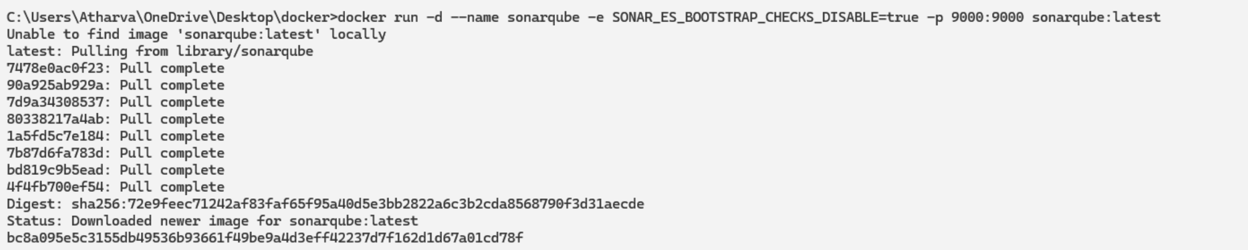
Atharva Prabhu EXPERIMENT 7

D15A 43

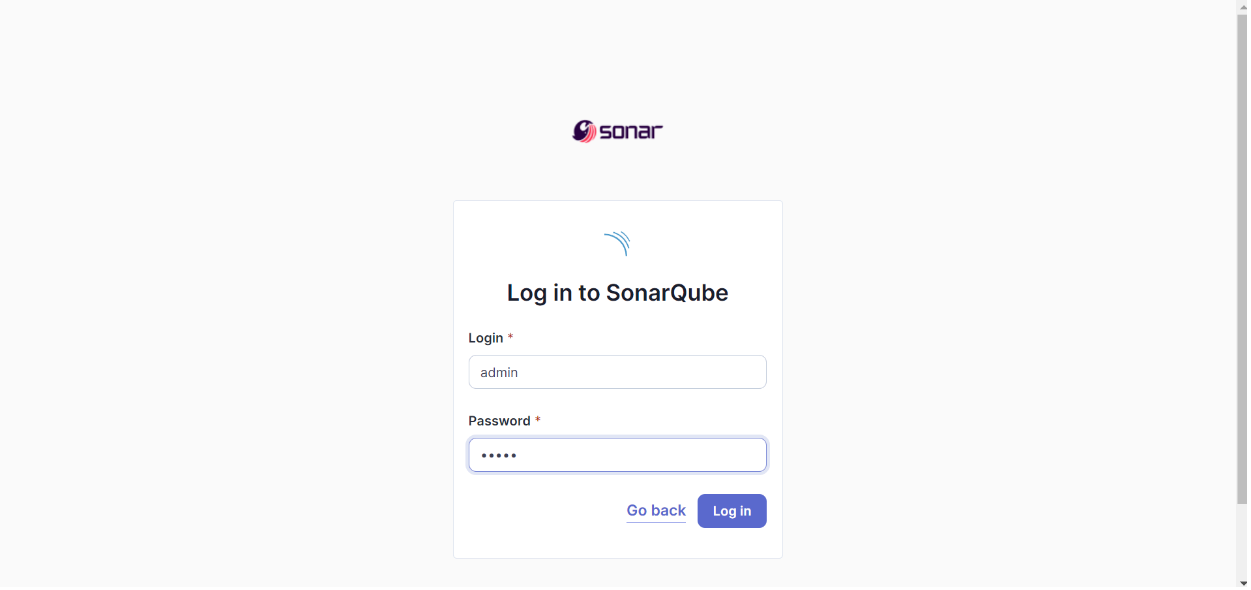
Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

Step 1: Open Windows PowerShell and run the following command – docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest WARNING: Run the following command only once



```
C:\Users\Atharva\OneDrive\Desktop\docker>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
bc8a095e5c3155db49536b93661f49be9a4d3eff42237d7f162d1d67a01cd78f
```

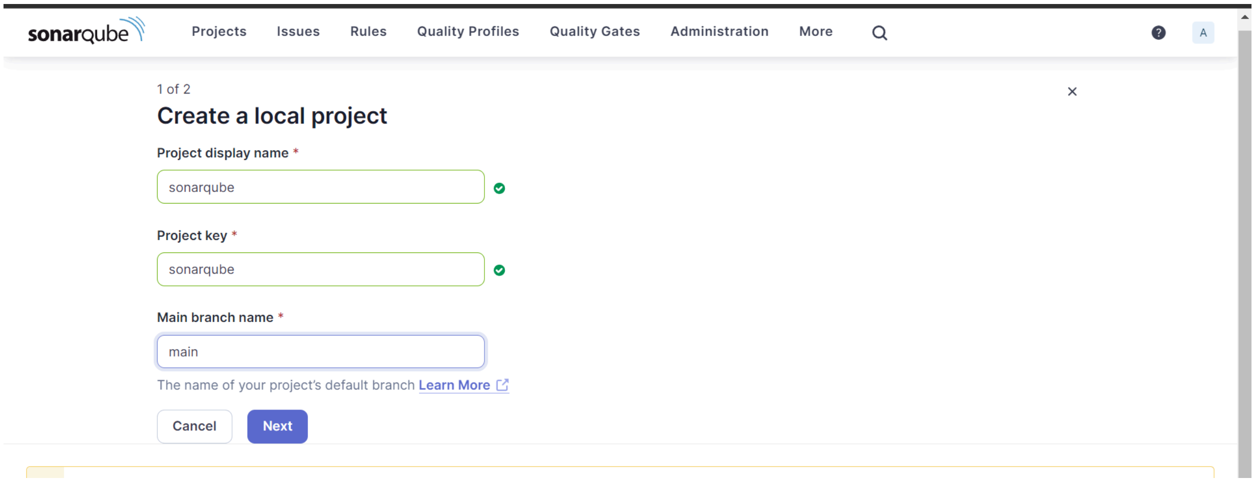
Step 2: Visit http://localhost:9000/ to open SonarQube. Login with username: admin and password: admin.



Login *
admin

Password *
•••••

Step 3: Click on create a local project and name the project as sonarqube-test and key as sonarqube-test and click on the next button. In the next step select the “Use the global setting” option and click on create project.



1 of 2

Create a local project

Project display name *

sonarqube

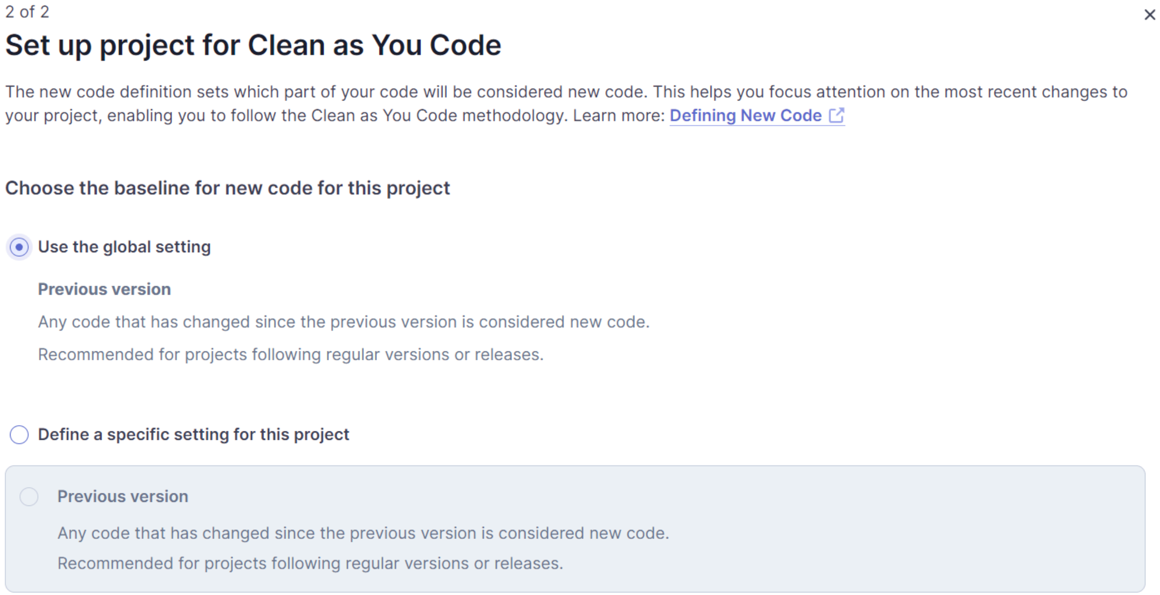
Project key *

sonarqube

Main branch name *

main

The name of your project's default branch Learn More


2 of 2

Set up project for Clean as You Code

The new code definition sets which part of your code will be considered new code. This helps you focus attention on the most recent changes to your project, enabling you to follow the Clean as You Code methodology. Learn more: Defining New Code

Choose the baseline for new code for this project

● Use the global setting

Previous version

Any code that has changed since the previous version is considered new code.

Recommended for projects following regular versions or releases.

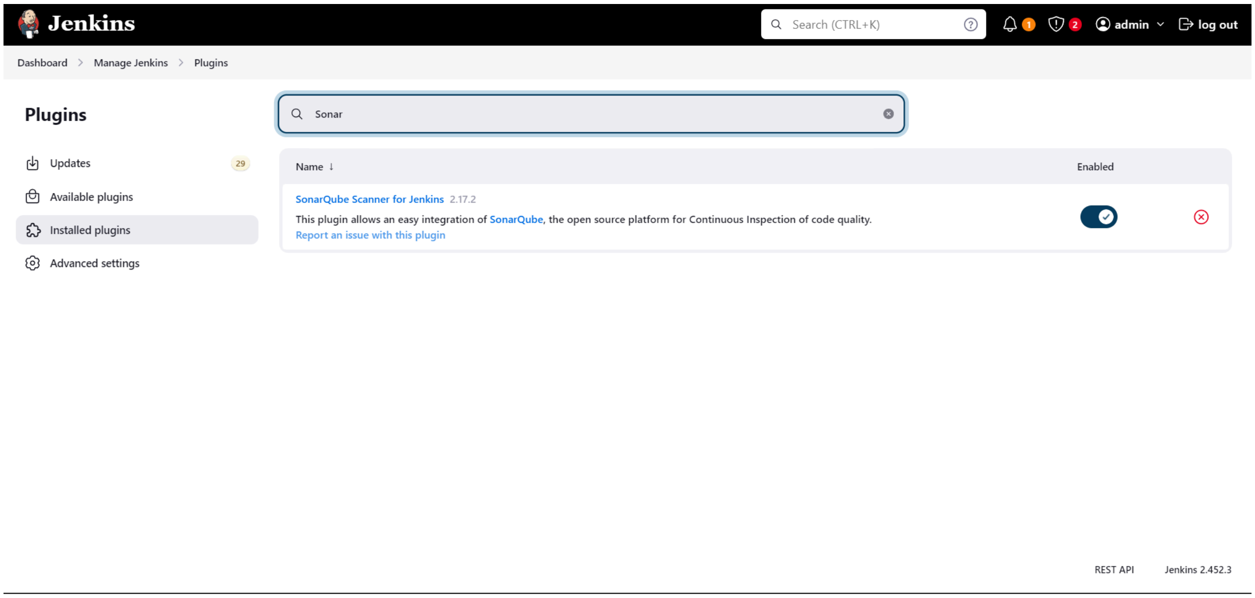
○ Define a specific setting for this project

○ Previous version

Any code that has changed since the previous version is considered new code.

Recommended for projects following regular versions or releases.

Step 4: Open Jenkins using http://localhost:8080/ and select Manage Jenkins, then select the Plugins and select available plugins from sidebar and search for SonarQube Scanner and install it. Once installed you can view the installed plugin in installed plugins section in sidebar.



Sonar

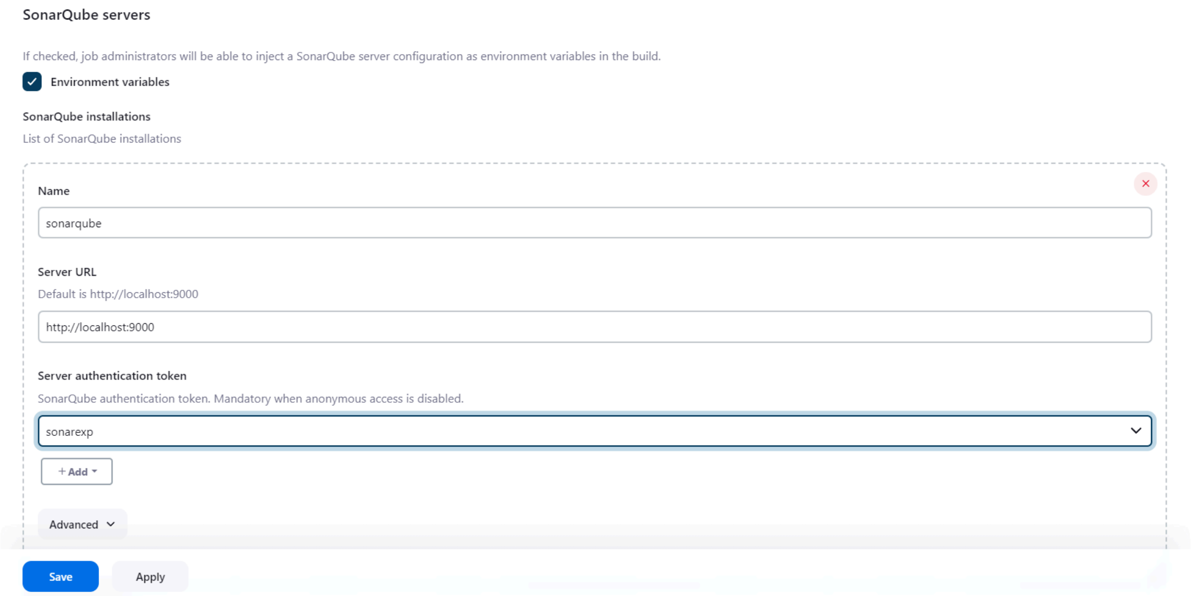
SonarQube Scanner for Jenkins 2.17.2

This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.

Report an issue with this plugin

Step 5: Select Manage Jenkins, then select the System and then scroll down to SonarQube Server. Name the server as sonarqube and set the server url as http://localhost:9000/ then click on save.

Step 6: Go to Jenkins Dashboard and select Manage Jenkins, then select the Tools and then scroll down to SonarQube Scanner installations. Name the sonarqube scanner as sonarqubescanner and select install automatically then click on save.



SonarQube servers

If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.

☑ Environment variables

SonarQube installations

List of SonarQube installations

Name

sonarqube

Server URL

Default is http://localhost:9000

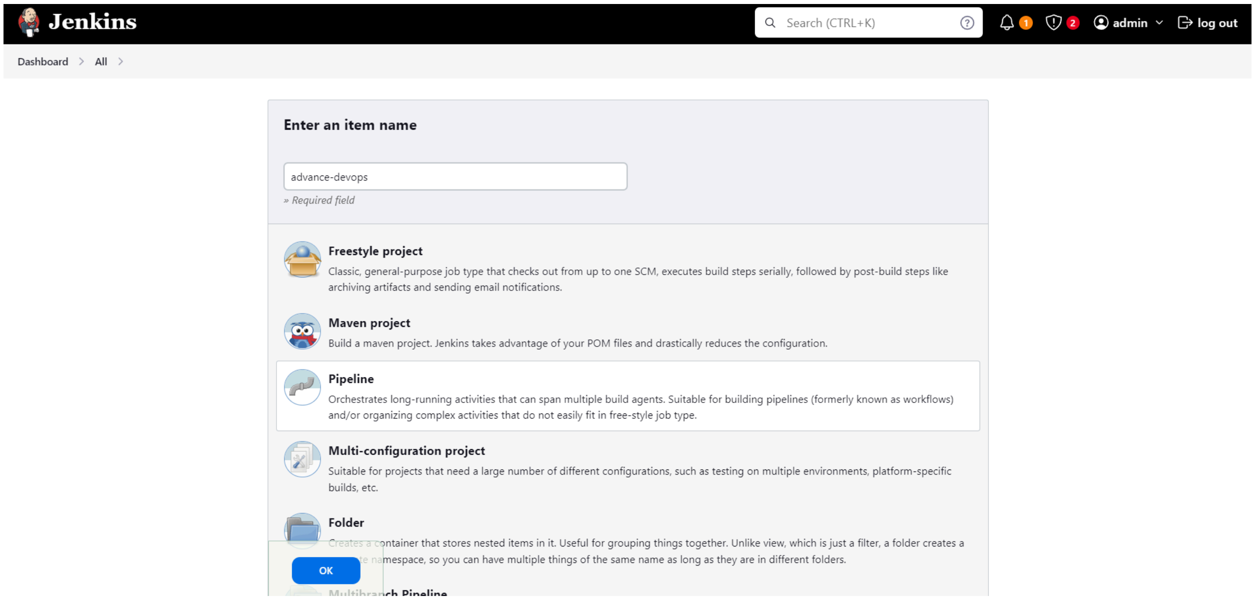
http://localhost:9000

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

sonarexp

Step 7: Go to Jenkins dashboard and click on New Item and select Freestyle project and name it as SonarQube and then click on ok.



Enter an item name

advance-devops

» Required field

Freestyle project
Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.

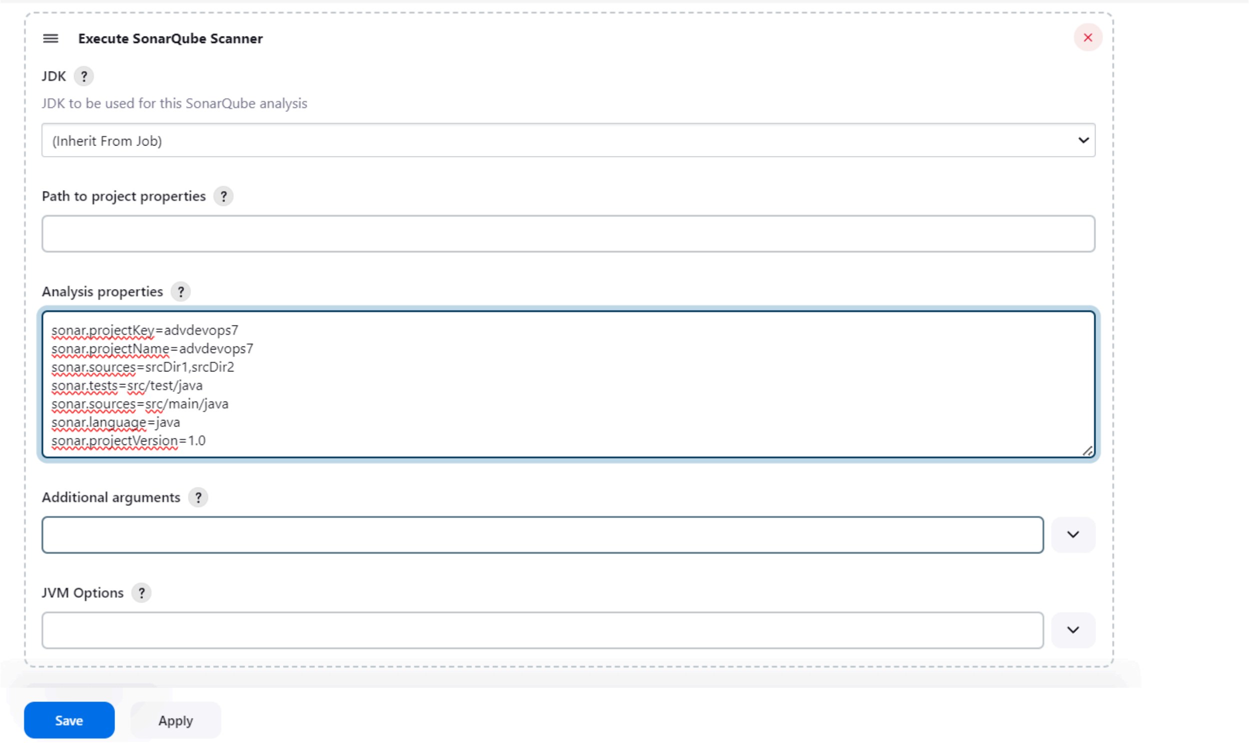
Maven project
Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.

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.

Step 8: For configuration, Select git and paste the following git repository in the repository url. https://github.com/shazforiot/MSBuild_firstproject This is a simple Hello world project Step 9: Under the Build steps select “Execute SonarQube Scanner” option and under Analysis Properties write the following - sonar.projectKey, sonar.login, sonar.password, sonar.hosturl. Then click on the save button.


Execute SonarQube Scanner

JDK ?

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties ?

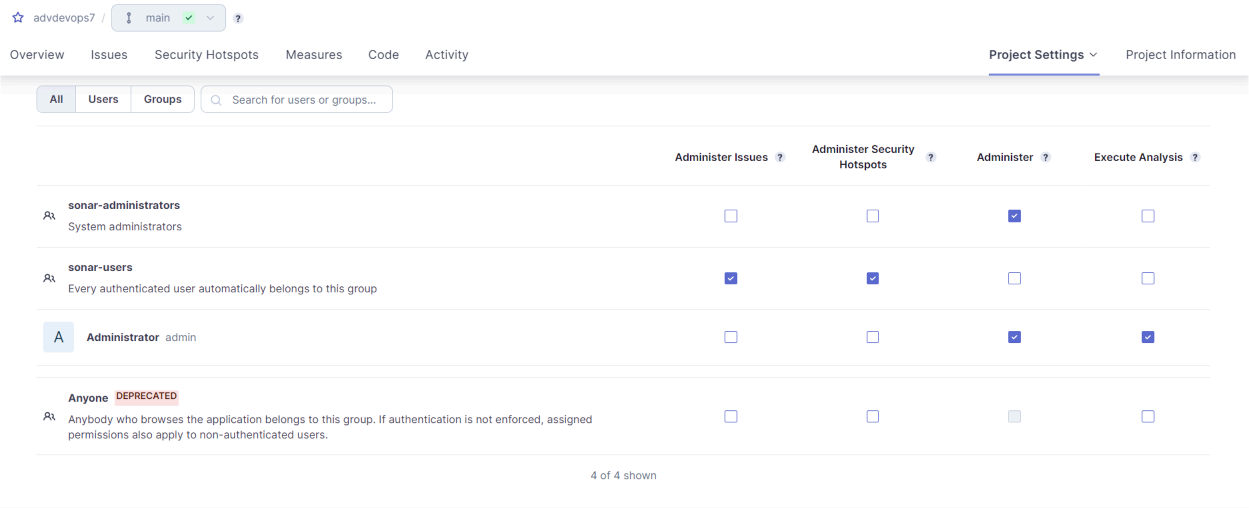
Analysis properties ?

```
sonar.projectKey=advdevops7
sonar.projectName=advdevops7
sonar.sources=srcDir1,srcDir2
sonar.tests=src/test/java
sonar.sources=src/main/java
sonar.language=java
sonar.projectVersion=1.0
```

Additional arguments ?

JVM Options ?

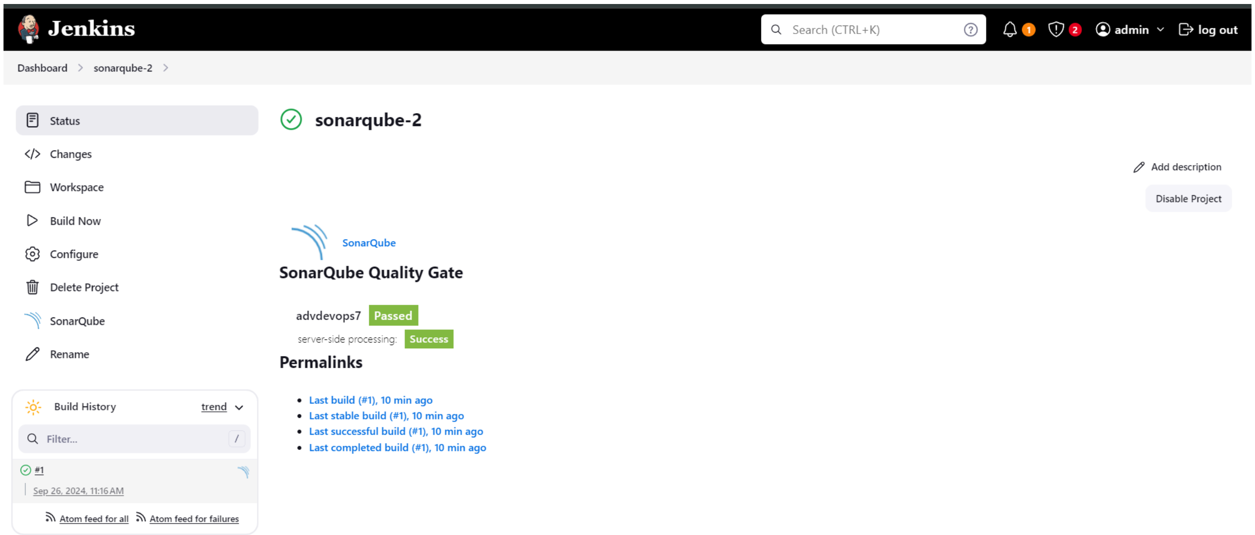
Step 10: Visit http://localhost:9000/admin/permissions and select the Users tab and for Administrator select the checkbox Execute Analysis.



	Administer Issues ?	Administer Security Hotspots ?	Administer ?	Execute Analysis ?
sonar-administrators System administrators	□	□	☑	□
sonar-users Every authenticated user automatically belongs to this group	☑	☑	□	□
A **Administrator** admin	□	□	☑	☑
Anyone DEPRECATED Anybody who browses the application belongs to this group. If authentication is not enforced, assigned permissions also apply to non-authenticated users.	□	□	□	□

4 of 4 shown

Step 11: Now, come back to Jenkins and click on Build Now. The build is success.



sonarqube-2

SonarQube Quality Gate

advdevops7 Passed

server-side processing: Success

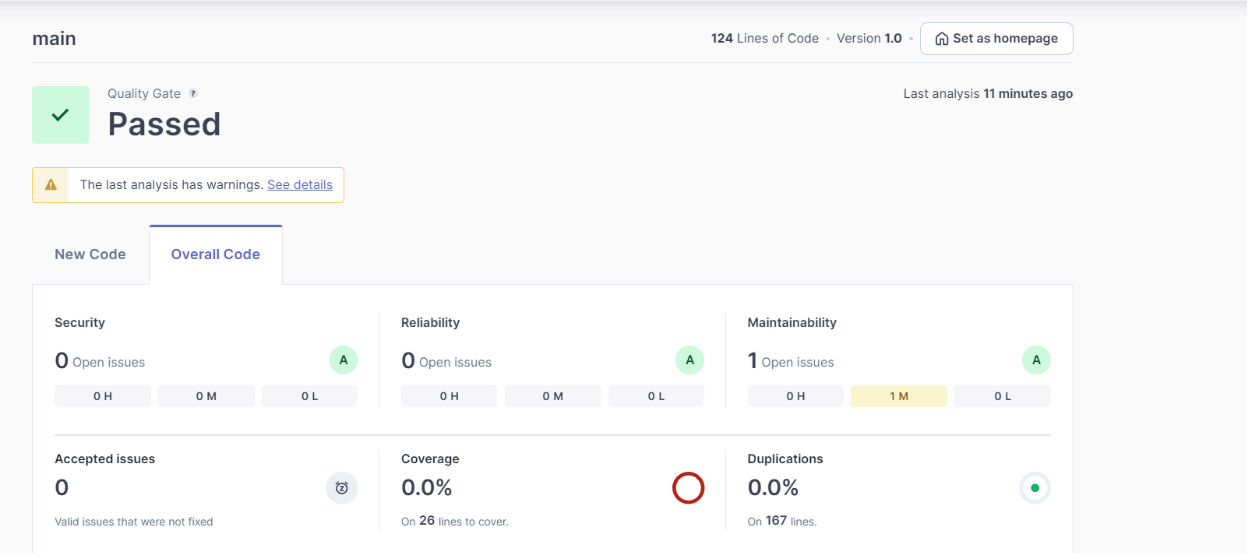
Permalinks

- Last build (#1), 10 min ago
- Last stable build (#1), 10 min ago
- Last successful build (#1), 10 min ago
- Last completed build (#1), 10 min ago

#1
Sep 26, 2024, 11:16 AM

Atom feed for all   Atom feed for failures

Step 12: Visit the following URL to see the result - http://localhost:9000/dashboard?id=sonarqubetest&codeScope=overall



main

124 Lines of Code · Version **1.0** ·

Quality Gate

Passed

Last analysis **11 minutes ago**

The last analysis has warnings. See details

Security

0 Open issues A

0 H | 0 M | 0 L

Reliability

0 Open issues A

0 H | 0 M | 0 L

Maintainability

1 Open issues A

0 H | 1 M | 0 L

Accepted issues

0

Valid issues that were not fixed

Coverage

0.0%

On **26** lines to cover.

Duplications

0.0%

On **167** lines.