**SonarQube – Code Quality Tool for DevOps**

**📌 Introduction & Architecture**

**What is SonarQube?**  
SonarQube is an open-source platform that performs **static code analysis** to detect bugs, vulnerabilities, and code smells in applications. It helps improve code quality, maintainability, and security.

**Languages Supported:** Java, JavaScript, Python, C#, PHP, etc.

**🏗️ Architecture Overview**

* **Developer** writes code and pushes to VCS (e.g., GitHub).
* **CI/CD Tool** (like Jenkins) triggers a SonarQube scan using the Sonar Scanner.
* **Sonar Scanner** sends analysis data to the **SonarQube Server**.
* SonarQube Server evaluates it against **Quality Gates** and stores results in its **Database**.
* Results are viewed through the **Web UI**.

📌 **Components:**

* SonarQube Server
* PostgreSQL/MySQL DB (backend storage)
* Sonar Scanner (CLI or integrated in Jenkins/Maven/Gradle)

**Sonarqube Instalation steps:  
  
Install Java (SonarQube requires Java 17 for the latest versions)**

Login to aws account and create sonarqube-server(ubuntu)

**Security group Open Port 9000**

In AWS Security Group:

* Go to **EC2 →Sonarqueserver🡪 Security Groups → Inbound Rules → Edit**
* Add a rule:
  + **Type:** Custom TCP Rule
  + **Port Range:** 9000
  + **Source:** select anywhereIPV4 and save it

login sonarqubeserver

sudo su –

sudo apt update

sudo apt install openjdk-17-jdk -y

Verify Java:

java -version

**Create a Dedicated SonarQube User**

SonarQube cannot run as root.

sudo useradd -m -d /opt/sonarqube sonar

sudo passwd sonar

**Download & Install SonarQube**

cd /opt

sudo wget https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-10.4.1.88267.zip

sudo apt install unzip -y

sudo unzip sonarqube-10.4.1.88267.zip

sudo mv sonarqube-10.4.1.88267 sonarqube

**Set Permissions**

sudo chown -R sonar:sonar /opt/sonarqube

**Configure Port (Optional - Default: 9000)**

Edit sonar.properties if you want to change the port:

sudo vi /opt/sonarqube/conf/sonar.properties

Uncomment & modify:

sonar.web.port=9000

*(You can change it to another port if needed.)*

**Start SonarQube as Non-Root User**

su - sonar

cd /opt/sonarqube/bin/linux-x86-64/

!!!![[[we got some eeror message

Then after we check pwd

We show as /opt/sobarcube

Then ls command is used

Then after we some sonarqube+number or id

logs sonarqube-10.4.1.88267 sonarqube-10.5.1.90531 some like

->we excute cd sonarqube-10.4.1.88267/bin/linux-x86-64

Ls command used

We show as SonarQube.pid sonar.sh

Then after we can start and status command used and give public id run it in server

./sonar.sh start

./sonar.sh status

**Access SonarQube UI**

Open in browser:

http://<server-publicip>:9000

(Default credentials: **admin / admin**)

**👥 Users, Tokens, Quality Profiles/Gates**

**✅ Create Users & Tokens:**

* Go to: **Administration → Security → Users**
* Click **Generate Token** for a user (used in CI tools like Jenkins or CLI Sonar Scanner)

**✅ Quality Profiles:**

* Define coding standards per language.
* Example: Disallow duplicate code in Java projects.

**✅ Quality Gates:**

* A set of rules that **must be passed** for code to be "clean":
  + No new bugs
  + Code coverage ≥ 80%
  + No duplicated blocks

🛑 If these rules fail → CI/CD pipeline fails!

**📧 Email Configuration**

Edit the conf/sonar.properties file:

sonar.email.smtp\_host.secured=true

sonar.email.smtp\_host=mail.smtpserver.com

sonar.email.smtp\_port=587

sonar.email.smtp\_username=admin@example.com

sonar.email.smtp\_password=yourpassword

sonar.email.from=admin@example.com

sonar.email.prefix=[SonarQube]

📩 Useful to send reports and alerts after analysis.

**📁 Project Creation & Static Code Analysis**

**✅ Steps to Analyze a Java Project**

1. **Login** → Create a new project from the UI.
2. Name: demo-java-app
3. Generate a **Project Token**.
4. Install Sonar Scanner:

wget https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-5.0.1.3006-linux.zip

unzip sonar-scanner-5.0.1.3006-linux.zip

export PATH=$PATH:/your/path/sonar-scanner/bin

1. Create a **sonar-project.properties** file in your source directory:

sonar.projectKey=demo-java-app

sonar.projectName=Demo Java Application

sonar.sources=src

sonar.host.url=http://localhost:9000

sonar.login=<your-token>

1. Run the scan:

sonar-scanner

✔️ Results will appear in SonarQube Web UI.

**Summary**

| **Feature** | **Description** |
| --- | --- |
| SonarQube | Static code analysis tool |
| Port | Default 9000 |
| Quality Profiles | Define coding rules per language |
| Quality Gates | Enforce pass/fail criteria |
| Tokens | Used to securely connect scanner to server |
| Email Alerts | Notifies about quality issues |
| CI/CD Integration | Easy with Jenkins, GitHub Actions, etc. |