SOLUTION BRIEF

Communications Service Providers

Common NFVI Telecom Taskforce Drives NFV Interoperability

The Common Network Function Virtualization Infrastructure Telecom Taskforce (CNTT) initiative and reference framework seek to continuously improve the predictability and efficiency for communications service providers and their supply chain, in consuming and deploying NFVI platforms, VNFs, and CNFs to accelerate network transformation, while driving lower deployment and operational costs.

Authors

Bob Monkman
Intel

Nick Chase
Mirantis

From the start, network function virtualization (NFV) has been a game-changing technology revolution for communications service providers (CommSPs). Initiated by 13 CommSP executives who jointly authored an introductory whitepaper, NFV adapted virtualization technology from data centers for telecom applications. This paradigm shift promised a new way to build telecom networks with lower capital expense and more service agility that would usher in a world of rapid deployment of new services and improved lifecycle management.

Since then, entirely new virtualized products have debuted, such as SD-WAN. In addition, brand new competitors have taken advantage of the NFV paradigm to compete with incumbent telecom equipment manufacturers (TEM).

But with great change comes new technical challenges, and one of the big challenges for NFV is the lack of true interoperability between virtual network functions (VNFs) and NFV infrastructure (NVFI). To move forward in their NFV plans, CommSPs have made NFV implementation decisions on a service-specific basis. This optimizes the NFVI for the performance of a vendor-specific VNF, but may be incompatible with other VNFs. Because of this, CommSPs have NFV silos that required complex integration work for compatibility. Onboarding a new VNF in this environment is a challenge and is difficult to automate or standardize. This challenge has been exacerbated in 5G networks and edge cloud applications where incompatibility impacts network scalability and operational complexity. As the industry begins to eye the promise for cloud native infrastructure and containerized network functions (CNFs), we want to solve some of these foundational challenges in a way that avoids similar issues going forward.

The Common NFVI Telecom Taskforce (CNTT) was incubated in early 2019 by 10 CommSPs to establish the group's essential framework and goals. Later that year the taskforce expanded to include more than 30 members, a number that is still growing, and opened membership to TEMs and other telecom vendors. These members joined to create a framework that includes a reference model, reference architectures, and compliance verification suites. When complete, the industry will be able to use NFVI platform and VNF compliance to this framework to create a more standard, predictable, and interoperable environment.

NFVI Interoperability and Operational Challenges

The foundation of the CNTT project comes from CommSPs who articulated the technical, operational, and business challenges from having a heterogenous NFVI expected to support multiple vendors' VNFs. These include the following:

- Higher development costs and longer time to operations due to the need to develop VNFs on multiple custom platforms for each CommSP.

- Increased development complexity due to the need to maintain multiple VNF versions that are needed to support multiple NFVI environments.
- Lack of testing and verification commonalities, leading to inefficiencies and increased time to market.
- Barriers to adoption of cloud-native network architectures that enable all the benefits obtained from true cloud models.
- Increased operational overhead due to the need for operators to integrate diverse and sometime conflicting VNF platform requirements.
- Inconsistent operating model within a CommSP's various services.
- Unpredictable NFVI and VNF lifecycle operations.
- Lack of automated deployment due to few or no known good configurations.

CNTT NFVI Reference Framework

To address this situation, CNTT has developed a reference for a unified NFVI platform, as seen in Figure 1. The framework is composed of a reference model (RM) that guides the development of reference architectures (RAs), which then are released as reference implementations (RIs). The reference conformance process (RC) provides a mechanism for testing for compliance to the reference implementation.

The taskforce is developing RAs for both OpenStack and Kubernetes. Since its founding in 2019, the task force has had two releases of its RM, as well as a release of its first-generation RA for OpenStack (RA1). In the first quarter of 2020, the taskforce expects to release RMv3.0 and RA1v2.0 along with first version of a RI and of the Kubernetes version of the RA (RA2v1.0).

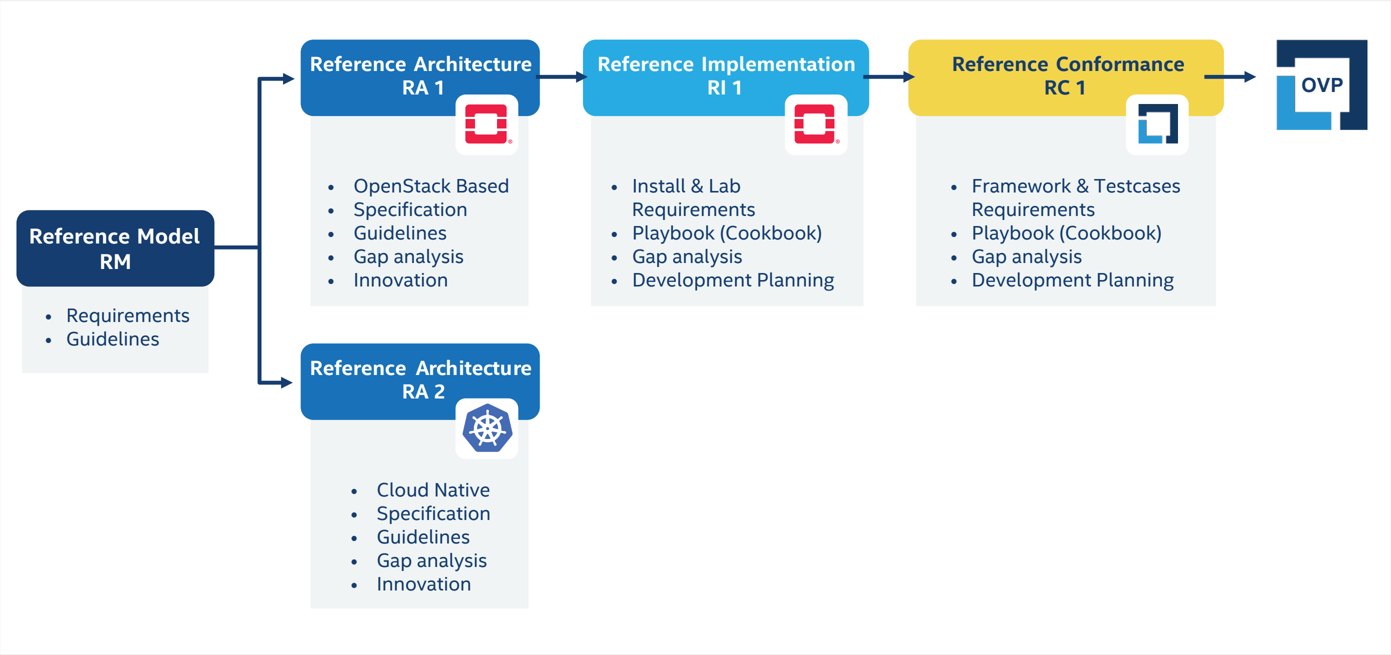

Figure 1. CNTT common NFVI reference platform.

CNTT Reference Model

The goal of the CNTT is to build a single, overarching RM that is technology agnostic and uses common methods and metrics for specifying NFVI capabilities. Commercial NFVI can be tested against reference implementations of the RAs built using the model.

As shown in Figure 2, the scope of the CNTT reference model starts with specifying profiles for both the NFVI hardware and the NFVI software. These profiles are based around a set of NFVI metrics and capabilities that VNFs require to create network services. This is designed to make available a set of well-understood characteristics that VNFs need to ensure capacity and performance predictability.

CNTT Reference Architectures

The RM has the smallest number of RAs tied to it as is practical. RAs are technology specific with the goal to combine as many compatible features as possible in an RA. A new RA will be created only in the event that any incompatibilities can't be overcome, for example to support different commonly used cloud virtualization and infrastructure management technologies. The CNTT has built this option for forking the architecture to support different paths, but its intention is to have the fewest possible architectures available. Currently two architectures are specified, one for VMs (OpenStack) and one for containers (Kubernetes).

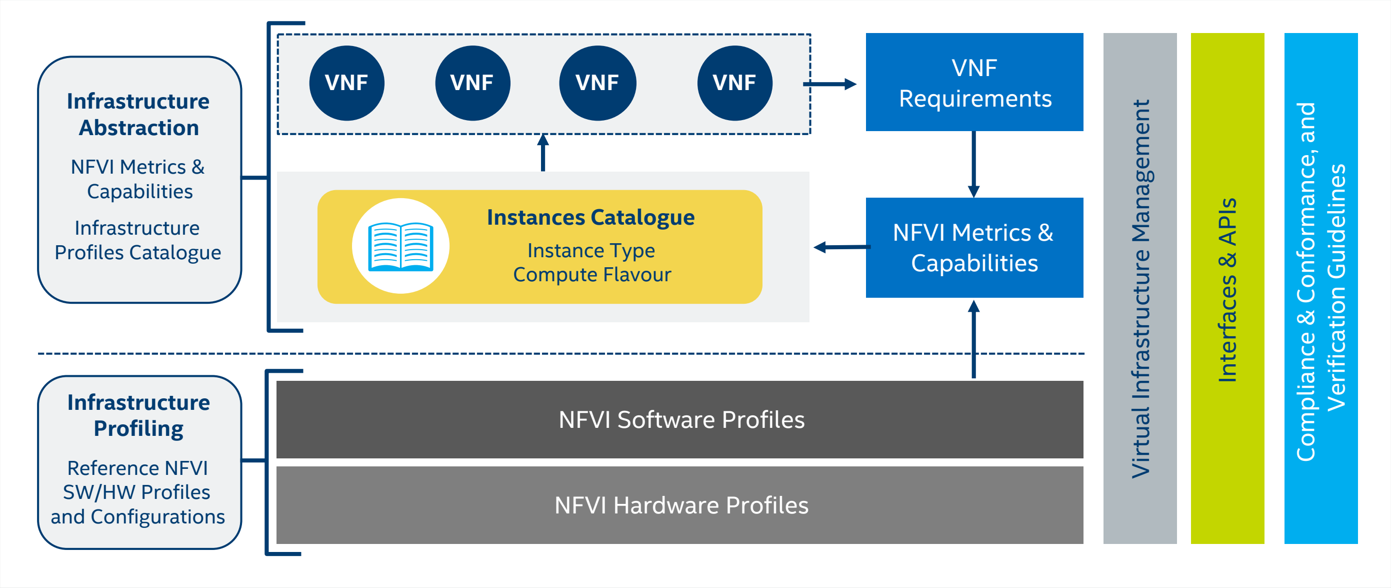
Infrastructure Abstraction
NFVI Metrics & Capabilities
Infrastructure Profiles Catalogue
VNF
VNF
VNF
VNF
VNF Requirements
Instances Catalogue
Instance Type
Compute Flavour
NFVI Metrics & Capabilities
Infrastructure Profiling
Reference NFVI SW/HW Profiles and Configurations
NFVI Software Profiles
NFVI Hardware Profiles
Virtual Infrastructure Management
Interfaces & APIs
Compliance & Conformance, and Verification Guidelines

Figure 2. Scope of CNTT reference model.

Another option is to create an RA annex to support different components that are otherwise compatible with the architecture. One early example is creating an annex for Ceph-based storage and an annex for Swift-based storage. Other design principles include the following:

- NFVI-exposed resources should be supplier independent.
- All NFVI APIs must support multi-vendor operation and feature component substitution interoperability.
- APIs must be designed for simplified operation and be open source implementations from organizations that support an open governance model.
- VNFs should be modular and be designed to utilize the minimum resources required for the service.
- NFVI shall support pre-defined and parameterized sizes with flexibility to support evolution of these sizes.
- NFVI provides certain resources, capabilities, and features, and VNFs should only consume these resources, capabilities, and features.
- VNFs that are designed to take advantage of NFVI accelerations shall still be able to run without these accelerations, with the understanding that there will be potential performance impacts.
- Workloads shall not require hardware-dependent software.

CNTT NFVI and VNF Verification

The CNTT will also provide a compliance program to ensure conformance to an RA by providing a framework of test suites and reference data for both VNFs and NFVI.

CNTT builds on and enhances the OPNFV Verification Program (OVP), an open source, community-led compliance and verification program that demonstrates the readiness of commercial NFVI and VNFs.

OPNFV 1.0 developed a framework of testing, and an initial conformance program called OPNFV Verification Program (OVP),[1] where entities could run the verification tests and get badged as OPNFV NFVI or VNF compliant. The OVP established basic functionality test framework for OpenStack- and VM-based infrastructure. Once CNTT reference models and architectures are implemented as reference implementations, commercial products adhering to these specifications can undergo an enhanced VNF and NFVI compliance testing.

It should be noted here that any code, tools, and test framework for CNTT will be developed under the Linux Foundation, within the OPNFV community, as a new area of focus, separate and distinct from the previous scope, but leveraging the learnings the original OPNFV scope. The first phase of OPNFV focused on creating reference implementations of an NFVI platform updated each year with the latest stable releases of the many open source components required for a deployable platform. This has included components such as OpenStack, KVM, OpenDaylight, Ceph, and Linux OS in addition to a number of installer sub projects, feature projects, and an excellent framework of test suites, tools, and performance benchmarks.

Intel Provides OPNFV Development Resources

In this first phase, Intel contributed resources, architectural input, and the fundamental open community lab playbook. The company began a number of development environments available to the CNTT community that were stocked with leading-edge Intel®-based servers for development, major release continuous integration / continuous delivery (CI/CD), and for OPNFV Verification Program (OVP) conformance. In addition, Intel pioneered and contributed to range of key projects, including performance-focused projects, as well as providing oversight and leadership in the governing board, technical steering committee, and marketing committee.

As CNTT fulfills its vision, it is expected that the CNTT compliance verification program will build off of many of these verification tools and processes, and Intel will bring its vast experience, expertise, and thought leadership to bear, including experience in working with partners and customers to deploy NFV solutions into the network to help guide, implement, verify, and realize the goals of the CNTT initiative.

Mirantis Tackles Operational Challenges of Virtualization

Mirantis works with CommSPs on NFV deployments, where the operational challenges of virtualization and containerization are acute. The company has championed open source cloud technology, including many that CommSPs have relied on for close to a decade and that form the underpinning of the CNTT effort. In fact, Mirantis Cloud Platform, which is being merged with the Docker Enterprise platform, integrates open source software such as OpenStack, Kubernetes, Calico, and Ceph alongside the company's own life cycle management and continuous monitoring software. Additionally, Mirantis is working to enhance the reliability and upgradeability of the NFVI platform with support for containerized OpenStack running on Kubernetes.

This perspective gives Mirantis insight into the many challenges that CommSPs face when ensuring a smooth deployment of virtual components such as VNFs and containerized network functions (CNFs). The company knows it is in its best interests, and those of its customers, to find common ground on which all vendors can agree. Mirantis is working to ensure both that this standard is sound, and that its products support and conform to it, whether they are based on OpenStack, Kubernetes, or some future cloud architecture.

Conclusion

With the full CNTT RM platform, CommSPs will be able to make NFVI decisions with the confidence that they will support a broader universe of VNFs or CNFs with predictable performance and capacity. Similarly, VNF and CNF developers will be able to maintain a single code base and build in configuration automation features rather than spend resources customizing the software for the full range of NFVI options. With the CNTT reference framework, the industry can accelerate interoperable NFVI and VNF deployment and fulfill the network agility promised by NFV from the start.

For More Information

CNTT Github: https://github.com/cntt-n/CNTT

CNTT Wiki: https://wiki.lfnetworking.org/display/LN/Common+NFVI+Telco+Task+Force+-+CNTT

Linux Foundation Networking:
https://www.linuxfoundation.org/projects/networking

Notices & Disclaimers

[1] https://wiki.opnfv.org/display/dovetail/OVP+Web+Portal

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.