Platform Maturity (S3P) Casablanca Proposal

Jason Hunt

June 21, 2018

Proposed Requirement Level Definition – Security

Project-level requirements

- Level 0: None
- Level 1: CII Passing badge
  - *Including no critical and high known vulnerabilities > 60 days old*
- Level 2: CII Silver badge, plus:
  - All internal/external system communications shall be able to be encrypted.
  - All internal/external service calls shall have common role-based access control and authorization using CADI framework.
- Level 3: CII Gold badge

ONAP Platform-level requirements per release

- Level 1: 70 % of the projects passing the level 1
  - with the non-passing projects reaching 80% passing level
  - Non-passing projects MUST pass specific cryptography criteria outlined by the Security Subcommittee*
- Level 2: 70 % of the projects passing silver
  - with non-silver projects:
    - completed passing level and 80% towards silver level
    - internal/external system communications shall be able to be encrypted.
- Level 3: 70% of the projects passing gold
  - with non-gold projects achieving silver level and achieving 80% towards gold level
- Level 4: 100 % passing gold.

Recommended Security Levels

Area	Priority	Min. Level	Stretch Goal	Level Description (abbreviated)
Security	High	~~**Platform Level 1**~~ **Absolute Minimum expectation:** • CII badging passing level • Continuously retaining no critical or high known vulnerabilities > 60 days old • All communication shall be able to be encrypted and have common role-based access control and authorization. Desired expectation is full CII badging silver level, if not 75% towards that.	Project Level 2	•1 – 70% pass level 1 (CII Passing plus more) •2 – 70% pass CII Silver (plus more) •3 – 70% pass CII Gold (plus more) •4 – 100% pass CII Gold

Recommended Performance Levels

Performance

- **Level 0:** no performance testing done
- **Level 1:** baseline performance criteria identified and measured (such as response time, transaction/message rate, latency, footprint, etc. to be defined on per component)
- **Level 2:** performance improvement plan created ~~& implemented for 1 release (improvement measured for equivalent functionality & equivalent hardware~~)
- **Level 3:** performance improvement plan implemented for ~~2~~ 1 ~~consecutive~~ release (improvement measured for equivalent functionality & equivalent hardware)

Area	Priority	Min. Level	Stretch Goal	Level Descriptions (abbreviated)
Performance	~~Low~~/Med	~~Level 1~~ **Level 2** – closed-loop projects **Level 0** – remaining projects	**Level 1** – remaining	•0 -- none •1 -- baseline performance criteria identified and measured •2 & 3 – performance improvement plans created & implemented

Recommended Platform Maturity Levels for Casablanca

Area	Priority	Min. Level	Stretch Goal	Level Descriptions (abbreviated)
Stability	Medium	~~**Level 1**~~ **Level 2**		•0 -- none •1 – 72 hour component level soak w/random transactions •2 – 72 hour platform level soak w/random transactions •3 – 6 month track record of reduced defect rate
Resiliency	High	**Level 2** – run-time projects **Level 1** – remaining projects	**Level 3** – run-time projects **Level 2** – remaining projects	•0 -- none •1 – manual failure and recovery (< 30 minutes) •2 – automated detection and recovery (single site) •3 – automated detection and recovery (geo redundancy)
Scalability	Low	**Level 1** – run-time projects **Level 0** – remaining projects	**Level 1**	•0 – no ability to scale •1 – single site horizontal scaling •2 – geographic scaling •3 – scaling across multiple ONAP instances

Proposed Requirement Level Definition – Manageability

Manageability

- **Level 1:**
  - All ONAP components will use a single logging system.
  - Instantiation of a simple ONAP system should be accomplished in <1 hour with a minimal footprint
- **Level 2:**
  - A component can be independently upgraded without impacting operation interacting components
  - ~~Transaction tracing across components~~
  - Component configuration to be externalized in a common fashion across ONAP projects
  - All application logging to adhere to ONAP Application Logging Specification v1.2
- **Level 3:**
  - Transaction tracing across components

Area	Priority	Min. Level	Stretch Goal	Level Descriptions (abbreviated)
Manageability	High	~~Level 1~~ Level 2	Level 3	•1 – single logging system across components; instantiation in < 1 hour •2 – ability to upgrade a single component; externalized configuration management; adhere to application logging spec V1.2 •3 - tracing across components;

Proposed Requirement Level Definition – Usability

- **Level 1**
  - User guide created
  - Deployment documentation
  - API documentation
  - Adherence to coding guidelines
- **Level 2**
  - API Documentation
    - All new API's must adhere to the ONAP API Common Versioning Strategy and Documentation Guidelines; All existing APIs must be documented in Swagger 2.0
  - ~~Consistent UI across ONAP projects~~
  - ~~Usability testing conducted~~
  - Projects contribute to end-to-end tutorials
- **Level 3**
  - Consistent UI across ONAP projects
  - Usability testing conducted
  - API Documentation
    - All new API's, all external APIs, and all existing API's that are modified must adhere to the ONAP API Common Versioning Strategy and Documentation Guidelines
- **Level 4**
  - API Documentation
    - All API's for a given project must adhere to the ONAP API Common Versioning Strategy and Documentation Guidelines

Recommended Platform Maturity Levels for Casablanca

Area	Priority	Min. Level	Stretch Goal	Level Descriptions (abbreviated)
Usability	Moderate	~~Level 1~~ **Level 2**	**External APIs follow Policy**	1 – user guide; deployment documentation; API documentation; adherence to coding guidelines 2 – API Documentation (new APIs follow policy, rest Swagger 2.0); tutorial documentation 3- UI consistency; usability testing; API Documentation (changed and external APIs follow policy) 4 – API Documentation (all follow policy)

BACKUP

Current Requirements Levels – Performance, Stability

Performance

- **Level 0:** no performance testing done
- **Level 1:** baseline performance criteria identified and measured (such as response time, transaction/message rate, latency, footprint, etc. to be defined on per component)
- **Level 2:** performance improvement plan created & implemented for 1 release (improvement measured for equivalent functionality & equivalent hardware)
- **Level 3:** performance improvement plan implemented for 2 consecutive releases (improvements in each release)

Stability

- **Level 0:** none beyond release requirements
- **Level 1:** 72 hour *component*-level soak test (random test transactions with 80% code coverage; steady load)
- **Level 2:** 72 hour *platform*-level soak test (random test transactions with 80% code coverage; steady load)
- **Level 3:** track record over 6 months of reduced defect rate

Current Requirements Levels – Resiliency

- **Level 0:** no redundancy
- **Level 1**: support manual failure detection & rerouting or recovery within a single site; tested to complete in 30 minutes
- **Level 2:** support automated failure detection & rerouting
  - within a single geographic site
  - stateless components: establish baseline measure of failed requests for a component failure within a site
  - stateful components: establish baseline of data loss for a component failure within a site
- **Level 3:** support automated failover detection & rerouting
  - across multiple sites
  - stateless components
    - improve on # of failed requests for component failure within a site
    - establish baseline for failed requests for site failure
  - stateful components
    - improve on data loss metrics for component failure within a site
    - establish baseline for data loss for site failure

Current Requirements Levels – Security

Project-level requirements

- **Level 0**: None
- **Level 1:** CII Passing badge
- **Level 2:** CII Silver badge, plus:
  - All internal/external system communications shall be able to be encrypted.
  - All internal/external service calls shall have common role-based access control and authorization.
- **Level 3**: CII Gold badge

ONAP Platform-level requirements per release

- **Level 1:** 70 % of the projects passing the level 1
  - with the non-passing projects reaching 80% passing level
  - Non-passing projects MUST pass specific cryptography criteria outlined by the Security Subcommittee*
- **Level 2:** 70 % of the projects passing silver
  - with non-silver projects completed passing level and 80% towards silver level
- **Level 3**: 70% of the projects passing gold
  - with non-gold projects achieving silver level and achieving 80% towards gold level
- **Level 4:** 100 % passing gold.

Current Requirements Levels – Scalability, Manageability

Scalability

- **Level 0:** no ability to scale
- **Level 1:** supports single site horizontal scale out and scale in, independent of other components
- **Level 2:** supports geographic scaling, independent of other components
- **Level 3:** support scaling (interoperability) across multiple ONAP instances

Manageability

- **Level 1:**
  - All ONAP components will use a single logging system.
  - Instantiation of a simple ONAP system should be accomplished in <1 hour with a minimal footprint
- **Level 2:**
  - A component can be independently upgraded without impacting operation interacting components
  - Transaction tracing across components
  - Component configuration to be externalized in a common fashion across ONAP projects

Current Requirements Levels – Usability

- **Level 1**
  - User guide created
  - Deployment documentation
  - API documentation
  - Adherence to coding guidelines
- **Level 2**
  - Consistent UI across ONAP projects
  - Usability testing conducted
  - Tutorial documented