Sonarqube

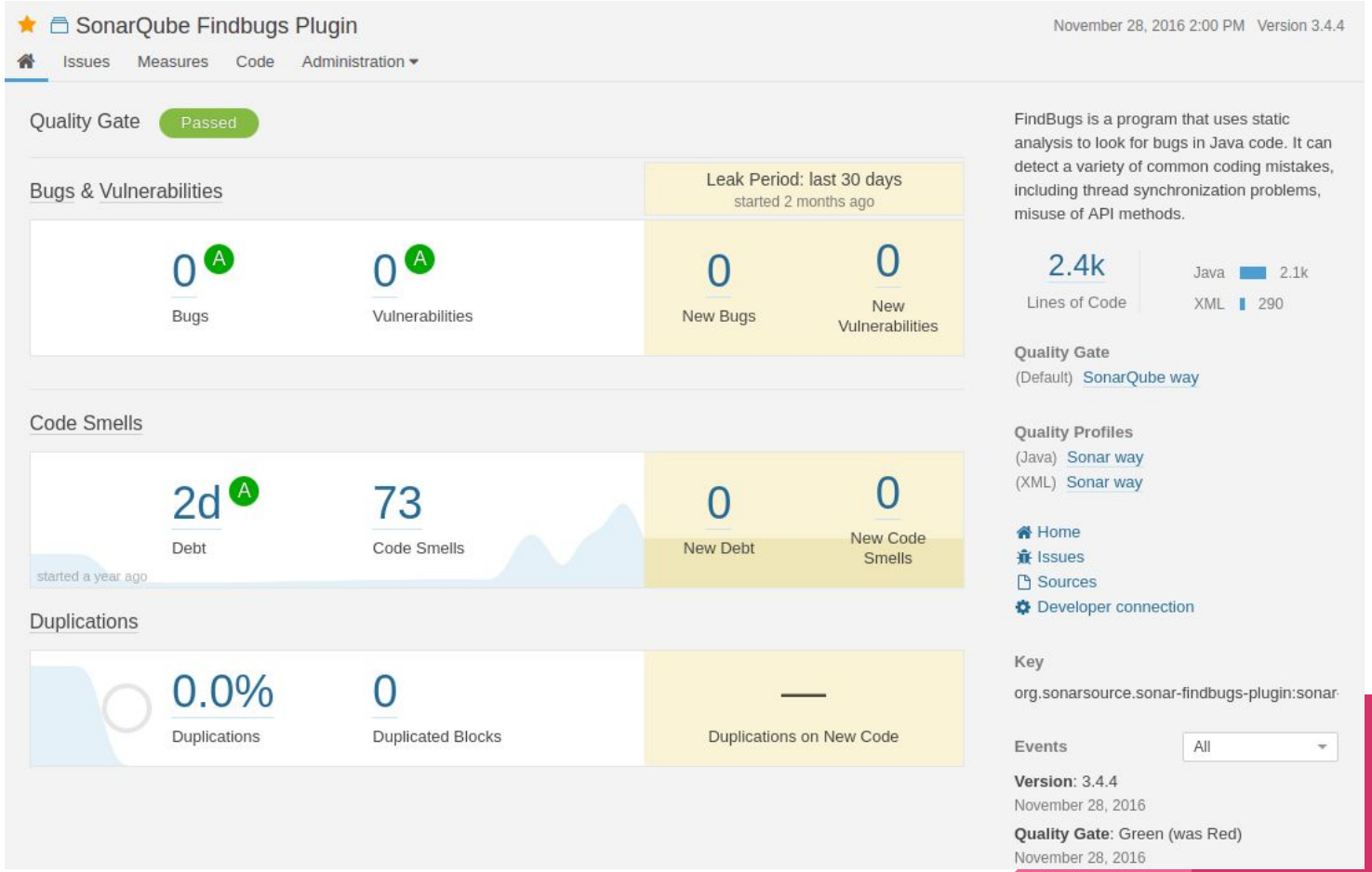
Sonarqube

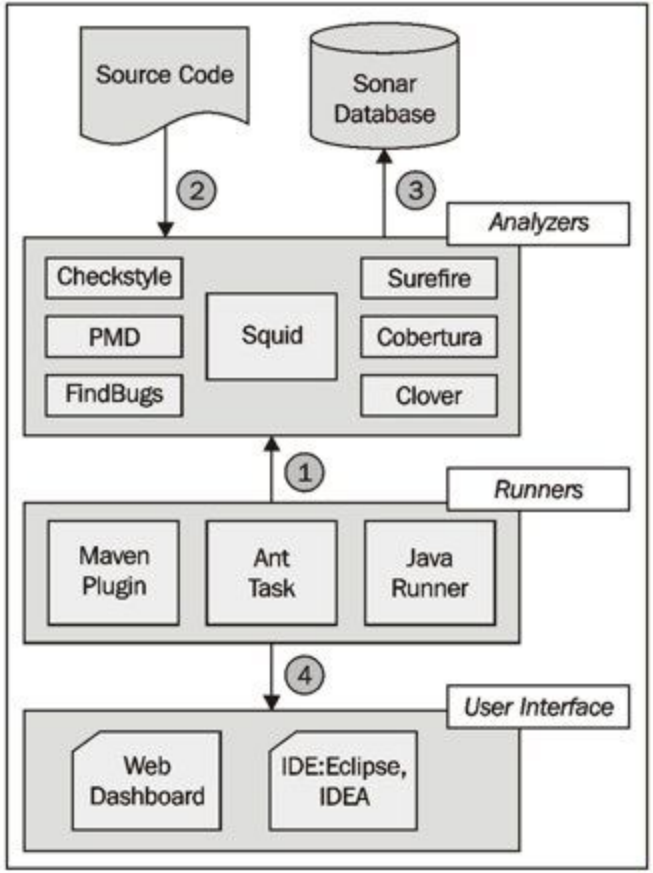
- Previously known as Sonar
- Open source platform for Continuous Inspection of code quality.
- Written in java and supported for 25+ languages such as Java, C/C++, C#, PHP etc, it is also used for Android Development
- Helps for various tasks and provide reports on duplicated code, coding standards, unit tests, code coverage, complex code, potential bugs, comments and design and architecture.
- Internally using PMD,Findbugs,CheckStyle etc. Can add additionally plugins according to your requirement

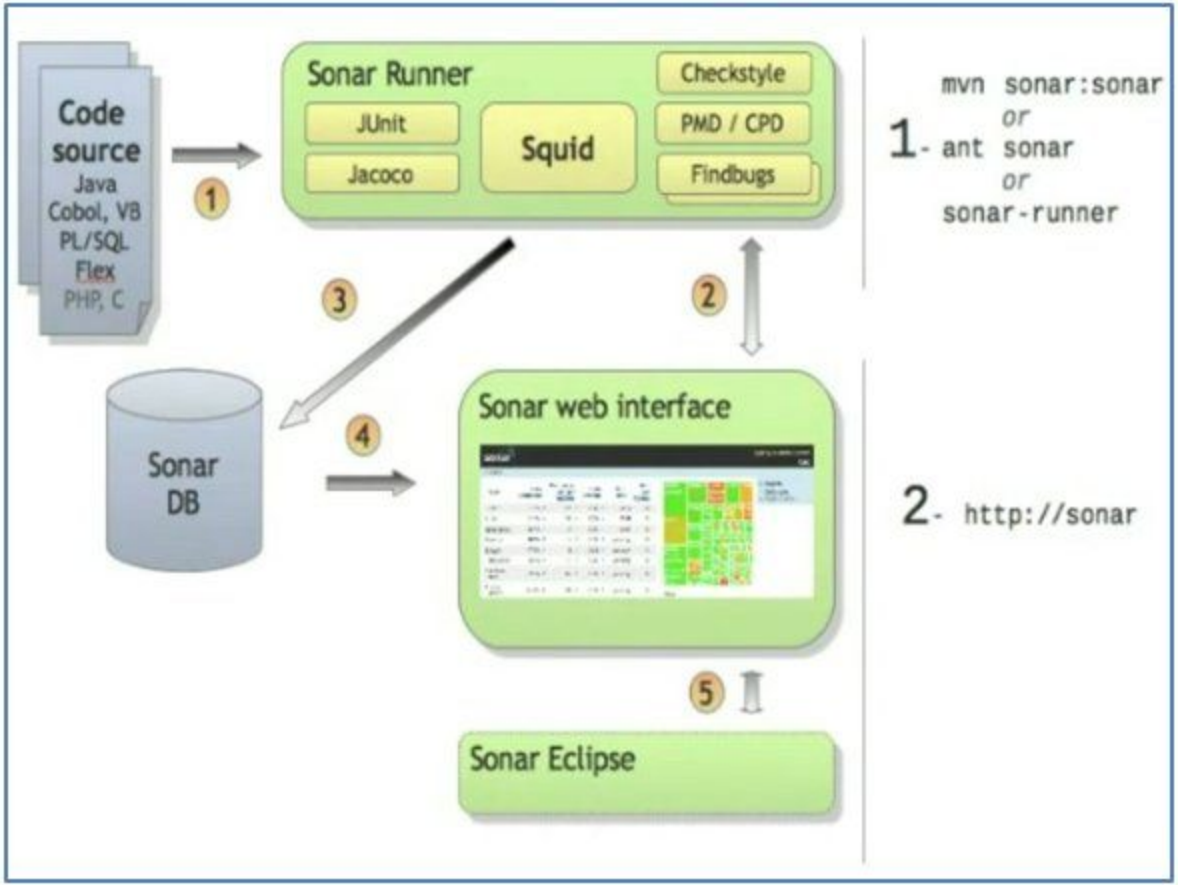
Install and start Sonarqube

Installing from a zip file

1. Download the SonarQube Community Edition.
2. Unzip it, let's say in *C:\sonarqube* or */opt/sonarqube*.
3. **Start the SonarQube Server:**
   a. Pre-requisite : Java 11 + version
   b. On Windows, execute: C:\sonarqube\bin\windows-x86-xx\StartSonar.bat
   c. On other operating systems, as a non-root user execute: /opt/sonarqube/bin/[OS]/sonar.sh console
   d. If your instance fails to start, check your logs to find the cause.
   e. Log in to http://localhost:9000 with System Administrator credentials (login=admin, password=admin).
   f. Click the **Create new project** button to analyze your first project.

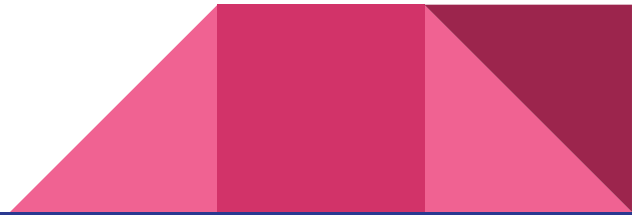

SonarQube Findbugs Plugin
November 28, 2016 2:00 PM Version 3.4.4
Issues Measures Code Administration
Quality Gate Passed
Bugs & Vulnerabilities
Leak Period: last 30 days
started 2 months ago
0 A
Bugs
0 A
Vulnerabilities
0
New Bugs
0
New Vulnerabilities
Code Smells
2d A
Debt
73
Code Smells
started a year ago
0
New Debt
0
New Code Smells
Duplications
0.0%
Duplications
0
Duplicated Blocks
—
Duplications on New Code
FindBugs is a program that uses static analysis to look for bugs in Java code. It can detect a variety of common coding mistakes, including thread synchronization problems, misuse of API methods.
2.4k
Lines of Code
Java 2.1k
XML 290
Quality Gate
(Default) SonarQube way
Quality Profiles
(Java) Sonar way
(XML) Sonar way
Home
Issues
Sources
Developer connection
Key
org.sonarsource.sonar-findbugs-plugin:sonar
Events
All
Version: 3.4.4
November 28, 2016
Quality Gate: Green (was Red)
November 28, 2016


Source Code
Sonar Database
2
3
Analyzers
Checkstyle
PMD
FindBugs
Squid
Surefire
Cobertura
Clover
1
Runners
Maven Plugin
Ant Task
Java Runner
4
User Interface
Web Dashboard
IDE:Eclipse, IDEA


Code source
Java
Cobol, VB
PL/SQL
Flex
PHP, C
1
Sonar Runner
JUnit
Jacoco
Squid
Checkstyle
PMD / CPD
Findbugs
3
2
Sonar DB
4
Sonar web interface
5
Sonar Eclipse
1- mvn sonar:sonar
or
ant sonar
or
sonar-runner
2- http://sonar

Benefits of SonarQube to Devops

1. To make sure software was built the right way.
2. Can integrate SonarQube with build tools like ant, gradle , maven
3. Enforce a set of quality criteria, which ensures that organizations deliver better software.
4. SonarQube reports for duplicate code, unit testing, code coverage, code complexity historical



Quality Gate

Quality Gate : A quality gate is the best way to enforce a quality policy in your organization

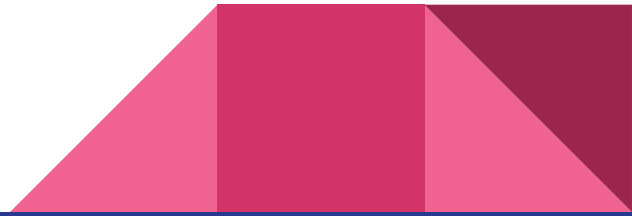
The quality gate "Sonar way" is provided by SonarSource, activated by default and considered as built-in and so read-only. It represents our view of the best way to implement the Fixing the Water Leak concept.

Each Quality Gate condition is a combination of:

- measure
- comparison operator
- error value

Quality Profile

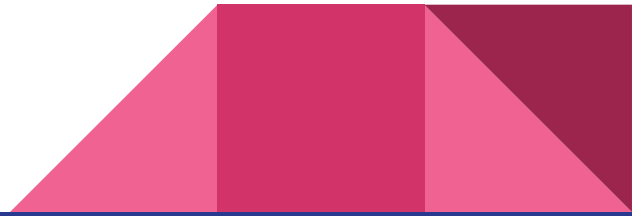
- Quality Profiles are a core component of SonarCloud, since they are where you define sets of Rules that when violated should raise issues on your codebase . Quality Profiles are defined for individual languages.
- The Sonar way Quality Profiles are a good starting-point as you begin analyzing code, and they start out as the default Quality Profiles for each language.
- Default Quality Profiles are not editable, so you won't be able to customize the Sonar way to your needs
- The Sonar way becomes a baseline against which you can track your own Quality Profiles



Concepts and definitions

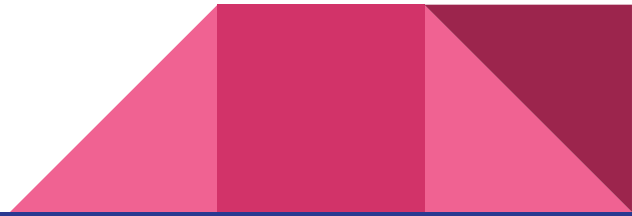
Bug:
An issue that represents something wrong in the code. If this has not broken yet, it will, and probably at the worst possible moment.

Code Smell:
A maintainability-related issue in the code. Leaving it as-is means that at best maintainers will have a harder time than they should making changes to the code. At worst, they'll be so confused by the state of the code that they'll introduce additional errors as they make changes.



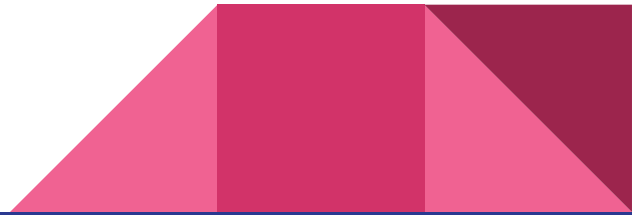
Issue:
When a piece of code does not comply with a rule, an issue is logged on the snapshot. An issue can be logged on a source file or a unit test file. There are 3 types of issue: Bugs, Code Smells and Vulnerabilities

Measure:
The value of a metric for a given file or project at a given time. For example, 125 lines of code on class MyClass or density of duplicated lines of 30.5% on project myProject



Vulnerability
A security-related issue which represents a backdoor for attackers.

Metric:
A type of measurement. Metrics can have varying values, or measures, over time. *Examples:* number of lines of code, complexity, etc. A metric may be either *qualitative* (gives a quality indication on the component, E.G. density of duplicated lines, line coverage by tests, etc.) or *quantitative* (does not give a quality indication on the component, E.G. number of lines of code, complexity, etc.)



Thank You