Training: Open Source Licenses and Copyright Notices

Steve Winslow

ONAP VF2F - February 8, 2018

THE LINUX FOUNDATION

Antitrust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Agenda

```
// WITHOUT WARRANTIES OR CONDI
// See the License for the spe
// limitations under the Licen
//
// SPDX-License-Identifier: Ap

package authenticator

type AuthenticatorConfig struc
  Anonymous bool
```

1. Licensing and Copyright Basics
2. LF License Scans
3. ONAP Processes and Best Practices
4. Q&A

Preliminary: Talk to your legal counsel!

- This training is intended to focus on community norms and best practices in license and copyright management. It is not intended as legal advice.
- The LF is not able to provide you with legal advice. For questions on interpretation of licenses contained in the code repository, ONAP members should consult with their own legal counsel.

An Ongoing Process

- License compliance is a matter of ongoing improvement
  - ...like all aspects of collaborative software development

- Areas of focus will change over time as we improve together
- Focusing on key priorities first

- Reach out with any questions!
  - Steve Winslow: swinslow@linuxfoundation.org
  - your in-house legal counsel (for any legal interpretation questions)

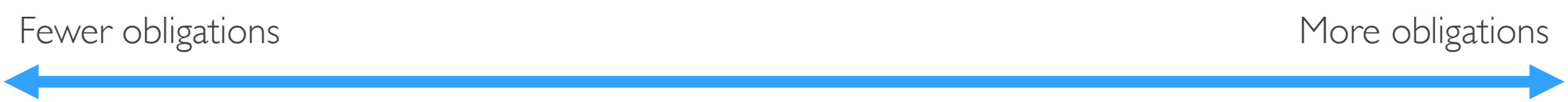
Licensing and Copyright Basics

THE LINUX FOUNDATION

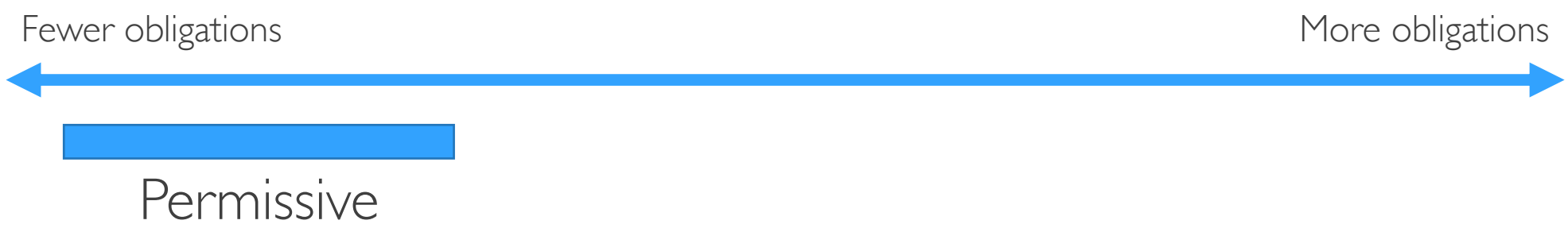
Open Source Licensing: Basics

- Copyright – certain rights owned in software code (among other things)
- License – permission to do something
  - "Proprietary" – typically very limited rights to use but not modify or redistribute; restrictive conditions and obligations
  - "Open Source" – typically broad rights to use, modify and redistribute, with varying conditions
- Standardized language for various (100+) open source licenses

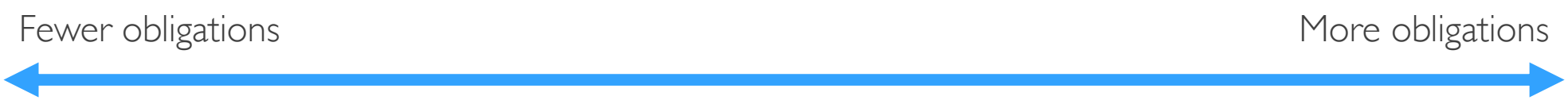
Open Source Licensing: Types



Open Source Licensing: Types



Open Source Licensing: Types



Permissive

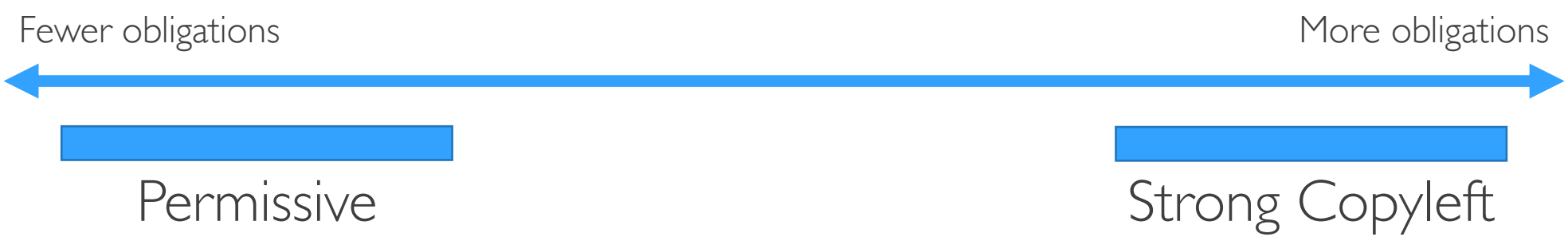
Examples

MIT

BSD-2-Clause
BSD-3-Clause

Apache-2.0

Open Source Licensing: Types



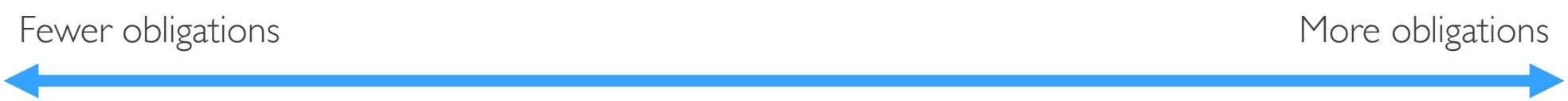
Examples

MIT

BSD-2-Clause
BSD-3-Clause

Apache-2.0

Open Source Licensing: Types



Permissive

Examples

MIT

BSD-2-Clause
BSD-3-Clause

Apache-2.0

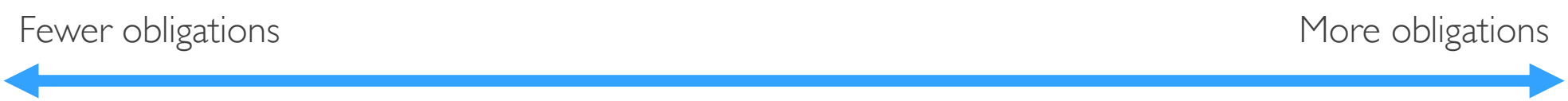
Strong Copyleft

Examples

GPL-2.0, GPL-3.0

Affero GPL (AGPL-3.0)

Open Source Licensing: Types



Permissive

Examples

MIT

BSD-2-Clause
BSD-3-Clause

Apache-2.0

Weak Copyleft

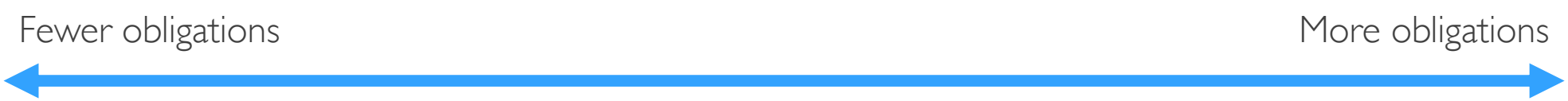
Strong Copyleft

Examples

GPL-2.0, GPL-3.0

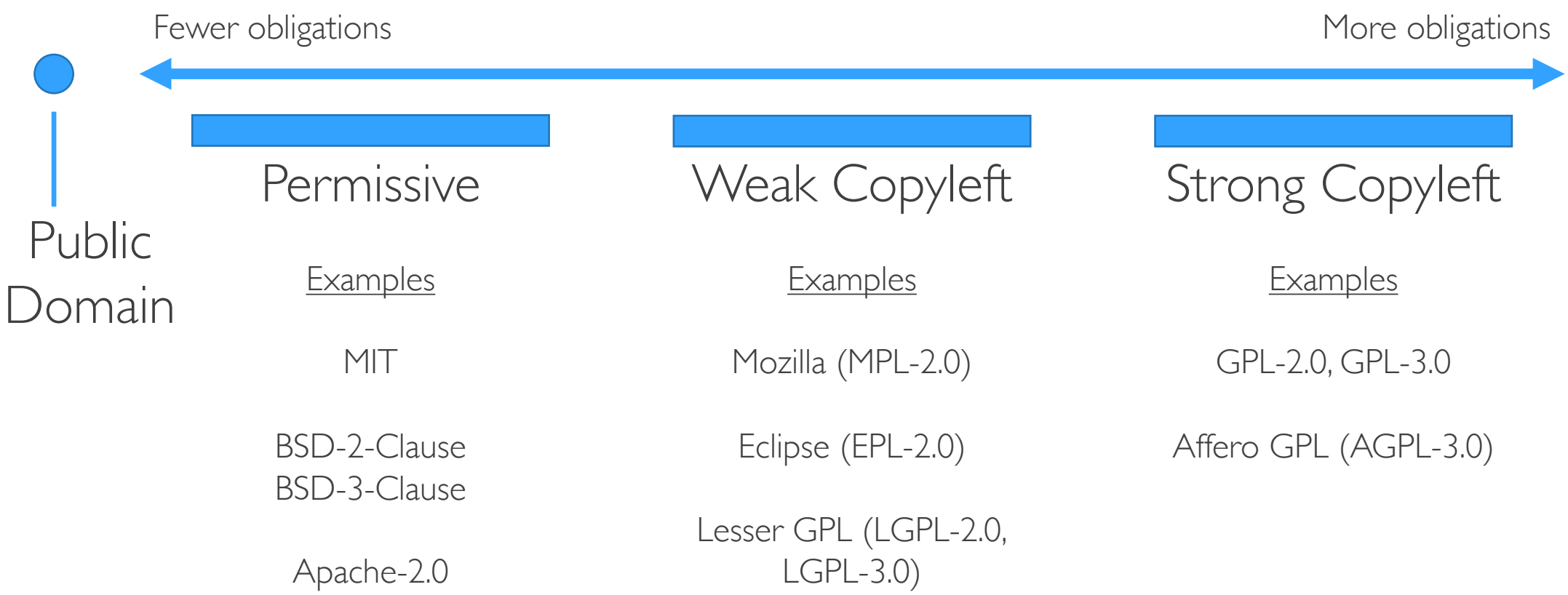
Affero GPL (AGPL-3.0)

Open Source Licensing: Types

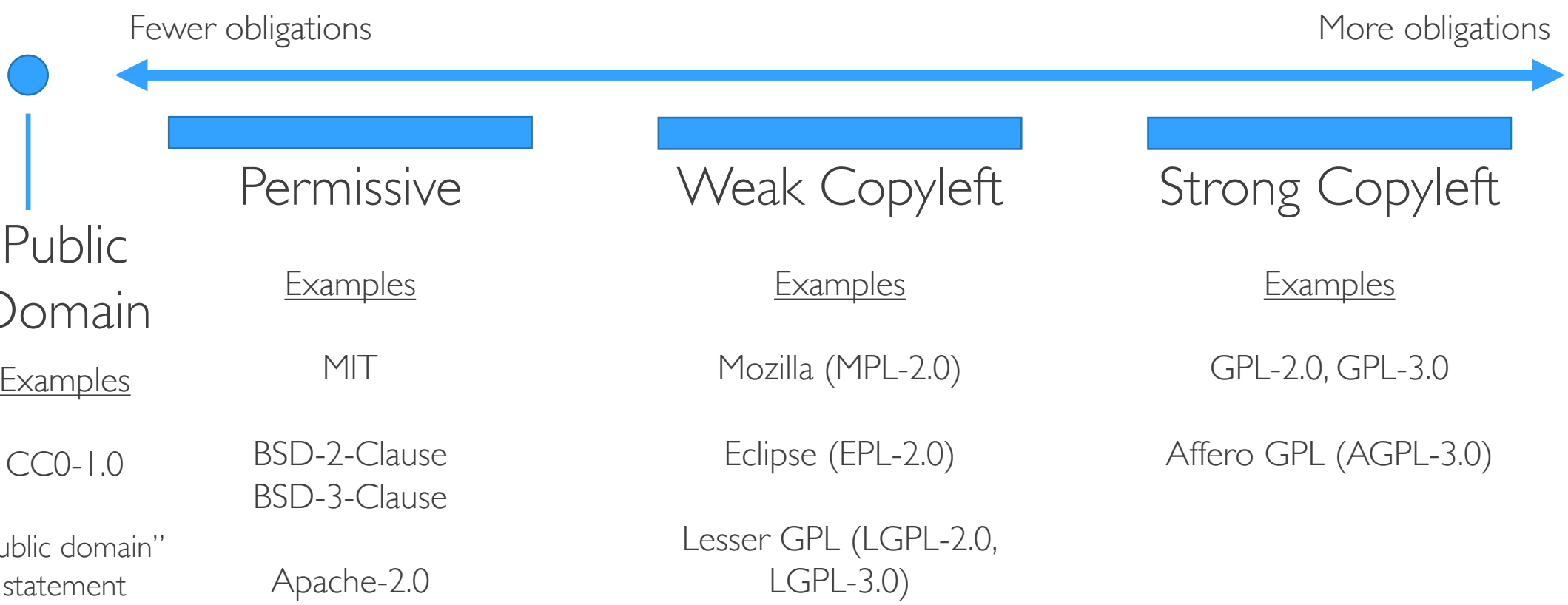


Permissive	Weak Copyleft	Strong Copyleft
Examples	Examples	Examples
MIT	Mozilla (MPL-2.0)	GPL-2.0, GPL-3.0
BSD-2-Clause BSD-3-Clause	Eclipse (EPL-2.0)	Affero GPL (AGPL-3.0)
Apache-2.0	Lesser GPL (LGPL-2.0, LGPL-3.0)	

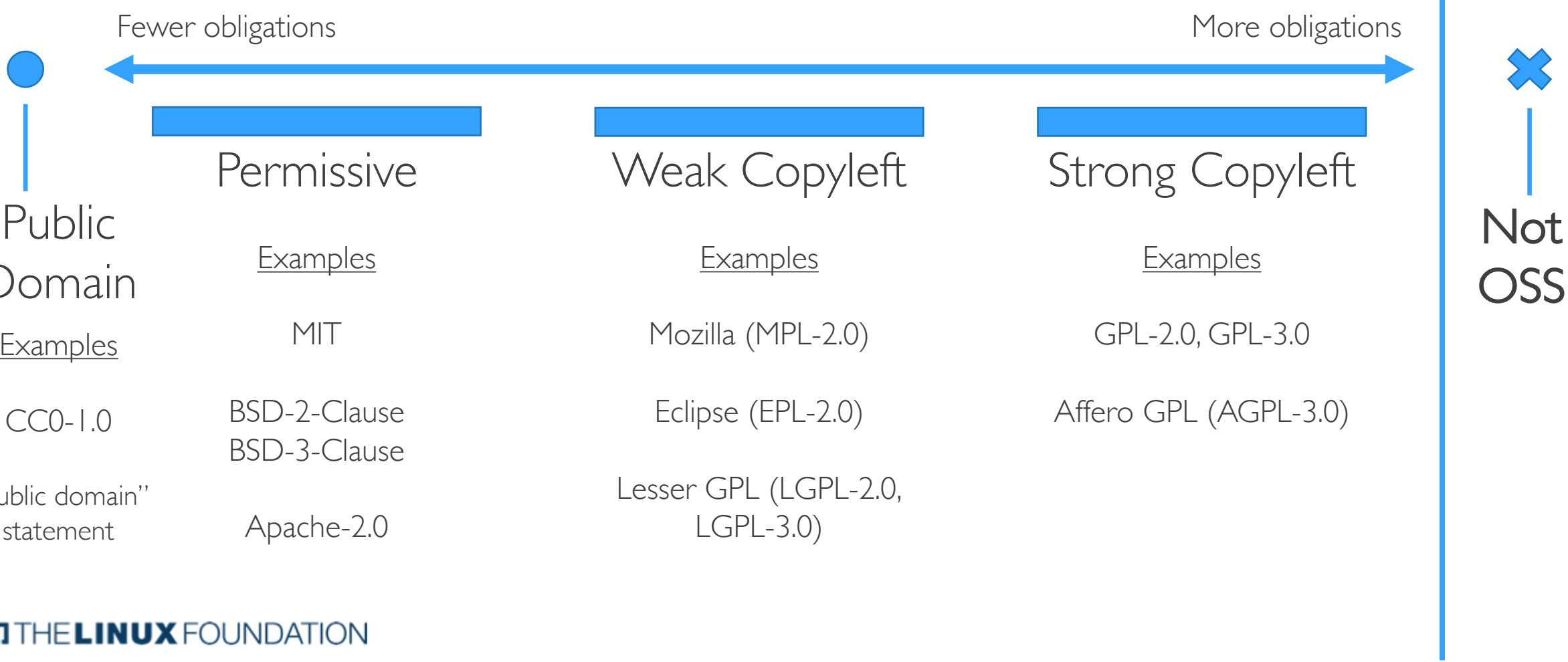
Open Source Licensing: Types



Open Source Licensing: Types



Open Source Licensing: Types



Open Source Licensing: Types

Public Domain

Examples

CC0-1.0

"Public domain" statement

Permissive

Examples

MIT

BSD-2-Clause
BSD-3-Clause

Apache-2.0

Weak Copyleft

Examples

Mozilla (MPL-2.0)

Eclipse (EPL-2.0)

Lesser GPL (LGPL-2.0, LGPL-3.0)

Strong Copyleft

Examples

GPL-2.0, GPL-3.0

Affero GPL (AGPL-3.0)

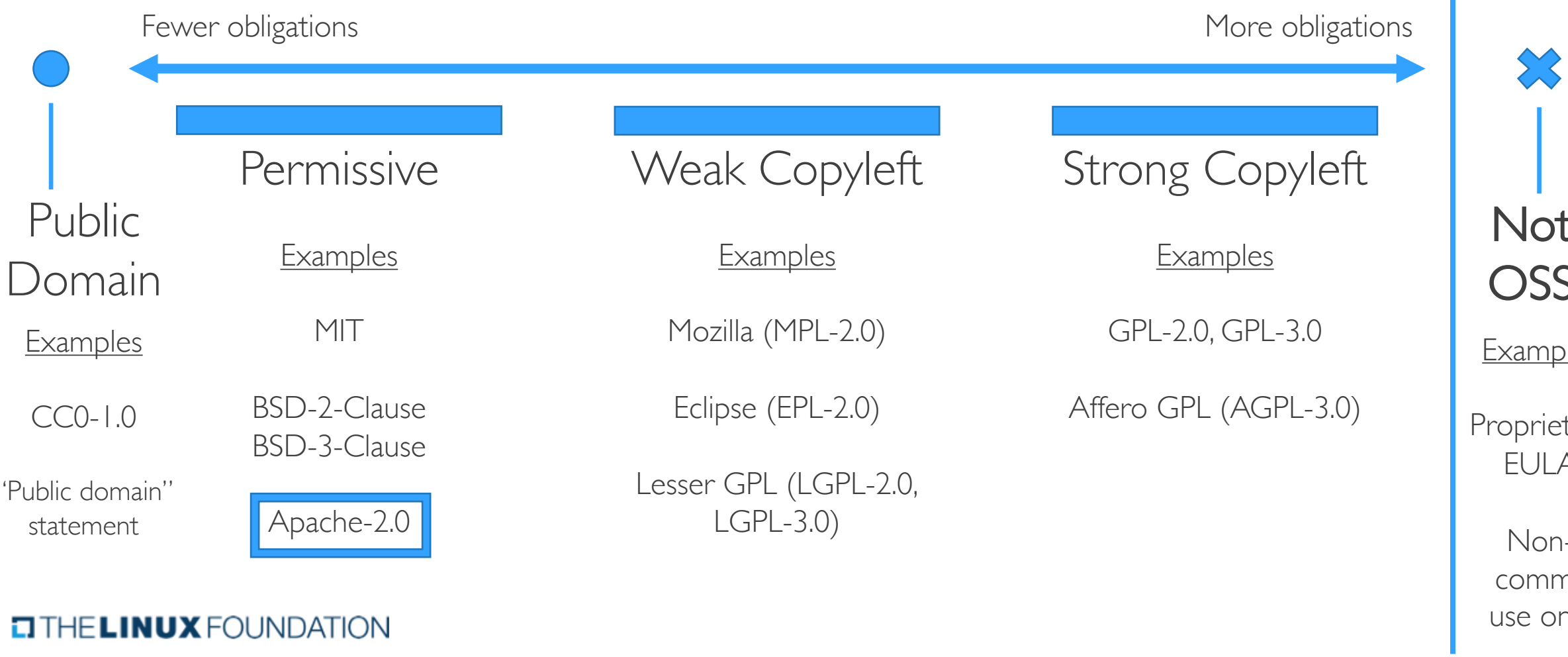
Not OSS

Examples

Proprietary EULA

Non-comm'l use only

Open Source Licensing: Types



Open Source Licensing: Basics

- But – more considerations than just permissive vs. copyleft:
  - Patent licenses?
  - Compatibility?
  - Other obligations? (e.g. advertising clauses; reverse-engineering)

Open Source Licensing: Basics

- Who cares about license compliance?
  - Contributors to the project
  - The project itself
  - Downstream users (expectations and compliance burdens)

Open Source Licensing: In ONAP

- ONAP's IP policy specifies the project's licenses for contributions:
  - Code: Apache License 2.0 (Apache-2.0)
  - Documentation: Creative Commons Attribution 4.0 (CC-BY-4.0)

- Exceptions for use of other licenses:
  - Subject to TSC approval...
  - ...with TSC informed by LF Networking Governing Board's Legal Committee

Open Source Licensing: Contexts

- Within ONAP code base:
  - snippets
  - entire files
- And beyond that – can be relevant for:
  - build-time dependencies (e.g., Java JARs)
  - install-time dependencies (e.g., Python packages)
  - run-time dependencies (e.g., system libraries)

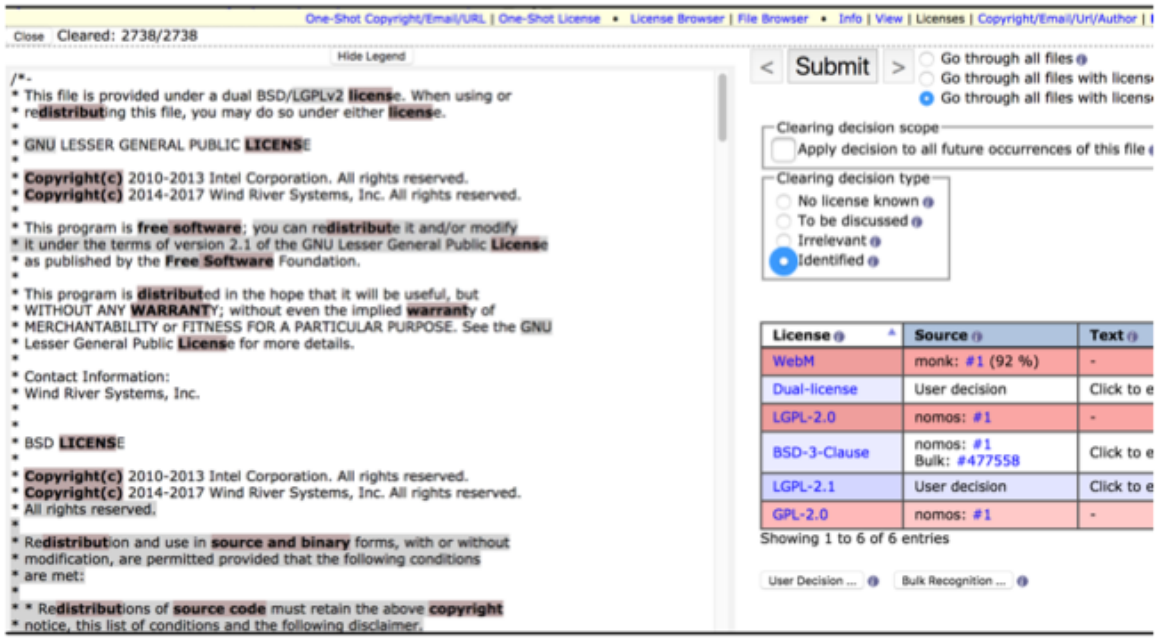
Open Source Licensing: Which license?

- Knowing what license applies isn't easy
  - "**declared**" licenses: LICENSE.txt; package manager metadata
  - "**observed**" licenses: what we find in source files
  - These are often different or incomplete
- Notices in individual files are important

LF License Scans

THE LINUX FOUNDATION

LF License Scans: Tools



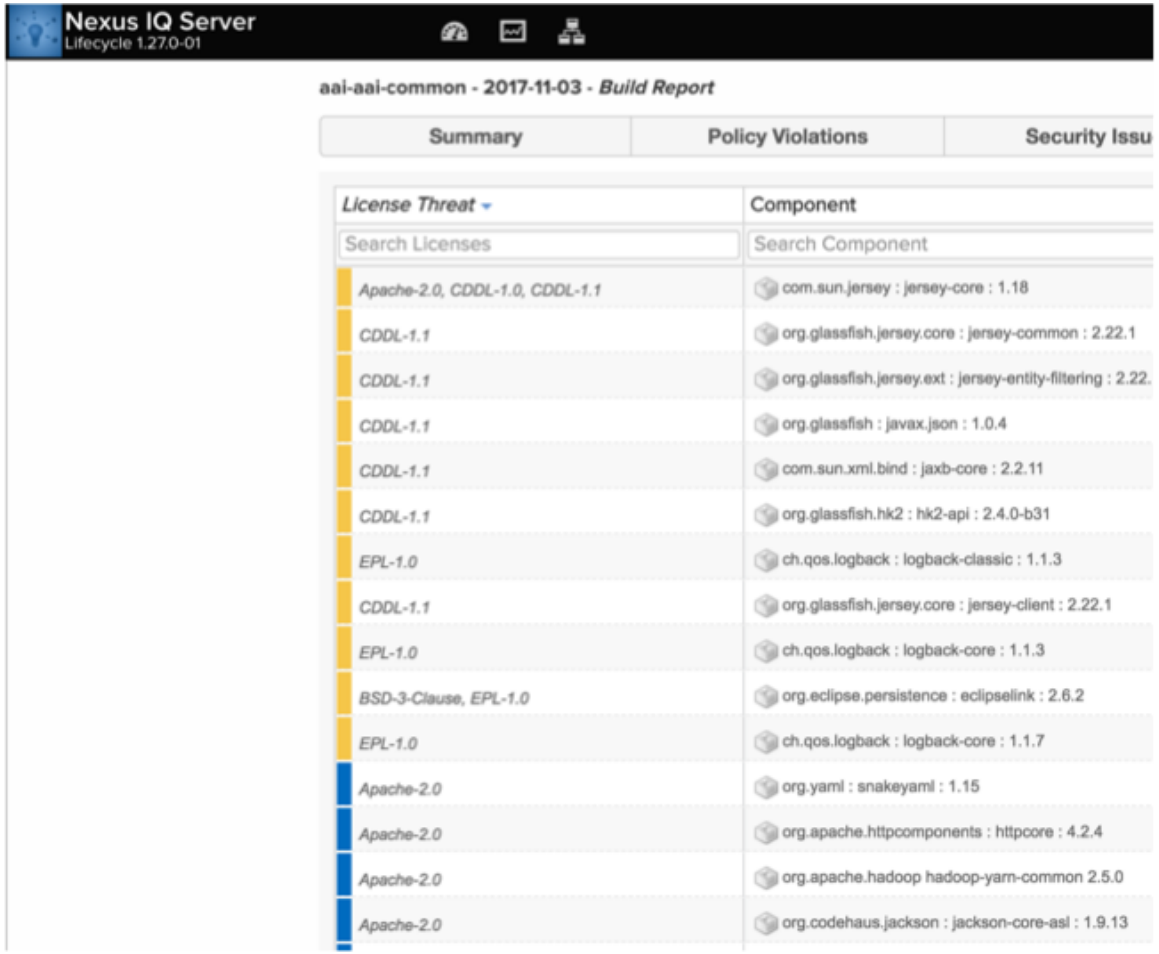
FOSSology

Used to scan a codebase for licenses

Performs textual analysis and regular expression scanning to identify likely license notices and references

Supplemented with manual review to remove false positives and investigate unusual findings

LF License Scans: Tools



Sonatype Nexus IQ

Used to scan Java dependencies imported at build time

Based on Sonatype (Maven) Java artifacts, with declared and observed licenses

Supplemented with manual review and, where appropriate, FOSSology scans of artifacts

LF License Scans: Tools

https://spdx.org

SPDX License List:
https://spdx.org/licenses

SPDX

Used to communicate license information in a standardized, machine-readable format

SPDX documents are produced from each FOSSology source code scan

SPDX short-form identifiers used to enable quickly adding license info to source code with minimal burden

LF License Scans: Reports

License	# of files
Project licenses:	
Apache-2.0	9209
CC-BY-4.0	1
Copyleft:	
(Apache-2.0 OR LGPL-3.0+) AND (GPL-2.0 OR LGPL-3.0+)	1
GPL-2.0 OR LGPL-3.0+	8
LGPL-3.0	4
MPL-2.0	2
Attribution:	
Apache-2.0 AND MIT	1
Apache-2.0 OR LGPL-3.0+	8
BSD-2-Clause	70
BSD-2-Clause AND MIT	1
BSD-3-Clause	25
BSD-3-Clause AND MIT	2
BSD-style	147
ISC	9
MIT	
MIT-style	

File	License
/vendor/github.com/heketi/heketi/LICENSE	(Apache-2.0 OR LGPL-3.0+) AND (GPL-2.0 OR LGPL-3.0+)
/vendor/github.com/heketi/heketi/pkg/utils/bodystring.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/jsonutils.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/log.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/sortedstrings.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/statusgroup.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/stringset.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/stringstack.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/heketi/heketi/pkg/utils/uuid.go	GPL-2.0 OR LGPL-3.0+
/vendor/github.com/juju/ratelimit/LICENSE	LGPL-3.0
/vendor/github.com/juju/ratelimit/ratelimit.go	LGPL-3.0
/vendor/github.com/juju/ratelimit/reader.go	LGPL-3.0
/vendor/gopkg.in/yaml.v2/LICENSE	LGPL-3.0
/vendor/github.com/hashicorp/golang-lru/LICENSE	MPL-2.0
/vendor/github.com/hashicorp/hcl/LICENSE	MPL-2.0

Reports for Developers

Summary and listing of license combinations identified per-file

Calls to discuss situations where remediation may be appropriate

Information gathering to facilitate license exception approvals

LF License Scans: Reports

License	# of files
Project licenses:	
Apache-2.0	19479
Apache-2.0 AND CC-BY-4.0	2285
Apache-2.0 OR EPL-1.0	129
CC-BY-4.0	431
Use restrictions:	
ATT-Proprietary	14
ATT-Proprietary AND Apache-2.0	8
Apache-2.0 AND CC-BY-4.0 AND Olympic-logo-reference	2
Dynamic-Drive-2015	2
bpmn.io License AND Apache-2.0 AND BSD-3-Clause AND MIT	1
Copyleft:	
Apache-2.0 AND (CDDL-1.1 OR GPL-2.0-WITH-classpath-excep	1
Apache-2.0 AND CC-BY-4.0 AND CC-BY-SA-4.0	1
BSD-3-Clause AND EPL-1.0 AND EDL-1.0 AND MIT	2
CC-BY-SA-4.0	1
GPL-2.0 AND Link-exception	3
GPL-3.0+-WITH-OpenSSL-linking-exception	32
LGPL	6
LGPL-3.0 AND Link-exception	3
MIT AND MPL-1.1	7
Attribution:	
(MIT OR GPL-2.0) AND (MIT OR BSD OR GPL)	4
Apache (version unspecified)	2

File	License	Notes
/policy-engine/PolicyEngineClient/src/test/java/org/onap/policyengine/GeneralTestClient.java	ATT-Proprietary AND Apache-2.0	Proprietary notice should be removed, or else file should be removed.
/policy-engine/PolicyEngineClient/src/test/java/org/onap/policyengine/PolicyEngineTestClient.java	ATT-Proprietary AND Apache-2.0	Proprietary notice should be removed, or else file should be removed.
/vvp-portal/vvp/app/welcome/welcome.html	Apache-2.0 AND CC-BY-4.0 AND Olympic-logo-reference	References in footer to "36USC220506" and (c) / trademark ownership by "Intellectual Property" should likely be removed.
/vvp-portal/vvp/dist/welcome/welcome.html	Apache-2.0 AND CC-BY-4.0 AND Olympic-logo-reference	References in footer to "36USC220506" and (c) / trademark ownership by "Intellectual Property" should likely be removed.
/portal-sdk/ecomp-sdk/epsdk-app-overlay/src/main/webapp/static/fusion/raptor/js/ajax_dynamic_content.js	Dynamic-Drive-2015	The license for this Dynamic Drive file (http://www.dynamicdrive.com/notice.htm) may not allow it to be redistributed, so this file should likely be removed and replaced with an alternative.
/usecase-ui/usecaseui-common/src/main/webapp/static/fusion/raptor/js/ajax_dynamic_content.js	Dynamic-Drive-2015	The license for this Dynamic Drive file (http://www.dynamicdrive.com/notice.htm) may not allow it to be redistributed, so this file should likely be removed and replaced with an alternative.
/clamp/src/main/resources/META-INF/resources/designer/index.js	bpmn.io License AND Apache-2.0 AND BSD-3-Clause AND MIT	In mid-2017, the team stated that they would replace the bpmn.io component (which is under a non-OSS license that prohibits certain modifications). This component from bpmn.io was approved for Amsterdam only and should be removed and replaced for Beijing.

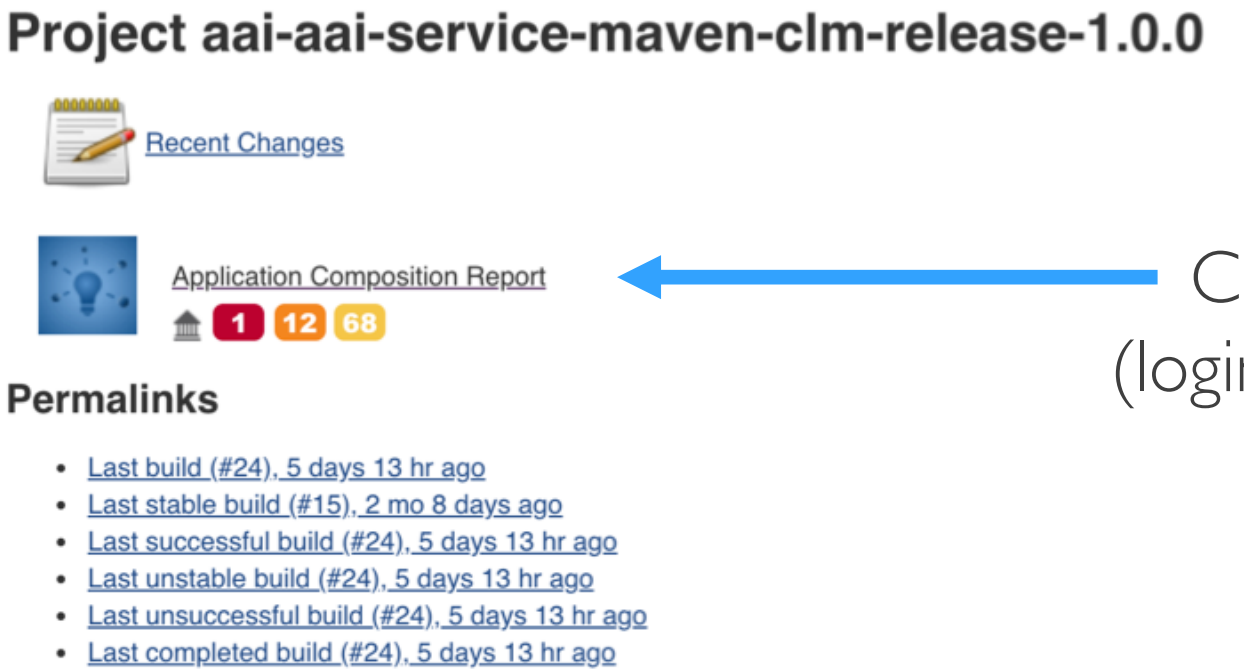
License counts | Project licenses | Use restrictions | Copyleft | Attribution | Other or Unknown

Sonatype Nexus IQ

S	W	Name ↓	Last Success	Last Failure	Last Duration	Policy Violations
		aaf-authz-docker-maven-clm-master	5 days 15 hr - #25	N/A	7 min 3 sec	10 18
		aaf-authz-maven-clm-master	4 days 19 hr - #20	11 days - #19	7 min 26 sec	10 18
		aaf-cadi-maven-clm-master	5 days 6 hr - #19	N/A	5 min 15 sec	5 4
		aaf-inno-maven-clm-master	5 days 11 hr - #18	N/A	2 min 11 sec	2
		aai-aai-common-maven-clm-amsterdam	4 days 21 hr - #9	N/A	12 min	6 38
		aai-aai-common-maven-clm-master	5 days 15 hr - #20	N/A	12 min	6 38
		aai-aai-service-maven-clm-release-1.0.0	5 days 13 hr - #24	N/A	32 min	1 12 68
		aai-babel-maven-clm-master	4 days 17 hr - #22	N/A	6 min 59 sec	12 34
		aai-champ-maven-clm-master	4 days 20 hr - #19	N/A	10 min	Nexus IQ Server error
		aai-data-router-maven-clm-amsterdam	12 days - #8	5 days 3 hr - #9	3 min 30 sec	
		aai-data-router-maven-clm-master	1 mo 10 days - #12	5 days 6 hr - #17	3 min 37 sec	
		aai-esr-gui-maven-clm-amsterdam	4 days 21 hr - #9	N/A	2 min 53 sec	2
		aai-esr-gui-maven-clm-master	5 days 9 hr - #19	8 days 7 hr - #17	3 min 24 sec	1 1
		aai-esr-server-maven-clm-amsterdam	4 days 21 hr - #9	N/A	6 min 30 sec	6 26
		aai-esr-server-maven-clm-master	1 day 13 hr - #25	N/A	6 min 25 sec	4 28
		aai-logging-service-maven-clm-amsterdam	5 days 2 hr - #9	N/A	2 min 24 sec	4

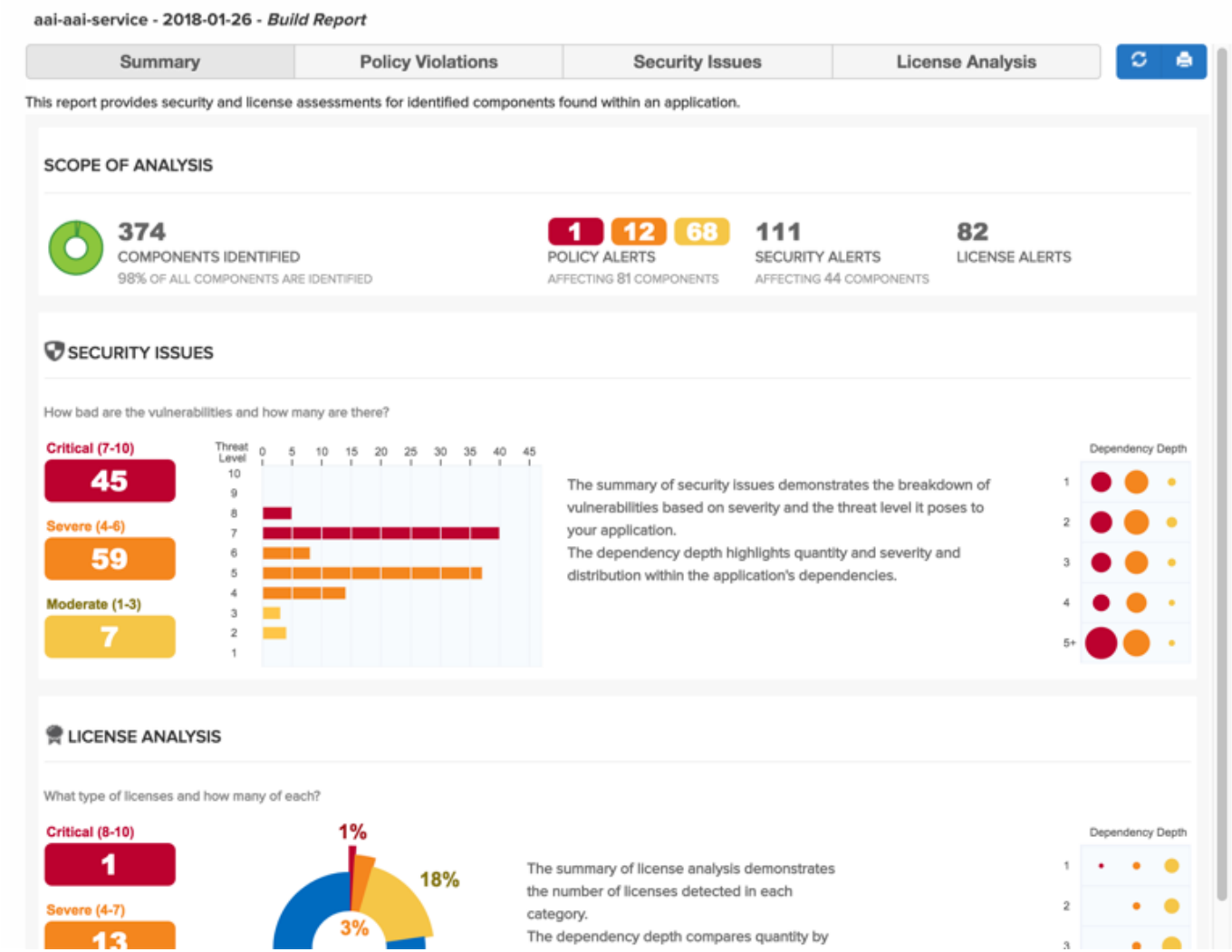
Jenkins view: https://jenkins.onap.org/view/CLM/

Sonatype Nexus IQ

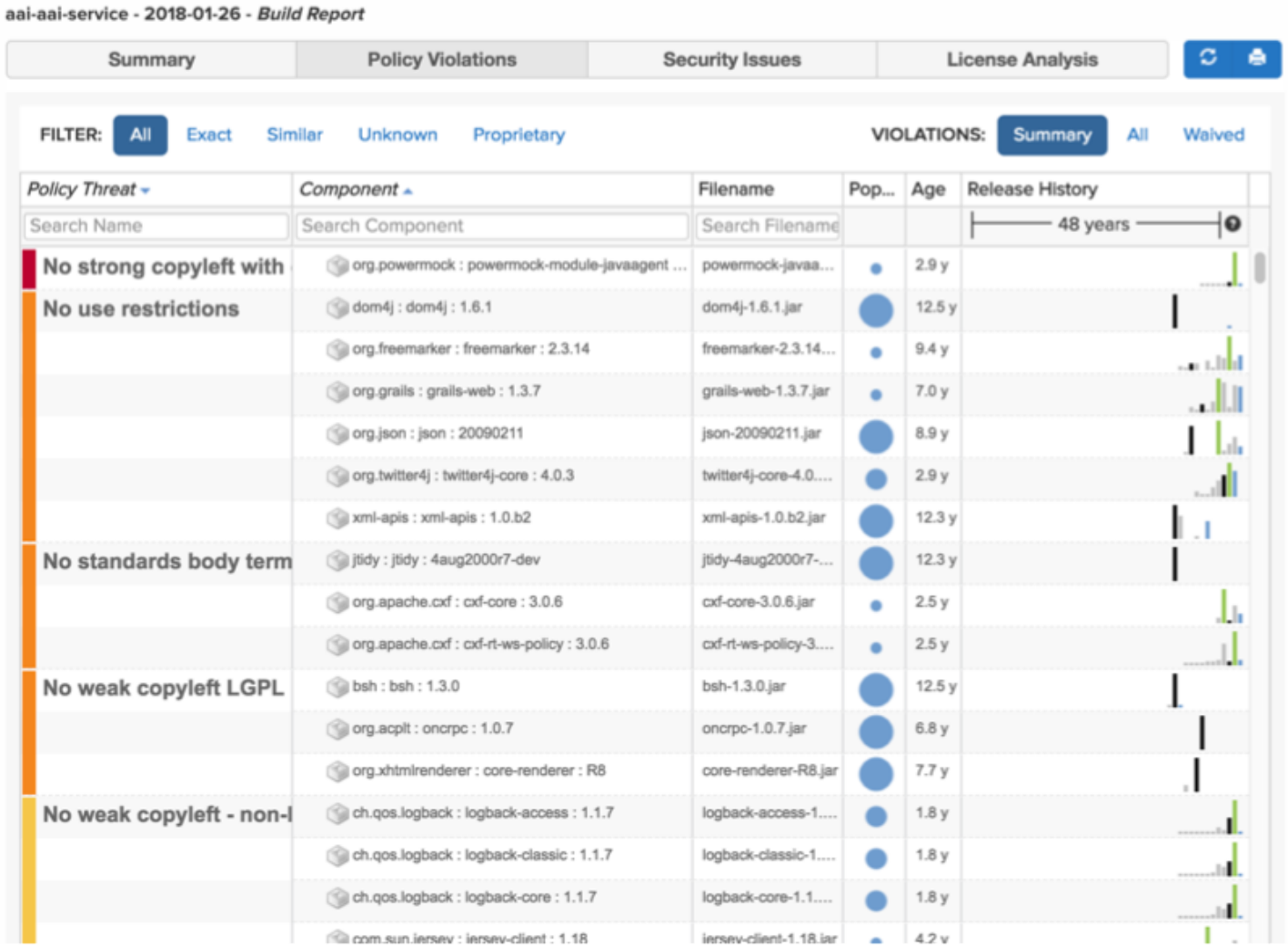


Click here
(login required)

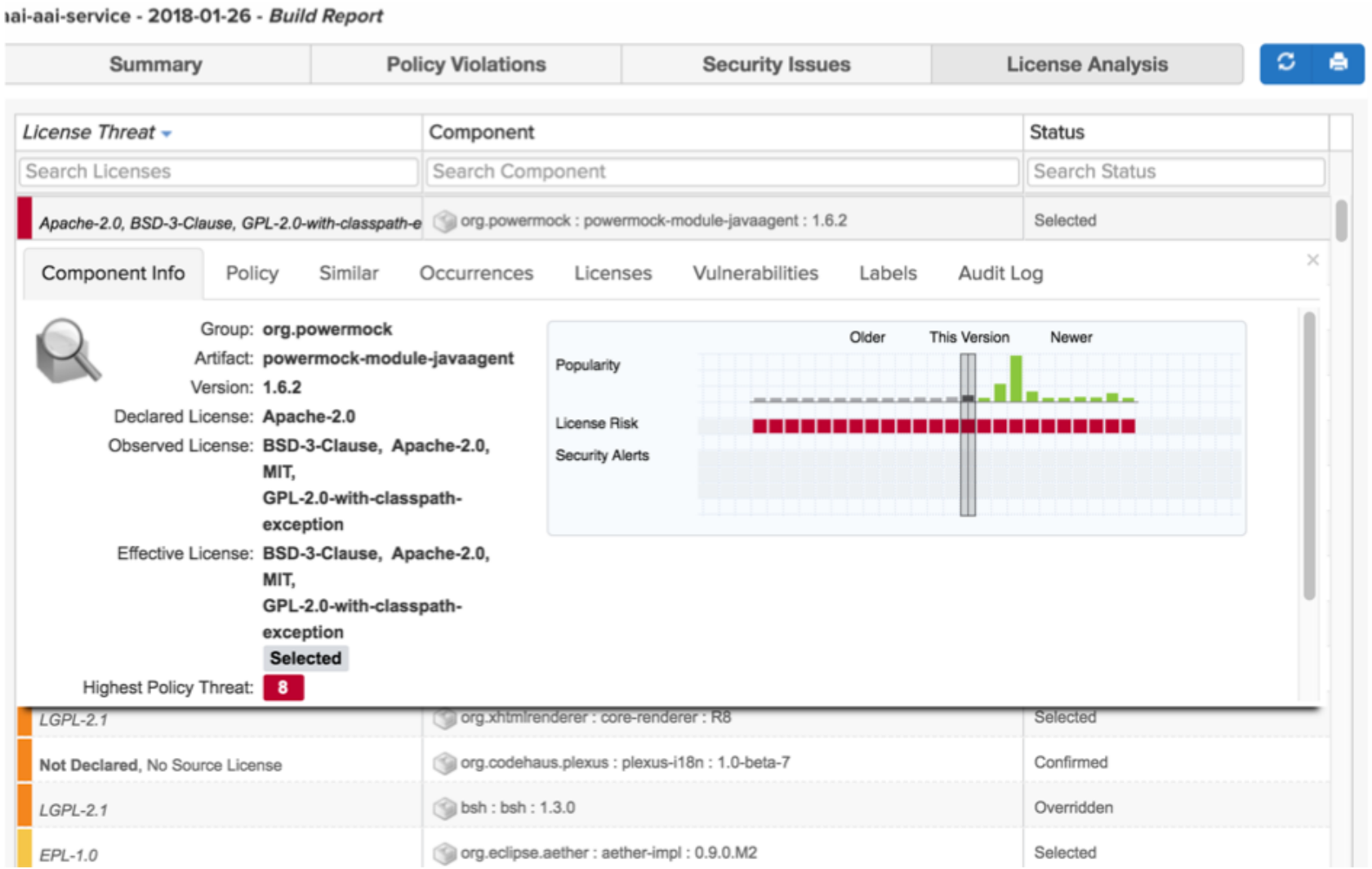
Sonatype Nexus IQ



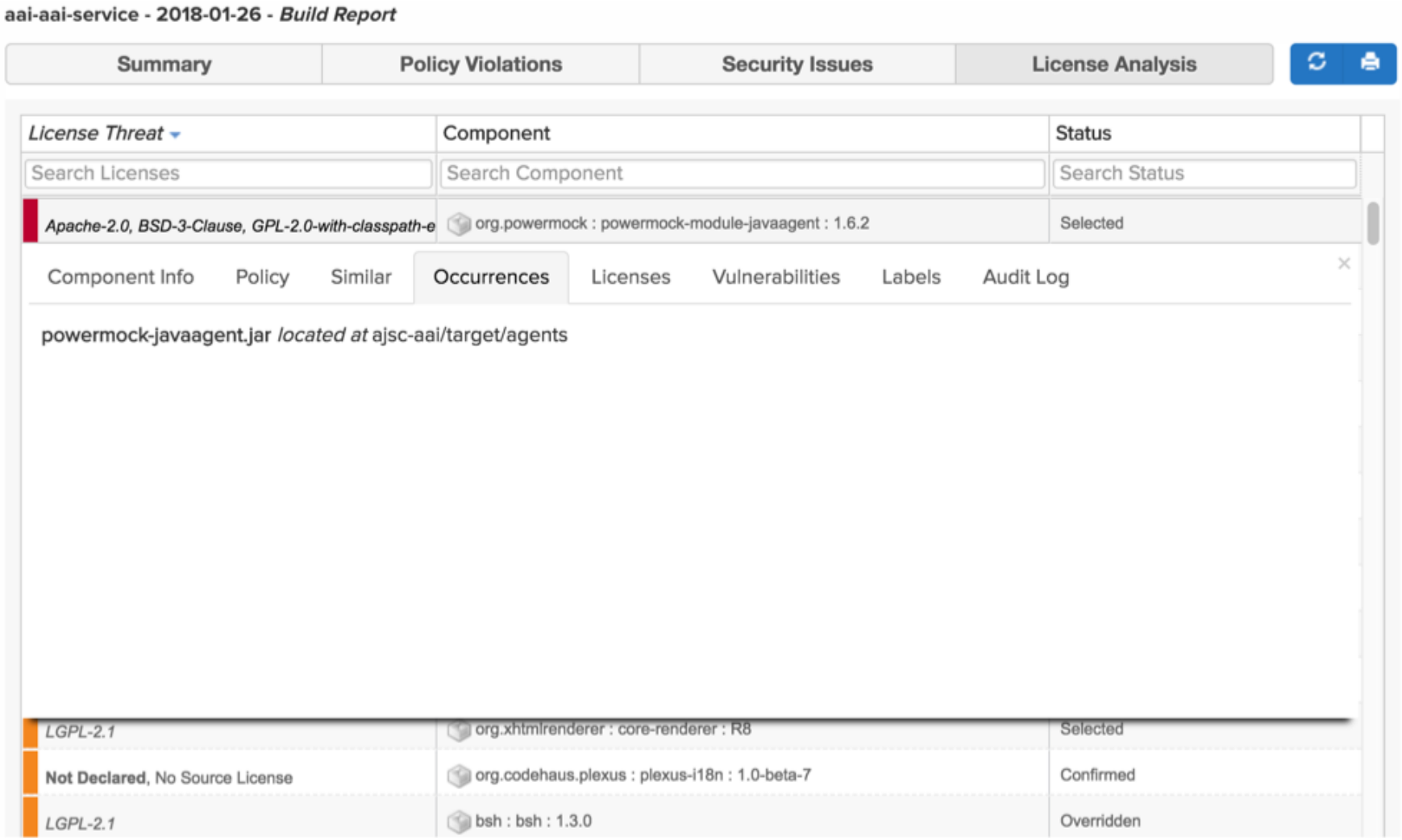
Sonatype Nexus IQ



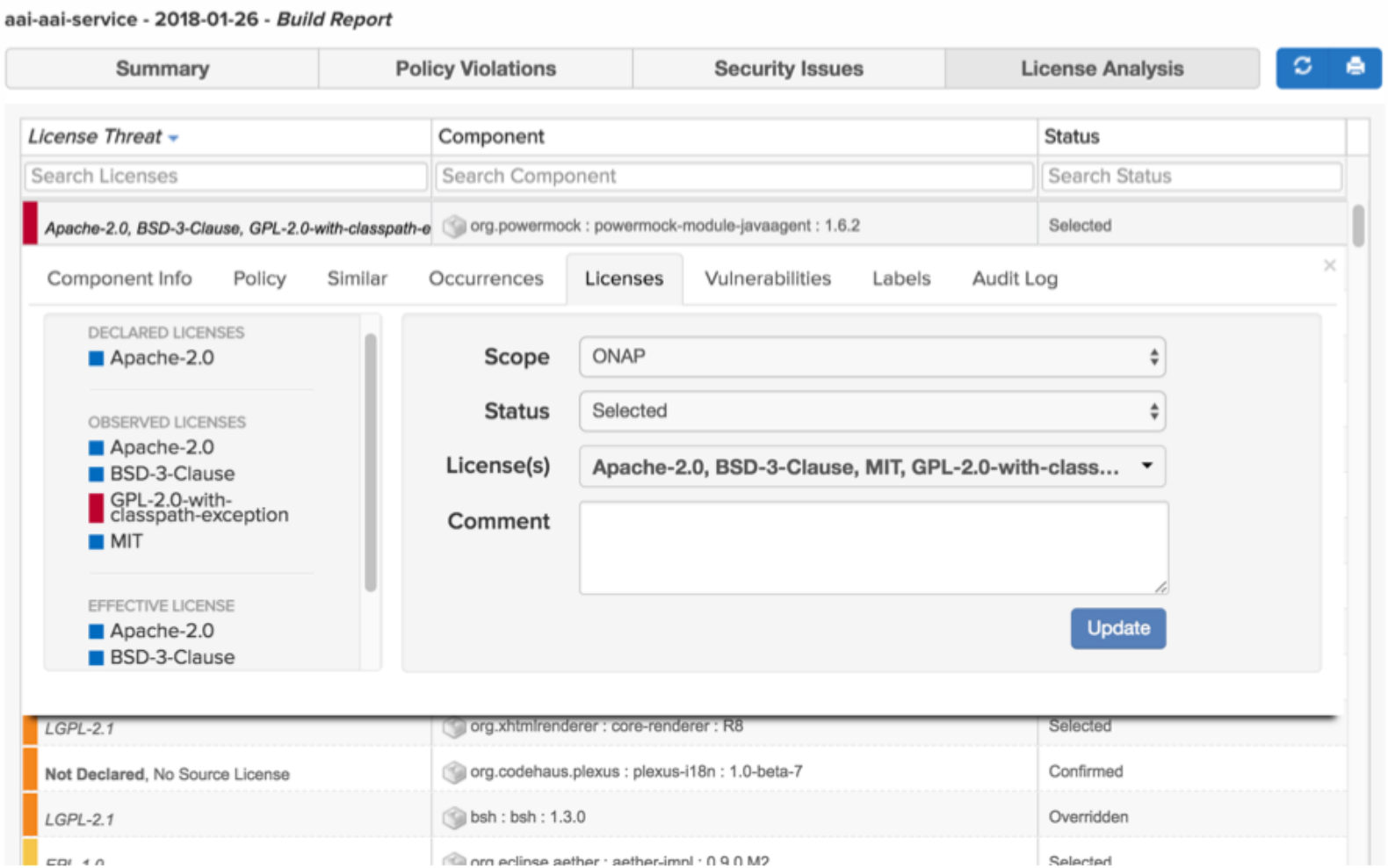
Sonatype Nexus IQ



Sonatype Nexus IQ



Sonatype Nexus IQ



ONAP Processes and Best Practices

THE LINUX FOUNDATION

ONAP: Review monthly reports

- LF will continue to send monthly to PTLs:
  - FOSSology reports (licenses detected within ONAP repos)
  - Nexus IQ reports (licenses detected in build-time JAR dependencies)
- Please review these reports for findings in your repos
- Discuss questions with me (and/or your legal counsel)

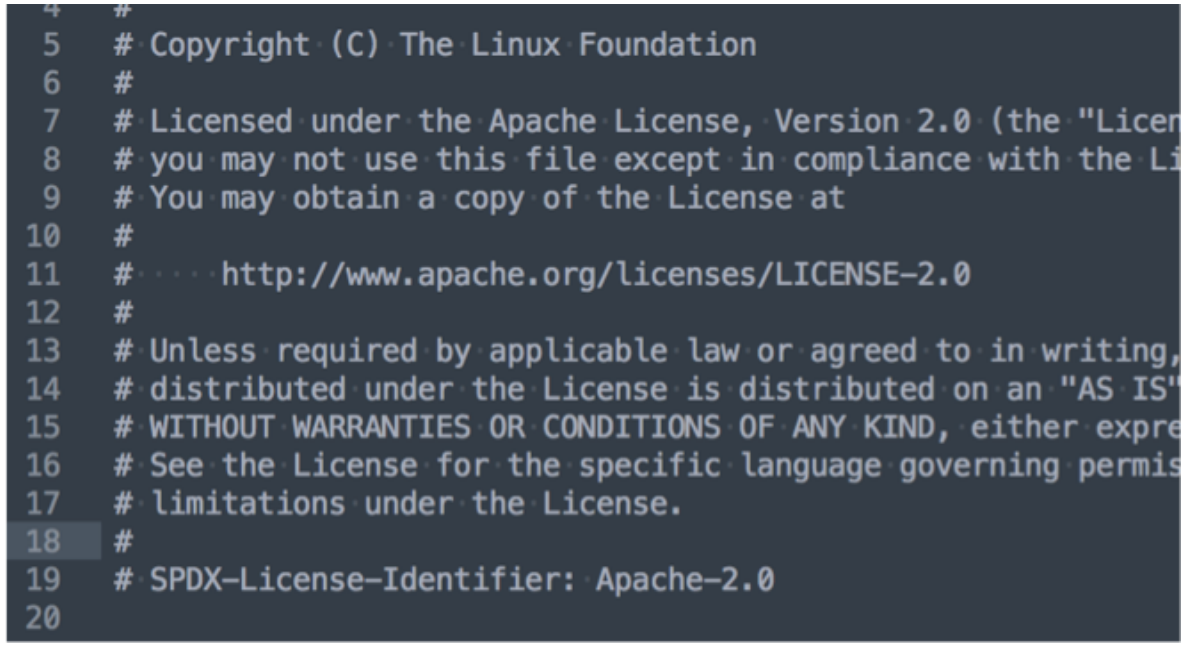
ONAP: License findings

- Remediate (e.g., remove and replace) where possible for high-priority findings:
  - Non-OSS / use restrictions
  - Copyleft (especially strong copyleft)
- Where any non-Apache.2.0, non-CC-BY-4.0 licenses will remain in the project, a license exception approval from the TSC will be required
  - This process is being defined, following transition to LF Networking

ONAP: License notices within individual files

- Different types of notices:
  - Full license text in top-level LICENSE.txt file
  - Copyright notice
  - Standard license headers in each file
  - SPDX short-form IDs in each file

(sample; not from ONAP)



ONAP: License notices within individual files

For files without license notices, we recommend developers add SPDX short-form IDs

Examples:

- For ONAP original code:

```
SPDX-License-Identifier: Apache-2.0
```

- For a file that contains ONAP-original code, together with third-party code under MIT:

```
SPDX-License-Identifier: (Apache-2.0 AND MIT)
```

- For ONAP-original documentation:

```
SPDX-License-Identifier: CC-BY-4.0
```

ONAP: License notices within individual files

Some files can't easily have license notices added.

Examples:

- Image files (.jpeg, .png, ...)
- Structured metadata without comment fields (.json, binary formats)
- Other binary files (e.g. test files)

For these types of files, the best that can easily be done is to rely on the top-level LICENSE.txt notices.

ONAP: Copyright notices within individual files

Many different formats possible; your company / legal counsel may have a preference.

Our recommendation:

```
Copyright (c) [your company name]
```

- It is not typically necessary to include the year
- If the year is present, you can choose to update your own copyright notices when you update the file, but it is not mandatory to do so

ONAP: Things Not to Do

Do NOT:

- Remove or modify a third party's license or copyright notice
- Add a license notice that is incompatible with one already present
  - E.g., don't add an Apache-2.0 notice to a GPL-2.0 file
- Add a reference to Apache-2.0 just to bypass the license checker
- Add third-party code from another source without including its license information

DO:

- If you aren't sure about what's compatible, please ask (and include your legal counsel). There are differences of opinions and no single definition of "compatible."

ONAP: Miscellaneous

- Brand new ONAP repos from existing seed code:
  - We'll run a quick initial scan before upload, looking for major red flags
  - After upload to ONAP repo, will become part of ongoing monthly scans

- Record-keeping for Open Source within repos:
  - Recommend using outputs from scanning process, rather than "Project FOSS" pages (manual updates not occurring)
  - To be discussed with the TSC

An Ongoing Process

- License compliance is a matter of ongoing improvement
  - ...like all aspects of collaborative software development

- Areas of focus will change over time as we improve together
- Focusing on key priorities first

- Reach out with any questions!
  - Steve Winslow: swinslow@linuxfoundation.org
  - your in-house legal counsel (for any legal interpretation questions)

Q&A

THE LINUX FOUNDATION

Contact Us

The Linux Foundation

1 Letterman Drive

Building D, Suite D4700

San Francisco CA 94129

Phone/Fax: +1 415 7239709

www.linuxfoundation.org

General Inquiries

info@linuxfoundation.org

Membership

membership@linuxfoundation.org

Corporate Training

training@linuxfoundation.org

Event Sponsorship

sponsorships@linuxfoundation.org

THE LINUX FOUNDATION

Legal Notices

- The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation's Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.
- Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute's trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.
- Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.
- TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.
- Facebook and the "f" logo are trademarks of Facebook or its affiliates.
- LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.
- YouTube and the YouTube icon are trademarks of YouTube or its affiliates.
- All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.
- The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy. each as may be modified from time to time. More information about The Linux Foundation's policies is available at https://www.linuxfoundation.org.
- Please email legal@linuxfoundation.org with any questions about The Linux Foundation's policies or the notices set forth on this slide.

THE LINUX FOUNDATION