SA4 T1

Service transition

Marcin Wolski

Task Leader

PSNC

08/04/2016

Introduction

- SA4 introduced the service validation and testing process as an important part of the service transition to production in GEANT.

- The purpose of the service validation and testing process in SA4 T1 is to ensure that only quality-tested products reach the production environment

- The process targets the Software Development Activities (SDA) – an entity responsible for the service development

- The SA4 T1 team conducts all necessary tests – a software quality review, security code audit, system testing, and others – to evaluate the service quality based on the acceptance criteria

- The ultimate result of the evaluation is a recommendation on service readiness for production, together with proposed improvements to the service development and maintenance

Service validation and testing process

Service Operation Manager
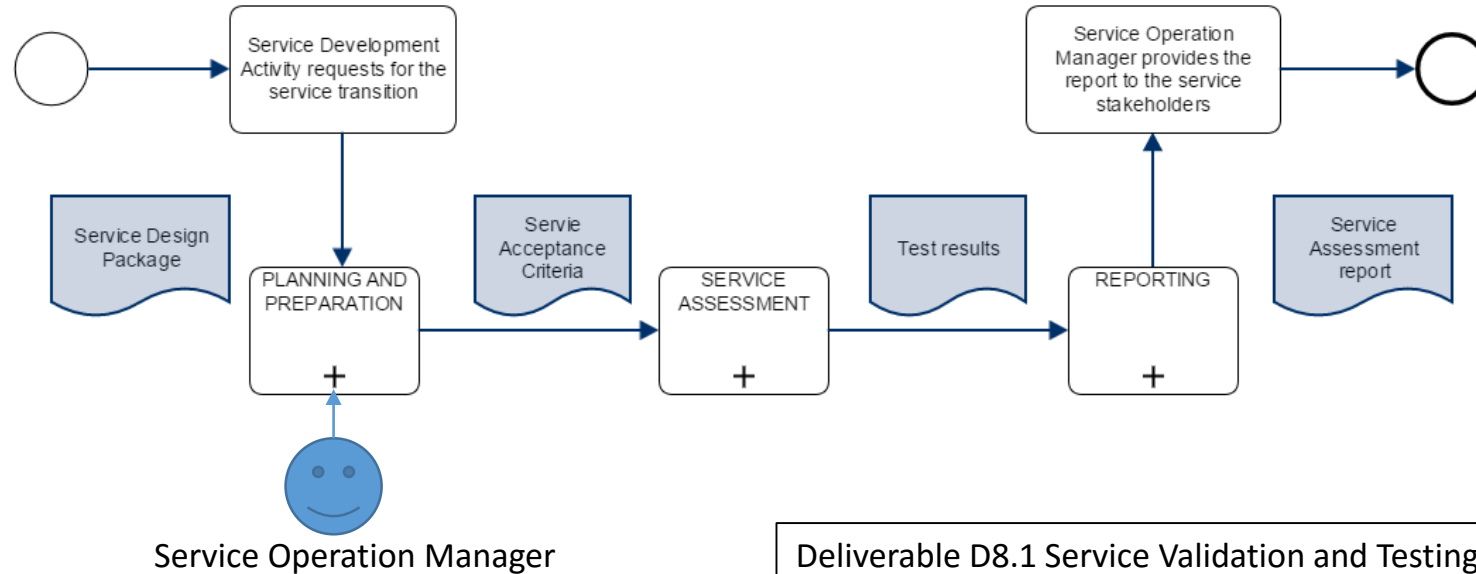
Deliverable D8.1 Service Validation and Testing Process
Document Code: GN4-1-16-22F69

Quality code audit

1. Objectives:
    1. Software maturity evaluation
    2. Validating software conformance to the GEANT best practices
2. Procedure
    1. Configuration and run of SonarQube instance.
    2. Verification of the SonarQube output
        a) found issues categorization,
        b) found issues prioritization,
        c) Recommendations.
    3. Expert code review, based on SonarQube results and performed with FishEye and Crucible tools.
    4. Report document.

...

Security code audit

- Two contradictory criteria: review quality and effort to be spent

- Besides the code, we work with a running instance
  - Better understanding of the tool
  - Input for **candidate point** review strategy
  - Easy verification of source code findings

- **Step 1**: automated tests (full code coverage)

- **Step 2**: manual tests
  - For small tools (< 10-15 KLOC) the whole code may be read
  - Verifying Step 1 results
  - Reading **candidates**
  - Reading **critical code parts**

- Time: up to 4-6 weeks

School For Developers

- Annual
- Since 2010
- Increase quality of software
- Improve skills of developers
- Hands-on workshop
- Domain expert with training skills
- 3 days
- State-of-the-art techniques

S4D 2015 Poznan

Behaviour Driven Development	Specification By Example	Test Driven Development

Secure Code Training

- The main goals of the training
  - To **keep the awareness**
  - To **practice** good templates
  - To **explain particular issues** useful for secure development of GN4 tools

  - We also want to **better understand** the way SDTs write source code

Threat modeling and risk assessment

Data Sanitization – meaning and techniques

Secure Web programming workshop

Secure file uploads mechanisms

Custom product evalution

1. System review (architecture, software stack).

2. Assessment of software management procedures (build process, continuous integration, license check).

3. Usability testing.

4. Documentation review.

5. User support verification.

….

Recommendations and best practices to operate perfSONAR in a deployment in a secure manner

PerfSonar case

- we understand that the main goal is to assure secure installation and maintenance of PerfSONAR nodes

- we think about the following:

  - reviewing an exemplary instance as it is currently deployed to the customer

  - assessment of the configuration of the node, guidelines for security hardening process (increasing security as much as possible but without losing on functionality)

  - issuing recommendations for the PerfSONAR mainteance team (administrators at the deployment site)

  - issuing recommendations for the PerfSONAR users at the deployment site

Find us on the GEANT wiki site

Pages / GN4-1 SA4 / Task 1 - Quality validation and testing

Public knowledge base

Created by Marcin Wolski, last modified on Jan 29, 2016

This Knowledge Base contains a set of useful documents we used during the service validation and testing process.

Document	Purpose
Acceptance Criteria (example)	Input to the service assessment (by Service Operation Manager, CSI manager)
User Support Survey	Evaluating service support (by users)
System Usability Scale [source: Brooke, J. "SUS: a "quick and dirty" usability scale". In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland. Usability Evaluation in Industry. London: Taylor and Francis, 1996]	SUS give us global view of subjective assessments of usability.
Test Plan description (applicable to any evaluation, test or audit that involves a group of participants)	Subjects that need to be discussed, defined and agreed between the requester and evaluators before the assessment is commenced
Input to the security audit (pen testing and security code audit)	Getting the input to start the audit
Pre-assessment survey	Grabbing the preliminary information about the service candidate to production
Automatic quality code review	A brief summary of the automated source code analyze procedure
User view on a software quality	A simple questionnaire to gather the user point of view about a software and its perception of quality

No labels

https://wiki.geant.org/display/gn41sa4/**GN4-1+SA4**

Thank you

Marcin.wolski@man.poznan.pl

GÉANT
Networks · Services · People
www.geant.org