LF NETWORKING

LFN Developer & Testing Forum

LF NETWORKING

LFN Developer & Testing Forum

ONAP SECCOM retrospectives

Pawel Pawlak, Amy Zwarico

Porto, June 14th

Anti-Trust 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/antitrustpolicy. 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

- Log4j fix implementation in Istanbul Maintenance Release
- Jakarta security status update

Log4j story… 1/2

- Log4j related vulnerabilities revealed in December'21 emphasized the challenges in open source supply chain management.
- Upon Security Subcommittee request, ONAP community agreed to reprioritize efforts and develop a dedicated Istanbul Maintenance release that upgraded vulnerable Log4j versions to latest greatest 2.17.1.
- Based on commercial NEXUS IQ tool used in ONAP for Software Composition Analysis (SCA) with weekly Jenkins jobs scans results reports, jira tickets were created for four ONAP projects that were affected with Log4j direct dependencies.
- So how did it go? The individual projects were efficient at upgrading to log4j 2.17.1 and one project was able to remove a vulnerable repository from the release because its functionality was no longer needed.
- Unfortunately, there were delays. It took some time for ONAP Operations Manager project to merge the code.
- Furthermore, while waiting for the merge, we observed a major failure in CI/CD automation pipeline causing problem with SCA reports generation. It took 19 days plus escalations for LFN IT to solve the problem. In the end we were able to use the final scan output to show that none of the ONAP projects had log4j direct dependencies.

Log4j story… 2/2

- The project teams discovered false positives in the Nexus IQ output, labeling some transitive dependencies as direct. These were manually whitelisted, and a ticket was opened with Sonatype, the Nexus IQ vendor, to address the false positives.
- The dependency inherited from OpenDayLight (ODL), an LFN project used in two ONAP projects, had to be resolved by ONAP developers because the ODL version with the log4j fix was delivered too late for the ONAP release.
- The final step was for each project to document the fixes and transitive dependencies in the Release Notes. Creating documentation jira tickets for each project was helpful in tracking progress. The Istanbul Maintenance release was publicly available end of March'22…
- Could we make it faster?
  - **with SBOM in place** we would know easily which projects are using directly log4j, faster merge and faster resolution of failing SCA scan jobs would definitely speed up the final check, and more focus on documentation would make us release faster as well. Last but not least, having an automated repo upgrade process in place would solve the issue "on the fly"... We learn, we adjust, we improve.

Jakarta security status update – GR 1/4

- REQ-1067 COMPLETION OF PYTHON LANGUAGE UPDATE (v2.7 → v3.8) link to scan

No	Project's jira	Status	Comment
1	VFC-1915	Closed	Merge done
2	VFC-1914	Closed	Filebeat related
3	DCAEGEN2-3020	Closed	Cloudify components migrated to Python 3.6
4	OOM-2900	Open	Cassandra
5	INT-2034	Open	Robot

Jakarta security status update – GR 2/4

- REQ-1068 COMPLETION OF JAVA LANGUAGE UPDATE (v8 → v11) – link to scan

No	Project’s jira	Status	Comment
1	AAI-3413	closed	Exceptions: java 8 due to the janusgraph dependency
2	DCAEGEN2-3019	closed	Exceptions: upstream NIFI base images are still built on java8
3	SDNC-1651	closed	Fixed in Istanbul
			Cassandra – upstream container
			Umaintained: message-router, msb-discovery, msb-eag, msb-iag
			srimzi-zk-entrance – OOM related

Jakarta security status update – GR 3/4

LFN Developer & Testing Forum

- REQ-1066 CONTINUATION OF PACKAGES UPGRADES IN DIRECT DEPENDENCIES
  - 299 recommended package upgrades
  - 73% of upgrades completed or requested waiver
    - 179 completed (60%)
    - 38 waivers requested and recommended (13%)
  - 82 updates not addressed
    - 4 projects did zero updates
    - 1 large project completed about half the updates

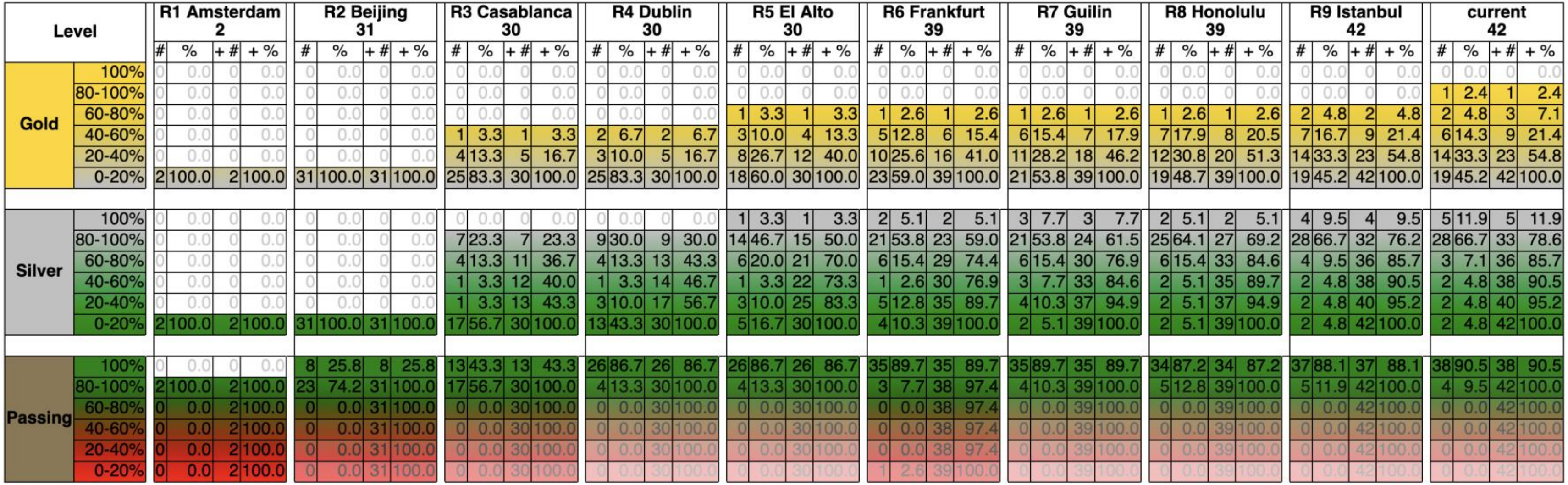
Jakarta security status update – GR 4/4

LF NETWORKING
LFN Developer & Testing Forum

REQ-1069 CONTINUATION OF CII BADGING SCORE IMPROVEMENTS FOR SILVER LEVEL

- Improvements in Passing, Silver and progress to Gold
- Top five projects (50-83% towards Gold Badge): DCAE Runtime, Policy, DCAE, VVP and CPS

Release Statistics



Level		R1 Amsterdam 2				R2 Beijing 31				R3 Casablanca 30				R4 Dublin 30				R5 El Alto 30			
		#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %
Gold	100%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	80-100%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	60-80%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	3.3	1	3.3
	40-60%	0	0.0	0	0.0	0	0.0	0	0.0	1	3.3	1	3.3	2	6.7	2	6.7	3	10.0	4	13.3
	20-40%	0	0.0	0	0.0	0	0.0	0	0.0	4	13.3	5	16.7	3	10.0	5	16.7	8	26.7	12	40.0
	0-20%	2	100.0	2	100.0	31	100.0	31	100.0	25	83.3	30	100.0	25	83.3	30	100.0	18	60.0	30	100.0
Silver	100%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	3.3	1	3.3
	80-100%	0	0.0	0	0.0	0	0.0	0	0.0	7	23.3	7	23.3	9	30.0	9	30.0	14	46.7	15	50.0
	60-80%	0	0.0	0	0.0	0	0.0	0	0.0	4	13.3	11	36.7	4	13.3	13	43.3	6	20.0	21	70.0
	40-60%	0	0.0	0	0.0	0	0.0	0	0.0	1	3.3	12	40.0	1	3.3	14	46.7	1	3.3	22	73.3
	20-40%	0	0.0	0	0.0	0	0.0	0	0.0	1	3.3	13	43.3	3	10.0	17	56.7	3	10.0	25	83.3
	0-20%	2	100.0	2	100.0	31	100.0	31	100.0	17	56.7	30	100.0	13	43.3	30	100.0	5	16.7	30	100.0
Passing	100%	0	0.0	0	0.0	8	25.8	8	25.8	13	43.3	13	43.3	26	86.7	26	86.7	26	86.7	26	86.7
	80-100%	2	100.0	2	100.0	23	74.2	31	100.0	17	56.7	30	100.0	4	13.3	30	100.0	4	13.3	30	100.0
	60-80%	0	0.0	2	100.0	0	0.0	31	100.0	0	0.0	30	100.0	0	0.0	30	100.0	0	0.0	30	100.0
	40-60%	0	0.0	2	100.0	0	0.0	31	100.0	0	0.0	30	100.0	0	0.0	30	100.0	0	0.0	30	100.0
	20-40%	0	0.0	2	100.0	0	0.0	31	100.0	0	0.0	30	100.0	0	0.0	30	100.0	0	0.0	30	100.0
	0-20%	0	0.0	2	100.0	0	0.0	31	100.0	0	0.0	30	100.0	0	0.0	30	100.0	0	0.0	30	100.0

Level		R6 Frankfurt 39				R7 Guilin 39				R8 Honolulu 39				R9 Istanbul 42				current 42			
		#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %	#	%	+ #	+ %
Gold	100%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	80-100%	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	2.4	1	2.4
	60-80%	1	2.6	1	2.6	1	2.6	1	2.6	1	2.6	1	2.6	2	4.8	2	4.8	2	4.8	3	7.1
	40-60%	5	12.8	6	15.4	6	15.4	7	17.9	7	17.9	8	20.5	7	16.7	9	21.4	6	14.3	9	21.4
	20-40%	10	25.6	16	41.0	11	28.2	18	46.2	12	30.8	20	51.3	14	33.3	23	54.8	14	33.3	23	54.8
	0-20%	23	59.0	39	100.0	21	53.8	39	100.0	19	48.7	39	100.0	19	45.2	42	100.0	19	45.2	42	100.0
Silver	100%	2	5.1	2	5.1	3	7.7	3	7.7	2	5.1	2	5.1	4	9.5	4	9.5	5	11.9	5	11.9
	80-100%	21	53.8	23	59.0	21	53.8	24	61.5	25	64.1	27	69.2	28	66.7	32	76.2	28	66.7	33	78.6
	60-80%	6	15.4	29	74.4	6	15.4	30	76.9	6	15.4	33	84.6	4	9.5	36	85.7	3	7.1	36	85.7
	40-60%	1	2.6	30	76.9	3	7.7	33	84.6	2	5.1	35	89.7	2	4.8	38	90.5	2	4.8	38	90.5
	20-40%	5	12.8	35	89.7	4	10.3	37	94.9	2	5.1	37	94.9	2	4.8	40	95.2	2	4.8	40	95.2
	0-20%	4	10.3	39	100.0	2	5.1	39	100.0	2	5.1	39	100.0	2	4.8	42	100.0	2	4.8	42	100.0
Passing	100%	35	89.7	35	89.7	35	89.7	35	89.7	34	87.2	34	87.2	37	88.1	37	88.1	38	90.5	38	90.5
	80-100%	3	7.7	38	97.4	4	10.3	39	100.0	5	12.8	39	100.0	5	11.9	42	100.0	4	9.5	42	100.0
	60-80%	0	0.0	38	97.4	0	0.0	39	100.0	0	0.0	39	100.0	0	0.0	42	100.0	0	0.0	42	100.0
	40-60%	0	0.0	38	97.4	0	0.0	39	100.0	0	0.0	39	100.0	0	0.0	42	100.0	0	0.0	42	100.0
	20-40%	0	0.0	38	97.4	0	0.0	39	100.0	0	0.0	39	100.0	0	0.0	42	100.0	0	0.0	42	100.0
	0-20%	1	2.6	39	100.0	0	0.0	39	100.0	0	0.0	39	100.0	0	0.0	42	100.0	0	0.0	42	100.0

Jakarta security status update – improvements

- RACI chart for unmaintained projects
  - proposed process related to technical debt
- Automating the process to mitigate security threats quicker
  - Removed a lot of manual work, saved a lot of time

LF
NETWORKING

LFN Developer & Testing Forum