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 NFVI operations and support Service Provider oriented features that ensure manageable, resilient and secure networks.

Meaning of Compliance

OPNFV Compliance indicates adherence to 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 Service Provider 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 OPNFV capabilities as well as industry expectations. Compulsory test cases may for example include NFVI management capabilities whereas tests for certain high-availability features may be deemed as optional.

In the future the scope of compliance will include platform “usability” to ensure that Network Services can be consistently managed. 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.

Test Tool Assumptions

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

- SUT implements the functions and complies with the APIs of various Virtual Infrastructure Manager (VIM) services included in the current OPNFV release. For the Danube release VIM APIs covered by Refstack are in scope.
- CVP tests for the Danube release of OPNFV require the SUT is deployed in a bare-metal infrastructure.
- The minimal specification of physical infrastructure (controller/compute nodes and network) is defined by “Pharos” https://wiki.opnfv.org/display/pharos/Pharos+Specification
- The SUT is fully deployed and operational (SUT deployment tools are out of scope).

Scope of Testing

While the current scope of compliance includes functional verification of certain performance-enhancing NFVI features, no performance measurements or assessment of performance capabilities are included as of this release.

The SUT is limited to NFVI and VIM functions. While testing MANO component capabilities is out of scope, certain APIs exposed towards MANO are used by the current OPNFV compliance testing suite. MANO and other operational elements may be part of the test infrastructure; for example used for workload deployment and provisioning.

The following table lists test areas that are in scope and references related test specifications from OPNFV, upstream projects and Industry Specification Groups. Dovetail documents include “Test Scope” which lists test areas and

respective test cases that are either compulsory or optional to include in a test run. Separate documents for each test area specify detailed test cases with test steps and associated pass/fail criteria.

Test Area	Danube Scope	Reference Project/s	Related Test Specifications
Cloud capabilities	Included	OpenStack	Refstack (OpenStack interoperability testing)
VNF lifecycle management	Basic functions	OpenStack	Refstack (OpenStack interoperability testing) ETSI NFV-TST007 (Guidelines on Interoperability Testing for MANO)
Carrier network capabilities	Limited (optional to run tests)	OPNFV-IPv6 OPNFV-SDNVPN	ETSI NFV-TST004 (Guidelines for Test plan for path implementation through NFVI) RFC4364, RFC 4659, RFC2547 (BGP VPN) Openstack IPv6 Guide RFC2460 (IPv6)
Service Availability	Limited (optional to run tests)	High Availability for OPNFV	ETSI NFV-REL001 (NFV Resiliency Requirements) OpenStack High Availability Guide

Criteria for Awarding Compliance

This section provides guidance on complianace criteia for each test area. The criteria described here are high-level, detailed pass/fail metrics are documented in Dovetail test specifications.

Dovetail Document	Description	Reference / link
Test Scope		
SDNVPN Test Spec		
HA Test Spec		
IPv6 Test Spec		
VIM Test Spec		

[Editor note: we need to describe general expectations for each of the capability areas and then where possible break down each area into functions or operations (such as those listed below) ... and say for each what the compliance bar is. This should include information regarding the expected pass rate for test suites to be awarded compliance.]

A. Cloud Capabilities

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

B. VNF Lifecycle Management

1. VNF image operations
2. Etc.

C. Carrier Network Capabilities

1. Networks and subnet operations
2. Port operations
3. Network security
4. Router operations
5. IP address mangement
6. Floating IP operations
7. Delagation of network functions to SDN Controllers
8. Etc.

D. Service Availability

1. Etc.
2.
3.

References

References should include any RFC, Spec, or published content referred to in the text.

Glossary

“CVP” “Dovetail”

“Test area” “Test domain” How is test domain different from test area?

“Test case” “Test suite”

etc.