ETSI GS NFV-REL 001 V1.1.1 (2015-01)

Network Functions Virtualisation (NFV); Resiliency Requirements

Disclaimer

This 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-REL001

Keywords
availability, network, network monitoring, reliability, resilience

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

Important notice

The present document can be downloaded from:
http://www.etsi.org

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

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**", "**may not**", "**need**", "**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 focuses on unique aspects related to network and service resiliency in a virtualised network environment. The challenges result from failures of virtualised network functions, failures of the underlying hardware and software infrastructure arising from conditions such as design faults, intrinsic wear out, operational mistakes, or other adverse conditions, e.g. natural disasters, excessive traffic demand, etc.

The scope of the present document includes:

- Usecase analysis for reliability and availability in a virtualised network environment.
- Analysis of service availability levels.
- Identification of requirements for maintaining network resiliency and service availability, the focus being additional requirements introduced by virtualisation. The mechanisms to be considered include the following:
  - Network function migration within and across system boundaries.
  - Failure detection and reporting at the various layers.
  - Failure prediction, prevention, and remediation.
  - State management.
  - Solving network availability issues caused by overload/call blocking conditions.
- Engineering and deployment guidelines for maintaining network resiliency and ensuring service availability.

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 http://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.

Not applicable.

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 ETSI GS NFV 002 (V1.1.1): "Network Functions Virtualisation (NFV); Architectural Framework".

[i.2] ETSI ETSI GS NFV 003 (V1.1.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Function Architecture".

[i.4] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.5] James P.G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, Paul Smith: "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines", Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET), vol.54 iss.8, June 2010, pp.1245-1265.

[i.6] Jean-Claude Laprie (ed.): "Dependability: Basic Concepts and Terminology", IFIP WG 10.4 - Dependable Computing and Fault Tolerance (draft), Aug. 1994.

[i.7] Malgorzata Steinder and Adarshpal S. Sethi: "A survey of fault localization techniques in computer networks", Science of Computer Programming, vol. 53, #2, November 2004, pp. 165-194.

[i.8] Recommendation ITU-T Y.2171 (2006): "Admission control priority levels in Next Generation Networks".

[i.9] Recommendation ITU-T Y.2172 (2007): "Service restoration priority levels in Next Generation Networks".

[i.10] Recommendation ITU-T E.800 (2008): "Terms and definitions related to quality of service and network performance including dependability".

[i.11] Recommendation ITU-T E.412 (2003): "Network management controls".

[i.12] 3GPP TR 32.814: "Telecommunication management; UTRAN and GERAN Key Performance Indicators (KPI)".

[i.13] ETSI TS 123 060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[i.14] Recommendation ITU-T Y.2801 (2006): "Mobility management requirements for NGN".

[i.15] ETSI TS 123 207: "End-to-end Quality of Service (QoS) concept and architecture".

[i.16] ETSI TS 102 250-2 (V2.2.1): "Speech and multimedia Transmission Quality (STQ); QoS aspects for popular services in mobile networks; Part 2: Definition of Quality of Service parameters and their computation".

[i.17] ETSI TS 102 250-5 (V2.2.1): "Speech and multimedia Transmission Quality Aspects (STQ); QoS aspects for popular services in mobile networks; Part 5: Definition of typical measurement profiles".

[i.18] ETSI TS 123 380: "IMS Restoration Procedures".

[i.19] T1A1.2 Working Group: "Network survivability performance." Technical Report T1A1.2/93-001R3, Alliance for Telecommunications Industry Solutions (ATIS), (1993).

[i.20] IETF RFC 5424 (2009): "The Syslog Protocol".

[i.21] IETF RFC 4412 (2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[i.22] IETF RFC 4594 (2006): "Configuration Guidelines for DiffServ Service Classes".

[i.23] IETF RFC 5865 (2010): "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic".

[i.24] IETF RFC 4090 (2005): "Fast Reroute Extensions to RSVP-TE for LSP Tunnels".

[i.25] QuEST Forum (2006): "TL 9000 (Telecom Leadership 9000)".

[i.26] ETSI NFV-INF 003: "Network Functions Virtualisation (NFV); Infrastructure; Compute Domain".

3 Definitions abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.2] and the following apply:

availability: availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided

NOTE: See [i.10].

challenge: characteristic or condition that may be manifest as an adverse event or condition that impacts the normal operation

NOTE: See [i.5].

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 [i.7].

failure: deviation of the delivered service from fulfilling the system function

NOTE: See [i.6].

fault: adjudged or hypothesized cause of an error

NOTE: See [i.6].

normal operations: state of the network when there are no adverse conditions present

NOTE 1: This loosely corresponds to the conditions for which the system was designed, when the network is not under attack, the vast majority of network infrastructure is operational, and connectivity is relatively strong.

NOTE 2: See [i.5].

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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization, Accountability
API	Application Programming Interface
BNA	Broad Network Access
BSS	Business Support System
CIMS	Cloud Infrastructure Management System
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSCF	Call Session Control Function
DAS	Direct Attached Storage
DDoS	Distributed Denial of Service
DIMM	Dual In-line Memory Module
DNS	Domain Name System
ECC	Error Correcting Code
EMS	Element Management System
ETS	Emergency Telecommunication Service
GERAN	GSM Edge Radio Access Network
GGSN	Gateway GPRS Support Node
HA	High Availability
IMS	IP Multimedia Subsystem
IO	Input/Output
IOMMU	Input/Output Memory Management Unit
IP	Internet Protocol
IS	Information Security
ISMS	Information Security Management System
ISP	Internet Service Provider
IT	Information Technologies
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Leightweight Directory Access Protocol
LSP	Label Switsch Path
LU	Logical Unit
MAC	Media Access Control
MITM	Man-in-the-Middle
MME	Mobility Management Entity
MPLS	Multi Protocol Label Switching
MS	Measured Service
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NEBS	Network Equipment-Building System
NF	Network Function
NFVI	Network Function Virtualisation Infrastructure
NFVI-PoP	Network Function Virtualisation Infrastructure Point of Presence
NFV-MANO	Network Function Virtualisation Management and Orchestration
NFVO	Network Function Virtualisation Orchestrator
NGN	Next Generation Networks
NIC	Network Interface Card
NIC-ID	Network Interface Card Identifier
NIST	National Institute of Standards and Technology
NSD	Network Service Descriptor
OAM	Operation, Administration, and Management
OI	Operational Issues
OS	Operating System
OSS	Operation Support System
OTT	Over The Top
PGW	Packet Data Network Gateway

PI	Physical Infrastructure
PNF	Physical Network Function
PoP	Point of Presence
QoS	Quality of Service
RAID	Redundant Array of Inexpensive/Independent Disks
RAS	Reliability, Availability, and Serviceability
RE	Rapid Elasticity
RNC	Radio Network Controller
RP	Resource Pooling
SA	Service Availability
SAN	Storage Area Network
SDN	Software Defined Networking
S-GW	Serving Gateway
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Messaging Service
SP	Service Provider
SQL	Structured Query Language
SQM	Service Quality Metrics
SR-IOV	Single Root I/O Virtualisation
SW	Software
TV	Television
UE	User Equipment
US	United States
UTRAN	UMTS Terrestrial Radio Access Network
VDU	Virtualisation Deployment Unit
VIM	Virtualised Infrastructure Manager
VLAN	Virtual Local Area Network
VM	Virtual Machine
VN	Virtualisation
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component
VNFD	Virtualised Network Function Descriptor
VNF-EMS	Virtualised Network Function Element Management System
VNF-FG	VNF Forwarding Graph
VNFM	Virtualised Network Function Manager
VoIP	Voice over IP
VoLTE	Voice over LTE
VPN	Virtual Private Network
VS	Virtual Storage
WAF	Web Application Firewall
WAN	Wide Area Network

4 Resiliency Problem Description & Objectives

4.1 Problem Description

Virtualised data centres are currently considered state-of-the-art technology in the Information Technology (IT) space, whereas in the telecom domain there are no widespread deployments yet. One key differentiator between the IT and telecom domains is the level of service continuity required (latency and throughput are other, but not in scope here): Whereas in the IT domain outages lasting seconds are tolerable and the service user typically initiates retries, in the telecom domain there is an underlying service expectation that outages will be below the recognizable level (i.e. in milliseconds), and service recovery is performed automatically. Furthermore, service impacting outages need to be limited to a certain amount of users (e.g. certain geography) and network wide outages are not acceptable for telecom providers: the customer impact of service failures is determined both by likelihood of failure and by the failure impact.

NOTE: The term "domain" is used throughout the present document in a general sense (e.g. not to imply "administrative domain").

Service continuity is not only a customer expectation, but often a regulatory requirement, as telecommunication networks are considered to be part of critical national infrastructure, and respective legal obligations for service assurance/business continuity are in place.

However, not every Network Function (NF) has the same requirements for resiliency: For example, whereas telephony usually has the highest requirements for availability, other services, e.g. Short Messaging Service (SMS), may have lower availability requirements. Thus, multiple availability classes are defined which should be supported by a Network Function Virtualisation (NFV) framework.

In a virtualised environment, there are certain important differences in approach relating to resiliency:

- from hardware availability to software availability
- from design for uptime to design for failure

Consequently, the virtualisation of NFs needs to fulfil certain top-level design criteria, which are outlined in the following clauses:

- Service continuity and failure containment
- Automated recovery from failures
- Prevent single point of failure in the underlying architecture
- Multi-vendor environment
- Hybrid Infrastructure

4.2 Network Function Virtualisation Resiliency Objectives

As outlined in the problem description, the key objective is to ensure service continuity, rather than focusing on platform availability. Both the application design itself as well as the virtualisation infrastructure are affected by this objective:

[Req.4.2.1] The Virtualised Network Function (VNF) needs to ensure the availability of its part of the end-to-end service, just as in the case of a non-virtualised NF.

[Req.4.2.2] The VNF designer needs to be able to define the requirements of the Network Function Virtualisation Infrastructure (NFVI), such as geo-redundancy requirements, resiliency requirements, etc., in the Network Service Descriptor (NSD) and VNF Descriptor (VNFD) passed to the NFV Management and Orchestration (NFV-MANO) function.

[Req.4.2.3] The NSD and VNFD need to provide capabilities to define resiliency requirements.

[Req.4.2.4] The NFV-MANO function shall provide the necessary mechanisms to recreate VNF automatically after a failure, such as a Virtual Machine (VM) failure.

[Req.4.2.5] The NFV-MANO function shall support failure notification mechanisms at run time. The VNF can optionally request notification of certain types of failures, and NFV-MANO need to support such a notification mechanism.

[Req.4.2.6] Failures in the NFVI shall be handled (i.e. detection and remediation) in the NFVI layer or the NFV-MANO (e.g. hardware failure, loss of connectivity, etc.).

[Req.4.2.7] The NFVI shall provide the necessary functionality to enable high availability at the VNF level, such as failure notification and remediation.

4.2.1 Service Continuity

The key design objective is the end-to-end availability of telecommunication services.

[Req.4.2.8] NFV frameworks shall ensure that not all services need to be "built to the peak", but Service Level Agreements (SLAs) can be defined and applied according to given resiliency classes.

[Req.4.2.9] Storage and transfer of state information need to be provided by the NFVI, where the VNF defines the information to be stored and the NFVI provides the respective object store.

Beside of the relative availability of a service, the impact of failures is the second important factor for service continuity for the service provider. It is up to the VNF to define limitations in terms of e.g. number of parallel users allowed, parallel transactions to be handled, etc. in order to limit potential failure impacts.

[Req.4.2.10] The NFV-MANO functions need to support capacity limitations per instance as part of the deployment instructions of a VNF.

The Virtualised Network Function Manager (VNFM) shall ensure these limitations and, for example, initiate the start of a new instance if the defined limits are reached. Furthermore, the NFVI shall ensure a strictly separated space where applications run: VNF failures (e.g. attempting to exceed processing or storage assignments) shall never impact other applications, hardware failures shall only affect those VMs assigned to that specific hardware, connectivity failures shall only affect connected NFs, etc. However, it is expected that these types of failure containment are already present in state-of-the-art IT virtualisation environments and that no specific requirements are needed.

[Req.4.2.11] In addition to the normal mode of service execution, service continuity shall be ensured in two situations, namely at session/service establishment and during relocation of a service.

Session/service establishment is a phase where only part of the functionality for a service is set-up, and only partial state information is available. Should a failure occur, very often the end user device has to re-initiate the service during this phase, and the NFs have to support this.

Relocation of a service within a NFVI-PoP or between NFVI-PoPs may occur, for example in the case of hardware failures or when changing traffic demand requires VNF scaling. This may involve the transfer of existing sessions or services with their respective state. Failures during this phase should also not result in service interruption.

4.2.2 Automated recovery from failures

A scalable NFVI, providing telecommunication service for millions of subscribers, shall support thousands of VMs, which requires a high degree of process automation. This automation shall also apply to failure situations.

[Req.4.2.12] On the NFVI level, there should be an automated fail-over in the case of for example compute, memory, storage or connectivity failures.

Within the deployment limitations defined by the VNF in the NSD and VNFD (e.g. latency requirements, processing capacity or storage requirements, etc.), the NFVO/VNFM shall re-assign NFV Resources to ensure service continuity. This re-assignment shall be seamless to the service user, but may involve notification to or interaction with the VNF. It should be noted, that hardware availability is not critical within a NFVI: hardware is always regarded as a pool of resources, and if some components are not accessible, VNFs are automatically re-assigned to different hardware from the same pool. Thereby, hardware repair becomes a scheduled maintenance activity rather than an emergency action.

4.2.3 No single point of failure

[Req.4.2.13] There is an overall requirement that a NFV framework shall not contain a single point of failure with the potential to endanger service continuity.

In conventional PNF implementations the hardware is a potential single point of failure (even though this hardware is typically duplicated within a node). With an NFVI, the dynamic allocation of highly standardized resources (processing, storage, connectivity) removes this bottleneck by design. However, an NFV framework requires a number of tools, such as hypervisors or NFV-MANO functions, which in themselves may become single points of failure. As long as these tools are only involved in loading or instantiating applications into a NFVI-PoP, this risk is comparable to that of today's Operation Administration and Management (OAM) tools, which typically have a lower availability than network nodes. However, tools required during VNF runtime shall be designed not to become a potential single point of failure.

A potential mechanism to avoid single points of failure is a hierarchical structure of resiliency measures. As an example, the risk of failure for a certain type of hypervisor may be mitigated by separating the NFVI into several blocks of resources managed by different types of hypervisors. In that case, the orchestration software can re-assign VMs to a different block in the case of a hypervisor failure.