OVP: OPNFV Verification Program

A community-led compliance and verification program to improve quality and interoperability in the NFV ecosystem.

Please direct any questions to **ovp-info@linuxfoundation.org**.

PROGRAM SCOPE:

- Compliance and verification testing of commercial products
- Requirements consolidation and implementation alignment
- ONAP and OPNFV-based tooling for NFVI/VIM and VNF testing

NFVI/VIM TESTING:

- Integrated tooling and vendor portal using Dovetail
- Focus on OpenStack API, High Availability, and stress testing
- Second iteration in late 2018

BENEFITS:

- Accelerates deployment of network services
- Improves quality, choice, and multi-vendor interoperability
- Reduces cost and risk for deployment

VNF TESTING:

- Integrated tooling using Dovetail and testing portal
- Focus on template compliance for both Heat and TOSCA
- Initial launch in April 2019

"No one vendor can manage the cost of interoperability testing, it must be a collective effort."

– Jehanne Savi, *Executive Leader of the All-IP and On-demand Networks Programs, Orange*

"Procurement and Introduction of VNFs into our network should be as simple and efficient as it is for Inducting an application in the Cloud, with this we will be able to deliver our services to our customers in a much more agile way and thereby introduce newer services faster. We believe OVP program can provide the much needed standardization for certification of VNFs to this account. This will benefit customers, carriers and VNF providers alike, making it easier also for VNF innovators to bring new solutions to market."

– Matt Beal, Vodafone Group Technology Director, Strategy & Architecture.

TABLE OF CONTENTS

INTEROPERABILITY
IN THE NFV/SDN ERA

Overcoming interoperability challenges in the NFV/SDN ecosystem has become a top priority.

Network functions virtualization (NFV) and software-defined networking (SDN) offer service providers increased service agility, OpEx improvements, and back-office automation. Disaggregation, the approach of decoupling the various layers of the stack, from hardware, to NFVI/VIM software, to dataplane acceleration, SDN controllers, MANO components, and VNFs, enables multi-vendor deployments with best-of-breed options at each layer.

As operations teams have started deploying these technologies over the past several years, however, operational challenges have called into question that original goal. Interoperability has always been a challenge, and as the number of vendors and interfaces between layers increases, those interoperability challenges increase proportionally. Service providers have long relied on compliance and verification programs through SDOs to help improve commercial product quality and ensure multi-vendor interoperability, and now look to bring that sort of rigor into the new software-defined world. Working in partnership with the same open source communities that are developing the next generation of open networking software, compliance and verification activities have entered the NFV/SDN world.

INTRODUCING OPNFV VERIFICATION PROGRAM (OVP)

In response to the above challenges, OPNFV launched the OPNFV Verification program in early 2018, focusing on commercial NFVI/VIM product offerings. Around that same time ONAP began activities in its Beijing and Casablanca releases to focus on compliance activities for VNF vendors.

As ONAP and OPNFV (as well as several other open source networking projects) came together under the LF Networking (LFN) umbrella, they have joined forces to add VNF compliance testing to OVP. This program is the first of its kind to combine automated compliance and verification testing for multiple parts of the NFV stack. OVP provides testing of commercial products built on top of the requirements from the ONAP VNF Requirements project, multiple SDOs such as ETSI and GSMA, and the LF Networking End User Advisory Group (EUAG). In doing so, OVP demonstrates the readiness and availability of commercial products based on these open source project requirements and software releases. Equally importantly, OVP expands the ecosystem of products based on these projects. The end goal of the program is to enable a longer-term industry effort focused on end to end system validation and interoperability improvements around all parts of the stack.

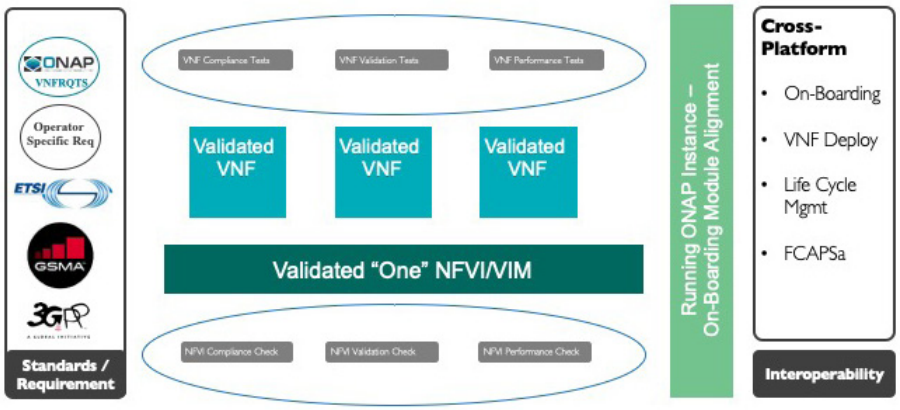

Figure 1: Vision – End to End Lifecycle System Validation

COMPLIANCE AND VERIFICATION THE COLLABORATIVE OPEN SOURCE WAY

OVP has led the way in thinking about compliance and verification from the open source perspective. While standards groups have long shown expertise in defining compliance or validation testing specifications, the implementation of test tooling for these standards has often been based on proprietary software built by a handful of companies.

In true open source fashion, the tooling used in the program's testing is freely available on the project repos, available for any vendor to use to self-test, or for any service provider to also use in their labs or CI/CD processes and toolchains. Anyone is welcome to contribute requirements, test cases, or new patches to the test tools themselves. The program values transparency, test tool automation, and multi-vendor and multi-service provider participation. It mirrors the values of the open source communities, while introducing more traditional telecom expectations around implementation quality to products and distributions based on open source components.

Term Definitions:

Compliance: Testing a product against a set of requirements or interfaces as outlined in a specification or a standard (e.g., MUST, MUST NOT statements).

Validation: Testing a product to validate it behaves as expected in real-life type conditions, such as testing High Availability in NFVI/VIM implementations or testing VNF success in on-boarding or life-cycle management functions.

Performance: Testing a product's performance in defined environments or against specific, defined profiles.

System Under Test (SUT): The commercial product being testing, e.g., VNF, NFVI/VIM, VNFM, etc.

BENEFITS OF OVP

The OVP program enables the industry to build an ecosystem of OPNFV and ONAP compliant components, which directly increases the overall choice of interoperable components available to a service provider and improves the health of the overall NFV ecosystem. The OVP program also provides specific benefits to both CSPs and vendors.

The **benefits to CSPs** are to:

- **Accelerate new service deployment:** By performing pre-testing against service-provider led requirements, OVP accelerates the qualification process and the time to new service revenue by allowing the procurement of components that work together. Including OVP compliance in a Request for Proposal (RFP) provides a convenient shortcut to procurement. Because OVP testing provides neutral testing based on community standards it also reduces risk during the sales process with new vendors.
- **Improve interoperability and software quality:** OVP improves the quality of tested products by ensuring compliance to key operator-generated requirements from open source projects and standards organizations. As the breadth and depth of testing in OVP increases with time, products will continue to become more “telco-grade” and the unification of VNF and NFVI/VIM testing through LFN cross-project collaboration reduces vendor lock-in as the friction of moving from one verified product to another is reduced and interoperability improves.
- **Reduce in-house testing effort and costs:** OVP also cuts cost and reduces testing effort on several fronts: allowing some testing to be pushed to the vendor, enabling in-house testing to focus more in each service provider specific environment. Service providers can also leverage the OVP open source toolchains and pre-scripted tests as gates in their own internal continuous integration (CI) testing.

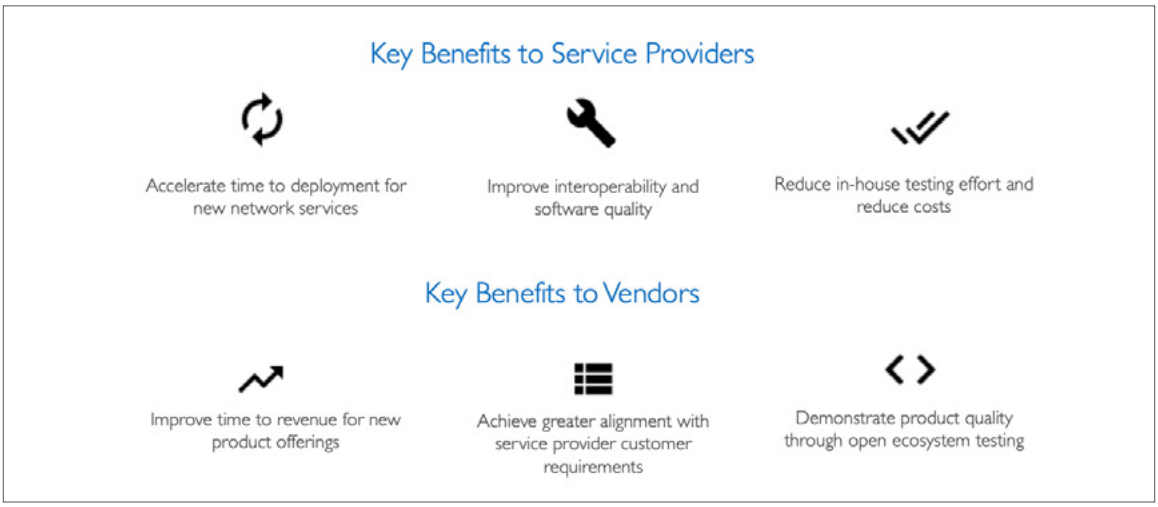

Figure 2: OVP Program Benefits

The **benefits to vendors** are to:

- **Improve time to revenue:** As OVP defines an industry threshold for entry into operator trials and baseline interop requirements, it streamlines the process of getting into customer qualifications. For RFQs based on OVP requirements, being compliant to those requirements may make it less burdensome to get into the vendor shortlist. It also streamlines the lab qualification testing process by pre-testing against many operator requirements, and enables a VNF to get to production more quickly.
- **Achieve greater alignment with SP requirements:** One major source of R&D cost and headache is multiple variations in requirements and interfaces across SPs. Through the open requirements process and common test tooling, OVP reduces this variance and improves product portability across customers. It also enables Product Management to focus on high-value differentiated features on top of the open source platform rather than triaging multiple, conflicting customer requirements.
- **Demonstrate Product Quality:** Gaining the OVP mark enables vendors to demonstrate product quality and commitment to open source. It also reduces the need for significant in-house interoperability testing with partners, a capital and manpower- intensive prospect. Use of OVP tools (as well as other freely available testing toolsets available from OPNFV and ONAP) also reduce the need to spend precious developer resources on developing test scripts in-house and enables agreed to requirements be built-in from the beginning during product design.

OVP Qualified Labs: OVP has also created a Qualified Labs Program to verify third-party testing services to the communities. In addition to a self-testing option, users can now choose to test their products or services with an OVP 3rd Party Verified lab. Working with a verified lab provides multiple benefits to vendors and end users, including access to testing subject matter experts in testing, additional test infrastructure. The program also benefits the ecosystem by enabling additional scaling as the number of VNFs needing

to undergo testing increases. The LF Networking Compliance and Verification committee (CVC) has outlined a number of requirements necessary for these labs to achieve this designation, including active participation in the technical community, demonstrated expertise with the toolchain and with LF Networking project CI/CD principles, as well as passing results from a System Under Test (SUT) in their environment.

BECOMING OPNFV VERIFIED:

PROCESS FOR NFVI/VIM OR VNF VENDORS

OVP incorporates on requirements from the EUAG as well as project requirements and SDOs. These requirements are translated into test cases, which are then automated in various test toolchains and test scripts.

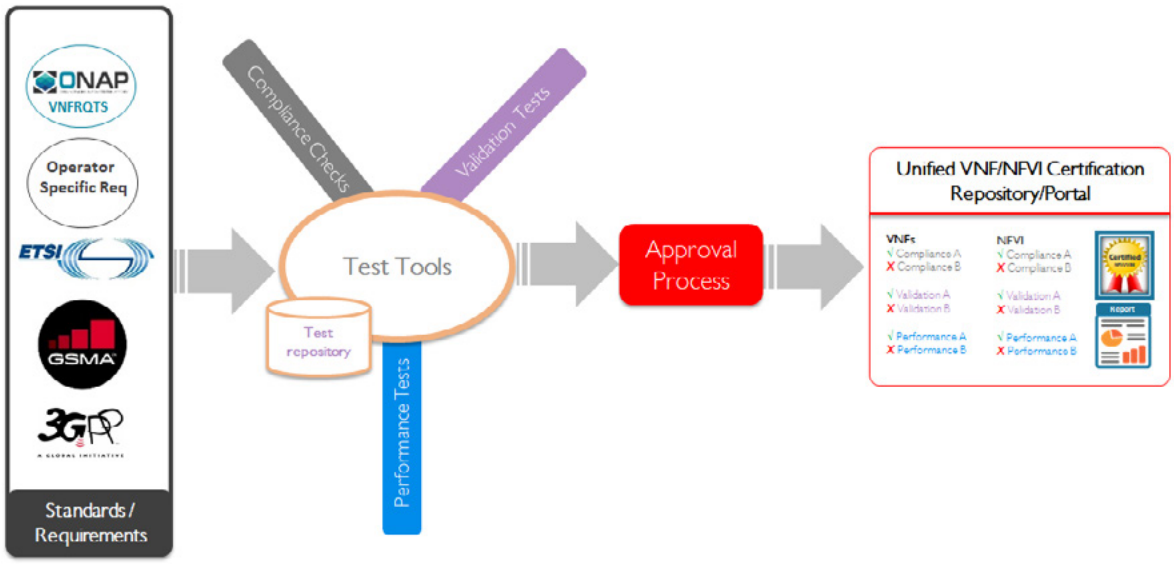

Figure 3: OVP Overview

Test Suites

The community creates test suites in response to EUAG requirements that might be project- specific, operator- specific, or standards related. These test suites are updated on a six month cycle. The OPNFV Dovetail project currently provides the top level compliance and verification test framework, and it calls out to various test suites from ONAP and OPNFV depending on the SUT. Dovetail also provides portal integration.

The program currently supports two Systems Under Test: NFVI/VIM and VNFs. For the OPNFV 2018.09 Infrastructure release, the tests are split into mandatory and optional. Mandatory tests cover 205 OpenStack API interoperability tests, 2 basic layer tests, 2 packet forwarding tests, and 8 OpenStack control service high- availability tests. Optional tests cover 25 IPv6 tenant network tests, 4 BGPVPN tests, and 30 fundamental VIM capability tests that include virtual IP Multimedia Subsystem (vIMS) and virtual Evolved Packet Core (vEPC) VNFs to provide realistic loads. These tests are derived from OPNFV Functest (API and functional), Yardstick (HA), and Bottlenecks (stress) projects.

For the VNF component of the program, the current test suites include VNFSDK to perform TOSCA VNF Package validation and VNF Validation Program (VVP) to perform OpenStack Heat VNF Package validation. In the Casablanca release, VNFSDK covers 11 requirements specified in the ONAP VNFRQTS document using 6 tests. VVP covers 298 VNFRQTS requirements using 180 tests. The goal of these initial tests is to ensure that a commercial VNF can be onboarded onto ONAP deployments using either HEAT or TOSCA for their template language.

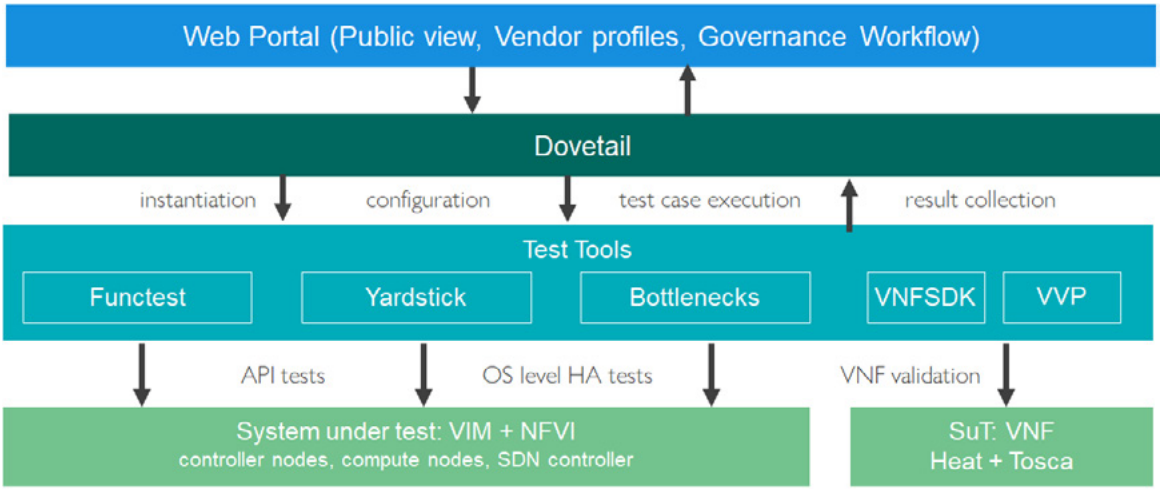

Figure 4: OVP Toolchain

OVP Portal

More information on the program is available on the LF Networking website here: www.lfnetworking.org/ovp. From here, users can begin their testing journey by accessing the portals where they can submit and review test results and get related status information. The specific testing path depends on the SUT chosen (NFVI or VNF).

THE OVP WORKFLOW

The OVP workflow has been streamlined to make it as easy as possible for the vendor to run the tests and submit the results. The overall workflow consists of six steps:

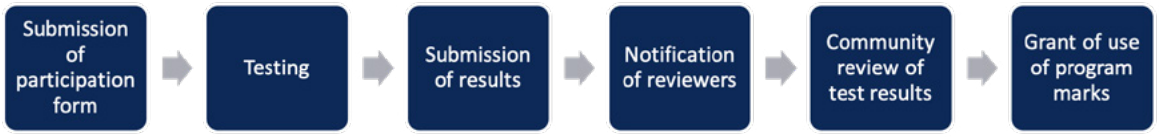

Figure 5: OVP Workflow

After a vendor submits a participation form, they can test their commercial product through a self-service mechanism or via a verified third party lab. Once the digitally signed results are securely submitted, they are reviewed by the program and the community. Results must be reviewed by at least two people from a company other than the submitting vendor, and agreed to by the group. Assuming all goes well, the process results in permission to use the appropriate program mark.

Figure 6: A Sample of OVP Marks

CALL TO ACTION – GET INVOLVED!

OVP has the opportunity to create significant value for the NFV/SDN ecosystem and for participating LF Networking projects.

It is the only unified open source-based compliance and verification program for the industry, and the only program to truly create an interoperable disaggregated software stack spanning multi-vendor NFVI/VIM, MANO, and VNFs. As an open source project, however, it will not succeed without leadership and participation of the community and ecosystem itself. Ways to get involved:

- Join the Compliance and Verification Committee
- Participate and contribute to the VNF Requirements Project in ONAP
- Provide feedback on the program through the LFN EUAG
- Contribute to the test projects supporting this program in ONAP and OPNFV
- Make OVP a requirement in your RFP process
- Test your products and get the OVP seal of approval

Open source networking has been a disruptive and valuable set of technologies for service providers looking to transform their networks. The OPNFV Verification Program can bring rigor and order to what can sometimes be an overwhelming amount of network innovation. Join OVP in growing and developing the NFV/SDN ecosystem.

RESOURCES

OPNFV Verification Program: https://www.lfnetworking.org/ovp
OPNFV Verification Portal (NFVI): https://nfvi-verified.lfnetworking.org
ONAP Verification Portal (VNF): https://vnf-verified.lfnetworking.org
OPNFV Dovetail wiki.opnfv.org/display/dovetail
ONAP VNFSDK: wiki.onap.org/display/DW/VNF+SDK+Project
ONAP VVP: wiki.onap.org/display/DW/VNF+Validation+Program+Project