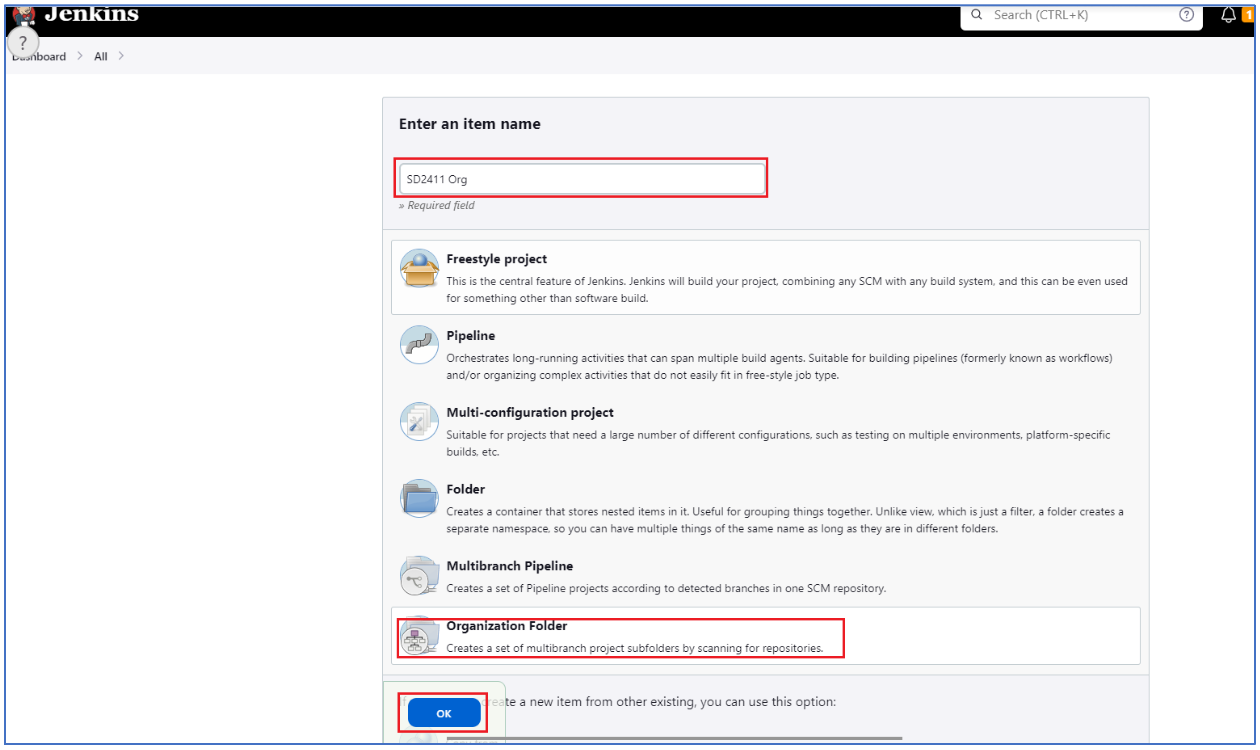
https://github.com/sieunhantanbao/sd2411-devops-ci.git

Credentials ?

sieunhantanbao/****** (Github credential)

    - Name: <any name that you want> // Please note it for later use.
    - Default version: main
    - Project repository: <URL of your git repository that contain the Jenkins Groovy scripts> // i.e. https://github.com/sieunhantanbao/sd2411-devops-ci.git
    - Credentials: <your github credentials> which is created in the Manage Jenkins -> Credentials.

- **Step 3**: Create **Organization Folder** project



Enter an item name

SD2411 Org

» Required field

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

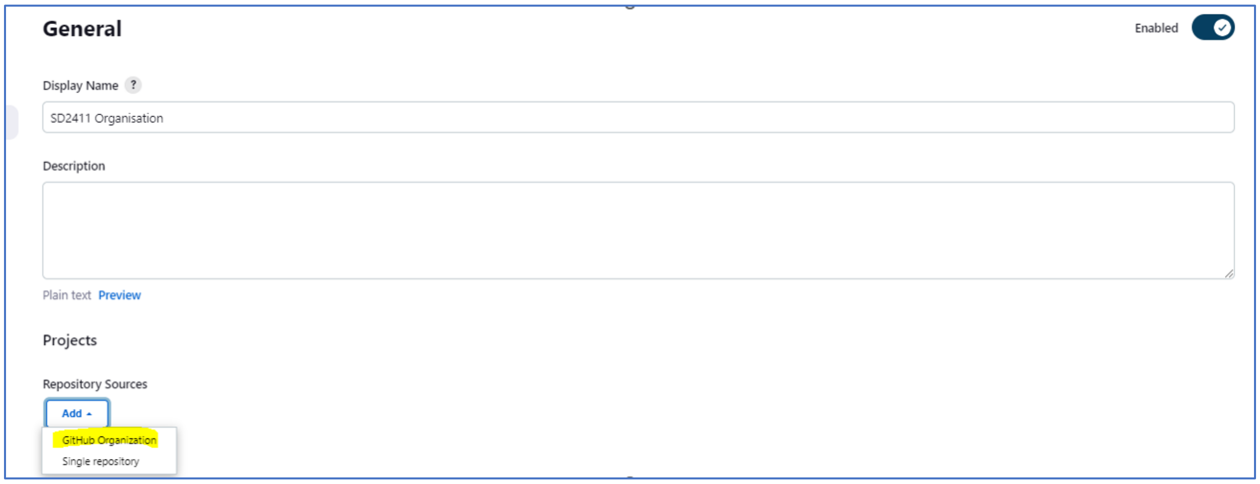
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

Multibranch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

Organization Folder
Creates a set of multibranch project subfolders by scanning for repositories.

…eate a new item from other existing, you can use this option:

- **Step 4**: Configure the Organization Folder as below



General

Enabled

Display Name: SD2411 Organisation

Description

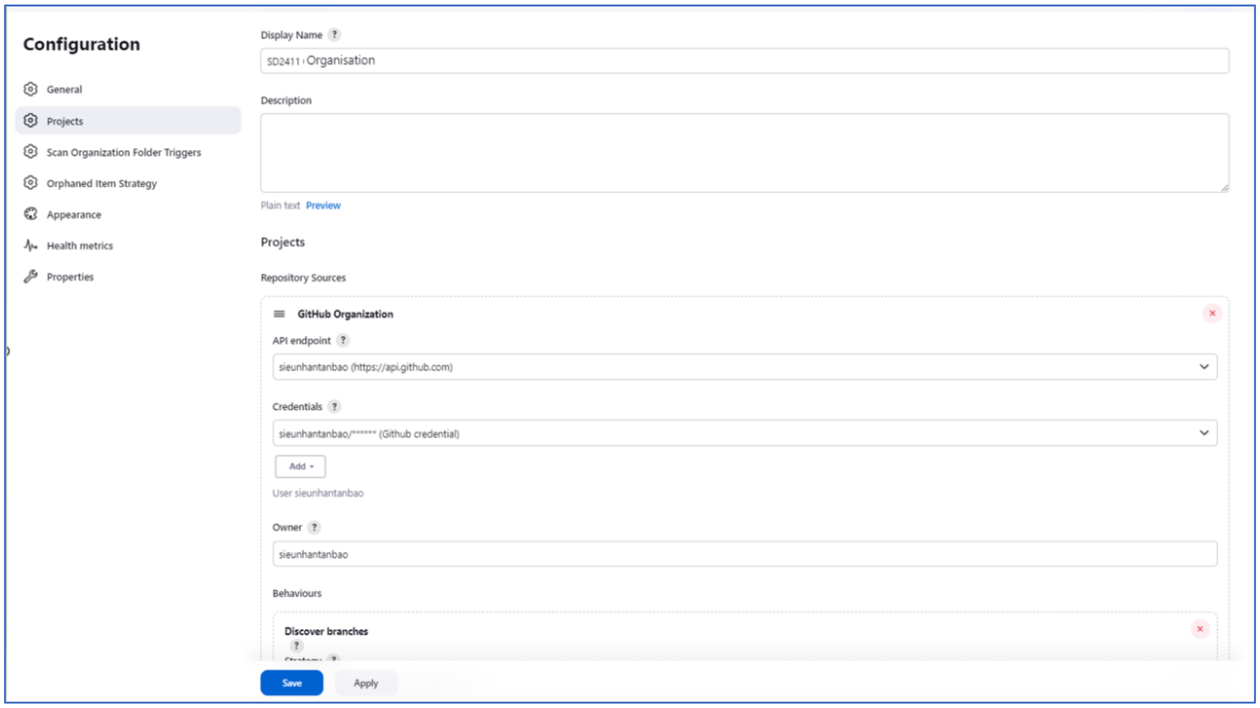
Plain text Preview

Projects

Repository Sources

Add

- GitHub Organization
- Single repository



Configuration

- General
- Projects
- Scan Organization Folder Triggers
- Orphaned Item Strategy
- Appearance
- Health metrics
- Properties

Display Name: SD2411 Organisation

Description

Plain text Preview

Projects

Repository Sources

GitHub Organization

API endpoint: sieunhantanbao (https://api.github.com)

Credentials: sieunhantanbao/****** (Github credential)

Add

User sieunhantanbao

Owner: sieunhantanbao

Behaviours

Discover branches

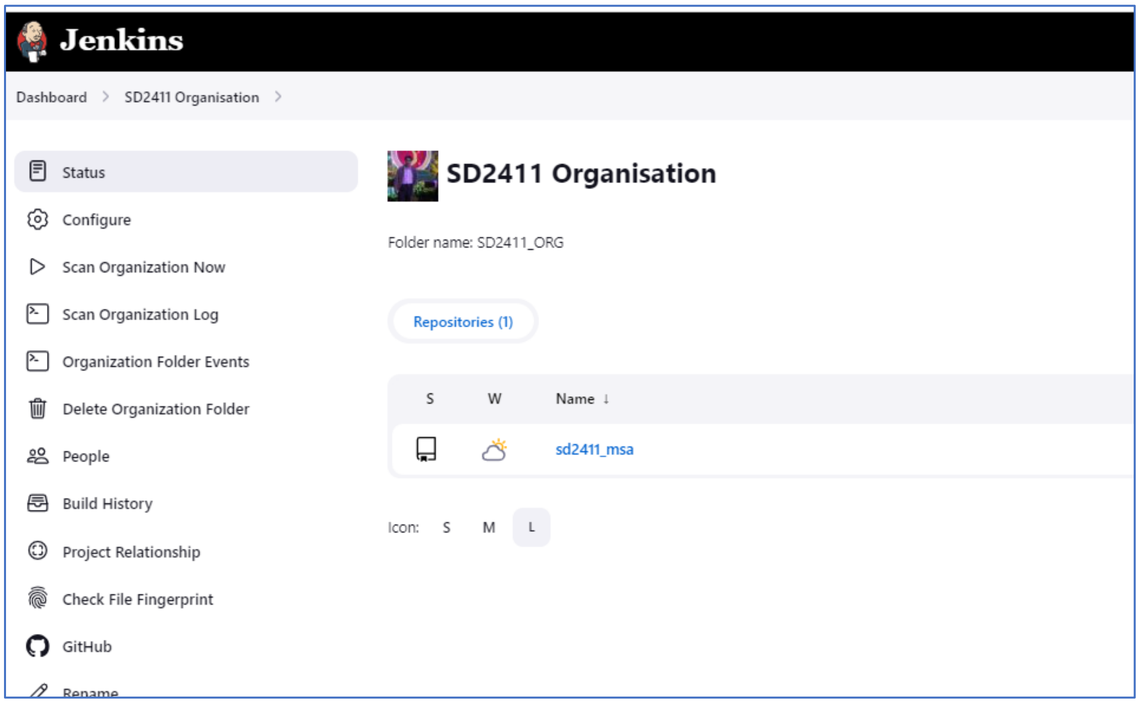
Save Apply

- Display Name: <Any name that you want or leave it as blank>
- API endpoint: select the **GitHub Enterprise Servers** that is created in step 1
- Credentials: <your github credentials> which is created in the Manage Jenkins -> Credentials.
- Owner: <your GitHub organization/ GitHub account>

=> After “Save” the Organization Folder project above. From the Jenkins home page:

- Click on: **SD2411 Organisation**
- Click on: **Scan Organization Now** *(from the left menu)*

- **Step 5**: Check the result/output. Confirm the **sd2411_msa** repository is added to your Organization Folder project



Jenkins

Dashboard > SD2411 Organisation >

SD2411 Organisation

Folder name: SD2411_ORG

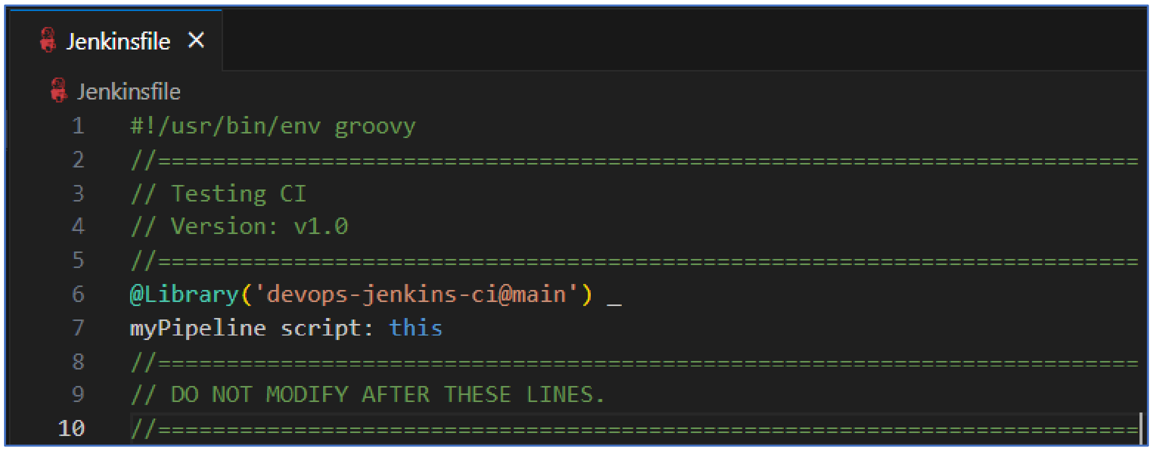
Repositories (1)

S	W	Name ↓
		sd2411_msa

Icon: S M L

2. Jenkins Groovy source code setup

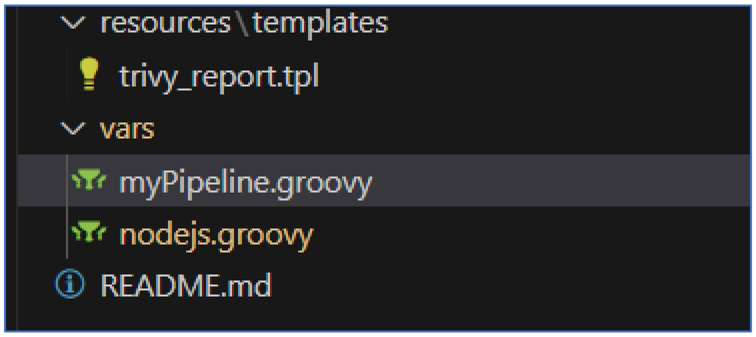
- From the Application source code (i.e. https://github.com/sieunhantanbao/sd2411_msa), in the root of the repository, create a Jenkins file with the following content



Jenkinsfile

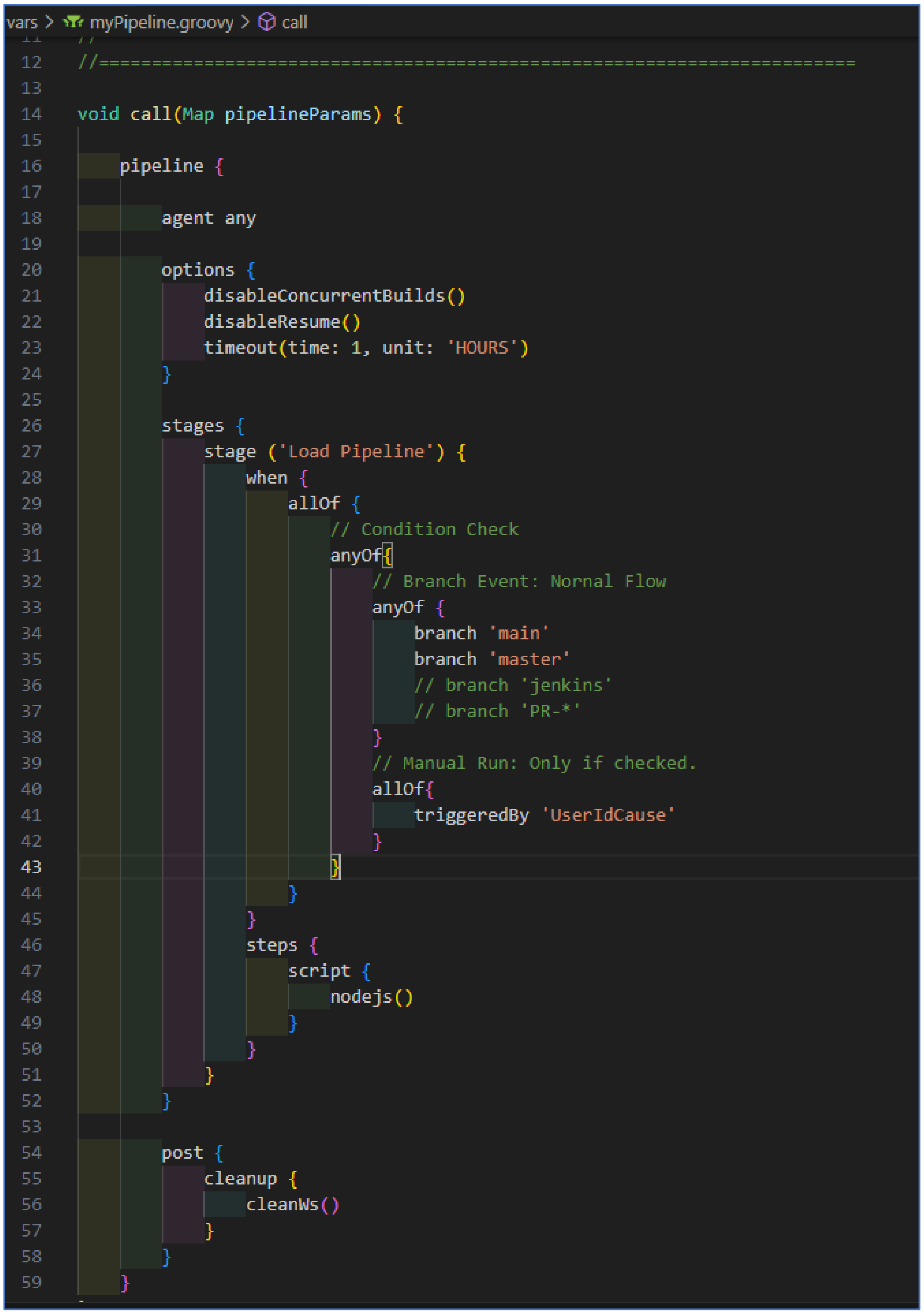
```groovy
#!/usr/bin/env groovy
//===========================================================================
// Testing CI
// Version: v1.0
//===========================================================================
@Library('devops-jenkins-ci@main') _
myPipeline script: this
//===========================================================================
// DO NOT MODIFY AFTER THESE LINES.
//===========================================================================
```

  - The '**devops-jenkins-ci**' is the name of the **Global Pipeline Libraries** that we have created earlier.
  - The '**main**' is the branch name of the devops-ci repository (https://github.com/sieunhantanbao/sd2411-devops-ci).
  - The '**myPipeline**' is the name of the Jenkins Groovy file in the devops-ci repository (https://github.com/sieunhantanbao/sd2411-devops-ci).
- From the devops-ci repository (i.e. https://github.com/sieunhantanbao/sd2411-devops-ci)
  - Source code structure



```
resources\templates
    trivy_report.tpl
vars
    myPipeline.groovy
    nodejs.groovy
README.md
```

- The **myPipeline.groovy** file

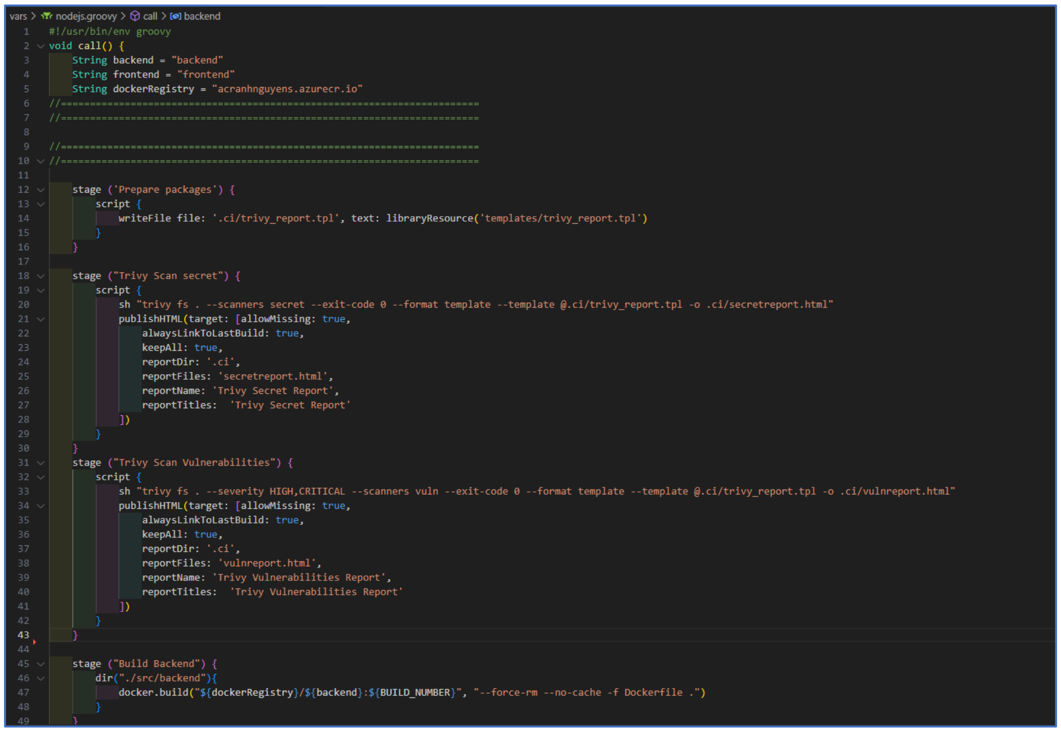


vars > myPipeline.groovy > call

```
//
//=========================================================================

void call(Map pipelineParams) {

    pipeline {

        agent any

        options {
            disableConcurrentBuilds()
            disableResume()
            timeout(time: 1, unit: 'HOURS')
        }

        stages {
            stage ('Load Pipeline') {
                when {
                    allOf {
                        // Condition Check
                        anyOf{
                            // Branch Event: Nornal Flow
                            anyOf {
                                branch 'main'
                                branch 'master'
                                // branch 'jenkins'
                                // branch 'PR-*'
                            }
                            // Manual Run: Only if checked.
                            allOf{
                                triggeredBy 'UserIdCause'
                            }
                        }
                    }
                }
                steps {
                    script {
                        nodejs()
                    }
                }
            }
        }

        post {
            cleanup {
                cleanWs()
            }
        }
    }
```

- This file will be called from the Jenkins file when having any changes are made to the main/master branches of the application source code.
- This file will call the nodejs.groovy file to run the stages (details of the steps).

- The **nodejs.groovy** file



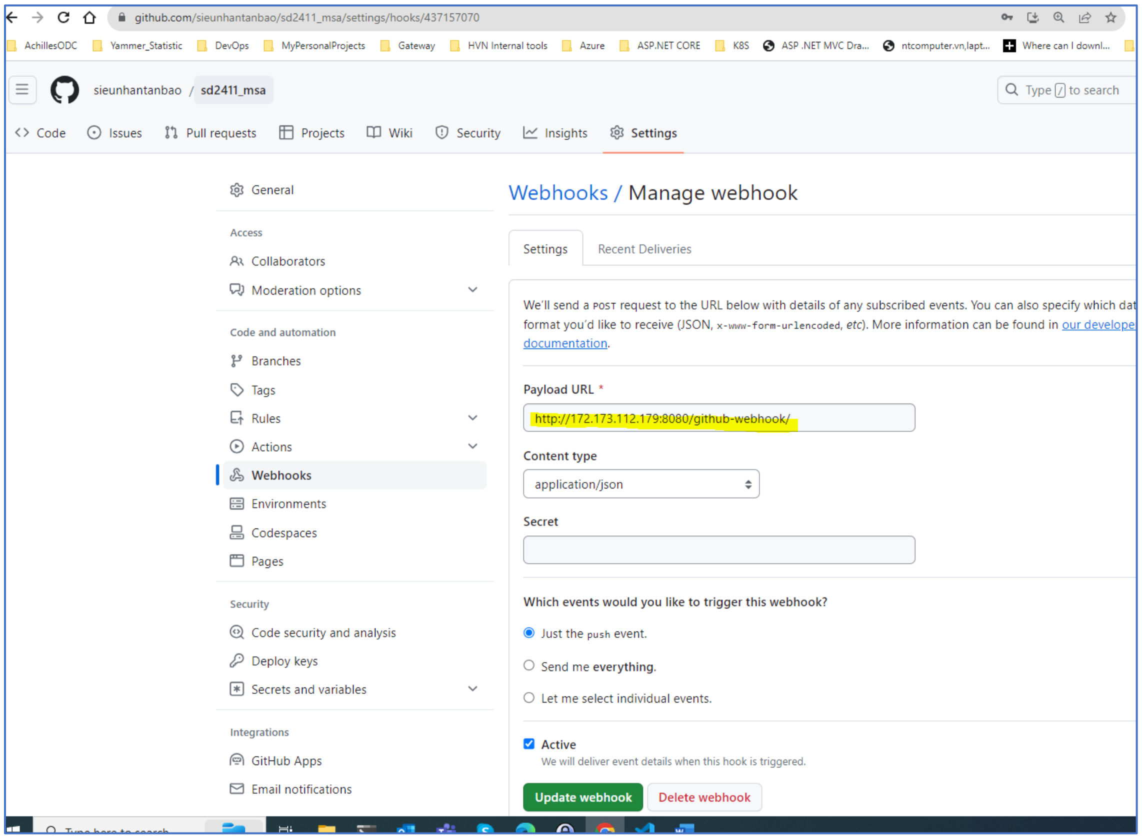
vars > nodejs.groovy > call > backend

```groovy
#!/usr/bin/env groovy
void call() {
    String backend = "backend"
    String frontend = "frontend"
    String dockerRegistry = "acranhnguyens.azurecr.io"
//========================================================================
//========================================================================

//========================================================================
//========================================================================

    stage ('Prepare packages') {
        script {
            writeFile file: '.ci/trivy_report.tpl', text: libraryResource('templates/trivy_report.tpl')
        }
    }

    stage ("Trivy Scan secret") {
        script {
            sh "trivy fs . --scanners secret --exit-code 0 --format template --template @.ci/trivy_report.tpl -o .ci/secretreport.html"
            publishHTML(target: [allowMissing: true,
                alwaysLinkToLastBuild: true,
                keepAll: true,
                reportDir: '.ci',
                reportFiles: 'secretreport.html',
                reportName: 'Trivy Secret Report',
                reportTitles:  'Trivy Secret Report'
            ])
        }
    }
    stage ("Trivy Scan Vulnerabilities") {
        script {
            sh "trivy fs . --severity HIGH,CRITICAL --scanners vuln --exit-code 0 --format template --template @.ci/trivy_report.tpl -o .ci/vulnreport.html"
            publishHTML(target: [allowMissing: true,
                alwaysLinkToLastBuild: true,
                keepAll: true,
                reportDir: '.ci',
                reportFiles: 'vulnreport.html',
                reportName: 'Trivy Vulnerabilities Report',
                reportTitles:  'Trivy Vulnerabilities Report'
            ])
        }
    }

    stage ("Build Backend") {
        dir("./src/backend"){
            docker.build("${dockerRegistry}/${backend}:${BUILD_NUMBER}", "--force-rm --no-cache -f Dockerfile .")
        }
    }
```

- Full detail can be found here https://github.com/sieunhantanbao/sd2411-devops-ci/blob/main/vars/nodejs.groovy
- This contains the list of build stages
  - Prepare packages: Copy the trivy report template (trivy_report.tpl) from the **resources/templates** to the **.ci** folder. This template is used for Trivy security and vulnerability reports.
  - Trivy Scan Secret: This stage is to use the Trivy command to scan the security from the application source code, and then export/publish the report to the Jenkins.
  - Trivy Scan Vulnerabilities: This stage is to use the Trivy command to scan the vulnerabilities from the application source code, and then export/publish the report to the Jenkins.
  - Build Backend: This stage is using the docker to build the image for the **backend** service of the application code.
  - Build Frontend: This stage is using the docker to build the image for the **frontend** service of the application code.
  - Push Docker Images to ACR – backend: This stage is pushing the **backend** image to the Azure Container Registry (ACR).
  - Push Docker Images to ACR – frontend: This stage is pushing the **frontend** image to the Azure Container Registry (ACR).
  - Clean up docker images: This stage is to clear all local docker images created in the Build Backend and Build Frontend in the Virtual Machine (build agent).
- Please be notified that you need to create a Jenkins credential (i.e. **acrcredential**) to allow pushing the docker images to the ACR.

- **<u>TODO:</u>** This should include some stages for checking Unit Test and SonarQube scan the quality of the application source code.

3. **Setup webhooks**



github.com/sieunhantanbao/sd2411_msa/settings/hooks/437157070

sieunhantanbao / sd2411_msa

Code · Issues · Pull requests · Projects · Wiki · Security · Insights · Settings

General

Access: Collaborators, Moderation options

Code and automation: Branches, Tags, Rules, Actions, Webhooks, Environments, Codespaces, Pages

Security: Code security and analysis, Deploy keys, Secrets and variables

Integrations: GitHub Apps, Email notifications

Webhooks / Manage webhook

Settings | Recent Deliveries

We'll send a POST request to the URL below with details of any subscribed events. You can also specify which dat format you'd like to receive (JSON, x-www-form-urlencoded, *etc*). More information can be found in our develope documentation.

Payload URL *: http://172.173.112.179:8080/github-webhook/

Content type: application/json

Secret:

Which events would you like to trigger this webhook?

- (●) Just the push event.
- ( ) Send me **everything**.
- ( ) Let me select individual events.

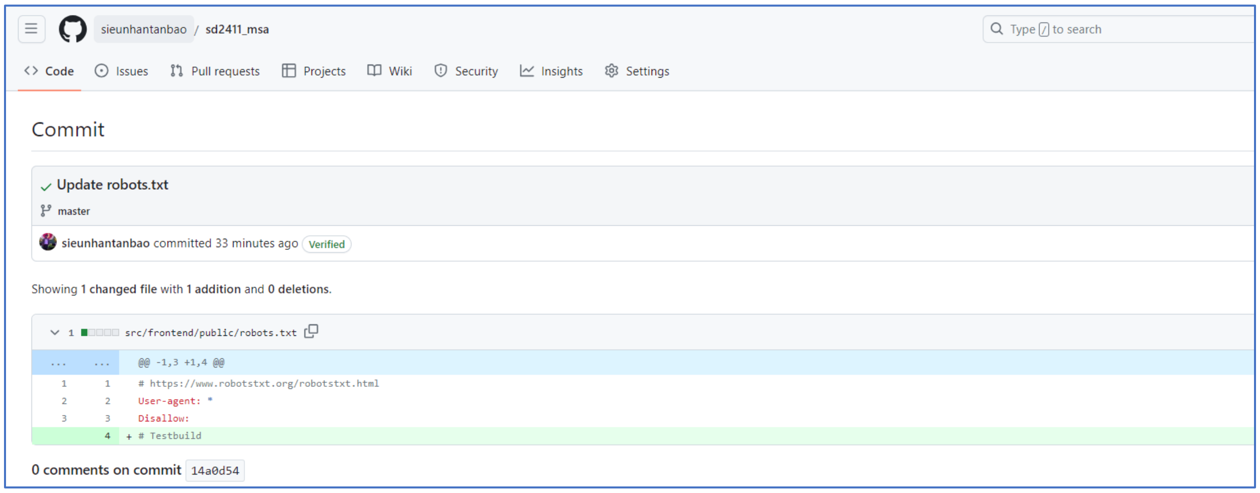
[✓] Active — We will deliver event details when this hook is triggered.

Update webhook | Delete webhook

From the GitHub of the Application Code (i.e. https://github.com/sieunhantanbao/sd2411_msa). Click on **Settings** -> **Webhooks**. Then input the URL of the Jenkins (i.e http://172.173.112.179:8080/github-webhook/). This is to make sure that if there is any change in this source code, it will make a call to the Jenkins (webhooks) to trigger the CI flow.

4. **Demonstration**

When there is a change in the App source code



sieunhantanbao / sd2411_msa

Code · Issues · Pull requests · Projects · Wiki · Security · Insights · Settings

Commit

✓ Update robots.txt

master

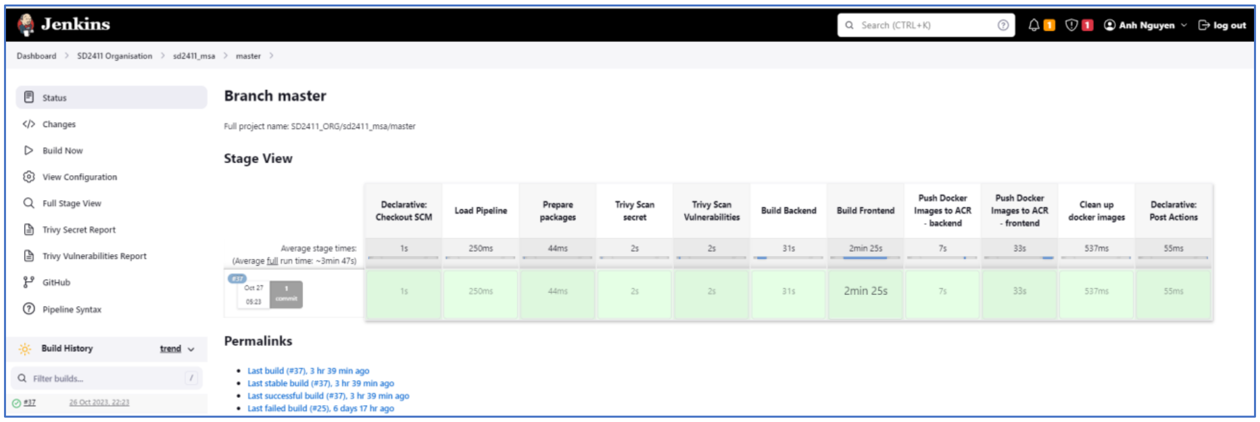
sieunhantanbao committed 33 minutes ago Verified

Showing **1 changed file** with **1 addition** and **0 deletions**.

```
1 src/frontend/public/robots.txt
@@ -1,3 +1,4 @@
  # https://www.robotstxt.org/robotstxt.html
  User-agent: *
  Disallow:
+ # Testbuild
```

0 comments on commit 14a0d54

The Jenkins job is triggered and run successfully



Branch master

Full project name: SD2411_ORG/sd2411_msa/master

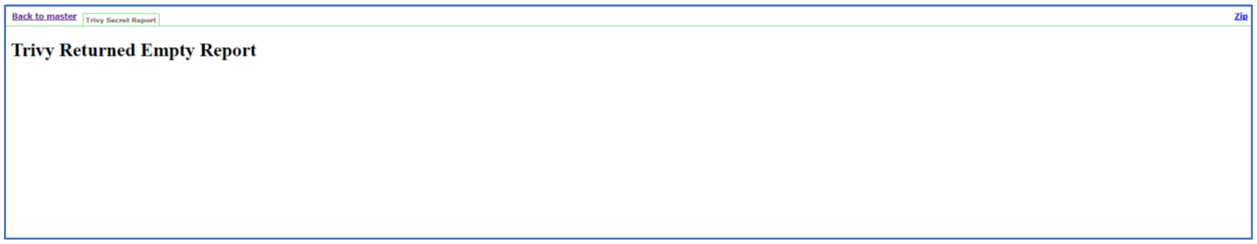
Stage View

	Declarative: Checkout SCM	Load Pipeline	Prepare packages	Trivy Scan secret	Trivy Scan Vulnerabilities	Build Backend	Build Frontend	Push Docker Images to ACR - backend	Push Docker Images to ACR - frontend	Clean up docker images	Declarative: Post Actions
Average stage times: (Average full run time: ~3min 47s)	1s	250ms	44ms	2s	2s	31s	2min 25s	7s	33s	537ms	55ms
#37 Oct 27 05:23 1 commit	1s	250ms	44ms	2s	2s	31s	2min 25s	7s	33s	537ms	55ms

Permalinks

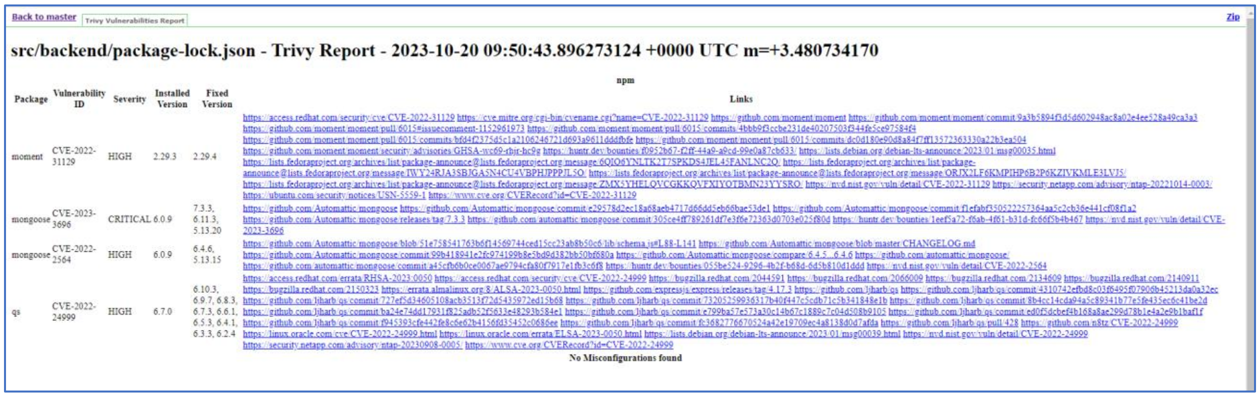
- Last build (#37), 3 hr 39 min ago
- Last stable build (#37), 3 hr 39 min ago
- Last successful build (#37), 3 hr 39 min ago
- Last failed build (#25), 6 days 17 hr ago

Check the security report



Trivy Returned Empty Report

Check the vulnerability report



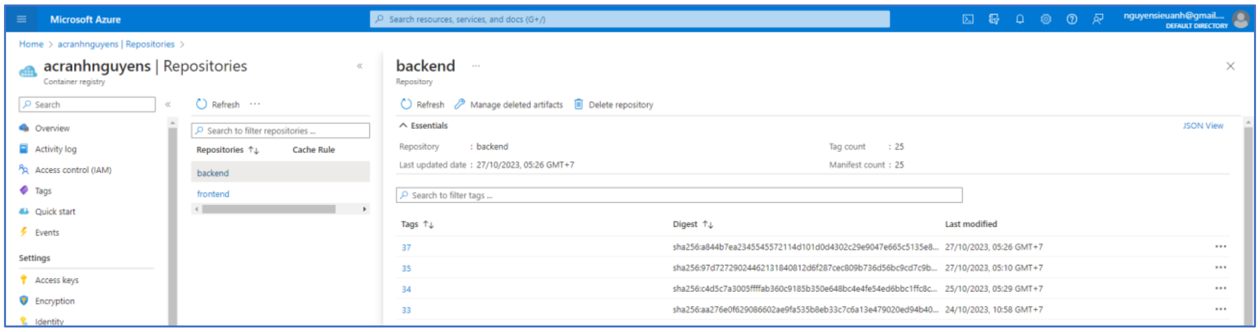
src/backend/package-lock.json - Trivy Report - 2023-10-20 09:50:43.896273124 +0000 UTC m=+3.480734170

npm

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
moment	CVE-2022-31129	HIGH	2.29.3	2.29.4	https://access.redhat.com/security/cve/CVE-2022-31129 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31129 https://github.com/moment/moment https://github.com/moment/moment/commit/9a3b5894f3d5d602948ac8a02e4ee528a49ca3a3 https://github.com/moment/moment/pull/6015#issuecomment-1152961973 https://github.com/moment/moment/pull/6015/commits/4bbb9f3ccbe231de40207503f344fe5ce97584f4 https://github.com/moment/moment/pull/6015/commits/bfd4f2375d5c1a2106246721d693a9611dddfbfe https://github.com/moment/moment/pull/6015/commits/dc0d180e90d8a84f7ff13572363330a22b3ea504 https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g https://huntr.dev/bounties/f0952b67-f2ff-44a9-a9cd-99e0a87cb633/ https://lists.debian.org/debian-lts-announce/2023/01/msg00035.html https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6QIO6YNLTK2T7SPKDS4JEL45FANLNC2Q/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/IWY24RJA3SBJGA5N4CU4VBPHJPPPJL5O/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ORJX2LF6KMPIHP6B2P6KZIVKMLE3LVJ5/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ZMX5YHELQVCGKKQVFXIYOTBMN23YYSRO/ https://nvd.nist.gov/vuln/detail/CVE-2022-31129 https://security.netapp.com/advisory/ntap-20221014-0003/ https://ubuntu.com/security/notices/USN-5559-1 https://www.cve.org/CVERecord?id=CVE-2022-31129
mongoose	CVE-2023-3696	CRITICAL	6.0.9	7.3.3, 6.11.3, 5.13.20	https://github.com/Automattic/mongoose https://github.com/Automattic/mongoose/commit/e29578d2ec18a68aeb4717d66dd5eb66bae53de1 https://github.com/Automattic/mongoose/commit/f1efabf350522257364aa5c2cb36e441cf08f1a2 https://github.com/Automattic/mongoose/releases/tag/7.3.3 https://github.com/automattic/mongoose/commit/305ce4ff789261df7e3f6e72363d0703e025f80d https://huntr.dev/bounties/1eef5a72-f6ab-4f61-b31d-fc66f5b4b467 https://nvd.nist.gov/vuln/detail/CVE-2023-3696
mongoose	CVE-2022-2564	HIGH	6.0.9	6.4.6, 5.13.15	https://github.com/Automattic/mongoose/blob/51e758541763b6f14569744ced15cc23ab8b50c6/lib/schema.js#L88-L141 https://github.com/Automattic/mongoose/blob/master/CHANGELOG.md https://github.com/Automattic/mongoose/commit/99b418941e2fc974199b8e5bd9d382bb50bf680a https://github.com/Automattic/mongoose/compare/6.4.5...6.4.6 https://github.com/automattic/mongoose/ https://github.com/automattic/mongoose/commit/a45cfb6b0ce0067ae9794cfa80f7917e1fb3c6f8 https://huntr.dev/bounties/055be524-9296-4b2f-b68d-6d5b810d1ddd https://nvd.nist.gov/vuln/detail/CVE-2022-2564
qs	CVE-2022-24999	HIGH	6.7.0	6.10.3, 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, 6.2.4	https://access.redhat.com/errata/RHSA-2023:0050 https://access.redhat.com/security/cve/CVE-2022-24999 https://bugzilla.redhat.com/2044591 https://bugzilla.redhat.com/2066009 https://bugzilla.redhat.com/2134609 https://bugzilla.redhat.com/2140911 https://bugzilla.redhat.com/2150323 https://errata.almalinux.org/8/ALSA-2023-0050.html https://github.com/expressjs/express/releases/tag/4.17.3 https://github.com/ljharb/qs https://github.com/ljharb/qs/commit/4310742efbd8c03f6495f07906b45213da0a32ec https://github.com/ljharb/qs/commit/727ef5d34605108acb3513f72d5435972ed15b68 https://github.com/ljharb/qs/commit/73205259936317b40f447c5cdb71c5b341848e1b https://github.com/ljharb/qs/commit/8b4cc14cda94a5c89341b77e5fe435ec6c41be2d https://github.com/ljharb/qs/commit/ba24e74dd17931f825adb52f5633e48293b584e1 https://github.com/ljharb/qs/commit/e799ba57e573a30c14b67c1889c7c04d508b9105 https://github.com/ljharb/qs/commit/ed0f5dcbef4b168a8ae299d78b1e4a2e9b1baf1f https://github.com/ljharb/qs/commit/f945393cfe442fe8c6e62b4156fd35452c0686ee https://github.com/ljharb/qs/commit/fc3682776670524a42e19709ec4a8138d0d7afda https://github.com/ljharb/qs/pull/428 https://github.com/n8tz/CVE-2022-24999 https://linux.oracle.com/cve/CVE-2022-24999.html https://linux.oracle.com/errata/ELSA-2023-0050.html https://lists.debian.org/debian-lts-announce/2023/01/msg00039.html https://nvd.nist.gov/vuln/detail/CVE-2022-24999 https://security.netapp.com/advisory/ntap-20230908-0005/ https://www.cve.org/CVERecord?id=CVE-2022-24999

No Misconfigurations found

The docker images are published to Azure Container Registry (ACR).



backend

Repository

Repository : backend

Last updated date : 27/10/2023, 05:26 GMT+7

Tag count : 25

Manifest count : 25

Tags	Digest	Last modified
37	sha256:a844b7ea2345545572114d101d0d4302c29e9047e665c5135e8...	27/10/2023, 05:26 GMT+7
35	sha256:97d72729024462131840812d6f287cec809b736d56bc9cd7c9b...	27/10/2023, 05:10 GMT+7
34	sha256:c4d5c7a3005ffffab360c9185b350e648bc4e4fe54ed6bbc1ffc8c...	25/10/2023, 05:29 GMT+7
33	sha256:aa276e0f629086602ae9fa535b8eb33c7c6a13e479020ed94b40...	24/10/2023, 10:58 GMT+7