Common NFVI Telco Taskforce
Paris Face-To-Face Sessions,

Walter Kozlowski, Telstra
Karine Sevilla, Orange
Pankaj Goyal, AT&T
Rabi Abdel, Vodafone

Reference Architecture Principles

July 2019
Common NFVI for Telco Reference Architecture

Agenda

• Introduction
• VMS or Containers?
• Open Source
• Published API
• Availability and Resilience
• Scalability and Immutability
• Automated Deployment and Life Cycle Management
• Operability and Maintainability
• Security
• Q&A
• Wrap-up
CNTT Reference Architecture

Introduction

CNTT Mission

CNTT Objectives
- Single NFVI Reference Model
- Limited number of NFVI Reference Architectures

REFERENCE MODEL
NFVI Infrastructure Abstraction Framework to drive consistency of infrastructure and continuity of Reference Architectures specifications

REFERENCE ARCHITECTURE
Discrete NFVI specifications based on the Reference Model optimised towards specific types of technology like VM or Container based and/or type of workloads
Industry is moving quickly to Container based Cloud Native solutions but about 80% of existing virtualized network services is VM-based. What should be our first Reference Architecture like?
Principle 1
CNTT operator/supplier community must use open source and proactively influence open source activities.

Goal
Ensure that suppliers’ and operators’ investment have a tangible pathway towards a standard and production ready NFVI solution portfolio.

Discussion Points
Which communities and open source projects need to be engaged, used and influenced to accelerate convergence of the NFVI standardization process? Where are the main areas requiring our attention?
Principle 2
Interaction between components of NFVI and with external systems like MANO must be implemented according to Open Published API specifications.

Goal
Minimize integration and interoperability efforts.

Discussion Points
We need to define standard technology specific API specifications for ETSI defined Integration Points. Also, we need to define standard APIs within NFVI itself. What is the current industry state? How to approach this? Where to start? Which API specs are critically needed as the first priority?
**Principle 3**

NFVI must be architected to allow High Availability and Resilience for hosted VNFs.

**Goal**

Network service resilience should come from the resilience in the application layer.

**Discussion Points**

While the software layer resilience is a long term goal (e.g. through cloud-nativeness of VNFs), how to get there? What are the main aspects of the NFVI Architecture that need to be standardized to accelerate this evolution? What NFVI platform resilience needs to be provided in the short term?
Principle 4

NFVI Architecture must support fast and reliable horizontal scaling of workloads, enabled by immutable infrastructure.

Goal

Scaling cost and operational impact reduction.

Discussion Points

We need to provide practical reference architecture analysis how to enable scaling out of workloads to minimize costs and minimize operational impacts. How to use immutability to allow fast and reliable scaling?
**Principle 5**

Deployment and zero-touch lifecycle management of NFVI instances must be done via an automated process.

**Goal**

Minimise costs of deployment and non-disruptive LCM across multiple physical locations.

---

**Discussion Points**

Infrastructure as a Code – is it real or myth? What technology developments should be considered for Automation of deployment and non-disruptive, zero-touch LCM? Balance use of NFVI resources between Control and Management Planes and User Plane.
Principle 6
NFVI Platform Architecture must support automated assurance and minimize complexity of operations and maintenance.

Goal
Minimise operational costs and simplify operations.

Discussion Points
How to minimise complexity of operations? What tooling is available for automation and Assurance across multiple layers of NFVI Architecture? How to deploy NFVI to optimise maintenance (availability zones, host aggregations,...)?

Operation needs
- Patching and Upgrades without service impact
- Service Assurance
  - Monitoring
  - Performance
  - Logging
- Security and Compliance Check
- Reporting
- Portal

Have we done much progress since 2017?

创业难守业更难
To start a business is difficult but to keep going is more difficult
CNTT Reference Architecture
Security

**Principle 7**
NFVI platform must at all levels comply with industry/regional security regulations, as well as with the industry security best practice.

**Goal**
Ensure security and compliance.

- Security certification using ISO27k suite of standards, higher on case-by-case basis
- 2FA authentication
- Encryption for all external and control comms
- Encryption for all data in motion and at rest
- Strong separation between tenants
- Strong RBAC schema
- Change control enforced
- Separation of control and execution zones
- IP filtering between zones

**Discussion Points**
What international security standards should be considered from the security perspective (e.g. ISO, NIST)? How to balance security versus performance and ease of use/operability (e.g. use of firewalls and encryption)?
Q&A
Wrap Up