**Sonar Qube**

=====================================================================-

**09-DevOps -21-OCT-24**

- Code Quality Checking Tool

- Using SonarQube we can perform code review to identify developers mistakes in the code

- SonarQube s/w developed by using Java Language

- SonarQube supports 30+ Programming Languages to perform Code Review

- Using SonarQube we can generate Code Review Report

- DevOps team is responsible to generate Project Code Review Report and share it with Development team.

**Note: Development is responsible to fix sonar issues.**

**Note: Code Review is part of project build process.**

=====================================================================-

**Sonar Issues**

=====================================================================-

- SonarQube server will identify below types of issues in the project

- Bugs (danger, It will harm our code execution)

- Critical problem, critical mistake that are available in project is called as bugs

- Vulnerabilities (security hotspots)

- Securities available in code that are called as vulnerabilities

- Customers password without encryption, customers numbers, pin code, any kind of . Personal data (PII data personal identification information data)

-Security related issues.

**Ex** – we have aadhar-card in our coutry with the aadhar number we can identify persons information

**Code Smells** (not danger but week design in program)

* Minor issue
* Code will not fail but we need to handle that issues

- Duplicate Code Blocks (Repeated code)

- Code Coverage (how many lines of code is tested in unit testing)

=====================================================================-

**Sonar Quality Profiles**

=====================================================================-

1. Quality Profile : Set of rules to perform code review

- In SonarQube, for every language one Quaylity Profile is available with set of rules to perform code review.

- When we perform code review using sonar then it will identify our project developed using which language based on that it will execute that language specific quality profile to perform code review.

Java Project --------> Java Quality Profile ---> Java Rules

Python Project -------> Python Quality Profile ---> Python Rules

PHP Project ----------> PHP Quality Profile ---> PHP Rules

=====================================================================-

**Sonar Quality Gate**

=====================================================================-

- Quality Gate Represents overall project code quality is Passed or Failed.

Note: If Code Quality Gate is Failed, we should not deploy that code.

=====================================================================-

**SonarQube Server Setup**

=====================================================================-

* Create a instance using t3 medium minimum 4gb ram required.
* Then open gitbash and check docker version
* We need to install docker in linux VM
* Open ashokit github profile
* Devops-Documents 🡪 Sonar-setup-docker
* Paste this Command

sudo yum update -y

sudo yum install docker -y

sudo service docker start

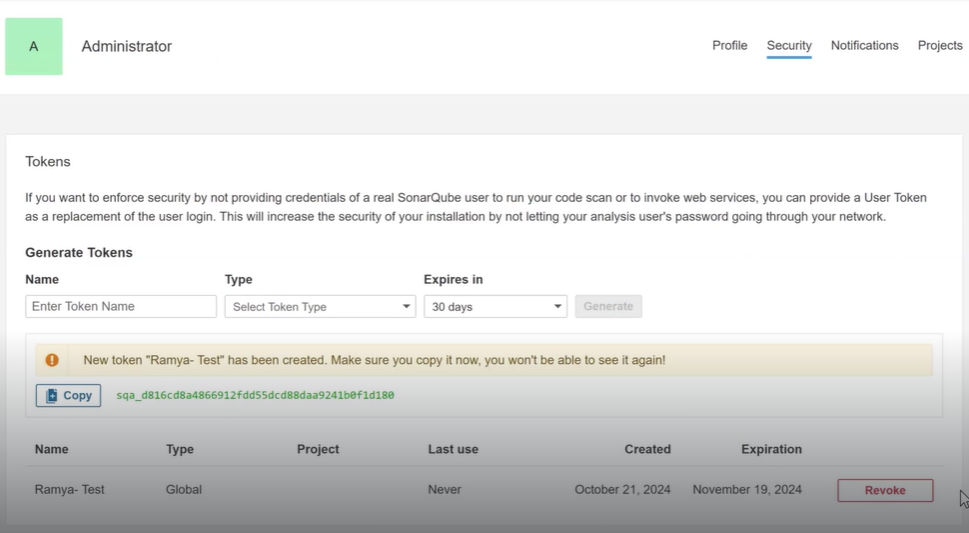
sudo usermod -aG docker ec2-user

exit

* Docker –v
* Skip 3-4 step
* Copy 5th step command
* docker run -d --name sonarqube -p 9000:9000 -p 9092:9092 sonarqube:lts-community
* go to the AWS and add security group enable port 9000
* sonar qube by default runs on 9000 port
* then copy public ip of sonar-qube vm and paste into brower 13.53.218.18:9000
* open sonar-Qube and click on profile🡪my account🡪security

**Sonar Token**

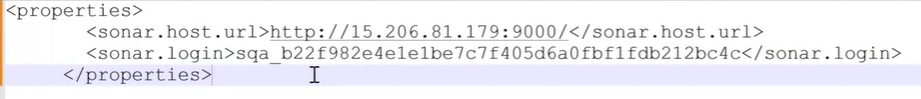
* sonar server is running in dockeer container and my application is available in windows machine , my application code review I want to perform using sonar-qube so we need to tintegrate sonar server with application in order to perform code review
* we can do the review using username and password but it is not recommended because username and password should not see every-body.
* We will generate sonar token for sonar details in order to perform code review.

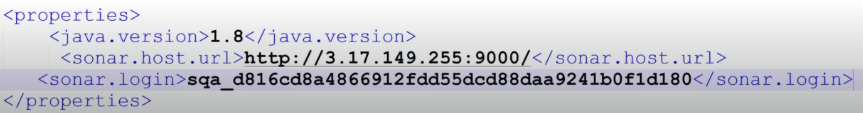


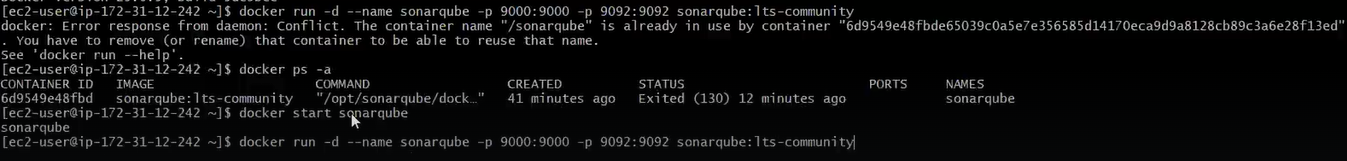
* Copy the token and save in notepad file.
* This sonar token we need to configure in our application for code review of our application

Que - How to integrate sonar server in maven application ?

Ans –

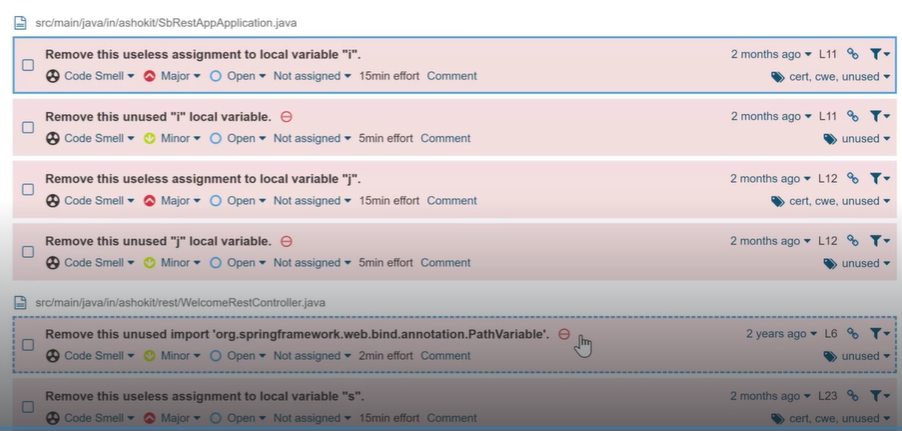


* In sonar host it will tell you where your sonar server is available.
* We need to give public ip of our linux machine in sonar host
* Copy sonar token and paste into the sonar.login
* In maven POM.xml we need to configure this
* Clone git repository
* Open pom.xml in notepad and paste the code
* 
* Maven clean package
* And run Command – mvn sonar:sonar this is the command that perform code review
* Go to the sonar qube and click on project our project report is available
* After completion task saonar server is also stopped so we need to start again
* For that run fifth command
* docker run -d --name sonarqube -p 9000:9000 -p 9092:9092 sonarqube:lts-community

\*\*\*\*\*\*\*\*\*\*If want to start sonar server again\*\*\*\*\*\*\*\*\*\*\*

**Interview question**

Que – what are the bugs you identified in sonarqube ?

Ans - 

Note – this is a manual process in realtime we will not do manual process , this task is done by using Jenkins

Ex- clone git repo , build the code , code review everything is done by Jenkins pipeline

If Quality gate is passed in sonarqube we will deploy the application , if not passed we will not deploy.

Sonar Setup Doc : https://github.com/ashokitschool/DevOps-Documents/blob/main/06-Sonar-Setup-Docker.md

- Below are the default credentials to login into server

username: admin

password: admin

=====================================================================-

**Integrate Sonar server with Java Maven App**

=====================================================================-

Step-1 : Generate sonar token for integration

Go to Sonar Server Dashboard -> Click on profile -> My Account -> Security -> Generate Token

Step-2 : Clone git repository : https://github.com/ashokitschool/SB-REST-H2-DB-APP

Step-3 : Configure Sonar Server details under <properties/> tag in "pom.xml" file below

<properties>

<sonar.host.url>http://15.206.81.179:9000/</sonar.host.url>

<sonar.login>sqa\_b22f982e4e1e1be7c7f405d6a0fbf1fdb212bc4c</sonar.login>

</properties>

Step-4 : Then build the project using "mvn sonar:sonar" goal

=====================================================================-

**Quality Profile**

=====================================================================-

-> For each programming language sonar qube provided one quality profile with set of rules

-> Quality Profile means set of rules to perform code review

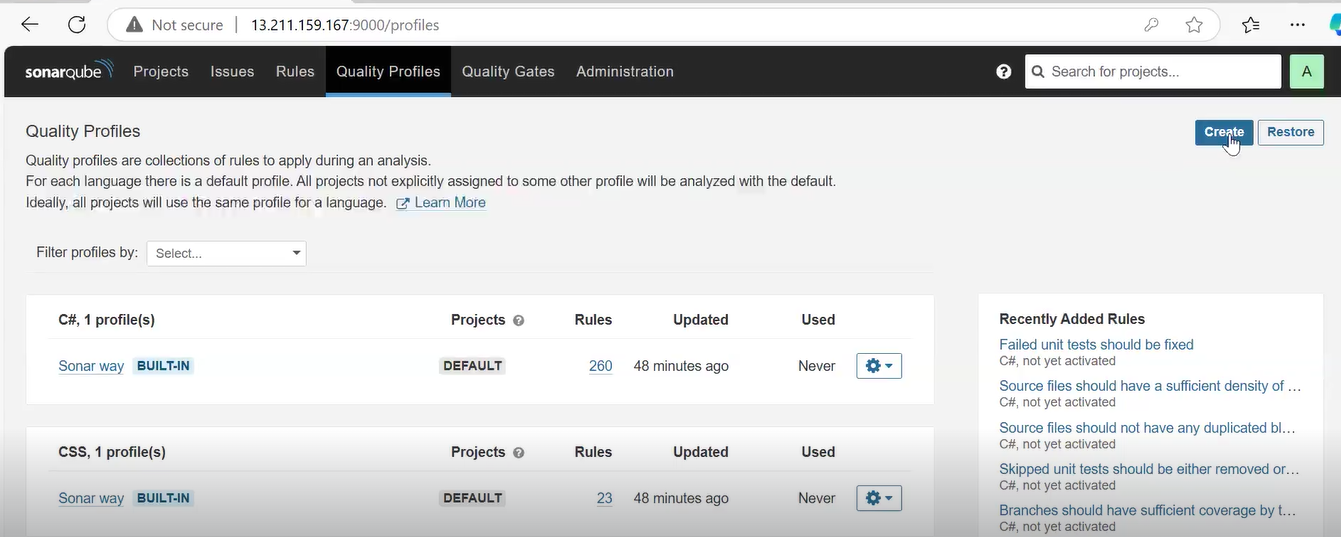
-> We can create our own quality profile based on project requirement

-> Create One Quality Profile

- Name : SBI\_Project\_QP

- Language: Java

- Parent : None



Note: We can make our quality profile as default one then it will be applicable for all the projects which gets reviewed under this sonar server.

Note: If we have any common ruleset for all projects then we can create one quality profile and we can use that as parent quality profile for other projects.

-> We can configure custom quality profile to a specific project using below steps

- Click on project name

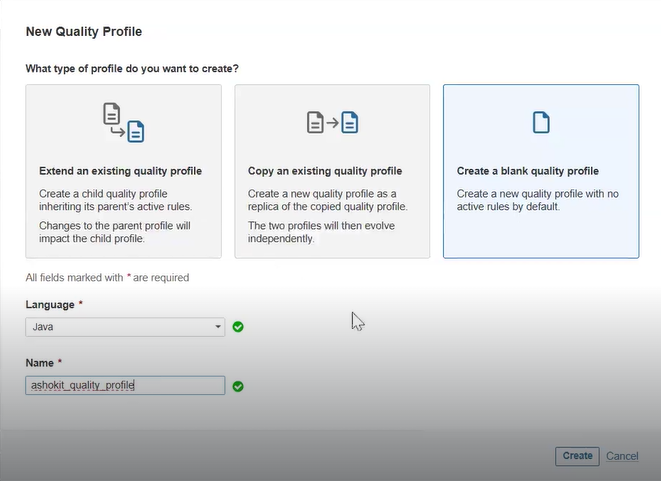
- Go to administration

- Click on quality profile

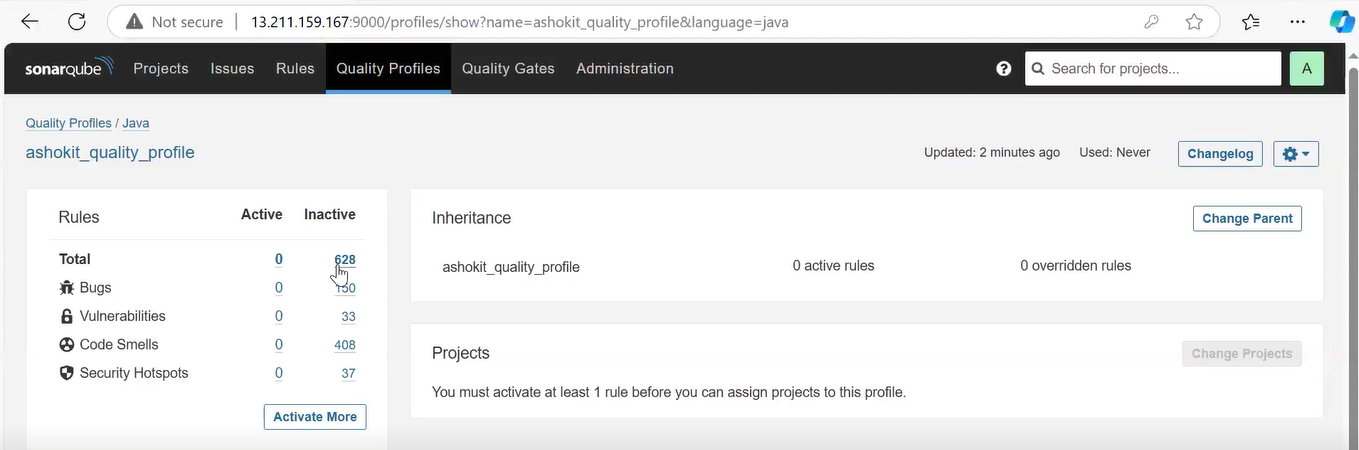
- Select profile required

Que -How to create a quality profile ?

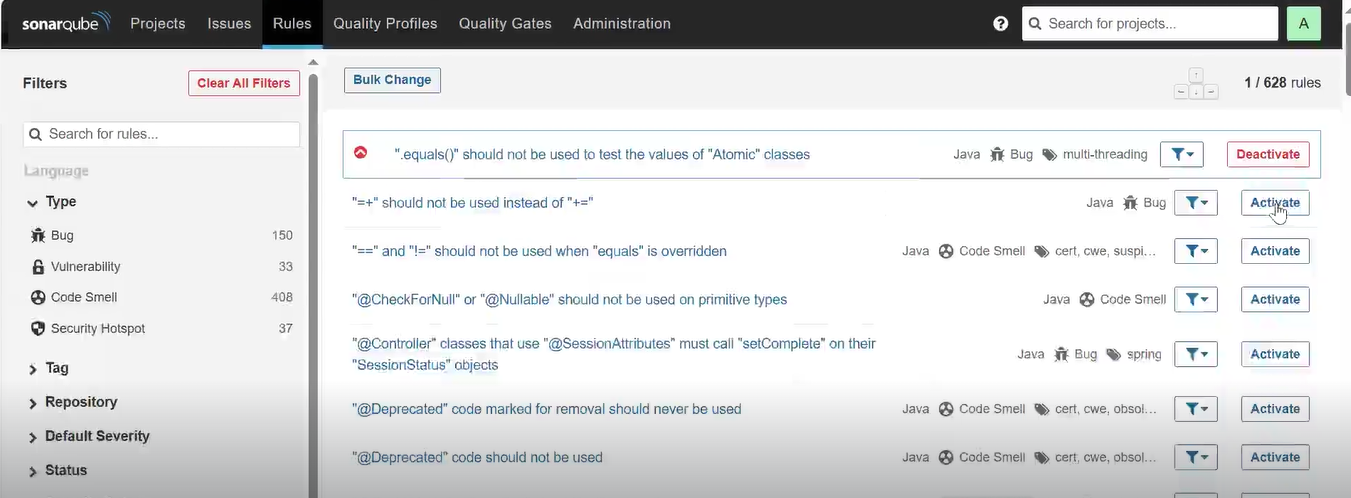
Ans – Click on create



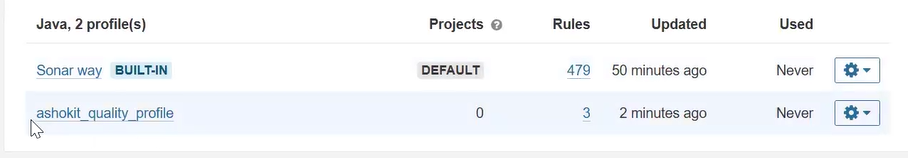
* Already one quality profile is created by default quality profile I can say built in quality profile.
* I don’t want a built in quality profile I want my own quality profile, so I have created one.



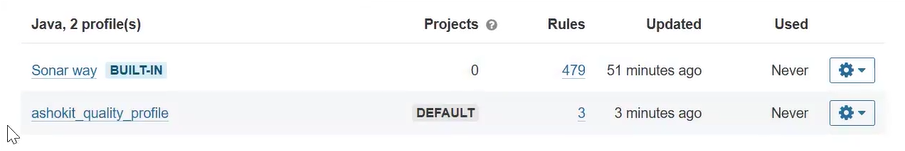
* We need to add rule in order to perform the code review.
* Click on activate more



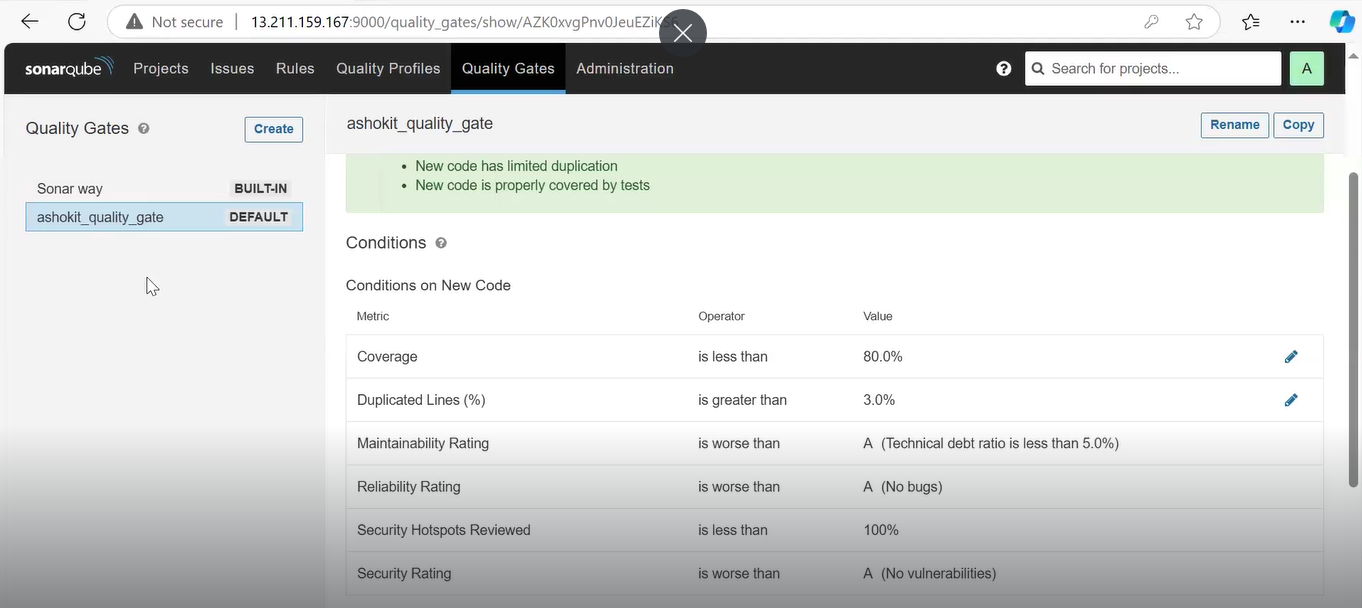
* Add rules according to project requirements.



* Click on settting icon and make our quality profile as a default



* Code review will happen based on our review
* We can also create quality gate



* We can customize quality gate conditions .

=====================================================================-

**Quality Gate**

=====================================================================-

-> Quality Gate represents set of metrics to identify project quality is Passed or Failed

-> Every Project Quality Gate should be passed

-> In Sonar We have default Quality Gate

-> If required, we can create our own Quality Gate also

=====================================================================

Conclusion

=====================================================================

-> If project quality gate is failed then we should not accept that code for deployment.

-> If project is having Sonar issues then development team is responsible to fix those issues

-> As a DevOps engineer, we will perform Code Review and we will send Code Review report to Development team (we will send sonar server URL to development team)

=====================================================================

Summary

=====================================================================

1) What is SonarQube

2) What is Code Review

3) Sonar Server setup in Linux Machine

4) Sonar Server Integration in Maven Project

5) Sonar Token Generation

6) Sonar Server Issue Types

7) Quality Profiles

8) Quality Gates