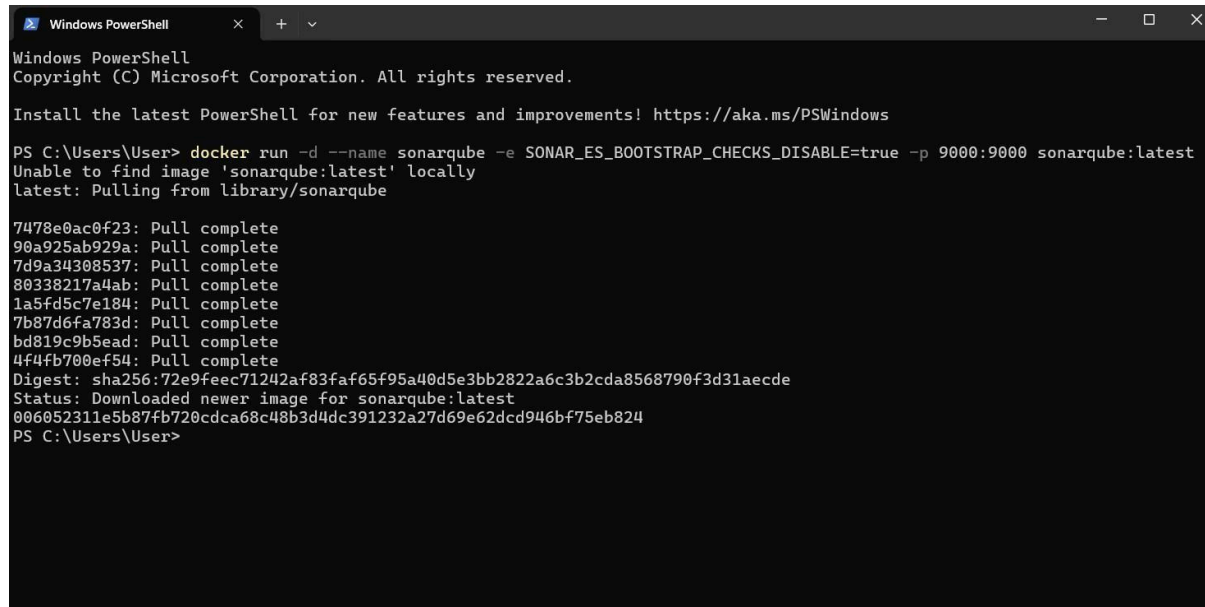


EXPERIMENT 7

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

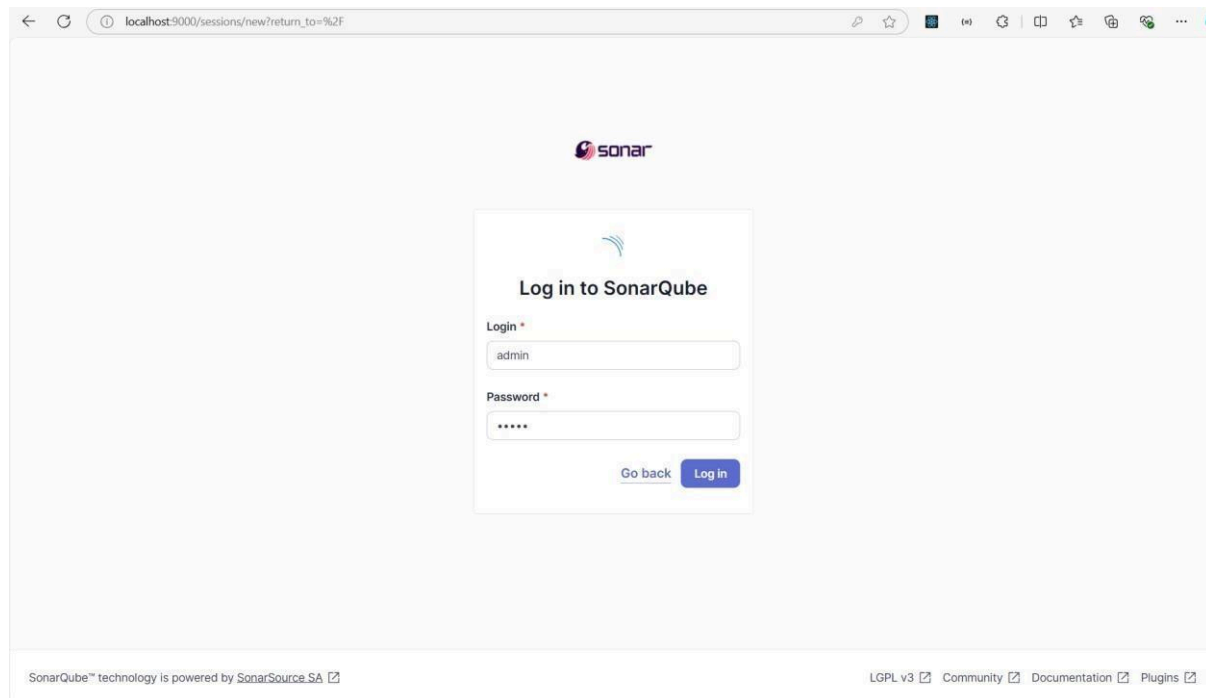


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\User> 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
006052311e5b87fb720cdca68c48b3d4dc391232a27d69e62dcd946bf75eb824
PS C:\Users\User>
```

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



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.

←↻🔍localhost:9000/projects/create

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore🔍

🔔A

How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)?
Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

🔄 Import from Azure DevOps

Setup

📁 Import from Bitbucket Cloud

Setup

📁 Import from Bitbucket Server

Setup

🐙 Import from GitHub

Setup

🐙 Import from GitLab

Setup

Are you just testing or have an advanced use-case? Create a local project.

Create a local project

⚠️ Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by [SonarSource SA](#)Community Edition v10.6 (92116) ACTIVE🔗 LGPL v3🔗 Community🔗 Documentation🔗 Plugins🔗 Web API

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore🔍

🔔A

1 of 2

Create a local project

✕

Project display name *

sonarqube-test

✓

Project key *

sonarqube-test

✓

Main branch name *

main

The name of your project's default branch [Learn More](#)🔗

Cancel

Next

⚠️ Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by [SonarSource SA](#)Community Edition v10.6 (92116) ACTIVE🔗 LGPL v3🔗 Community🔗 Documentation🔗 Plugins🔗 Web API

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

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.

☐ Number of days

Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.
Recommended for projects following continuous delivery.

☐ Reference branch

Choose a branch as the baseline for the new code.
Recommended for projects using feature branches.

Step 2: In the Jenkins dashboard, click on the **Manage Jenkins** link in the left sidebar. This will take you to the Jenkins configuration page. In the **System Configuration** section, click on the **Plugins** tab. This will show you the list of installed plugins and the option to select new plugins to install.

Step 2: In the Jenkins dashboard, click on the **Manage Jenkins** link in the left sidebar. This will take you to the Jenkins configuration page. In the **System Configuration** section, click on the **Plugins** tab. This will show you the list of installed plugins and the option to select new plugins to install.

Jenkins

Search (CTRL+K)

Anuprita Mhapankar

log out

Dashboard > Manage Jenkins

+ New Item

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

1 idle

2 idle

Slave1 (offline)

localhost:8080/manage/pluginManager

Manage Jenkins

Search settings

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See [the documentation](#).

Warnings have been published for the following currently installed components:
Jenkins 2.452.3 core and libraries:
Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier
A fix for this issue is available. Update Jenkins now.

System Configuration

System

Configure global settings and paths.

Tools

Configure tools, their locations and automatic installers.

Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds

Add, remove, and configure cloud instances to provision agents on-demand.

Plugins

Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Appearance

Configure the look and feel of Jenkins

Jenkins

Search (CTRL+K)

Anuprita Mhapankar

log out

Dashboard

Manage Jenkins

Plugins

Plugins

Updates

Available plugins

Installed plugins

Advanced settings

sona

Name	Enabled
<div>SonarQube Scanner for Jenkins 2.17.2</div> <div>This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality. Report an issue with this plugin</div>	<div><div></div><div></div></div>

REST API

Jenkins 2.452.3

St

SO

the server as

Jenkins

Search (CTRL+K)

Anuprita Mhapankar

log out

Dashboard

Manage Jenkins

New Item

Build History

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

Manage Jenkins

New version of Jenkins (2.462.2) is available for [download](#) ([changelog](#)).

Or Upgrade Automatically

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See [the documentation](#).

ManageDismiss

Warnings have been published for the following currently installed components:

Jenkins 2.452.3 core and libraries:
Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier
A fix for this issue is available. Update Jenkins now.

Configure which of these warnings are shown

System Configuration

System

Configure global settings and paths.

Tools

Configure tools, their locations and automatic installers.

Plugins

Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds

Add, remove, and configure cloud instances to provision agents on-demand.

Appearance

Configure the look and feel of Jenkins

localhost:8080/manage/configure

Dashboard > Manage Jenkins > System >

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.

- none -

+ Add

Advanced

SaveApply

Step 2: Configure Jenkins to SonarQube

Scenario: You have a SonarQube server running on your local machine. You want to configure Jenkins to use this SonarQube server for code quality checks.

Solution: In this step, we will configure Jenkins to use the SonarQube server. We will do this by configuring the SonarQube server in the Jenkins system configuration.

Dashboard > Manage Jenkins

+ New Item

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

Built-In Node

1 Idle

2 Idle

Slave1 (offline)

Manage Jenkins

Search settings

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See the documentation.

Warnings have been published for the following currently installed components:
Jenkins 2.452.3 core and libraries
Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier
A fix for this issue is available. Update Jenkins now.

System Configuration

System
Configure global settings and paths.

Tools
Configure tools, their locations and automatic installers.

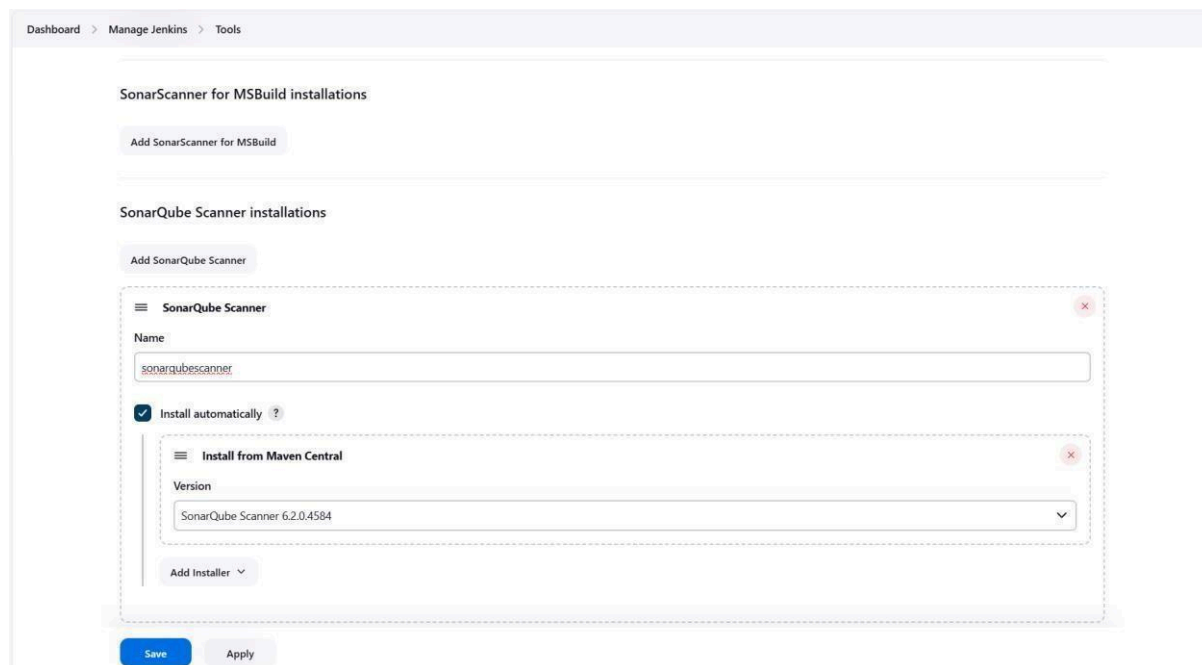
Nodes
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds
Add, remove, and configure cloud instances to provision agents on-demand.

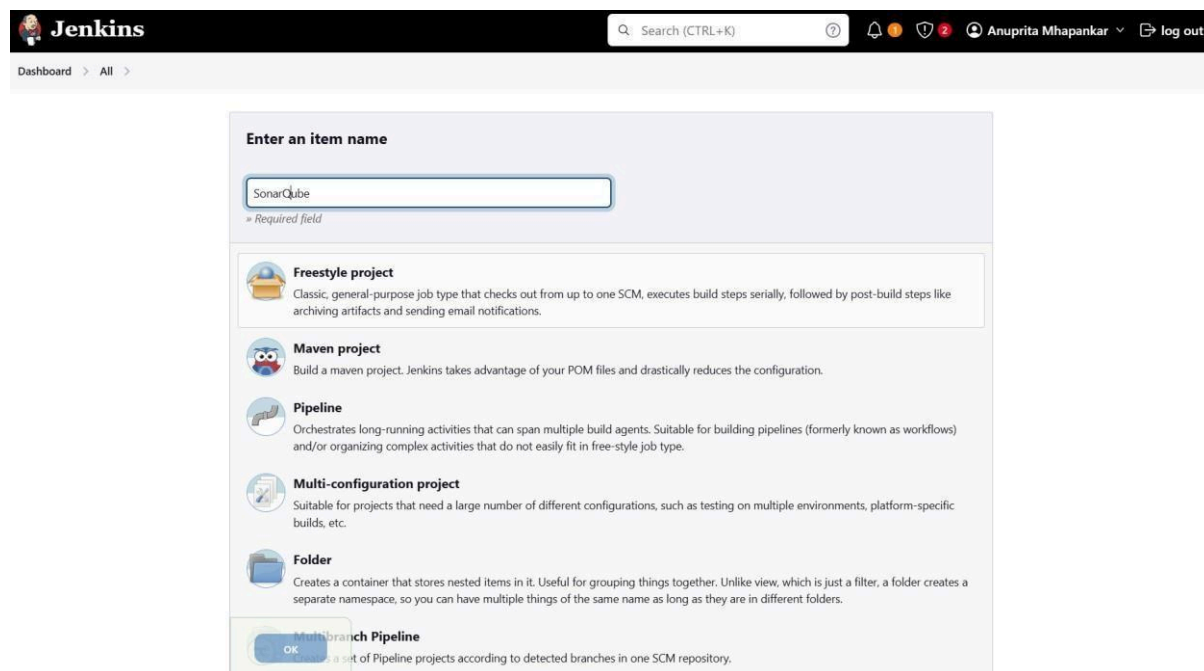
Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Appearance
Configure the look and feel of Jenkins.

localhost:8080/manage/configureTools



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.



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

Dashboard > SonarQube > Configuration

Configure

- General
- Source Code Management**
- Build Triggers
- Build Environment
- Build Steps
- Post-build Actions

Source Code Management

☐ None

☒ **Git** ?

Repositories ?

Repository URL ?

https://github.com/shazforiot/MSBuild_firstproject.git

Credentials ?

- none -

+ Add

Advanced

Add Repository

Branches to build ?

Branch Specifier (blank for 'any') ?

*/master

Save Apply

Step 9: Under the Build steps select “Execute SonarQube Scanner” option and under Analysis Properties write the following -

sonar.projectKey=sonarqube-test

sonar.login=admin

sonar.password=sonarqube

sonar.hosturl=http://sonarqube:9000

0 Then click on the save button.

Dashboard > SonarQube > Configuration

Configure

- General
- Source Code Management
- Build Triggers
- Build Environment
- Build Steps**
- Post-build Actions

Build Steps

Execute SonarQube Scanner

JDK ?

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties ?

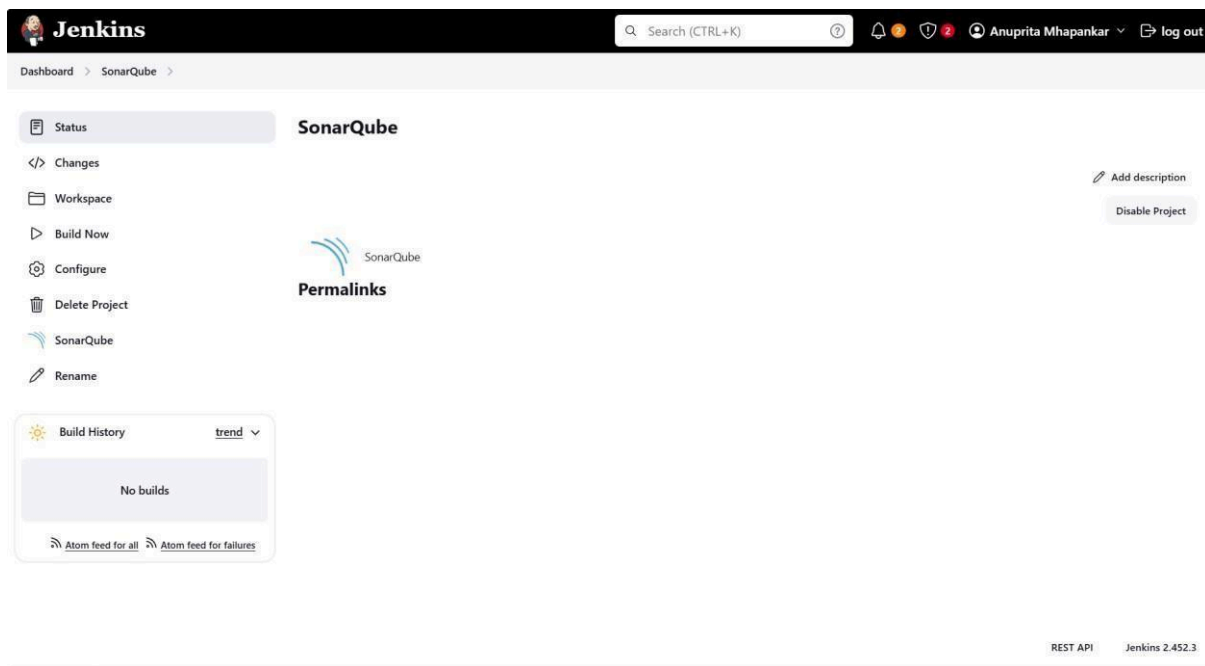
Analysis properties ?

sonar.projectKey=sonarqube-test
sonar.login=admin
sonar.password=sonarqube
sonar.hosturl=http://sonarqube:9000

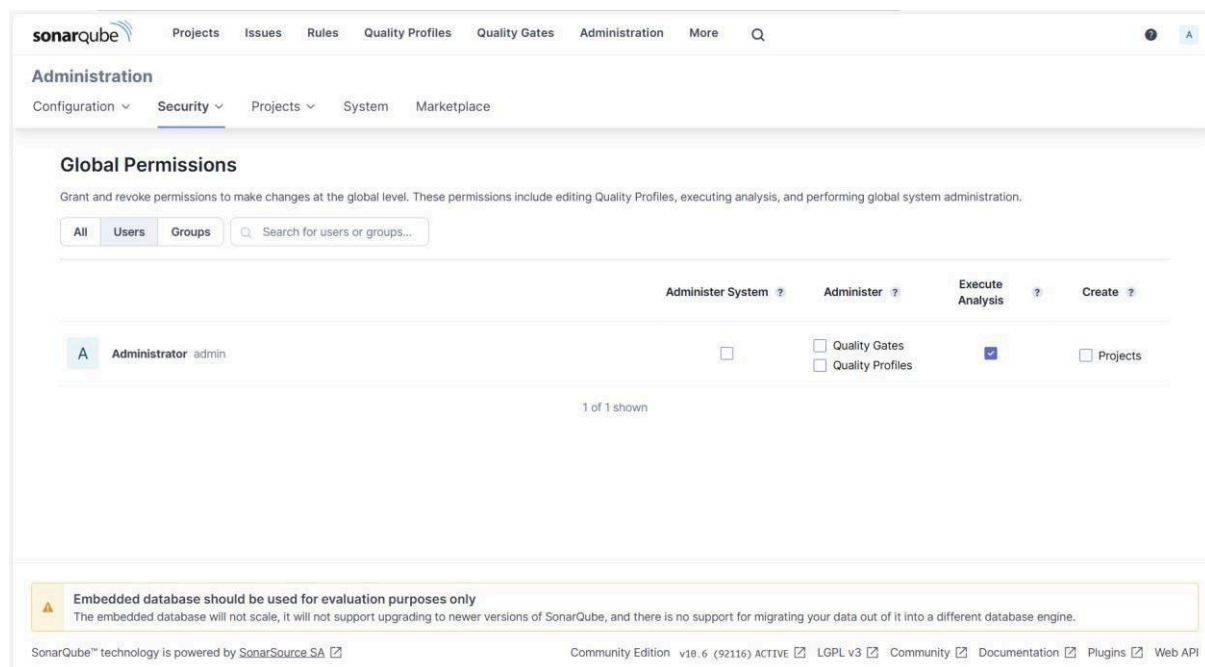
Additional arguments ?

JVM Options ?

Save Apply



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



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

REST API Jenkins 2.452.3

localhost:9000/dashboard?id=sonarqube-test&codeScope=overall

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

main

Version not providedSet as homepage

Quality Gate

Passed

Last analysis 14 minutes ago

The last analysis has warnings. See details

New Code

Overall Code

Security

0 Open issues

0 H0 M0 L

A

Reliability

0 Open issues

0 H0 M0 L

A

Maintainability

0 Open issues

0 H0 M0 L

A

Accepted issues

0

Valid issues that were not fixed

Coverage

On 0 lines to cover.

Duplications

0.0%

On 86 lines.

Security Hotspots