ADVANCE DEVOPS EXP 7

Name:VAISHNAL MALI
Class:D15A
Roll No:27

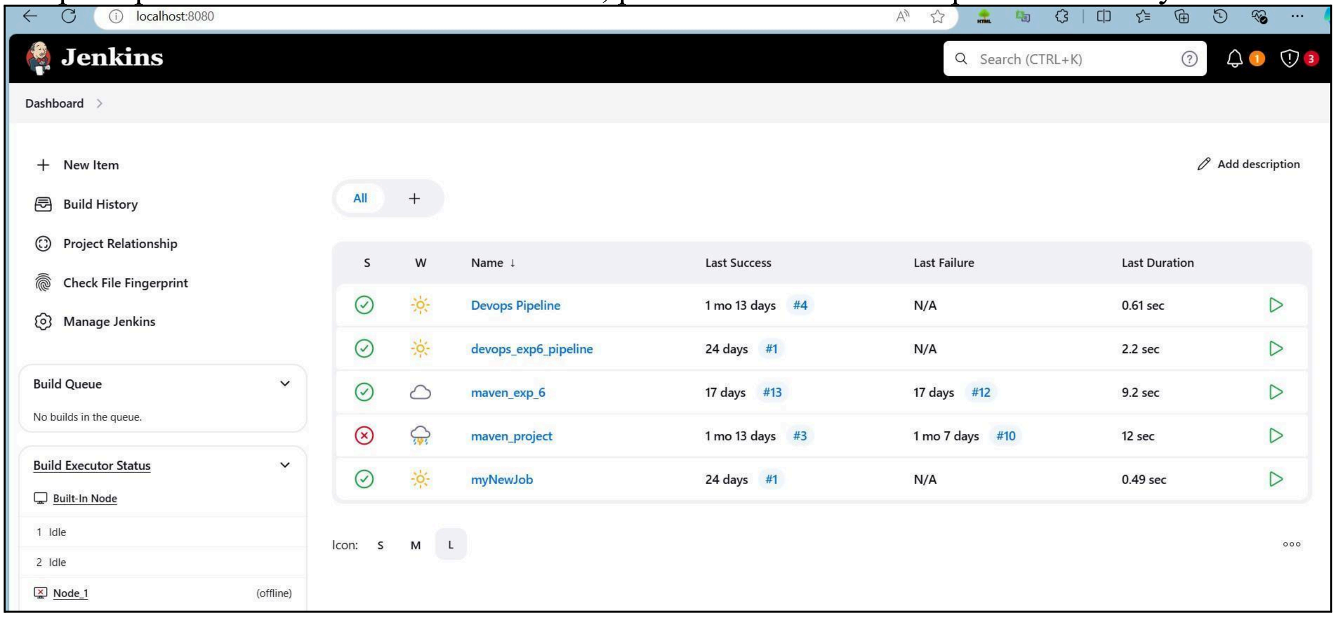
Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

Integrating Jenkins with SonarQube:

- Jenkins installed
- Docker Installed (for SonarQube)
- SonarQube Docker Image

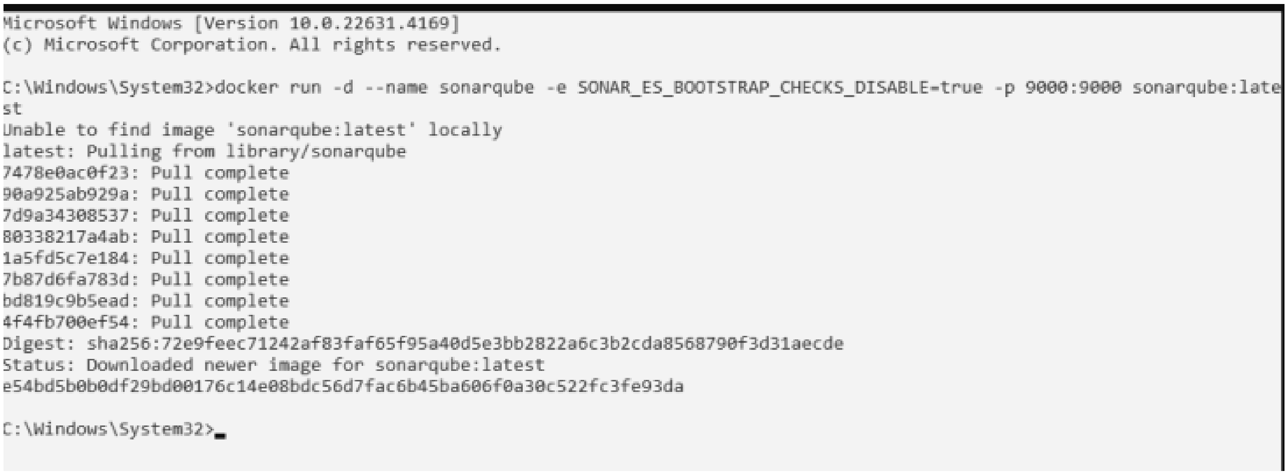
Steps to integrate Jenkins with SonarQube

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



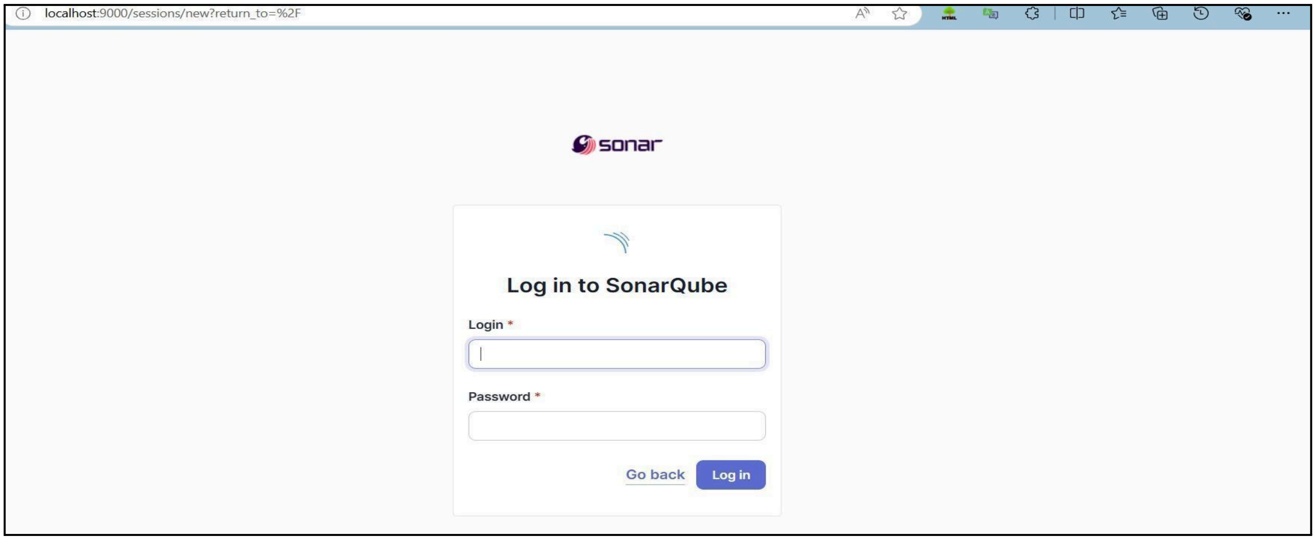
S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	Devops Pipeline	1 mo 13 days #4	N/A	0.61 sec
✓	☀	devops_exp6_pipeline	24 days #1	N/A	2.2 sec
✓	☁	maven_exp_6	17 days #13	17 days #12	9.2 sec
✗	⛈	maven_project	1 mo 13 days #3	1 mo 7 days #10	12 sec
✓	☀	myNewJob	24 days #1	N/A	0.49 sec

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



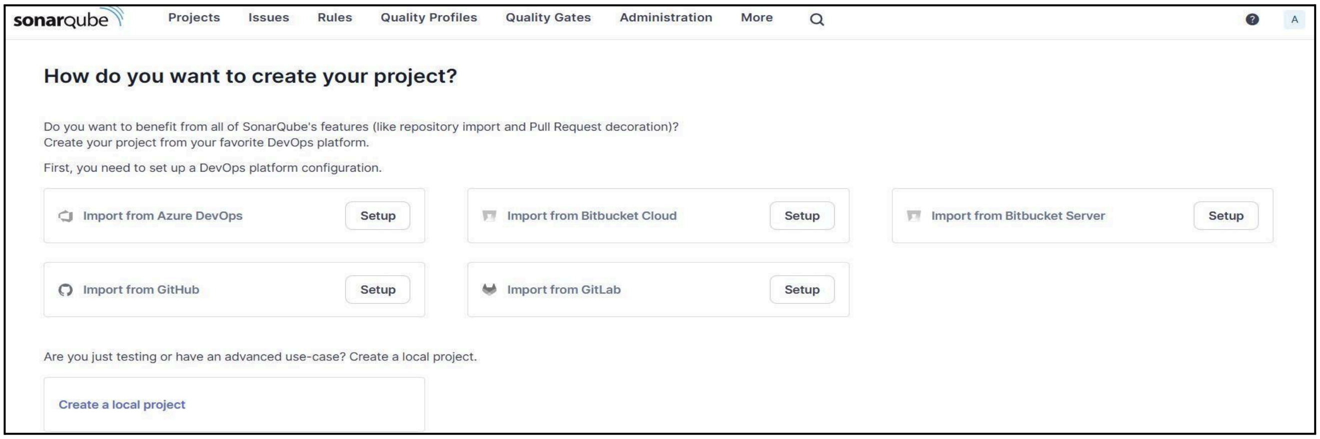
```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:late
st
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
e54bd5b0b0df29bd00176c14e08bdc56d7fac6b45ba606f0a30c522fc3fe93da

C:\Windows\System32>
```

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



localhost:9000/sessions/new?return_to=%2F

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



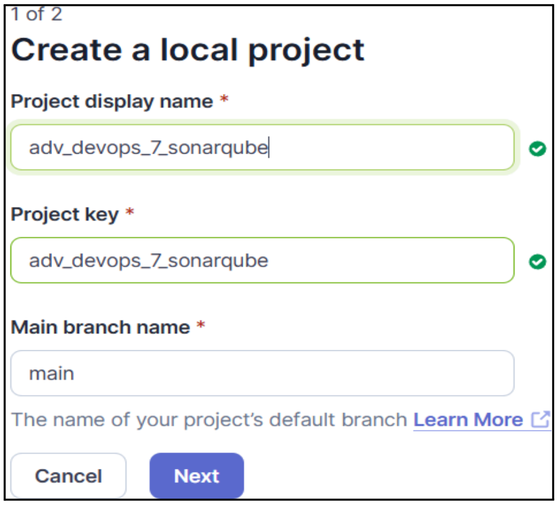
How do you want to create your project?

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.

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



1 of 2

Create a local project

Project display name *

adv_devops_7_sonarqube

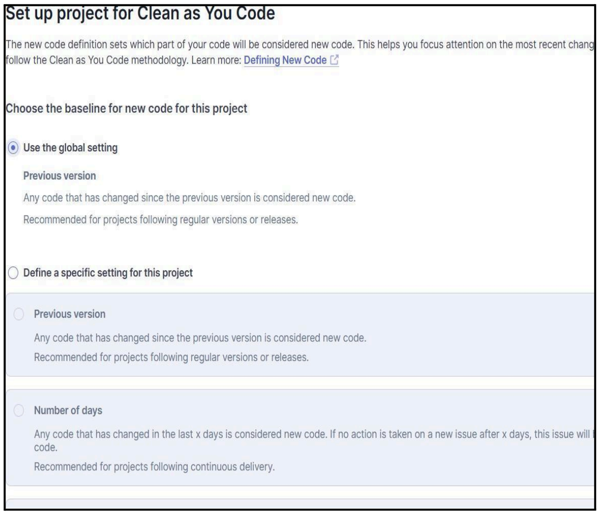
Project key *

adv_devops_7_sonarqube

Main branch name *

main

The name of your project's default branch Learn More



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 chang 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.

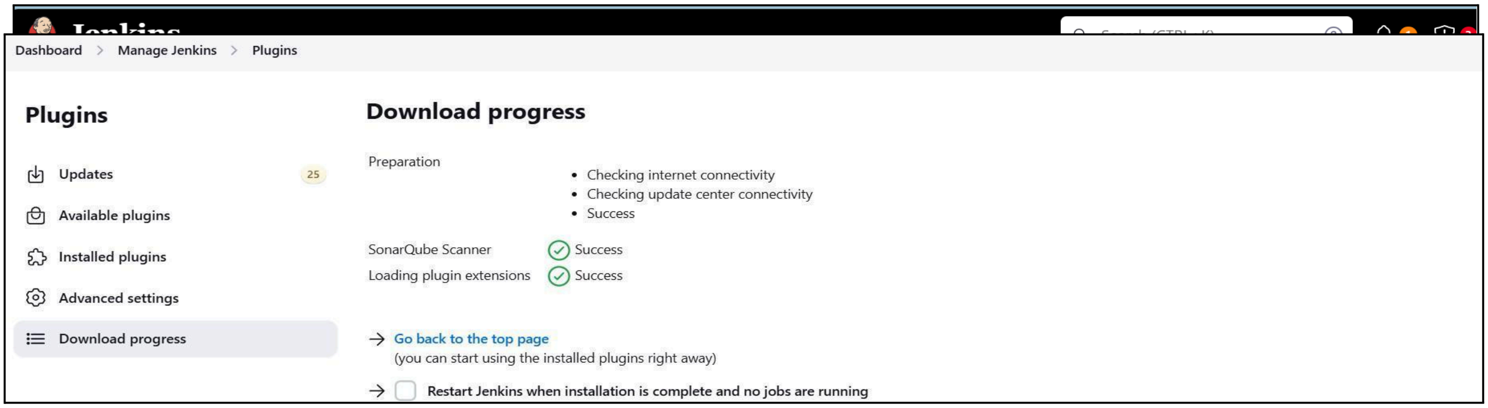
Recommended for projects following regular versions or releases.

○ 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 code.

Recommended for projects following continuous delivery.

Setup the project and come back to Jenkins Dashboard.
Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.


Dashboard > Manage Jenkins > Plugins

Plugins

- Updates 25
- Available plugins
- Installed plugins
- Advanced settings
- Download progress

Download progress

Preparation
- Checking internet connectivity
- Checking update center connectivity
- Success

SonarQube Scanner ✓ Success
Loading plugin extensions ✓ Success

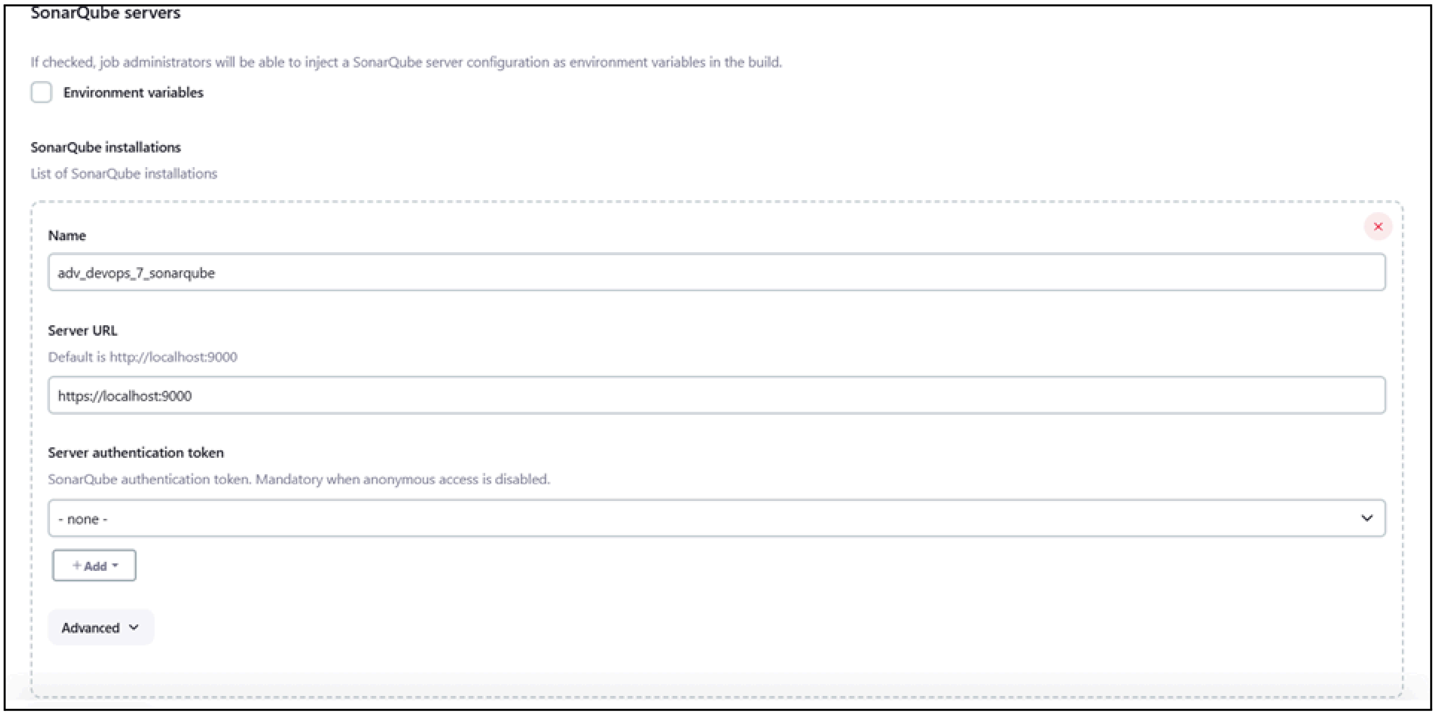
→ Go back to the top page
(you can start using the installed plugins right away)

→ □ Restart Jenkins when installation is complete and no jobs are running

6. Under Jenkins 'Manage Jenkins' then go to 'system', scroll and look for **SonarQube Servers**

and enter the details.
Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube>,here we have named it as **adv_devops_7_sonarqube**
In **Server URL** Default is http://localhost:9000


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
adv_devops_7_sonarqube

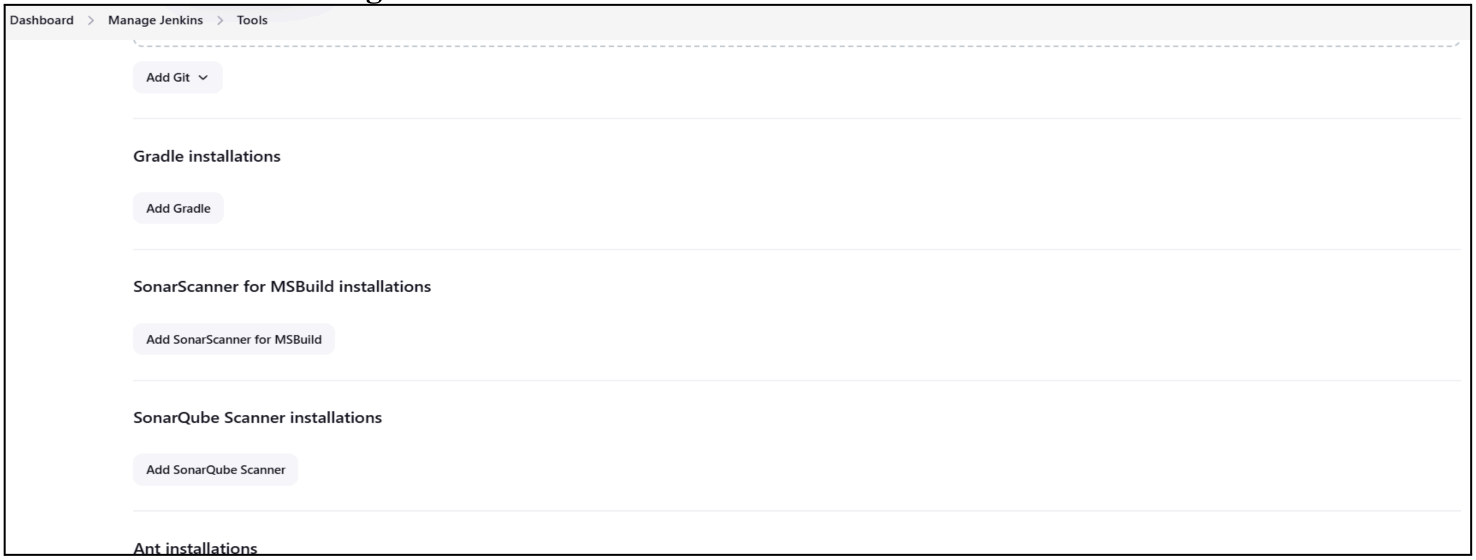
Server URL
Default is http://localhost:9000
https://localhost:9000

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.
- none -

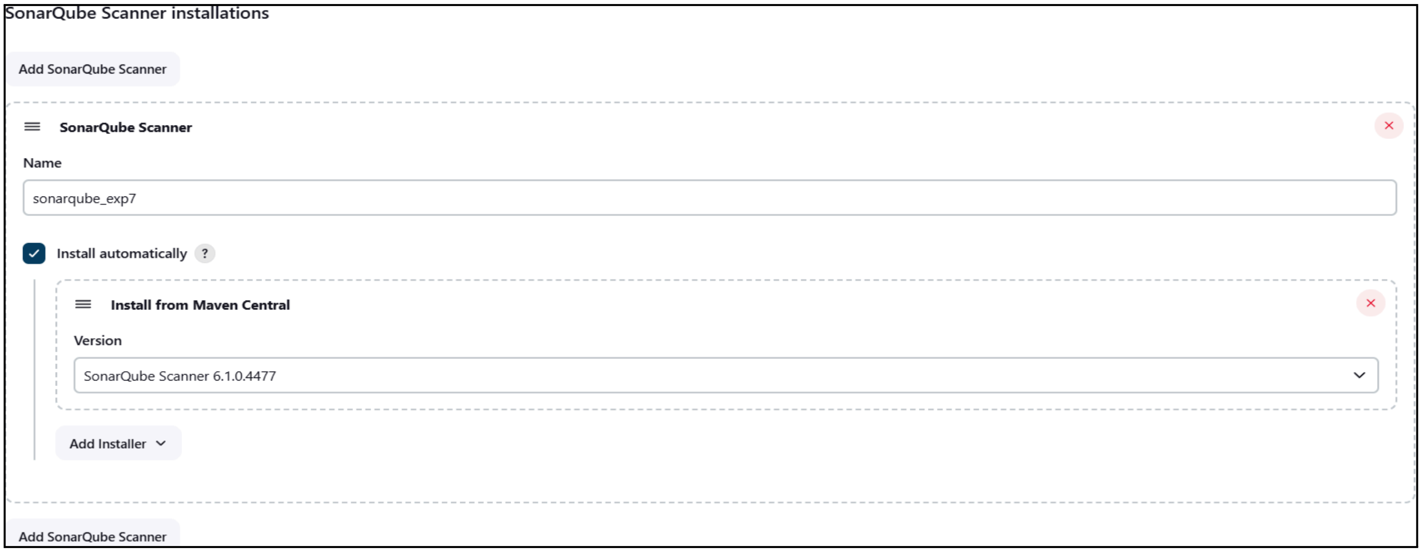
7. Search for SonarQube Scanner under Global Tool Configuration.

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools


Dashboard > Manage Jenkins > Tools
Add Git
Gradle installations
Add Gradle
SonarScanner for MSBuild installations
Add SonarScanner for MSBuild
SonarQube Scanner installations
Add SonarQube Scanner
Ant installations

Check the “Install automatically” option. → Under name any name as identifier → Check the “Install automatically” option.

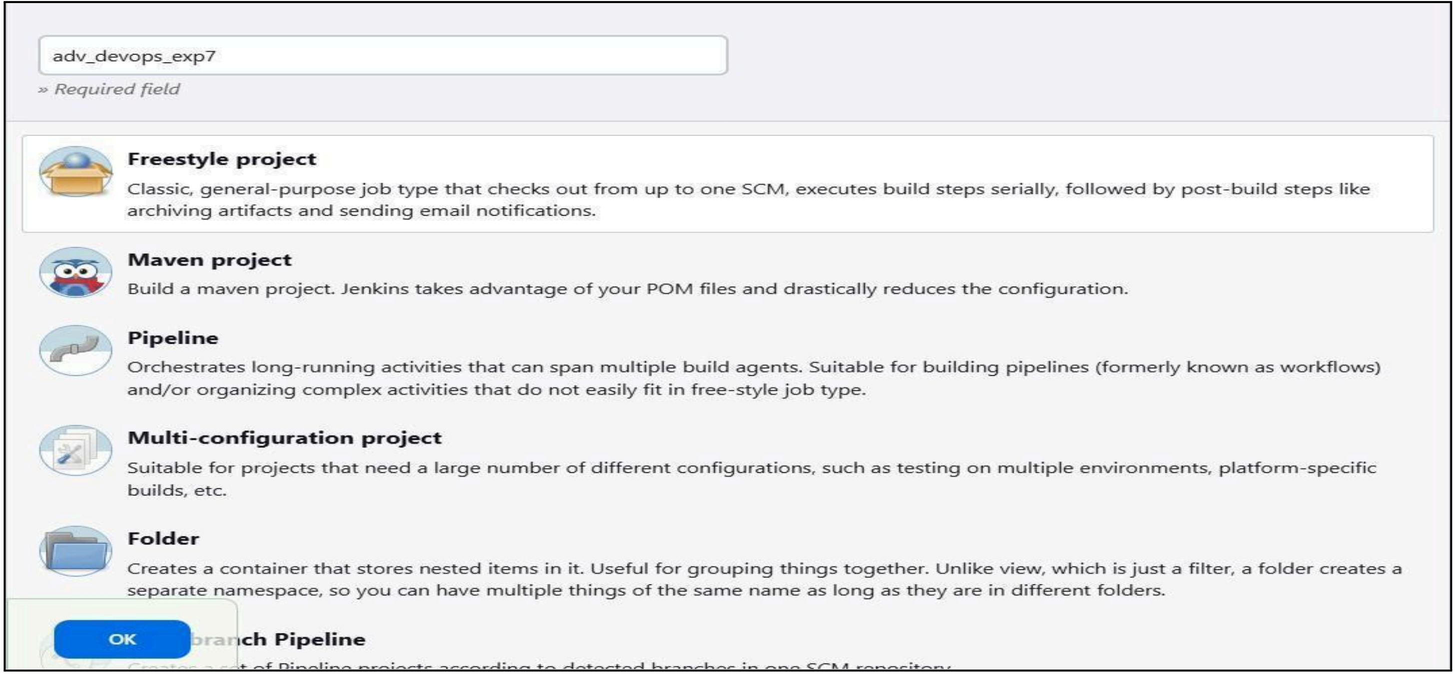


Name: sonarqube_exp7

☑ Install automatically

Version: SonarQube Scanner 6.1.0.4477

8. After the configuration, create a New Item in Jenkins, choose a freestyle project.



adv_devops_exp7

» 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.

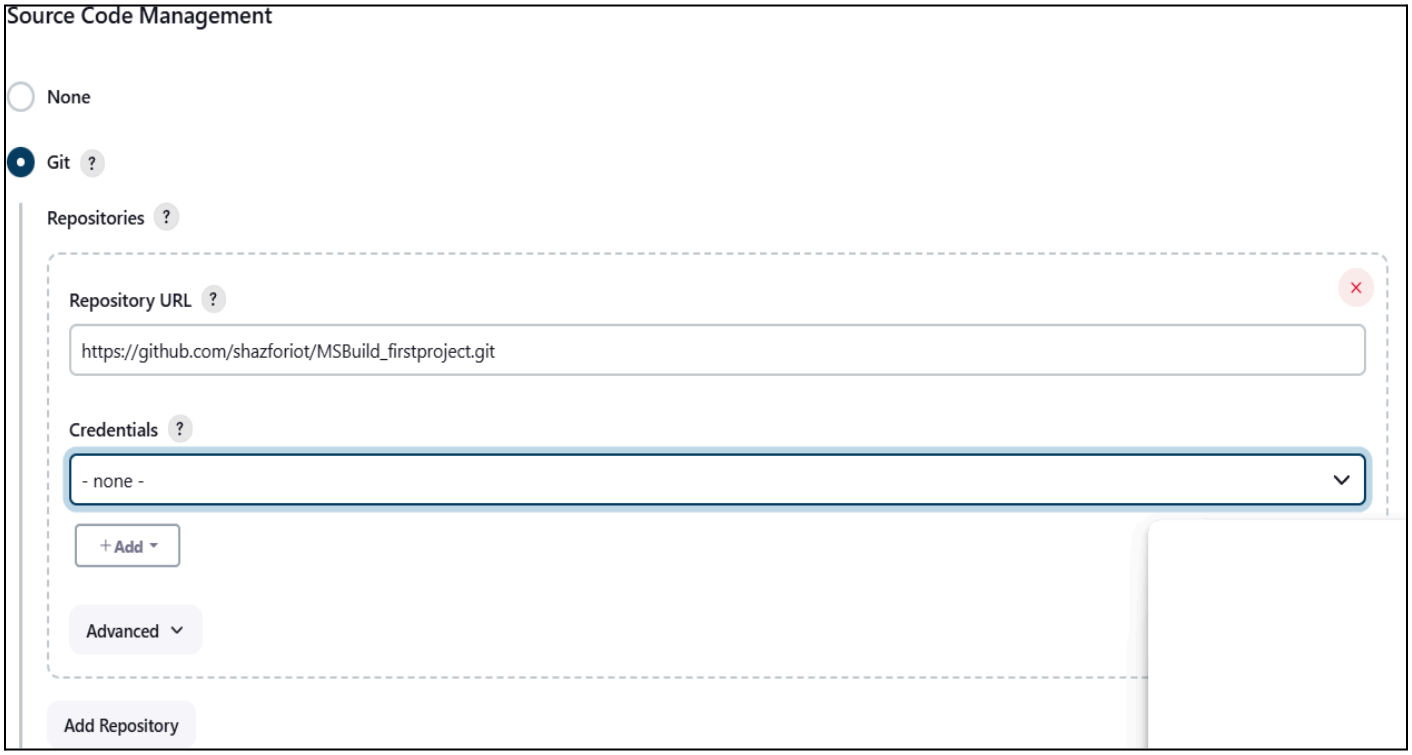
Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

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

branch Pipeline

9. Choose this GitHub repository in Source Code Management.
https://github.com/shazforiot/MSBuild_firstproject.git
It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.



Source Code Management

○ None

● Git ?

Repositories ?

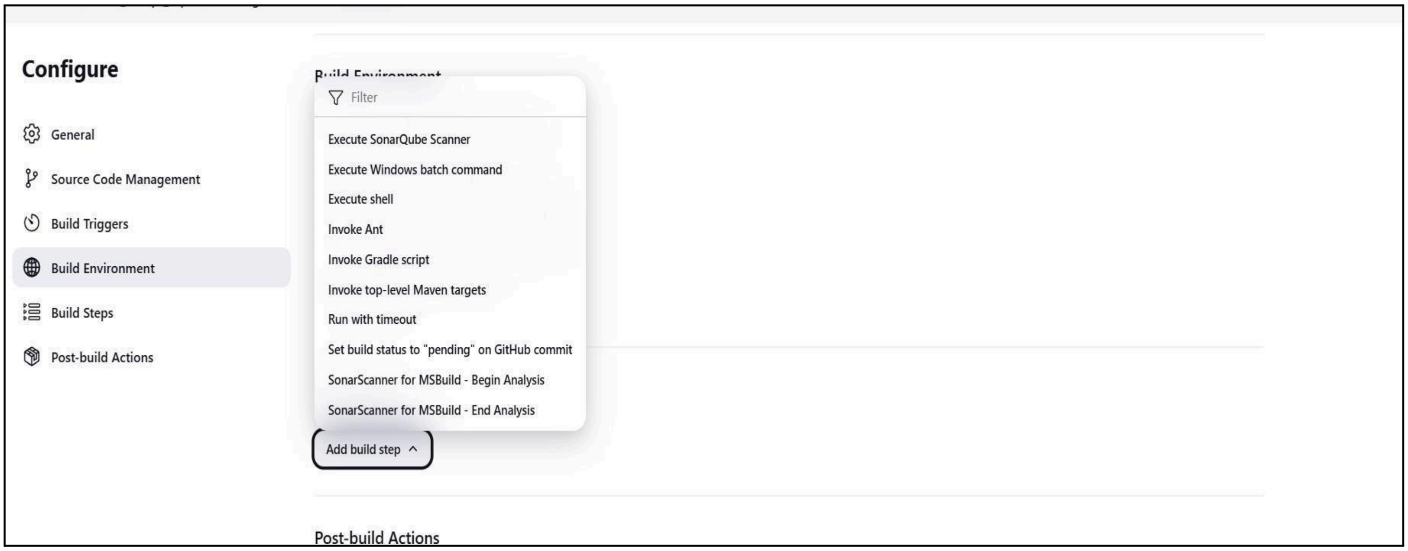
Repository URL ?

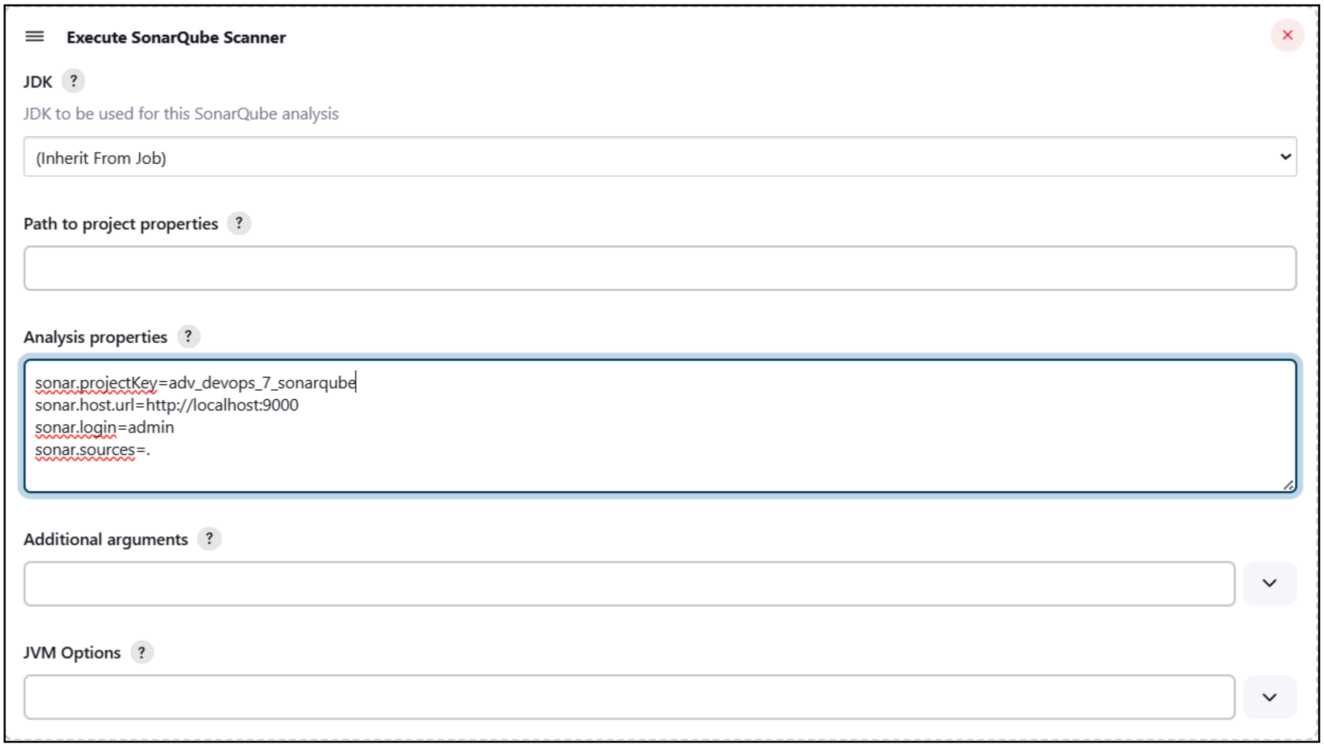
https://github.com/shazforiot/MSBuild_firstproject.git

Credentials ?

- none -

10. Under **Select project → Configuration → Build steps → Execute SonarQube Scanner**, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.


Configure
General
Source Code Management
Build Triggers
Build Environment
Build Steps
Post-build Actions
Build Environment
Filter
Execute SonarQube Scanner
Execute Windows batch command
Execute shell
Invoke Ant
Invoke Gradle script
Invoke top-level Maven targets
Run with timeout
Set build status to "pending" on GitHub commit
SonarScanner for MSBuild - Begin Analysis
SonarScanner for MSBuild - End Analysis
Add build step
Post-build Actions



JDK ?

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties ?

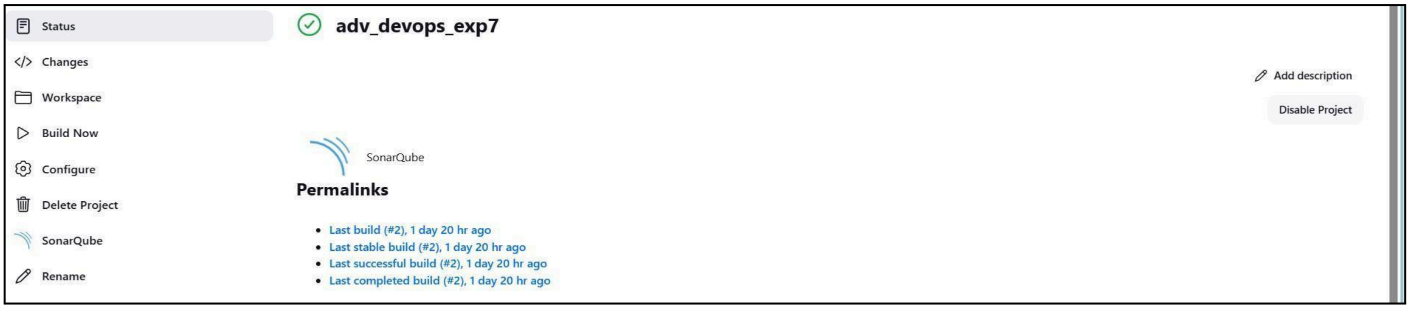
Analysis properties ?

```
sonar.projectKey=adv_devops_7_sonarqube
sonar.host.url=http://localhost:9000
sonar.login=admin
sonar.sources=.
```

Additional arguments ?

JVM Options ?

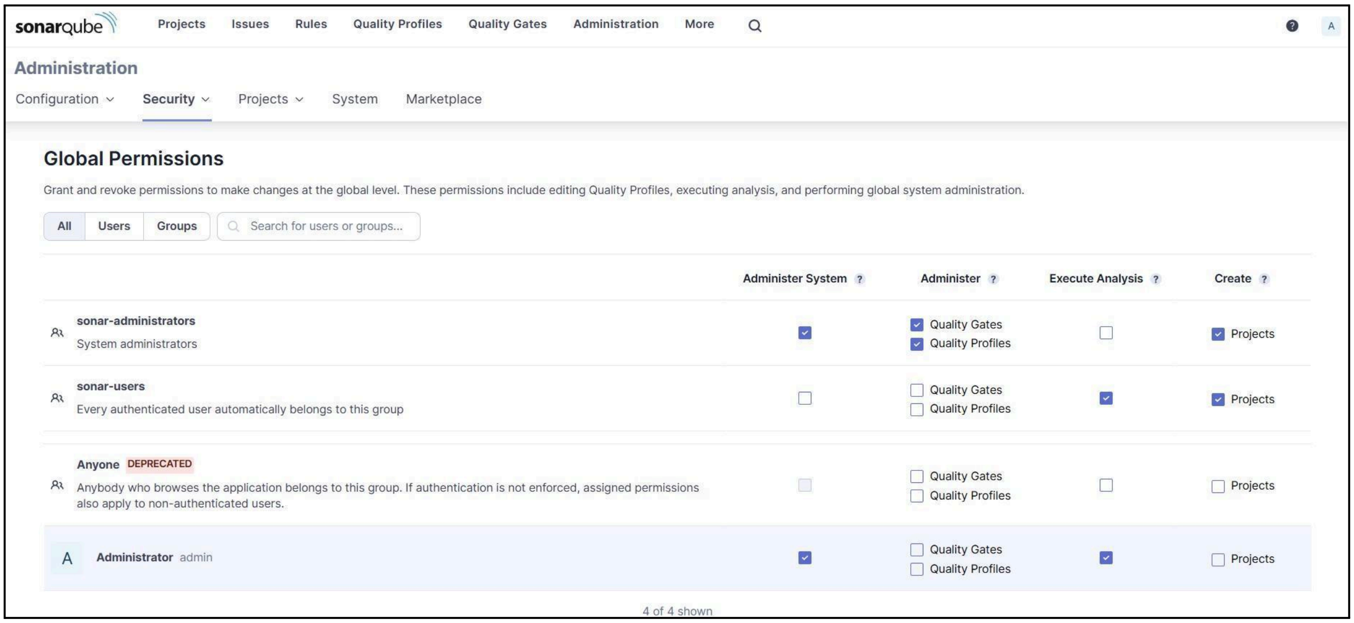
Then save



Permalinks

- Last build (#2), 1 day 20 hr ago
- Last stable build (#2), 1 day 20 hr ago
- Last successful build (#2), 1 day 20 hr ago
- Last completed build (#2), 1 day 20 hr ago

11. Go to http://localhost:9000/<user_name>/permissions and allow Execute Permissions to the Admin user



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

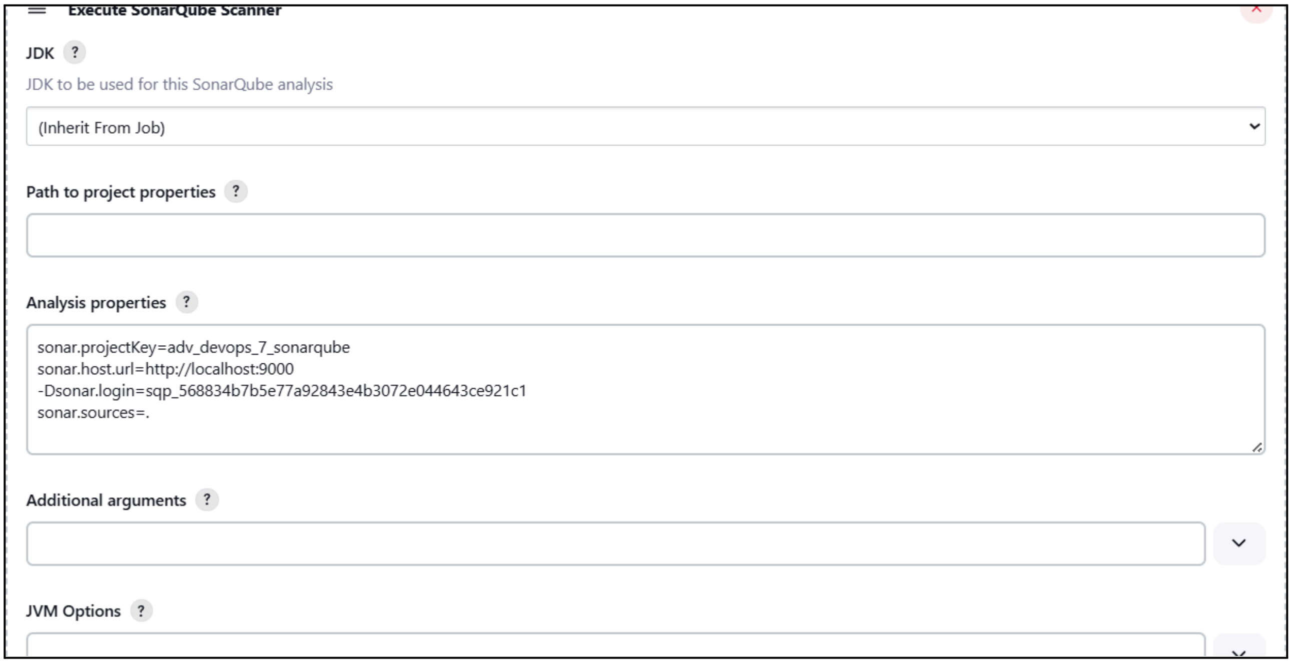
IF CONSOLE OUTPUT FAILED:

Step 1: Generate a New Authentication Token in SonarQube

1. **Login to SonarQube:**
   - Open your browser and go to **http://localhost:9000**.
   - Log in with your admin credentials (default username is **admin**, and the password is either **admin** or your custom password if it was changed).
2. **Generate a New Token:**
   - Click on your **username** in the top-right corner of the SonarQube dashboard.
   - Select **My Account** from the dropdown menu.
   - Go to the **Security** tab.
   - Under **Generate Tokens**, type a name for the token (e.g., "Jenkins-SonarQube").
   - Click **Generate**.
   - Copy the token and save it securely. You will need it in Jenkins.

Step 2: Update the Token in Jenkins

1. **Go to Jenkins Dashboard:**
   - Open Jenkins and log in with your credentials.
2. **Configure the Jenkins Job:**
   - Go to the job that is running the SonarQube scanner (adv_devops_exp7).
   - Click **Configure**.
3. **Update the SonarQube Token:**
   - In the SonarQube analysis configuration (either in the pipeline script or under "Build" section, depending on your job type), update the sonar.login parameter with the new token.



JDK

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties

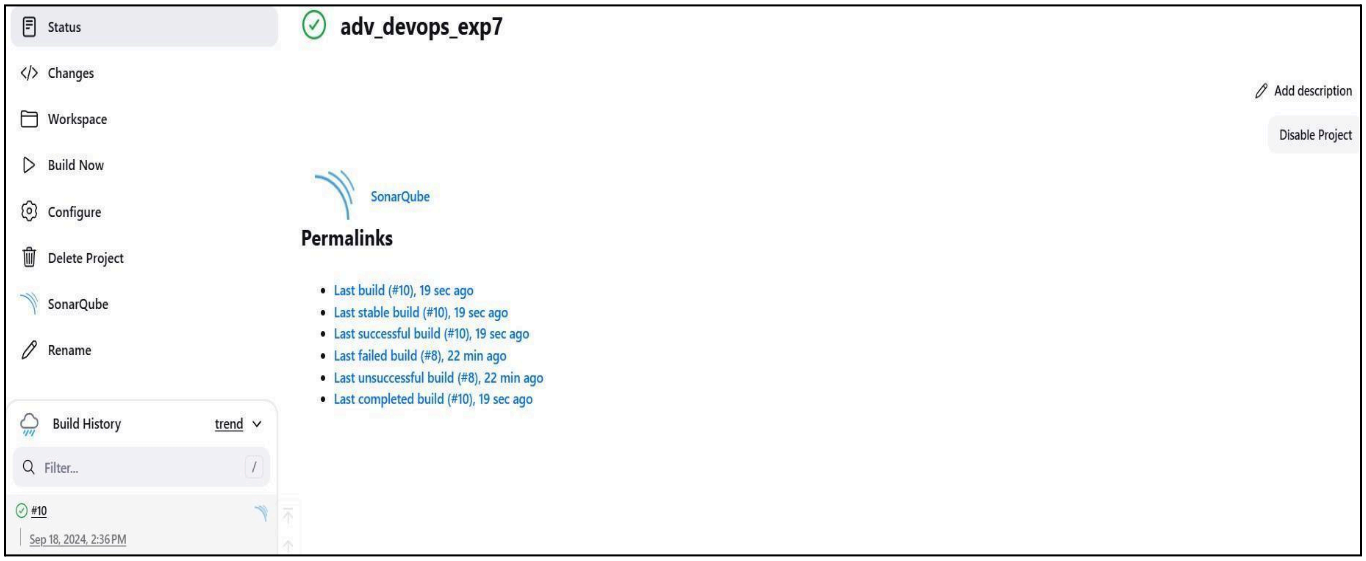
Analysis properties

```
sonar.projectKey=adv_devops_7_sonarqube
sonar.host.url=http://localhost:9000
-Dsonar.login=sqp_568834b7b5e77a92843e4b3072e044643ce921c1
sonar.sources=.
```

Additional arguments

JVM Options

12.Run the Jenkins build.



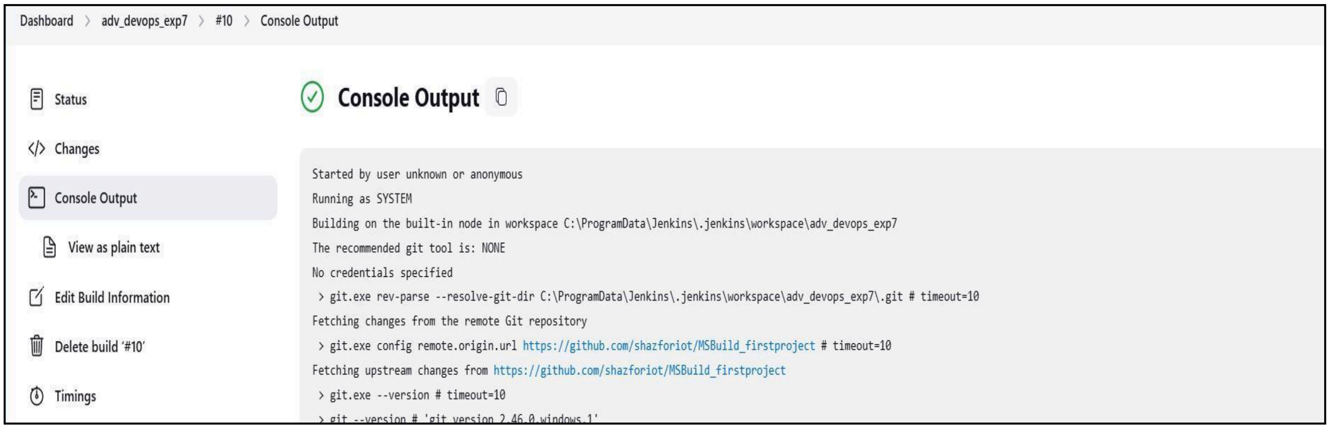
adv_devops_exp7

Permalinks

- Last build (#10), 19 sec ago
- Last stable build (#10), 19 sec ago
- Last successful build (#10), 19 sec ago
- Last failed build (#8), 22 min ago
- Last unsuccessful build (#8), 22 min ago
- Last completed build (#10), 19 sec ago

#10 Sep 18, 2024, 2:36 PM

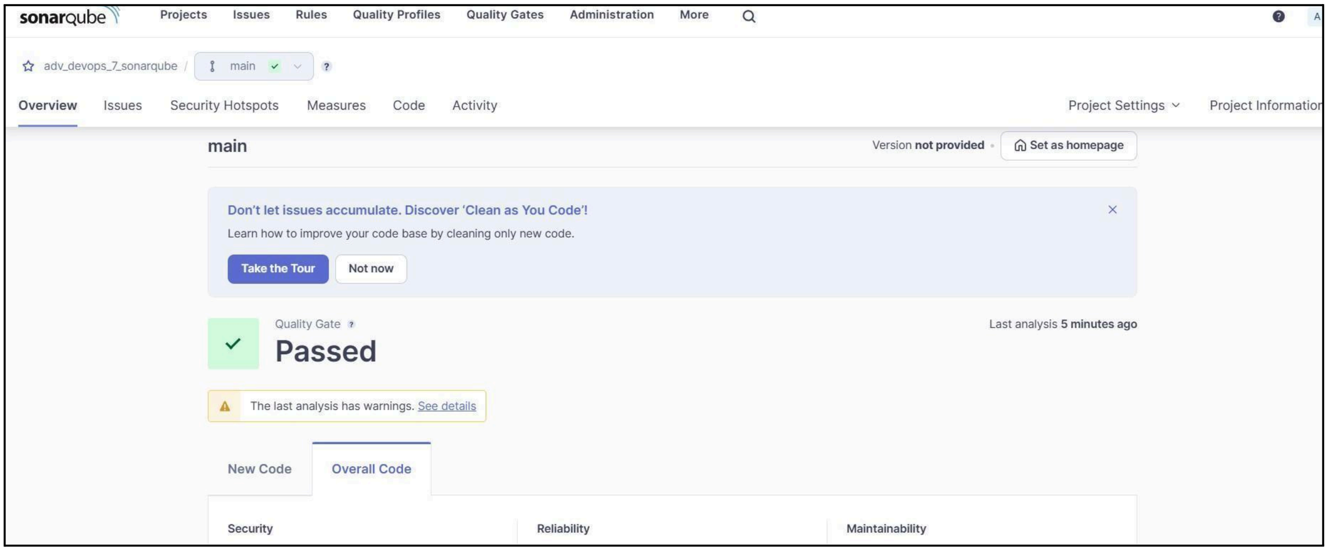
Check the console Output



Console Output

```
Started by user unknown or anonymous
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\.jenkins\workspace\adv_devops_exp7
The recommended git tool is: NONE
No credentials specified
 > git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\adv_devops_exp7\.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'
```

13.Once the build is complete, check project on SonarQube



main

Version **not provided**

Don't let issues accumulate. Discover 'Clean as You Code'!

Learn how to improve your code base by cleaning only new code.

Quality Gate

✓ **Passed**

Last analysis **5 minutes ago**

The last analysis has warnings. See details