ETSI GR NFV 003 V1.9.1 (2024-12)

GROUP REPORT

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

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or
print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any
existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI
deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to
the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of
experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law
and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness
for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not
limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property
rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages
for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use
of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 terms and abbreviations from different NFV specifications and reports in order to provide a common reference and facilitate shared understanding.

Introduction

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

# 1	Scope

The present document provides terms and abbreviations for NFV in order to achieve a "common language" across all the ISG NFV deliverables.

# 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; 5G; 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 15939:2017: "Systems and software engineering — Measurement process".

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

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

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

[i.9]	Void.

[i.10]	Void.

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

[i.12]	ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.13]	ETSI GS NFV 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architectural Framework Specification".

[i.14]	ETSI TS 123 501 (V17.11.0): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 17.11.0 Release 17)".

[i.15]	ETSI GS NFV-IFA 036: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Requirements for service interfaces and object model for container cluster management and orchestration specification".

3   Definition of terms, symbols and abbreviations

3.1   Terms

0-9

Void.

A

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 connectivity (virtual or physical)

> NOTE 1: "Persistent" is used here and in the following terms 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.

alarm: information about a specific condition requiring attention

> NOTE: An alarm does or does not represent an error.

alarm notification: message used to report an alarm

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 connectivity (virtual or physical)

> 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: Affinity and 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.

B

Void.

C

CIS cluster: set of CIS instances, and one or multiple CISM instances managing them

> NOTE: At minimum, the CIS cluster contains one CISM instance and one CIS instance.

CIS cluster enhancement capability: MCCO that provides additional capabilities to a CIS cluster

> NOTE: Clause C.2 of ETSI GS NFV-IFA 036 [i.15] introduces various examples of CIS cluster enhancement capabilities.

CIS cluster management: management of one or more CIS clusters

> NOTE: The CIS cluster management provides lifecycle management and FCAPS management of CIS clusters.

CIS cluster node: compute resource that runs a Container Infrastructure Service (CIS) instance or a Container Infrastructure Service Management (CISM) instance, or both

> NOTE: The CIS cluster node can be either based on physical resource (e.g. a bare-metal server), or virtualised resource (e.g. a virtual machine) in the NFVI.

CIS cluster nodes network: network connecting part of or the whole set of CIS cluster nodes conforming the CIS cluster

CIS cluster storage: set of storage resources attached to one or multiple CIS clusters

cloud-native: software design principle with certain properties and non-functional characteristics

> NOTE: Cloud-native principles include (but are not limited to): loose coupling, elasticity, resiliency, micro-service-based design, declarative consumption, automation and immutability.

cloud-native NF (CNF): software implementation which realizes all or part of an NF, which can be deployed on a Network Function Virtualisation Infrastructure (NFVI), and that adheres to cloud-native principles

> NOTE 1: In ETSI NFV, cloud-native VNF and cloud-native NF refer to same concept and can be used interchangeably.

> NOTE 2: A CNF can be realized as a containerized VNF, VM-based VNF or hybrid VNF.

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

compute domain: domain within the NFVI that includes compute and storage related resources

> NOTE: A compute domain can be made up of any type (e.g. physical, virtualised) or combination of different types of NFVI resources that perform computation and storing of data.

compute MCIO: MCIO which declarative descriptor specifies compute infrastructure resource requests

compute node: abstract definition of a server

connectivity service endpoint: network connectivity termination point of a site representing the user network interface between the site and the external network that interconnects the site

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

> NOTE: Virtualised resources comprise compute, network and storage resources.

> EXAMPLE: A volume or object based virtual storage.

consumer: role played by a functional block or function that consumes certain services, which are exposed by another functional block or function through interfaces

consumer VNF: VNF that consumes services

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

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 managed container infrastructure object.

containerized NF: VNF whose software components are deployed within OS containers

NOTE: In ETSI NFV, containerized NF, container-based VNF and containerized VNF refer to the same concept and can be used interchangeably.

containerized workload: VNF or VNF component designed to be deployed and managed on Container Infrastructure Service (CIS) instances

D

daemon object: MCCO acting as a background process to run in the CISM to deploy MCCO instances having the same functionality onto applicable CIS cluster nodes

NOTE: Clause C.3 of ETSI GS NFV-IFA 036 [i.15] introduces examples of daemon objects.

declarative API: API enabling a consumer to declare the desired state of one or multiple managed objects without defining the actions to reach such a state

deployment flavour: specific deployment configuration 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-REL 001 [i.12].

F

failure: deviation of the service from fulfilling its functionality

NOTE: Adapted from ETSI GS NFV-REL 001 [i.12].

fault: adjudged or hypothesized cause of an error

NOTE: See ETSI GS NFV-REL 001 [i.12].

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

G

Void.

H

hybrid CIS cluster: CIS cluster composed of a mixture of virtual and bare-metal CIS cluster nodes

hybrid VNF: VNF composed of a mixture of software components deployed in various forms

> NOTE: Forms of deployment of software components are OS containers and VMs. See also definitions of VM-based VNF and containerized NF.

hypervisor: software which partitions the underlying physical resources of a compute node, 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 NFVI resources via a service abstraction to another Administrative Domain, and is responsible for the management and orchestration of those resources

> NOTE: This term is from ETSI GR NFV-MAN 001 [i.8].

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

> NOTE: It pre-exists the realization of VNFs.

infrastructure resource: See virtualised infrastructure resource.

infrastructure resource group: See virtualised infrastructure resource group.

intent: formal specification of all expectations including requirements, goals and constraints

intent-driven management: network management paradigm that enables the intent owner to communicate intents to the intent handler, enabling the achievement of intent expectations without describing how to fulfil the intents

> NOTE: Declarative API can be an enabler for intent-driven management.

intent handler: role performed by a management entity when processing an intent object and being responsible for its fulfilment

intent object: management object whose information (models, properties and/or artifacts) is capable to capture the expectations of the intent

intent object instance: managed object instance that is instantiated at the intent handler based on the intent object received from the intent owner

intent owner: role performed by a management entity when formulating an intent object and using it in intent-driven management

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 CIS cluster object: abstract NFV object for CIS cluster management characterized by its configuration, state, requested and allocated infrastructure resources and applicable operational policies

managed container infrastructure object: object managed and exposed by the container infrastructure service management, representing the desired and actual state of a containerized workload **or of a subset of it**, 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 term "Measurement" in ISO/IEC 15939 [i.5], as cited in NIST Special Publication 500-307 [i.6]).

metric: 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 of term 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.

MSCS endpoint: logical network endpoint of an MSCS which represents the binding of a connectivity service endpoint with the MSCS

Multi-Site Connectivity Service (MSCS): connectivity service abstracting the details of information regarding the connections between two or more site connectivity service endpoints

Multi-Site Network Connection (MSNC): provisioned multi-site network connectivity enabling the data forwarding between two or more network edge points

> NOTE: The network edge points represent the ingress/egress ports of the network(s) in between the sites.

multi-site network service: network service whose constituent NFs/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 of term has been specialized from the term "multi-tenancy" as defined in Recommendation ITU-T Y.3500 [i.7].

N

namespace: logical grouping for a particular set of identifiers, resources, policies and authorizations

namespace quota: upper limit on specific types of resources that can be used by one or more managed container infrastructure objects within the scope of a namespace

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 optionally provides 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 that has well-defined external interfaces and well-defined functional behaviour

> EXAMPLE: Examples of NF as specified by 3GPP are listed in clause 4.2.2 of ETSI TS 123 501 [i.14], such as Access and Mobility Management Function (AMF).

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

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

NOTE 1: 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.

NOTE 2: There can be different infrastructure layers (or grouping sets) in the NFVI, i.e. physical infrastructure layer, virtualised infrastructure layer and CIS infrastructure layer, which together build up the environment for the deployment of VNFs.

Network Functions Virtualisation Infrastructure (NFVI) component: 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 Infrastructure (NFVI) resource: building block in the NFVI

NOTE 1: NFVI resource can be physical resource, virtualised resource or CIS resource.

NOTE 2: Virtualised resources include virtual compute, virtual network and virtual storage resources.

EXAMPLE 1: Example of virtual compute resource is a Virtual Machine (VM).

EXAMPLE 2: Examples of CIS resource are CIS instance, CISM instance and CIS cluster node.

EXAMPLE 3: Example of virtual storage resource is a volume or object based virtual storage.

Network Functions Virtualisation Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, VIM and other NFV-MANO functions, including CISM, CCM, PIM, MDAF, etc.

NOTE: The full set of functional blocks and functions in the NFV-MANO architectural framework is specified in ETSI GS NFV 006 [i.13].

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 MCIO: MCIO which declarative descriptor specifies network infrastructure resource requests

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 (NSD): template that describes the deployment of a Network Service including service topology (constituent VNFs and the relationships between them, virtual links, VNF Forwarding Graphs (VNFFGs)) 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

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

NFV intent: intent related to NFV capabilities

NOTE: Examples of NFV capabilities are lifecycle management of NS, VNF and virtualised resources, descriptors for NS and VNF, etc.

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 of term 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 of term 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

NOTE: NFV-resource can be any type (i.e. physical, virtualised and CIS cluster) or combination of different types of NFVI resources.

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

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

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 terms 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

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.

O

OS container: virtualisation container utilizing a shared Operating System (OS) kernel of its host

NOTE: The host providing the shared OS kernel can be a physical compute node or another virtualisation container.

P

PaaS Service: modular service or function provided by PaaS that can be used by one or more applications or services to complement or extend their functionality

NOTE: A PaaS Service for VNFs can be a VNF common service or a VNF dedicated service.

EXAMPLE: Messaging and storage services in PaaS systems, monitoring service, networked (or network-based) services like authentication, synchronization and encryption service.

PaaS Service consumer: specific set of applications or services that consume a PaaS Service

EXAMPLE: Consumers can be VNFs, NSs or other services.

path: data communications feature of a communication 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 can be unidirectional or bi-directional. Paths can 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 the NFVO to control resource consumption by VNFMs in relation with VNF lifecycle operation granting

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

physical infrastructure: set of physical resources comprising the NFVI

Physical Infrastructure Management (PIM): management of physical resources and associated firmware/software elements

Physical Infrastructure Management (PIM) function: function within NFV-MANO which is responsible for management of physical resources

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 an NS.

physical resource: hardware component that makes up the physical infrastructure of the NFVI

NOTE: Physical resource can be physical compute, physical network or physical storage, and have respective firmware/software enabling its operation and usage.

EXAMPLE: Servers, switches, routers, storage systems.

physical resource inventory: collection of all physical assets within NFVI

physical resource pool: logical grouping of physical resources within NFVI

NOTE 1: A physical 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: A physical resource can be part of none, one or more than one physical resource pool.

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 as defined in 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.

producer: role played by a functional block or function that produces certain services, and exposes them externally through interfaces to other functional blocks or functions

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: See virtualised 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 can 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 Virtualised Network Function (VNF) as needed

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

scaling out/in: ability to scale by adding/removing 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, functionality offered to a user

> NOTE 1: As defined in ETSI TR 121 905 [i.2].

> NOTE 2: A user can be an end-customer, a network or some intermediate entity.

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

> NOTE: A 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

> NOTE: Service continuity applies to any initiated transaction or session till its full completion even in the event of intervening exceptions or anomalies, whether scheduled or unscheduled, malicious, intentional or unintentional.

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 term 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

> NOTE: 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.

site: NFVI Point of Presence (NFVI-PoP)

> NOTE: "site" and "NFVI-PoP" terms can be used interchangeably in the context of management of connectivity for multi-site services.

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

storage MCIO: MCIO which declarative descriptor specifies storage infrastructure resource requests

T

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

> NOTE 1: This definition of term 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" (also known as "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 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 (e.g. VNF components, VNFs or PNFs) and it is supported by one or more 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) instance.

Virtual Network (VN): virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity

> NOTE: The Virtual Network (VN) is bounded by its set of permissible network interfaces.

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

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

NOTE: Examples of virtualisation container includes Virtual Machine (VM) 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 VNFC

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 can be a time sharing of a real CPU and/or in the case of multi-core CPUs, it can be an allocation of one or more cores to a VM. It is also possible that the hypervisor emulates 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 virtualised compute, storage and network resources in the NFVI, usually within one operator's Infrastructure Domain, e.g. NFVI-PoP

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

NOTE 1: Virtualised infrastructure resource can either be a virtualised compute, storage, or network resource.

NOTE 2: Virtualised infrastructure resource is sometimes also referred to as virtualised resource in the present document. Both terms refer to the same concept and can be used interchangeably.

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

Virtualised Network Function (VNF): software implementation which realizes all or part of an NF and 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 instance of an atomic deployable unit

NOTE: An instance of an atomic deployable unit is represented by a single VM for hypervisor-based virtualisation, or represented by one or a set of OS containers for OS virtualisation.

Virtualised Network Function Component (VNFC) instance: instance of a VNFC deployed in a specific atomic deployable unit instance

NOTE: A VNFC instance 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 resource pool: logical grouping of virtualised resources in the NFVI

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

> NOTE 2: A virtualised resource in the NFVI can be part of none, one or more than one virtualised resource pool.

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

virtual Switch (vSwitch): Ethernet switch implemented as a software application in a compute node that enables communication between virtualisation containers within the compute node and between virtualisation containers and the NICs of the compute node

> NOTE 1: When the virtualisation container is a VM, the vSwitch interconnects vNICs of VMs with each other and with the NIC of the compute node.

> NOTE 2: In previous versions of the present document the term was referred as "virtualised Switch".

VM-based VNF: VNF whose software components are deployed within VMs

VNF Common Service: PaaS Service for VNFs with a lifecycle independent from its consumers and that is consumable by one or more PaaS Service consumers

VNF Component (VNFC): See Virtualised Network Function Component (VNFC).

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 Dedicated Service: PaaS Service for VNFs with a lifecycle dependent on its consumers and that can only be consumed by a specific set of PaaS Service consumers

VNF descriptor: See Virtualised Network Function Descriptor (VNFD).

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 Instance).

VNF license terms information: human readable document by which the licensor of the VNF (e.g. VNF provider) describes the terms and conditions for granting the usage of the software to a licensee

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

VNF manager: See Virtualised Network Function Manager (VNFM).

VNF package: See Virtualised Network Function Package (VNF 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-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: 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 VNF runtime information (including state and settings of Virtual Links and Connection Points associated to this VNF)

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

W

WAN Infrastructure Manager (WIM): functional block that is responsible for the management of network connectivity between connectivity service endpoints in different sites

X 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

CCD	CIS Cluster Descriptor
CCEC	CIS Cluster Enhancement Capability
CCM	CIS Cluster Management
CCND	CIS Cluster Node Descriptor
CCNRD	CIS Cluster Node Resource Descriptor
CDN	Content Delivery Network
CIR	Container Image Registry
CIS	Container Infrastructure Service
CISM	Container Infrastructure Service Management
CNF	Cloud-native NF
CNI™	Container Network Interface
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	Element Management

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 Subsystem
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
MCCO	Managed CIS Cluster Object
MCIO	Managed Container Infrastructure Object
MCIOP	Managed Container Infrastructure Object Package
MDAF	Management Data Analytics Function
MME	Mobility Management Entity
MMI	Man-Machine Interface
MPLS	Multi-Protocol Label Switching
MSCS	Multi-Site Connectivity Service
MSNC	Multi-Site Network Connection

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	Network Functions Virtualisation Resource
NFVI	Network Functions Virtualisation 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
PIM	Physical Infrastructure Management
PM	Performance Management
PNF	Physical Network Function
PNFD	Physical Network Function Descriptor
PoP	Point of Presence
PSD	PaaS Services Descriptor
PSF	Physical Security Function
PSM	PaaS Services Management
PSR	PaaS Services Repository

Q

QE	Qualified Equipment
QF	Qualified Function
QoS	Quality of Service

R

RBAC	Role-Based Access Control
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
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   Network Functions Virtualisation Component Instance
VNFD   Virtualised Network Function Descriptor
VNFFG   VNF Forwarding Graph
VNFFGD   VNF Forwarding Graph Descriptor
VNFI   Network Functions Virtualisation 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
March 2020	V1.5.2	Early draft
June 2020	V1.5.3	Addition of contribution NFVEVE(20)000062r1 with REL changes
September 2020	V1.5.4	Incorporating contributions NFVEVE(20)000122 and NFVEVE(20)000126, with editorial fixes
January 2021	V1.5.5	Incorporating contribution NFVEVE(20)000150 and NFVEVE(21)000003 Incorporating NFVEVE(21)000010 and the online change to the vNIC term
February 2022	V1.6.3	Incorporating NFVEVE(22)000008r1 with terminology from MSCS
June 2022	V1.6.4	Incorporating NFVEVE(22)000084r1 with terminology for VNF licence management
September 2022	V1.6.5	Incorporating NFVEVE(22)000122 (some FEAT17 definitions) and NFVEVE(22)000132r1 (Producer and Consumer definitions)
October 2022	V1.6.6	Incorporating NFVEVE(22)000166 NFV003 - Aligning consumer's definition with producer's definition
October 2022	V1.6.7	Incorporating NFVEVE(21)000049 with definitions of compute/network/storage MCIO coming from IFA040
Jan 2023	V1.7.2	New draft
May 2023	V1.7.3	Incorporating NFVEVE(23)000059 with definitions related to CCM
Aug 2023	V1.7.4	Incorporating NFVEVE(23)000123 with abbreviations about PaaS Services management
May 2024	V1.8.2	New draft
May 2024	V1.8.3	Incorporating NFVEVE(24)000078_*FEAT17_NFV003ed191_Add_definition_CNF* with correction of alphabetical order for new abbreviation. Removal of spare spaces.
June 2024	V1.8.4	Incorporating: NFVEVE(24)000081_NFV003_Adding_the_existing_definition_of_intent_from_IFA050
September 2024	V1.8.5	Incorporating: NFVEVE(24)000103_FEAT33_NFV003ed191_Add_definitions_from_IFA053_v5_1_1_ NFVEVE(24)000109_NFV003_update_the_MAN001_reference NFVEVE(24)000112_NFV003_update_the_EM_abbreviation NFVEVE(24)000118r1_FEAT33_NFV003ed191_Update_existing_definitions_in_NFV003_ Adding missing CRs: NFVEVE(24)000029_FEAT21_NFV003ed191_Update_definition_of_VNF NFVEVE(24)000068_FEAT21_NFV003ed191_Update_definitions_related_to_PaaS
October 2024	V1.8.6	Incorporating: NFVEVE(24)000111_NFV003_Adding_definitions_for_Declarative_API_and_Intent-dri Rapporteur actions: - update of alphabetical order of terms in parts "I" and "V" - removal of duplicated term "VNF instance"

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
V1.6.1	March 2021	Publication
V1.7.1	January 2023	Publication
V1.8.1	September 2023	Publication
V1.9.1	December 2024	Publication