TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL - VTICT

TÀI LIỆU HƯỚNG DẪN CÀI ĐẶT VÀ PHÂN TÍCH MÃ NGUỒN SỬ DỤNG SONARQUBE

Hà Nội, 10/2105

BẢNG GHI NHẬN THAY ĐỔI

*A – Tạo mới, M – Sửa đổi, D – Xóa bỏ

Date Modify	A, D, M	PIC	Old version	Description	New version
14/09/2015	A	Tandd		First create	1.0
24/10/2015	M	Dungdb1		Thêm phần sử dụng so-narQube để quét với .NET project.	
30/10/2015	M	Dungdb1		Thêm phần sử dụng sonar với maven và các rules lập trình.	1.1

MỤC LỤC

1. GIỚI THIỆU

1.1. Mục đích và ý nghĩa của Tài liệu

Tài liệu hướng dẫn cấu hình cài đặt và sử dụng SonarQube để quét mã nguồn với các dự án Java và .NET.

1.2. Phạm vi tài liệu

Tài liệu phục vụ các đối tượng sau:

Cán bộ phát triển: Người thực hiện trực tiếp dự án sử dụng để quét mã nguồn.

1.3. Các thuật ngữ và từ viết tắt

N/A

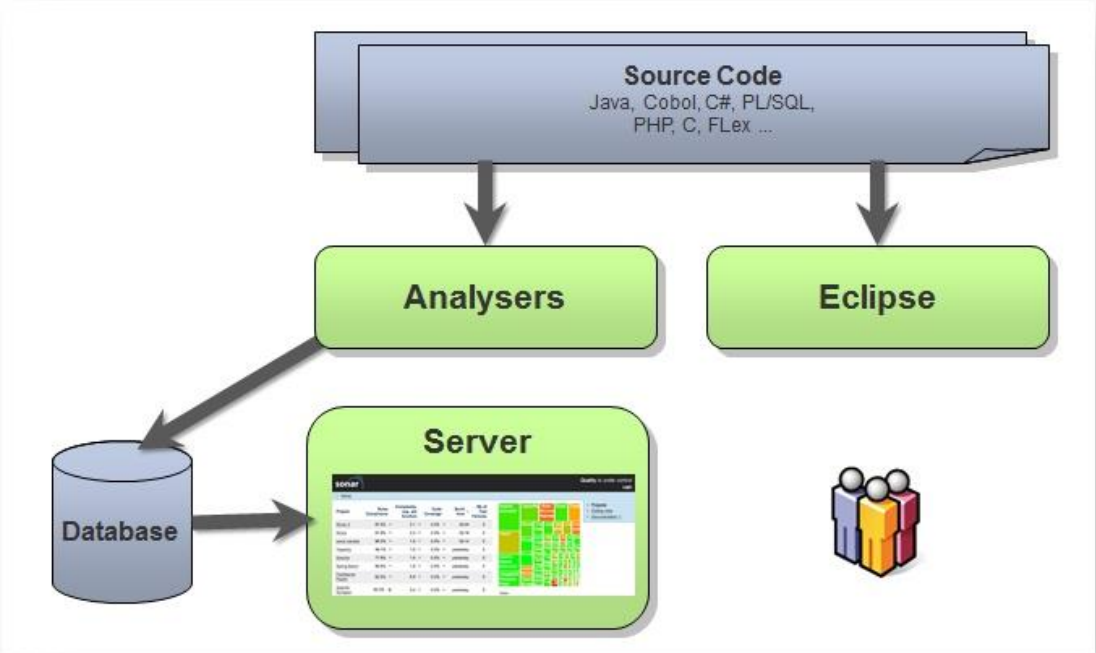
2. CÀI ĐẶT SERVER SONARQUBE

2.1. Kiến trúc SonarQube

SonarQube là một nền tảng mã nguồn mở để quản lý chất lượng mã nguồn. SonarQube hỗ trợ khá nhiều ngôn ngữ: Java, C#, C/C++, PL/SQL, Cobol, ABAP…

SonarQube platform gồm 3 thành phần:

1. **Database** lưu trữ:
    - Cấu hình của SonarQube (security, plugins settings, etc.)
    - Quality snapshots của các dự án
2. **Web Server** giúp người dùng xem xét trạng thái chất lượng của các dự án một các trực quan và giúp người dùng cấu hình Sonar
3. Một hoặc vài **Analyzers** dùng để phân tích chất lượng.



2.2. Cài đặt Database

Sonar có thể làm việc được với nhiều loại DBMS khác nhau, để đơn giản hóa và thống nhất thì chúng ta sẽ chỉ dùng MySQL bản opensource.

Việc cài đặt MySQL không được đề cập đến trong tài liệu này, chỉ có lưu ý về việc sử dụng engine InnoDB cho tất cả các table của database.

Để đạt được hiệu năng cao cho DB của Sonar, làm 2 bước sau:

1. Set giá trị Maximum của RAM cho parameter: innodb_buffer_pool_size
2. Set giá trị ít nhất 15Mb cho parameter: query_cache_size

2.3. Cài đặt Web Server

Download Web Server tại địa chỉ: http://www.sonarqube.org/downloads/

unzip tại địa chỉ: *<install_directory>*

<install_directory> được hiểu là nơi giải nén gói Web Server, ví dụ: D:\Sonar\sonarqube-4.5.1

Cấu hình kết nối với database:

Sửa file *<install_directory>/conf/sonar.properties* để cấu hình các tùy chọn kết nối tới database. Trong file này sẽ có đầy đủ templates cho tất cả các database mà Sonar hỗ trợ, tuy nhiên sẽ chỉ có một kết nối duy nhất đươc sử dụng, với MySQL thì phần cầu hình sẽ như sau:

<install_*directory>/conf/sonar.properties*

```
sonar.jdbc.username=sonar
sonar.jdbc.password=sonar
#----- MySQL 5.x
sonar.jdbc.url=jdbc:mysql://localhost:3306/sonar?useUnicode=true&characterEncoding=
utf8&rewriteBatchedStatements=true&useConfigs=maxPerformance
```

*Chú ý tạo trước một database **sonar** ở trên cơ sở dữ liệu MySql!*

Đối với Windows Server 64 bits (tốt nhất là Windows Server 2012 R2), phải cấu hình Sonar hỗ trợ server mode. Tìm tham số sonar.web.javaOpts và xóa comment của nó đi:

```
sonar.web.javaOpts=……..
```

Khởi động Web Server:

Port mặc định sẽ là "9000" và context path mặc định là "/". Các giá trị này có thể được thay đổi bằng cách thay đổi các giá trị trong file *<install_directory>/conf/sonar.properties*. Ví dụ, muốn đổi thành port 80 và context part thành *sonar* thì cần cấu hình như sau:

<install_directory>/conf/sonar.properties

```
sonar.web.host=192.0.0.1
sonar.web.port=80
sonar.web.context=/sonar
```

Chạy file bat *<install_directory>/bin/windows-x86-XX/StartSonar.bat* để khởi động Web Server. Có thể truy cập địa chỉ sau để xem server dùng chung cho VTICT: http://10.61.68.127:9000/

3. CÀI ĐẶT VÀ SỬ DỤNG SCANER

3.1. Quét mã nguồn JAVA project với Sonar-runner.

Cài đặt Sonar-runner:

- Download Sonar-runner từ website. Click here
- Giải nén vào thư mục cài đặt *<install_directory>*
- Trong file *<install_directory>/conf/sonar-runner.properties*, cầu hình cho Sonar-runner như sau:

```
#----- MySQL
sonar.jdbc.url=jdbc:mysql://localhost:3306/sonar?useUnicode=true&amp;characterEncoding=utf8
#----- Oracle
#sonar.jdbc.url=jdbc:oracle:thin:@localhost/XE
#----- Microsoft SQLServer
#sonar.jdbc.url=jdbc:jtds:sqlserver://localhost/sonar;SelectMethod=Cursor
#----- Global database settings
sonar.jdbc.username=sonar
sonar.jdbc.password=sonar
```

- Tạo biến môi trường *SONAR_RUNNER_HOME* tới thư mục *<install_directory>*.
- Thêm *<install_directory>/bin* vào biến môi trường path.
- Sử dụng command sau để phân tích code:

```
sonar-runner [options]

Options:
 -D,--define <arg>     Define property
 -e,--errors           Produce execution error messages
 -h,--help             Display help information
 -v,--version          Display version information
 -X,--debug            Produce execution debug output
```

3.2. Quét mã nguồn maven project

Điều kiện cần: Đã download và cài đặt Maven

Cấu hình maven:

- Chỉnh sửa file *setting.xml* trong *$MAVEN_HOME/conf* hoặc trong thư mục *~/.m2* như sau:

```
<settings>
  <profiles>
    <profile>
      <id>sonar</id>
      <activation>
        <activeByDefault>true</activeByDefault>
      </activation>
      <properties>
        <!-- Example for MySQL-->
        <sonar.jdbc.url>
          jdbc:mysql://localhost:3306/sonar?useUnicode=true&amp;characterEncoding=utf8
        </sonar.jdbc.url>
        <sonar.jdbc.username>sonar</sonar.jdbc.username>
        <sonar.jdbc.password>sonar</sonar.jdbc.password>
        <!-- Optional URL to server. Default value is http://localhost:9000 -->
        <sonar.host.url>
          http://myserver:9000
        </sonar.host.url>
      </properties>
    </profile>
  </profiles>
</settings>
```

Chú ý:

Trong trường hợp gặp lỗi java.lang.OutOfMemoryError, đặt lại giá trị biến môi trường MAVEN_OPTS như sau:

Với linux:

```
export MAVEN_OPTS="-Xmx512m -XX:MaxPermSize=128m"
```

Với windows:

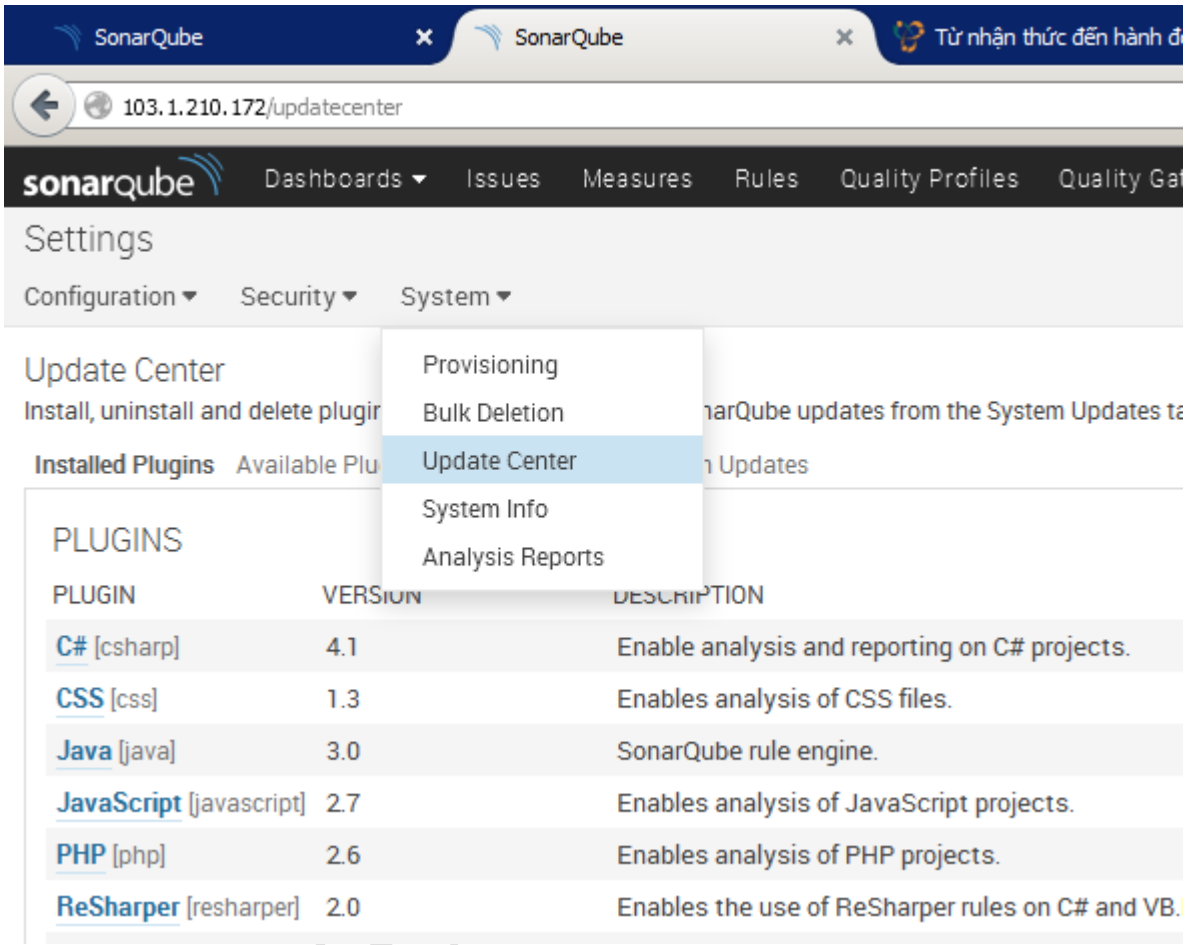
```
set MAVEN_OPTS=-Xmx512m -XX:MaxPermSize=128m
```

Thực hiên quét với maven project:

```
# The sonar:sonar goal must be executed in a dedicated mvn command
mvn clean install
mvn sonar:sonar
# The following command may lead to unexpected issues
mvn clean install sonar:sonar
```

3.3. Sử dụng Sonar để quét với .NET project

3.3.1. Install C# plugin



1. Chọn Available Plugins, lựa chọn cài đặt C# plugin để cài đặt cho Plugin này.
2. Sau khi cài đặt thành công, khởi động lại SonarQube Server để active C# Plugin

3.3.2. Cấu hình MSBuild SonarQube Runner và thực hiện quét với .NET project

Cấu hình MSBuild SonarQube Runner trên Build Agent Machine (Cài đặt trên máy muốn phân tích code, ví dụ máy phát triển hoặc build agent)

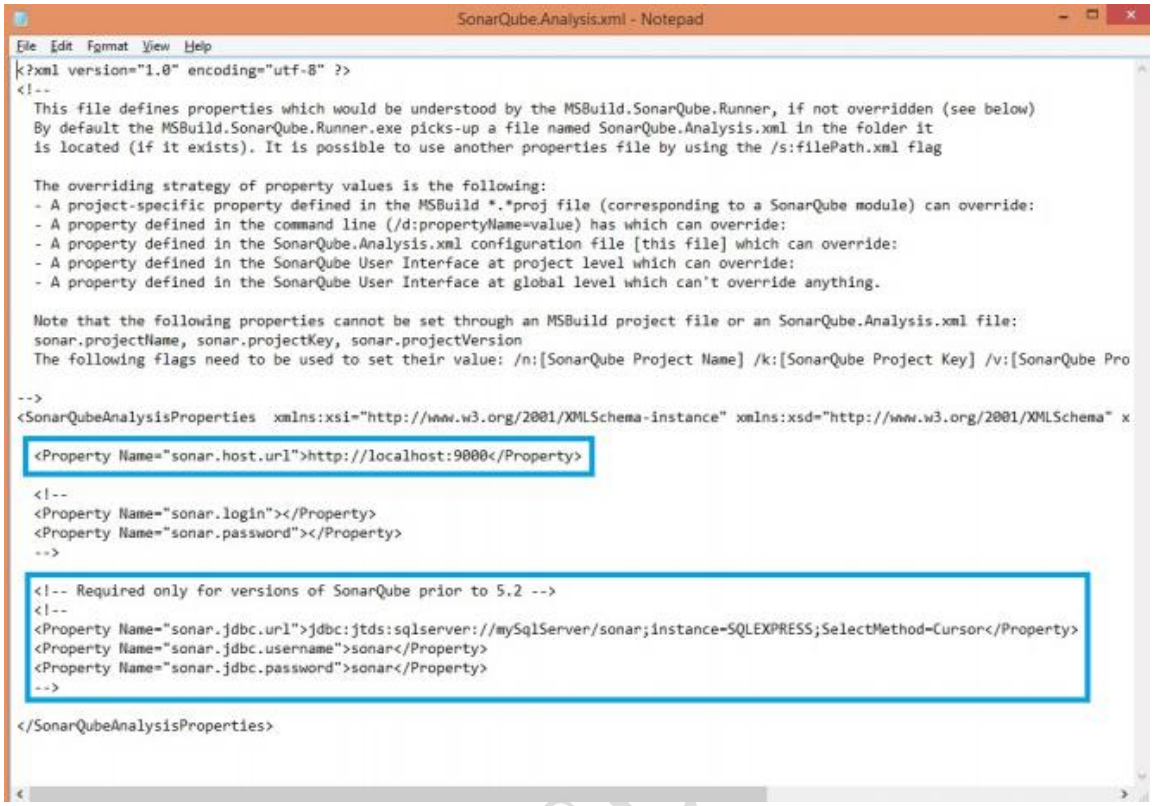
Extract:

- Download MSBuild SonarQube Runner từ website của Sonar
- Giải nén MSBuild.SonarQube.Runner-[version] trên thư mục bạn muốn. Ví dụ: C:\SonarQube\bin

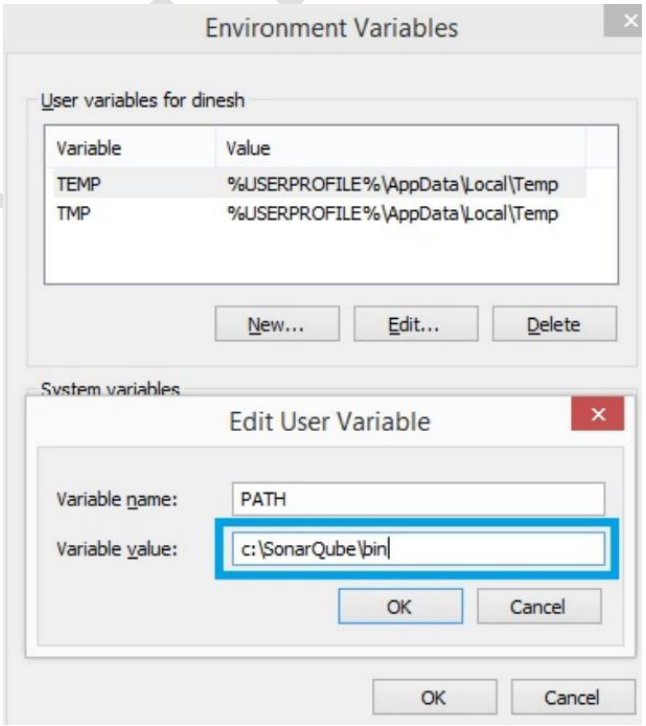
Cấu hình:

- Chỉnh sửa file C:\SonarQube\bin\SonarQube.Analysis.xml để có các tham số sau(đối với SonarQube 5.1.x):
    - sonar.jdbc.url
    - sonar.jdbc.username

- sonar.jdbc.password



- Cập nhật đường dẫn %PATH% cho file chạy MSBuild SonarQube Runner. Nếu thư mục giải nén là C:\SonarQube\bin thì cấu hình như sau:



- Thực hiện quét:
  - Chạy *MSBuild.SonarQube.Runner.exe begin* với cú pháp:

MSBuild.SonarQube.Runner.exe begin /v:1.0 /n:"BUGD UNIONE" /k:BUGD.UNI.ONE

Trong đó:

- /v:"Version project"
- /n:"Name project"
- /k:"Key project"

- Build project:

msbuild

Trường hợp sử dụng nuget:

nuget restore
msbuild

Chú ý: *Chạy MSBuild.SonarQube.Runner trong "MSBuild console", hoặc "VS Developer Command Prompt" để có thể chạy được MSBuild command*

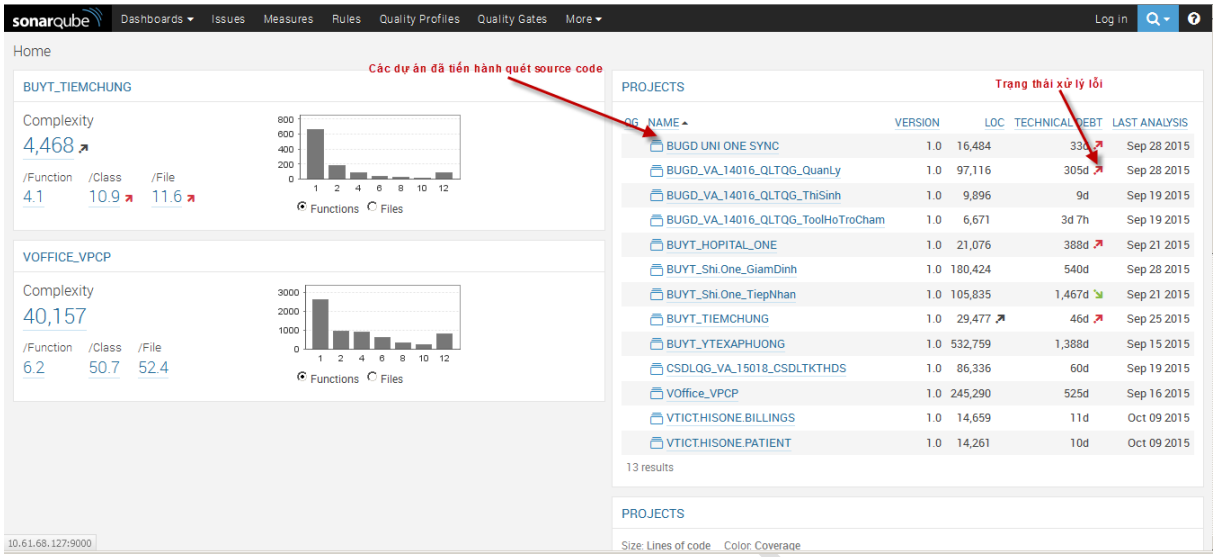
- Kết thúc

MSBuild.SonarQube.Runner.exe end

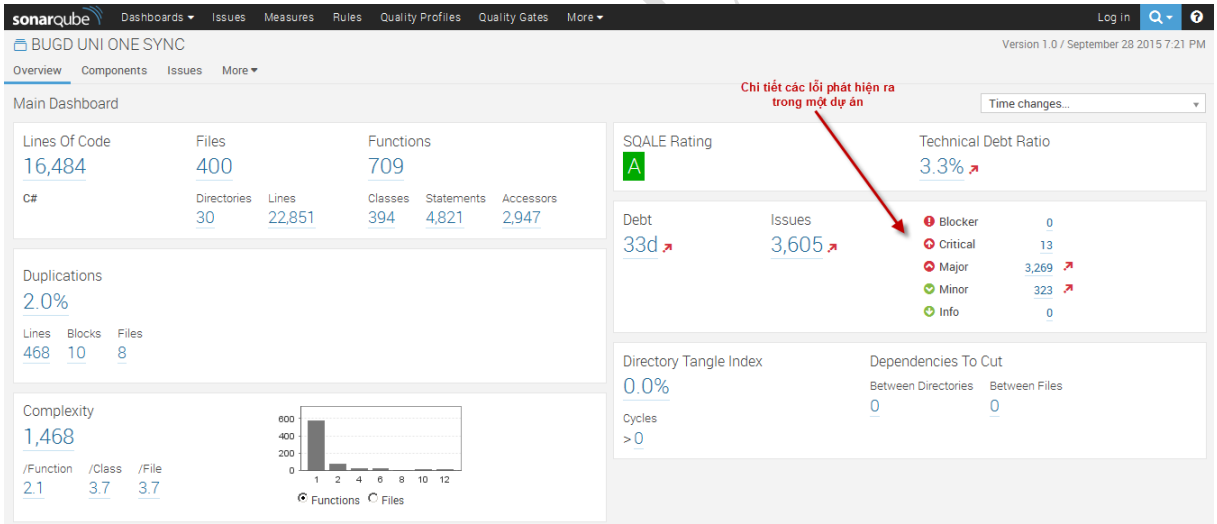
4. HƯỚNG DẪN SỬ DỤNG VÀ TÙY CHỈNH CÁC RULES

4.1. Một số màn hình chung

- Truy cập vào server dùng chung của VTICT theo địa chỉ sau: http://10.61.68.127:9000/ để xem thông tin của các dự án đã tiến hành phân tích code.Màn hình dashboard hiển thị như sau:



- Chi tiết thông tin dự án sau khi quét như sau:



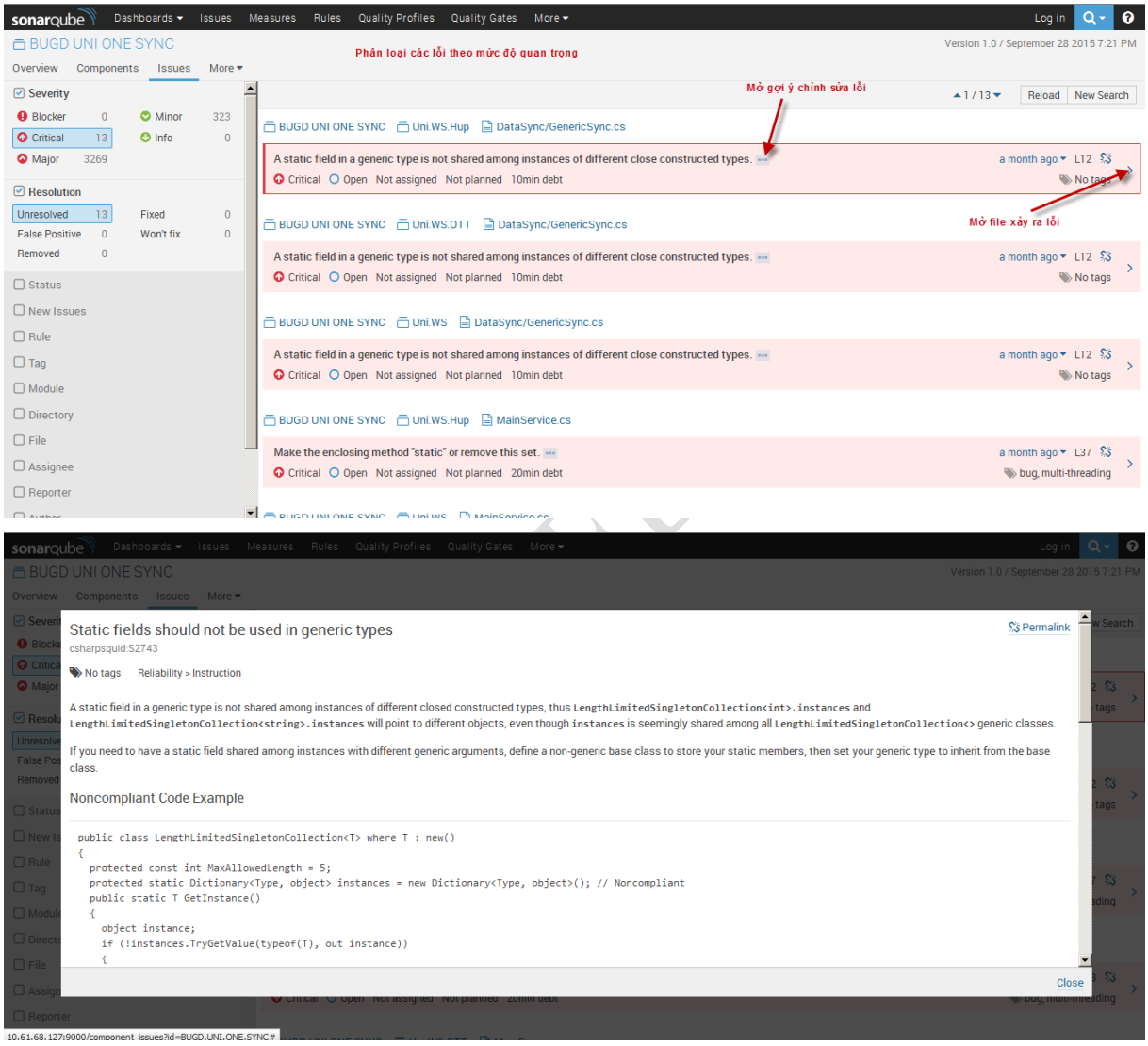
- Độ nghiêm trọng của các lỗi được phân chia như sau:

Severity	Mô tả
Blocker	Những rủi ro (risk) về hoạt động hoặc an toàn thông tin có thể gây đến sự mất ổn định cho toàn hệ thống.
Critical	Những rủi ro (risk) về hoạt động hoặc an toàn thông tin trong một số trường hợp cụ thể, không ảnh hưởng tới toàn bộ hệ thống. Ví dụ: NullPointerException, badly caught exceptions...
Major	Những vấn đề có thể gây ra tác động đáng kể về hiệu năng. Ví dụ: too complex methods, package cycles, etc.

Severity	Mô tả
Minor	Các vấn đề về coding conventions....
Info	Những rủi ro chưa xác định rõ.

Những lỗi Blocker và Critical là lỗi quan trọng → cần được ưu tiên xử lý triệt để!

- Xem lỗi xảy ra trong từng file và gợi ý sửa lỗi.



4.2. Add thêm bộ rule

Login vào hệ thống với tài khoản mặc định là **admin/admin.**

Sonar cung cấp một số bộ rule khác nhau tương ứng với từng ngôn ngữ.

Java:

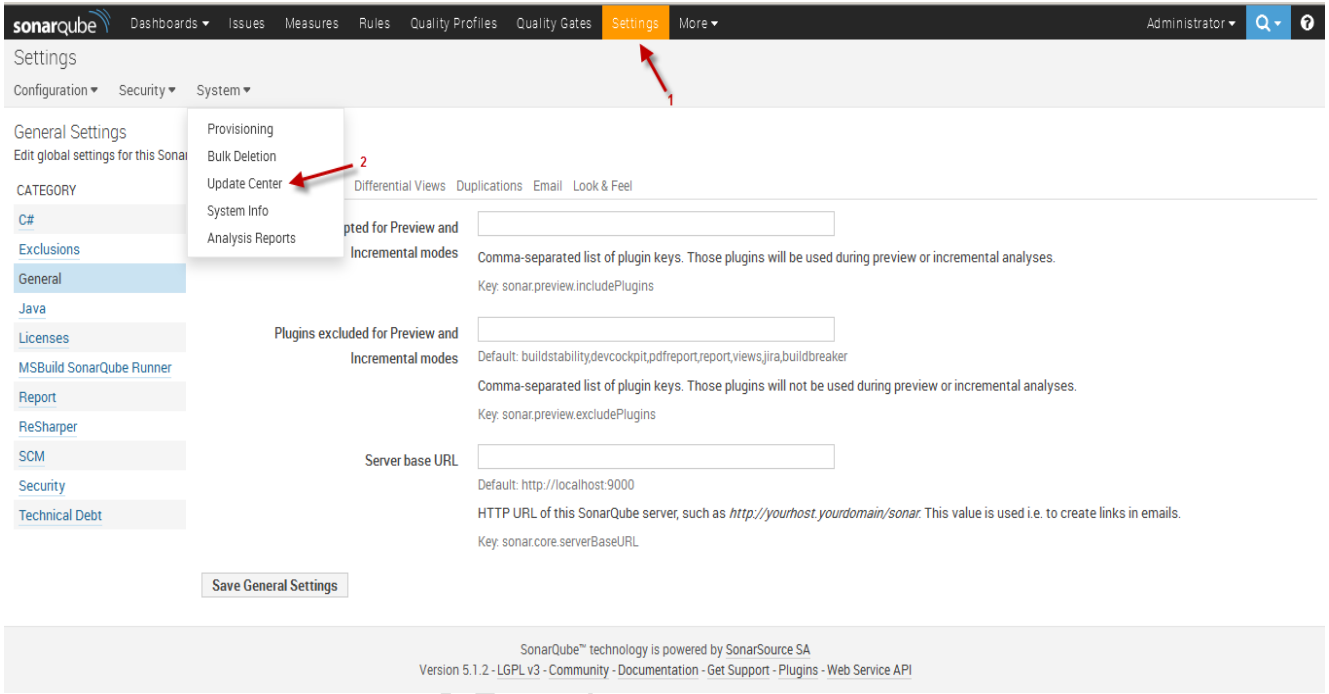
- SonarQube for java
- PMD
- Findbug
- Checkstyle
- Find security bugs

- ...

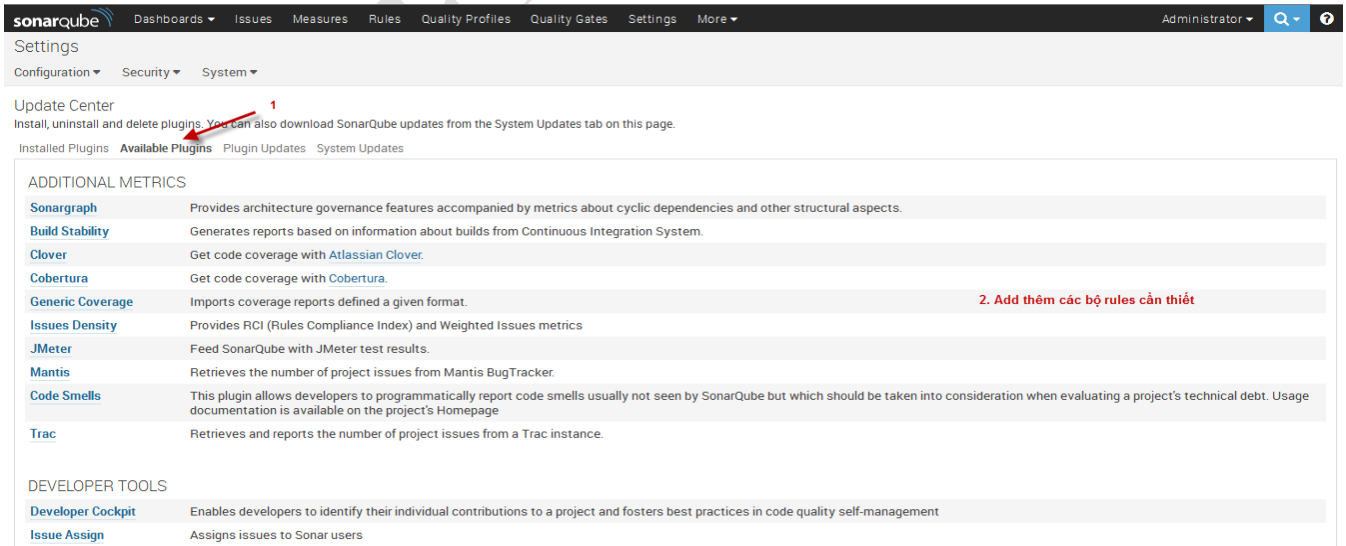
.NET

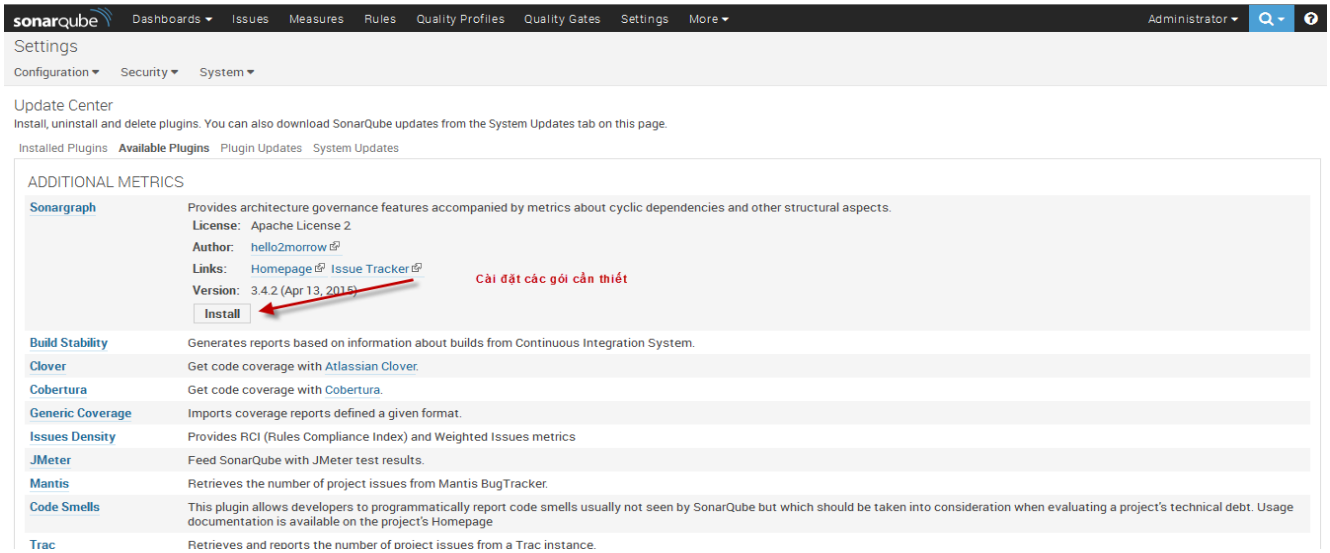
- SonarQube for .NET
- Fxcop/ Code analytic C#
- StyleCop
- ....

Các bước để thêm các bộ rule như sau:

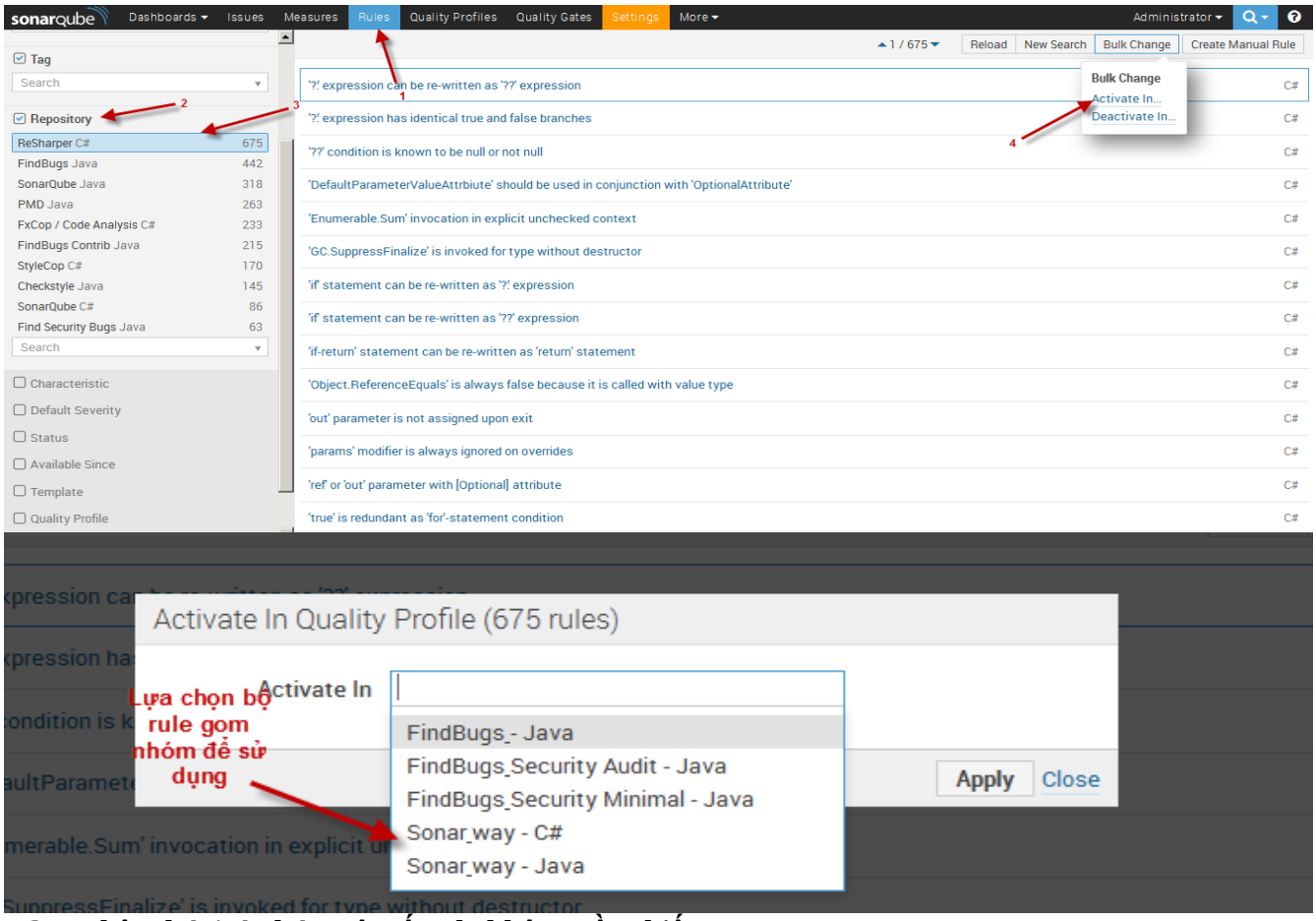


- Cài đặt thêm các rules muốn sử dụng





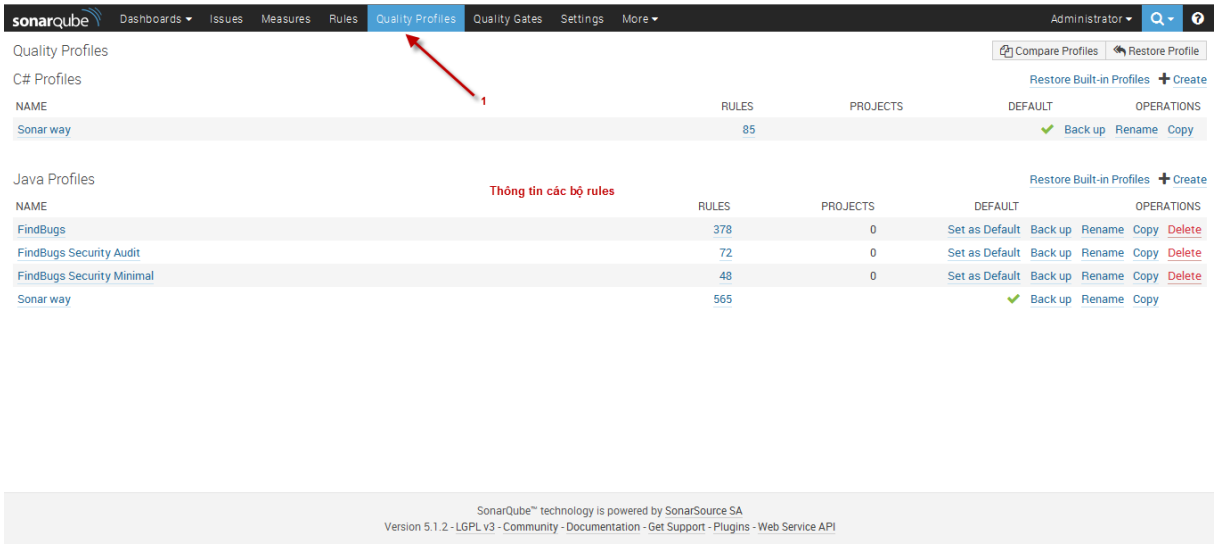
- Gom nhóm các bộ rules vừa cài đặt để sử dụng.



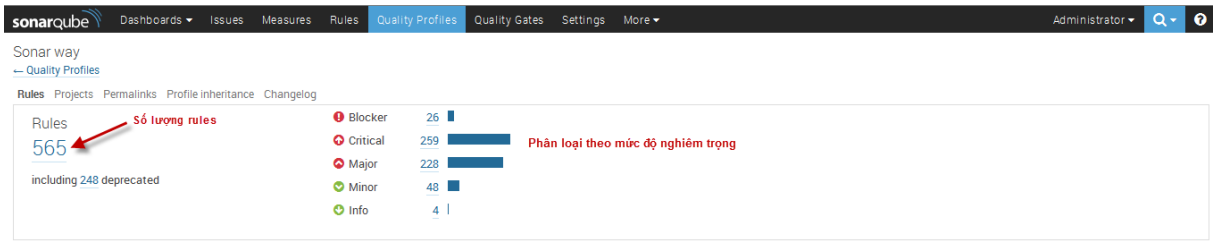
4.3. Thêm bớt/xóa bớt một số rule không cần thiết

Đối với từng bộ rules, sẽ có một số rules khi sử dụng chúng ta thấy không cần thiết. Để tiến hành loại bỏ chúng ra khỏi tập rules sử dụng để quét, tiến hành các bước như sau:

- Xem thông tin các bộ rules đang áp dụng.



- Lựa chọn một bộ rules, xem xét các mức độ phân loại nghiêm trọng.



- Active/deactive các rules không cần thiết.