SonarQube Tutorial

SonarQube Tutorial comprises all details of this tool. I will start with the outline and then I will explain each topic one by one in detail. Let's get started!

SonarQube Tutorial Outline

We will look at requirements and prerequisites for SonarQube:

What is code quality?

What is SonarQube?

Why SonarQube?

How SonarQube works?

Sonar Structure & CI

SonarQube Features

Cyclomatic Complexity

Installation of SonarQube

Prerequisites

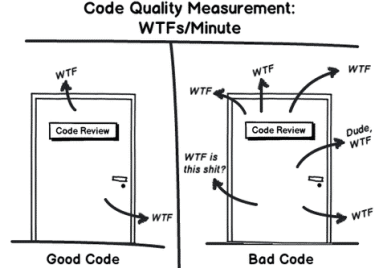
SonarQube

Java JDK

You can also check the prerequisites here.

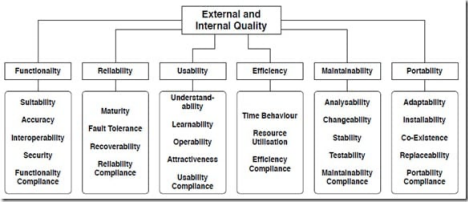
What is Code Quality?

I watched a presentation of Patroklos Papapetrou and I liked his description of code quality. He says that “Code quality is an indicator about how quickly developers can add business value to software system“.



Software Quality Characteristics: ISO/IEC 9126

In order to evaluate software, it is necessary to select relevant quality characteristics. ISO/IEC 9126 defines a quality model which is applicable to every kind of software. It defines six product quality characteristics.



What is SonarQube?

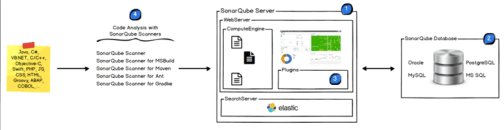
Sonar is an open-source software quality platform. SonarQube saves

the calculated measures in a database and showcases them in a rich web based dashboard. Provides trends and leading indicators.

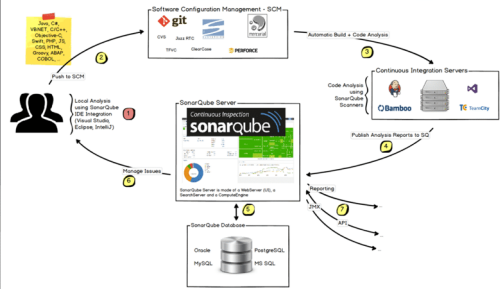
How Sonar Works?

Sonar uses various static & dynamic code analysis tools such as Checkstyle, PMD, FindBugs, FxCop, Gendarme, and many more to extract software metrics, which then can be used to improve software quality. Provides lots of plugins.

SonarQube Structure



SonarQube CI



SonarQube Features

Supports languages: Java, C/C++, Objective-C, C#, PHP, Flex, Groovy, JavaScript, Python, PL/SQL, COBOL, etc. (note that some of them are commercial)

Can also be used in Android development.

Offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, potential bugs, comments, design, and architecture.

Records metrics history and provides evolution graphs (“time machine”) and differential views.

Provides fully automated analyses: integrates with Maven, Ant, Gradle, and continuous integration tools (Atlassian Bamboo, Jenkins, Hudson, etc.).

Integrates with the Eclipse development environment

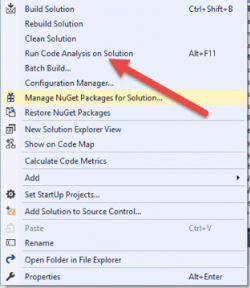
Integrates with external tools: JIRA, Mantis, LDAP, Fortify, etc. Is expandable with the use of plugins.

Implements the SQALE methodology to compute technical debt. (wiki)

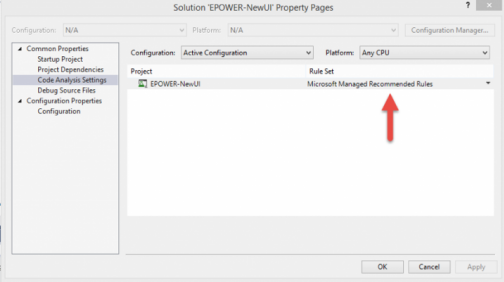
What is Static Code Analysis?

Computer code that is performed without actually executing programs. Source code will be checked for compliance with a predefined set of rules or best practices set by the organization.

Visual Studio has a built-in tool or this you can follow: In Solution Explorer, right-click the project, and then click Properties.



We can configure the rules or analyze



Technical debt is caused by the 7 deadly sins of the developer:

1. Duplications: SonarQube has a copy/paste detection engine to find duplications

2. Bad distribution of complexity: *Cyclomatic complexity* [wiki] (or McCabe metric)

3. Spaghetti Design

Spaghetti code is a **pejorative phrase for unstructured and difficult-to-maintain source code**. Spaghetti code can be caused by several factors, such as volatile project requirements, lack of programming style rules, and software engineers with insufficient ability or experience.

4. Lack of unit tests

5. No coding standards

6. Potential bugs

7. Not enough or too many comments or incorrect comments

**What is SonarQube?**

SonarQube is an open-source platform developed by SonarSource for continuous inspection of code quality. Sonar does static code analysis, which provides a detailed report of bugs, code smells, vulnerabilities, code duplications.

It supports 25+ major programming languages through built-in rulesets and can also be extended with various plugins.

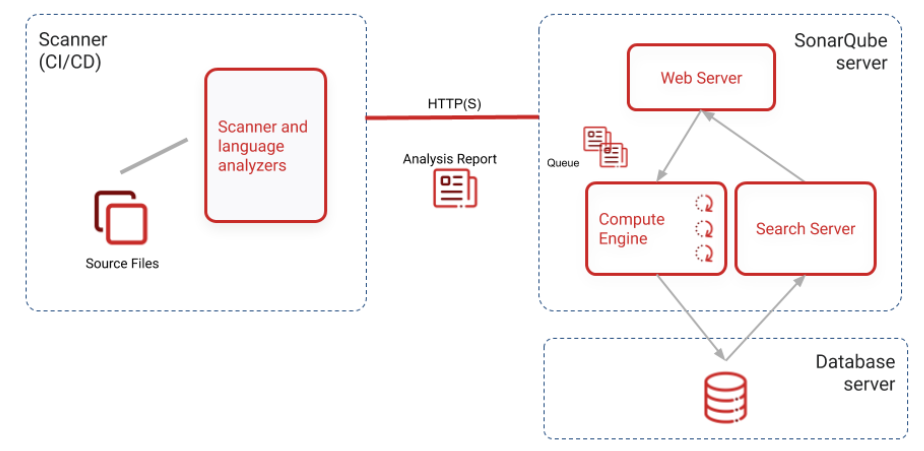
**Benefits of SonarQube**

1. Sustainability - Reduces complexity, possible vulnerabilities, and code duplications, optimising the life of applications.
2. Increase productivity - Reduces the scale, cost of maintenance, and risk of the application; as such, it removes the need to spend more time changing the code
3. Quality code - Code quality control is an inseparable part of the process of software development.
4. Detect Errors - Detects errors in the code and alerts developers to fix them automatically before submitting them for output.
5. Increase consistency - Determines where the code criteria are breached and enhances the quality
6. Business scaling - No restriction on the number of projects to be evaluated
7. Enhance developer skills - Regular feedback on quality problems helps developers to improve their coding skills

**Instance components**

A SonarQube instance comprises three components:

1. The SonarQube server running the following processes:
   * a web server that serves the SonarQube user interface.
   * a search server based on Elasticsearch.
   * the compute engine in charge of processing code analysis reports and saving them in the SonarQube database.
2. The database to store the following:
   * Metrics and issues for code quality and security generated during code scans.
   * The SonarQube instance configuration.
3. One or more scanners running on your build or continuous integration servers to analyze projects.



Note: Install server with atleast 2 GB of RAM.

$ docker run -d --name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest

Installing SonarQube

Download SonarQube 5.3 (version in 2016) and MSBuild SonarQube Runner from the SonarQube from downloads.

Important Note: In 2021 August, the new versions are listed as follows: SonarQube(9.0.1): https://www.sonarqube.org/downloads/

SonarScanner for .NET(5.2):

https://docs.sonarqube.org/latest/analysis/scan/sonarscanner-for msbuild/

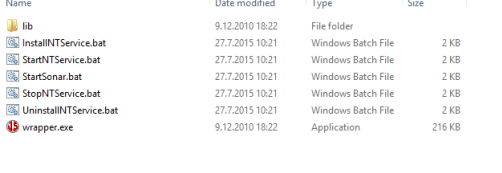
We also need Java JDK 11 so you can visit and download it from here.

*From now on, I will explain the installation for SonarQube 5.3 but you can apply it for the new SonarQube versions.*

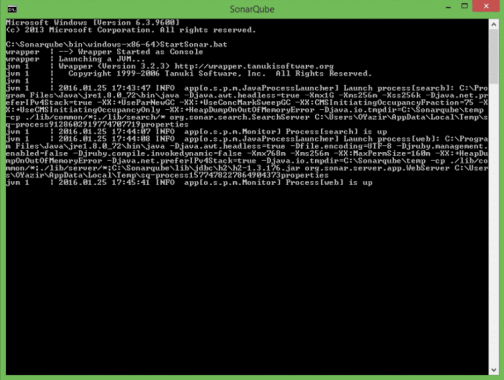
Right-click on sonarqube-5.3.zip, select Properties and then click on the Unblock button.

Unzip SonarQube-x.x.zip on to a folder, for example, use C:\SonarQube\SonarQube-5.3

You should see the files inside the extracted folder.

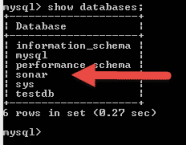


Execute **c:\sonar-5.3\bin\windows-x86-64\StartSonar.bat** file using command-line.The expected output should look like

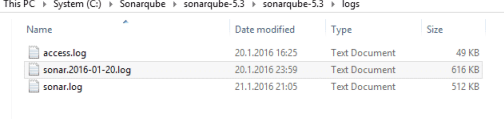
*Tip: Can’t load AMD 64-bit .dll on a IA 32-bit platform Error message says you need to install 64 bit java*

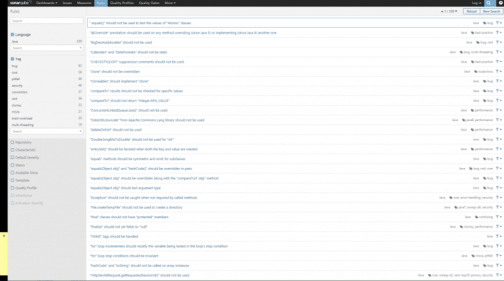
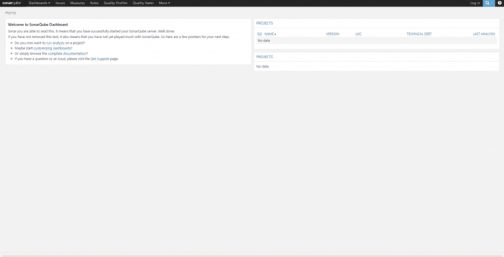
Database Integration

I use MySQL as the database. It needs to create a new schema and a sonar user and I give the user permissions to create, update and delete objects in the schema.

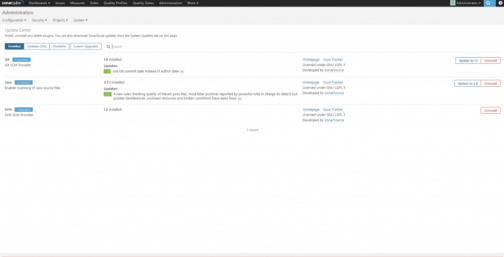


Troubleshooting: for log checking log files located under sonarqube/logs

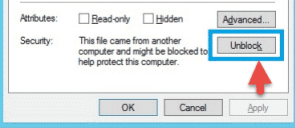
You can login using default user / password = admin / admin



Plugin installation: Update Center (Settings | System | Update Center), and installed the SonarQube C# Plug-in.



Now we need to install MS Build QubeRunner, you can download it here. First, need to be unblocked.



Now we need some modifications on SonarQube.Analysis.xml file.

sonar.jdbc.url

sonar.jdbc.username

Sonar.jdbc.password



Installing the mysql server:

https://phoenixnap.com/kb/install-mysql-on-windows