LFNETWORKING
Developer & Testing Forum

ONAP SECCOM activities in London release

Pawel Pawlak, F5
Amy Zwarico, AT&T

https://lfnetworking.org

Agenda

LFN Developer & Testing Forum

- London Global Requirements and Best Practices review
- Recent achievements
- Major issues
- What is new
- Q&A

LF NETWORKING

LFN Developer & Testing Forum

SECCOM
London Requirements

SECCOM London Requirements

LFN NETWORKING
LFN Developer & Testing Forum

- Existing Global Requirements
  - Epic REQ-437: COMPLETION OF PYTHON LANGUAGE UPDATE (v2.7 → v3.8)
    - London Task: REQ-1208 ,
    - On horizon: New python version: 3.11
  - Epic REQ-438: COMPLETION OF JAVA LANGUAGE UPDATE (v8 → v11)
    - London Task: REQ-1209
    - On horizon: New Java version: 17
  - Epic REQ-439: CONTINUATION OF PACKAGES UPGRADES IN DIRECT DEPENDENCIES
    - London Task: REQ-1211
    - Projects progressing: CPS – done!, DCAE – WIP, DMaaP – WIP
    - The log4j, jackson-databind are good examples of package upgrades
  - Epic REQ-443: CONTINUATION OF CII BADGING SCORE IMPROVEMENTS FOR SILVER LEVEL
    - London Task: REQ-1210
- London recommended versions:
  - https://wiki.onap.org/display/DW/Database%2C+Java%2C+Python%2C+Docker%2C+Kubernetes%2C+and+Image+Versions

SECCOM London Requirements

LFN Developer & Testing Forum

- Proposed Global Requirements
  - Epic REQ-1072: Standardized logging fields
    - London Task: REQ-1341 Standardized logging fields – Java London release
  - **Epic REQ-1342: Retirement of unmaintained repos**
    - **London Task:** REQ-1343 Retirement of unmaintained repos London release
    - **SECCOM and Architecture developed process for retiring unmaintained repos**
      - **Unmaintained repo process wiki: https://wiki.onap.org/display/DW/Project+State%3A+Unmaintained**
      - **Link to unmaintained repo list: https://wiki.onap.org/display/DW/London+Unmaintained+Repo+Resolution+Activity**
      - **Gerrit query to get json formatted read only repo list: GET** https://gerrit.onap.org/r/projects/?state=READ_ONLY
    - **Process reviewed with PTLs and TSC and updated with feedback**
    - **POC in Kohn tested successfully**
    - **Best Practice does not apply because no new repos/code will be Unmaintained: not touched in at least 2 releases**
    - **Request approved by TSC that Retirement of unmaintained repos is promoted from POC to Global Requirement**

SECCOM London Requirements

LFN Developer & Testing Forum

- Best Practice
  - Epic REQ-1073: Using basic images from Integration
    - no progress in Jakarta, Kohn
    - London task: REQ-1348 Using basic image from Integration - London Release
  - Epic REQ-1346: Software BOMs – Informing TSC
    - no impact on pipeline
    - London task: REQ-1347 Software BOMs London release
    - SBOM versioning issue under investigation: https://jira.linuxfoundation.org/browse/RELENG-4472
- PoC
  - Epic REQ-441: LOGS MANAGEMENT - PHASE 1: COMMON PLACE FOR DATA
    - POC in Jakarta, Kohn – no progress
    - Identifying resources to implement
    - London task: REQ-1344 LOGS MANAGEMENT - PHASE 1: COMMON PLACE FOR DATA - LONDON RELEASE
  - NEW: Epic REQ-1072: Standardized logging fields
    - London task: REQ-1345 SECURITY LOGS FIELDS – Python - PoC

LF NETWORKING

LFN Developer & Testing Forum

Recent Achievements

SBOMs

- SBOMs generated for each ONAP project?
  - Stretched goal due to some unmaintained projects
- Sharing SBOMs idea across LFN community
  - Already presented to LFN Board and LFN TAC
  - Community Support
  - ONAP and ODL already impelmented
  - Strong suport for LFN wide required CI/CD

Unmaintained Projects Management

LFN Developer & Testing Forum

Goals

- Remove unmaintained projects from future ONAP releases
- Remove unmaintained repos and containers from future ONAP releases

Why

- Reduces the complexity of ONAP
- Improves the security and reliability of ONAP by removing code that is not maintained
- Improves the security by removing code and packages with vulnerabilities

How

- Candidates
- Projects with no PTLs
- Repos with no merges in over 12 months (programmatically identified via Jenkins APIs)

Next steps

- Is it needed
  - Is the image used by the project?
  - Is the image used by any other project?
  - What is the repo associated with the image or component?
  - Does the repo contain anything else that is still in use within the project, or anywhere in ONAP?
- Remove or find PTL
  - Needed repos: find a committer & plan retirement of repos (TSC)
  - Unneeded repos: remove from Jenkins (LFIT)

https://wiki.onap.org/display/DW/Unmaintained+Projects+Taskforce

Logging

- Architecture
  - Log generation
  - Collection
  - Sharing
- App logging at node vs. pod level
- Proof of Concept Projects

5 Year Security Review Questionnaire

- Required by charter
- Continous Improvement
- Review completed for DCAE pioneer !
- Review ongoing for CPS

Major Issues

Issues

Projects Are Short On Resources!

- Poor progress for packages upgrades
- Still some projects running old Python or Java
- Recurring waiver requests for more than 2-3 releases
- No weekly scans assured by Integration Team

LFN NETWORKING

LFN Developer & Testing Forum

New Initiatives

Signing Artifacts

- SBOMs
- Image Signing
- LF existing tool vs. Sigstore

Service Mesh

- Super important initiative led by Andreas
- We remove AAF dependencies
- We get better control over ONAP communication

- Please join dedicated session: today at 6:30 PM CET

LFN NETWORKING

LFN Developer & Testing Forum

Thank you!