

SonarQube / SonarLint



SonarQube / SonarLint

https://www.sonarsource.com/products/sonarqube

SonarQube

- créé en 2006, maintenue par l'entreprise SonarSource (freemium)
- plateforme open-source pour l'inspection continue de la qualité du code
- serveur Web fournissant des pages d'analyse de la qualité du code
- s'intègre facilement avec les moteurs de production (e.g. Gradle) et les outils de CI/CD comme GitLab

SonarLint

- plugin pour IDE qui permet une partie de l'analyse pendant le codage
- peut être lié à une instance de SonarQube

SONARQUBE FEATURES

the code quality tool for better code

Enable your team to systematically deliver and meet high code quality standards, for every project, at every step of the workflow.

()

30+ languages, frameworks & laC platforms

Analyze the code quality of all the languages in your projects. Patch bugs, close vulnerabilities and follow best practices with a single source of truth.

25

 \bigcirc

integration with DevOps platforms

Easy project onboarding with integration to GitHub, GitLab, Azure and Bitbucket; in-cloud & on-prem. Plus a Jenkins plugin and easy integration with popular CI tools and build systems.

క్ర

clear go/no-go Sonar Quality Gate

Fail pipelines when the code quality doesn't meet your defined requirements and prevent problems from being merged or deployed.

2

high operability

Run your instance your way, as a service, on Docker, or with Kubernetes with vertical and horizontal scaling support, plus multi-threaded, server-side processing.

0

super-fast analysis

Super-fast analysis gets you actionable Clean Code metrics in minutes instead of hours.

critical security rules for vital languages

Receive actionable, high-precision feedback at the right place and time. Benefit from 5,000+ coding rules and industry-leading taint analysis of Java, C#, PHP, Python, TypeScript & JavaScript.

shared, unified configurations

Ô.

Align your team with a consistent definition of code health. Collaborate efficiently in making your code clean and meeting your team's code quality expectations.



Sonarlint IDE integration

Add the SonarLint extension to your favorite IDE and find code issues on the fly. SonarQube rules and analysis settings synchronize to SonarLint, aligning teams around a single standard of Clean Code.

Utilisation du SonarQube de l'IUT

Nous utiliserons l'instance suivante : • SonarQube IUT

Premier login
Log in to SonarQube
Login
Password
Log in Cancel

Utilisez vos identifiants habituels.

Première page d'accueil



Quality Profiles

sona	arqube	Projects	Issues	Rules	Quality Profiles	Quality Gate	es More	Q	
	JSP, 1 profile(s)				Projects 😡	Rules	Updated	Used	
	Sonar way BUILT	-IN			DEFAULT	<u>0</u>	6 months ago	Never	Q -
	Java 1 profile(s)				Projecte O	Bulae	Undated	llead	
	Sonar way BUILT	'-IN			DEFAULT	483	6 months ago	19 days ago	٥-
	JavaScript, 1 pro	file(s)			Projects @	Rules	Updated	Used	
	Sonar way BUILT	'-IN			DEFAULT	237	6 months ago	Never	Q •

Java Quality Profile

sonarqube	Projects	Issues	Rules	Quality Pro	files	Quality Gates	More	Q				0	м
Quality ProfilesJava Sonar way DEFAULT This is a built-in quality pr	BUILT-IN ofile that might b	e updated a	utomatically.						Updated: 6 months ago	Used: 19 days ago	Changelog	٥-	
Rules	Active	Inactive		Inheritance									
Total	483	143		Sonar way	UILT-IN			483 active rules	0.0	werridden rules			
賽 Bugs	135	10											
6 Vulnerabilities	31	2											
Code Smells	276	131		Projects									
Security Hotspot	s 37	o ctivate More		DEFAULT Eve	ry project n	ot specifically assoc	ciated with a	quality profile will be	associated to this one by de	fault.			

Le profile Java par défaut : 483 règles actives, i.e. une norme ou une pratique de codage qui doit être suivie

- Bugs : anomalies évidentes du code, qui impactent la fiabilité.
- Vulnerabilities : faiblesses du code pouvant nuire au système.
- codes smells : code mal écrit qui peut ralentir le développement et augmenter les coûts de maintenance.
- Security hotspot : code sensible à la sécurité et qui doit être examiné manuellement.



Permet de définir des seuils de qualité pour le code ajouté après une analyse : par exemple pour stopper un pipeline de Cl

sonarqube Projects Issue	s Rules Quality Profiles	Quality Gates More	Q	0
Quality Gates	Sonar way BUILT-IN			Сору
Sonar way DEFAULT BUILT-N	This quality gate complies with This quality gate complies with th the neures that: • Nonew bugs are introduced • Nonew vulnerabilities are intro- • New code has imitted duplicat • New code has imitted duplicat • New code has imitted duplicat	t Clean as You Code e (<u>* Clean as You Code</u> methodolo oduced eviewed ii debt ion by tests	gy, so that you benefit from the most efficient approach to delivering	g Clean Code.
	Conditions @			
	Conditions on New Code Metric	Operator	Value	
	Reliability Rating	is worse than	A (No bugs)	
	Security Rating	is worse than	A (No vulnerabilities)	
	Security Hotspots Reviewed	is less than	100%	
	Maintainability Rating	is worse than	A (Technical debt ratio is less than 5.0%)	
	Coverage	is less than	80.0%	
	Duplicated Lines (%)	is greater than	3.0%	

Import d'un projet depuis GitLab



Création d'un token pour l'interaction SonarQube / GitLab

Pour pouvoir importer vos projets depuis GitLab, il faut que SonarQube puisse communiquer avec notre instance de GitLab.

SonarQube demande de créer un token depuis l'IU de GitLab :

⊌ Gitlab project onboarding						
Grant access to your projects Sona-Oube needs a personal access token to access and list your projects from GitLab. You have to do this again as your token may have expired or has been revoked. If this does contain your system administrator.	How to create a personal access token? Click the following link to generate a token in GilLab, and copy-paste it into the personal access token field.					
Enter personal access token '	Set a name, for example "SonarQube", and select the following scope: read_api					

Dans GitLab

Dans le paramétrage de votre profil :





Une fois le token ajouté, la liste des projets GitLab appraît dans SonarQube :

➡ Gitlab project onboarding		
Q. Search for projects		
Cl_CD_gitlab_java_gradle MICHEL Fabien	g* See on GitLab	Set up
Merge_request_reviewing michel fabien	🖉 See on GitLab	Set up
	2 of 2 shown	

Choix du type de Cl

Choisir permet d'obtenir des squelettes pour les scripts de Gradle et de Cl

sonar qube	Projects Issues	Rules Quali	ty Profiles	Quality Gates	Administration	More	Q
☆ Merge_request_review	wing / 🚺 main ~	?					
Overview Issues	Security Hotspots	Measures	Code Act	ivity			
How do you want to a	nalyze your repository?						
Do you want to integrate	with your favorite CI? Choo	se one of the following	tutorials.				
With Jenkins	With GitL	ab Cl	Other CI				

Are you just testing or have an advanced use-case? Analyze your project locally.

Info à utiliser dans GitLab

Création des variables qui seront utilisées dans le script de CI

Overview	Issues	Security Hotspots	Measures	Code	Activity		
1	Add environment variables 1. Define the SonarQube Token environment variable. In GitLab, go to Settings > Cl/CD > Variables to add the following variable and make sure it is available for your project: a. In the Key field, enter sowar Token b. In the Value field, enter an existing token, or a newly generated one: c. Uncheck the Protect Variable checkbox. d. Check the Mask Variable checkbox.						
	2. Define the S Still in Settin a. In the Key b. In the Val c. Uncheck d. Leave the Continue	onarQube URL environment gs > Cl/CD > Variables add y field, enter sowar Host_veru ue field, enter https://sqtai the Protect Variable checkb y Mask Variable checkbox un	variable. a new variable and b 'o. tutnontp.untv.ne ox. hchecked.	d make sure	it is available for your project:		

Info à utiliser dans GitLab

Attention à bien mettre l'URL suivante ; en http et avec le bon port

Update variable						
Key						
SONAR_HOST_URL						
Value						
http://sqinfo.iutmontp.univ-montp2.fr:9333						
Туре	Environment scope 🕜					
ENV_VAR ~	All (default) ~					
Flags ⑦ Protect variable Export variable to pipelines running on protected bra	Flags ⑦ Protect variable Export variable to pipelines running on protected branches and tags only.					
 Mask variable Mask this variable in job logs if it meets regular expr 						
 Expand variable reference \$ will be treated as the start of a reference to anot 	her variable.					

Variables							
Variables store information, the passwords and secret keys, that you can use in job scripts. Each project can define a maximum of 8000 variables. Learn more.							
Variables can have seven							
Protecting: Only exposed to protected branches or protected lags. Water in pile logs. Must enough exposing regularments. Expensing: material must be transformed to transformed to another variable.							
+ Key		Attributes	Environments				
SONAR, HOST, URL B.			At (banad) 👌 🛛 🚺				
SONAR, TOKEN (Å			At (MAND) 🖏 🖉				
Addivariable Proved values							

Mise en place dans le projet GitLab

2	Create or update the configuration file	
	1. What option best describes your build?	
	Maven Gradle .NET Other (for JS, TS, Go, Python, PHP,)	
	2. Add the following to your build.gradle 📋 or build.gradle.kts 🏮 file:	
	build.gradle build.gradle.kts	
	<pre>plugins { id "erg.somrqube" version "4.2.1.3168" } somar { properties { properties { property 'somer.projectRey", "etuntCohl_werge_request_reviewing_WIPy=066gDYCEDitp property 'somer.quesitypete.weit", "reviewing" } }</pre>	D Cop
	3. Create or update your .gttlab-ct.ynl 🏮 file with the following content.	
	<pre>sourcebe-cbeck: toage:graphic-beck: vertables: SOBM_USELIVET."S(CL_PROJECT_DIB).sour" # Defines the location of the analyst CT_DEFE: "0" # Fills git to fetch all the branches of the project, required by cache:</pre>	D Cop

II faudra corriger ce script : vous trouverez un projet
Gradle_Sonar_Java_Template dans notre GitLab, afin d'avoir un
exemple pour app/build.gradle et .gitlab-ci.yml

Il n'y a plus qu'à faire un commit pour que le résultat de l'analyse soit disponible sous SonarQube

You're all set!

You're all set and ready to improve the quality and security of your code!



Commit and push your code to start the analysis.

Each new push you make on your main branch will trigger a new analysis in SonarQube.



This page will then refresh with your analysis results.

If the page doesn't refresh after a while, please double-check the analysis configuration, and check your logs.

Waiting for the first analysis to come in...

Exemple d'un résultat d'analyse

Overview Issues Security Hotspots Me	asures Code Activity	Project Settin	gs - III Project Information
QUALITY GATE STATUS ®	MEASURES		
Failed 1 conditions failed	New Code Overall Code Since Septemb Started 4 months ago		
9.4% Coverage on New Code is less than 80.0%	35 * Bugs		Reliability (E)
	2 & Vulnerabilities		Security (E)
	51 Security Hotspots e	0.0% Reviewed	Security Review
	6d 3h Debt	446 Code Smells	Maintainability 🛕
	Overage on 3.1k Lines to cover	143 Unit Tests 0.3% Duplications on 6.3k Lines	2 Duplicated Blocks

SonarQube peut fonctionner avec Jacoco

Jacoco est un outil qui mesure la couverture des tests des projets Java Première étape : ajout de la fonctionnalité dans le build de Gradle



SonarQube peut fonctionner avec Jacoco

Deuxième étape : modification du script de CI. Exemple :

```
stages:
  - test
  - check
before script:

    GRADLE_USER_HOME="$(pwd)/.gradle"

    export GRADLE_USER_HOME

test:
  image: gradle:ire11-slim
 stage: test
  script: ./gradlew test
sonargube-check:
  stage: check
  image: gradle:jre11-slim
 variables:
    SONAR_USER_HOME: "${CI_PROJECT_DIR}/.sonar" # Defines the location of the analysis task cache
    GIT_DEPTH: "0" # Tells git to fetch all the branches of the project, required by the analysis task
 cache:
    key: "${CI_JOB_NAME}"
    paths:

    .sonar/cache

  script: ./gradlew sonar
  allow failure: true
```

Exemple de résultat obtenu pour la couverture dans SonarQube

Overview Issues	Security Hotspots	Measures Code Activity		Project Settings -	Project In	nformatic
Project Overview		Madkit	View as	↑ ↓ to select files ←	→ to navigate	99 files
> Reliability @		src/main/iava/madkit/logging/TextAreaHandler i	iava	0.0%	9	2
> Security @		src/main/java/madkit/simulation/viewer/Viewer/	2D iava	0.0%	15	4
> Security Review ©		src/main/java/madkit/messaries/XMI Messare i	iava	0.0%	37	6
> Maintainability ©		src/main/java/madkit/kernal/MadkitClassLoade	r iava	8.4%	155	107
~ Coverage COVER	AGE		n.java	0.4%	100	107
Overview	P	Siciliarityava/maukit/simulation/simul-anicipan		21.4%	11	-
On new code		Src/main/java/madkit/kernel/AbstractScheduler.	.java	22.1%	113	39
Coverage	9.4%	src/main/java/madkit/kernel/MDKCommandLine	e.java	25.0%	9	-
Lines to Cover	28	src/main/java/madkit/messages/ObjectMessage	e.java	25.0%	15	6
Uncovered Lines	25	src/main/java/madkit/simulation/Environment.ja	iva	26.1%	13	4
Line Coverage	10.7%	B src/main/java/madkit/messages/Messages.java	a	30.8%	5	4
Conditions to Cover	4	src/main/java/madkit/simulation/SimulationTime	er.java	32.0%	15	2
Uncovered Condition	ns 4	src/main/java/madkit/kernel/ConversationID.jav	/a	33.3%	8	10
Condition Coverage	0.0%	src/main/java/madkit/gui/fx/FXManager.java		36.8%	32	11
Overall		src/main/java/madkit/simulation/TickBasedTime	er.java	42.9%	8	-
Coverage	38.6%	src/main/iava/madkit/kernel/Mailbox.iava		44.1%	49	17
Lines to Cover	3,116	src/main/iava/madkit/kernel/KernelConfiguratio	in iava	44.4%	8	2
Line Coverage	1,868	src/main/java/madkit/kernel/Bole java	. I Jana	49.8%	99	47
Conditions to Cover	883	B erc/main/iava/madkit/simulation/scheduler/Tick	BasedScheduler java	50.0%	1	
Uncovered Condition	ns 586	are/main/ava/madult/kernel/AgentThreadEaster	nuisua	50.0% E0.1%		2
Condition Coverage	33.6%	Sichainjava/naukukemenAgent meadractor	iy.java	38.1%		2
Tests		src/main/java/madkit/Kernel/Madkit/Warning.java	a	60.0%	3	1
Unit Tests	143	Src/main/java/madkit/kernel/AgentAddress.java		62.5%	10	14
Errors	0	src/main/java/madkit/kernel/Overlooker.java		63.0%	18	2



Plugin pour IDE qui permet de vérifier les règles sonarqube pendant l'édition du code source.

harness the power of Clean Code

Connected Mode provides consistent and cohesive analysis at every step in your development workflow – in the IDE, in your Pull Requests & branches, and back.

powerful in itself, more benefits when connected



continuous Clean Code

SonarLint provides great benefits in standalone mode as you code. Get end-to-end additional coverage through your dev cycle when paired with SonarQube or SonarCloud.



everyone on the same page

When 'connected', rules and analysis settings from SonarQube or SonarCloud are automatically and real-time synchronized to SonarLint, aligning your project and entire team on a single standard of Clean Code.



Plugin pour Eclipse :





Depuis le marketplace sous Eclipse :







Pour importer des projets Gradle proprement :

1. Ajoutez le plugin 'eclipse' au fichier build.gradle de votre projet

2. Ajoutez le plugin 'EGradle IDE' à Eclipse





EGradle

Puis faire, file -> import

	ic paul	/home/fab/Programming/Java-work	Browse
GRADLE_USER_HOME (optional) JAVA HOME (optional)		per default: '{user.home}/.gradle'	Browse
Gradle call			
Call type	Linux/Mac - 0	Gradle wrapper in root project	
Shell	(no shell use	d)	
Gradle call	./gradlew		
Gradle bin folder:	Browse		
alidate preferenc	es correct		
OK - your gradle	settings are co	rrect and working.	

Sélectionnez ensuite le répertoire du projet et vérifiez le avec *Start* validation

Une fois SonarLint installé

On peut lier SonarLint à un serveur SonarQube, pour recevoir des notifications dans l'IDE Connected mode

Dans le menu Sonarlint:

Bind du projet sur le SonarQube

SonarQube Server URL		
URL: http://sqinfo.iutmontp.u	iniv-montp2.fr:9333	
	< Back Next >	Cancel Finish

 \Rightarrow

Choose authentication method				
• Token • Username + Password				
	< Back	Next >	Cancel	Finish



Génération du token sous SonarQube

Dans votre profil -> Onglet Security:

Tokens

If you want to enforce security by not providing credentials of a real SonarCube 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.

Generate	Tokens
----------	--------

Name		Туре	Expires in				
Eclipse		User Token	 1 year 	 Generate 			
Name	Туре	Project	Last use	Created	Expiration	Actions	
Sonar_testing	Project	Sonar_testing	< 1 hour ago	December 21, 2023	March 20, 2024	Revoke	

 \Rightarrow

(SonarLint

Bind du projet sur le SonarQube







Bind du projet sur le SonarQube

Select projects to bi	nd			
Complete your Conner or SonarCloud project inspect the project on	ted Mode setup to benefit from the server.	by binding your i the same rules a	local project to you ind settings that ar	ur SonarQube e used to
😂 Virtual Root				Add
ist ⊌app				Remove
🕞 utilities				
	< Back	Next >	Cancel	Finish

 \Rightarrow Sélection du projet enregistré dans SonarQube

Choose the Sona	arQube/SonarCloud	project		
michel_sonar_t	testing_AYvjFaEozFtxo	do272WOC		
	< Back	Next >	Cancel	Finish



Conclusion

SonarQube

- Principe CaYC : Clean as You Code
- Permet de s'assurer du niveau de qualité du code : Quality Gates
- Peut être intégré dans un piepeline de CI
- Peut inclure la couverture des tests

SonarLint

- Plugin pour les IDE
- Peut être connecté à une instance de SonarQube
- Un must have !