

SONARQUBE

I. Installer et créer un projet

II. Profile Qualité

III. Gate Qualité

Job Sonar

I. Installer et créer un projet

SAST

- « **S**tatic **A**nalysis **S**ecurity **T**ests »
 - analyse de code statique
- **DAST** « **D**ynamic **A**nalysis **S**ecurity **T**ests »
 - analyse de conformité en exécution *PAYANT*
- « **pentesting** » ou test d'intrusion
 - simuler une attaque => *CONTRAT*

installation d'un serveur

- avec Docker

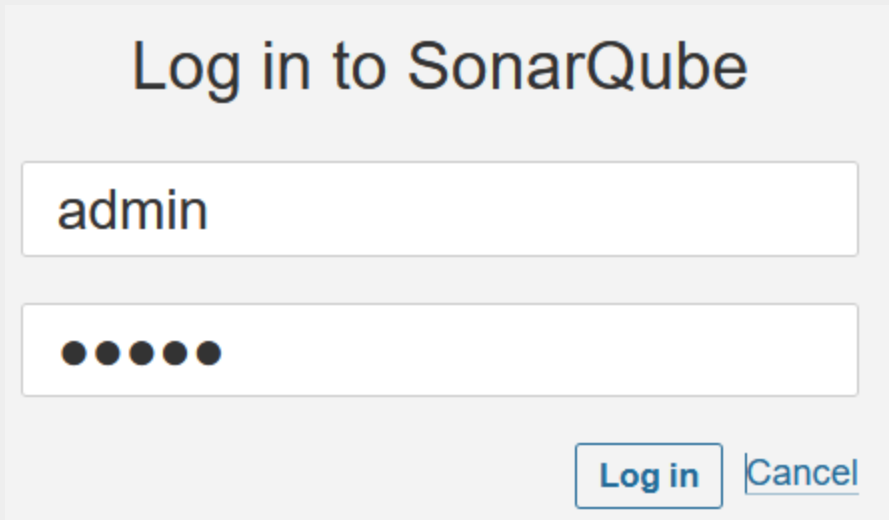
```
docker run \  
  --name sonar \  
  -d --restart unless-stopped \  
  -p 9000:9000 \  
  --memory 2g \  
  sonarqube:lts
```

“ *il faut augmenter la RAM à 10Go Gitlab + Sonarqube* ”

connexion

1. **http://gitlab.ian.fr:9000**

2. login/mdp: `admin / admin`



Log in to SonarQube

admin

●●●●●

[Log in](#) [Cancel](#)

3. old/new IDS: `admin / roottoor / roottoor`

Old Password *

New Password *

Confirm Password *

Update

4. config manually (self-signed cert !!!)



5. projet: project / project / main

Project display name *



Up to 255 characters. Some scanners might override the value you provide.

Project key *



The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.

Main branch name *

6. config locally (self-signed cert !!!)



Locally

7. token: grain de sel + generate

1 Provide a token

Analyze "project": **sqp_78a1ad5694b16e47e3ad9bdb6cbf053d7634183b** 

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your [user account](#).

Continue

8. Langage / Linux

2 Run analysis on your project

What option best describes your build?

Maven

Gradle

.NET

Other (for JS, TS, Go, Python, PHP, ...)

What is your OS?

Linux

Windows

macOS

9. copier la commande à injecter dans le **job sonar sur gitlab**

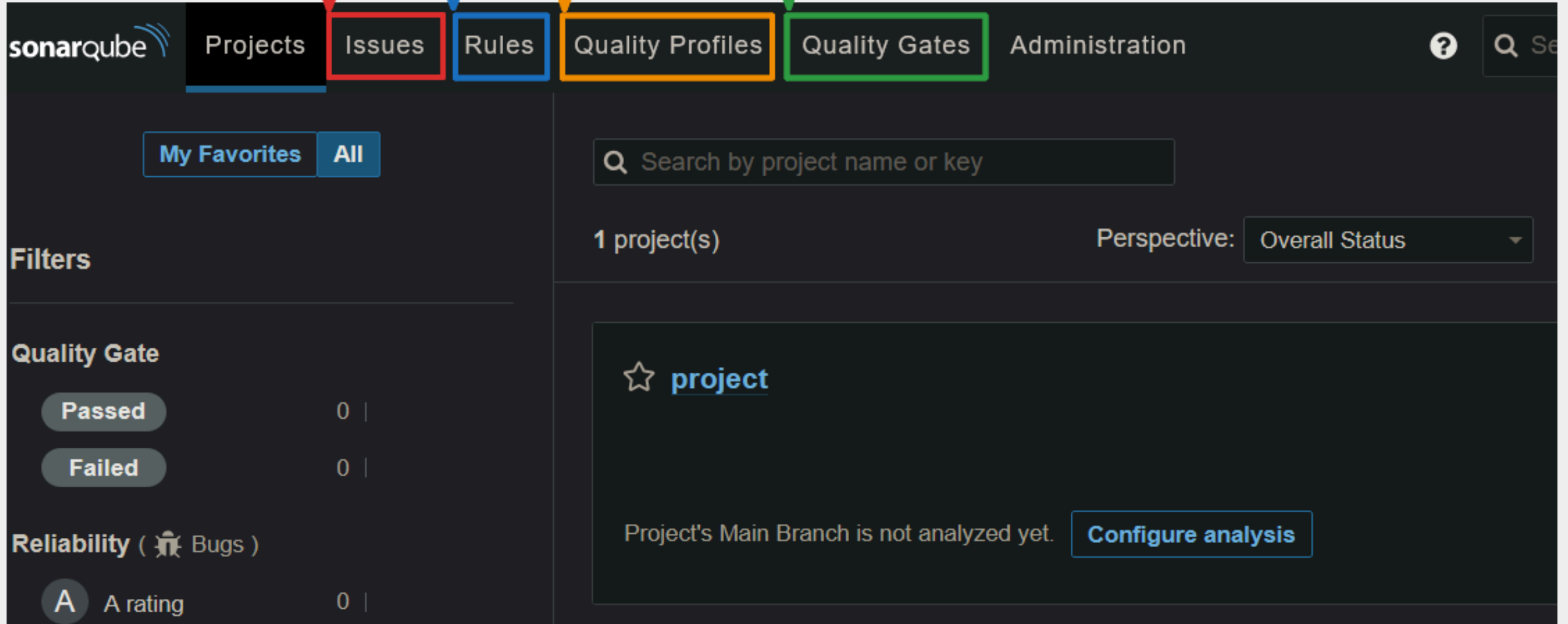
```
sonar-scanner \  
-Dsonar.projectKey=project \  
-Dsonar.sources=. \  
-Dsonar.host.url=http://gitlab.lan.fr:9000 \  
-Dsonar.login=sqp_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

erreurs
d'analyse
à corriger

base de
données de
règles

configurer
son analyse

seuil de
validité de
l'analyse




sonarqube Projects **Issues** Rules Quality Profiles Quality Gates Administration

My Favorites All

Filters

Quality Gate

Passed	0
Failed	0

Reliability ( Bugs)

A	A rating	0
---	----------	---

Search by project name or key

1 project(s) Perspective: Overall Status

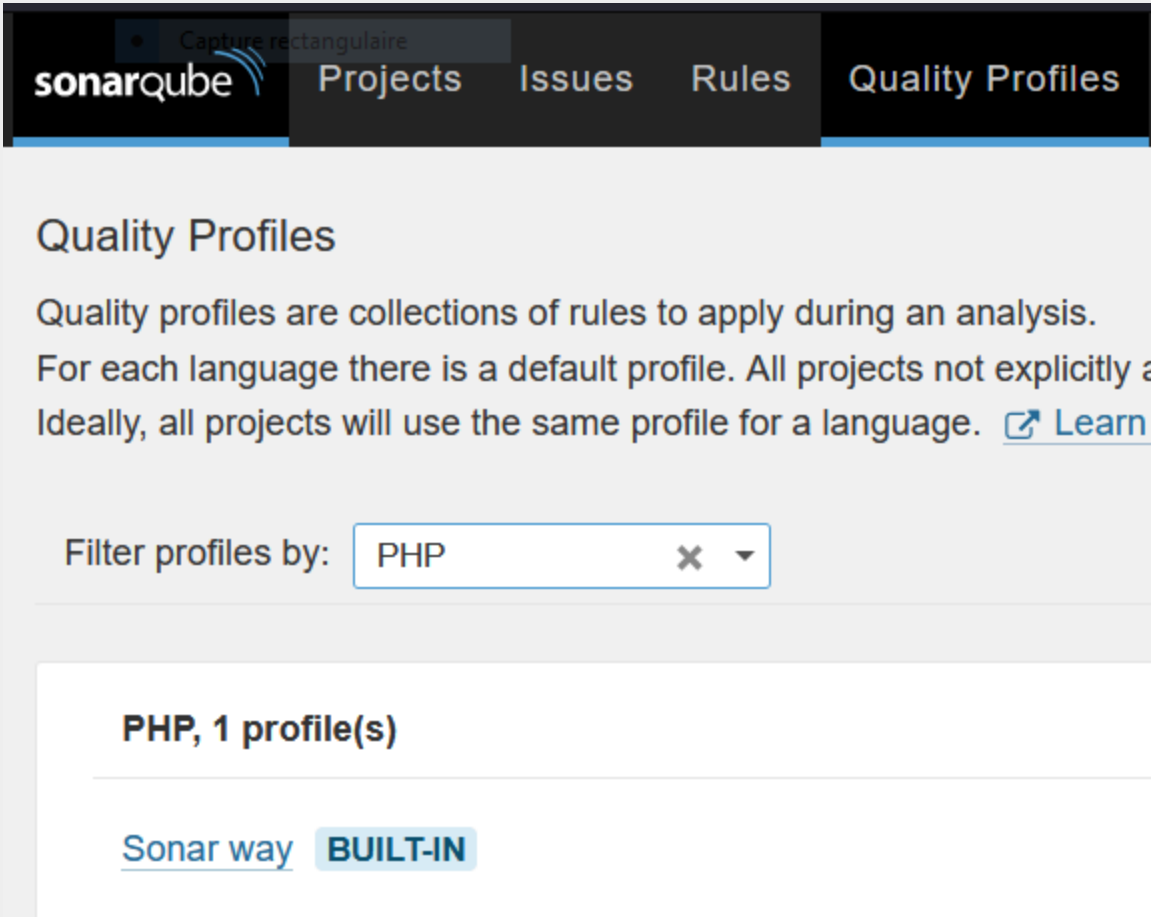
☆ **project**

Project's Main Branch is not analyzed yet. [Configure analysis](#)

II. Profile Qualité

créer un profile

1. filtrer sur un Langage



The screenshot shows the SonarQube web interface. At the top, there is a navigation bar with the SonarQube logo and tabs for 'Projects', 'Issues', 'Rules', and 'Quality Profiles'. The 'Quality Profiles' tab is selected. Below the navigation bar, the page title is 'Quality Profiles'. A descriptive text explains that quality profiles are collections of rules and that each language has a default profile. A filter section labeled 'Filter profiles by:' has a dropdown menu set to 'PHP'. Below this, a summary box indicates 'PHP, 1 profile(s)'. The first profile listed is 'Sonar way' with a 'BUILT-IN' badge.

sonarqube Projects Issues Rules Quality Profiles

Quality Profiles

Quality profiles are collections of rules to apply during an analysis.
For each language there is a default profile. All projects not explicitly a
Ideally, all projects will use the same profile for a language. [Learn](#)

Filter profiles by: PHP x ▼

PHP, 1 profile(s)

[Sonar way](#) **BUILT-IN**

2. **étendre** le *profile par défaut* en lecture seule, en activant des règles supplémentaires
3. ou **copier** IDEM en activant OU désactivant

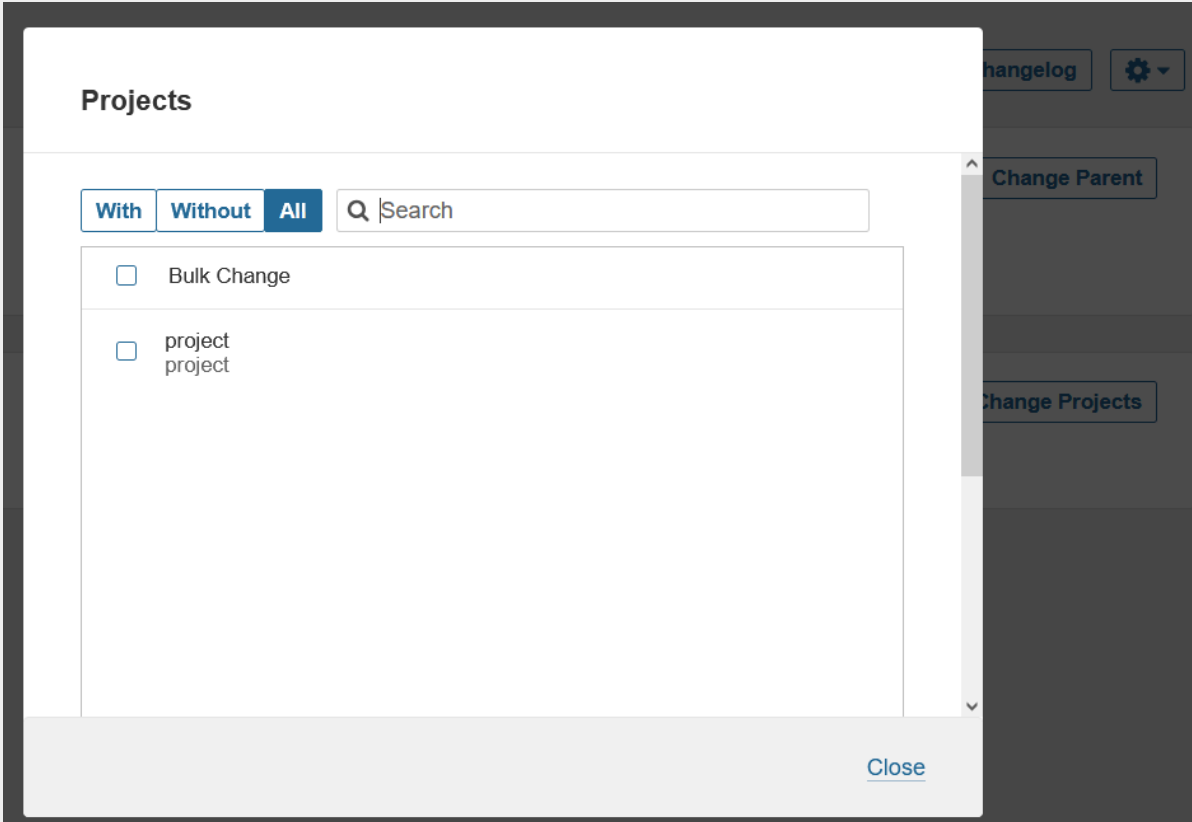
PHP, 1 profile(s)	Projects ?	Rules	Updated	Used
Sonar way BUILT-IN	DEFAULT	180	19 minutes ago	Never
<div>  <ul style="list-style-type: none"> Extend Copy </div>				

Filter profiles by: ✕ ▼

PHP, 2 profile(s)

[My Sonar way](#)

4. associer projet <=> profile



Projects





With Without **All**

- ☐ Bulk Change
- ☐ project project

[Close](#)

5. faire son marché dans le nouveau profile custom

My Sonar way

Rules	Active	Inactive
Total	185	72
 Bugs	43	9
 Vulnerabilities	18	6
 Code Smells	101	48
 Security Hotspots	23	9
Activate More		

← Détermine la note de Fiabilité

← Détermine la note de Sécurité

← Détermine la note de Maintenabilité (dette technique)

← Détermine la note de Sécurité Relative

“ *dette technique: retard lié à tout développement non optimal !!* ”

Filters

Clear All Filters

Search for rules...

Language

Type

Bug

Vulnerability

Code Smell

Security Hotspot

Tag

PHP-INI

Clear

Search for tags...

convention

brain-overload

pitfall

cwe

owasp-a6

php-ini

Bulk Change

Activate In...

Activate In **My Sonar way**

Deactivate In...

1 / 6 rules

"allow_url_include" should be disabled	PHP	Vulnerability	cwe, owasp-a1, php-ini, sans-top25-risky	Activate
"cgi.force_redirect" should be enabled	PHP	Vulnerability	cwe, owasp-a6, php-ini	Activate
"enable_dl" should be disabled	PHP	Vulnerability	cwe, owasp-a6, php-ini	Activate
"open_basedir" should limit file access	PHP	Vulnerability	cwe, owasp-a6, php-ini	Activate
"session.use_trans_sid" should not be enabled	PHP	Vulnerability	owasp-a6, php-ini	Activate
Session-management cookies should not be persistent	DEPRECATED	PHP	Vulnerability	php-ini

6 of 6 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

“ *pas de bouton «OK», «Confirmer», «Retour»!*
Maintenant on peut analyser le projet en regard du profile

”


20


III. Gate Qualité

créer un seuil de validité

1. ajouter une gate custom

- *par défaut* une gate est évaluée en face du **nouveau code**
- => code lié à la **MR Gitlab**
- sauf la première fois (code total)
- créer des conditions sur le code total

sonarqube  Projects Issues Rules Quality Profiles **Quality Gates** Administration

Quality Gates  [Create](#)

Sonar way **DEFAULT** BUILT-IN

Create Quality Gate

All fields marked with * are required

Name *






[Save](#) [Cancel](#)

2. "unlock editing"

- ajout de couverture code sur tout le code

Conditions ?
Add Condition

Conditions on New Code

Metric	Operator	Value	
Coverage	is less than	80.0%	 
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)	 

my gate

Rename Copy Set as Default Delete

Add Condition

☐ On New Code ☒ On Overall Code

Quality Gate fails when

Search for metrics...

- Complexity
- Cognitive Complexity
- Cyclomatic Complexity
- Coverage
- Condition Coverage
- Conditions to Cover
- Coverage
- Line Coverage
- Lines to Cover
- Skipped Unit Tests

Add Condition




Mail (Technical debt ratio is less than 5.0%)

Rel (No bugs)

Security Hotspots Reviewed is less than 100%


3. associer la gate <=> projet

Conditions on Overall Code

Metric	Operator	Value	
Coverage	is less than	60.0%	  

Projects

With Without All

 Search

☐

project
project

Permissions

Users with the global "Administer Quality Gates" permission and those listed below can manage this Quality Gate.

Grant permissions to a user or a group

étudier les métriques

- **paramètres**
- **definitions de métriques**
- **scope**

configurer le job sonar dans Gitlab

- utiliser l'image `sonarsource/sonar-scanner-cli:11`
- on doit « **neutraliser le ENTRYPOINT** » de cette image Docker

```
image:  
  name: sonarsource/sonar-scanner-cli:11  
  entrypoint: [ "" ]
```

“ *les autres configurations du job sont liées au langage utilisé !!!* ”