Open Compliance Reference Tooling

Welcome

- Marcel Kurzmann
- Working at Bosch.IO GmbH
- Represents Bosch in the OpenChain Governance board
- Regular participant of the tooling group

INAL: I ‘m not a lawyer!

Disclaimer:

- The following presentation is only for demonstration of the process and the tooling. The metadata was partly manipulated for the showcases.
- If you plan to deploy a tool-suite comparable to the Open Compliance Reference Tooling please consult your legal team before applying license-classifications, rules and the output formats in your specific context.
Reference Tooling Work Group

We are building an open source compliance toolchain ecosystem with open source tools as an open source project. To accomplish this we:

- Use existing independent tooling projects
- Provide reference workflows to allow their adoption
- Provide the concepts and glue to ensure easy interoperability and integration in existing environments
- Provide reference turnkey toolchains that can be used without fees by anybody

World-Wide Collaboration, World-Wide Availability

Example Automation Implementation Using Open Source Tools

Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Online meetings: Bi-weekly - Invitations are sent to the mailing list

Website: https://oss-compliance-tooling.org/

And of course we are on GitHub:
https://github.com/Open-Source-Compliance/Sharing-creates-value
Open Compliance Reference Tooling
“Metadata debts”?

“Technical debts” and “Metadata debts”

3.3 Open source content review and approval

3.3.1 Bill of materials

A process shall exist for creating and managing a bill of materials that includes each open source component (and its identified licenses) from which the supplied software is comprised.

Verification material(s):

- 3.3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of open source components from which the supplied software is comprised.
- 3.3.1.2 Open source component records for the supplied software that demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing an open source component bill of materials used to construct the supplied software. A bill of materials is needed to support the systematic review and approval of each component’s license terms to understand the obligations and restrictions as it applies to the distribution of the supplied software.
Open Compliance Reference Tooling

Range of application

- No single reference but depending on context e.g. heterogeneous vs. homogenous OSM setups

Sync metadata btw.
Tools &
sync metadata with other sources

Sync metadata with other sources
Open Compliance Reference Tooling

End to end process flow

- Business Process Modeling Notation
- Details see BPMN [http://www.bpmb.de/index.php/BPMNPoster](http://www.bpmb.de/index.php/BPMNPoster)

- Events

- Activities

- Gateways

- Lanes
Open Compliance Reference Tooling

And now ...

...the process in action

The process in bpmn and png + a role-description is available here:

It is planned to enhance the process picture with a mapping to respective tools.

To keep it simple, the todays demo is based on OSS Review Toolkit as orchestrator. In the scan step ScanCode will be used.
Open Compliance Reference Tooling
If you want to repeat steps on your own that I will present...

Preparation:

- Take a Windows Computer and create a new user (ideally with administrator rights)
- Install java from [https://www.codejava.net/java-se/download-and-install-java-11-openjdk-and-oracle-jdk](https://www.codejava.net/java-se/download-and-install-java-11-openjdk-and-oracle-jdk) => OpenJDK11 ; set JAVA_HOME & set PATH as described
- Install git from [https://git-scm.com/download/win](https://git-scm.com/download/win)
- Get a ort-binary (by building it on your own or from a colleague who has an IDE ready anyway)
- Install ort
- run “ort requirements”
Open Compliance Reference Tooling
Expected ort requirements feedback
Open Compliance Reference Tooling

About the example...

- Based on semver4j see [https://github.com/vdurmont/semver4j.git](https://github.com/vdurmont/semver4j.git)
- Comes with a dependency to junit that will be used for the demo and some manipulations will be applied mainly to the ort-files
System correctly configured?

- Yes
- No

Configure Automation

Customize Output

URL

Re-iterate
Open Compliance Reference Tooling
Happy Path

- Case 1: Continuous Development/Continuous integration => fast feedback
Case 1: Continuous Development/Continuous integration => fast feedback
### Rule Violation Summary (0 errors, 0 warnings, 0 hints to resolve)

No rule violations found.

**Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)**

<table>
<thead>
<tr>
<th>Package</th>
<th>Scopes</th>
<th>Licenses</th>
<th>Analyzer Issues</th>
<th>Scanner Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maven:com.vdurmont:semver4j:3.1.0</td>
<td></td>
<td>Declared Licenses: MIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detected Licenses: BSD-3-Clause (link to the location) MIT exemplary link to the first of S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**BOM - list of raw components**

**BOM.1 - list of components with metadata**

**BOM.2 - BOM.1**

**BOM.3 - evaluated BOM**
Open Compliance Reference Tooling

Reality – subset of potential real world cases

- **Case 2:**
  - Open Source Office issue: a license classification is missing
  - solution: Open Source Office provides an updated license-classifications.yml

- **Case 3:**
  - Development Team issue: a license is classified non-suitable to the context
  - solution: development team provides a new development increment where the component is removed

- **Case 4**
  - Development Team + Open Source Office issue: a license is classified non-suitable to the context
  - solution: development team excludes „test“ pattern in .ort.yml in project root directory

- **Case 5**
  - Curation Team issue: metadata missing for a dependency
  - solution: curation team investigates the situation and provides the metadata in curations.yml
## Open Compliance Reference Tooling

### Reality – subset of potential real world cases

- **Case 2:**
  - Open Source Office issue: a license classification is missing
  - Solution: Open Source Office provides an updated license-classifications.yml

- **Case 3:**
  - Development Team issue: a license is classified non-suitable to the context
  - Solution: Development team provides a new development increment where the component is removed

- **Case 4**
  - Development Team + Open Source Office issue: a license is classified non-suitable to the context
  - Solution: Development team excludes “test“ pattern in .ort.yml in project root directory

- **Case 5**
  - Curation Team issue: metadata missing for a dependency
  - Solution: Curation team investigates the situation and provides the metadata in curations.yml
Case 2: Open Source Office - issue

<table>
<thead>
<tr>
<th>#</th>
<th>Rule</th>
<th>Package</th>
<th>License</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>COPYLEFT_LIMITED_IN_SOURCE</td>
<td>Maven junit:4.12</td>
<td>DECLARED: EPL-1.0</td>
<td>The package Maven.junit:4.12 has the declared ScanCode copyright-limited categorized license EPL-1.0.</td>
</tr>
<tr>
<td>2</td>
<td>UNHANDLED_LICENSE</td>
<td>Maven junit:4.12</td>
<td>DETECTED: EPL-2.0</td>
<td>The license EPL-2.0 is currently not covered by policy rules. The license was detected in package Maven.junit:4.12.</td>
</tr>
<tr>
<td>3</td>
<td>UNHANDLED_LICENSE</td>
<td>Maven junit:4.12</td>
<td>DETECTED: NOASSERTION</td>
<td>The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven.junit:4.12.</td>
</tr>
</tbody>
</table>
Case 2: Open Source Office - issue

license-classifications.yml
PROBLEM: License not classified

=> Open Source Office needs to classify and license_classification.yml needs to be updated
Only 2 errors left!

<table>
<thead>
<tr>
<th>#</th>
<th>Rule</th>
<th>Package</th>
<th>License</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>COPYLEFT_LIMITED_IN_SOURCE</td>
<td>Maven:junit:junit:4.12</td>
<td>DECLARED: EPL-1.0</td>
<td>The package Maven:junit:junit:4.12 has the declared ScanCode copyleft-limited categorized license EPL-1.0.</td>
</tr>
<tr>
<td>2</td>
<td>UNHANDLED_LICENSE</td>
<td>Maven:junit:junit:4.12</td>
<td>DETECTED: NOASSERTION</td>
<td>The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12.</td>
</tr>
</tbody>
</table>

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)

VCS Information

Type | Git
-----|-----
URL  | https://github.com/ndurmont/semver4j.git
Open Compliance Reference Tooling
Reality – subset of potential real world cases

- **Case 2:**
  - Open Source Office issue: a license classification is missing
  - solution: Open Source Office provides an updated license-classifications.yml

- **Case 3:**
  - Development Team issue: a license is classified non-suitable to the context
  - solution: development team provides a new development increment where the component is removed

- **Case 4**
  - Development Team + Open Source Office issue: a license is classified non-suitable to the context
  - solution: development team excludes „test“ pattern in .ort.yml in project root directory

- **Case 5**
  - Curation Team issue: metadata missing for a dependency
  - solution: curation team investigates the situation and provides the metadata in curations.yml
Case 3: Development Team + Open Source Office - issue

ISSUE for the Development Team: License classification ok => Development Team needs to check with Open Source Office if License may be applied
Case 3: Development Team + Open Source Office - issue

new increment
Open Compliance Reference Tooling

Reality – subset of potential real world cases

- Case 2:
  - Open Source Office issue: a license classification is missing
  - solution: Open Source Office provides an updated license-classifications.yml

- Case 3:
  - Development Team issue: a license is classified non-suitable to the context
  - solution: development team provides a new development increment where the component is removed

- Case 4
  - Development Team + Open Source Office issue: a license is classified non-suitable to the context
  - solution: development team excludes „test“ pattern in .ort.yml in project root directory

- Case 5
  - Curation Team issue: metadata missing for a dependency
  - solution: curation team investigates the situation and provides the metadata in curations.yml
Case 4: Development Team + Open Source Office - issue
Case 4: Development Team - issue

BUT – Development Team states that it is only for testing and will not be distributed! – team configures this in .ort.yml in the project repository root folder by excluding the „test“ pattern.
### Rule Violation Summary (0 errors, 0 warnings, 0 hints to resolve)

No rule violations found.

**Maven:com.vdurmont:semver4:3.1.0 (pom.xml)**

**VCS Information**

<table>
<thead>
<tr>
<th>Type</th>
<th>Git</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td><a href="https://github.com/vdurmont/semver4-gt">https://github.com/vdurmont/semver4-gt</a></td>
</tr>
<tr>
<td>Path</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td>7653e410b1100b1c26b100b100b200b5020b5020b5020b5020b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Package</th>
<th>Scopes</th>
<th>Licenses</th>
<th>Analyzer Issues</th>
<th>Scanner Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maven.com.vdurmont:semver4:3.1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Declared Licenses:
- MIT

Detected Licenses:
- BSD-3-Clause (link to the location)
- MIT (see the license link to the first of 3)
Open Compliance Reference Tooling
Reality – subset of potential real world cases

- **Case 2:**
  - Open Source Office issue: a license classification is missing
  - Solution: Open Source Office provides an updated license-classifications.yml

- **Case 3:**
  - Development Team issue: a license is classified non-suitable to the context
  - Solution: development team provides a new development increment where the component is removed

- **Case 4**
  - Development Team + Open Source Office issue: a license is classified non-suitable to the context
  - Solution: development团队 excludes “test” pattern in .ort.yml in project root directory

- **Case 5**
  - Curation Team issue: metadata missing for a dependency
  - Solution: curation team investigates the situation and provides the metadata in curations.yml
Case 5: Curation Team - issue

ISSUE for the Curation Team: Component detected with „No Assertion“
=> Curation Team needs to investigate the situation
Case 5: Curation Team - issue

For demonstration: scan-result.yml manipulated => deleted the license declaration for junit to pretend it would be missing

ISSUE for the Curation Team:
Component with no declared but only detected licenses
=> Curation Team needs to investigate the situation
Case 5: Curation Team - issue

For demonstration: scan-result.yml manipulated => deleted the license declaration for junit to pretend it would be missing

ISSUE for the Curation Team: Component with no declared but only detected licenses => Curation Team needs to investigate the situation, the result may be globally provided in the curations.yml in the ort-config-folder or as project specific resolution or curation in the .ort.yml in the project repository root folder.
Case 5: Curation Team issue
## License Browser

### Folder: Software Repository/ INST/ INST Checks/ junit4-r4.12.zip/junit4-r4.12

### Display 50 x files (tree view or flat)

<table>
<thead>
<tr>
<th>Scanner Count</th>
<th>Concluded License Count</th>
<th>License Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>EPL-1.0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>CPL</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Apache-2.0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSD-3-Clause</td>
</tr>
</tbody>
</table>

Showing 1 to 4 of 4 licenses

Hint: Click on the license name to search for where the license is found in the file listing.

### Summary

<table>
<thead>
<tr>
<th>Unique licenses</th>
<th>4</th>
<th>565 Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique scanner detected licenses</td>
<td>5</td>
<td>0 Unique concluded licenses</td>
</tr>
<tr>
<td>Licenses found</td>
<td>11</td>
<td>0 Licenses concluded</td>
</tr>
<tr>
<td>Files with no detected licenses</td>
<td>554</td>
<td>0 Concluded files with no detected licenses</td>
</tr>
</tbody>
</table>

### Files

<table>
<thead>
<tr>
<th>Files</th>
<th>Scanner Results (N: nomos, M: monk, Nk: ninja, I: reportImport, O: ojo)</th>
<th>Edited Results</th>
<th>Clearing Status</th>
<th>Files Cleared</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>src</td>
<td>Apache-2.0, EPL-1.0, No_license_found</td>
<td></td>
<td></td>
<td>0/3</td>
<td>[Tag][Ed]</td>
</tr>
<tr>
<td>epl-v10.html</td>
<td>EPL-1.0 [M: 87%]</td>
<td></td>
<td></td>
<td>0/1</td>
<td>[View][Edit]</td>
</tr>
<tr>
<td>LICENSE-junit.txt</td>
<td>EPL-1.0 [M: 99%]</td>
<td></td>
<td></td>
<td>0/1</td>
<td>[View][Edit]</td>
</tr>
<tr>
<td>pom.xml</td>
<td>EPL-1.0 [N]</td>
<td></td>
<td></td>
<td>0/1</td>
<td>[View][Edit]</td>
</tr>
</tbody>
</table>
Open Compliance Reference Tooling
Sharing the metadata...

- The curations in the tool may be shared with ClearlyDefined if configured accordingly
- This way it is also possible to benefit from curations that were already shared in the community and reduce the effort

https://clearlydefined.io
Case 5: Curation Team - issue

```yaml
# Manipulation for DEMO
- id: "Maven:junit:junit:4.12" # For Demo reason
  curations:
    comment: >-
      For the demo, the scan-result was manipulated and now for demo-reason shall show that this may be fixed in the curation file.
    concluded_license: "EPL-1.0"
# End Manipulation for DEMO
```
Case 5: Curation Team - issue

Scan Report

Created by ORT, the OSS Review Toolkit, version f5a1d22 on 2021-01-24T13:27:23.578054Z.

Project

Scanned revision 7653e418d810ffcd2811bcb55f72d00d42050b of Git repository https://github.com/vdurmont/semver4j.git

Index

Rule Violation Summary (1 errors, 0 warnings, 0 hints to resolve)
Maven:com.vdurmont:semver4j:3.1.0
Repository Configuration

Rule Violation Summary (1 errors, 0 warnings, 0 hints to resolve)

<table>
<thead>
<tr>
<th>#</th>
<th>Rule</th>
<th>Package</th>
<th>License</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>COPYLEFT_LIMITED_IN_SOURCE</td>
<td>Maven:junit:junit:4.12</td>
<td>CONCLUDED: EPL-1.0</td>
<td>The package Maven:junit:junit:4.12 has the concluded SonarQube copyleft-limited categorized license EPL-1.0.</td>
</tr>
</tbody>
</table>

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)

VCS Information

Type | Git
---|---
URL | https://github.com/vdurmont/semver4j.git
Path | 
Revision | 7653e418d810ffcd2811bcb55f72d00d42050b

Packages
### Case 5: Curation Team - issue

<table>
<thead>
<tr>
<th>#</th>
<th>Package</th>
<th>Scopes</th>
<th>Licenses</th>
<th>Analyzer Issues</th>
<th>Scanner Issues</th>
</tr>
</thead>
</table>
| 1 | Maven:com.vdurmont:semver4j:3.1.0 |        | Declared Licenses:  
MIT  
Detected Licenses:  
BSD-3-Clause (link to the location)  
MIT (exemplary link to the first of 3 locations) |                |                |
| 2 | Maven:junit:junit:4.12   | test   | Conclusion License:  
EPL-1.0  
Detected Licenses:  
Apache-2.0 (exemplary link to the first of 3 locations)  
EPL-1.0 (exemplary link to the first of 4 locations)  
EPL-2.0 (link to the location)  
NOASSERTION (link to the location) |                |                |
| 3 | Maven:org.hamcrest:hamcrest-core:1.3 | test   | Declared Licenses:  
BSD-3-Clause |                |                |
| 4 | Maven:org.mockito:mockito-all:1.10.19 | test   | Declared Licenses:  
MIT |                |                |
THANK YOU!

Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Online meetings: Bi-weekly - Invitations are sent to the mailing list

Website: https://oss-compliance-tooling.org /

And of course we are on GitHub:
https://github.com/Open-Source-Compliance/Sharing-creates-value