ENFV: Edge NFV requirements project

Release draft (bf21603)

OPNFV

April 07, 2016

CONTENTS

CHAPTER

ONE

INTRODUCTION

The purpose of this Requirements Project is to articulate the capabilities and behaviours needed in Edge NFV platforms, and how they interact with centralized NFVI and MANO components of NFV solutions.

1.1 Problem description

Edge NFVI location has certain specific requirements related to:

1. Appropriate Tunneling for User Traffic across WAN (Ethernet, IP/MPLS) links
2. Appropriate Tunneling for Management Traffic across WAN links
3. Including reachability requirements to the compute platform ('eth0' resilience, this also include backup path through other media e.g. 4G/5G)
4. Extending Multi-data center management to address many small or micro data center locations
5. Monitoring Capabilities required for a remote Compute Node
6. Squaring Bare Metal with remote survivability and whether IaaS is more appropriate for remote locations
7. Security. As demarcation technology is operated in an un-trusted environment (CSP perspective) additional means need to be implemented. Similarly, the enterprise might have concerns if the security architecture is impacted as VNFs provide functions at different locations than the precious hardware; topics like authentication, authorization, securing the traffic.

CHAPTER

TWO

USE CASES AND SCENARIOS

There are several use cases related to Edge NFV. This section will briefly describe them, along with the issues or complexities that they introduce versus a typical data center (DC) deployment.

1. **vE-CPE.** *[vE-CPE]* is related to most popular NFV use case where a NFVI compute node is located at customer premises. Typical applications are virtual firewall and virtual router to replace physical equivalents. The service chain can include VNFs hosted in vE-CPE host and/or a centralized data center. Complexities include:
   - This application is very cost-sensitive, so the server will typically be lower performance than in the DC.
   - There may not be layer 2/Ethernet connectivity at the deployment site, so tunneling may be required.
   - There may not be initial connectivity to the node, so some sort of zero-touch protocol may be required.
2. **Stand-alone vE-CPE.** It is the same as above but all virtual network functions are hosted at the same CPE compute node.
3. **Residential GW.** Similar to vE-CPE, the major difference is scale. Typical VNFs are "WAN fault monitoring", "Performance monitoring". Ratio between deployed vE-CPE and Residential GW might reach 1:100 or even 1:1000, so VNF management overhead must be minimized. For instance, self-termination after predefined activity period seems preferable over explicit VNF removing via management system.
4. **Distributed Base station.** TBD. What is the difference for it?
5. **Network connectivity.** In most cases CPE is connected to Metro Ethernet [1] .
6. **Micro Data Center** NFVI resources may be located at the edge of the network for the use cases listed above. Doing so increases the scale of the clouds or locations that must be orchestrated and controlled. If OpenStack is run in a distributed fashion, with a central node controlling distributed NFVI servers, the following issues may be seen:
   - Lack of compatibility between different versions of OpenStack.
   - Scalability of OpenStack.
   - Operation in low speed or lossy networks is complicated by the amount of messaging required.
   - OpenStack numbers VNF ports in a sequential manner, with the sequence serially numbered in the VM/VNF. The difficulty comes when trying to verify that the LAN has been connected to the correct LAN port, the WAN has been connected to the correct WAN port and so on.
   - While OpenStack provides a rich set of APIs, critical support is lacking:
     - No APIs for ssh access to VM/VNFs.
     - No APIs for port mirroring in Neutron.

[1] In all above use cases management traffic is coming inband with tenant traffic.

- No APIs for OpenStack oversubscription parameter setting

CHAPTER

THREE

HIGH LEVEL ARCHITECTURE AND GENERAL FEATURES

3.1 Functional overview

We foresee two OpenStack deployment models:

1. Single-cloud. Centralized OpenStack controller and ENFVI nodes are Compute nodes
2. Multi-cloud. Each NFVI node contains OpenStack controller, thus it becomes an “embedded cloud” with single internal compute node

3.2 Architecture Overview

Architecture overview is here.

3.3 General Features and Requirements

This is main part.

3.4 High level northbound interface specification

What is northbound here? VIM controller?

CHAPTER

FOUR

GAP ANALYSIS IN UPSTREAM PROJECTS

4.1 Network related gaps

1. **Terminology.** Consider to keep upstream/downstream terminology for the traffic leaving/coming to Edge NFV. This gives unambiguous names 'uplink/downlink' or 'access/network' for CPE interfaces. Inside DC this traffic is called east-west and no special meaning for interfaces on compute/network node.
2. **Uplink interface capacity.** In most cases those are 1GE as opposite to DC where 10/40G interfaces are prevailing. As result 1GE interfaces are not part of CI.
3. **Tunneling technology:**
   (a) Case stand-alone NFVI - 802.1ad S-VLAN or MPLS.
   (b) **Case distributed NFVI - VXLAN or NVGRE over 802.1ad.**
      - VXLAN and NVGRE tunnels don't support OAM check.
   (c) All above tunneling technology don't support integrity check.
   (d) All above tunneling technology don't support payload enryption (optional).
4. **Management traffic:**
   (a) Management traffic should come inband with tenant traffic.
   (b) Management traffic should easily come through firewalls, i.e. single IP/port would be ideal (compare with OpenStack bunch of protocols *[firewall]*).
   (c) Management connection might be disrupted for a long period of time; once provisioned Edge NFV device must keep its functionality with no respect of management connection state.
5. **Resiliency:**
   (a) Network resiliency is based on dual-homing, service path shall be forked in that case. A VM presumable shall be able to select active virtual link for data forwarding
   (b) SLA assurance for tenant virtual link - mandatory
   (c) Fault propagation towards VM is mandatory

4.2 Hypervisor gaps

1. Monitoring Capabilities required for a remote Compute Node; Hypervisor shall provide extended monitoring of VM and its resource usage.

4.3 OpenStack gaps

Later should be per specific component? (nova, neutron...)

OpenStack Nova

1. Management system should support dozen of thousands individual hosts. Currently each Edge Host is allocated in individual zone, is this approach scalable?
2. Host is explicitly selected effectively bypassing NOVA scheduler

4.4 Deployment gaps

1. Only traffic interfaces are exposed (e.g. no eth0, no USB); SW deployment is different from DC.
2. Linux shell shall not be exposed; linux CLI shall be replaced presumable by REST.
3. Kernel and Hypervisor are hardened. Only OpenStack agents might be added during deployment.
4. AMT or IPMI shall not be used for SW deployment.

CHAPTER

FIVE

DETAILED IMPLEMENTATION PLAN

TBD

5.1 Functional Blocks

TBD

5.2 Sequence

TBD.

5.3 Implementation plan for OPNFV Release XYZ

TBD.

5.4 Information elements

TBD.

5.5 Detailed northbound interface specification

TBD.

5.6 Blueprints

TBD

CHAPTER

SIX

SUMMARY AND CONCLUSION

TBD

CHAPTER

SEVEN

REFERENCES AND BIBLIOGRAPHY

CHAPTER

EIGHT

GLOSSARY

Definition of terms

Different SDOs and communities use different terminology related to NFV/Cloud/SDN. This list tries to define an OPNFV terminology, mapping/translating the OPNFV terms to terminology used in other contexts.

CPE Customer Premises Equipment

CSP Communication Service Provider

DC Data Center

NFV Network Function Virtualization

NFVI Network Function Virtualization Infrastructure

vE-CPE Virtual Enterprise-Customer Premises Equipment

[OPSK] OpenStack, [Online]. Available at https://www.openstack.org/

[ENFV] ETSI NFV, [Online]. Available at http://www.etsi.org/technologies-clusters/technologies/nfv

[vE-CPE] ETSI NFV Use Cases, [Online]. Available at http://www.etsi.org/deliver/etsi_gs/nfv/001_099/001/01.01.01_60/gs_nfv001v01

[security] IETF, [Online]. Available at https://tools.ietf.org/html/draft-ietf-nvo3-security-requirements-06

[firewall] OpenStack FW, [Online]. Available at http://docs.openstack.org/juno/config-reference/content/firewalls-default-ports.html

C

D

N

V