SONARQUBE

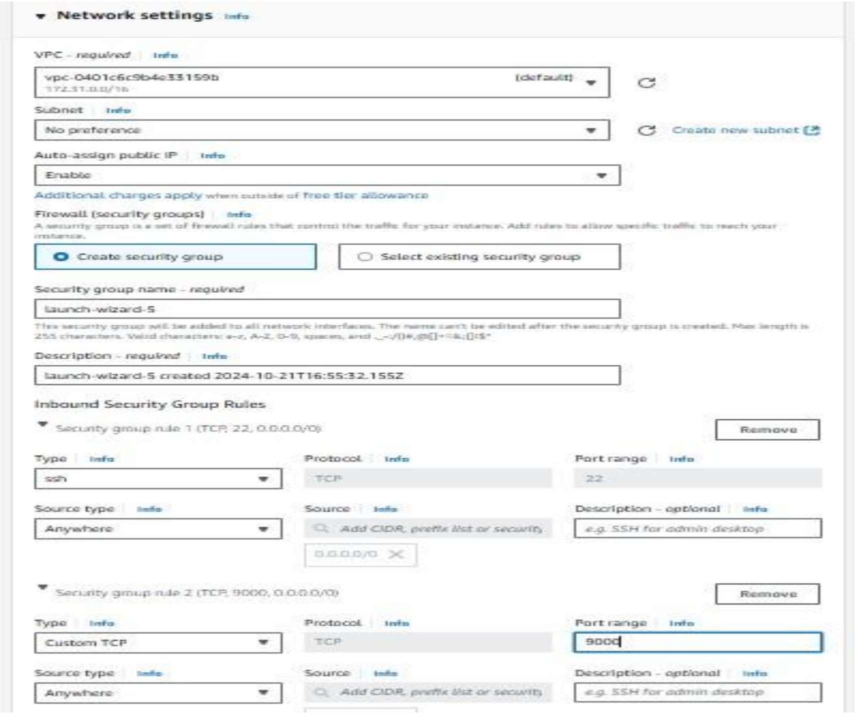
What is SonarQube

SonarQube is an open-source platform used to check the code quality like Bugs, vulnerabilities, code smells

Steps to create SonarQube

Step 1:

1. Launch the instance with ubuntu
    - Give the name for instance
    - Select the AMI as ubuntu
    - Select the instance type as t2.medium and keypair
    - Edit the network settings
    - Click on add security group rules
    - Give port number is 9000 and source type is anywhere as shown in below figure



Network settings

VPC - required: vpc-0401c6c9b4e33159b (default) 172.31.0.0/16

Subnet: No preference

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - required: launch-wizard-5

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - required: launch-wizard-5 created 2024-10-21T16:55:32.155Z

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type: ssh | Protocol: TCP | Port range: 22

Source type: Anywhere | Source: 0.0.0.0/0 | Description - optional: e.g. SSH for admin desktop

Security group rule 2 (TCP, 9000, 0.0.0.0/0)

Type: Custom TCP | Protocol: TCP | Port range: 9000

Source type: Anywhere | Source: Add CIDR, prefix list or security | Description - optional: e.g. SSH for admin desktop

Step 2:

1. Select the instance and connect to the terminal
2. Install some packages with commands

Commands	
sudo -i	To switch root user
apt update -y	To update the server
apt install openjdk-17-jre -y	To install java packages
apt install unzip	To install unzip packages
add user sonar	Set the password give enter up to y
su - sonar	To switch created user

Step 3:

1. Install SonarQube packages
2. Go to new web page and type binaries.sonarsource.com
    - Select the distributions
    - Select the SonarQube
    - Copy the latest link as 9.9
    - Return back to SonarQube terminal
3. After switching into the sonar user
4. Install the sonar by using the copied sonar zip link by using wget command

Wget – paste the copied sonar zip link
ll – to see the list of files

5. After installing SonarQube copy the zip file

unzip – paste the copied zip file

```
ll – to list the files
```

6. Rename the sonar unzip file as sonar

```
mv sonarqube-9.9.7.96285 space sonar
ll – to see the replaced name
```

7. Change the owner permissions as sonar

```
chown sonar:sonar sonar -R
```

8. Change the file permissions

```
chmod 777 sonar
ll – to list the files
```

9. Change to sonar directory

```
cd sonar – to change into sonar directory
ll – to list the files
cd bin – to change into bin directory
ll – to list the files
cd linux-x86-64 – to change into Linux directory
ll – to list the files
```

10. Start the sonar

```
./sonar.sh start
```

11. Check the status of sonar

```
./sonar.sh status
```

Step 4:

1. Copy the public IP of SonarQube and paste in new web page with port number :9000
2. By default sonar user name and password is admin

3. Generate the new password in SonarQube server and click on update
4. SonarQube server is created

Step 5:

1. Go to Jenkins server
2. Click on manage Jenkins
3. Select the plugins and select available plugins
4. Search for SonarQube canner plugin and click on install
5. Enable the restart option
6. Select the manage Jenkins and select the systems
7. Select the environment variables in SonarQube server
8. Add SonarQube credentials
    - Give the name as sonar
    - Copy the sonar server URL and paste in server URL
    - Click on add-to-add the credentials
    - Select the secret text in kind block
    - Go to SonarQube server and select the administrator icon and click on my account and select the security and generate the token
    - Copy the generated key and paste in Jenkins secret block
    - Give ID as sonar and description as sonar
    - Click on add then credentials is added
9. Then click on apply and save

Step 6:

1. Create a new job with free style in Jenkins
2. Click on configure in job
3. Select the git in source code management

4. Copy the GitHub java code URL and paste in Jenkins repository URL
5. Give main in branches to build block
6. Select the prepare SonarQube scanner environment in build environment
7. Select the created credentials In server authentication token
8. Click on apply and save
9. Click on build now option
10. It will shows that build is success or failed

Step 7:

1. Create a job by using pipeline
2. Select the hello world sample program in script
3. Click on pipeline syntax
4. Select the git in sample step block
5. Copy the URL of GitHub java code and paste in repository URL
6. Give main in branch block
7. Click on generate pipeline syntax
8. Copy the generated pipeline syntax
9. And paste in script
10. Add sonar code scanner in script
11. Click on pipeline syntax
12. Select SonarQube scanner environment in sample step
13. Provide created credentials in server block
14. Click on generate pipeline script and copy the script
15. Paste the copied script in code
16. Click on apply and save
17. Click on build now option
18. It can shows that build is success or failed