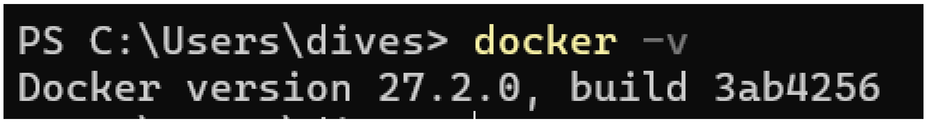
Name: Divesh Lulla Class: D15C Roll No: 31

Experiment No: 7

Aim: To understand static analysis SAST process and learn to integrate Jenkins SAST to Sonarqube/GitLab.

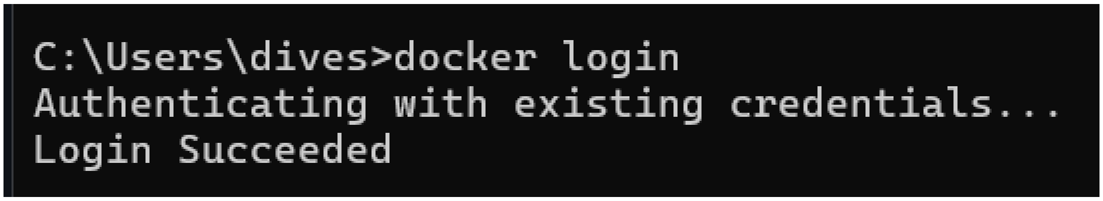
Steps:

1) First lets check whether the docker is installed or not by checking its version.



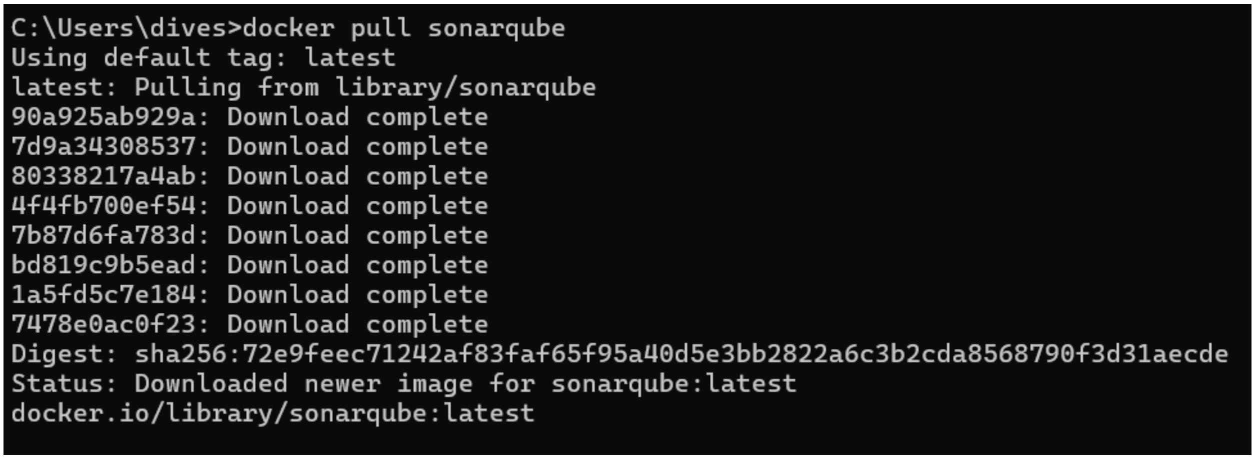
```
PS C:\Users\dives> docker -v
Docker version 27.2.0, build 3ab4256
```

2) Run docker login command and write down the login id and password.



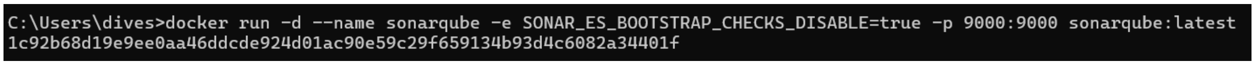
```
C:\Users\dives>docker login
Authenticating with existing credentials...
Login Succeeded
```

3) Run docker pull Sonarqube command to install Sonarqube image.



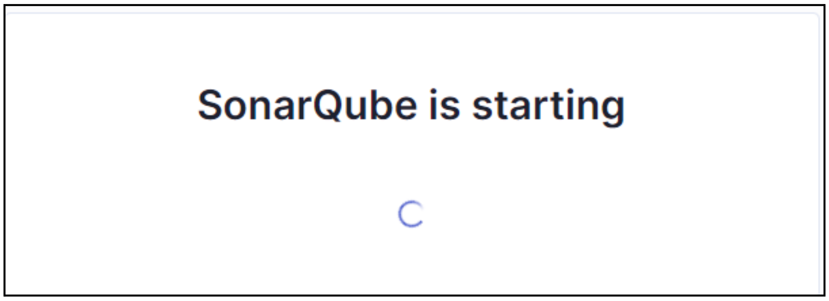
```
C:\Users\dives>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
90a925ab929a: Download complete
7d9a34308537: Download complete
80338217a4ab: Download complete
4f4fb700ef54: Download complete
7b87d6fa783d: Download complete
bd819c9b5ead: Download complete
1a5fd5c7e184: Download complete
7478e0ac0f23: Download complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
docker.io/library/sonarqube:latest
```

4) Run docker run -d –name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest Command to run the sonarqube.



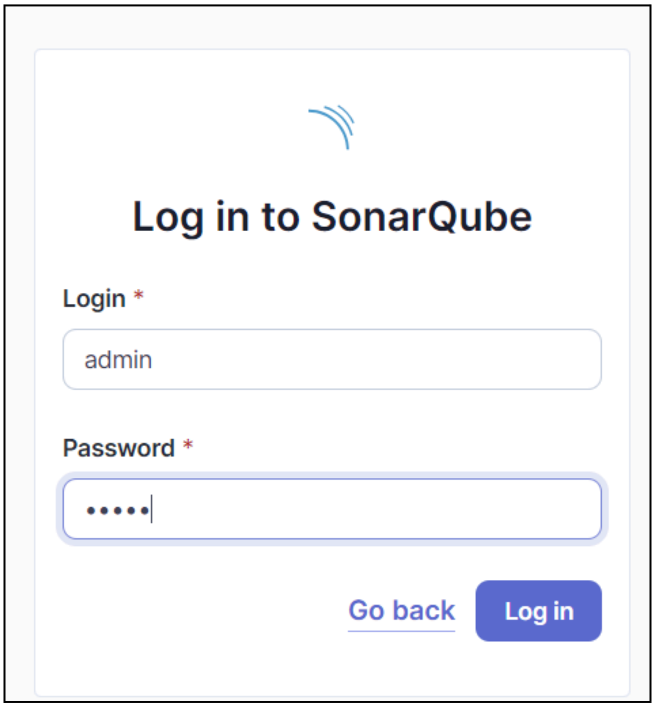
```
C:\Users\dives>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
1c92b68d19e9ee0aa46ddcde924d01ac90e59c29f659134b93d4c6082a34401f
```

5)Once the container is running go to your web browser and check status of sonarqube at port localhost:9000.



SonarQube is starting

6) Once the sonarqube is started it will redirect to the login page. The login id and password for sonarqube is admin.



Log in to SonarQube

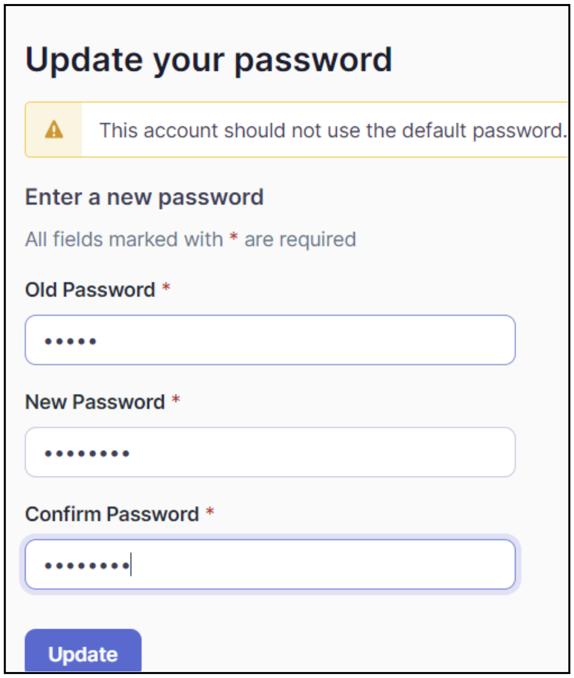
Login *

admin

Password *

•••••

7) Change the password for the Sonarqube account.



Update your password

⚠ This account should not use the default password.

Enter a new password

All fields marked with * are required

Old Password *

•••••

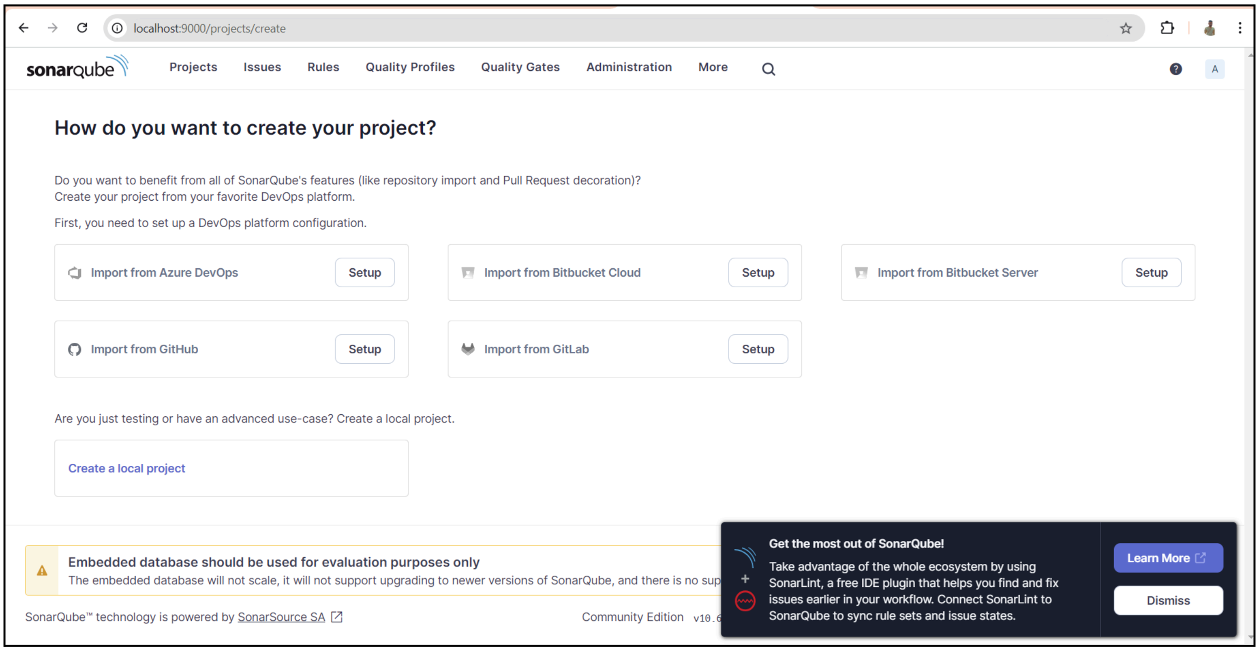
New Password *

••••••••

Confirm Password *

••••••••

8) After changing the password you will be redirected to this screen Click on create a local project.



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.

Are you just testing or have an advanced use-case? 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 sup

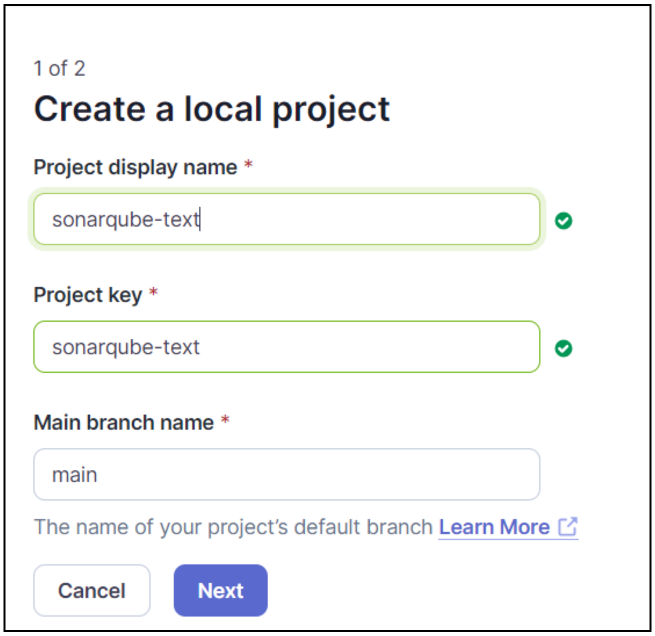
SonarQube™ technology is powered by SonarSource SA

Community Edition v10.6

Get the most out of SonarQube!

Take advantage of the whole ecosystem by using SonarLint, a free IDE plugin that helps you find and fix issues earlier in your workflow. Connect SonarLint to SonarQube to sync rule sets and issue states.

9) Add the name of the project and the project key and select the main branch name and click on the next.



1 of 2

Create a local project

Project display name *

sonarqube-text ✓

Project key *

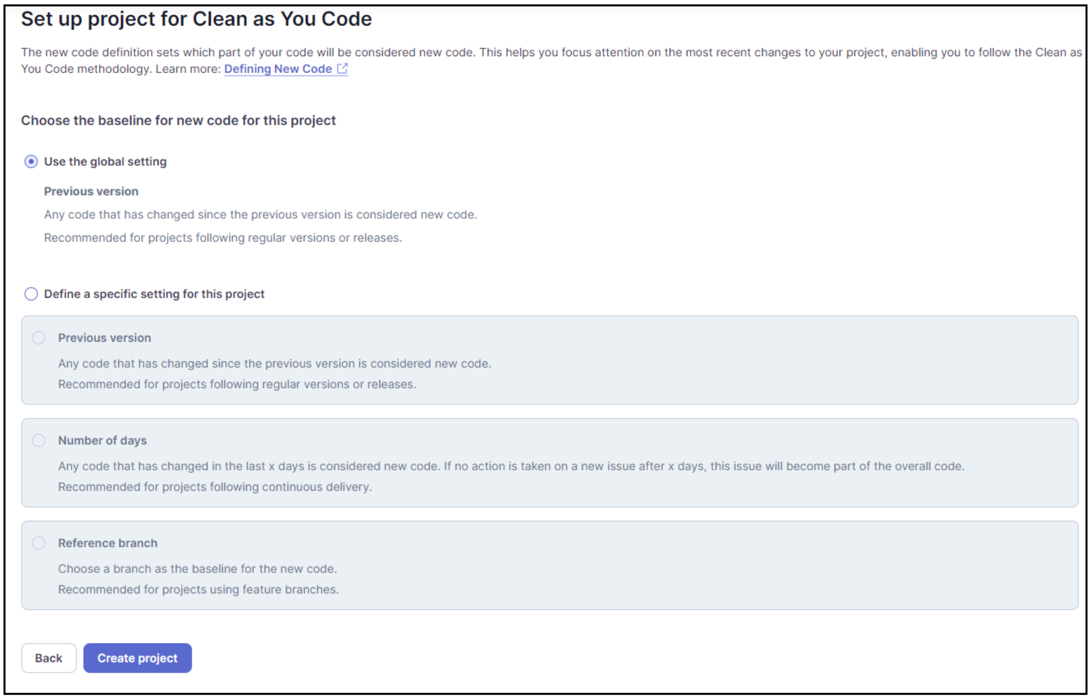
sonarqube-text ✓

Main branch name *

main

The name of your project's default branch Learn More

10) Setup the project as required and click on the create.



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.

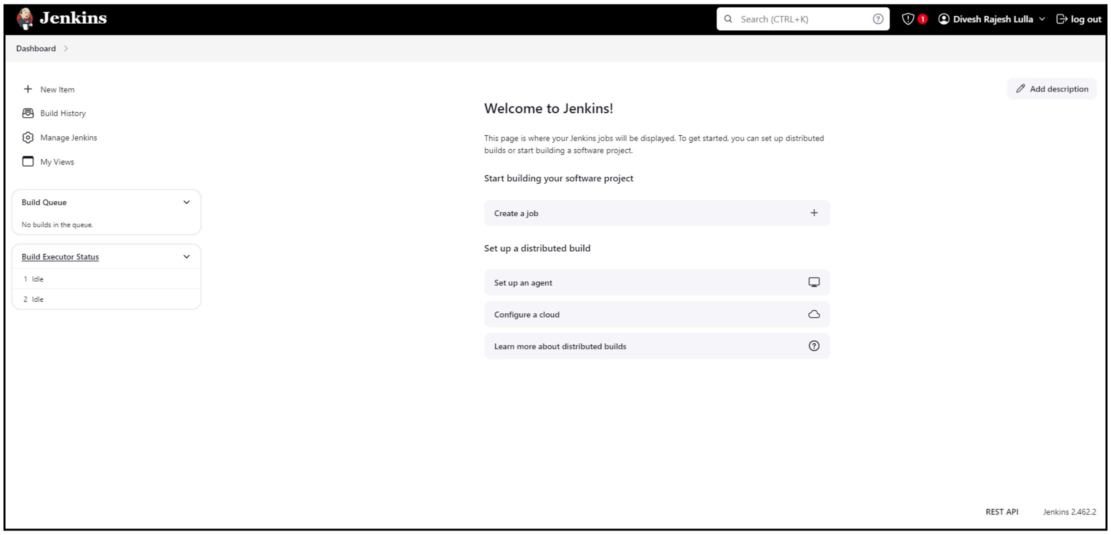
Recommended for projects following continuous delivery.

○ Reference branch

Choose a branch as the baseline for the new code.

Recommended for projects using feature branches.

11) Go to Jenkins log into your account and go to dashboard in the dashboard click on System and scroll down to SonarQube Installations. Enter the name and URL in the fields and save the changes.

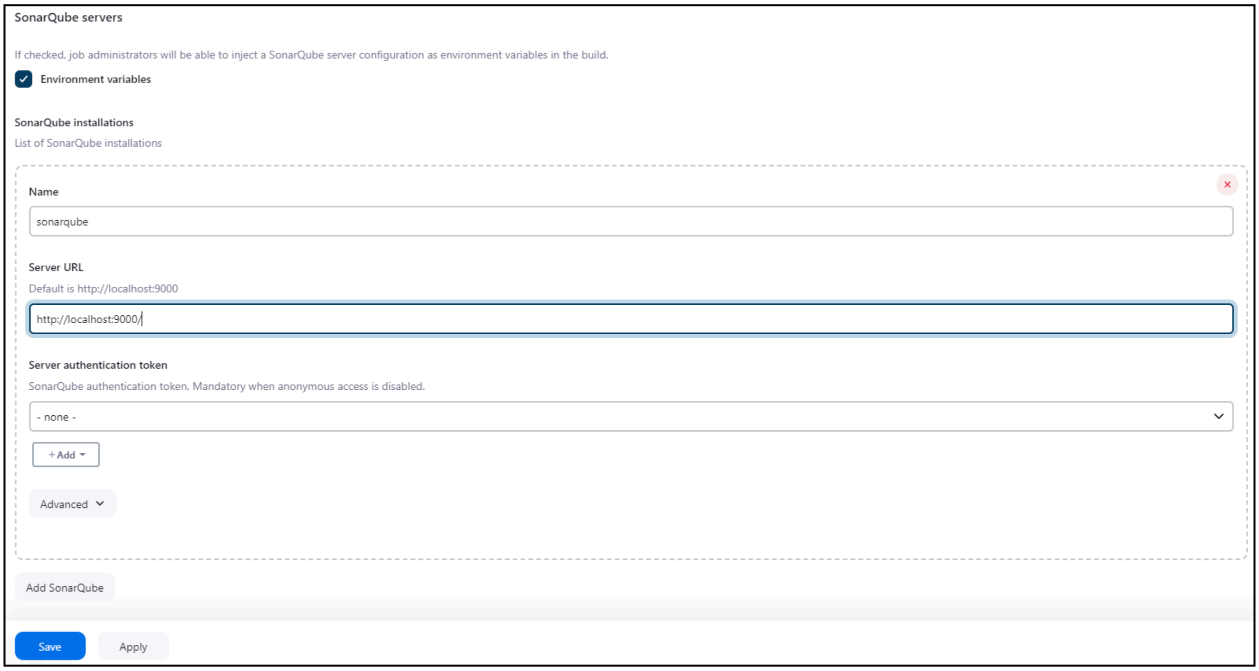


Welcome to Jenkins!

This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.

Start building your software project

Set up a distributed build



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

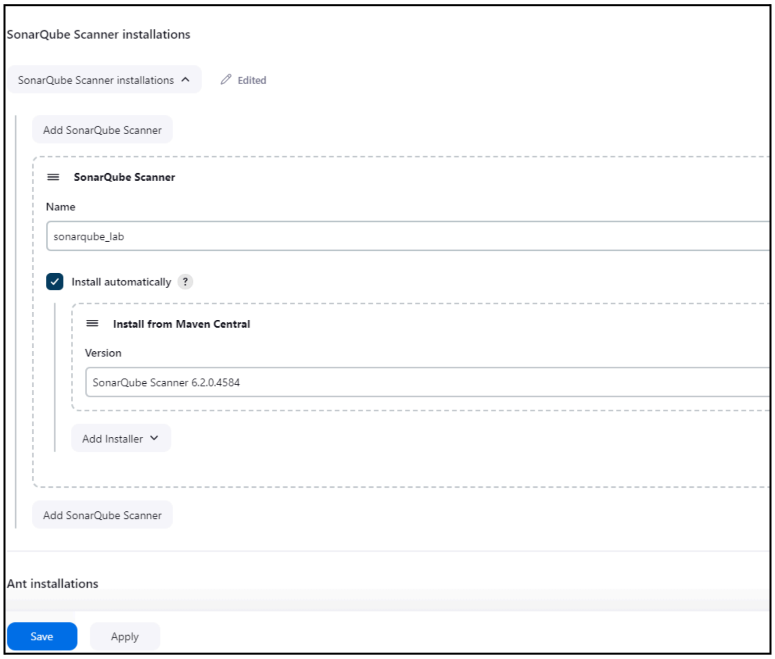
http://localhost:9000/

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

12) Go to Sonarcube scanner and add the latest version then apply changes and save it.



SonarQube Scanner installations

SonarQube Scanner

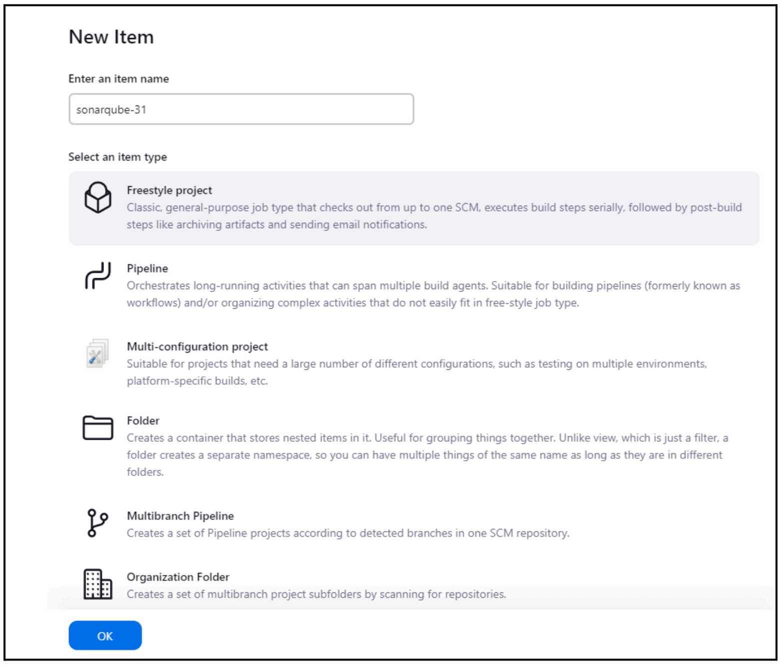
Name: sonarqube_lab

☑ Install automatically

Install from Maven Central

Version: SonarQube Scanner 6.2.0.4584

13) Go to the Jenkins, create a new item , enter the item name, select “Freestyle project” and click ok.



New Item

Enter an item name: sonarqube-31

Select an item type

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.

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.

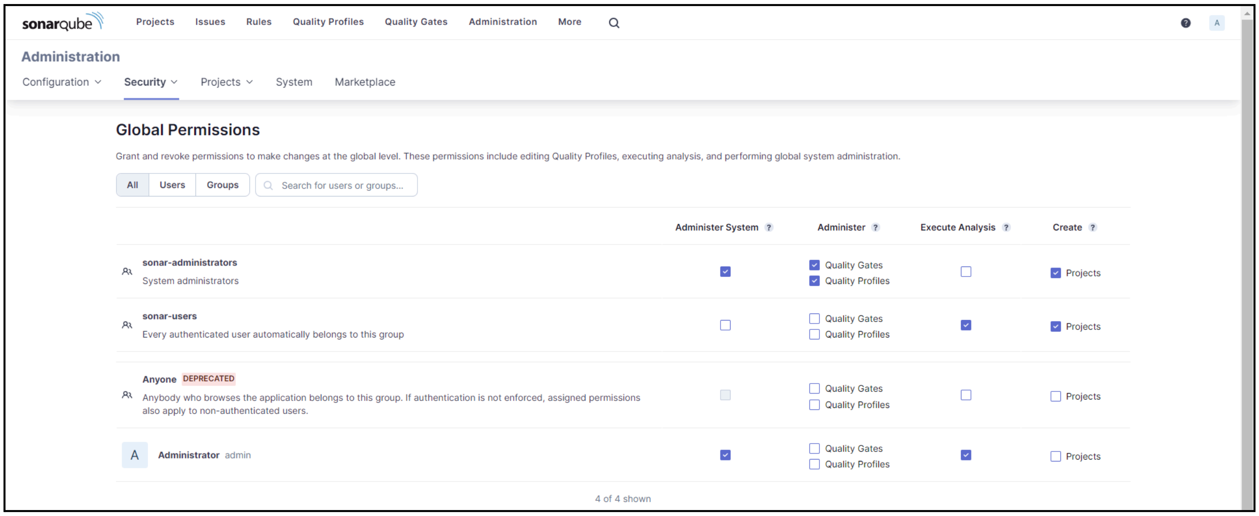
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

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.

14) After creating the item, Now, you need to grant the local user (here admin user) permissions to Execute the Analysis stage on SonarQube.

For this go to http://localhost:<port_number>/admin/permissions and check the 'Execute Analysis' checkbox under Administrator.



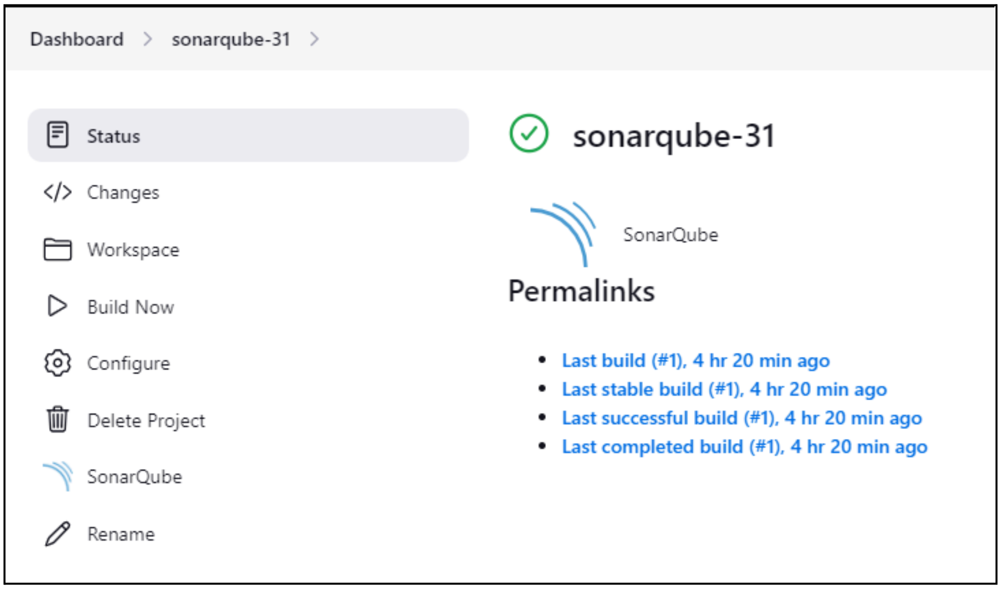
Global Permissions

Grant and revoke permissions to make changes at the global level. These permissions include editing Quality Profiles, executing analysis, and performing global system administration.

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

4 of 4 shown

15) Go to the job you have just built and click on Build Now.

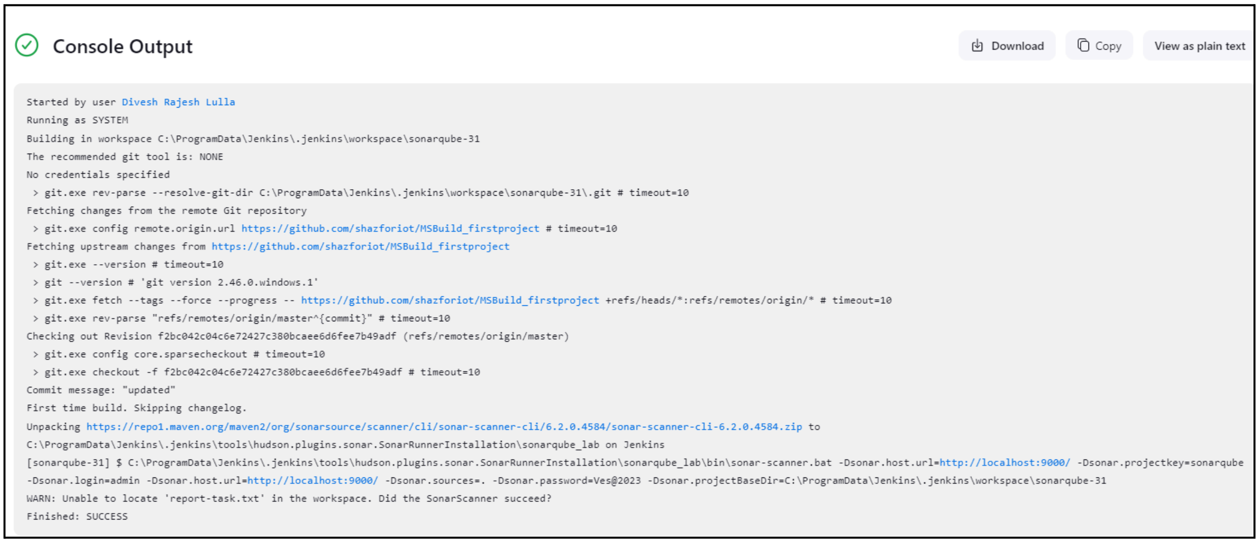


sonarqube-31

Permalinks

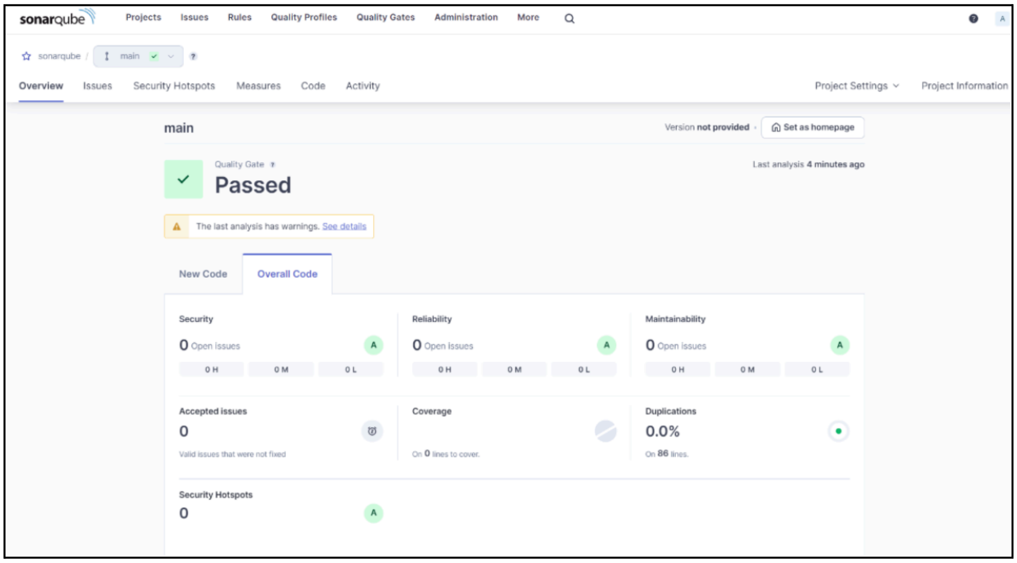
- Last build (#1), 4 hr 20 min ago
- Last stable build (#1), 4 hr 20 min ago
- Last successful build (#1), 4 hr 20 min ago
- Last completed build (#1), 4 hr 20 min ago

16) Check the console output.



```
Started by user Divesh Rajesh Lulla
Running as SYSTEM
Building in workspace C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube-31
The recommended git tool is: NONE
No credentials specified
 > git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube-31\.git # timeout=10
Fetching changes from the remote Git repository
 > git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject
 > git.exe --version # timeout=10
 > git --version # 'git version 2.46.0.windows.1'
 > git.exe fetch --tags --force --progress -- https://github.com/shazforiot/MSBuild_firstproject +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision f2bc042c04c6e72427c380bcaee6d6fee7b49adf (refs/remotes/origin/master)
 > git.exe config core.sparsecheckout # timeout=10
 > git.exe checkout -f f2bc042c04c6e72427c380bcaee6d6fee7b49adf # timeout=10
Commit message: "updated"
First time build. Skipping changelog.
Unpacking https://repo1.maven.org/maven2/org/sonarsource/scanner/cli/sonar-scanner-cli/6.2.0.4584/sonar-scanner-cli-6.2.0.4584.zip to
C:\ProgramData\Jenkins\.jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\sonarqube_lab on Jenkins
[sonarqube-31] $ C:\ProgramData\Jenkins\.jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\sonarqube_lab\bin\sonar-scanner.bat -Dsonar.host.url=http://localhost:9000/ -Dsonar.projectkey=sonarqube
-Dsonar.login=admin -Dsonar.host.url=http://localhost:9000/ -Dsonar.sources=. -Dsonar.password=Ves@2023 -Dsonar.projectBaseDir=C:\ProgramData\Jenkins\.jenkins\workspace\sonarqube-31
WARN: Unable to locate 'report-task.txt' in the workspace. Did the SonarScanner succeed?
Finished: SUCCESS
```

17) Go back to the Sonarqube and check the project.



main

Version not provided

Quality Gate

Passed

Last analysis 4 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
0 Open issues A
0 H 0 M 0 L

Accepted issues
0
Valid issues that were not fixed

Coverage
On 0 lines to cover.

Duplications
0.0%
On 86 lines.

Security Hotspots
0 A

Conclusion: In this experiment, we have performed and learnt about Jenkins SAST using sonarqube, For this we used a docker image of the sonarqube to not install it locally in our system. We created a freestyle project and tried to learn about sonarqube.