Sonatype CLM Enforcement Points - SonarQube

Contents

List of Figures

Chapter 1

Introduction

Sonatype CLM integrates with a wide range of external enforcement points that include continuous integration servers (Hudson/Jenkins), the IDE (Eclipse), and repository management (Nexus). This is in addition to the Sonatype CLM stand-alone/command line scanner and Maven plugin.

The enforcement points are a common aspect of the development lifecycle, and in Sonatype CLM, each represents a unique stage. This creates an invaluable integration of Sonatype CLM with industry standard tools that already make the lives of your business and development process even better. This also means, your team has greater overall control in identifying and reducing open source component risk.

Better component usage doesn't just lead to risk reduction though, it also leads to better applications. This is something that ties closely with code analysis, and tools such as SonarQube.

As a user of SonarQube, you know first hand the impact that principles such as the 7 Axes of Code Quality can have on the applications and projects your teams create. Paralleling this, as a user of Sonatype CLM you also know how policy management is a critical and essential part of open source component usage.

Sonatype CLM for SonarQube brings both of these together, and in this guide we'll cover everything you need to get going as quickly as possible. This includes:

- Download, installation, and configuration
- Application Composition Report access

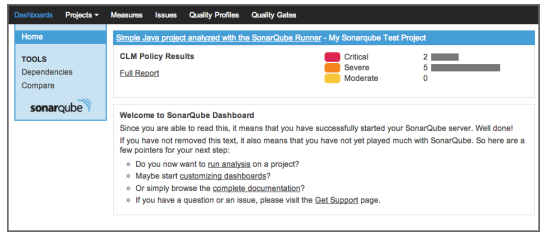

Figure 1.1: SonarQube Overview

Note

This guide assumes that you have installed and are running the Sonatype CLM Server. You must have at least one organization and an application created, as well as at least one policy the application can be evaluated against.

Chapter 2

Downloading, Installing, and Configuring

As mentioned in the introduction there are a few things that must be done prior to getting the Sonatype CLM for SonarQube functional. This includes:

- Installed and configured the Sonatype CLM Server
- Created an organization, and at least one application
- Evaluated the application at least once
- Have an existing SonarQube project

With these items completed, you can download Sonatype CLM for SonarQube from our Sonatype CLM downloads page.

Note
Sonatype CLM for SonarQube supports the latest and LTS (long-term-support) versions.

2.1 Install Sonatype CLM for SonarQube

Once downloaded, find the *extensions>plugins* directory in your installation of SonarQube. Next, copy the Sonatype CLM for SonarQube JAR file (the one just downloaded from the link above) into this directory. Finally, start your SonarQube instance, and log in with your administrator account.

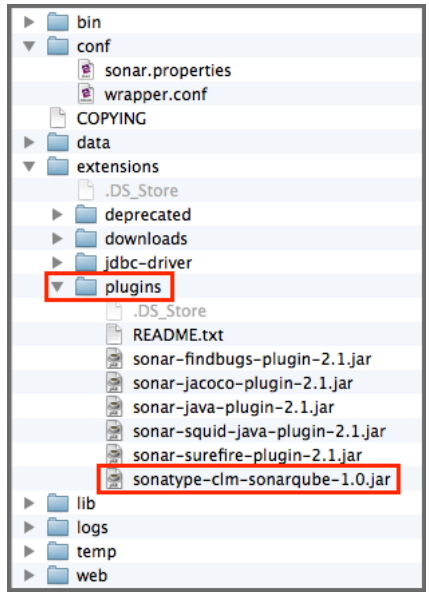

Figure 2.1: SonarQube Plugin Directory

Note
If your installation of SonarQube is running, stop it before adding the plugin.

2.2 Configure Sonatype CLM Server Settings

The Sonatype CLM Server settings allow you to specify the location of your CLM server. In the example below, basic defaults for configuration have been used. Yours will likely be different.

1. From the main SonarQube interface, click on the *Settings* menu item. This is located in the upper right corner of *SonarQube Home Page*.

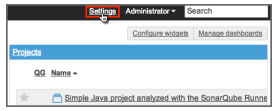

Figure 2.2: SonarQube Settings Menu

2. On the left hand side, in the *Configuration menu*, click on *CLM Settings*.

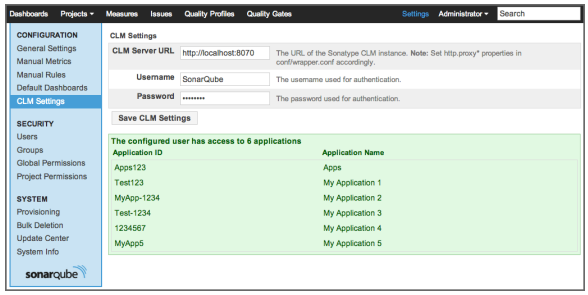

Figure 2.3: SonarQube CLM Server Settings

3. Enter the details for your Sonatype CLM Server location, as well as the user name and password that is at least a member of the developer role for the application you wish to associate with this SonarQube project.

Note

These settings will be used across all projects for your SonarQube installation. Because of this we suggest creating a single account in Sonatype CLM for SonarQube, and then associating that account with the Developer role for the applications you will be linking to SonarQube.

---

4. Click the *Save CLM Settings* button to save your Sonatype CLM settings, and then return to the SonarQube Dashboard home.

2.2.1 A Special Note About Proxy Configuration

In some instances, your CLM server may be setup behind a proxy. If this is the case, be sure to have your SonarQube admin configure your proxy via wrapper.conf file located within the conf directory of your

SonarQube installation.

Within this file you will need to add several parameters to the *Java Additional Parameters* section. Here's an example of how this configuration might look.

```
wrapper.java.additional.7=-Dhttp.nonProxyHosts=disable-default- ↩
    nonproxyhosts
wrapper.java.additional.8=-Dhttp.proxyHost=192.168.2.97
wrapper.java.additional.9=-Dhttp.proxyPort=8888
```

Tip
For more information on adding additional java properties, we suggest an internet search for *additional parameters wrapper tanukisoftware*.

2.3 Select the CLM Application

Now, you are ready to select the application that is associated with your SonarQube project.

1. Open the project you want to associate the application with, and then click the *Configuration* menu located just below the SonarQube Search field. A menu will drop down; Choose *Sonatype CLM*.

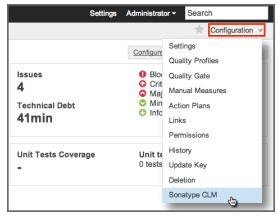

Figure 2.4: SonarQube Sonatype CLM Configuration Menu

2. You will now see the Sonatype CLM Configuration Area. This consists of a drop down menu allowing you to see all Sonatype CLM applications that the Sonatype CLM user account you entered earlier has access to. Choose the application that should be associated to your SonarQube Project.

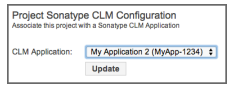

Figure 2.5: SonarQube Sonatype CLM Application Selection

3. Click the *Update* button.

2.4 Add and Configure the Sonatype CLM Widget

The final step is to add the Sonatype CLM Widget to your SonarQube project. This is done from the *SonarQube Widget Configuration area*.

1. Click on the *Configure widgets* link located just below and to the left of the SonarQube main search field (upper right of SonarQube page).

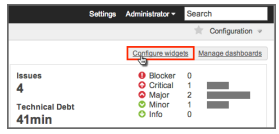

Figure 2.6: SonarQube Configure Widgets Menu

2. The easiest way to find the Sonatype CLM Report Summary widget is by using the SonarQube widget search (just enter Sonatype). Click on the *Add widget* button to add the widget to your Home page.

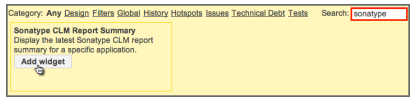

Figure 2.7: SonarQube Search for CLM Widget

3. Next, click on the *Edit* link in the top right of the Sonatype CLM Report Summary widget box. Several options will display.

    a. Select the *Project* you want to see Sonatype CLM data in.

Tip
The option to select a project is only available when adding the widget from a non-project-specific dashboard.

b. Enter a *Title*. This will appear above the summary information for the Sonatype CLM data.

c. Choose the *CLM Stage*. The Sonatype CLM stage selected affects which Application Composition Report will be used to display summary-level data. Be sure to pick the stage that best represents the state of your application when it is scanned by SonarQube. *Default* will use the *Build stage*.

Note
Due to technical constraints, the dropdown option also includes stages that might not be available for your Sonatype CLM license. Selecting any of those will however yield an error when accessing the Sonatype CLM server.

Figure 2.8: SonarQube Configure Sonatype CLM Widget options

4. Click the *Save* button to save your selections.

Chapter 3

Accessing the Application Composition Report

Within SonarQube, you will be provided with basic summary information for the Application, as well as a link to the associated Application Composition Report. To access the detailed information provided by this report, click on the *Full Report* link displayed in the Sonatype CLM Report Summary widget in your project.

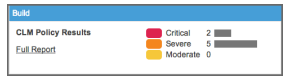

Figure 3.1: SonarQube Sonatype CLM Widget Example

Chapter 4

Conclusion

By now, you should have Sonatype CLM for SonarQube installed, and you should be seeing information from the corresponding Application Composition Report. There really isn't much more to it, and now you have seamless analysis of your open source component usage right inline with all the information provided by SonarQube.

Just to recap, here are a few of the topics covered regarding the Sonatype CLM for SonarQube:

- Download, installation, and configuration
- Application Composition Report access