Compliance and Verification Program - Guidelines Addendum for Danube

Introduction

This addendum provides a high-level description of the testing scope and pass/fail criteria used in the Compliance Verification Program (CVP) for the OPNFV Danube release. This information is intended as an overview for CVP testers and for the Dovetail Project to help guide test-tool and test-case development for Danube. Detailed information about the test tool as well as test-cases can be found in Dovetail documents https://git.opnfv.org/dovetail/tree/docs/testing CVP testing focuses on establishing the ability of the SUT to perform basic NFVI operations such as managing VNFs, instantiating workloads and creating secure and resilient networks.

Meaning of Compliance

OPNFV Compliance indicates deployed Telco NFV platform behavior defined as various platform capabilities or features to prepare, instantiate and remove VNFs running on the NFVI. Danube compliance evaluates the ability of a platform to support Telco Network capabilities and workloads that are supported in the OPNFV platform as of this release. Compliance test cases shall be designated as compulsory or optional based on the maturity of current OPNFV core capabilities and tested scenarios. Examples of capabilities include workload management and support for high-availability.

Ultimately it will be desirable to expand the scope of testing to include platform “user experience” to ensure that Network Services are “easy” to instantiate and manage. Test coverage is designed to ensure an acceptable level of compliance but not be so restrictive as to disqualify variations in platform capabilities and features.

Assumptions and Scope

Assumptions about the System Under Test (SUT) include ...

- The Virtual Infrastructure Manager (VIM) complies with Open Stack management APIs
- The deployment is on a bare-metal environment
- Controller/Compute nodes and network environment complies with the minimal specification defined by “Pharos” https://wiki.opnfv.org/display/pharos/Pharos+Specification [Note Pharos spec may need to be updated]
- The SUT is fully deployed and hence tools and APIs related to deployment are out of scope

[Note: we need to point to or define the minimum viable execution environment ...

- Any tested hardware should also be able to run an OPNFV Danube deployment?
- What can we support now?
- What is minimum hw & nw environment?
- What is recommended?
- What can deviate?

end]

Performance measurements are out of scope for the Danube version of CVP. Note however that certain functional capabilities of the platform that are in scope may be valuable for enhancing platform performance.

The SUT is limited to NFVI and VIM functions. While MANO, VNFs and other operational elements are out of scope for the Danube version of CVP they may be part of the test infrastructure; for example used for platform setup, workload management, etc. Certain APIs exposed towards MANO are used for CVP testing.

Test Areas

The following table lists test areas and relevant Test specifications as well as OPNFV and upstream projects.

While MANO is out of scope, there are APIs exposed towards MANO that are used in the testing suite.

[Provide pointers to specific Dovetail test documents for each area]

Test Domain	Mandatory	Relevant Project/s	Test Specifications	Test Tools
Cloud capabilities	Yes	Open Stack		RefStack
VNF lifecycle management	Yes	Copper	ETSI NFV-TST007 Guidelines on Interoperability Testing for MANO	
Carrier network capabilities			ETSI NFV-TST004 Guidelines for Test plan for path implementation through NFVI	
• IPv6	No	IPv6		
• HA	Yes			
• VPN	No	BGPVPN		

Pass/Fail Criteria

Criteria used to decide what aspects of each test area indicates complinace is described here. Criteria here are described at a high-level and are translated into specific pass/fail criteria for each test case by the Dovetail project.

1. Instance management
2. Key manipulation
3. Compute node capability / operations
4. Storage information
5. Identification services
6. Admin operations
7. Secure Server access
8. Software versions
9. Quota management
10. Volume management
11. Authorization management
12. Etc.

1. VNF image operations
2. Etc.

1. Subnet operations
2. Port operations
3. Network security
4. Etc.