SonarQube Code analysis

Hardware requirements.

Min 8 GB Ram and 4 vCPU

A white background with black text

Description automatically generated

1. Install Sonarqube on server, create sonarqube container.  
     
   >> docker container run --dt -–name sonarqube –restart always -p 9000:9000
2. Open sonarqube on browser and complete sign in  
     
   browse by server ip and followed by port

Ex:- 10.30.10.105:9000

Sign in as default user and reset the password

Username- admin

Password- admin

Reset the password

Create project

A screenshot of a computer

Description automatically generated

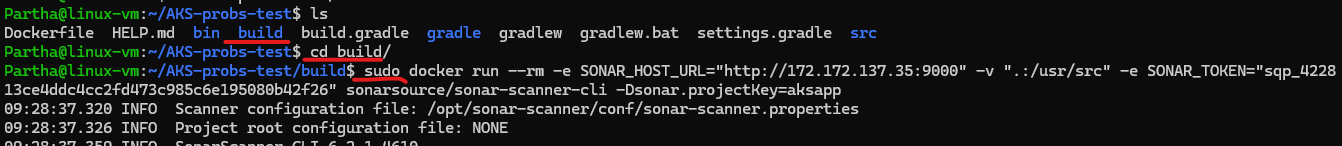
Issues

A screenshot of a computer

Description automatically generated

Note running for html, js, node will directly get compiled.

Running with Gradel project we need to build the project first and the scanning will run on build folder where the code is in .class format. It does not compile .java files.



Disadvantages –

to compile and get result only after build. in this case build is not not syntex it's artifect. then how can i check my actual code?

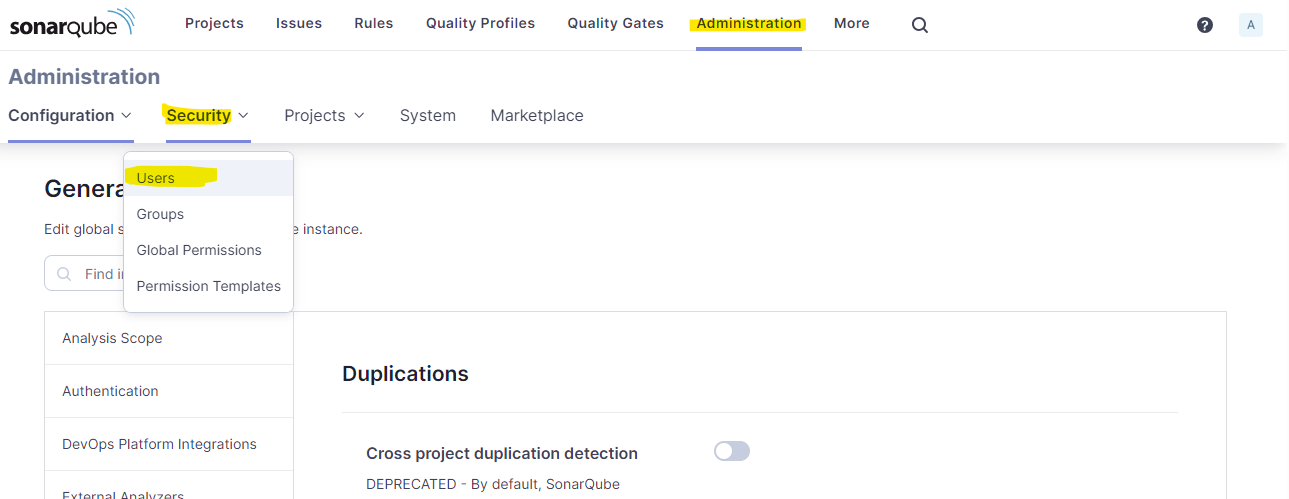
1. Create users and allow access  
     
   a. Create user DevOps with all permissions

b. Create user Developer with read-only access

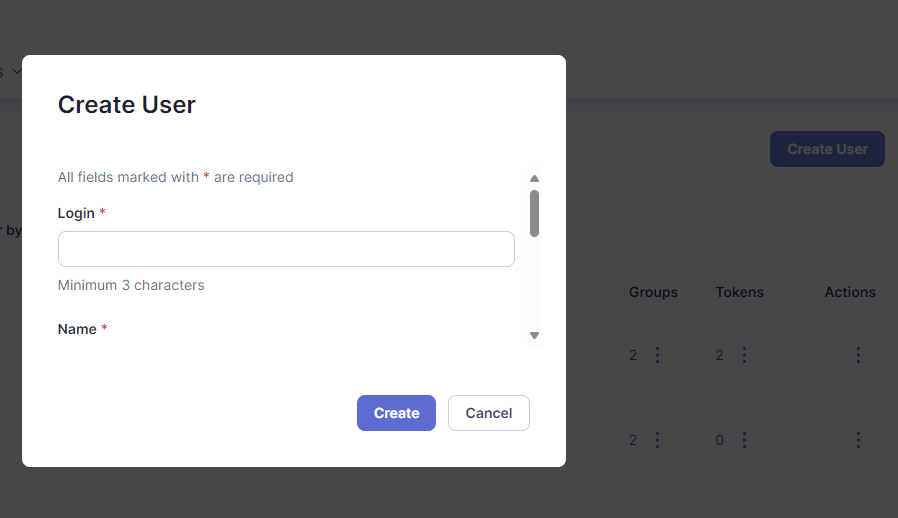
login as administrator

go to Administrator choose security

go to users

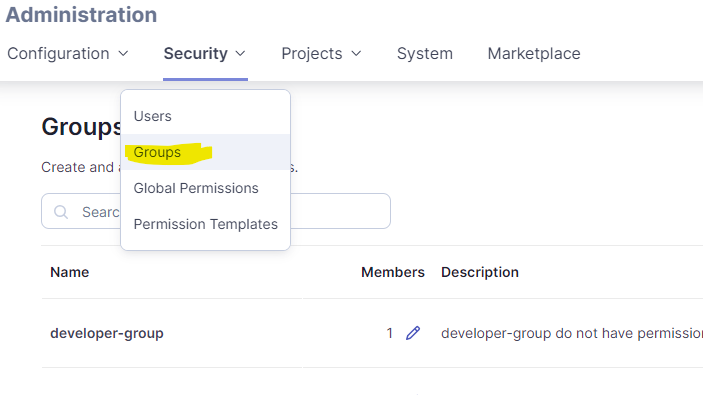


Click on create user and define user datalogin will be username and paddword for that user authentication



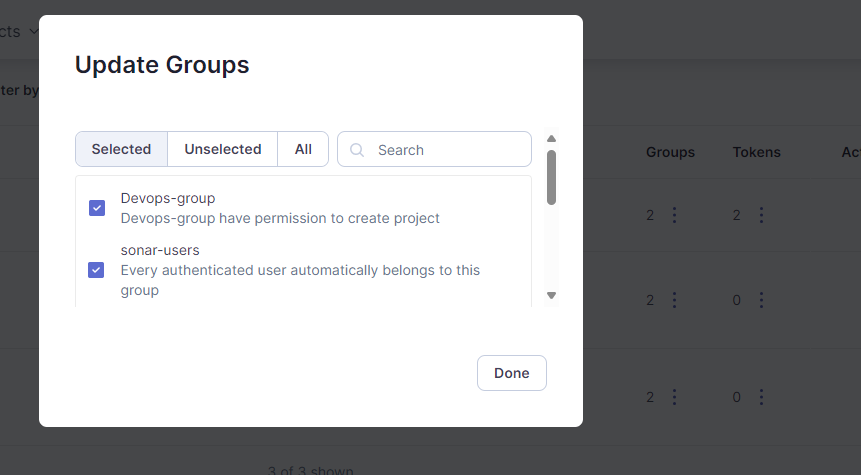
User will be added to sonar-users group by default. Delete all access for sonar-users group so that we can create custom groups and allow permissions to groups

To create group go to security and choose group



Can add users to group or In users page go down choose user and go to group can add or remove user from group

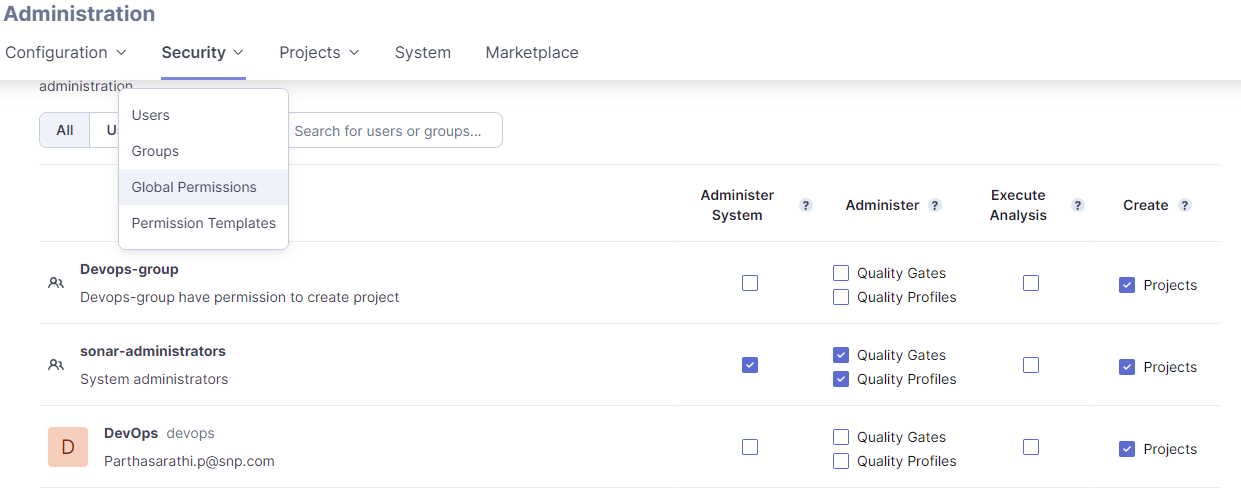
In my case I have created devops group and added devops user to that group



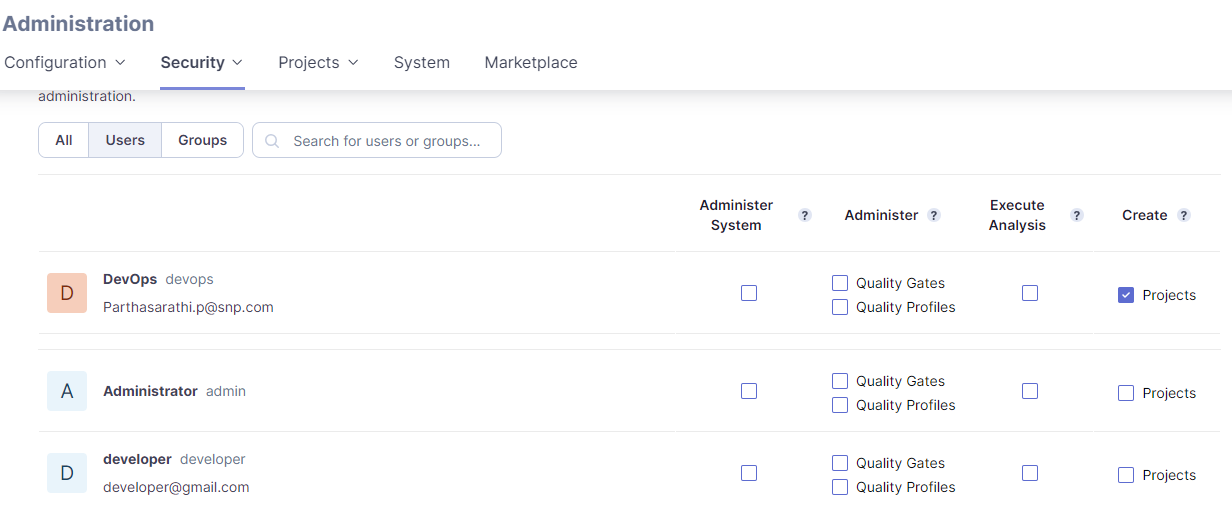
Allow or deny permission for that group

Go to security -> global permissions and allow or deny permission to the user

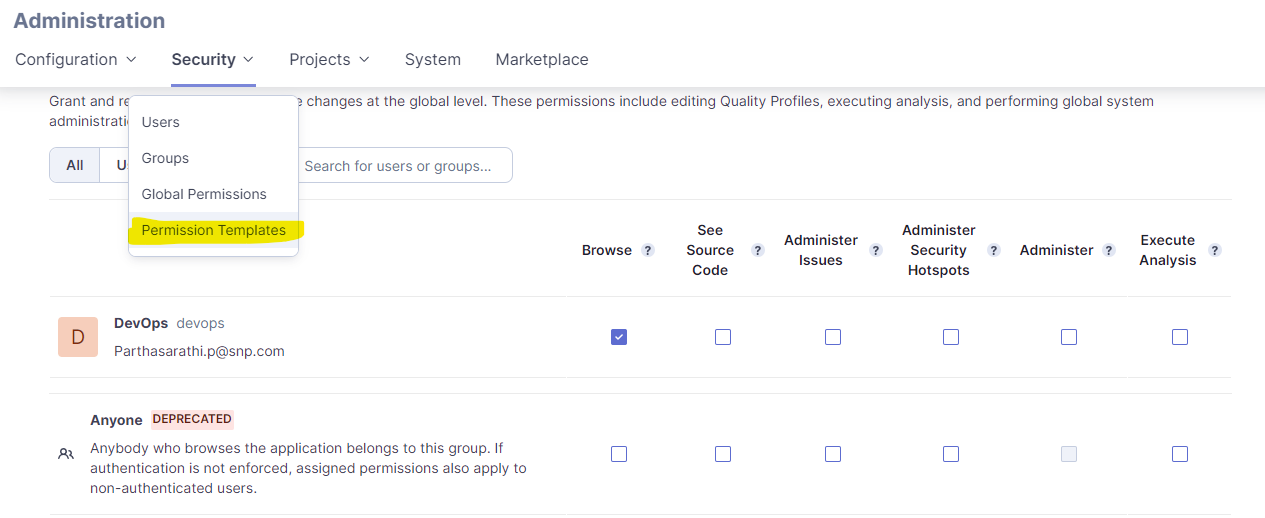
Here we can define permission like can create project ot not, analysis access, admin etc..



If we don’t want to go through groups we can allow or disallow permission as user lavel as well

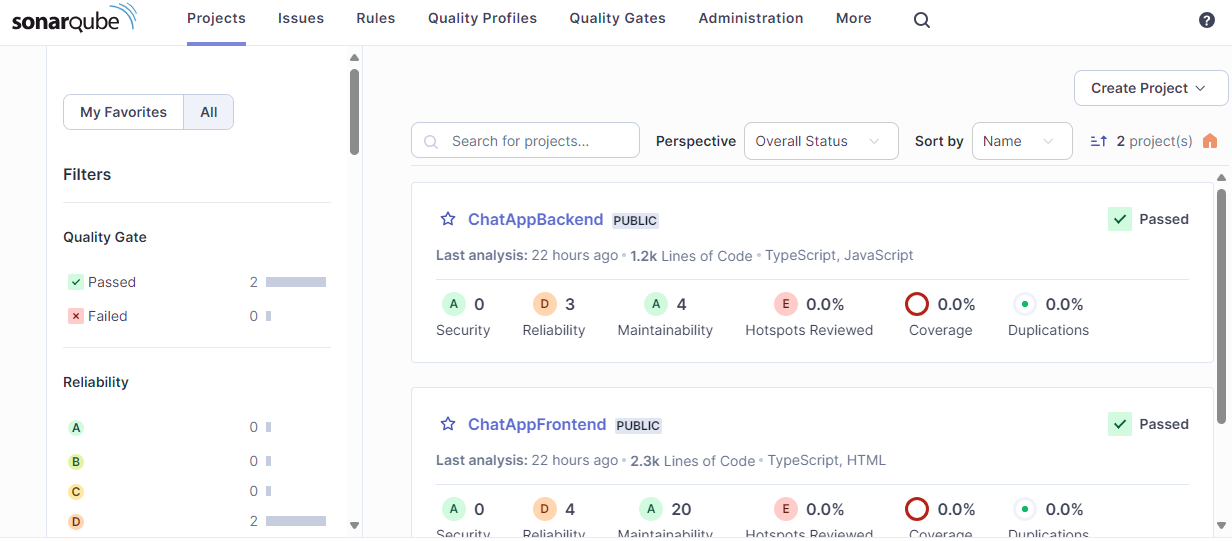


For more permission like browse projects, see code, fix issue or execute analysis we can go to permission templates and give permission.



1. Analyze code from standard vm  
   Project is on vm analyze code from there and publish result (manual)  
     
   create project on sonarqube backend, frontend etc..  
   choose loal project option, will generate key and token.

Modify in below code with key and token go to project file and run it.  
  
>> sudo docker run  --rm -e SONAR\_HOST\_URL="http://35.90.93.22:9000" -e SONAR\_LOGIN="sqp\_aca3716695f93a33e306b925beb34976caf13502"  -v ".:/usr/src" sonarsource/sonar-scanner-cli -Dsonar.projectKey=lms  
  
will see analysis result post successful run



1. Build CI/CD pipelines from azure devops repos to connect to sonar server and automatically runs analysis when any changes happened.