

VISUALIZING CODE QUALITY WITH SonarQube

Philipp Salvisberg
22nd September 2022

2 WELCOME



PHILIPP SALVISBERG SENIOR PRINCIPAL CONSULTANT

- Database centric development
- Model Driven Software Development
- Author of free SQL Developer Extensions
PL/SQL Unwrapper, db* CODECOP, utPLSQL,
plscope-utils, oddgen and Bitemp Remodeler



INTRODUCTION

4 WHAT IS SonarQube?

- Automatic code review tool
- Continuous code inspection for various programming languages
- Based on files

Source: <https://docs.sonarqube.org/latest/>

5 SonarQube EDITIONS

Community

EDITION

Used and loved by 200,000+ companies

FREE & OPEN SOURCE

 Download for free

All the following features:

- ✓ Static code analysis for 18 languages
Java, C#, JavaScript, TypeScript, CloudFormation, Terraform, Kotlin, Ruby, Go, Scala, Flex, Python, PHP, HTML, CSS, XML and VB.NET and YML in 9.6.2
- ✓ Detect Bugs & Vulnerabilities
- ✓ Review Security Hotspots
- ✓ Track Code Smells & fix your Technical Debt
- ✓ Code Quality Metrics & History
- ✓ CI/CD integration
- ✓ Extensible, with 50+ community plugins

Developer

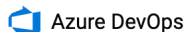
EDITION

Built for developers by developers

 Download

Community Edition plus:

- ✓ C, C++, Obj-C, Swift, ABAP, T-SQL, PL/SQL support
- ✓ Detection of Injection Flaws in Java, C#, PHP, Python, JavaScript, TypeScript
- ✓ Analysis of feature and maintenance branches
- ✓ Pull Request decoration for:



Enterprise

EDITION

Designed to meet Enterprise Requirements

 Download

Developer Edition plus:

- ✓ Portfolio Management & PDF Executive Reports
- ✓ Project PDF reports
- ✓ Security Reports
- ✓ Project Transfer
- ✓ Parallel processing of analysis reports
- ✓ Support for Apex, COBOL, PL/I, RPG, VB6

Data Center

EDITION

Designed for High Availability

 Download

Enterprise Edition plus:

- ✓ Component redundancy
- ✓ Data resiliency
- ✓ Horizontal Scalability

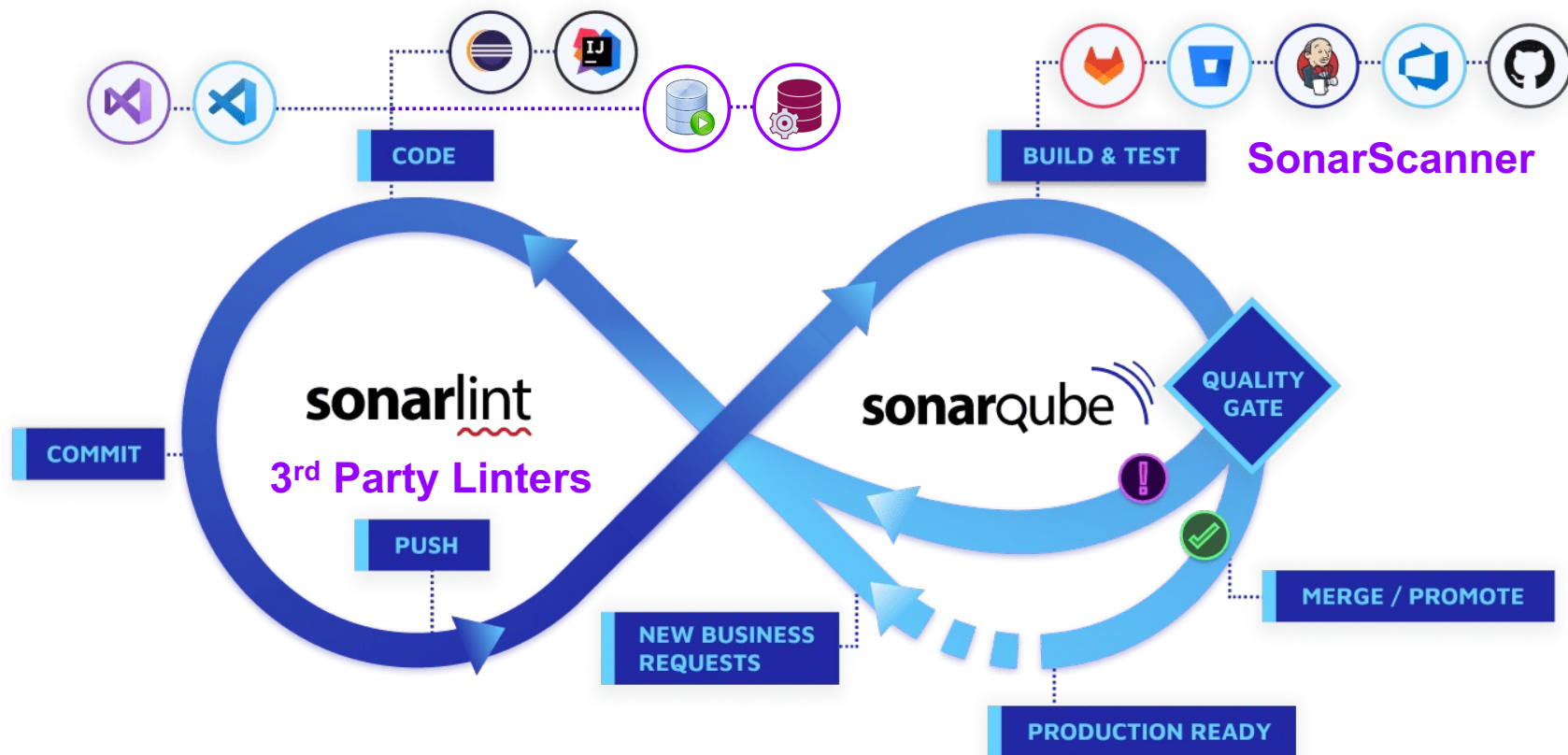
Source: <https://www.sonarqube.org/downloads/>

6 SonarQube LICENSE COSTS PER YEAR

Max. Lines of Code	Developer Edition	Enterprise Edition	Data Center Edition	SonarCloud (~Dev.Ed.)
100'000	\$150	-	-	€120
250'000	\$1'200	-	-	€900
500'000	\$2'400	-	-	€1'800
1'000'000	\$4'000	\$20'000	-	€3'000
2'000'000	\$8'000	-	-	€6'000
5'000'000	\$23'000	\$32'500	-	€18'000
10'000'000	\$48'000	\$50'000	-	€43'200
20'000'000	\$65'000	\$65'000	\$130'000	€60'000
30'000'000	-	\$100'000	-	-
50'000'000	-	\$120'000	\$200'000	-
75'000'000	-	\$165'000	\$260'000	-
100'000'000	-	\$240'000	\$325'000	-
250'000'000	-	-	\$520'000	-
500'000'000	-	-	\$780'000	-
1'000'000'000	-	-	\$1'300'000	-
>1'000'000'000	-	-	Upon request	-

Source: <https://www.sonarsource.com/plans-and-pricing/> and <https://sonarcloud.io/pricing>

7 DEVELOPING WITH SonarQube



Source: <https://docs.sonarqube.org/latest/>

8 SonarQube LANGUAGE PLUGIN SETTING & RESULTS

Languages

PL/SQL

General

File Suffixes

List of suffixes for files to analyze.
Key: sonar.plsql.file.suffixes

sql

tab

pkb

(default)

Ignore Header Comments

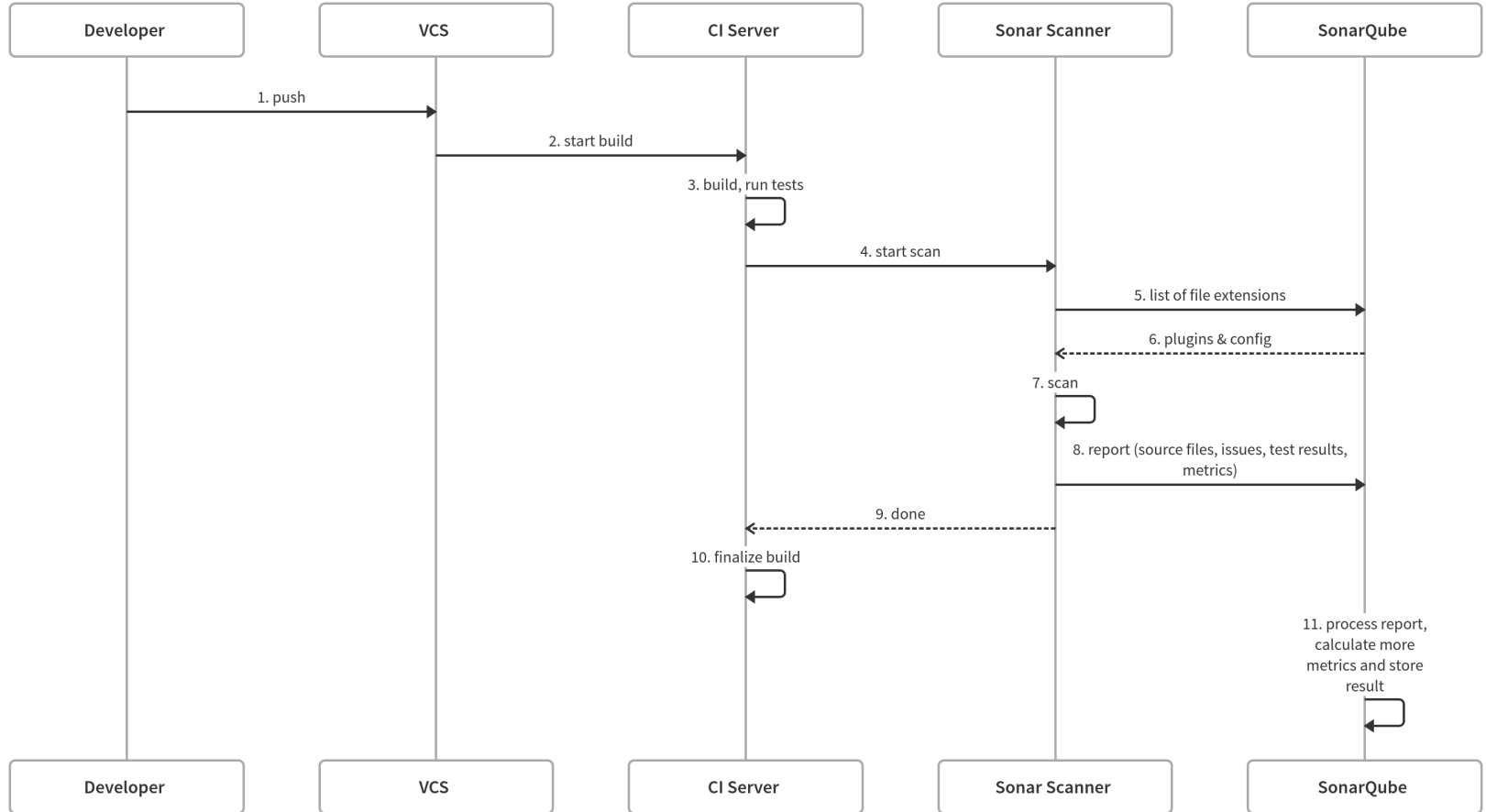
If set to "true", the file headers (that are usually the same on each file: licensing information for example) are not considered as comments. Thus metrics such as "Comment lines" do not get incremented. If set to "false", those file headers are considered as comments and metrics such as "Comment lines" get incremented.
Key: sonar.plsql.ignoreHeaderComments

(default)

- Rules
- Issues
- Core metrics
(non commenting lines, comment lines, statements, functions, complexity)
- Custom metrics
(blank lines, max. cyclomatic complexity, max. Halstead volume, bytes, min. maintainability index, total commands)
- Tokens for copy & paste detection
- Tokens for syntax highlighting
- Executable lines for code coverage metrics

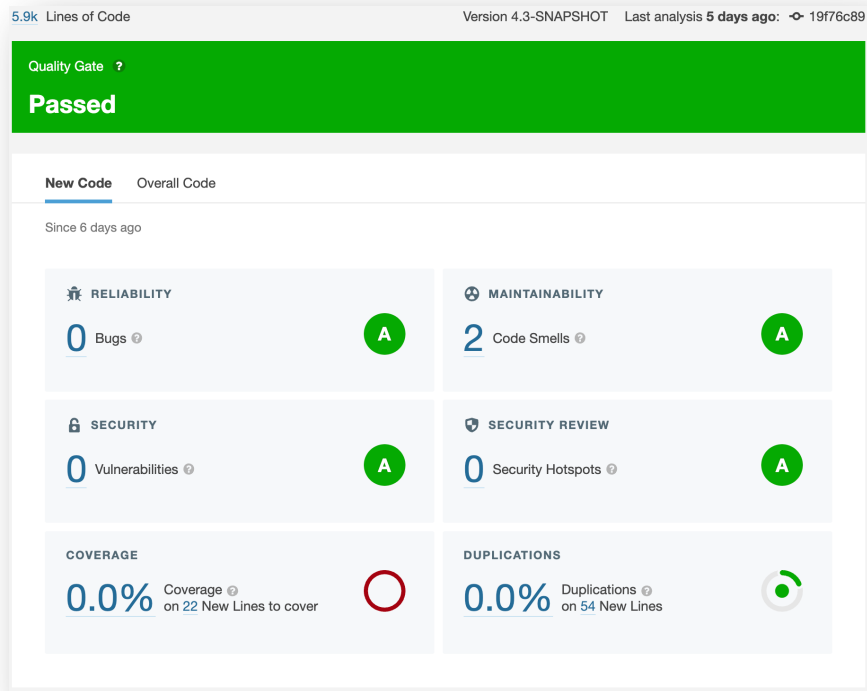
9

CI PROCESS BEHIND THE SCENES (SIMPLIFIED)

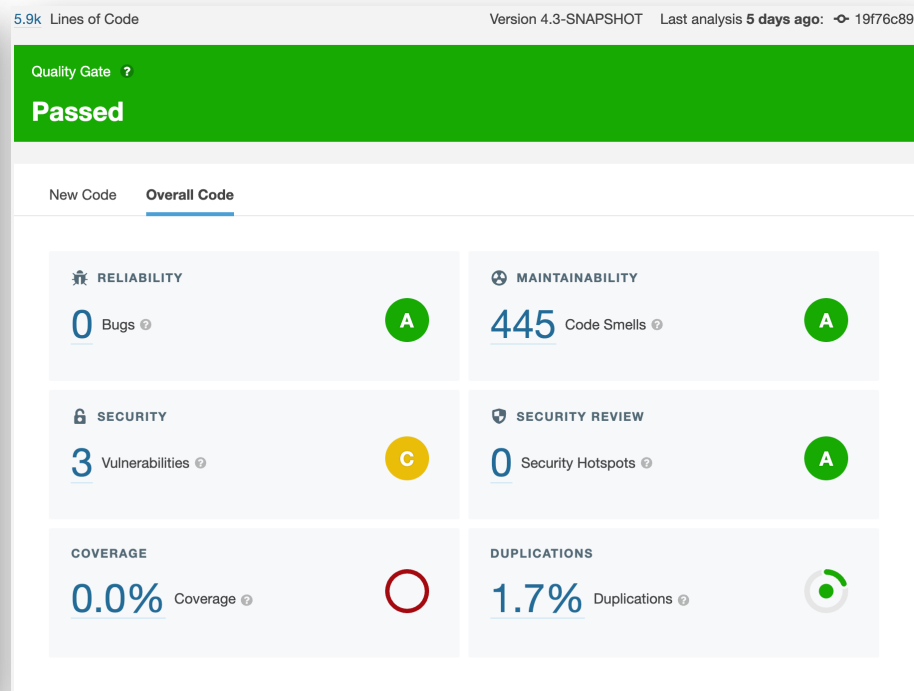


10 SonarQube / SonarCloud DASHBOARD

NEW CODE



OVERALL CODE



Source: <https://sonarcloud.io/summary/overall?id=Trivadis-plsql-and-sql-coding-guidelines>

11 NEW CODE?

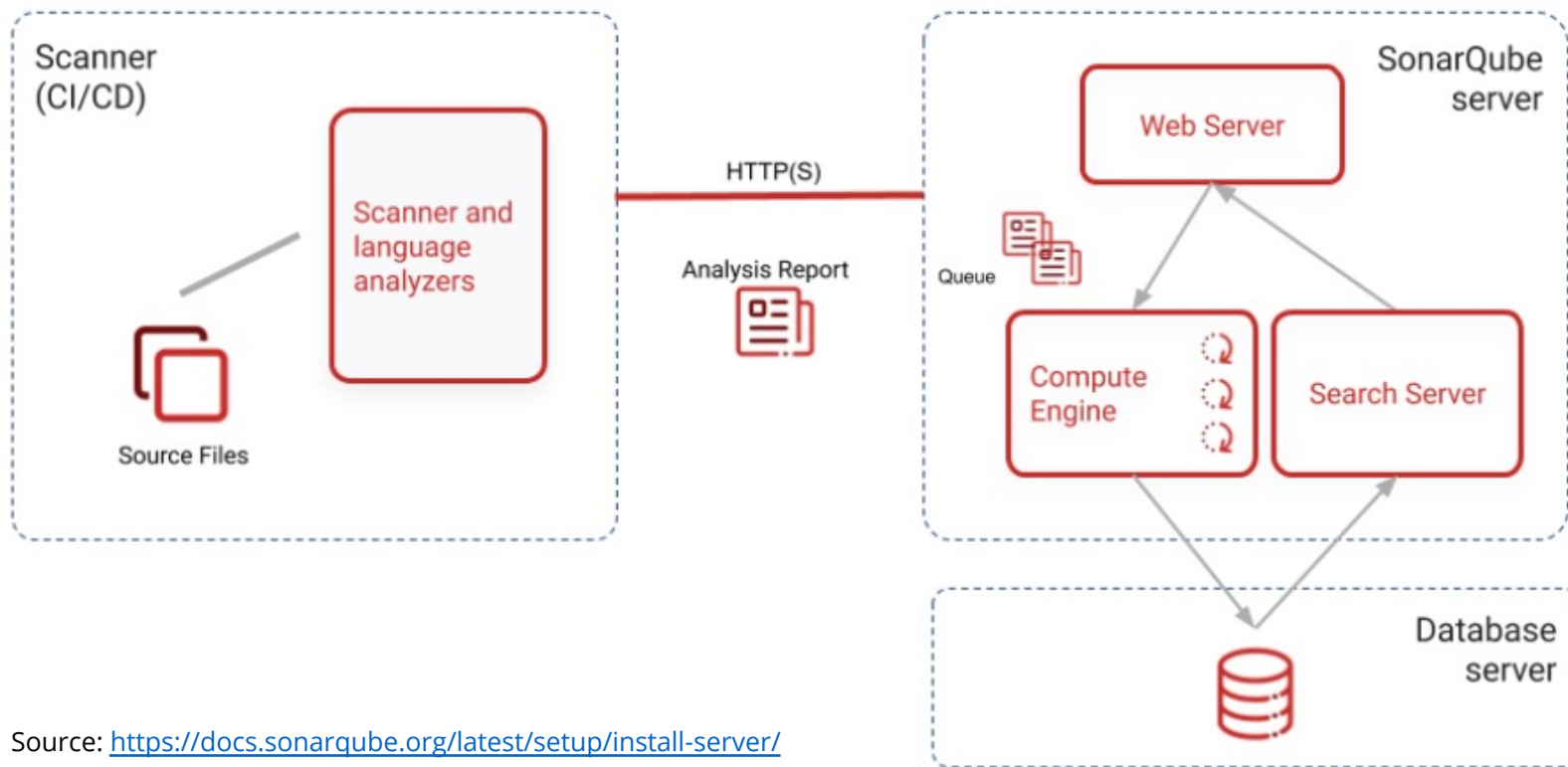
New Code Period for main

☐ Previous version The New Code will be based on the analysis following the previous version.	☐ Number of days A floating window set to a specific number of days used to define New Code.	☐ Specific analysis Choose an analysis as the baseline for the New Code.	☐ Reference branch Choose a branch as the reference for the New Code.
--	---	---	--

- Definition on global/project/branch level
- Override per analysis with `sonar.newCode.referenceBranch`
- New lines highlighted in code
- Metrics, issues based on new code
- Quality gate based on new code
 - Branches
 - Pull Requests
 - Use to prohibit merge
- Low entry barrier for legacy code

INSTALLATION

13 ARCHITECTURE



Source: <https://docs.sonarqube.org/latest/setup/install-server/>

14 SERVER

- Download from <https://www.sonarqube.org/downloads/>
- Extract ZIP File in a folder of your choice
- Open a terminal window, Navigate to the bin directory of your OS
- Start SonarQube with "sonar.sh console"
- Wait until message "SonarQube is operational" is shown
- Login as "admin" and password "admin" at <http://localhost:9000>
- Configure details in conf/sonar.properties

```
2022.09.07 14:26:41 WARN app[][startup] #####
2022.09.07 14:26:41 WARN app[][startup] Default Administrator credentials are still being used. Make sure to change the password or deactivate the account.
2022.09.07 14:26:41 WARN app[][startup] #####
2022.09.07 14:26:41 INFO web[][o.s.s.p.Platform] Web Server is operational
2022.09.07 14:26:41 WARN ce[][o.s.db.dialect.H2] H2 database should be used for evaluation purpose only.
2022.09.07 14:26:44 INFO ce[][o.s.s.p.ServerFileSystemImpl] SonarQube home: C:\app\sonarqube-9.6.1.59531
2022.09.07 14:26:45 INFO ce[][o.s.c.c.CePluginRepository] Load plugins
2022.09.07 14:26:47 INFO ce[][o.s.c.c.ComputeEngineContainerImpl] Running Community edition
2022.09.07 14:26:47 INFO ce[][o.s.ce.app.CeServer] Compute Engine is started
2022.09.07 14:26:47 INFO app[][o.s.a.SchedulerImpl] Process[ce] is up
2022.09.07 14:26:47 INFO app[][o.s.a.SchedulerImpl] SonarQube is operational
```

15 PLUGINS



VIA MARKETPLACE

- For non-competing, open-sourced plugins
- Only in Community Edition
- <http://localhost:9000/admin/marketplace>
- Restart SonarQube server
- Configure plugin



MANUALLY

- Copy plugin .jar file to extensions/plugins directory
- Restart SonarQube server
- Configure plugin
- PL/SQL plugins for all SonarQube editions:
 - <https://github.com/felipebz/zpa/releases>
 - <https://github.com/Trivadis/plsql-cop-sonar/releases>
 - <https://github.com/Trivadis/plsql-cop-validators/releases>
 - <https://github.com/mc1arke/sonarqube-community-branch-plugin/releases>

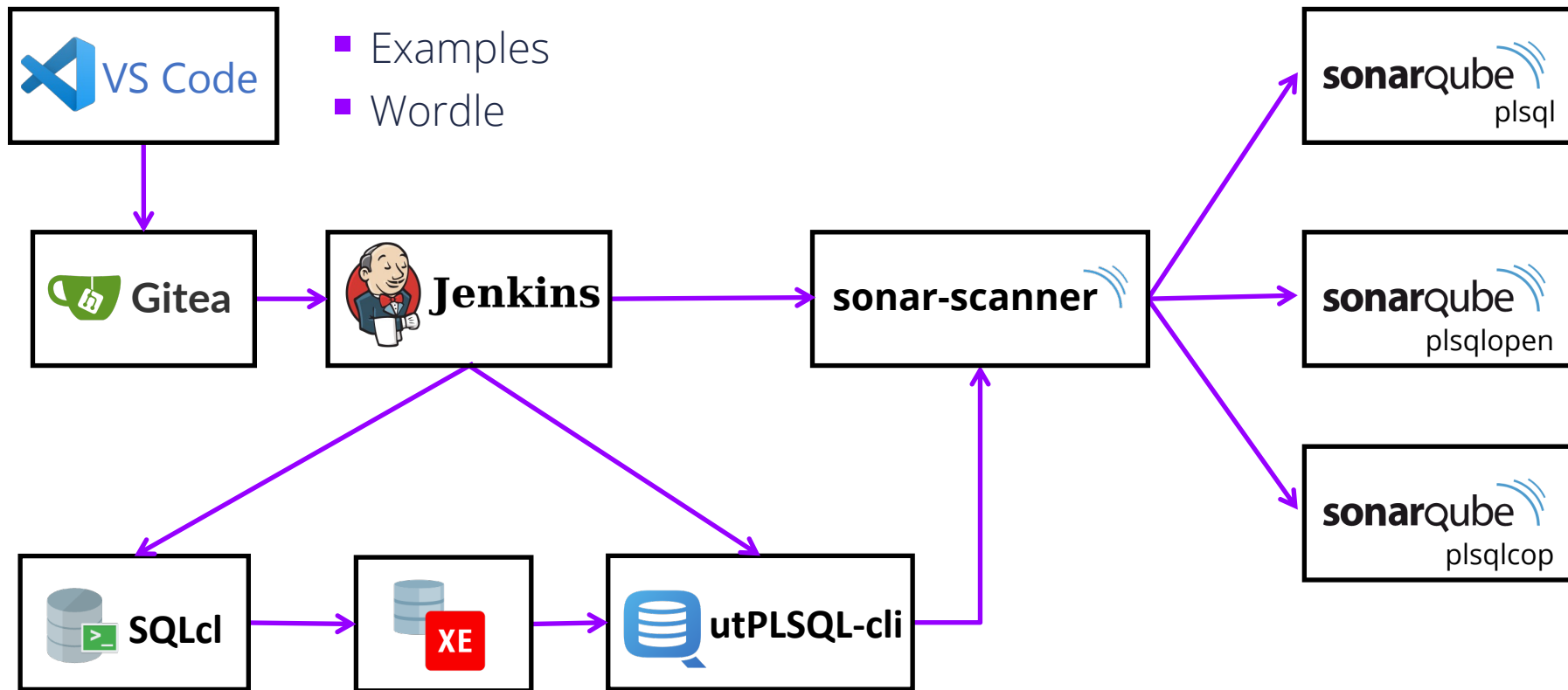
16 SCANNER

- Download from <https://docs.sonarqube.org/latest/analysis/scan/sonarscanner/>
- Extract ZIP File in a folder of your choice
- Add bin folder to your path
- Configure sonar-project.properties in the root of your project
see <https://docs.sonarqube.org/latest/analysis/analysis-parameters/>

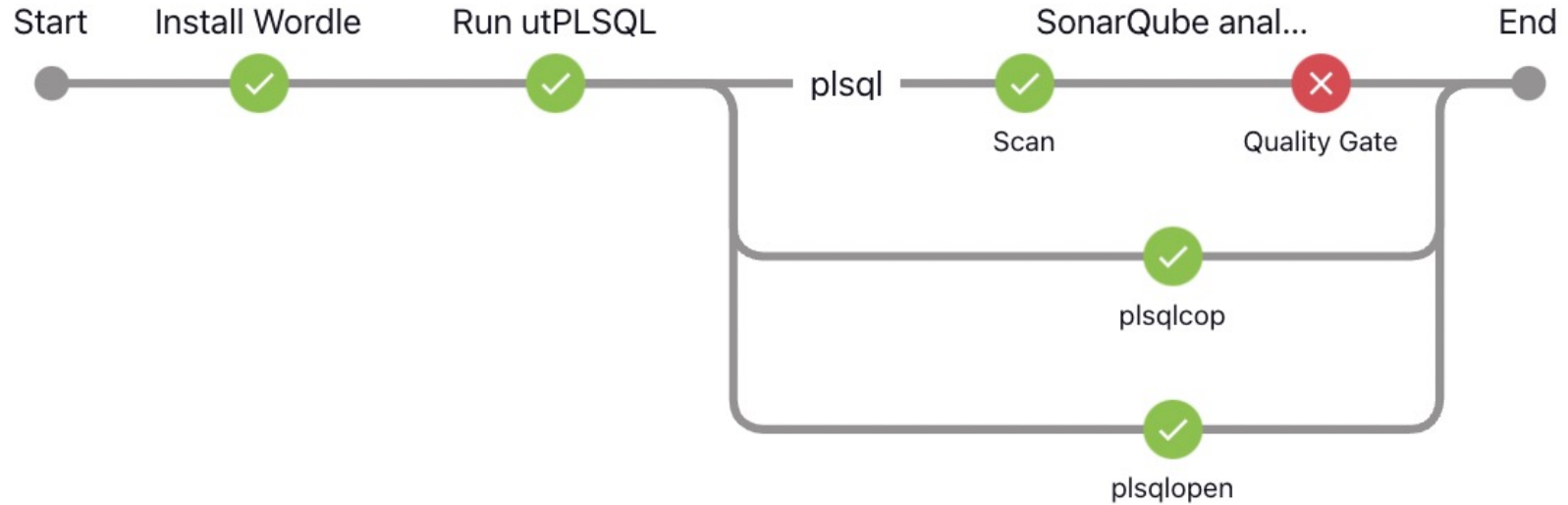
```
$ sonar-scanner --help
INFO:
INFO: usage: sonar-scanner [options]
INFO:
INFO: Options:
INFO:  -D,--define <arg>      Define property
INFO:  -h,--help              Display help information
INFO:  -v,--version            Display version information
INFO:  -X,--debug              Produce execution debug output
$
```


DEMO

18 DEMO SETUP



19 PULL REQUEST – JENKINS PIPELINE



20 PULL REQUEST – QUALITY GATE STATUS "FAILED"

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration ? Search for projects... A

Wordle 6 – feature/number-of-games for merge into main from feature/number-of-games September 15, 2022 at 1:00 PM

Overview Issues Security Hotspots Measures Code **Failed**

QUALITY GATE STATUS Conditions on New Code **Failed**

FAILED CONDITIONS 0.0% Coverage on New Code is less than 80.0%

MEASURES

0 New Bugs	Reliability A
0 New Vulnerabilities	Security A
0 New Security Hotspots	Security Review A
1 New Code Smells	Maintainability A
0.0% Coverage on 2 New Lines to cover	94.4% Estimated after merge
0.0% Duplications on 40 New Lines	0.0% Estimated after merge

21 UNCOVERED LINES ON NEW CODE

The screenshot displays the SonarQube web interface for a project named 'Wordle'. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, Quality Gates, and Administration. A search bar is present on the right. The main header shows the project name 'Wordle', a star icon, a branch '6 - feature/number-of-games', and a merge status 'for merge into main from feature/number-of-games'. The date and time 'September 15, 2022 at 1:00 PM' are also shown. Below the header, there are tabs for Overview, Issues, Security Hotspots, Measures, and Code. A red 'Failed' button is visible in the top right corner of the main content area.

The left sidebar contains a 'Project Overview' section with various metrics:

- Reliability
- Security
- Security Review
- Maintainability
- Coverage: **COVERAGE ON NEW CO...**
 - On new code
 - Coverage: 0.0%
 - Lines to Cover: 2
 - Uncovered Lines: 2
 - Line Coverage: 0.0%
 - Conditions to Cover: 0
 - Uncovered Conditions: 0
 - Duplications
 - Size
 - Issues

Wordle / main/package / wordle.pkb

```
67 phili...
68
69
70 phili...
71 phili...
72
73
74
75 phili...
76 phili...
77
78
79
80
81
82
83
84
85
86
87
88
89 phili...
90
91
92
93
94
95
96
```

```
-- -----
-- set_hard_mode (public)
-- -----
procedure set_hard_mode(in_hard_mode in boolean default true) is
begin
    g_hard_mode := in_hard_mode;
end set_hard_mode;

-- -----
-- number_of_games (public)
-- -----
function number_of_games(in_game_date in date default trunc(sysdate)) return integer is
    l_number_of_games integer;
begin
    select count(*)
    into l_number_of_games
    from words
    where game_date >= trunc(in_game_date);
    return l_number_of_games;
end number_of_games;

-- -----
-- bulkplay (public)
-- -----
function bulkplay(
    in_from_game_id in integer default null,
    in_to_game_id in integer default null
) return xmltype is
    t_games game_ct := game_ct();
```

22 TEST FOR FULL CODE COVERAGE

The screenshot displays the SonarQube web interface. At the top, the navigation bar includes 'sonarqube' logo, 'Projects', 'Issues', 'Rules', 'Quality Profiles', 'Quality Gates', and 'Administration'. A search bar on the right says 'Search for projects...' with a magnifying glass icon. A green badge with the letter 'A' is in the top right corner.

Below the navigation bar, the project path is 'Wordle' with a star icon, followed by a dropdown menu showing '6 - feature/number-of-games' and a note 'for merge into main from feature/number-of-games'. The date and time 'September 15, 2022 at 2:30 PM' are on the right. A green badge with the word 'Passed' is in the top right corner.

The main content area is divided into two sections. On the left, the 'Project Overview' sidebar lists various metrics: Reliability, Security, Security Review, Maintainability, Duplications, and Size. The 'Size' metric is highlighted with a 'NEW LINES' badge and a value of 17. Below this, there is a 'New Lines' section with a value of 17. The 'Issues' section is also visible.

On the right, the code editor shows a snippet of SQL code. The code is as follows:

```
132  
133 phili...  
134 -- number_of_games  
135  
136 procedure number_of_games is  
137     l_actual integer;  
138     l_expected integer;  
139 begin  
140     -- act  
141 phili...     l_actual := wordle.number_of_games(date '2027-01-01');  
142 phili...  
143     -- assert  
144 select count(*) into l_expected  
145     from words  
146     where game_date >= date '2027-01-01';  
147 phili... ut.expect(l_actual).to_equal(l_expected);  
148 phili... end number_of_games;  
149  
150 phili... -- -----
```

23 PULL REQUEST – QUALITY GATE STATUS "PASSED"

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministration

?

Q Search for projects...

A

Wordle

6 – feature/number-of-games

for merge into main from feature/number-of-games

September 15, 2022 at 2:30 PM

OverviewIssuesSecurity HotspotsMeasuresCode

Passed

QUALITY GATE STATUS

Conditions on New Code

Passed

MEASURES

0	New Bugs	Reliability	A
0	New Vulnerabilities	Security	A
0	New Security Hotspots	Security Review	A
1	New Code Smells	Maintainability	A
100%	Coverage on 2 New Lines to cover	95.0%	Estimated after merge
0.0%	Duplications on 40 New Lines	0.0%	Estimated after merge

COMPARISON

25 COMMERCIAL CHARACTERISTICS

Characteristic	plsql	plsqlopen	plsqlcop
License	commercial	LGPL	commercial
Licensing unit	LOC/server	n/a	users
Licensing type	rent	n/a	perpetual
Upgrade rights	included	n/a	15%
License costs starting at	€150	n/a	€3'400

26 BASIC FEATURES

Feature	plsql	plsqlopen	plsqlcop
Rules repository	✓	✓	✓
Issues (rule violations)	✓	✓	✓
Syntax highlighting of main code	✓	✓	✓
Syntax highlighting of test code	✗	✓	✓
Copy & paste detection (relevant lexical tokens)	✓	✓	✓
Code coverage (executable lines)	✓	✓	✓
Core metrics (LOC, comment lines, statements, functions, ...)	✓	✓	✓
Custom metrics (max. cyclomatic complexity, commands, ...)	✗	✗	✓
Only register executable lines for objects covered by utPLSQL	✗	✗	✓

27 TOOLING

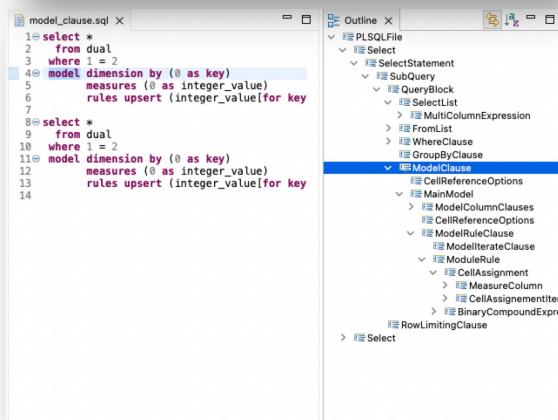
Feature	plsql	plsqlopen	plsqlcop
Standalone Toolkit to visualize AST (based on SSLR)	✓	✓	✗
Eclipse PL/SQL editor to visualize Ecore model (based on EMF)	✗	✗	✓
CLI to analyze code independent of SonarQube	✗	✓	✓
CLI to create HTML and Excel reports	✗	✗	✓
CLI to create generic issue import file (for SonarCloud)	✗	✓	✓
SQL Developer extension	✗	✗	✓
PL/SQL Developer plugin	✗	🚧👷	✗

28 GRAMMAR SUPPORT

Topic	plsql	plsqlopen	plsqlcop
Supported SQL*Plus version	?	?	19c/21c
Supported SQLcl version	?	?	21.1
Supported SQL version	?	?	7-21c
Supported PL/SQL version	?	?	7-21c
Support of SQL code blocks in Markdown files	🚫	🚫	✅
Number of parse errors in Examples project	• 49	121	0
Number of parse errors in Wordle project	• 0	2	0

Not all cases
are reported!

plsql



30 RULES REPOSITORY

Feature	plsql	plsqlopen	plsqlcop
Active rules	132	49	134
Support for SonarCloud (quality profiles, quality gates)	✓	✗	✗
Parameterized rules	✓	✓	✗
Rules with Oracle data dictionary access	✓	✗	✗
Oracle Forms rules	✓	✓	✗
Rules for test code	✗	✓	✗
SQL injection vulnerabilities detection	✗	✗	✓
Rules for optimizer hints	✗	✗	✓
Rules for naming conventions	✓	✗	✓
Custom rules via XPath	✓	✓	✗
Custom rules via JVM language (Java, Kotlin, Xtend, etc)	✗	✓	✓

31 RULE VIOLATIONS – ISSUES

Feature	plsql	plsqlopen	plsqlcop
Support for SonarCloud	✓	✓	✓
Using secondary locations	✓	✓	✗
Disable via NOSONAR comment	✓	✓	✓
Manage issues via SonarQube	✓	✓	✓

CORE MESSAGES

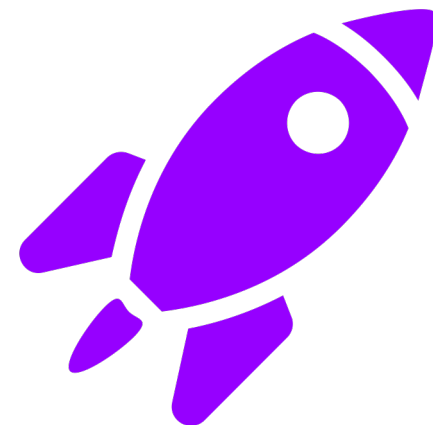
33 INTEGRATE SonarQube INTO YOUR CI ENVIRONMENT



- Start with Community Edition and ZPA (plsqlopen)
 - define quality profile with reasonable set of rules
 - use utPLSQL to publish test and code coverage results
 - define quality gate for new code
 - install the SonarQube Community Branch Plugin
- Upgrade to Developer Edition or SonarCloud (plsqli)
 - for support of C, C++, Obj-C, Swift, ABAP, T-SQL
 - for detection of injection vulnerabilities in Java, C#, PHP, Python, JavaScript, TypeScript
 - for more PL/SQL rules

34 USE db* CODECOP FOR MORE

- Check compliance of Trivadis PL/SQL & SQL Guidelines
- Detect SQL injection vulnerabilities in PL/SQL
- Validate optimizer hints
- Run checks in SQL Developer
- utPLSQL compliant code coverage
- Implement checks for your own rules with most complete 3rd party PL/SQL parser
- You can combine it with plsql or plsqlopen



**TOGETHER WE ARE
#1 PARTNER FOR BUSINESSES TO
HARNESS THE POWER OF DATA
FOR A SMARTER LIFE**