ETSI GS NFV-EVE 011 V3.1.1 (2018-10)

Network Functions Virtualisation (NFV) Release 3; Virtualised Network Function; Specification of the Classification of Cloud Native VNF implementations

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
DGS/NFV-EVE011

Keywords
cloud, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms and abbreviations 7
3.1 Terms 7
3.2 Abbreviations 7
4 Overview 8
5 Non-functional parameters for cloud native VNF Classification 9
5.1 Resiliency 9
5.1.1 Introduction 9
5.1.2 Intra-VNF redundancy 10
5.1.3 Inter-VNF redundancy 10
5.1.4 Monitoring and failure detection 11
5.1.5 Healing 11
5.1.6 Requirements 12
5.2 Scaling 12
5.2.1 Introduction 12
5.2.2 Scale-out and scale-in 13
5.2.3 Scaling in different dimensions 13
5.2.4 Scaling on NS level 14
5.2.5 Requirements 14
5.3 Composition 14
5.3.1 Introduction 14
5.3.2 Cloud native VNF composition 14
5.3.3 Requirements 15
5.4 VNF design for location independence 15
5.4.1 Introduction 15
5.4.2 Location independence 15
5.4.3 Requirements 15
5.5 VNF state handling 16
5.5.1 Introduction 16
5.5.2 State management 16
5.5.3 Requirements 17
5.6 Published APIs 17
5.6.1 Introduction 17
5.6.2 Requirements 17
5.7 Management aspects of Cloud Native VNFs 18
5.7.1 Introduction 18
5.7.2 Requirements 18
5.8 Use of containers 19
5.8.1 Introduction 19
5.8.2 Requirements 19
5.9 Zero-touch Management 19
5.9.1 Introduction 19
5.9.2 Automated configuration 19
5.9.3 Automated resource management 19
5.9.4 Requirements 20
5.10 Load-balancing 20
5.10.1 Introduction 20
5.10.2 Requirements 21

6 Classification of cloud native VNF implementations 21
6.1 Introduction 21
6.2 Cloud native VNF characteristics 21
6.2.1 Cloud native VNF characteristics and their classifications 21
6.3 Cloud native VNF Product Characteristic Descriptor 22
6.4 Cloud native VNF Package 22
6.4.1 Cloud native VNF capacity profile 22
6.4.2 Cloud native VNF operational profile 22
6.4.3 Requirements 22

Annex A (informative): Authors & contributors 24

Annex B (informative): Bibliography 25

Annex C (informative): Change History 26

History 30

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

1 Scope

The present document specifies a set of non-functional parameters to classify and characterize any VNF implementation including, for example, level of separation of logic and state, degree of scale-out, memory footprint, use of accelerators, and more. The present document contains normative provisions using this set of non-functional parameters in order to classify the VNF implementations as cloud native.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

[1] ETSI GS NFV-REL 006 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Reliability; Maintaining Service Availability and Continuity Upon Software Modification".

[2] ETSI GS NFV-IFA 010 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification".

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 NFV Network Operators Council White Paper (02-2017): "Network Operator Perspectives on NFV priorities for 5G".

[i.2] ETSI GS NFV-SWA 001 (V1.1.1) "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture".

[i.3] NFV White Paper: "Network Function Virtualization: An Introduction, Benefits, Enablers, Challenges & Call for action", Oct 22-24, 2012.

NOTE: Available at: https://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[i.4] ETSI GS NFV-REL 003 (V1.1.2): "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability".

[i.5] ETSI GS NFV-REL 001 (V1.1.1): "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.6] ISO/IEC 17788:2014: "Information technology - Cloud computing - Overview and vocabulary".

[i.7] ETSI GS NFV-EVE 004 (V1.1.1): "Network Functions Virtualisation (NFV); Virtualisation Technologies; Report on the application of Different Virtualisation Technologies in the NFV Framework".

[i.8] ETSI GR NFV-EVE 010 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Licensing Management; Report on License Management for NFV".

[i.9] ETSI GR NFV-EVE 008 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Charging; Report on Usage Metering and Charging Use Cases and Architectural Study".

[i.10] 3GPP TS 23.501 (V15.1.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15)".

[i.11] 3GPP TS 23.502 (V15.1.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 (Release 15)".

[i.12] ETSI GS NFV 003 (V1.4.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

3 Definition of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.12] and the following apply:

cloud native VNF: VNF with a full adherence to cloud native principles, or a VNF that is transitioning to cloud native principles

NOTE: The definition captures the understanding of the term as used in the present document.

data repository: volumes of storage in a dedicated entity that persists the VNF data and exposes access to the stored data

NFV micro-service: atomic service module, delivered as an all-inclusive software package, that covers a specific and coherent functional scope, is consumable over network interfaces, is managed independently from other micro-services, and runs as a computing process

published API: publicly available application programming interface that provides developers with programmatic access to a software application or web service

remote storage: data storage approach where the Data repository used by VNF/C instances is located in different NFVI-node/s than the VNF and is accessible over network interfaces

VNF Product Characteristics Descriptor (VNFPCD): artefact describing the non-functional characteristics of a VNF product

NOTE: Non-functional characteristics described in the VNFPCD include qualitative characteristics regarding VNF resiliency, performance, scalability, design, capacity, security, usability.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.12] and the following apply:

API	Application Programming Interface
CPU	Computer Processor Unit
DOPFR	Dynamic Optimization of Packet Flow Routing
EM	(network) Element Manager
LCM	Lice Cycle Management
MANO	Management and Orchestration
NSD	Network Service Descriptor
OS	Operating System

PaaS	Platform as a Service
SLA	Service Level Agreement
UE	User Equipment
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNFPCD	VNF Product Characteristics Descriptor

4 Overview

The present document focusses on the characterization of Virtualised Network Functions (VNF) as part of their configuration and deployment in "the Cloud". Such VNFs are assumed to be implemented using generic cloud computing techniques beyond virtualization [i.1]. For example, the VNFs can be built with re-usable components as opposed to a unique - and potentially proprietary - block of functions.

Cloud native VNFs are expected to function efficiently on any network Cloud, private, hybrid, or public. The VNF developer is therefore expected to carefully engineer VNFs such that they can operate independently in the desired Cloud environment. Cloud environment can be implemented based on hypervisor/VM or container technology. This is an indication of the "readiness" of VNFs to perform as expected in the Cloud. The objective of the present document is to develop the characterization of the "Cloud Readiness" of VNFs.

From an operator perspective, it is essential to have a complete description of cloud native readiness of VNFs; this description will help operators in their VNF selection process. To do this, it is essential that a set of non-functional parametric characterizations be developed that appropriately describe the cloud native nature of VNFs. Non-functional parameters describe the environmental behaviour of VNFs residing in the Cloud. They do not describe the actual working functions of the VNF; rather they describe how the VNF can reside independently in the Cloud without constant operator involvement.

The present document considers not only the "pure" cloud native VNF implementations (e.g. no internal resiliency or state) but also some transition implementations to cloud native such as the VNFs with internal resiliency.

Non-functional characteristics of a cloud native VNF are described through a VNF Product Characteristic Descriptor (VNFPCD) created by the VNF provider. Usage of the cloud native VNFPCD is as follows:

- The cloud native VNFPCD is used by an operator to decide on what VNF product to deploy to fulfil a particular functionality, when the decision is based on non-functional parameters.
- The VNFPCD can be used in a VNF market place for a standardized description of the VNF products non-functional characteristics and as such can be checked/searched for automatically.

The intent of the present document is to identify a minimum set of non-functional parameters by which VNFs are characterized as cloud native. The non-functional parameters are classified according to the specific environmental behaviour of the VNF.

Each behaviour then provides a list of specific non-functional parameters along with specific requirements such that the cloud native nature of the VNF can be satisfactorily established.

5 Non-functional parameters for cloud native VNF Classification

5.1 Resiliency

5.1.1 Introduction

One of the benefits expected from NFV is the option to repair service failures through automated reconfiguration of the service to move traffic loads to new VNF/VNFC software instances [i.3]. VNFCs are essentially components of applications deployed via cloud computing. The cloud computing paradigm [i.4] treats all applications as replaceable commodity units using the same mechanisms (e.g. create new instance and transfer load). In this paradigm, operation of the system is expected to continue despite the presence of failures. Some cloud operating environments continually exercise failover mechanisms during normal operations [i.5]. In such an environment, a cloud native VNF contributes to the resiliency of the network services. The high resiliency mechanisms are internal to the VNF itself; alternately the network service (NS) provides the mechanisms such that VNFs can be replaced quickly without negative effects on the NS's resiliency.

The resiliency of a VNF is impacted by characteristics such as the level of separation of logic and state. VNF state handling is addressed in clause 5.5. A cloud native VNF is responsible for meeting its resiliency goals, taking into account the expected availability of the targeted virtualization environment. To comply with the VNF resiliency expectations, the VNF design is expected to satisfactorily overcome problem situations such as the following:

- Resource outage caused by a single failure platform problem including potential failures of:
  - Hypervisor or other components of the virtualisation layer;
  - Compute resources;
  - Storage (outage or inaccessibility with or without data loss);
  - Connections (inter or intra VNF);
- Other outage situations would include multiple failures or outage of complete NFVI PoP;
- Significant planned downtime for NFVI PoP or parts of it such as the infrastructure goes through hardware and software upgrades;
- Failures of MANO:
  - functional blocks;
  - interworking between functional blocks;
- Failure of interworking between MANO functional blocks with the VNF;
- Planned downtime due to MANO upgrades.

A number of software resiliency characteristics are considered here to demonstrate how cloud native VNFs can achieve their resiliency expectations:

- VNFs with high resiliency expectations implemented using internal mechanisms;
- VNFs with low resiliency expectations are covered by external mechanisms, but need to support those mechanisms by providing certain information.

NOTE 1: VNFs with low resiliency guarantee may still implement internal mechanisms, e.g. for redundancy, but in their case e.g. a VNF internal single point of failure can be easier to accept because they can rely on external mechanisms in some situations.

NOTE 2: In some cases, both internal and external mechanisms for service recovery might be in place. External mechanism needs to be triggered any time virtualised resources fail, as that cannot be repaired by the VNF. In this respect, the description of VNFs with high or low resiliency expectations cannot really classify the cloud native VNF, but rather the implemented mechanisms for service recovery. Nevertheless, this clause uses an outside view on the VNF for the description.

NOTE 3: Aspects of geographic redundancy of VNFs are not covered here, since these aspects are not useful to realize a classification of VNFs.

The main mechanisms and requirements are listed in the following clauses.

5.1.2 Intra-VNF redundancy

In many cases resiliency is achieved on VNF level through redundancy of VNFCs, by distributed VNF architecture. By having multiple VNFC instances, it is possible to spread the VNFC instances out across servers, racks, data centres, and geographic regions. This level of redundancy can mitigate most failure scenarios and has the potential to provide a service with acceptable availability. Careful consideration of VNFC modularity also minimizes the impact of failures when an instance does fail.

In this case cloud native VNFs will be developed with sufficient levels of redundancy such that these VNFs perform in compliance with the resiliency requirements. It is critical that the redundancy mechanisms that are built into these VNFs are suitable to achieve the resiliency required by the service provider. The level of resiliency of the VNF constitutes a comparison criterion between different VNF implementations. VNF redundancy characteristics that need to be accurately described include the following:

- Redundancy Model: Active-active, active-spare, N+M redundancy.

NOTE 1: The redundancy model could be different per VNFC type in a cloud native implementation.

- Recovery Time: The mean time between the moment when a failure is detected and until the service provided by the VNFC is available again.

- Single Point of Failure: Typically, VNFs can only meet high resiliency expectations by providing redundancy for all components, links, etc. If a VNF can meet the resiliency expectations without redundancy on a certain point (e.g. because the failure probability is low enough), this single point of failure needs to be documented by the VNF provider.

- Impact of failure: Expected number of connections/sessions/flows/subscribers/, etc. impacted by common failures, e.g. VNFC/VNF/links instance failures.

NOTE 2: The impact of a failure will vary largely depending on the failure, the load on a VNFC/VNF and the VNF deployment flavour.

Details are discussed in ETSI GS NFV-REL 003 [i.4].

5.1.3 Inter-VNF redundancy

In this case, resiliency is achieved on NS level through redundancy of VNFs. Like described on VNFC level in clause 5.1.2, it is possible to spread the VNF instances out across servers, racks, data centres, and geographic regions. In this model, single VNFs may fail, since all services can quickly be moved to another VNF without violating resiliency expectations of the NS.

NOTE: The same holds true in case of PNFs being involved.

In case only inter-VNF redundancy is used i.e. cloud native VNFs do not implement redundancy internally by duplicating components, then they support other functional blocks, e.g. partner VNFs, load balancers, management systems, to take the necessary actions in case of failures.

These models are also discussed in ETSI GS NFV-REL 003 [i.4].

Possible mechanisms include:

- Health-check protocols e.g. between VNFs or to load balancers. The used protocols and way of decision-making for failovers need to be documented by the VNF provider.

- Storage for state data outside the VNF if necessary: Dependency on database or redundant file systems need to be documented by the VNF provider.
- As above, recovery times and risk factor need to be accurately documented by the VNF provider.

In this case the NSD needs an appropriate flavour with appropriate instantiation levels of these VNFs, in the appropriate locations to meet the SLA expectations.

5.1.4 Monitoring and failure detection

A cloud native VNF is responsible for accurate monitoring and detection of failures affecting the VNF and its components, by either supporting it in the VNF or exposing the necessary capabilities to other entities. Specifically, some of the cloud native VNFs are expected to be equipped with appropriate mechanisms to monitor and support the general operational health of the VNF. This is critical for supporting the implementation of many resiliency patterns essential to the maintenance of network service for the identification of unusual conditions that might indicate failure or the potential for failure.

Monitoring and failure detection characteristics include the following:

- Monitoring metrics: Detailed set of metrics provided by the monitoring capability that describes the state and health of the VNF;
- Error logging: The logging mechanism capture critical events at an appropriate level of detail;
- Failure detection scheme: The ability to detect appropriate levels of failures at:
  - VNF/VNFC level;
  - Intra VNF connections;
  - Inter VNF connections;
- Mechanisms to support fault analysis;
- Mechanisms for failure prediction (optional).

5.1.5 Healing

Cloud computing technology allows for several mechanisms for healing.

The redundancy mechanisms described in previous clauses already provide a certain level of healing. However, after a failure has occurred and the service has been recovered by performing some failover (at the VNFC or VNF level), the redundancy is lost (in case of active-standby) or reduced (in case of active-active or N+M). A second subsequent failure in that stage may lead to an outage.

However, for VNFs implemented in a cloud native approach the redundancy is not affected and no healing is required in the failover scenarios.

ETSI GS NFV-REL 001 [i.5] describes the two stages with remediation and recovery in detail:

- In case the cloud native VNF provides internal mechanisms for redundancy, these mechanisms should be supplemented with automated recovery actions. Typically, an automatic recovery action within the resource assigned to the VNF will be tried and the affected resource, if it cannot recover, needs to be replaced by a new resource allocated via the VIM. The resource replacement process needs to be controlled by MANO;
- In case of redundancy mechanisms outside the VNF (i.e. after a failure, another VNF takes over the service), typically an automatic repair action will be tried, and a notification is needed about success or failure of the automatic recovery. If the VNF cannot be recovered from the failure, MANO needs to terminate the VNF, free all resources and instantiate a replacement VNF.