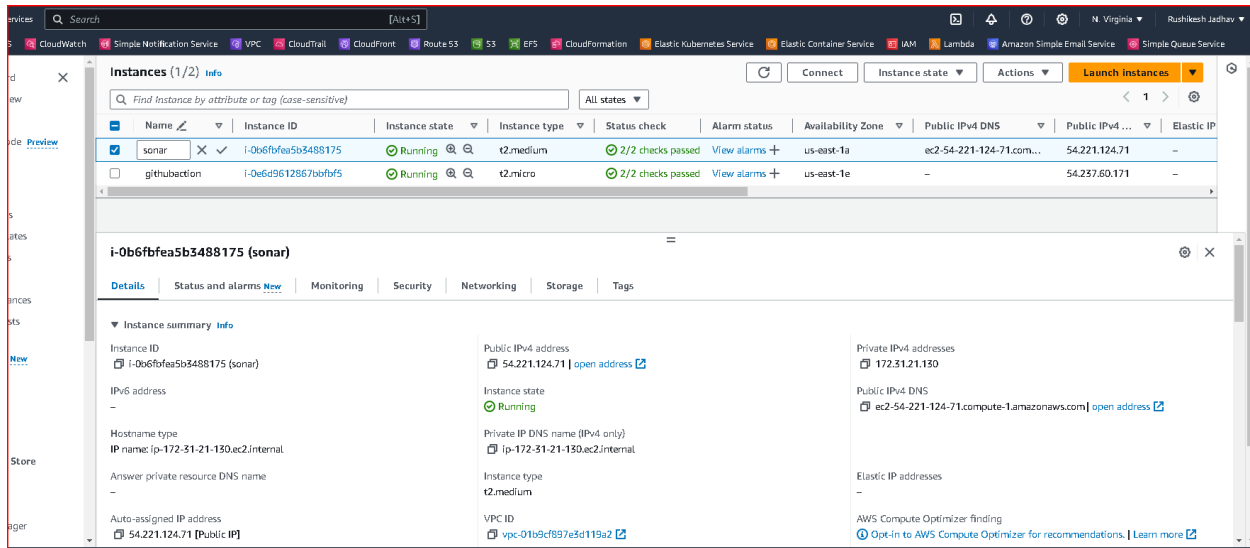


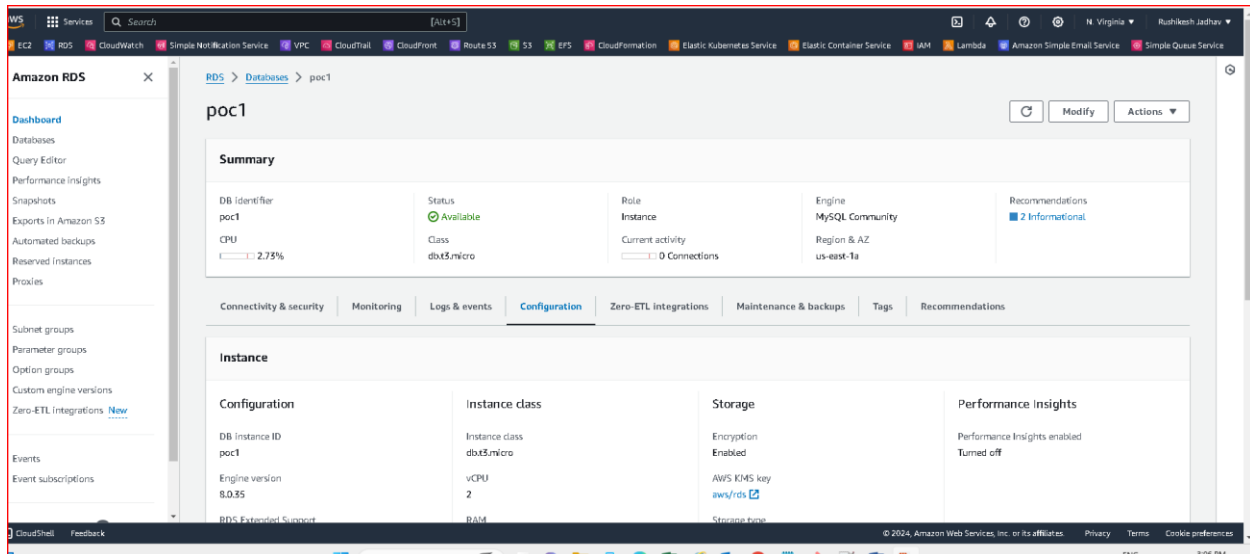
Sonarqube

Deploy a java/python application on amazon EC2 and while utilising RDS database(Mysql/Postgres) for data storage to scan and evaluate the code quality in SonarQube.

amazon EC2



RDS setup in AWS



Install Maven and JAVA

```
aws Services Search [Alt+S]
https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.
4 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Wed May 22 04:44:51 2024 from 18.206.107.27
ubuntu@ip-172-31-21-130:~$ sudo su -
root@ip-172-31-21-130:~# ls
snap
root@ip-172-31-21-130:~# cd /opt/
root@ip-172-31-21-130:/opt# ls
employee-management sonarqube-9.9.0.65466 sonarqube-9.9.0.65466.zip
root@ip-172-31-21-130:/opt# cd employee-management/
root@ip-172-31-21-130:/opt/employee-management# ls
Dockerfile README.md deploy key.pem manifests pom.xml sonar-project.properties src target
root@ip-172-31-21-130:/opt/employee-management# mvn -version
Command 'mvn' not found, did you mean:
  command 'aven' from deb survex-aven (1.4.4-1build1)
Try: apt install <deb name>
root@ip-172-31-21-130:/opt/employee-management# mvn -version
Apache Maven 3.8.7
Maven home: /usr/share/maven
Java version: 17.0.11, vendor: Ubuntu, runtime: /usr/lib/jvm/java-17-openjdk-amd64
Default locale: en, platform encoding: UTF-8
OS name: "linux", version: "6.8.0-1008-aws", arch: "amd64", family: "unix"
root@ip-172-31-21-130:/opt/employee-management#
```

i-0b6fbfea5b3488175 (sonar)
PublicIPs: 54.221.124.71 PrivateIPs: 172.31.21.130

Download and Install SonarQube

wget https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-8.9.0.43852.zip

unzip sonarqube-8.9.0.43852.zip

sudo chown -R sonaradmin:sonaradmin sonarqube-9.9.0.65466/*

cd sonarqube-9.9.0.65466/bin/linux-x86-64/

./sonar.sh start

./sonar.sh status

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&conntype=standard&iinstanceid=i-0b6fbfea5b3488175&osUser=ubuntu&sshPort=22#/  
ChatGPT The Hub Cybage MIS Home - Cylintranet  
AWS Services [Alt+S]  
EC2 RDS CloudWatch Simple Notification Service VPC CloudTrail CloudFront Route 53 S3 EFS CloudFormation Elastic Kubernetes Service Elastic Container Service IAM Lambda  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466/logs$ cd ..  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466$ chown -R sonaradmin:sonaradmin *  
chown: changing ownership of 'logs/sonar.log': Operation not permitted  
chown: changing ownership of 'logs/es.log': Operation not permitted  
chown: changing ownership of 'logs/nohup.log': Operation not permitted  
chown: changing ownership of 'temp/conf/es/jvm.options': Operation not permitted  
chown: changing ownership of 'temp/conf/es/elasticsearch.keystore': Operation not permitted  
chown: changing ownership of 'temp/conf/es/elasticsearch.yml': Operation not permitted  
chown: changing ownership of 'temp/conf/es/log4j2.properties': Operation not permitted  
chown: changing ownership of 'temp/conf/es': Operation not permitted  
chown: changing ownership of 'temp/conf': Operation not permitted  
chown: changing ownership of 'temp/sharedmemory': Operation not permitted  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466$ sudo chown -R sonaradmin:sonaradmin *  
[sudo] password for sonaradmin:  
sonaradmin is not in the sudoers file.  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466$ sudo su  
[sudo] password for sonaradmin:  
sudo: no password was provided  
sudo: a password is required  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466$  
exit  
root@ip-172-31-21-130:/opt# sudo chown -R sonaradmin:sonaradmin sonarqube-9.9.0.65466/*  
root@ip-172-31-21-130:/opt# su sonaradmin  
sonaradmin@ip-172-31-21-130:/opt$ cd sonarqube-9.9.0.65466/bin/linux-x86-64/  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466/bin/linux-x86-64$ ./sonar.sh start  
/usr/bin/java  
Starting SonarQube...  
Started SonarQube  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466/bin/linux-x86-64$ ./sonar.sh status  
/usr/bin/java  
SonarQube is running (6823)  
sonaradmin@ip-172-31-21-130:/opt/sonarqube-9.9.0.65466/bin/linux-x86-64$  
exit  
  
i-0b6fbfea5b3488175 (sonar)  
PublicPcs: 54.221.124.71 PrivatePcs: 172.31.21.130
```

Mvn clean install sonar:sonar

```
ChatGPT The Hub Cybage MIS Home - Cylintranet  
AWS Services [Alt+S]  
EC2 RDS CloudWatch Simple Notification Service VPC CloudTrail CloudFront Route 53 S3 EFS CloudFormation Elastic Kubernetes Service Elastic Container Service IAM Lambda Amazon S3  
[INFO] 0 source files to be analyzed  
[INFO] 0/0 source files have been analyzed  
[INFO] Sensor IaC Docker Sensor [iac] (done) | time=60ms  
[INFO] ----- Run sensors on project  
[INFO] Sensor Analysis Warnings Import [csharplint] (done) | time=1ms  
[INFO] Sensor Analysis Warnings Import [csharplint] (done) | time=1ms  
[INFO] Sensor Zero Coverage Sensor (done) | time=1ms  
[INFO] Sensor Java CPD Block Indexer (done) | time=28ms  
[INFO] Sensor Java CPD Block Indexer (done) | time=28ms  
[INFO] SCM Publisher SCM provider for this project is: git  
[INFO] SCM Publisher 10 source files to be analyzed  
[INFO] SCM Publisher 9/10 source files have been analyzed (done) | time=282ms  
[WARNING] Missing blame information for the following files:  
[WARNING] * pom.xml  
[WARNING] This may lead to missing/broken features in SonarQube  
[INFO] CPD Executor 0 files had no CPD blocks  
[INFO] CPD Executor Calculating CPD for 2 files  
[INFO] CPD Executor CPD calculation finished (done) | time=6ms  
[INFO] Analysis report generated in 137ms, dir size=158.1 kB  
[INFO] Analysis report compressed in 36ms, zip size=36.9 kB  
[INFO] Analysis report uploaded in 230ms  
[INFO] ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=net.java.guides42.springboot-backend  
[INFO] Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report  
[INFO] More about the report processing at http://localhost:9000/api/ce/task?id=AY-bUm4i1WqImpuak71p  
[INFO] Analysis total time: 10.104 s  
[INFO] -----  
[INFO] BUILD SUCCESS  
[INFO] -----  
[INFO] Total time: 30.560 s  
[INFO] Finished at: 2024-05-21T13:23:41Z  
[INFO] -----  
root@ip-172-31-21-130:/opt/employee-management#
```

i-0b6fbfea5b3488175 (sonar)

Generate token

The screenshot shows the SonarQube Security page. At the top, there's a navigation bar with 'sonarqube' logo and links to Projects, Issues, Rules, Quality Profiles, Quality Gates, and Administration. A search bar is also present. Below the navigation bar, the user is logged in as 'Administrator'. The main content area is titled 'Tokens'. It contains a paragraph explaining the purpose of tokens: 'If you want to enforce security by not providing credentials of a real SonarQube user to run your code scan or to invoke web services, you can provide a User Token as a replacement of the user login. This will increase the security of your installation by not letting your analysis user's password going through your network.' Below this, there's a 'Generate Tokens' section with a form. The form has three fields: 'Name' (with a placeholder 'Enter Token Name'), 'Type' (a dropdown menu with 'Select Token Type'), and 'Expires in' (a dropdown menu with '30 days'). A 'Generate' button is to the right of these fields. Below the form, there's a table with columns: Name, Type, Project, Last use, Created, and Expiration. The table has one row with the following data: Name: 'github action', Type: 'Global', Project: (empty), Last use: 'Never', Created: 'May 21, 2024', and Expiration: 'June 20, 2024'. A 'Revoke' button is next to the last row. Below the table, there's a section titled 'Enter a new password' with a note: 'All fields marked with * are required'. It has three input fields: 'Old Password *', 'New Password *', and 'Confirm Password *'.

After running mvn clean install sonar:sonar command project will appear in dashboard

The screenshot shows the SonarQube Projects dashboard. At the top, there's a navigation bar with 'sonarqube' logo and links to Projects, Issues, Rules, Quality Profiles, Quality Gates, and Administration. A search bar is also present. Below the navigation bar, the user is logged in as 'Administrator'. The main content area is titled 'Projects'. It has a search bar 'Search by project name or key' and a 'Create Project' button. Below the search bar, there's a list of projects. The first project is 'sonarqube' with a status of 'Passed'. Below it, there's a section for 'springboot-backend' with a status of 'Passed'. This section shows various metrics: Bugs (0), Vulnerabilities (0), Hotspots Reviewed (0.0%), Code Smells (2), Coverage (93.3%), Duplications (0.0%), and Lines (208). A 'Configure analysis' button is also present. At the bottom, there's a warning message: '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 support for migrating your data out of it into a different database engine.' Below the warning, there's a footer with the text: 'SonarQube™ technology is powered by SonarSource SA. Community Edition - Version 9.9 (build 65466) - LGPL v3 - Community - Documentation - Plugins - Web API'.

Create a custom Quality Profile

There's an update available for your SonarQube instance. Please update to make sure you benefit from the latest security and bug fixes. [Learn More](#)

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministration

Search for projects...A

Quality Profiles / Java

Sonar

Updated: 20 hours agoUsed: Never

Changelog

⚙

This profile extends [Sonar way](#).

Rules

ActiveInactive

Total

479149

Bugs

13911

Vulnerabilities

312

Code Smells

272136

Security Hotspots

370

Activate More

Permissions

Users with the global "Administer Quality Profiles" permission and those listed below can manage this quality profile.

Grant permissions to more users

Inheritance

Change Parent

Sonar way

BUILT-IN

479 active rules

0 overridden rules

Sonar

479 active rules

0 overridden rules

Projects

Change Projects

springboot-backend

1 of 1 shown

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 support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by [SonarSource SA](#)

Community Edition - Version 9.9 (build 85466) - [LGPLv3](#) - [Community](#) - [Documentation](#) - [Plugins](#) - [Web API](#)

Quality Gate within SonarQube configured to enforce a code coverage threshold of 90%

There's an update available for your SonarQube instance. Please update to make sure you benefit from the latest security and bug fixes. [Learn More](#)

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministration

Search for projects...A

Quality Gates

Create

RenameCopySet as DefaultDelete

QG

Sonar way

DEFAULTBUILT-IN

This quality gate complies with Clean as You Code

This quality gate complies with the [Clean as You Code](#) methodology, so that you benefit from the most efficient approach to delivering Clean Code. It ensures that:

• No new bugs are introduced

• No new vulnerabilities are introduced

• All new security hotspots are reviewed

• New code has limited technical debt

• New code has limited duplication

• New code is properly covered by tests

Conditions

Conditions on New Code

Metric	Operator	Value	
Coverage	is less than	90.0%	
Duplicated Lines (%)	is greater than	3.0%	
Maintainability Rating	is worse than	A (Technical debt ratio is less than 5.0%)	
Reliability Rating	is worse than	A (No bugs)	
Security Hotspots Reviewed	is less than	100%	
Security Rating	is worse than	A (No vulnerabilities)	

You may click unlock to edit this quality gate. Adding extra conditions to a compliant quality gate can result in drawbacks. Are you reconsidering [Clean as You Code](#)? We strongly recommend this methodology to achieve a Clean Code status.