

SonarQube

Utilisation pour un projet en C++

Copyright © 2022, **Sébastien Dinot**

Licence Creative Common Attribution 4.0 (CC By 4.0)

Atelier C++ Toulire – 2022-09-03



Sommaire

- Besoin
- Outil et concepts
- Comprendre les indicateurs
- Greffons indispensables
- Mise en œuvre avec Gitlab CI

Besoin

- Mauvaises pratiques, complexité, erreurs de conception et de codage → Bogues, failles de sécurité, code difficile à maintenir
- Remède : la **qualimétrie** (mesure de la qualité du code) :
 - Définir les règles de codage et les pratiques à proscrire
 - Vérifier dans le code l'application des règles et l'absence de mauvaises pratiques
 - Produire des indicateurs guidant les actions correctives

Quand mesurer ?

- Autrefois, bilans qualité manuels et fastidieux, réalisés juste avant la livraison → Trop tard !
- Aujourd'hui, génération automatisée et à la demande de bilans qualité
- Mise en œuvre dans les pipelines d'intégration continue → Correction possible au fil de l'eau

SonarQube

- Outil qualimétrique développé par SonarSource
- Open Core : version libre (GNU LGPL v3.0) et version propriétaire bien plus riche
- Greffons propriétaires et communautaires
- Indicateurs quantitatifs et qualitatifs

Greffons indispensables

- Indispensables (avec la version libre) :
 - Sonarqube Community Branch (multi-branches)
 - SonarQube C++ Community (support C/C++)
- Indispensables avec SonarQube < 8.6
 - Sonar GitLab (intégration GitLab / SonarQube)
 - Sonar Auth GitLab (authentification via Gitlab)

Indicateurs quantitatifs

- Faits dénombrables : bogues, vulnérabilités, violations des règles de codage, occurrences de mauvaises pratiques, résultats et taux de couverture des tests
- Valeurs factuelles à prendre au pied de la lettre, mais criticité individuelle variable → Correction à prioriser

Indicateurs qualitatifs

- Estimations résultant d'abaques et de calculs
 - Dette technique → évalue l'effort de remédiation
 - Complexité du code → évalue la maintenabilité
- Valeurs arbitraires et contestables → tendance (évolution dans le temps) plus révélatrice que la valeur brute

Règles et profils qualité

- Une règle (rule) :
 - Un élément vérifiable par un outil
 - Une sévérité de la violation
- Profil qualité (**Quality Profile**)
 - Sélection de règles à vérifier parmi celles disponibles pour le langage considéré, prises en compte avec une sévérité éventuellement ajustée

Ajustements

- La base de règles peut être enrichie
- Modifications propres au profil qualité, valeurs par défaut inchangées
- Un profil qualité par langage à analyser doit être associé à chaque projet
- Import / export de profil possible

Grille de qualité

- La grille de qualité (**Quality Gate**) est le contrat qualité du projet
- Elle fixe un seuil ou un plafond à respecter pour les indicateurs sélectionnés
- Si les seuils ou plafonds sont respectés, le contrat est rempli

Qui mesure ?

- Historiquement, pour Java, SonarQube lui-même
- Autres langages : outils externes et spécifiques
 - Les outils externes procèdent aux analyses
 - Ils génèrent des rapports aux formats gérés par SonarQube
 - Le client **SonarScanner** les soumet à SonarQube
- SonarQube intègre, consolide et scénarise les résultats

Quels outils pour le C++ ?

- Greffon C++ Community
 - Outils libres : g++ (warnings), Clang Static Analyzer, Clang Tidy, Valgrind, Infer...
 - Propriétaires : PC-Lint, Visual Studio CG Checker
- Greffons propriétaires
 - Greffon C/C++ de SonarSource
 - Greffons fournis par des éditeurs (CppDepend...)

Difficultés de mise en œuvre

- Greffon multi-branches
 - Amorçage en dehors de la CI nécessaire
- Définition du Quality Profile et du Quality Gate
 - Règles à (dés)activer, seuils de déclenchement
- Introduction tardive → Stratégie de prise en compte progressive des règles

Exemples de mise en œuvre

- <https://sonar.orfeo-toolbox.org/>
 - Langage cible : C++
 - Greffons : Community Branch, Gitlab, Gitlab Auth, C/C++
- <https://sonar.orekit.org/>
 - Langage cible : Java
 - Greffons : Community Branch, Gitlab, Gitlab Auth, Checkstyle, FindBugs

Copyright © 2022 – **Sébastien Dinot**

<https://www.palabritudes.net/>

Cette présentation est mise à disposition selon les termes de la
Licence Creative Commons Attribution 4.0 International (CC By 4.0)

<http://creativecommons.org/licenses/by/4.0/>

