

Steps to create a Jenkins CI/CD Pipeline and use SonarQube to perform SAST:

1. Open up Jenkins Dashboard on localhost, port 8080, or whichever port it is at for you.

2. Run SonarQube in a Docker container using this command -

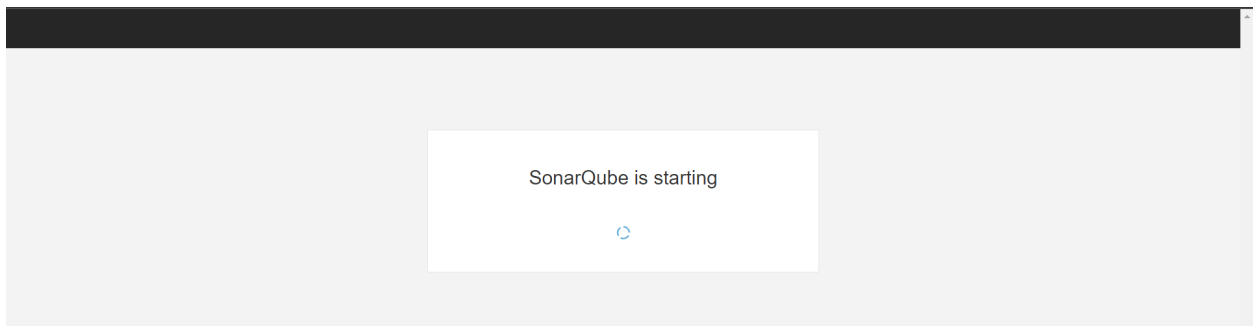
```
docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Mikil> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:lates
t
5d39cfd39cc2dcc0bdcad5f0111585930bda84d835a8c79f0ea0377c50a1de70
PS C:\Users\Mikil> |
```

3. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.



4. Login to SonarQube using username admin and password admin.

5. Create a manual project in SonarQube with the name sonarqube-test

sonarqube Projects Issues Rules Quality Profiles Qu

Create a project

All fields marked with * are required

Project display name *

 ✓

Up to 255 characters. Some scanners might override the value you provide.

Project key *

 ✓

The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.

Set Up


Set up the project and come back to Jenkins Dashboard.

6. Create a New Item in Jenkins, choose Pipeline.

Search (CTRL+K) ?


Enter an item name

» 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 namespace, so you can have multiple things of the same name as long as they are in different folders.

OK

7. Under Pipeline Script, enter the following -

```
node {
  stage('Cloning the GitHub Repo') {
```

```

    git 'https://github.com/shazforiot/GOL.git'
  }
  stage('SonarQube analysis') {
    withSonarQubeEnv('sonarqube') {
      sh
"/c/ProgramData/Jenkins/.jenkins/tools/hudson.plugins.sonar.SonarRunnerInstallation/sonarqube/bin/sonar-scanner \
-D sonar.login=admin \
-D sonar.password=mikami \
-D sonar.projectKey=demoapp-project \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://127.0.0.1:9000/"
    }
  }
}

```

Definition

Pipeline script

Script ?

```

1 node {
2   stage('Cloning the GitHub Repo') {
3     git 'https://github.com/shazforiot/GOL.git'
4   }
5   stage('SonarQube analysis') {
6     withSonarQubeEnv('sonarqube') {
7       sh "/c/ProgramData/Jenkins/.jenkins/tools/hudson.plugins.sonar.SonarRunnerInstallation/sonarqube/bin/sonar-scanner \
8         -D sonar.login=admin \
9         -D sonar.password=mikami \
10        -D sonar.projectKey=demoapp-project \
11        -D sonar.exclusions=vendor/**,resources/**,**/*.java \
12        -D sonar.host.url=http://127.0.0.1:9000/"
13     }
14   }
15 }

```

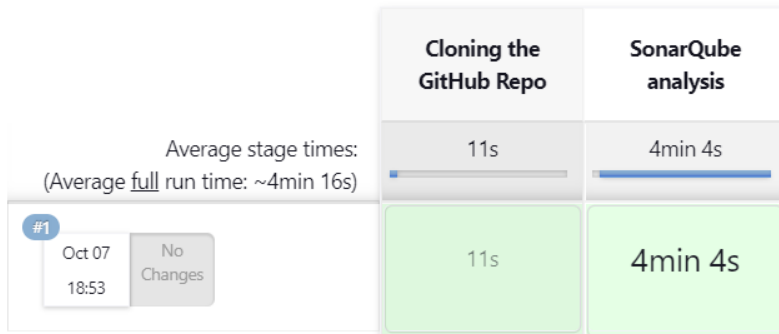
try sample Pipeline...

It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

8. Run The Build.

Pipeline sonarqube

Stage View



Permalinks

- [Last build \(#1\), 13 min ago](#)
- [Last stable build \(#1\), 13 min ago](#)
- [Last successful build \(#1\), 13 min ago](#)
- [Last completed build \(#1\), 13 min ago](#)

9. Check the console output once the build is complete.



Console Output

```

Started by user admin
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning the GitHub Repo)
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
Cloning the remote Git repository
Cloning repository https://github.com/shazforiot/GOL.git
> git.exe init C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube # timeout=10
Fetching upstream changes from https://github.com/shazforiot/GOL.git
> git.exe --version # timeout=10
> git --version # 'git version 2.37.3.windows.1'
> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/GOL.git +refs/heads/*:refs/remotes/origin/* # timeout=10
> git.exe config remote.origin.url https://github.com/shazforiot/GOL.git # timeout=10
> git.exe config --add remote.origin.fetch +refs/heads/*:refs/remotes/origin/* # timeout=10
Avoid second fetch
> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 (refs/remotes/origin/master)

```

```

WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/engine/util/CompoundVariable.html for block at line
17. Keep only the first 100 references.
WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/engine/util/CompoundVariable.html for block at line
151. Keep only the first 100 references.
WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/engine/util/CompoundVariable.html for block at line
610. Keep only the first 100 references.
WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/engine/util/CompoundVariable.html for block at line
74. Keep only the first 100 references.
INFO: CPD Executor CPD calculation finished (done) | time=82320ms
INFO: Analysis report generated in 1968ms, dir size=129.8 MB
INFO: Analysis report compressed in 8183ms, zip size=29.8 MB
INFO: Analysis report uploaded in 3365ms
INFO: ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9000/dashboard?id=demoapp-project
INFO: Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
INFO: More about the report processing at http://127.0.0.1:9000/api/ce/task?id=AYOyoTWoSTNws3yuswAt
INFO: Analysis total time: 3:57.572 s
INFO: -----
INFO: EXECUTION SUCCESS
INFO: -----
INFO: Total time: 3:59.581s
INFO: Final Memory: 16M/88M
INFO: -----
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS

```

10. After that, check the project in SonarQube.
Under different tabs, check all the different issues with the code.

11. Code Problems -

demoapp-project ☆ master October 7, 2022 at 6:53 PM Version not provided

Overview **Issues** Security Hotspots Measures Code Activity Project Settings Project Information

My Issues **All** Bulk Change 1 / 253,159 issues 3171d effort

Filters

- Period
 - New code
- Type
 - Bug 111k
 - Vulnerability 0
 - Code Smell 142k
- Severity
 - Blocker 0
 - Critical 0
 - Major 188k
 - Minor 65k
 - Info 2
- Scope
- Resolution
- Status
- Security Category
- Creation Date
- Language

gameoflife-core/build/reports/tests/all-tests.html

- ☐ Insert a <!DOCTYPE> declaration to before this <html> tag. 2 years ago L1 user-experience
- ☐ Add "lang" and/or "xml:lang" attributes to this "html" element 2 years ago L1 accessibility, wcag2-a
- ☐ Add "<th>" headers to this "<table>". 2 years ago L9 accessibility, wcag2-a
- ☐ Remove this deprecated "width" attribute. 2 years ago L9 html5, obsolete
- ☐ Add a description to this table. 2 years ago L9 accessibility, wcag2-a
- ☐ Remove this deprecated "align" attribute. 2 years ago L11 html5, obsolete
- ☐ Remove this deprecated "align" attribute. 2 years ago L12 html5, obsolete
- ☐ Remove this deprecated "size" attribute. 2 years ago L17

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration Search for projects...

demoapp-project ☆ master October 7, 2022 at 6:53 PM Version not provided

Overview **Issues** Security Hotspots Measures Code Activity Project Settings Project Information

My Issues **All** Bulk Change 1 / 141,803 issues 1477d effort

Filters Clear All Filters

- Period
 - New code
- Type **CODE SMELL** Clear
 - Bug 111k
 - Vulnerability 0
 - Code Smell 142k
- Severity
 - Blocker 0
 - Critical 0
 - Major 142k
 - Minor 0
 - Info 2
- Scope
- Resolution
- Status
- Security Category
- Creation Date

gameoflife-core/build/reports/tests/all-tests.html

- ☐ Remove this deprecated "width" attribute. 2 years ago L9 html5, obsolete
- ☐ Remove this deprecated "align" attribute. 2 years ago L11 html5, obsolete
- ☐ Remove this deprecated "align" attribute. 2 years ago L12 html5, obsolete
- ☐ Remove this deprecated "size" attribute. 2 years ago L17 html5, obsolete
- ☐ Remove this deprecated "cellpadding" attribute. 2 years ago L19 html5, obsolete
- ☐ Remove this deprecated "cellspacing" attribute. 2 years ago L19 html5, obsolete
- ☐ Remove this deprecated "width" attribute. 2 years ago L19 html5, obsolete
- ☐ Remove this deprecated "valign" attribute. 2 years ago L20

In this way, we have created a CI/CD Pipeline with Jenkins and integrated it with SonarQube to find issues in the code like bugs, code smells, duplicates, cyclomatic complexities, etc.