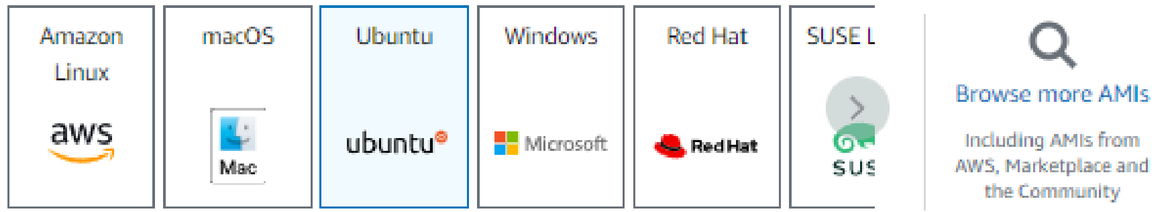
Project on

CI PIPELINE SETUP WITH VARIOUS TOOLS

(JENKINS, DOCKER, SONARQUBE, MAVEN, TRIVY(FOR DOCKER IMAGE SCAN))

Step 1 – Create the Ec2 instance in AWS account with these parameters

- EC2 type – Ubuntu t2.medium
- EBS volume – 30 GB
- Region – Asia Pacific (Mumbai)ap-south-1



Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0dee22c13ea7a9a67 (64-bit (x86)) / ami-0c8eea98010057bd0 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Architecture: 64-bit (x86)

AMI ID: ami-0dee22c13ea7a9a67

Username: ubuntu — Verified provider

Instance type

t2.medium
Family: t2 2 vCPU 4 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0496 USD per Hour
On-Demand Windows base pricing: 0.0676 USD per Hour
On-Demand RHEL base pricing: 0.0784 USD per Hour
On-Demand SUSE base pricing: 0.1496 USD per Hour

All generations

Compare instance types

Mumbai ▾ Aman Dandale

lFront Lambda CloudTrail IAM

Summary

Number of instances | Info

1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd64 noble image
ami-0dee22c13ea7a9a67

Virtual server type (instance type)
t2.medium

Firewall (security group)
default

Storage (volumes)
1 volume(s) - 30 GiB

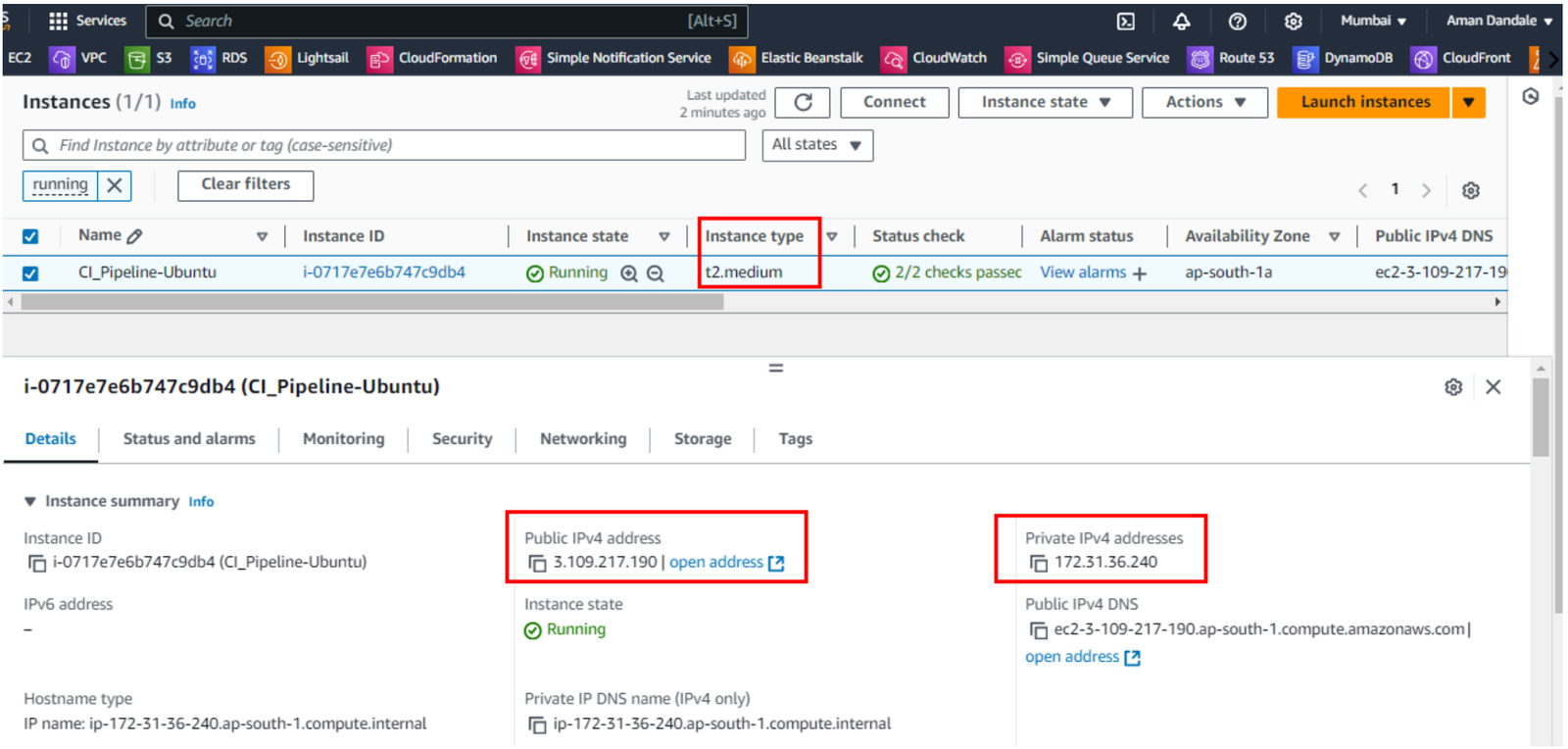
Cancel | Launch instance

Review commands

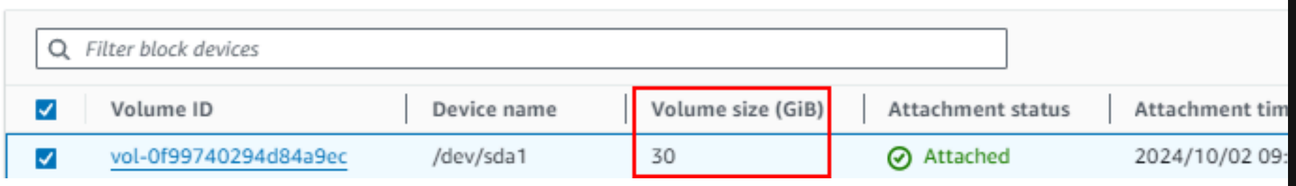
Configure storage Info

1x 30 GiB gp3 Root volume (Not encrypted)

Step 2 – Connect to EC2 and Install all tools in that system as root user



- Use your EC2 Private key properly
- Take SSH of your instance through MobXterm, VS code, Putty or CMD
- To login as root user - sudo su




```
ubuntu@ip-172-31-36-240:~$ sudo su
root@ip-172-31-36-240:/home/ubuntu# curl ifconfig.io
3.109.217.190
root@ip-172-31-36-240:/home/ubuntu# cd
root@ip-172-31-36-240:~# ifconfig
enX0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 172.31.36.240  netmask 255.255.240.0  broadcast 172.31.47.255
        inet6 fe80::1c:60ff:fe13:6c7b  prefixlen 64  scopeid 0x20<link>
        ether 02:fc:60:13:6c:7b  txqueuelen 1000  (Ethernet)
```

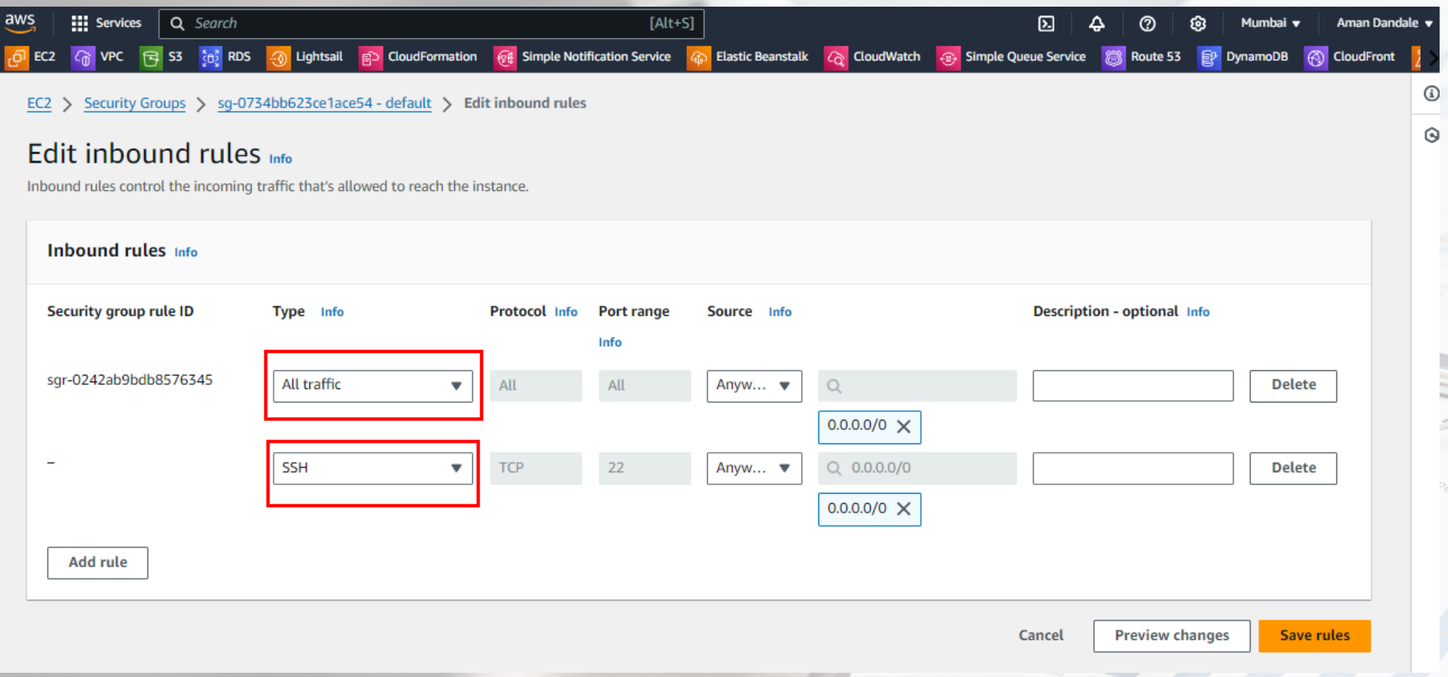
Step 3 – Install Jenkins on Ubuntu

Follow step-by-step properly

- sudo apt update -y
- sudo apt upgrade -y
- sudo apt install openjdk-17-jre -y
- curl -fsSL https://pkg.jenkins.io/debian-stable/jenkins.io-2023.key | sudo tee /usr/share/keyrings/jenkins-keyring.asc > /dev/null
- cat /usr/share/keyrings/jenkins-keyring.asc ====> To see the public key of Jenkins
- echo deb [signed-by=/usr/share/keyrings/jenkins-keyring.asc] https://pkg.jenkins.io/debian-stable binary/ | sudo tee /etc/apt/sources.list.d/jenkins.list > /dev/null
- cat /etc/apt/sources.list.d/jenkins.list
- sudo apt-get update -y
- sudo apt-get install jenkins -y
- dpkg -s jenkins

```
root@ip-172-31-36-240:~# dpkg -s jenkins
Package: jenkins
Status: install ok installed
Priority: optional
Section: devel
Installed-Size: 91248
Maintainer: Kohsuke Kawaguchi <kk@kohsuke.org>
Architecture: all
Version: 2.462.3
Depends: adduser, lsb-base (>= 3.2-14), net-tools, sysvinit-utils (>= 2.88dsf-50)
Pre-Depends: init-system-helpers (>= 1.54~)
```

Step 4 – Change the security group of EC2 instance



Details

Security group name	Security group ID	Description	VPC ID
default	sg-0734bb623ce1ace54	default VPC security group	vpc-0ed78ddb4cc11fd3f

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Tags

Inbound rules (2)

Manage tags | Edit inbound rules

Search

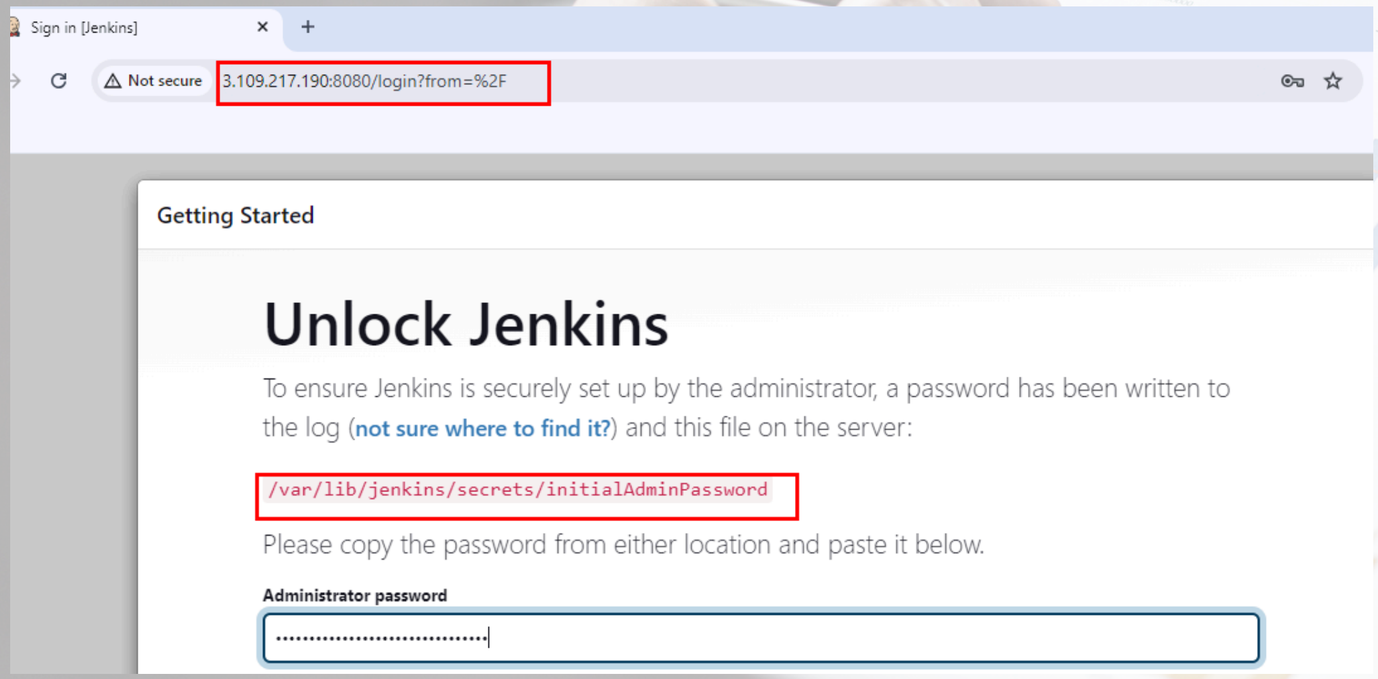
1

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-0242ab9bdb8576...	IPv4	All traffic	All	All	0.0.0.0/0
sgr-08b0b340cae8bbd...	IPv4	SSH	TCP	22	0.0.0.0/0

Step 5– Sign Into Jenkins console

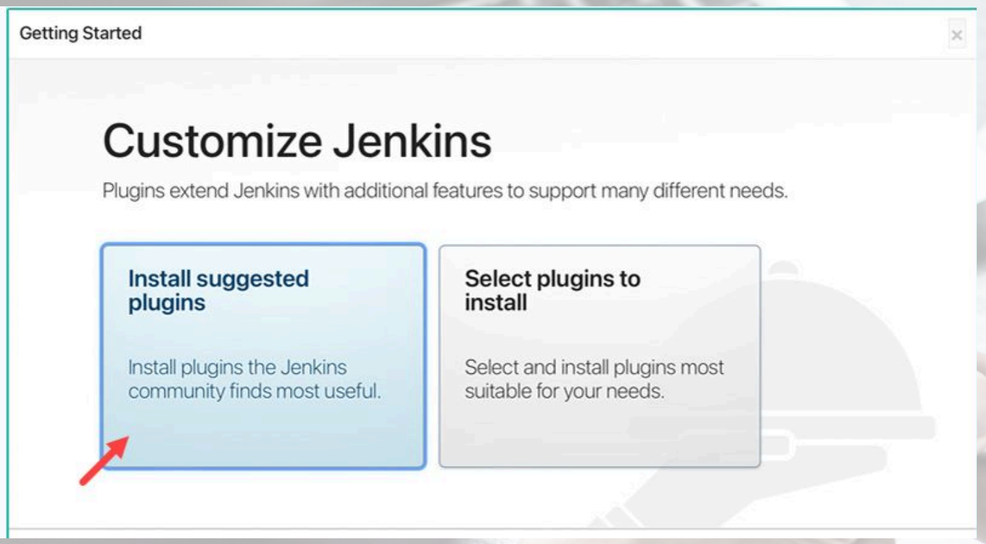
- http://<EC2_Public_IP>:8080/
- http://3.109.217.190:8080/

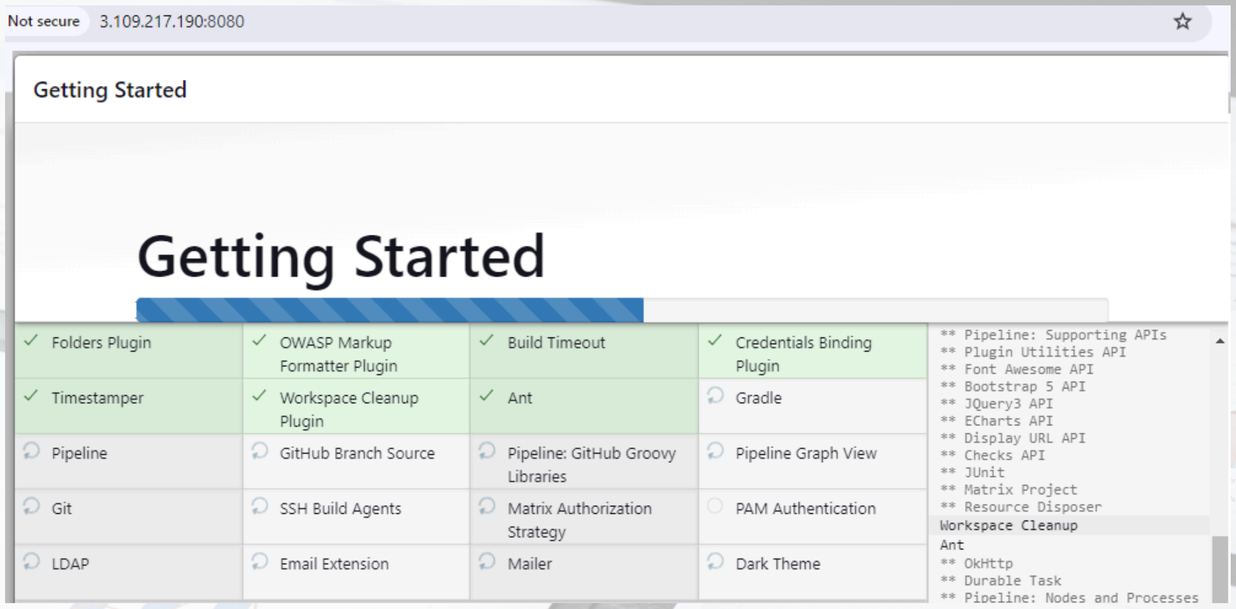
Step 6 – Get the Administrator password by hitting the below command in EC2



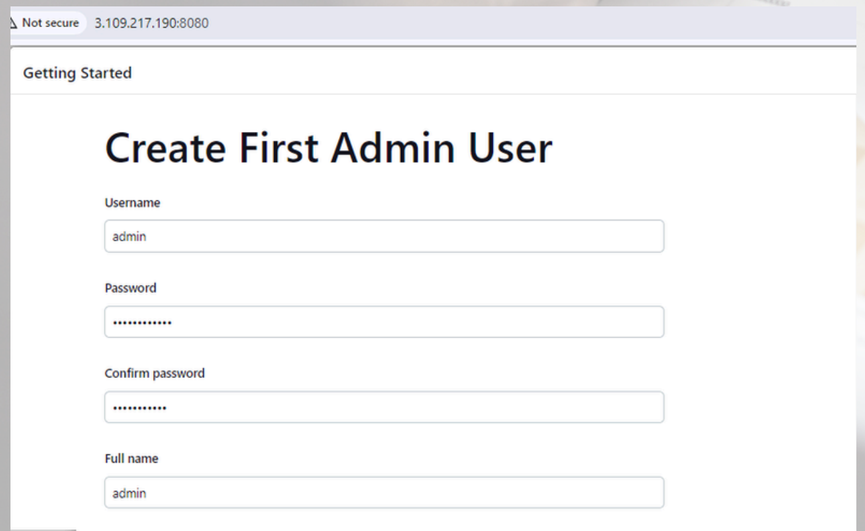

```
root@ip-172-31-36-240:~# cat /var/lib/jenkins/secrets/initialAdminPassword
a2fe583cb8e14f83a6e98f6ae2ae92ad
root@ip-172-31-36-240:~#
```

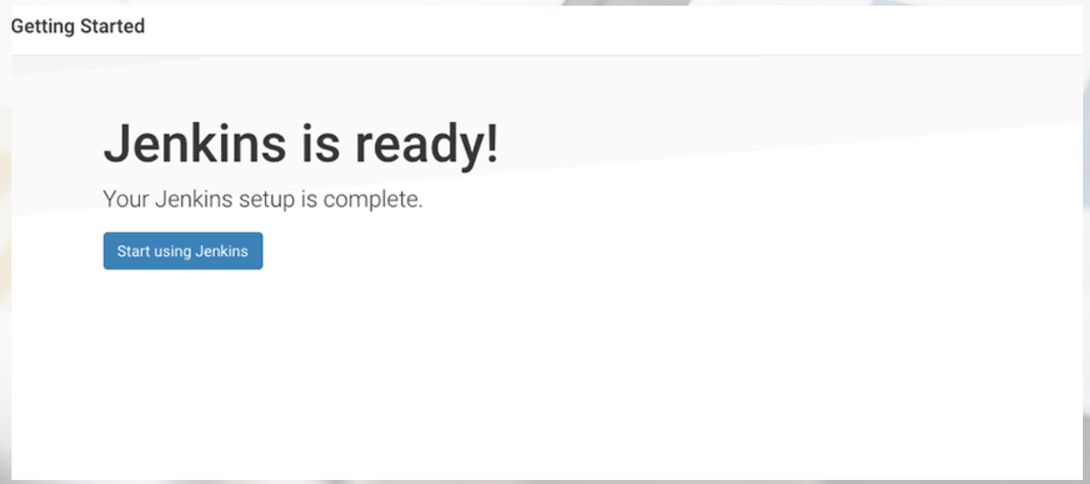
Step 7 – Install all suggested plugins



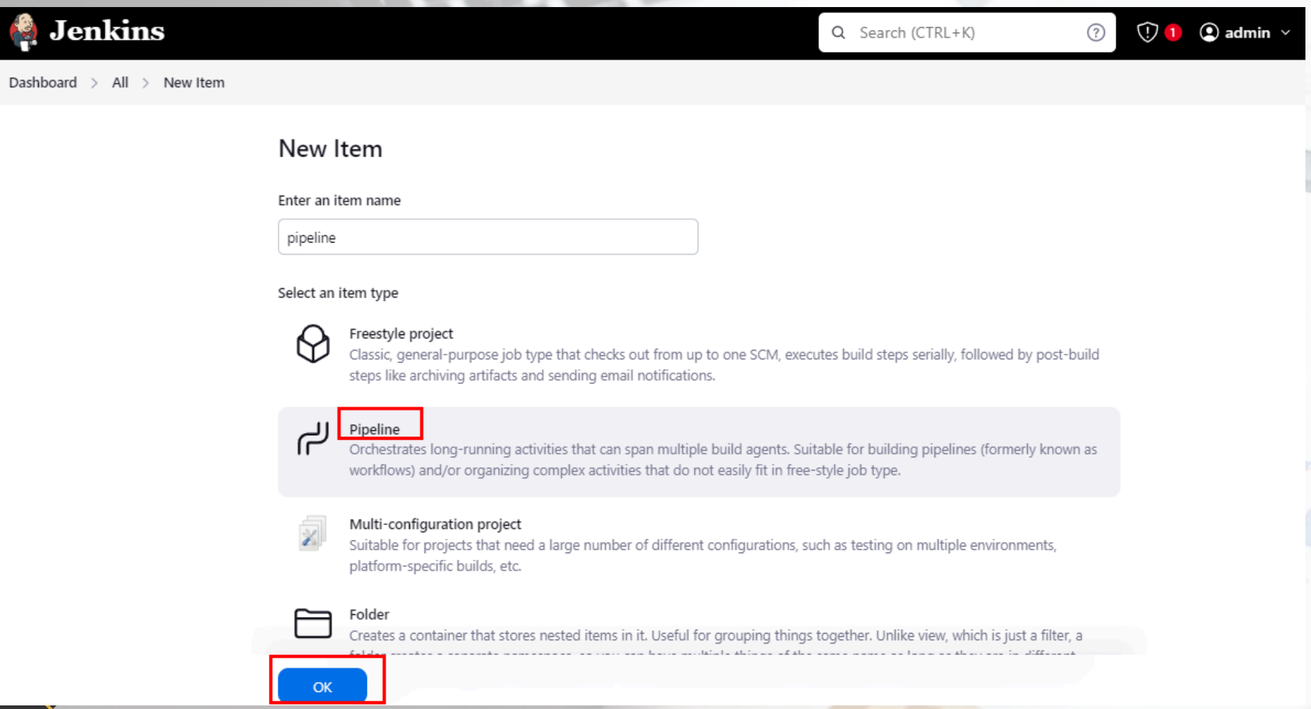


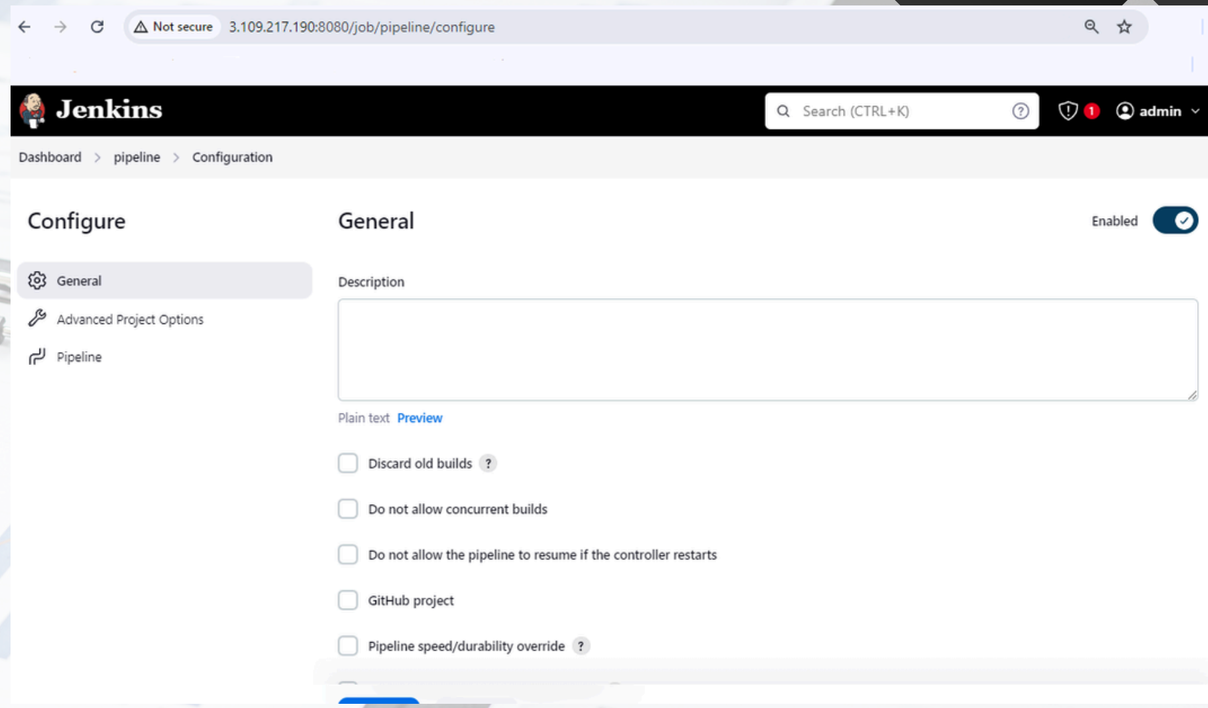
Step 8 –Create first user

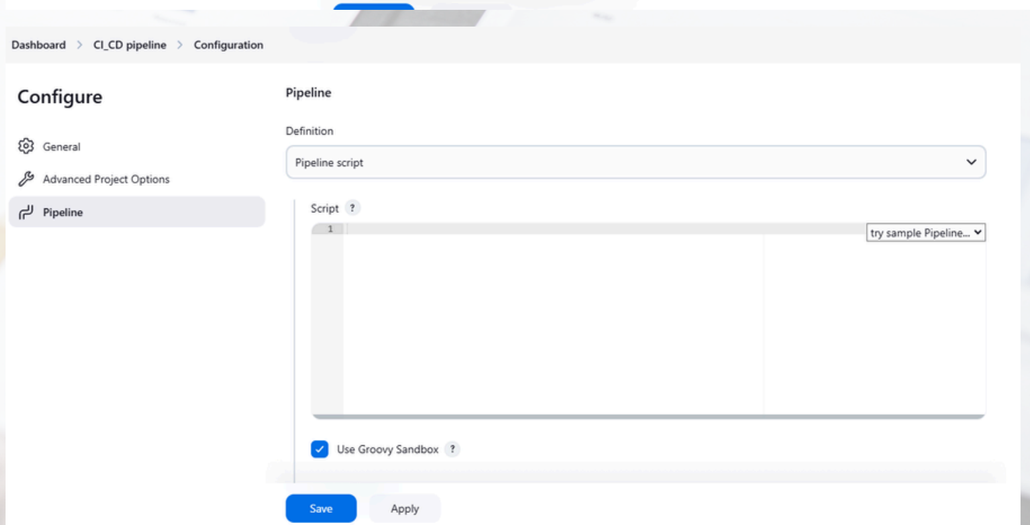




Step 9 – Create a pipeline Job

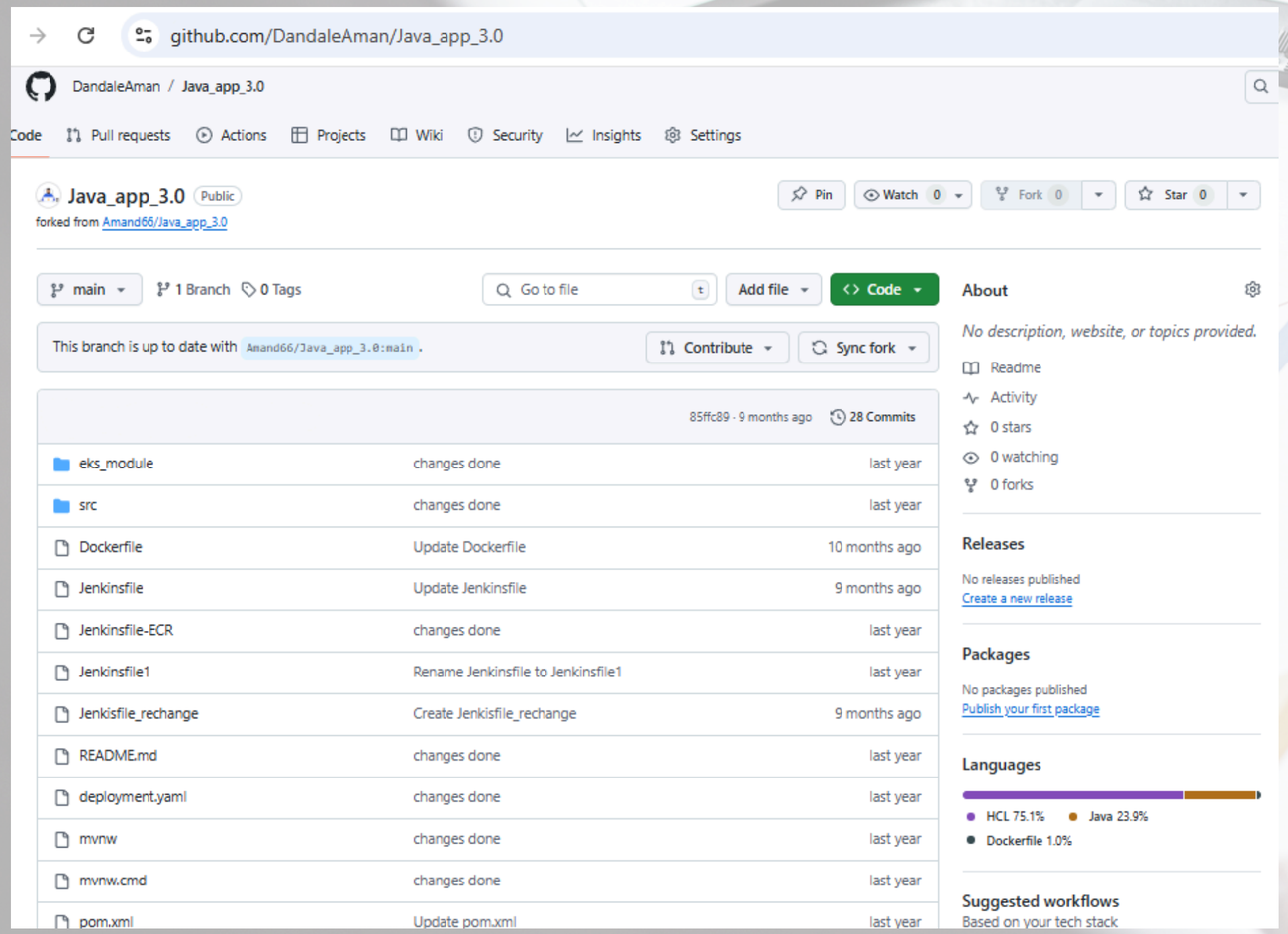


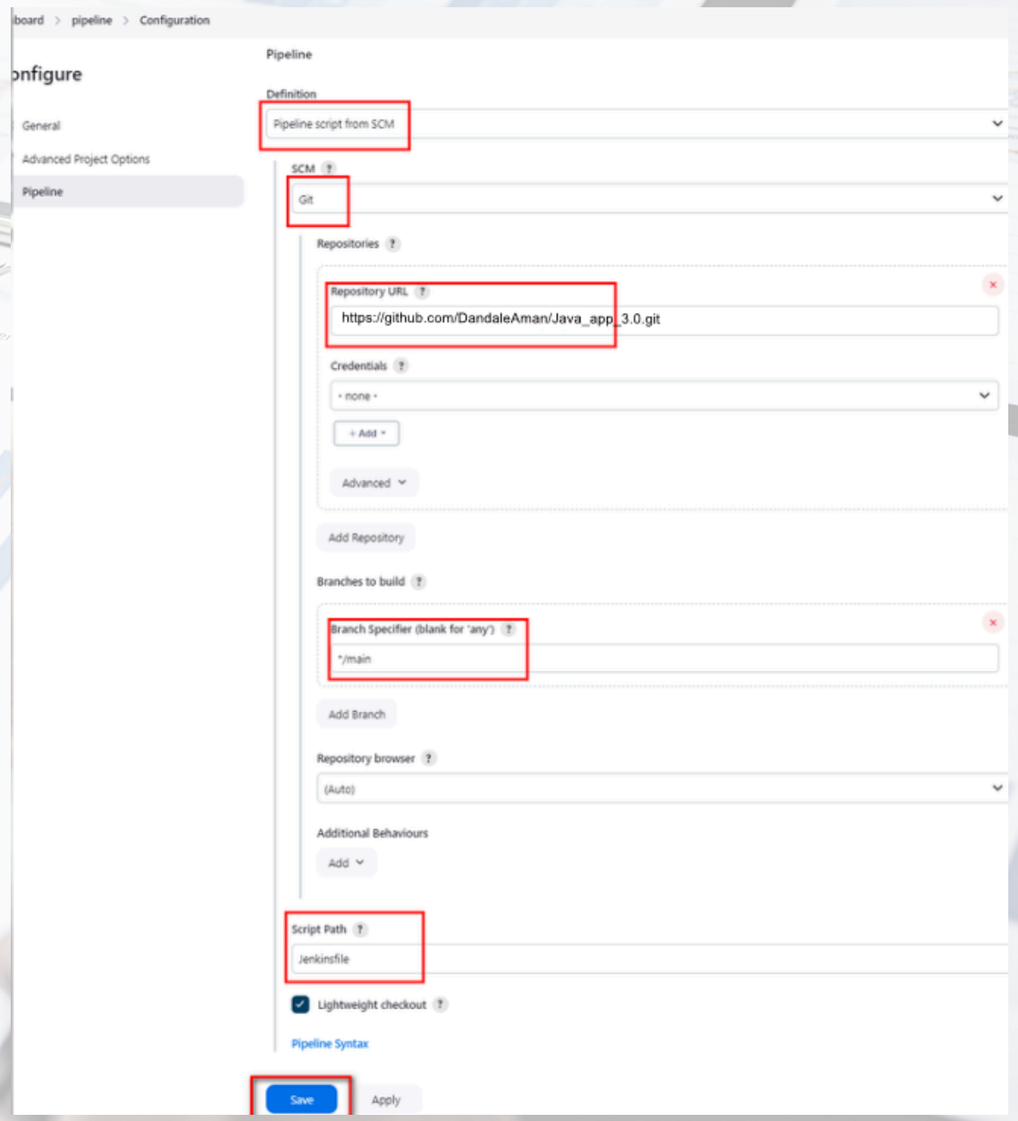




Step 10 – Add pipeline script as SCM

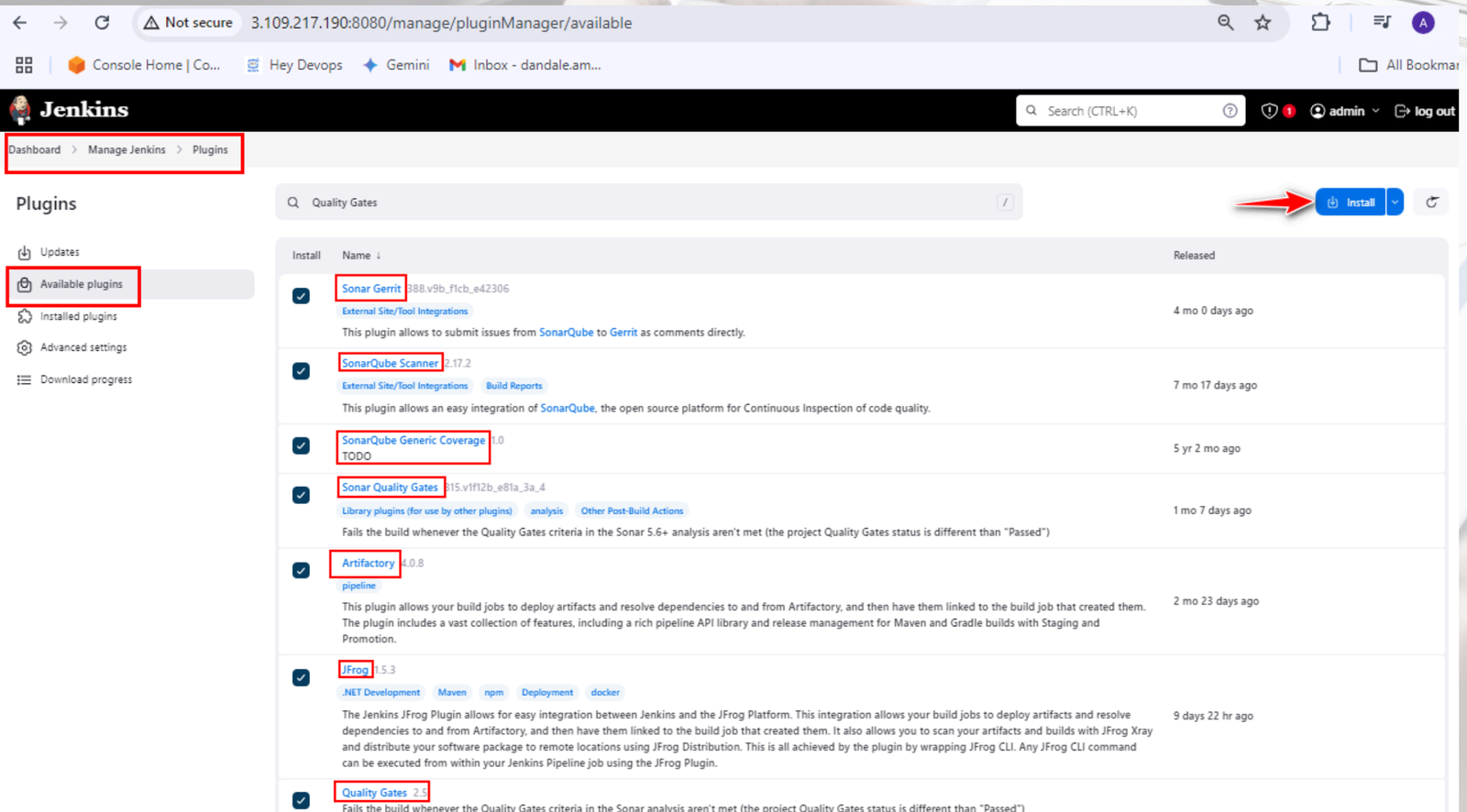
- Add git repository as: https://github.com/DandaleAman/Java_app_3.0.git
- Add branch Specifier: */main
- Add Script Path: Jenkinsfile





Step 11 –Add the Plugins

- **Follow: Dashboard -> Manage Jenkins -> Plugins -> Available plugins**



- **Plugins for Sonar/Jfrog**

- **Sonar Gerrit**
- **SonarQube Scanner**
- **SonarQube Generic Coverage**
- **Sonar Quality Gates**
- **Quality Gates**
- **Artifactory**
- **Jfrog**

Step 12– Setup Docker

- sudo apt update -y
- sudo apt install apt-transport-https ca-certificates curl software-properties-common -y
- curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
- sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable" -y
- sudo apt update -y
- apt-cache policy docker-ce -y
- sudo apt install docker-ce -y
- sudo systemctl status docker
- sudo chmod 777 /var/run/docker.sock
- docker -v

Step 13- Install SonarQube

- docker run -d --name sonarqube -p 9000:9000 -p 9092:9092 sonarqube

Step 13.1 - Start docker container if it's not up

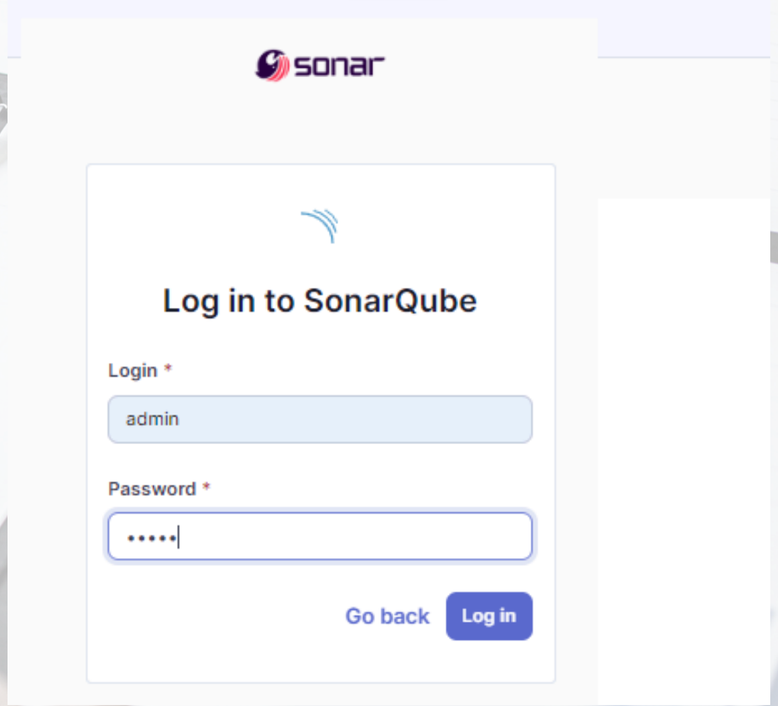
- docker ps -a
- docker start <Container ID>

```
root@ip-172-31-36-240:~# docker images
REPOSITORY   TAG       IMAGE ID       CREATED      SIZE
sonarqube    latest    862025bf322c   4 days ago   1.1GB
root@ip-172-31-36-240:~# docker ps -a
CONTAINER ID   IMAGE       COMMAND                  CREATED       STATUS       PORTS
                                NAMES
ad5fc9d5d11a   sonarqube   "/opt/sonarqube/dock…"   7 hours ago   Up 7 hours   0.0.0.0:9000->9000/tcp, :::9000->9000/tcp, 0.0.0.0:
9092->9092/tcp, :::9092->9092/tcp   sonarqube
root@ip-172-31-36-240:~#
```

Step 13.2 - Login into sonar dashboard

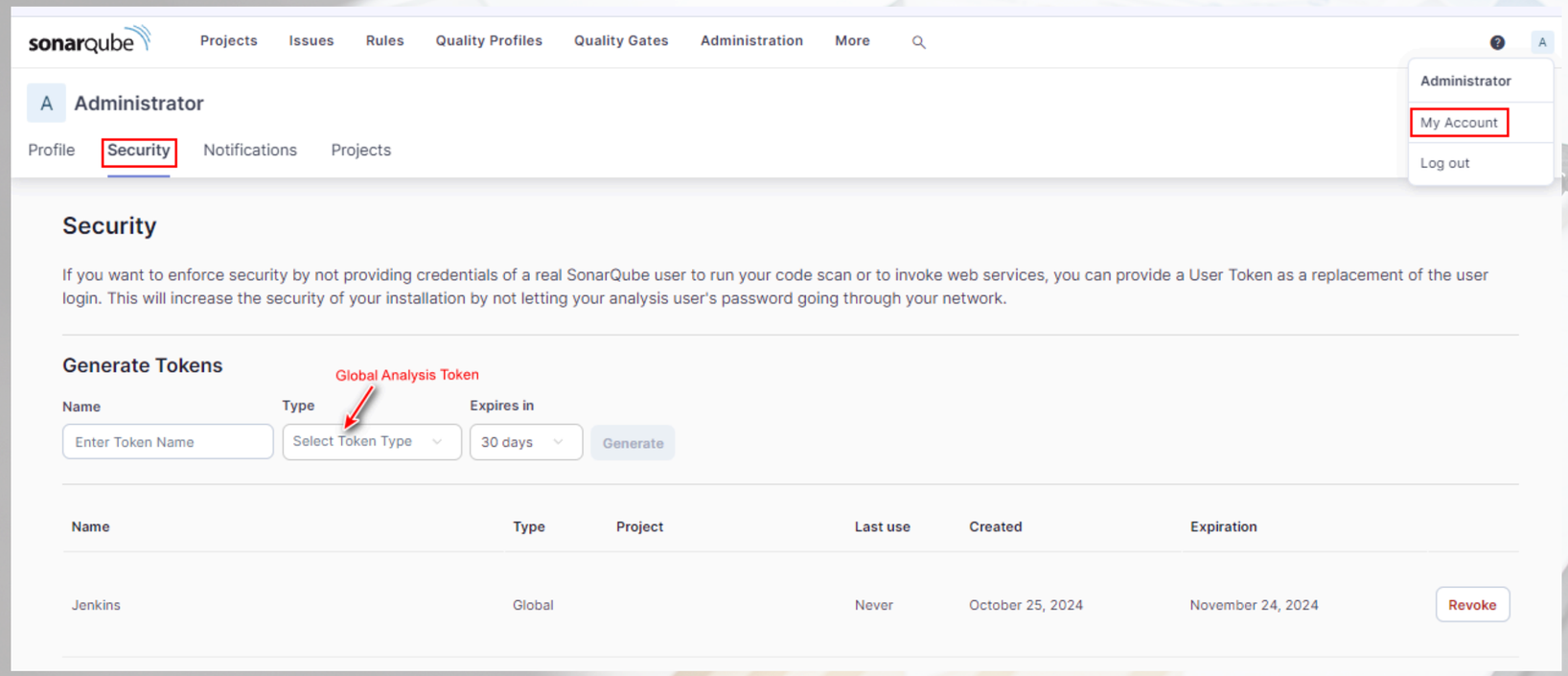
- http://<EC2_Public_IP>:9000/
- Username – admin
- Password – admin

```
root@ip-172-31-36-240:~# docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
sonarqube    latest    862025bf322c   3 weeks ago   1.1GB
root@ip-172-31-36-240:~# docker ps -a
CONTAINER ID   IMAGE       COMMAND                  CREATED       STATUS                       PORTS     NAMES
ad5fc9d5d11a   sonarqube   "/opt/sonarqube/dock…"   2 weeks ago   Exited (130) 15 seconds ago            sonarqube
root@ip-172-31-36-240:~# docker start ad5fc9d5d11a
ad5fc9d5d11a
root@ip-172-31-36-240:~# docker ps -a
CONTAINER ID   IMAGE       COMMAND                  CREATED       STATUS         PORTS
                                  NAMES
ad5fc9d5d11a   sonarqube   "/opt/sonarqube/dock…"   2 weeks ago   Up 4 seconds   0.0.0.0:9000->9000/tcp, :::9000->9000/tcp,
 0.0.0.0:9092->9092/tcp, :::9092->9092/tcp   sonarqube
```



Step 13.3 - Create Sonar token for Jenkins

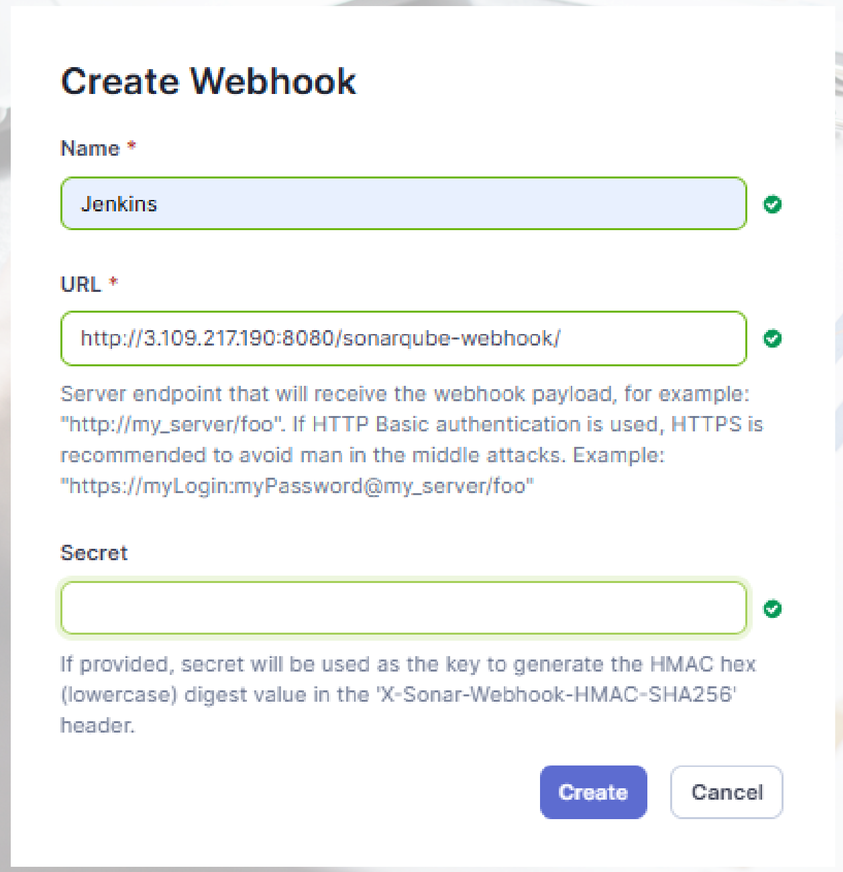
Sonar Dashboard -> Administration -> My Account -> Security -> Create token -> Save the token to some text file



Step 13.4 - Integrate Sonar to Jenkins

Sonar Dashboard -> Administration -> Configuration -> webhooks -> Add the below name and url and save

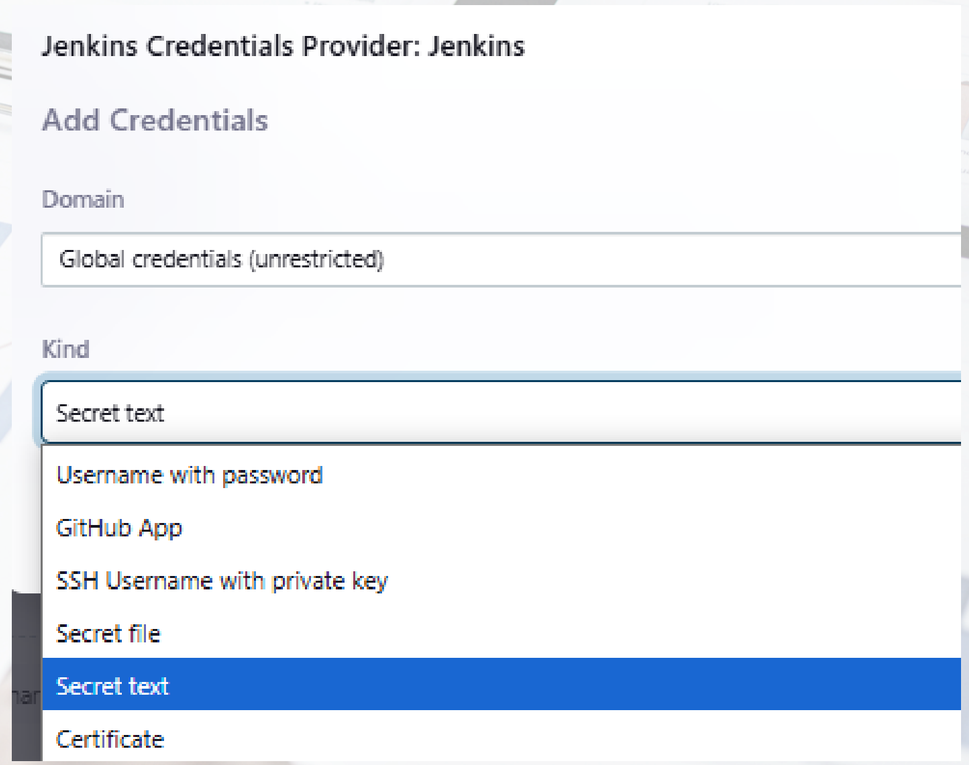
- **http://<EC2_Public_Ip>:8080/sonarqube-webhook/**



Step 13.5– Add Sonarqube to Jenkins

Jenkins Dashboard -> Manage Jenkins -> system configuration

- **Click on sonarqube servers -> add url and name -> Click on add token -> Select Secret text -> Add the sonar token from step13.3 -> Give name of token as *sonarqube-api***



Step 14– Install Maven

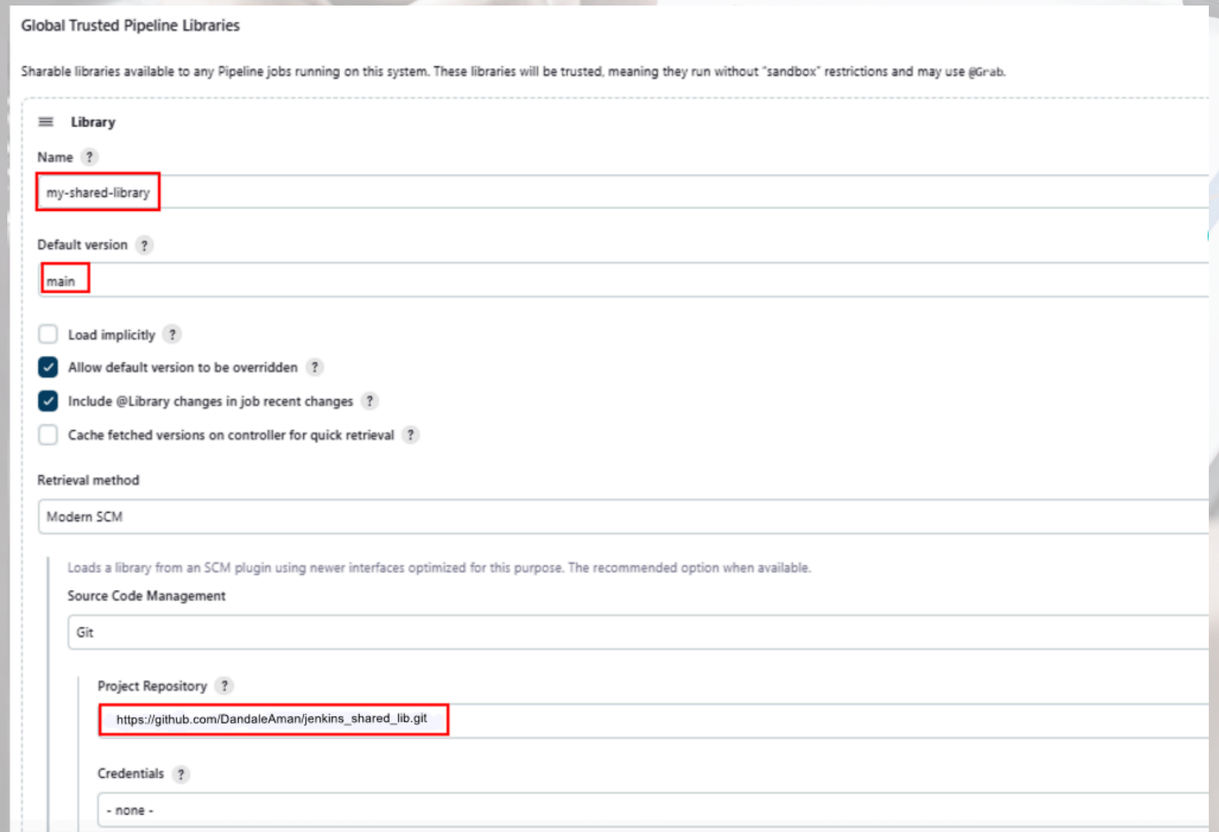
- sudo apt update -y
- sudo apt install maven -y
- mvn -version

Step 15 – Install TRIVY for docker image scan

- sudo apt-get install wget apt-transport-https gnupg lsb-release
- wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -
- echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.list.d/trivy.list
- sudo apt-get update
- sudo apt-get install trivy

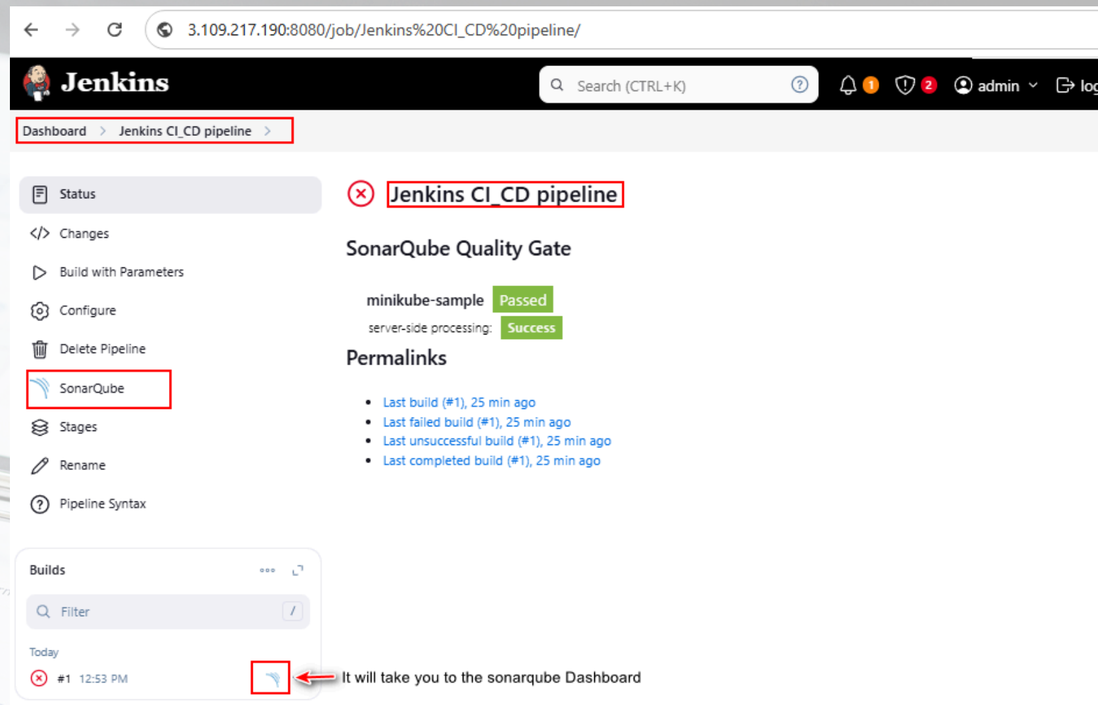
Step 16– Add the Jenkins Shared library (Global Trusted Pipeline Libraries)

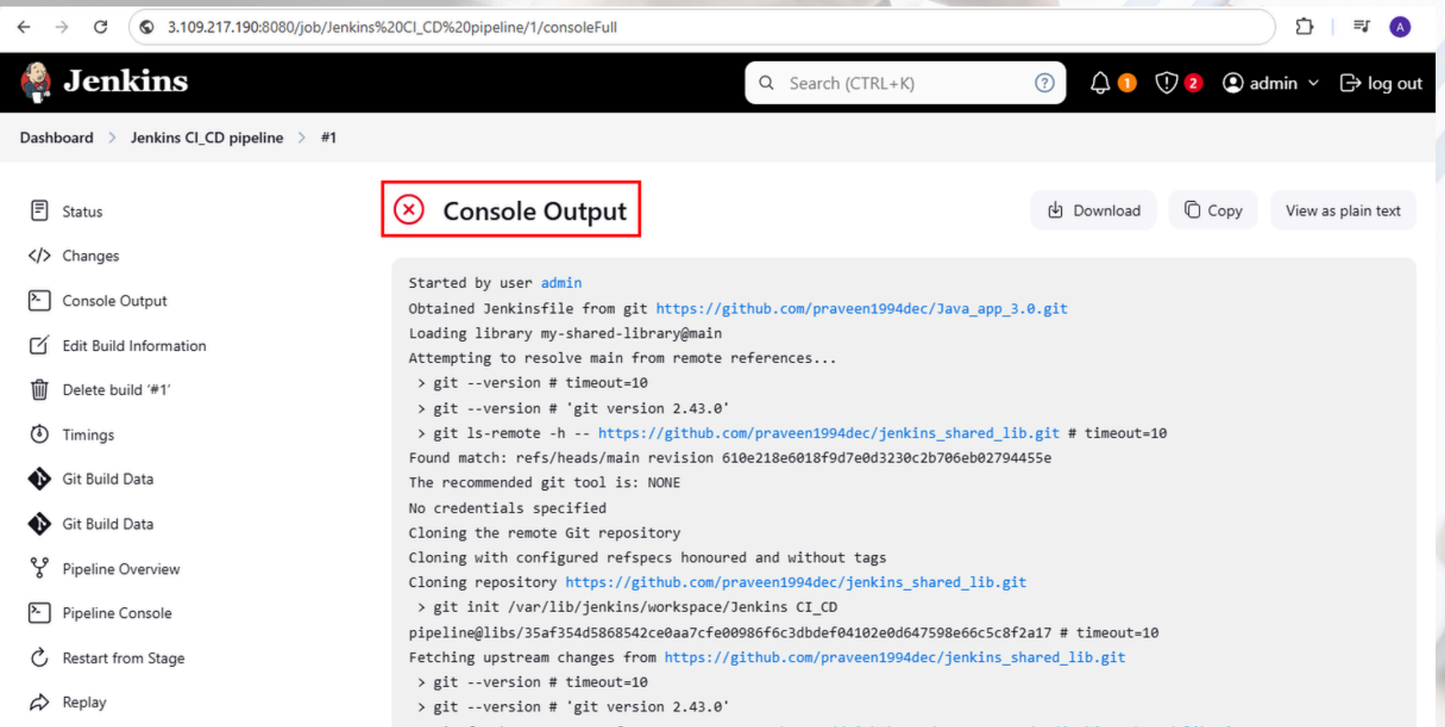
- Go to Manage Jenkins -> Configure system -> Global Trusted Pipeline Libraries-> Add below data
- Name - my-shared-library
- Default version – main
- Git - https://github.com/DandaleAman/jenkins_shared_lib.git



Step 17– Once pipeline is Run Check

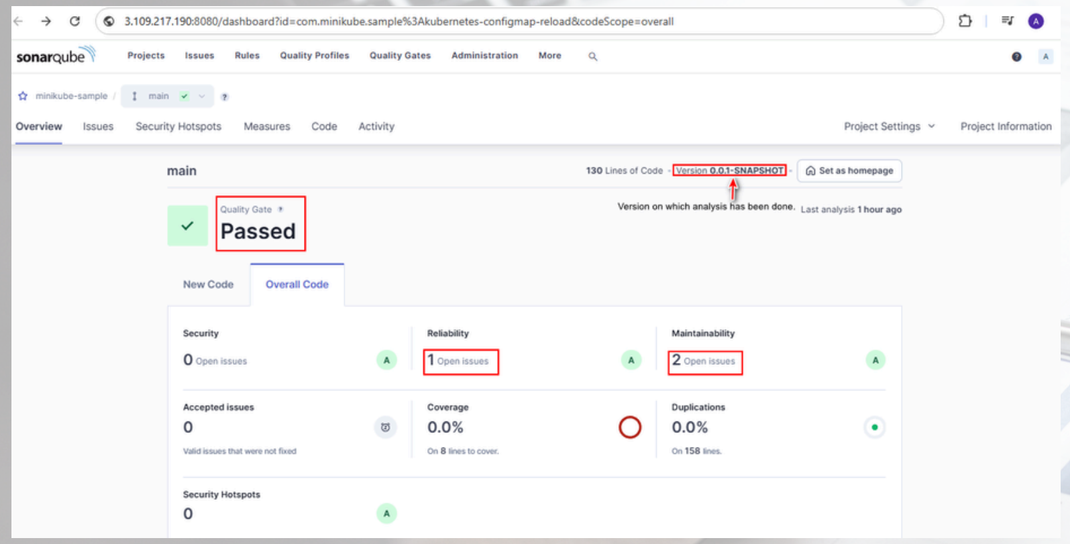
- Console Output
- The Jenkins logs
- The Trivy scan vulnerabilities
- The sonarqube dashboard for report

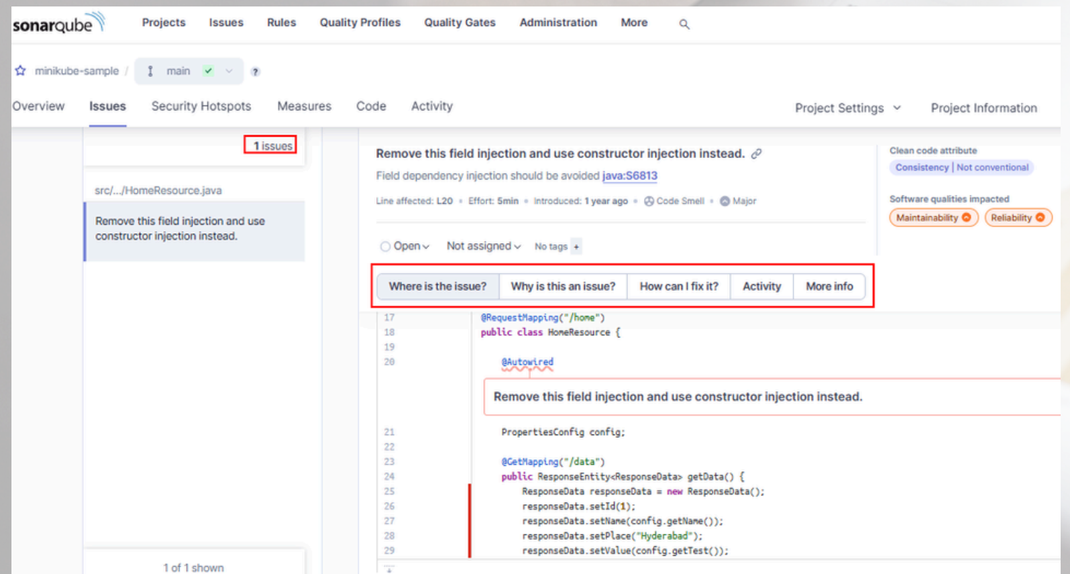


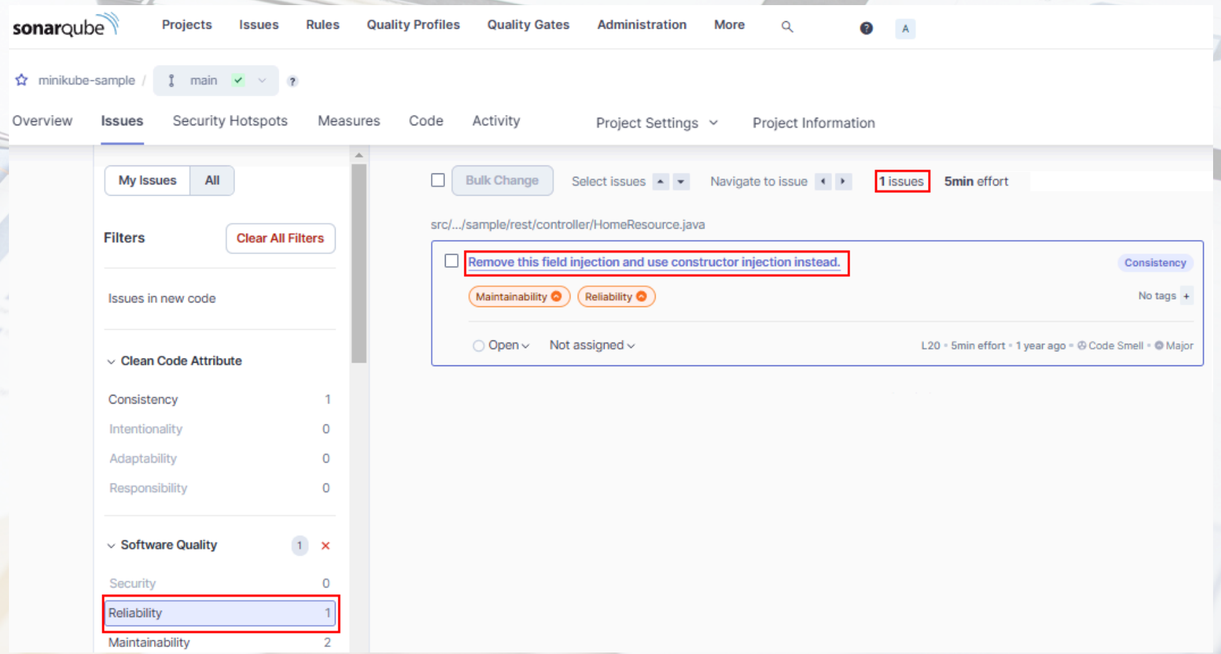


Step 18– Sonarqube Dashboard for improve the quality of code

- SonarQube is a Code Quality Assurance tool that collects and analyzes source code, and provides reports for the code quality of your project.







THANK YOU

https://www.linkedin.com/in/amandandale/