ETSI GR NFV 003 V1.5.1 (2020-01)

Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGR/NFV-003ed151

Keywords
NFV, terminology

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document collects selected definitions and abbreviations from different NFV specifications in order to provide a common reference and facilitate shared understanding.

Introduction

ETSI NFV has produced a number of specifications over the years since its creation. According to ETSI rules, each of these specifications contains its own definitions and abbreviations clause. The present document was created to host definitions and abbreviations that are thought to be common to NFV documents to constitute a single source and facilitate common references.

1 Scope

The present document provides terms and definitions for conceptual entities within the scope of the ISG NFV, in order to achieve a "common language" across all the ISG NFV working groups.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI Directives: Annex 1: "Definitions in relation to the member categories of ETSI".

[i.2] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.3] IETF RFC 2330: "Framework for IP Performance Metrics".

[i.4] IETF RFC 6390: "Guidelines for Considering New Performance Metric Development".

[i.5] ISO/IEC 15939:2007: "Systems and software engineering -- Measurement process".

[i.6] NIST Special Publication 500-307: "Cloud Computing Service Metrics Description".

NOTE: Available at http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf.

[i.7] Recommendation ITU-T Y.3500: "Information technology - Cloud computing - Overview and vocabulary".

[i.8] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.9] Recommendation ITU-T E.800 (2008): "Terms and definitions related to quality of service and network performance including dependability".

[i.10] Void.

[i.11] NIST Special Publication 800-146: "Cloud Computing Synopsis and Recommendations", 2012.

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

0-9

Void.

A to B

administrative domain: collection of systems and networks operated by a single organization or administrative authority

NOTE: The components which make up the domain are assumed to interoperate with a significant degree of mutual trust among them based on a stable trust relationship, while a transient, specific trust relationship is established for interoperating with components in other domains.

affinity of virtualised network resources: persistent policy that forces Virtual Links (VLs) to share the same physical connectivity

NOTE 1: "Persistent" is used here and in the following definitions to indicate that the affinity remains in effect until a change is requested by the consumer.

NOTE 2: This may be stipulated to ensure the same transmission characteristics (such as delay) for VLs.

allocate virtualised resource: operation that creates an instance of a virtualised resource, involving the assignment of NFVI resources

NOTE 1: Virtualised resources can include virtualised compute resources, virtualised network resources or virtualised storage resources.

NOTE 2: Throughout the present document the term "instantiated virtualised resource" is used to describe an instance of a virtualised resource.

anti-affinity of virtualised network resources: persistent policy that forces Virtual Links (VLs) to not share any physical connectivity

NOTE: This may be stipulated to ensure that VLs do not fail at the same time.

area affinity: policy that qualifies an affinity (or anti-affinity) policy with respect to location restrictions

NOTE: Anti-affinity can be used to support availability, survivability and performance needs with respect to virtualised resources.

EXAMPLE: The anti-affinity policy of having virtualised compute resources on different compute nodes can be further restricted by mandating to locate the compute nodes on different shelves, racks, bays, sites, geographic areas or similar restriction.

C

Central Processing Unit (CPU): device in the compute node that provides the primary container interface

Composite Network Service (CNS): network service containing at least one network service

compute domain: domain within the NFVI that includes servers and storage

compute node: abstract definition of a server

consumable virtualised resource: virtualised resource that can be requested for reservation and/or allocation

NOTE: Virtualised resources comprise compute, network and storage.

EXAMPLE: A volume or object based virtual storage.

consumer: role played by a functional block that consumes certain functions exposed by another functional block

consumer VNF: VNF that consumes services

container image registry: function that stores container images and makes them available to other functions

NOTE: No assumption is made on the location of such a function.

container infrastructure service: service that provides runtime environment for one or more container virtualisation technologies

NOTE: Container infrastructure service can run on top of a bare metal or hypervisor-based virtualisation.

container infrastructure service instance: instance providing runtime execution environment for container

container infrastructure service management: function that manages one or more container infrastructure services

NOTE: The container infrastructure service management provides mechanisms for lifecycle management of the containers, which are hosting application components as services or functions.

D

deployment flavour: template that describes a specific deployment (of a Network Service or VNF) supporting specific KPIs (such as capacity and performance)

E

error: discrepancy between a computed, observed, or measured value or condition and a true, specified, or theoretically correct value or condition

NOTE 1: Error is a consequence of a fault.

NOTE 2: See ETSI GS NFV-MAN 001 [i.8].

F

fault: adjudged or hypothesized cause of an error

NOTE: See Recommendation ITU-T E.800 [i.9].

fault detection: process of identifying an undesirable condition (fault or symptom) that may lead to the loss of service from the system or device

fault diagnosis: high confidence level determination of the required repair actions for the components that are suspected to be faulty

NOTE: Diagnosis actions are generally taken while the component being diagnosed is out of service.

fault isolation: isolation of the failed component(s) from the system

NOTE: The objectives of fault isolation include avoidance of fault propagation to the redundant components and/or simultaneous un-intended activation of active and backup components in the context of active-standby redundancy configurations (i.e. "split-brain" avoidance).

fault localization: determining the component that led to the service failure and its location

fault management notification: notification about an event pertaining to fault management

EXAMPLE: Fault management notifications include notifications of fault detection events, entity availability state changes, and fault management phase related state progression events.

fault remediation: restoration of the service availability and/or continuity after occurrence of a fault

field replaceable unit: unit of hardware resources designed for easy replacement during the operational life of a network element

G

Void.

H

hypervisor: software which partitions the underlying physical resources, creates Virtual Machines, and isolates them from each other

NOTE: The hypervisor is software running either directly on top of the hardware (bare metal hypervisor) or running on top of a hosting operating system (hosted hypervisor). The abstraction of resources comprises all those entities inside a computer/server which are accessible, like processor, memory/storage, NICs.

I

infrastructure domain: administrative domain that provides virtualised infrastructure resources such as compute, network, and storage or a composition of those resources via a service abstraction to another Administrative Domain, and is responsible for the management and orchestration of those resources

NOTE: This definition is from ETSI GS NFV-MAN 001 [i.8].

infrastructure network domain: domain within the NFVI that includes all networking that interconnects compute/storage infrastructure

NOTE: It pre-exists the realization of VNFs.

infrastructure resource: resource provided by the infrastructure that can be used by virtualisation containers

NOTE: Infrastructure resource can either be a virtualised compute, storage, or network resource.

infrastructure resource group: logical resource collection grouping virtual resource instances assigned to a tenant along with software images

J to K

Void.

L

lifecycle management: set of functions required to manage the instantiation, maintenance and termination of a VNF or NS

M

managed container infrastructure object: object managed and exposed by the container infrastructure service management, representing the desired and actual state of a containerized workload, including its requested and allocated infrastructure resources and applicable policies

managed container infrastructure object package: aggregate of declarative descriptor and configuration files for multiple managed container infrastructure objects

measurement: set of operations having the object of determining a measured value or measurement result

NOTE: The actual instance or execution of operations leading to a Measured Value. (Based on the definition of Measurement in ISO/IEC 15939 [i.5], as cited in NIST Special Publication 500-307 [i.6]).

metric: standard definition of a quantity, produced in an assessment of performance and/or reliability of the network, which has an intended utility and is carefully specified to convey the exact meaning of a measured value

NOTE: This definition is consistent with that of Performance Metric in IETF RFC 2330 [i.3] and IETF RFC 6390 [i.4].

EXAMPLE: Packet transfer performance or reliability of a network.

multi-site network service: network service whose constituent Network Functions/NSs are deployed in more than one site

multi-tenancy: feature where physical, virtual or service resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible by each another

NOTE: This definition has been specialized from the term "multi-tenancy" as defined in Recommendation ITU-T Y.3500 [i.7].

N

Nested Network Service (NNS): network service that is part of a composite network service

NOTE: A Composite Network Service is a Network Service containing at least one Network Service.

network controller: functional block that centralizes some or all of the control and management functionality of a network domain and may provide an abstract view of its domain to other functional blocks via well-defined interfaces

network forwarding path: ordered list of connection points forming a chain of NFs, along with policies associated to the list

Network Function (NF): functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behaviour

NOTE: In practical terms, a Network Function is today often a network node or physical appliance.

Network Functions Virtualisation (NFV): principle of separating network functions from the hardware they run on by using virtual hardware abstraction

Network Functions Virtualisation Infrastructure (NFVI): totality of all hardware and software components that build up the environment in which VNFs are deployed

NOTE: The NFV-Infrastructure can span across several locations, e.g. places where data centres are operated. The network providing connectivity between these locations is regarded to be part of the NFV-Infrastructure. NFV-Infrastructure and VNF are the top-level conceptual entities in the scope of Network Function Virtualisation. All other components are sub-entities of these two main entities.

Network Functions Virtualisation Infrastructure (NFVI) components: NFVI hardware resources that are not field replaceable, but are distinguishable as COTS components at manufacturing time

Network Functions Virtualisation Infrastructure Node (NFVI-Node): physical device[s] deployed and managed as a single entity, providing the NFVI Functions required to support the execution environment for VNFs

Network Function Virtualisation Infrastructure Point of Presence (NFVI-PoP): N-PoP where a Network Function is or could be deployed as Virtual Network Function (VNF)

Network Functions Virtualisation Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM

Network Functions Virtualisation Management and Orchestration Architectural Framework (NFV-MANO Architectural Framework): collection of all functional blocks (including those in NFV-MANO category as well as others that interwork with NFV-MANO), data repositories used by these functional blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFV

Network Functions Virtualisation Orchestrator (NFVO): functional block that manages the Network Service (NS) lifecycle and coordinates the management of NS lifecycle, VNF lifecycle (supported by the VNFM) and NFVI resources (supported by the VIM) to ensure an optimized allocation of the necessary resources and connectivity

Network Interface Controller (NIC): device in a compute node that provides a physical interface with the infrastructure network

network operator: operator of an electronics communications network or part thereof

NOTE: An association or organization of such network operators also falls within this category (as defined in ETSI Directives [i.1]).

Network Point of Presence (N-PoP): location where a Network Function is implemented as either a Physical Network Function (PNF) or a Virtual Network Function (VNF)

Network Service (NS): composition of Network Function(s) and/or Network Service(s), defined by its functional and behavioural specification

NOTE: The Network Service contributes to the behaviour of the higher layer service, which is characterized by at least performance, dependability, and security specifications. The end-to-end network service behaviour is the result of the combination of the individual network function behaviours as well as the behaviours of the network infrastructure composition mechanism.

network service descriptor: template that describes the deployment of a Network Service including service topology (constituent VNFs and the relationships between them, Virtual Links, VNF Forwarding Graphs) as well as network service characteristics such as SLAs and any other artefacts necessary for the Network Service on-boarding and lifecycle management of its instances

network service orchestration: subset of NFV Orchestrator functions that are responsible for network service lifecycle management

network service provider: type of service provider implementing the network service

network stability: ability of the NFV framework to maintain steadfastness while providing its function and resume its designated behaviour as soon as possible under difficult conditions, which can be excessive load or other anomalies not exceeding the design limits

NF forwarding graph: graph of logical links connecting NF nodes for the purpose of describing traffic flow between these network functions

NF set: collection of NFs with unspecified connectivity between them

NFVI component: NFVI hardware resource that is not field replaceable, but is distinguishable as a COTS component at manufacturing time

NFV framework: totality of all entities, reference points, information models and other constructs defined by the specifications published by the ETSI ISG NFV

NFV Infrastructure (NFVI): totality of all hardware and software components which build up the environment in which VNFs are deployed

NOTE: The NFV-Infrastructure can span across several locations, i.e. multiple N-PoPs. The network providing connectivity between these locations is regarded to be part of the NFV-Infrastructure.

NFV-MANO management service: one or more capabilities offered by an NFV-MANO functional block for the support of its operations, administration and maintenance

NFV-MANO service: one or more capabilities offered via NFV-MANO functional blocks invoked using a defined interface

NOTE: This definition has been specialized from the term "cloud service" as defined in Recommendation ITU-T Y.3500 [i.7].

EXAMPLE: The VNFM offers a NFV-MANO service for VNF lifecycle management to the NFVO. The NFVO offers a NFV-MANO service for Network Service lifecycle management to OSS/BSS functions and uses the NFV-MANO service provided by the VNFM.

NFV-MANO service interface: interface, associated to an NFV-MANO service, over which operations can be invoked and/or notifications issued

NFV-MANO service user: natural person, or entity acting on their behalf, associated with an organization that uses NFV-MANO services

NOTE: This definition has been specialized from the term "cloud service user" as defined in Recommendation ITU-T Y.3500 [i.7].

NFVO-C: NFVO that manages a composite NS instance that has one or more nested NS instances as constituents which are managed by an NFVO in another administrative domain

NFVO-N: NFVO that manages an NS instance which is used as a nested NS of a composite NS instance managed by an NFVO in another administrative domain

NFV-Resource (NFV-Res): resource within the NFVI that can be used by the NS/VNF to allow for their execution

NFV security controller: trusted security management entity that provides secure dynamic delivery of security policies and services into the virtual network

NFV security services agent: entity responsible for securely receiving the Security Monitoring policy and implementing the same

NS healing: procedure that includes all virtualisation related corrective actions to repair a faulty Network Service (NS) instance including components/functionalities which make up the instance, and have been associated with this fault situation

NOTE 1: In a virtualised environment network service healing focuses only on the virtualised components/functionalities. In case of a NS consisting of virtualised and non-virtualised parts a procedure able to handle both parts is needed. This will be done in connection with components/functionalities that are located outside the virtualised environment.

NOTE 2: "Virtualisation related corrective actions" refers to action(s) toward virtualised resource(s) and associated NS instance.

node affinity for virtualised compute resources: persistent policy that forces virtualised compute resources to be on the same compute node

NOTE 1: "Persistent" is used here and in the following definitions to indicate that the affinity remains in effect until a change is requested by the consumer.

NOTE 2: This is to avoid cases where, for example, virtualised compute resource are initially on the same compute node but then later moved to separate nodes by the provider without any requested policy change from the consumer.

node affinity for virtualised storage resources: persistent policy that forces virtualised storage resources to be on the same storage node

node anti-affinity for virtualised compute resources: persistent policy that forces each virtualised compute resource to be on different compute nodes

node anti-affinity for virtualised storage resources: persistent policy that forces each virtualised storage resources to be on different storage nodes

O

Void.

P

PaaS Service: modular service or a function provided by PaaS to Consumer VNFs

NOTE: A PaaS service can be a VNF Common Service or a VNF dedicated service.

path: data communications feature of the system describing the sequence and identity of system components visited by packets, where the components of the path may be either logical or physical

NOTE: Examples of physical components include a physical switch or a network interface of a host, and an example of a logical component is a virtual network switch. Paths may be unidirectional or bi-directional. Paths may be further characterized as data plane or control plane when serving these classes of traffic, and as packet payload-agnostic or payload processing (as in the case of transcoding, compression, or encryption).

permitted allowance: constraint in terms of resource capacity, used by NFVO to control resource consumption by VNFMs in relation with VNF lifecycle operation granting

NOTE: Permitted allowances are maintained by the NFVO and might vary in granularity (VNFM, VNF, group of VNFs, NS, etc.).

Physical Network Function (PNF): implementation of a NF via a tightly coupled software and hardware system

Physical Network Function Descriptor (PNFD): template that describes the connectivity requirements of connection point(s) attached to a physical network function

NOTE: It is used by the NFVO to integrate PNF(s) into a NS.

Platform as a Service (PaaS): capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications

NOTE: Cloud Computing Services are typically offered to consumers in one of three service models NIST SP 800-146 [i.11], page 2-1 - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). In particular for PaaS, the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, platform services, but has control over the deployed applications and possibly over application hosting environment configurations.

Q

quota: upper limit on specific types of resources, usually used to prevent excessive resource consumption in the VIM by a given consumer

NOTE: Quota is enforced by the VIM.

R

reliability: probability that an item can perform a required function under stated conditions for a given time interval

resiliency: ability of the NFV framework to limit disruption and return to normal or at a minimum acceptable service delivery level in the face of a fault, failure, or an event that disrupts the normal operation

resource pool: logical grouping of NFVI hardware and software resources

NOTE 1: A resource pool can be solely based on a certain resource type (e.g. compute, storage, networking) or include a combination of them, and can span zero, one or multiple resource zones.

NOTE 2: An NFVI resource can be part of none, one or more than one resource pool.

resource zone: set of NFVI hardware and software resources logically grouped according to physical isolation and redundancy capabilities or to certain administrative policies for the NFVI

NOTE: The same resource cannot be part of two different resource zones.

EXAMPLE 1: Physical isolation may be achieved for example using a separate power supply, network equipment or physical building sites.

EXAMPLE 2: One example of resource zones are the Availability Zones in OpenStack.

S

scaling: ability to dynamically extend/reduce resources granted to the Virtual Network Function (VNF) as needed

NOTE: This includes scaling up/down and scaling out/in.

scaling out/in: ability to scale by add/remove resource instances (e.g. VM)

scaling up/down: ability to scale by changing allocated resource, e.g. increase/decrease memory, CPU capacity or storage size

service: component of the portfolio of choices offered by service providers to a user, a functionality offered to a user, as defined in ETSI TR 121 905 [i.2]

NOTE: A user may be an end-customer, a network or some intermediate entity.

Service Access Point (SAP): connection point where a NS can be accessed

NOTE: An SAP can either provide access to an NS, e.g. to an end-user, or interconnect different NS.

service consumer: person, device or company consuming a service provided by a service provider

service continuity: continuous delivery of service in conformance with service's functional and behavioural specification and SLA requirements, both in the control and data planes, for any initiated transaction or session till its full completion even in the events of intervening exceptions or anomalies, whether scheduled or unscheduled, malicious, intentional or unintentional

NOTE 1: From an end-user perspective, service continuity implies continuation of ongoing communication sessions with multiple media traversing different network domains (access, aggregation and core network) or different user equipment.

NOTE 2: End to end service continuity requires that the service is delivered with service quality defined by an SLA. This is true regardless if the service is delivered via a non-virtual network, virtual network or a combination.

Service Level Agreement (SLA): negotiated agreements between two or more parties, recording a common understanding about the service and/or service behaviour (e.g. availability, performance, service continuity, responsiveness to anomalies, security, serviceability, operation) offered by one party to another, and the measurable target values characterizing the level of services

NOTE: The scope of the above definition does not include business aspects of the SLA.

service provider: company or organization, making use of an electronics communications network or part thereof to provide a service or services on a commercial basis to third parties (as defined in ETSI Directives [i.1])

service resource: logical resource that can be used directly in a network service

NOTE: A service resource can be a NS, VNF, PNF, VNFFG or NFP.

service resource group: logical resource collection that groups a subset of service resource instances assigned to a tenant

NOTE: A service resource group can include NS, VNF, PNF, VNFFG and NFP.

software rollback: software modification process that reverts the system from the newly deployed software version to the previously deployed software version

software update: software modification process for bug fixes or enhancements without adding, modifying or removing functionality, interfaces or protocols

software upgrade: software modification process aimed at adding, modifying or removing functionality, interfaces or protocols

T

tenant: one or more NFV-MANO service users sharing access to a set of physical, virtual or service resources

NOTE 1: This definition has been specialized from the term "tenant" as defined in Recommendation ITU-T Y.3500 [i.7].

NOTE 2: The "tenant" concept in NFV should not be confused with the "tenant" (aka "project") concept in OpenStack. The OpenStack implementation covers a subset of the overall functionalities required by multi-tenancy in NFV.

tenant domain: domain that provides VNFs, and combinations of VNFs into Network Services, and is responsible for their management and orchestration, including their functional configuration and maintenance at application level

trust domain: collection of entities that share a set of security policies

U

user service: component of the portfolio of choices offered by service providers to the end-users/customers/subscribers

V

Virtual Application (VA): more general term for a piece of software which can be loaded into a virtual machine

NOTE: A VNF is one type of VA.

virtual link: set of connection points along with the connectivity relationship between them and any associated target performance metrics (e.g. bandwidth, latency, QoS)

NOTE: The virtual link can interconnect two or more entities (VNF components, VNFs, or PNFs) and it is supported by a Virtual Network (VN) of the NFVI.

Virtual Machine (VM): virtualised computation environment that behaves very much like a physical computer/server

NOTE: A VM has all its ingredients (processor, memory/storage, interfaces/ports) of a physical computer/server and is generated by a Hypervisor, which partitions the underlying physical resources and allocates them to VMs. Virtual Machines are capable of hosting a VNF Component (VNFC).

virtual network: virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity

NOTE: The virtual network is bounded by its set of permissible network interfaces.

Virtual Security Function (VSF): security enabling function within the NFV architecture

virtualisation container: partition of a compute node that provides an isolated virtualised computation environment

NOTE: Examples of virtualisation container includes virtual machine and OS container.

Virtualisation Deployment Unit (VDU): construct that can be used in an information model, supporting the description of the deployment and operational behaviour of a subset of a VNF, or the entire VNF if it was not componentized in subsets

NOTE: In the presence of a hypervisor, the main characteristic of a VDU is that a single VNF or VNF subset instance created based on the construct can be mapped to a single VM. A VNF may be modelled using one or multiple such constructs, as applicable.

Virtualised CPU (vCPU): virtualised CPU created for a VM by a hypervisor

NOTE: In practice, a vCPU may be a time sharing of a real CPU and/or in the case of multi-core CPUs, it may be an allocation of one or more cores to a VM. It is also possible that the hypervisor may emulate a CPU instruction set such that the vCPU instruction set is different to the native CPU instruction set (emulation will significantly impact performance).

Virtualised Infrastructure Manager (VIM): functional block that is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure Domain (e.g. NFVI-PoP)

Virtualised Network Function (VNF): implementation of an NF that can be deployed on a Network Function Virtualisation Infrastructure (NFVI)

Virtualised Network Function Component (VNFC): internal component of a VNF providing a VNF Provider a defined sub-set of that VNF's functionality, with the main characteristic that a single instance of this component maps 1:1 against a single Virtualisation Container

Virtualised Network Function Component (VNFC) Instance: instance of a VNFC deployed in a specific Virtualisation Container instance. It has a lifecycle dependency with its parent VNF instance

Virtualised Network Function Descriptor (VNFD): configuration template that describes a VNF in terms of its deployment and operational behaviour, and is used in the process of VNF on-boarding and managing the lifecycle of a VNF instance

Virtualised Network Function Instance (VNF Instance): run-time instantiation of the VNF software, resulting from completing the instantiation of its components and of the connectivity between them, using the VNF deployment and operational information captured in the VNFD, as well as additional run-time instance-specific information and constraints

Virtualised Network Function Manager (VNFM): functional block that is responsible for the lifecycle management of VNF

Virtualised Network Function Package (VNF Package): archive that includes a VNFD, the software image(s) associated with the VNF, as well as additional artefacts, e.g. to check the integrity and to prove the validity of the archive

Virtualised NIC (vNIC): virtualised NIC created for a VM by a hypervisor

virtualised resource migration: process of relocating the virtualised resource from one physical node to another physical node

NOTE: Examples of physical nodes are compute nodes and storage nodes.

virtualised Storage (vStorage): virtualised non-volatile storage allocated to a VM

virtualised Switch (vSwitch): Ethernet switch implemented by the hypervisor that interconnects vNICs of VMs with each other and with the NIC of the compute node

VNF component: See virtualised network function component.

VNFC instance: See virtualised network function component instance.

VNFC snapshot: replication of a VNFC instance at a specific point in time, capturing its full or partial state (such as state and content of the disks, memory and devices attached to the VNFC instance plus the infrastructure configuration of the VNFC instance)

VNFc snapshot package: collection of files representing a VNFC Snapshot which can be physically stored and transferred

VNF descriptor: See Virtualised Network Function Descriptor.

VNF Forwarding Graph (VNFFG): NF forwarding graph where at least one node is a VNF

VNF healing: procedure that includes all virtualisation-related corrective actions to repair a faulty VNF, and/or its VNFC instances and internal VNF Virtual Link(s)

NOTE: "Virtualisation related corrective actions" refers to the corrective action(s) toward virtualised resources and associated VNF/VNFC instance(s), and/or internal VNF Virtual Link(s).

VNF instance: See Virtualised Network Function Instance.

VNF lifecycle operation granting: permission to perform a VNF lifecycle management operation and the resource management operations necessary to complete it, if any apply

NOTE: There is no guarantee that the necessary resources are available after the grant is given. Information on resource requirements to execute a VNF LCM request is included in the Grant request. Granting of individual resource management operations is not in scope of VNF Lifecycle Operation Granting.

VNF manager: See virtualised network function manager.

VNF package: See virtualised network function package.

VNF provider: person or company that provides the VNF

NOTE: This includes, but is not limited to vendor, integrator or in-house developer. VNF Snapshot: replication of a VNF instance at a specific point in time, containing a consistent set of VNFC snapshots of all VNFC instances associated to the VNF instance, the VNF Descriptor and the VnfInfo (including state and settings of Virtual Links and Connection Points associated to this VNF).

VNF-related resource management in direct mode: mode of operation where the VNFM invokes on the VIM Virtualised Resources Management operations

NOTE 1: Resource reservation and quota management operations are out of the scope of this mode of operation, with the exception of query reservations and query quota.

NOTE 2: Virtualised Resources Management operations include allocation, migration, scaling, update, query, operation and termination of virtualised resources.

VNF-related resource management in indirect mode: mode of operation where the VNFM invokes on the NFVO Virtualised Resources Management operations and the NFVO in turn invokes them towards the VIM

NOTE 1: Resource reservation and quota management operations are out of the scope of this mode of operation, with the exception of query reservations and query quota.

NOTE 2: Virtualised Resources Management operations include allocation, migration, scaling, update, query, operation and termination of virtualised resources.

VNF set: collection of VNFs with unspecified connectivity between them

VNF Snapshot Package: collection of files representing a VNF Snapshot which can be physically stored and transferred

W to Z

Void.

3.2 Symbols

Void.

3.3 Abbreviations

0-9

5GCN 5G Core Network

A

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface

B

BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BSS	Business Support System

C

CIS	Container Infrastructure Service
CISM	Container Infrastructure Service Management
CDN	Content Delivery Network
CNS	Composite Network Service
COTS	Commercial Off The Shelf
CON	CONformance
CP	Connection Point
CPD	CP Descriptor
CPU	Central Processing Unit
CRUD	Create, Read, Update, and Delete

D

DF	Deployment Flavour
DHCP	Dynamic Host Configuration Protocol
DUT	Device Under Test

E

EM	(Network) Element Manager

F

FB	Functional Block
FCAPS	Fault, Configuration, Accounting, Performance and Security
FM	Fault Management
FUT	Function Under Test

G

Void.

H

HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure

I

IFS	Interoperable Features Statement
IMS	IP Multimedia System
I/O	Input/Output
IOP	InterOPerability
IP	Internet Protocol

ISF	Infrastructure Security Function
ISM	Infrastructure Security Manager
IT	Information Technology
IUT	Implementation Under Test

J

Void.

K

KPI	Key Performance Indicator

L

LAN	Local Area Network
LCM	Life Cycle Management

M

MAC	Medium/Media Access Control
MANO	Management and Orchestration
MCIO	Managed Container Infrastructure Object
MCIOP	Managed Container Infrastructure Object Package
MME	Mobility Management Entity
MMI	Man-Machine Interface
MPLS	Multi-Protocol Label Switching

N

N-PoP	Network Point of Presence
NAT	Network Address Translation
NETCONF	Network Configuration Protocol
NF	Network Function
NFP	Network Forwarding Path
NFPD	Network Forwarding Path Descriptor
NFV	Network Functions Virtualisation
NFV-Res	NFV Resource
NFVI	NFV Infrastructure
NFV-MANO	Network Functions Virtualisation Management and Orchestration
NFVI-Node	Network Functions Virtualisation Infrastructure Node
NFVI-PoP	Network Function Virtualisation Infrastructure Point of Presence
NFVO	Network Functions Virtualisation Orchestrator
NFV-SC	NFV Security Controller
NIC	Network Interface Controller
NNS	Nested Network Service
NS	Network Service
NSD	Network Service Descriptor
NSM	NFV Security Manager

O

OAM	Operations, Administration and Management
ONF	Open Networking Foundation
OS	Operating System
OSPF	Open Shortest Path First
OSS	Operation Support System

P

PaaS	Platform as a Service
PICS	Protocol Implementation Conformance Statement
PM	Performance Management
PNF	Physical Network Function
PNFD	Physical Network Function Descriptor
PoP	Point of Presence
PSF	Physical Security Function

Q

QE	Qualified Equipment
QF	Qualified Function
QoS	Quality of Service

R

RESTCONF	Representational State Transfer Configuration Protocol
RPC	Remote Procedure Call

S

SAL	Service Availability Level
SAP	Service Access Point
SAPD	Service Access Point Descriptor
SDN	Software Defined Networking
SEM	Security Element Manager
SFC	Service Function Chaining
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SP	Service Provider
SR-IOV	Single Root Input/Output Virtualisation
SSA	Security Services Agent
SUT	System Under Test
SW	SoftWare

T

TCP	Transmission Control Protocol
TD	Test Description
TOSCA	Topology and Orchestration Specification for Cloud Applications
TPM	Trusted Platform Module (TCG)
TSS	Test Suite Structure

U

UML®	Unified Modelling Language

V

VA	Virtual Application
vCPU	Virtualised CPU
VDU	Virtualisation Deployment Unit
VIM	Virtualised Infrastructure Manager
VL	Virtual Link
VLAN	Virtual LAN
VLD	Virtual Link Descriptor
VM	Virtual Machine

VN	Virtual Network
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component
VNFCI	VNF Component Instance
VNFD	Virtualised Network Function Descriptor
VNFFG	VNF Forwarding Graph
VNFFGD	VNFFG Descriptor
VNFI	VNF Instance
VNFM	Virtualised Network Function Manager
VNI	VXLAN Network Identifier
vNIC	Virtualised NIC
VPN	Virtual Private Network
VR	Virtualised Resource
vRouter	virtual Router
VSF	Virtual Security Function
vStorage	virtualised Storage
vSwitch	virtualised Switch
VXLAN	Virtual eXtensible LAN

W

WAN	Wide Area Network
WIM	WAN Infrastructure Manager

X

XML	eXtensible Markup Language
XPath	XML Path Language

Y

YANG	Yet Another Next Generation

Z

Void.

Annex A: Bibliography

ETSI GS NFV-EVE 011: "Network Functions Virtualisation (NFV) Release 3; Virtualised Network Function; Specification of the Classification of Cloud Native VNF Implementations".

Annex B:
Change History

Date	Version	Information about changes
May 2019	1.4.3	Addition of contributions nfv(18)000280r1 and nfv(18)000281, editorial changes
May 2019	1.4.4	Addition of nfv(19)000123 Introduction and Executive Summary
Oct-Nov 2019	1.4.5	Addition of IFA029-originated changes from nfveve(19)000083 with removal of Cloud Native which could not be agreed in EVE#120

History

Document history		
V1.1.1	October 2013	Publication as ETSI GS NFV 003
V1.2.1	December 2014	Publication as ETSI GS NFV 003
V1.3.1	January 2018	Publication as ETSI GS NFV 003
V1.4.1	August 2018	Publication as ETSI GS NFV 003
V1.5.1	January 2020	Publication