

Las acciones de GitHub le permiten realizar la mayoría de las tareas de CI/CD de forma gratuita, directamente desde su repositorio de GitHub. Sin embargo, uno de los desafíos es que no hay una instalación integrada como, por ejemplo, SonarQube para administrar la calidad del código.

Afortunadamente, SonarSource proporciona SonarCloud; una oferta de SonarQube SaaS que es gratuita para proyectos públicos! También es fácil alimentar SonarCloud desde GitHub Actions.

Use [el siguiente repositorio de GitHub](#) con código Java para generar información sobre la calidad del código.

Configuración Sonarcloud

Para enviar datos a SonarCloud, es necesario realizar alguna configuración en el lado de SonarCloud y GitHub. Primero inicia sesión en [SonarCloud](#) usando tu cuenta de GitHub.



Clean Code Rockstar Status

Eliminate bugs and vulnerabilities.
Champion quality code in your projects.

Go ahead! Analyze your repo:



GitHub



Bitbucket






Azure DevOps




GitLab


Free for Open-Source Projects


A continuación tienes que autorizar SonarCloud:




SonarCloud by **sonarcloud** would like permission to:

**Verify your GitHub identity** (MaartenSmeets)

**Know which resources you can access**

**Act on your behalf**

Resources on your account


**Email addresses** (read)
View your email addresses


SonarCloud has not been installed on any accounts you have access to.
[Learn more about SonarCloud](#)


Cancel

Authorize SonarCloud

Authorizing will redirect to
<https://sonarcloud.io>

 Not owned or operated by GitHub

 Created 3 years ago

 More than 1K GitHub users


Ahora puede agregar una organización de GitHub que esté utilizando a SonarCloud haciendo clic en + junto a su cuenta.

Create an organization


An organization is a space where a team or a whole company can collaborate across many projects.




You will be asked to grant access to the SonarCloud application on your organization or user account, which will allow you to choose which repositories you want to analyze.

 [Choose an organization on GitHub](#)


Elegí mi organización personal. SonarCloud se instalará como una aplicación de GitHub para esa organización.


 / [Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)




Install SonarCloud


Where do you want to install SonarCloud?

 MaartenSmeets [Configure >](#)

 AMIS-Services [>](#)

Puedes dar acceso a SonarCloud a tu repositorio

 Search or jump to... Pull requests Issues Marketplace Explore



Install SonarCloud

Install on your personal account Maarten Smeets

☐ All repositories

This applies to all current and future repositories.

☒ Only select repositories

Select repositories

Selected 1 repository.

MaartenSmeets/java_sec_demo

...with these permissions:

✓ Read access to code and metadata

✓ Read and write access to checks, commit statuses, and pull requests

User permissions

SonarCloud can also request users' permission to the following resources. These permissions will be requested and authorized on an individual-user basis.


✓ Read access to emails

Install

Cancel

Next: you'll be directed to the GitHub App's site to complete setup.


En SonarCloud ya puedes crear una organización

 My Projects My Issues NEW JS/TS SAST precision improve... Explore Search for projects and files...

Create an organization

An organization is a space where a team or a whole company can collaborate across many projects.

1 Import organization details

Import  Maarten Smeets into a SonarCloud organization

Key*
maartensmeets

Organization names must start with a letter or number, followed by letters, numbers or hyphens, and must end with a letter or number. Maximum length: 255 characters.

Add additional info

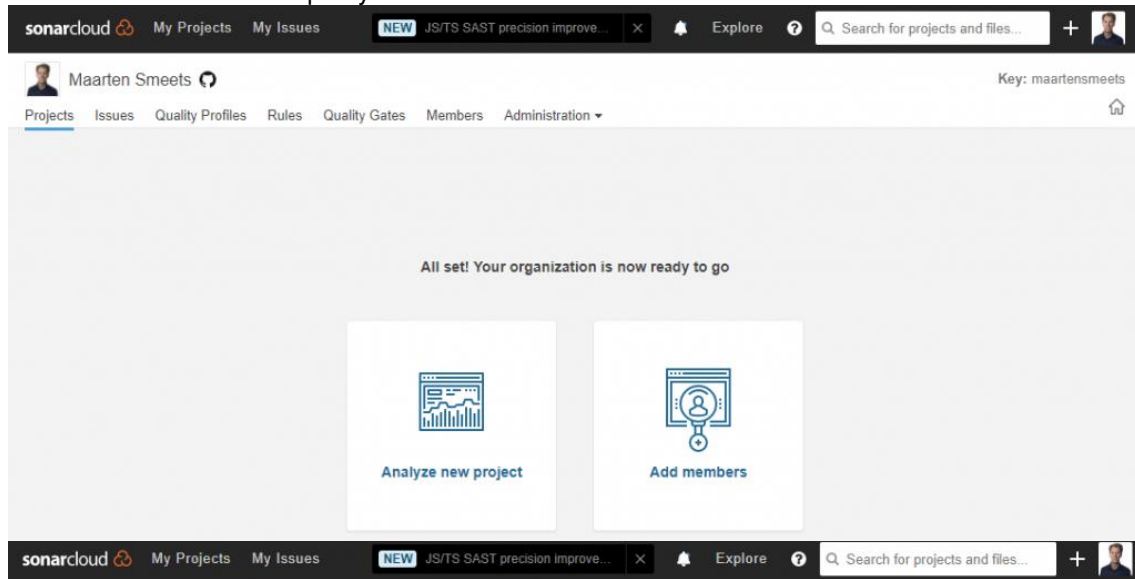
1

All members from your GitHub organization Maarten Smeets will be added to your SonarCloud organization. As they connect to SonarCloud with their GitHub account, members will automatically have access to your SonarCloud organization and its projects. [See all members on GitHub](#)

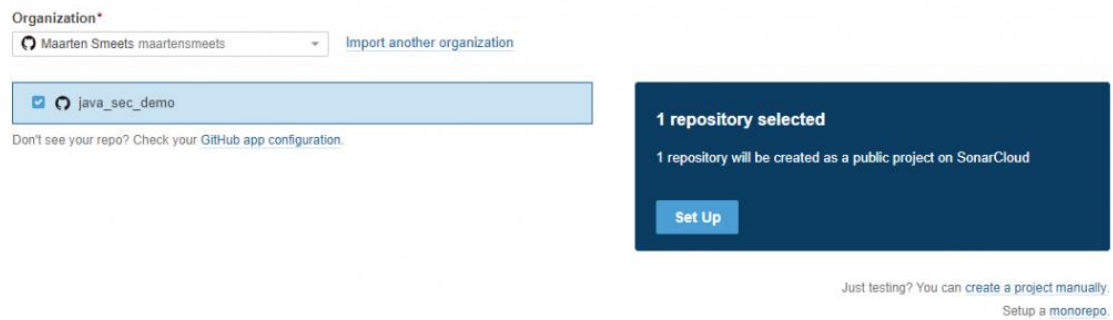
Continue

2 Choose a plan

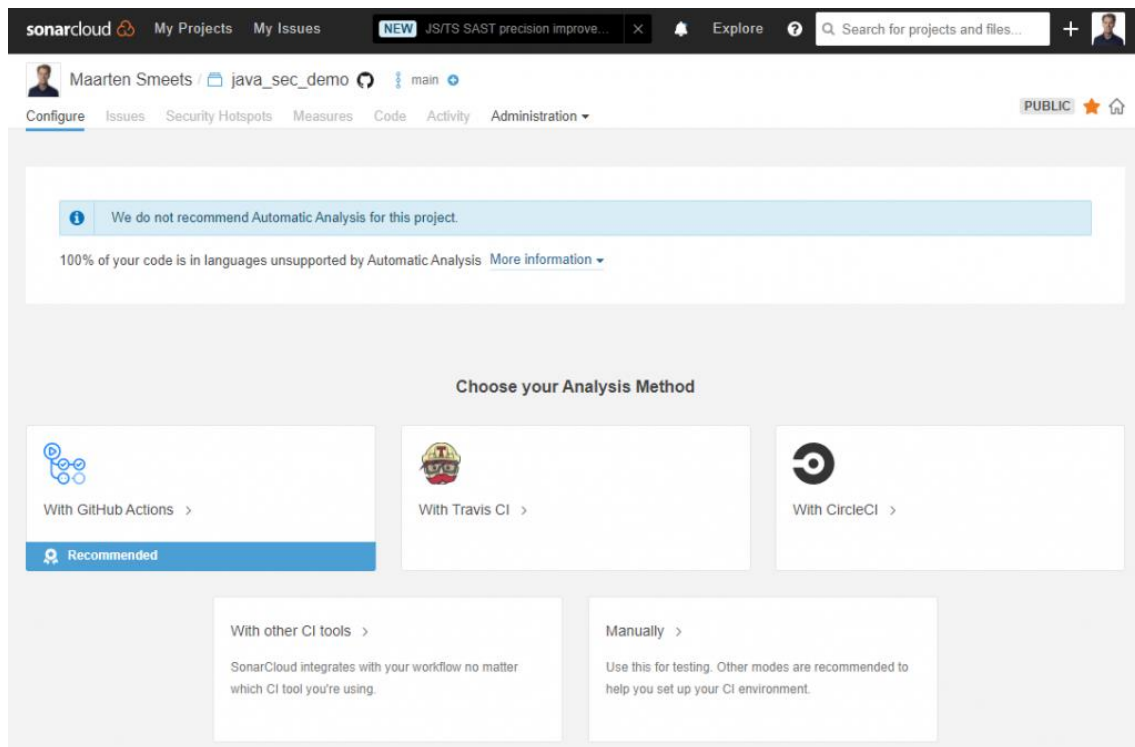
Y analizar un nuevo proyecto



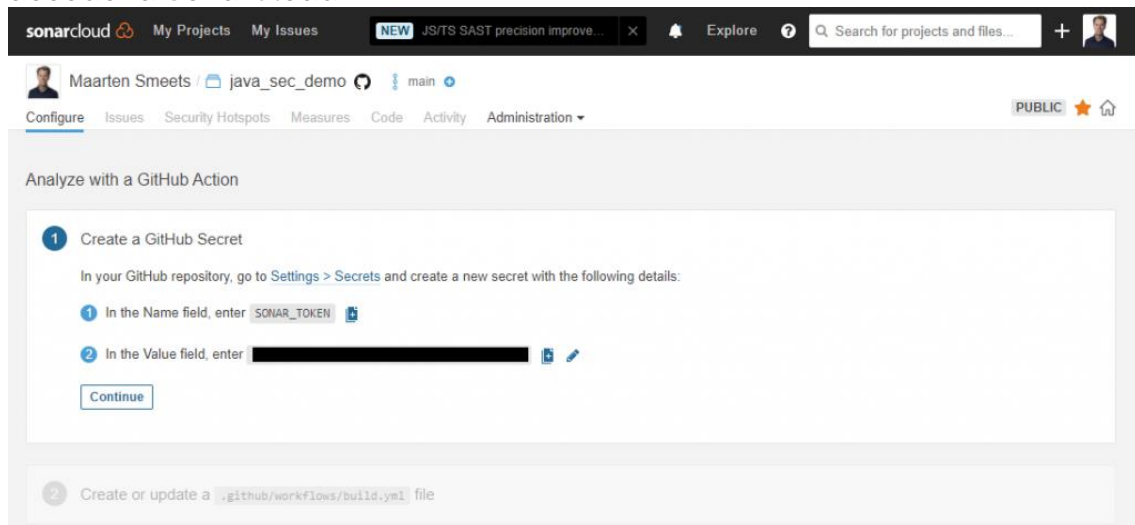
Analyze projects - Select repositories



Cuando haces clic en Configurar, SonarCloud sugiere hacer un análisis con GitHub Actions



En tu repositorio de GitHub, necesitas crear un token para que GitHub pueda acceder a SonarCloud:



Convenientemente, SonarCloud proporciona instrucciones sobre lo que debe hacer para permitir que las GitHub Actions alimenten a SonarCloud. Estos incluyen la actualización de su archivo pom.xml para especificar el objetivo del complemento SonarSource y la creación de un flujo de trabajo o la adición de algunas acciones específicas para el análisis. Específicos son la opción de clonación superficial, el caché de artefactos de SonarCloud y, por supuesto, el paso de compilación y análisis.

2 Create or update a `.github/workflows/build.yml` file


What option best describes your build?

Maven Gradle .NET Other (for JS, TS, Go, Python, PHP, ...)

Update your `pom.xml` file with the following properties:

```
<properties>
<sonar.projectKey>MaartenSmeets_java_sec_demo</sonar.projectKey>
<sonar.organization>maartensmeets</sonar.organization>
<sonar.host.url>https://sonarcloud.io</sonar.host.url>
</properties>
```

 Copy

Create or update your `.github/workflows/build.yml`  yml file with the following content:

```
name: Build
on:
  push:
    branches:
      - master
  pull_request:
    types: [opened, synchronize, reopened]
jobs:
  build:
    name: Build
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v2
        with:
          fetch-depth: 0 # Shallow clones should be disabled for a better relevancy of analysis
      - name: Set up JDK 11
        uses: actions/setup-java@v1
        with:
          java-version: 11
      - name: Cache SonarCloud packages
        uses: actions/cache@v1
        with:
          path: ~/.sonar/cache
          key: ${ runner.os }-sonar
          restore-keys: ${ runner.os }-sonar
      - name: Cache Maven packages
        uses: actions/cache@v1
        with:
          path: ~/.m2
          key: ${ runner.os }-m2-${ hashFiles('**/pom.xml') }
          restore-keys: ${ runner.os }-m2
      - name: Build and analyze
        env:
          GITHUB_TOKEN: ${ secrets.GITHUB_TOKEN } # Needed to get PR information, if any
          SONAR_TOKEN: ${ secrets.SONAR_TOKEN }
        run: mvn -B verify org.sonarsource.scanner.maven:sonar-maven-plugin:sonar
```

 Copy

En el flujo de trabajo de ejemplo proporcionado por SonarCloud, la compilación se activa en cada confirmación. Cambié esto para hacerlo manualmente. Puede buscar mi definición de flujo de trabajo [aquí](#).

Workflows

New workflow

CI

main.yml

All workflows

🔗 CI

10 workflow runs

Event ▾ Status ▾ Branch ▾ Actor ▾

This workflow has a workflow_dispatch event trigger.

Run workflow ▾

✓ CI

CI #31: Manually run by MaartenSmeets

✗ CI

Use workflow from

Branch: main ▾

Run workflow

The screenshot shows the GitHub Actions interface for a workflow named 'build' in the repository 'MaartenSmeets / java_sec_demo'. The workflow is in a 'Completed' state, indicated by a green checkmark and the label 'CI CI #31'. The workflow summary shows it 'succeeded 6 minutes ago in 5m 25s'. The workflow steps are listed in a dark-themed panel on the right, each with a green checkmark indicating successful completion. The steps are: Set up job, Set environment variables, Checkout sources, Setup Java 11, Cache Maven packages and Google Jib cache, Cache SonarCloud packages, Static checks, Publish image to DockerHub, Anchore scan, Start service, OWASP ZAP scan, Build and analyze, Publish Test Report, Post Cache SonarCloud packages, Post Cache Maven packages and Google Jib cache, Post Setup Java 11, Post Checkout sources, and Complete job.

Search or jump to... / Pull requests Issues Marketplace Explore

MaartenSmeets / java_sec_demo

<> Code ⓘ Issues 🔗 Pull requests ▶ Actions 📄 Projects 📖 Wiki 🛡 Security 📈 Insights ⚙ Settings

✓ CI CI #31

Summary

Jobs

✓ build

build
succeeded 6 minutes ago in 5m 25s

- > ✓ Set up job
- > ✓ Set environment variables
- > ✓ Checkout sources
- > ✓ Setup Java 11
- > ✓ Cache Maven packages and Google Jib cache
- > ✓ Cache SonarCloud packages
- > ✓ Static checks
- > ✓ Publish image to DockerHub
- > ✓ Anchore scan
- > ✓ Start service
- > ✓ OWASP ZAP scan
- > ✓ Build and analyze
- > ✓ Publish Test Report
- > ✓ Post Cache SonarCloud packages
- > ✓ Post Cache Maven packages and Google Jib cache
- > ✓ Post Setup Java 11
- > ✓ Post Checkout sources
- > ✓ Complete job

Después de que los resultados se hayan enviado a SonarCloud, puede buscarlos allí;

Filters

Type

Bug0

Vulnerability1

Code Smell3

Severity

Blocker1

Critical0

Major1

Minor1

Info1

Resolution

Status

Security Category

SonarSource

Others4

OWASP Top 10

SANS Top 25

CWE

Creation Date

Language

Rule

Tag

Directory

File

Assignee

Author

Bulk Change

to select issues

to navigate

1 / 4 issues

22m

src/.../smeetsm/demoservice/controller/DemoRestController.java

nLamis.smeetsm.demoservice.controller.DemoRestController is a Spring endpoint (Controller) Why is this an issue? FINDSECBUGS

VulnerabilityMajorOpenNot assigned5min effortComment

src/.../nl/amis/smeetsm/demoservice/DemoserviceApplicationTests.java

Add at least one assertion to this test case. Why is this an issue?

Code SmellBlockerOpenNot assigned10min effortComment

src/.../smeetsm/demoservice/controller/DemoRestControllerTest.java

Remove this 'public' modifier. Why is this an issue?

Code SmellInfoOpenNot assigned2min effortComment

4 of 4 shown