ETSI GR NFV-REL 010 V3.1.1 (2019-06)

Network Functions Virtualisation (NFV) Release 3; Reliability; Report on NFV Resiliency for the Support of Network Slicing

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
DGR/NFV-REL010

Keywords
network, NFV, resiliency, slicing

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

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

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

Introduction

The present document studies diverse NFV resiliency facets for supporting network slicing. Following a reminder of the way slicing can be conducted with respect to the NFV framework, several aspects of slicing oriented NFV design are described, including the design of network services for network slices with availability targets. In support of network slicing, the following network service operations are discussed:

- scaling, i.e. the dynamic provisioning or deprovisioning of resources granted to VNFs;
- migration, i.e. the move of virtualised resources from one set of physical resources to another;
- restoration following failures if resources are available;
- resource reallocation, i.e. restoration if the desired resources are insufficient.

Modification of VNF software and NFVI resource software and their impact on network slice resiliency are examined. Recommendations regarding the support of network slicing are finally provided covering:

1) design time;
2) run time;
3) VNF and /NFVI software modification.

It is noteworthy that NFV-MANO resiliency is considered in ETSI GR NFV-REL 007 [i.11], i.e. it is not discussed in the present document.

1 Scope

The present document reports on the guiding principles of NFV resiliency assurance for the support of network slicing based on an NFV infrastructure. In order to achieve this objective, it covers all resiliency related operational facets supporting network slicing. This includes design, scaling, migration, software modification, resource reallocation in time of scarcity, and restoration following a failure (including failure containment). The present document finally provides recommendations for building NFV based dependable network slicing.

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] Recommendation ITU-R M.2083-0 (2015): "IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond".

[i.2] ETSI TS 128 530 (V15.0.0) (2018): "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 15.0.0 Release 15)".

[i.3] ETSI GR NFV-EVE 012: "Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework".

[i.4] 3GPP TR 28.801 (V15.1.0) (2018): "Study on management and orchestration of network slicing for next generation network (Release 15)".

[i.5] ETSI TS 123 501 (V15.5.0) (2019): "5G; System architecture for the 5G system (3GPP TS 23.501 version 15.5.0 Release 15)".

[i.6] 3GPP TS 22.261 (V15.2.0) (2017): "Service requirements for next generation new services and markets".

[i.7] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.8] ETSI GS NFV-REL 003: "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability".

[i.9] Network Functions Virtualisation (NFV) - Network Operator Perspectives on NFV priorities for 5G, February 21st, 2017.

NOTE: Available at http://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

[i.10] ETSI GS NFV-REL 006: "Network Functions Virtualisation (NFV) Release 3; Reliability; Maintaining Service Availability and Continuity Upon Software Modification".

[i.11] ETSI GR NFV-REL 007: "Network Functions Virtualisation (NFV); Reliability; Report on the resilience of NFV-MANO critical capabilities".

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

3 Definition of terms, symbols 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:

dedicated network service: nested network service which is only part of a single composite network service

N+M: Pool of N+M active resources allowing the failure of M (typically $M \leq N$) resources without impacting the availability of the service capacity of N resources

shared network service: nested network service which is shared by two (or more) composite network services

3.2 Symbols

Void.

3.3 Abbreviations

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

(R)AN	(Radio) Access Network
3GPP	3rd Generation Partnership Project
5G	5th Generation
AF	Application Function
AMF	Access and Mobility Management Function
AN	Access Network
API	Application Programming Interface
AUSF	Authentication Server Function
CN	Core Network
CS	Communication Service
CSMF	Communication Service Management Function
DC	Data Center
DN	Data Network
eMBB	enhanced Mobile Broadband
IMT	International Mobile Telecommunications
IoT	Internet of Things
ITU-R	International Telcommunication Union - Radiocommunication Sector
MIMO	Multiple Inputs, Multiple Outputs
mMTC	massive Machine Type Communications
NOMA	Non Orthogonal Multiple Access
NSMF	Network Slice Management Function
NSS	Network Slice Subnet
NSSF	Network Slice Selection Function
NSSMF	Network Slice Subnet Management Function
OSS	Operations Support System
PCF	Policy Control Function
RM	Redundancy Model
SDN	Software Defined Networking
SMF	Session Management Function
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
uRLLC	ultra Reliable and Low Latency Communications

4 NFV for supporting network slicing

4.1 Network slicing for providing diverse SLA

Although network slicing is not a new feature in the context of 5G systems, its applicability comes to fruition in the context of the new capabilities enabled by 5G. The 5G technologies can be viewed as disruptive technologies allowing to go beyond mass market mobile communications which can/will unify extremely diverse applications and use cases within a single framework. As an enabler for all types of usage in a digital society, e.g. energy, health, media and entertainment, factories of the future, automotive, these technologies do not focus exclusively on bandwidth increase, as the previous mobile generations. Instead they are being developed and offered as a universal technology: 5G is presented as a polymorphous approach capable of handling, from its conception, a variety of needs.

IMT 2020, defined by ITU-R, has listed some usage scenarios covering these needs [i.1]:

- enhanced Mobile Broadband (eMBB), i.e. improved performance and increased user experience, both outdoor (wide area coverage) and indoor (hotspot) - both scenarios have different requirements, i.e. seamless coverage and medium to high mobility for the former, high traffic capacity and high user data rate for the latter;
- ultra Reliable and Low Latency Communications (uRLLC), i.e. stringent requirements for capabilities such as throughput, latency, reliability and availability - the scenarios include critical needs for wireless control of industrial manufacturing or production processes, remote medical surgery, distribution automation in a smart grid, transportation safety, etc.;
- massive Machine Type Communications (mMTC), i.e. low volume of data not sensitive to latency transmitted by a very large number of connected devices - this scenario tackles the exponential increase of low cost and long battery life objects for IoT.

To address such diverse market segments, the multiservice 5G network will leverage new technologies at the air interface, e.g. MIMO (Multiple Inputs, Multiple Outputs), NOMA (Non Orthogonal Multiple Access), and new networking architectures relying on recent paradigms such as NFV (Network Functions Virtualisation) and SDN (Software Defined Networking). An expectation for the 5G system is to be able to provide optimized support for a variety of different services with diverse reliability and availability requirements, different traffic loads, and different end user communities through the use of network slicing. Network slicing uses virtualisation rather than provisioning dedicated physical networks for each type of usage, e.g. current Long Range network for IoT.

Indeed, the technical requirements for the wide variety of usage scenarios targeted cannot be met simultaneously. Instead usage classes are defined, each of which is being fulfilled by a network slice. Based on a common physical infrastructure providing virtualised resources, all slices may comprise one or more subnet slices that cover various components of the end-to-end network, such as the Access Network (AN) part and the Core Network (CN) part, and are optimized to fulfill the requirements of the network functions needed to support those use cases.

The current 3GPP vision [i.2] relates each *Communication Service (CS)*, e.g. usage scenario, to a particular *network slice* spanning over both the access network and the core network (Figure 4.1). Each slice is made of *network slice subnets* composed of network functions (not shown in the figure) which in the present document are assumed to share the same infrastructure.

The illustrative figure shows three communication services (CS_1, CS_2, CS_3) designed to use three network slices. Each of these network slices is composed of dedicated network slice subnets, and/or shared network slice subnets. For instance, network slice 1 is formed by one dedicated core network slice subnet (NSS_CN_1) and one dedicated access network slice subnet (NSS_AN_1). In contrast, network slice 3 is formed by two dedicated network slice subnets (NSS_CN_3, NSS_AN_3) and one network slice subnet shared with network slice 2 (NSS_AN_2).

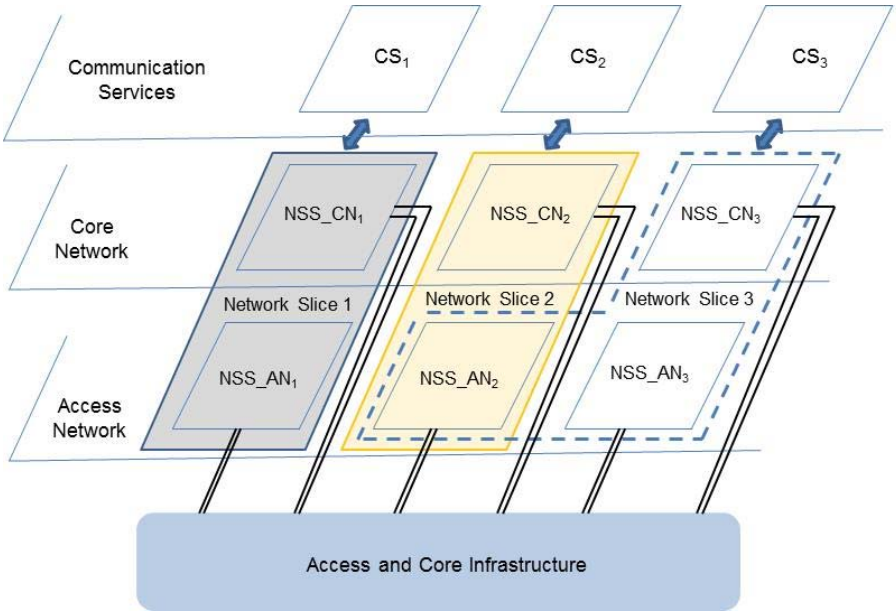


Figure 4.1: Customized slices for communication services

4.2 Mapping of NFV and network slicing concepts

Network slices and network slice subnets contain 3GPP network functions. If any of these functions is virtualised, the NFV approach can be utilized. For such cases, the 3GPP slicing concepts were mapped to the NFV concepts in ETSI GR NFV-EVE 012 [i.3]. A network slice or a network slice subnet can contain other network slice subnets, and their resources view can be realized via the network service concept in NFV, which also supports a nested network service hierarchy. Figure 4.2 (extracted from [i.3]) shows the proposed touchpoints between network slices and network services. This representation shows the relation between network slices, or network slice subnets, and the network services from a resource-centric standpoint.

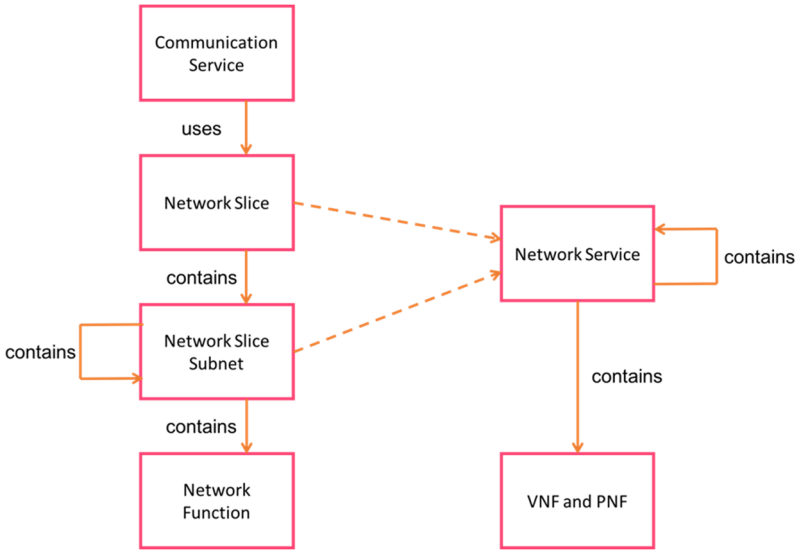


Figure 4.2: Network slicing and its counterpart in NFV [i.3]

Although 3GPP SA5 currently favours, in the context of network slicing, a service-based approach to the management of 3GPP 5G Core systems ETSI TS 128 530 [i.2], i.e. dealing with REST API services instead of management functional blocks, their previous report 3GPP TR 28.801 [i.4] has defined three management functions:

- Communication Service Management Function (CSMF) used to translate the communication service requirements to network slice requirements;

- Network Slice Management Function (NSMF) managing/orchestrating network slices, and deriving network slice subnet requirements from the network slices requirements;
- Network Slice Subnet Management Function (NSSMF) managing/orchestrating network slice subnets.

These management functions can interact with the NFV architecture as shown in Figure 4.3 via the Os-Ma-Nfvo interface.

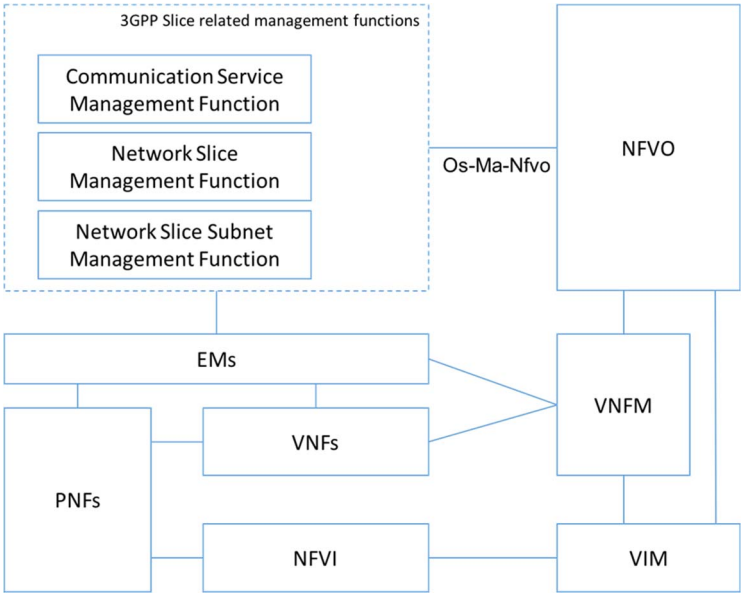


Figure 4.3: Network slice management in an NFV framework [i.3]

4.3 Network services and 3GPP network functions

As shown in Figure 4.2, 3GPP network functions are the constituents of network slices or network slice subnets. These network slices or network slice subnets can in turn be mapped to network services from a resource management viewpoint. These network services can be made of VNF(s) and can contain PNF(s), together with the Virtual Links between them, or can be made of *nested* network service(s) in addition to the VNF(s)/PNF(s) and the Virtual Links for the connectivity between them.

The 3GPP reference architecture for a 5G core system consists of different 3GPP network functions interacting with each other through various reference points N_i [i.5]:

- Application Function (AF);
- Access and Mobility Management Function (AMF);
- Authentication Server Function (AUSF);
- Network Slice Selection Function (NSSF);
- Policy Control Function (PCF);
- Session Management Function (SMF);
- Unified Data Management (UDM);
- User Plane Function (UPF);
- etc.

As an example, Figure 4.4 shows the non-roaming 5G system architecture using the reference point representation.

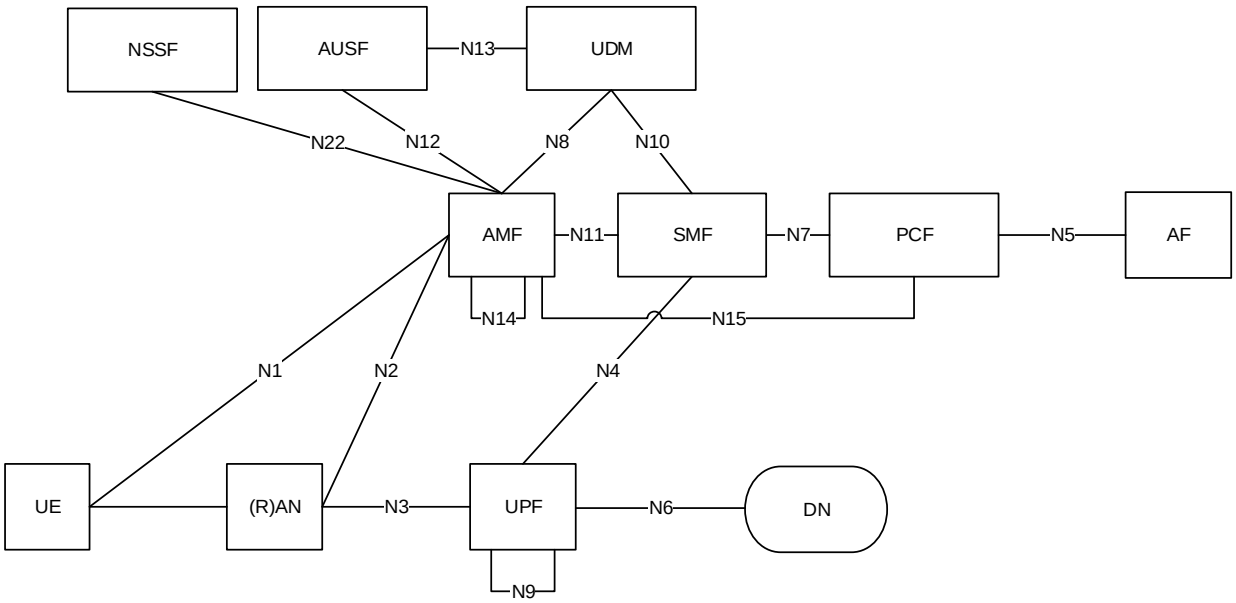


Figure 4.4: (Non-roaming) 5G system architecture [i.5]

A 5G system can be exposed and managed by using different network slice (or slice subnet) instances, for which the resources can be managed via NFV network service instances (see clause 4.2). While many models can be used to support the deployment of 3GPP network functions that are part of a network slice or a network slice subnet, two of the more complex deployment cases are selected below for analysis from a resiliency perspective:

- a 3GPP network function deployed as a network service instance, which is shared by different slice (slice subnet) instances. As the NFV-MANO is not aware of how the consumer (e.g. NSMF, NSSMF, OSS) is using the NS instances, then NFV-MANO does not know if a NS instance is shared or not between either network slice instances nor by different tenants;
- a 3GPP network function deployed as a network service instance dedicated to a given slice (subnet) instance.

It is noteworthy that a group of 3GPP network functions may be deployed as one VNF. In this case, the VNF resiliency and availability aspects apply, so it not further analysed in the present document.

The choice between these options is outside of the scope of NFV. NFV-MANO is not aware of the network slice instances, of network slice subnet instances, nor of the 3GPP network function instances that may be using a network service as part of their deployment. However, the information on whether a network service is shared or not has an impact on how NFV-MANO handles resiliency for the network service (e.g. see clause 6.1.1).

Figure 4.5 shows the example of a composite network service 1 (corresponding to a network slice or network slice subnet) instance with its dedicated network service NS_1 instance and sharing the network service NS_3 instance with a network service 2 (corresponding to another network slice or network slice subnet) instance. The latter also includes a dedicated network service NS_2 instance.

It is noteworthy to mention that the concept of shared network service instance is only visible to NFV-MANO in a nesting configuration. The analysis of the reliability and resiliency aspects in this study focuses then on the scenarios where nested NS instances are shared between composite NSs.

The NFV-MANO is only aware of the network service instances and their constituents, i.e. NS_1, NS_2 and NS_3, i.e. it is not aware of the network slices (or network slice subnets) using these resources.

NOTE: A top-level composite NS instance can also be shared by multiple network slices (or network slice subnets). However, this is not visible to NFV-MANO.

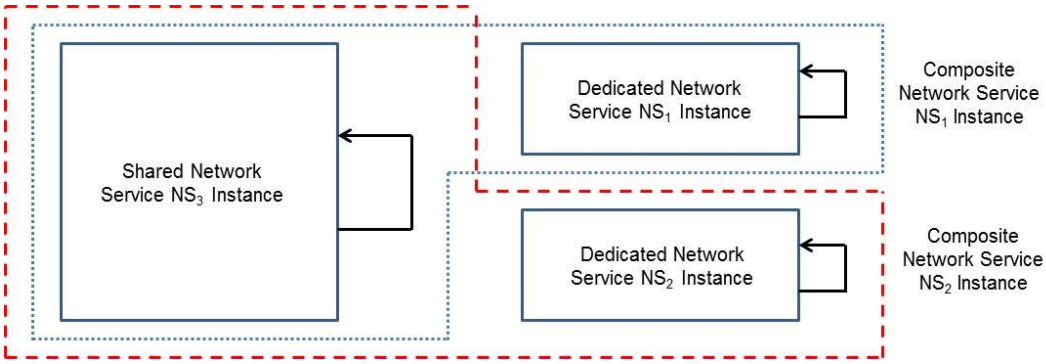


Figure 4.5: Composite network service instances with nested shared and dedicated network service instances

5 NFV resiliency concerns for network slice design

5.1 General considerations

The shared network service NS_3 instance in Figure 4.5 is a single logical entity of the whole 5G system architecture considered here, and might consist of VNFs/PNFs, virtual links and nested network services. Some constraints are thus imposed on the deployment, operation and maintenance of this network service instance. The first constraint is about *resiliency*. It is critical that the shared network service instance has the resiliency level needed to support each network slice (subnet) instance which uses it. Note that for the dedicated network services NS_1 and NS_2 instances, their need for reliability and availability strongly depends on the usage scenario sketched in clause 4.1. The second constraint is related to *isolation*. It needs to be ensured that the performance provided by NS_3 instance for each network slice satisfies the requirements and does not have negative impact in two different situations:

- the overload of one network slice instance should not impact the performance of the other network slice instance;
- the failure of one network slice instance should not cause operation anomalies in the other network slice instance.

If these cannot be guaranteed, then the network service instance should not be shared, but rather different network service instances (even using same NSD) should be created for each network slice.

NOTE 1: Failure isolation will be discussed in the clause 6.

As an example, Ultra Reliable and Low Latency Communications (uRLLC) requirements for this matter are obviously more stringent than for those expected for the massive Machine Type Communications (mMTC) scenario.

Actually, the availability values needed by different communication services of uRLLC range between 99,9 % and 99,9999 % according to 3GPP [i.6], i.e. beyond the traditional five 9 s commonly known as carrier grade. In order to reach such objectives, the supporting network services have to be designed and deployed appropriately, guidelines for which will be outlined in the following clauses.

The service availability of a network slice is realized by resiliency of its NSs (e.g. use of redundant network functions), the internal resiliency mechanisms of its network functions (VNFs/PNFs) and the related infrastructure resiliency. The different requirements of reliability and availability for uRLLC [i.5] imply that appropriate resiliency rules, e.g. anti-affinity placement for redundant network functions, resiliency class determining resource selection and handling policies, can be specified for the corresponding network services of uRLLC slices, which then can be deployed and maintained by the NFV-MANO. Accordingly, the service provider might deploy one (or several) network slice(s) to support uRLLC services.

NOTE 2: The availability figures have to be understood as applied to the whole 5G system from an end-to-end standpoint, e.g. from the UE "input" to the UPF "output" in Figure 4.4.

5.2 NFV NS resiliency for supporting network slices

As discussed in clause 4.3, the design of a network slice instance might consist of, for example, shared and dedicated network service instances. The availability/reliability requirements of network slice instances impose, on the one hand side, resiliency expectations on the virtualised resources supporting the slice instances; and on the other hand, the application of appropriate operational rules. Thus, appropriate anti-affinity, scaling policy configuration, reliability of virtualised resources, etc., have to be considered during the deployment of the network service instances supporting the creation and operation of network slice instances.

NOTE 1: The present document only considers VNFs resiliency. If the network slice instances comprise PNFs, the availability/reliability requirements for these PNFs have to be apprehended, according to the related slice use case, as in a legacy context, e.g. request for "five 9 s" availability.

Accordingly, to meet the availability/reliability requirements of a network slice instance, the supporting network service instances, made of virtualised/physical network functions (VNFs/PNFs), have to be designed and deployed with the following considerations:

- creating the proper NS design, e.g. NS deployment flavor by choosing VNFs deployment flavours and defining VL flavours to set up such NS and VNFs;
- specifying the appropriate reliability class of resources (for compute, storage, networking) for the related VNFs;
- assign and apply the appropriate policies.

Combinations of these features could be abstracted into resiliency classes targeting given availability/reliability requirements. For example, an availability expectation of five "9 s" and higher could be represented by resiliency class "high", an availability expectation of four "9 s" and up to five "9 s" by resiliency class "medium", an availability expectation below four "9 s" by resiliency class "low".

To minimize the probability of VNFs failure, a protection scheme has to be considered to face unavoidable errors. For this purpose, depending on the VNFs internal architecture, the selection of VNF deployment flavours needs to be consistent with the resiliency class requirements expressed for the associated network services. Table 5.1 shows some potential redundancy options for VNFs deployment. Such choices have to be communicated to the network services designer by the VNF vendors, e.g. through the VNF documentation. It is noteworthy to mention that, based on the requirements of the service provider, some redundancy options can be considered as shown in Table 5.1.

Table 5.1: Redundancy options

Level	Type	Localization
• VNFC: intra-VNF redundancy (i.e. built into the application logic) • VNF: intra-NS redundancy	• 1+1 Active-Active • 1:1 Active-Standby • N+M Pool/Cluster	• Local (on-site) redundancy (with anti-affinity rules) • Geo (off-site) redundancy

As for the related virtual links, the redundancy techniques include link aggregation, redundant single-homed or dual-homed connections, virtual networks providing alternative paths, etc.

NOTE 2: As for redundancy, diversity is another means for building resiliency [i.8], but it might not be reasonable, mainly for costs constraints, to apply this approach even to the highest resiliency class related VNFs. Actually, the use of redundant VNFs from different vendors in a NS is an attractive perspective, but may raise interoperability issues. The application of diversity to the virtualisation layer, e.g. using two different types of hypervisors, one for active VNFs and the other for standby VNFs in the 1:1 redundancy type, makes the operations not easy to manage.

As the VNFs resiliency partly depends on the underlying NFVI reliability, equipment of highest reliability would need to be allocated to the VNFs involved in the creation of network service instances of the highest resiliency class. In conjunction with the slice management function(s), at deployment, the NFV-MANO thus needs to provision the pertinent infrastructure means for realizing them.

To illustrate the options presented above for the creation of network service instances of different resiliency, Table 5.2 shows an example of network service configuration for both VNFs architecture and resources allocated to them.

Table 5.2: Examples of network service resiliency configuration

Network service resiliency class	Storage resource reliability	Compute resource reliability	Network service VNFs redundancy			Link redundancy
			Level	Type	Technique	
High	High	High	VNF and VNFC	1+1	Local + Geo redundancy	Redundant dual-homed
Medium	Medium	Medium	VNF and VNFC	1+1	Local + Geo redundancy	Redundant single-homed
Low	Regular	Regular	VNFC	N+M	Local redundancy	Link aggregation

If the first composite network service instance (NS_1I) has to be highly resilient, while the second composite network service instance (NS_2I) resiliency is medium, an application of this example to the two composite network services shown in Figure 4.5 could be the following (Table 5.3).

Table 5.3: Examples of composite network service resiliency configuration

Composite network service	Composite NS resiliency class	Shared or dedicated network service	Shared or dedicated NS resiliency class	Characteristics
NS_1I	High	NS_1	High	see Table 5.2
		NS_3	High	
NS_2I	Medium	NS_3	High	
		NS_2	Medium	

5.3 Designing network service for certain availability

5.3.1 Overall considerations

Since a network slice instance is deployed in the NFV environment as a concatenation of one or more Network Service (NS) instances [i.9], it can be said that the network slice instance availability depends on the availability of these NS instances, any of which may be a nested instance. Note that if two NS instances are redundant and backing up each other they can be considered as nested NS instance.

Accordingly, the network slice instance is available when all of the NS instances are available, which can be formulated as the product of the availability of the individual NS instances (A_{NSi}).

$$A_{Slice} = A_{NS1} * A_{NS2} * \ldots * A_{NSn} \quad (1)$$

Since typically an NS instance availability is less than 100 % or $A_{NSi} < 1$, the multiplication in equation (1) implies that at minimum the availability of each NS instance needs to be greater than the target availability of the network slice instance, i.e. $\forall A_{NSi} > A_{Slice}$.

Each of the NS instances themselves are compositions of VNF instances and nested NS instances. Unfolding the nested NS instances, the NS instance becomes a concatenation of VNFs, some or all of which might be deployed with redundant instances, in which case a Redundancy Model (RM) applies.

The VNF instances resulting from the unfolding of the NS instances can be re-grouped into new NS instances in such a way that it does not change the graph interconnecting the VNF instances, and each new NS instance contains only instances of a single VNF. E.g. if two instances of the same VNF are in sequence then they will form two NSs each with one VNF instance. If two instances of a VNF are redundant and are in parallel then they form a single NS with the two VNF instances related through a RM. Thus, these new simple NS instances consist of possibly redundant instances of a particular VNF. It can be said that the availability of such an NS instance depends on the availability of the one or more VNF instances (each with the availability of A_{VNF}) and the availability of the NFVI (A_{NFVI}) on which they are deployed.

Considering the NFVI and the VNF instances independent, the NS instance availability (A_{NS}) is:

$$A_{NS} = A_{NFVI} \times RM(A_{VNF}) \quad (2)$$

For the calculations, the NFVI can be considered as a whole, or as different subsets of components hosting different VNF instances. An example of the latter case is, when the NFVI hosting an NS is distributed over different locations and deployed with heterogeneous resources.

Assumption: For simplicity in equation (2) the NFVI is considered as a whole.

The RM function depends on the redundancy model used with the VNF instances, but in general it can be stated that $RM(A_{VNF}) \geq A_{VNF}$. That is, using some redundancy improves the availability of the individual VNF instances, i.e. $RM(A_{VNF}) > A_{VNF}$, while using no redundancy $RM(A_{VNF}) = A_{VNF}$.

Considering equations (1) and (2), to achieve a given availability for a network slice instance (A_{Slice}), it can be said that the availability of all NSs composing the network slice instance has to be greater than the targeted availability for the network slice instance. That is, $\forall A_{NSi} > A_{Slice}$, where A_{NSi} indicates the availability of the *i*th NS of the network slice instance. Therefore, the conditions $A_{NFVIi} > A_{NSi} > A_{Slice}$ and $RM(A_{VNFi}) > A_{NSi} > A_{Slice}$ need to be fulfilled, where A_{NFVIi} indicates the availability of the NFVI on which the *i*th NS is built and A_{VNFi} is the availability of the VNF composing it.

In Table 5.2, three different configurations were proposed to achieve different resiliency levels represented by NS resiliency classes. Each row proposed a selection of NFVI components and redundancy models of the VNFs and VLs to achieve a given NS resiliency class. However, the above considerations suggest that this approach may not be suitable, and it is necessary to know the absolute availability value a VNF can provide under ideal conditions. That is, when the availability is influenced only by the VNF implementation itself without external assistance and without external hindering, i.e. the interest is in the availability, the VNF can provide on its own without the help of an admin or external availability management.

With respect to Table 5.2, let consider only two different resiliency classes and define resiliency class "high" with an availability of equal to or greater than 99,999 % and "low" if the availability is below this. This means that if this classification is applied individually to the different NFVI resources represented in the columns and if the availability of each of them is equal to 99,999 % (or A = 0,99999), then they are each considered of the category "high" as the first row of the table shows. If these different resources are used to compose an NS, then the availability of the resources needs to be multiplied to calculate the availability of the composed NS. Since all the composing resources have an availability A = 0,99999 any multiplication will result in an availability lower than A = 0,99999 (e.g. 0,99999 × 0,99999 = 0,9999800001), which according to the definition falls into the "low" category. The more such resources are needed for the NS the more the overall availability falls below expected by the "high" category.

Considering the redundancy models as discussed with respect to equation (2), they can improve the availability of the individual VNF instances which is discussed next. This discussion is based on the considerations in ETSI GS NFV-REL 003 [i.8].

5.3.2 Availability of redundant entities

5.3.2.1 Consideration of VNF-internal redundancy

For the NFV-MANO, the VNF is a black box with respect to its internal redundancy. The NFV-MANO does not manage nor is aware of the redundancy applied to the VNFC instances. Instead the NFV-MANO instantiates a VNF according to the instantiation level of the deployment flavour (DF) selected and for scaling it follows the scale levels associated with the DF.

The scale levels dictate the number of VNFC instances the NFV-MANO should instantiate for each VNFC. Since redundancy is reflected in the number of VNFC instances, it is safe to assume that scale levels of a DF of a VNF reflect the redundancy model used within the VNF for each VNFC. Note that different VNFCs may utilize different redundancy models within the same VNF and may be scaled differently. It is also possible that a given VNFC is used with different redundancy models in different DFs of the same VNF and accordingly it may be scaled differently in different DFs. That is, the scale levels associated with a DF take into consideration both the workload related performance and the needs of the redundancy model used for each of the VNFCs used in the DF.

Therefore, it is better to know the absolute availability a VNF DF provides than the redundancy model(s) used by that DF for the different VNFCs. In this respect however, it is expected that the different scale levels of a DF and any applicable scaling policy in the VNFD are provided in such a way that the availability indicated for the DF, for example, in the VNF documentation is guaranteed at each scale level of the DF assuming ideal conditions. That is, the absolute availability is the availability influenced only by the VNF implementation itself without external assistance and without external hindering. This mean for example that the NFVI is 100 % reliable i.e. $A_{NFVI} = 1$. Thus, the availability of a VNF DF (A_{VNF-DF}) is given according to equation (2) for the case when an instance of the VNF is deployed with the given DF under such ideal conditions.

$$A_{NS} = 1 * A_{VNF-DF}$$

NOTE: Since currently there is no standard method of evaluating the absolute availability of VNFs under ideal conditions (e.g. 100 % NFVI availability), the values provided by different vendors for their VNF products may not be comparable or repeatable by the service providers.

When this DF is deployed on a less than ideal NFVI then without VNF-level redundancy the NS availability achievable can be calculated as:

$$A_{NS} = A_{NFVI} * A_{VNF-DF}$$

Or the VNF DF can be selected according to the target NS availability and the available NFVI availability as:

$$A_{VNF-DF} \geq \frac{A_{NS}}{A_{NFVI}} \quad (3)$$

Depending on the NFVI resources and VNFs at disposal this availability may not be sufficient for the NS, in which case the VNF instances have to be deployed redundantly. For example, a redundant deployment of VNF instances is used in geo-redundant configurations, i.e. when disaster recovery is a requirement.

5.3.2.2 Availability estimation for the 1+1 and 1:1 redundancy models

In the 1+1 and 1:1 redundancy models, each VNF instance has a redundant VNF instance as protection. The first VNF instance is active and serves the workload. The protecting VNF instance may also be active in which case the two VNFs share the actual workload; or it may be a standby for the first/active VNF instance. In either case, the NFV-MANO does not manage the active/standby role assignments of the VNF instances nor it is aware of these role assignments.

The NFV-MANO is only responsible to provide virtualised resources of enough capacity that allow full protection for the entire workload handled by the VNF instance-pair so that there is no service degradation in case one of the instances fails. Hence, the availability estimation is the same for both redundancy models and reflects the availability with respect to the resources provided by the NFV system.

Figure 5.1 depicts an instance of a simple Network Service (NS), which is composed of one VNF. In the NS instance the VNF has an active (VNF^a) and a standby (VNF^b) instance. They are hosted on the same NFVI, but they form an anti-affinity group therefore rely on different physical resources within the NFVI.

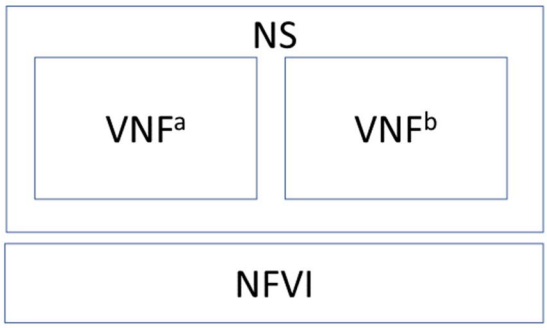


Figure 5.1: 1:1 redundancy model

To calculate the overall availability in this case, the NS instance is available when the NFVI and at least one of the VNF instances are available. So, the NS instance is not available if the NFVI or both VNF instances fail. Therefore:

$$A_{NS} = A_{NFVI} * (1 - (F_{VNF^a} * F_{VNF^b}))$$

where, $F_{VNF} = 1 - A_{VNF}$

$$A_{NS} = A_{NFVI} * (1 - ((1 - A_{VNF^a}) * (1 - A_{VNF^b})))$$

If VNF[a] and VNF[b] are deployed using the same DF, which provides the same availability for all scale levels, then:

$$A_{VNF^a} = A_{VNF^b}$$

Therefore, the NS instance availability becomes:

$$A_{NS} = A_{NFVI} * (1 - (1 - A_{VNF^a})^2)$$

$$A_{NS} = A_{NFVI} * (1 - (1 + A_{VNF^a}^2 - 2 * A_{VNF^a}))$$

Which can be re-written as:

$$A_{NS} = A_{NFVI} * (2 * A_{VNF} - A_{VNF}^2) \quad (4)$$

5.3.2.3 Availability estimation for the N+M and N:M redundancy models

As in the previous case the NFV-MANO does not manage nor is aware of the active/standby roles of the VNF instances. It only manages the number of VNF instances based on the volume of the workload handled by the instances. Therefore, from the NFV-MANO perspective these models indicate the number of VNF instances needed to serve the workload without protection (N) and the number of VNF instances that can fail (M) before any workload degradation occurs; i.e. M instances provide protection for the workload capacity of N instances. Hence, from the NFV perspective only resource level availability can be considered, i.e. any of the M redundant instances can replace any of the N instances.

Let assume again that an instance of a simple NS with one VNF, which has four instances as shown in Figure 5.2. The VNF instances use the 3:1 redundancy model which means that, out of the four, three are active VNF instances (e.g. VNF[a], VNF[b] and VNF[c]) and one is standby (VNF[d]). All of them are deployed on the same NFVI, but they form an anti-affinity group therefore rely on different physical resources.

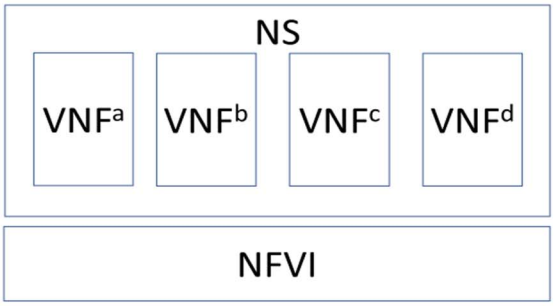


Figure 5.2: 3:1 redundancy model

Since there is only one redundant VNF instance (M = 1), if more than one (generally, more than M) VNF instance(s) fail(s), the overall availability goal is not met, i.e. the service becomes degraded or fails completely. To avoid this, the minimum number of VNF instances N has to be available, which is three in this case. As a result, the availability of the NS instance would be:

$$A_{NS} = A_{NFVI} * (the\ probability\ of\ having\ at\ least\ three\ available\ VNF\ instances)$$

$$A_{NS} = A_{NFVI} * (A_{VNF^a} * A_{VNF^b} * A_{VNF^c} * F_{VNF^d} + A_{VNF^a} * A_{VNF^b} * F_{VNF^c} * A_{VNF^d} +$$

$$A_{VNF^a} * F_{VNF^b} * A_{VNF^c} * A_{VNF^d} + F_{VNF^a} * A_{VNF^b} * A_{VNF^c} * A_{VNF^d} +$$

$$A_{VNF^a} * A_{VNF^b} * A_{VNF^c} * A_{VNF^d})$$

Assuming that all the VNF instances are deployed with the same VNF DF, then:

$$A_{VNF^a} = A_{VNF^b} = A_{VNF^c} = A_{VNF^d} = A_{VNF}$$

Therefore, the availability of the NS instance is:

$$A_{NS} = A_{NFVI} * (4 * A_{VNF}^{3} * F_{VNF} + A_{VNF}^{4})$$

Accordingly, to keep the NS instance available, the NFVI has to be available and, in addition, a selection of three VNF instances out of the four, or a selection of four VNF instances out of the four has to be available. This means that the above can be re-written as:

$$A_{NS} = A_{NFVI} * (\binom{4}{3} * A_{VNF}^{3} * (1 - A_{VNF})^{1} + \binom{4}{4} * A_{VNF}^{4} * (1 - A_{VNF})^{0})$$

This equation can be generalized as:

$$A_{NS} = A_{NFVI} * (\sum_{k=0}^{M} \binom{N+M}{N+k} A_{VNF}^{N+k} * (1 - A_{VNF})^{M-k})$$

where $N > 0$ & $M \geq 0$ (5)

5.3.2.4 Availability estimation for single- and dual-homed link redundancy

The availability of an NS instance also depends on the availability of the virtual links (VLs) interconnecting the different VNF instances. For the estimation of the availability of the virtual links single- and dual-homing are considered.

To begin with, two simple cases of VL redundancy are considered in an NS with two VNFs:

- NS_1 uses single-homing as redundancy for the VLs between the instances of VNF1 and VNF2 as shown in Figure 5.3.
- In contrast, NS_2 uses dual-homing as shown in Figure 5.4.

The assumption is that the redundant VLs form anti-affinity groups therefore rely on different physical resources.

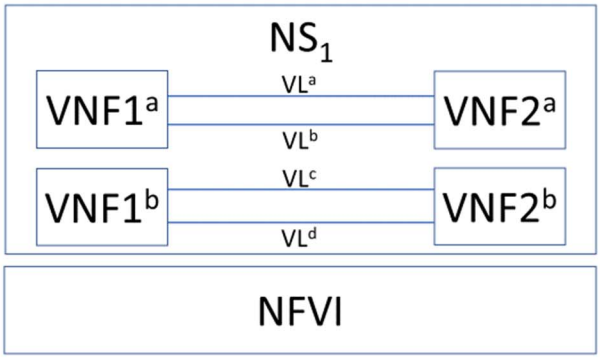


Figure 5.3: Single-homed link redundancy

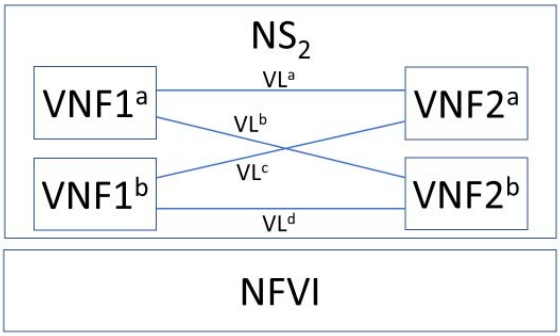


Figure 5.4: Dual-homed link redundancy

To calculate the availability for these NS instances, it is assumed:

$$A_{VNF1^a} = A_{VNF1^b} \text{ and } A_{VNF2^a} = A_{VNF2^b}$$

$$A_{VL^a} = A_{VL^b} = A_{VL^c} = A_{VL^d} = A_{VL}$$

Then, NS_1 is available if the NFVI is available and:

1) *VNF1*^{a} and *VNF2*^{a} and at least one of *VL*^{a} and *VL*^{b} is available; or

2) *VNF1*^{b} and *VNF2*^{b} and at least one of the *VL*^{c} and *VL*^{d} is available; or

3) Both above conditions are met.

Therefore:

$$A_I = A_{II} = A_{VNF1} \times (1 - F_{VL}^2) \times A_{VNF2}$$

$$A_{NS_1} = A_{NFVI} \times (1 - F_I \times F_{II})$$

where A_I and F_I indicate the availability and the failure (i.e. non-availability) for case I, and A_{II} and F_{II} indicate the same for case II. Since $F_I = F_{II}$ based on the assumptions and $A = 1 - F$, A_{NS_1} can be re-written as (6):

$$A_{NS_1} = A_{NFVI} \times (1 - (1 - A_{VNF1} \times (1 - F_{VL}^2) \times A_{VNF2})^2) \quad (6)$$

NS_2 is available if at least one of *VNF1*^{a} and *VNF1*^{b} is available and one of the *VNF2*^{a} and *VNF2*^{b} is available and at least one link between a couple of available VNFs is available. This means:

- four cases when one of VNF1s and one of VNF2s are failed with the link available between the remaining available VNFs, i.e. $4 \times (A_{VNF1} \times F_{VNF1}) \times (A_{VNF2} \times F_{VNF2}) \times A_{VL}$;

- two cases when one of VNF1s failed, both VNF2s are available and links available between the available VNF1 and the VNF2s, i.e. $2 \times (A_{VNF1} \times F_{VNF1}) \times A_{VNF2}^2 \times (1 - F_{VL}^2)$;

- similarly, two cases when one of VNF2s failed, i.e. $2\times A_{VNF1}^2\times (A_{VNF2}\times F_{VNF2})\times (1-F_{VL}^2)$; and
- one case when all VNFs and all the links between them are available, i.e. $A_{VNF1}^2\times A_{VNF2}^2\times (1-F_{VL}^4)$.

As a result:

$$A_{NS_2} = A_{NFVI}\times(\quad 4\times A_{VNF1}\times F_{VNF1}\times A_{VNF2}\times F_{VNF2}\times A_{VL} + 2\times A_{VNF1}\times F_{VNF1}\times A_{VNF2}^2\times (1-F_{VL}^2) + 2\times A_{VNF1}^2\times A_{VNF2}\times F_{VNF2}\times (1-F_{VL}^2) + A_{VNF1}^2\times A_{VNF2}^2\times (1-F_{VL}^4)) \quad (7)$$

NOTE: The same logic applies within the VNF with respect to the redundancy and availability of the links interconnecting VNFC instances.

5.3.3 Analysis of service resiliency configuration examples

After determining $RM(A_{VNF})$ function for different redundancy configurations the resiliency configurations of Table 5.2 can be further analysed. The question is whether different redundancy models of VNF instances and VLs could be used depending on the availability provided by different VNFs or VNF DFs (A_{VNF}) and the NFVI (A_{NFVI}).

In fact, equations (2) and (3) propose that if a given value for A_{NS} is needed, a provider can select a NFVI with lower availability and provide the same NS availability by constructing an $RM(A_{VNF})$ with higher availability. Alternatively, one can exploit a more reliable NFVI or use redundancy to compensate for a lower A_{VNF}. This is demonstrated this in the following examples based on equations (4), (5), (6) and (7) by considering different VNFs (or different DFs of a VNF) to achieve a certain availability.

Assuming that the minimum absolute availabilities a VNF can provide using its different DFs is known, each of which is defined according to some VNF-internal redundancy model known by the VNF vendor. That is, the different scale levels of a DF and its associated scaling policies if needed are defined in such a way in the VNFD that all of them guarantee the availability indicated in the VNF documentation for the DF provided it is deployed under ideal conditions on a 100 % reliable NFVI i.e. $A_{NFVI} = 1$.

EXAMPLE 1: VNF availability compensating for weaker redundancy model.

Assume an NS is needed with a single function provided with four 9 s availability ($A_{NS} = 0{,}9999$). The availability of the NFVI is $A_{NFVI} = 0{,}99999$.

The NS can be built in different ways, e.g. using VNFs from different vendors that implement the needed function; or using different DFs of the same VNF implementing the needed function using different redundancy models. Let assume DF1 of a VNF provides two 9 s availability for a VNF instance, i.e. $A_{VNF-DF1}$= 0,99, and DF2 of the same VNF provides three 9 s availability for a VNF instance, i.e. $A_{VNF-DF2}$= 0,999. Since $A_{VNF-DF1} < A_{VNF-DF2}$ NS_1 is composed with two redundant VNF instances using DF1 according to the 1+1 redundancy model; while NS_2 with three VNF instances of DF2 with the 2+1 redundancy model.

Using equation (4) for NS_1 the estimated availability is:

$$A_{NS_1} = A_{NFVI} * (2 * A_{VNF-DF1} - A_{VNF-DF1}^2) = \mathbf{0,999}890001$$

Using equation (5) for NS_2 its estimated availability is:

$$A_{NS_2} = A_{NFVI} * (\sum_{k=0}^{M} \binom{N+M}{N+k} A_{VNF-DF2}^{N+k} * (1 - A_{VNF-DF2})^{M-k}) = \mathbf{0,9999}8700202998$$

NOTE: If DF1 and DF2 are default deployment flavours of two different VNFs i.e. VNF1 and VNF2 the notation $A_{VNF-DF1}$ can be replaced by A_{VNF1} and $A_{VNF-DF2}$ by A_{VNF2}.

Thus, despite the weaker redundancy model used in NS_2 it meets the expected four 9 s availability due to the significantly higher availability that the DF2 provides. On the other hand, NS_1 even with the stronger redundancy model cannot be used to meet the expectations.

This example demonstrates that depending on the availability of the VNF instances, it is possible to achieve better availability (e.g. four 9 s versus three 9 s) with a redundancy model typically considered to be weak (i.e. for lower availability in the third row of Table 5.2). Thus, the redundancy model by itself does not characterize the achievable availability. A VNF with a higher availability can compensate for the lower capability of the redundancy model. Moreover, using a stronger redundancy model with such a VNF may result in lower utilization of resources.

The same logic applies within the VNF with respect to the redundancy and availability of the VNFC instances. This reinforces the point made earlier that characterizing the VNF by the redundancy model used for the VNFC instances is not sufficient to characterize the overall availability a VNF or its DF can provide.

EXAMPLE 2: NFVI availability compensating for VNF availability.

Considering the NSs of the previous example and deploying them on an NFVI with six 9 s availability ($A_{NFVI} = 0{,}999999$), if all other conditions remain the same, the calculations result in:

$$A_{NS_1} = \mathbf{0,999}8990001 > \mathbf{0,999}890001$$

$$A_{NS_2} = \mathbf{0,99999}6002002998 > \mathbf{0,9999}8700202998$$

Thus, the availability of the NSs increased in both cases, which indicates that the NFVI availability can compensate to some extent for the shortcomings of the VNF. In case of NS_2 deployed with the N+M redundancy model such improvement of the NFVI availability results in achieving even five 9 s availability. However, for NS_1 deployed with the 1+1 redundancy model the higher availability of the NFVI is still not enough to provide the targeted four 9 s.

These results together with the previous ones show how the combination of the NFVI, the VNF availabilities and the redundancy model have to be considered.

EXAMPLE 3: VNF availability compensating for VL redundancy.

To compare the NS availability when used with different VNFs and different VL redundancy models the cases shown in Figures 5.3 and 5.4 are considered.

In this example the NS is built from two interconnected VNFs: VNF1 and VNF2. Again, VNF instances are used with different DFs providing different availabilities and interconnect them through links with different redundancies. That is, NS_1 uses single-homing as redundancy for the VLs between the instances of VNF1 and VNF2, while NS_2 uses dual-homing. Further, the following is assumed:

For all cases A_{VL} = 0,9999 and A_{NFVI} = 0,99999

For NS_1 A_{VNF1}= A_{VNF2} = 0,999

For NS_2, A_{VNF1}= A_{VNF2} = 0,99

Then using equations (6) and (7) respectively the availability of the NS instances is estimated as:

$$A_{NS_1} = \mathbf{0,9999}860039990602294211962058 96$$

$$A_{NS_2} = \mathbf{0,999}789972408176225137359596 01$$

This shows that NS_1 deployed with single-homing (the weaker link redundancy) but built with instances of higher availability can provide the targeted four 9 s availability. On the other hand, NS_2 deployed with dual-homing does not provide the expected four 9 s due to the lower availability of the VNF instances used, i.e. the availability of the VNFs used in NS_1 compensates for the difference in the VL redundancy. This again shows that using a better link redundancy model by itself does not necessarily provide better availability. It needs to be considered together with the other composing elements of the NS and their redundancy.

5.3.4 Summary of availability design considerations

These examples demonstrate that at the time of the NS design, it is important to know the absolute availability provided by the different elements that can be used for composing an NS. With this information, an appropriate combination can be selected and combined using appropriate redundancy models as necessary for the VNF and VL instances.

In case of the VNF, the information necessary includes the minimum absolute availability that can be provided by each DF indicated in the VNFD. Each DF needs to be designed in such a way that this absolute availability is maintained throughout the different scale levels described for the DF when scaling according to the applicable scaling policies described in the VNFD.

Any information about redundant deployment of a VNF is reflected in the NSD; therefore, the VNF documentation needs to include the information based on which a service provider can design an NS for a desired availability. The information may include:

- Indicating the DF(s) of the VNF, which are designed to be used redundantly within an NS (i.e. redundant VNF instances).
- The redundancy capability of such DF(s) in terms of the N and M ratio of VNF instances that can be used together, where N represents the number of VNF instances providing active capacity which have to be protected by M instances providing standby capacity - since multiplicities of N and M are possible, at least their ratio needs to be provided.
- The communication needs of the redundant VNF instances.

NOTE: Since the NFV-MANO does not manage nor is aware of the active/standby roles of the VNF instances, the N and M ratio only provides information in terms of redundant capacity of resources provided by the NFV system.

According to (1), $\forall A_{NSi} > A_{Slice}$ needs to be fulfilled, that is, the availability of any NS instance used for a network slice instance needs to provide an availability greater than the availability of the network slice instance. This means that the availability needed by the network slice instance provides a lower bound of availability for the NS design.

Considering the availability of the NFVI, and the different VNF DFs, it can be determined whether VNF redundancy (i.e. redundant deployment of instances of the VNF) is necessary for each applicable VNF DF. If the following condition (8) is satisfied, no VNF redundancy is needed from an availability perspective for the given VNF DF (i.e. a single VNF instance can deliver the required availability possibly as a result of its internal redundancy - however, it is still possible that multiple VNF instances are needed to support higher workload.) In equation (8) A_{NFVI} is the availability of the NFVI on which the VNF instance is to be deployed. A_{Slice} is the availability of the network slice instance for which the VNF instance is considered.

$$A_{VNF-DF} > \frac{A_{Slice}}{A_{NFVI}} \quad (8)$$

If this is not the case it may still be possible to use the VNF in a redundant configuration. For this, the considered VNF DF needs to support redundant configurations. If so, the information on the N and M values and communication needs can be used according to equations (4) to (7) to determine if condition (9) can be satisfied.

$$RM(A_{VNF-DF}) > \frac{A_{Slice}}{A_{NFVI}} \quad (9)$$

Note that the multiplication in equation (1) means that satisfying (9) for each NS_i composing the network slice instance does not mean that the overall network slice instance availability requirement is met as it has been shown at the resiliency configuration. (8) and (9) are only the necessary conditions that provide the starting point for the design.

It is recommended to standardize the evaluation of VNF absolute availability, that is, considering 100 % NFVI availability, so that it is repeatable and comparable for performing the test by vendors and by service providers.

6 NFV resiliency for composite network service operations

6.1 Scaling and migration

6.1.1 Scaling

Scaling, i.e. the dynamic provisioning or deprovisioning of resources granted to VNFs, is undoubtedly among the most attractive features of NFV. This elastic capacity expansion/reduction can be initiated when the traffic load increases/decreases. Network service scaling can be realized in different ways:

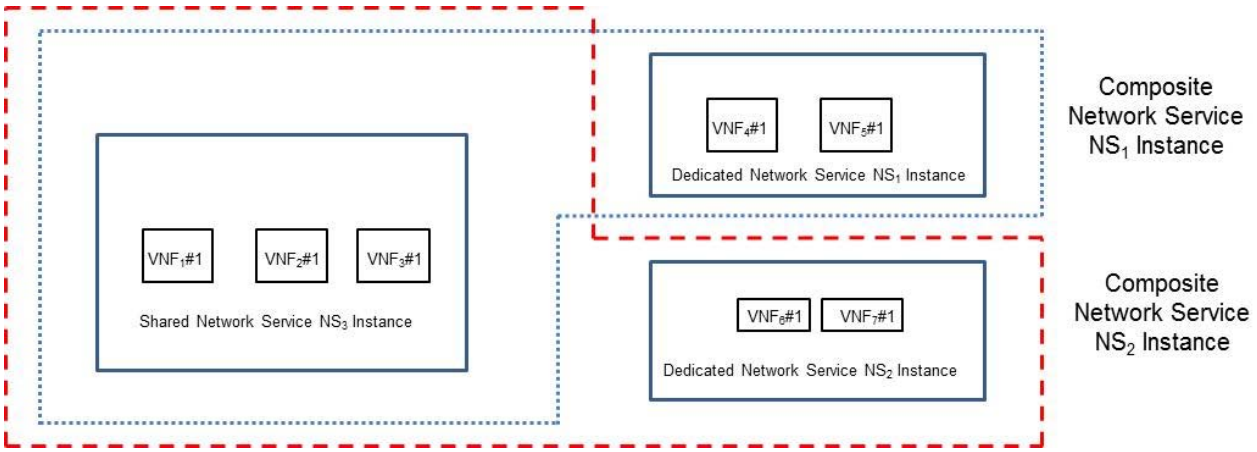
- VNF scaling: increase/decrease the number of VNFC instances in one (or several) VNF(s) of the network service;
- NS scaling: increase/decrease the number of VNF instances of one (or several) VNF(s) of the network service.

Clause 5.1 has shown that a composite network service can contain shared and dedicated network service instances. Scaling out a composite network service instance may thus mean the addition of VNF instances in shared network services instances and/or dedicated network services instances. Based on the example introduced in clause 4.3, the composite network service 1 instance of Figure 6.1 is deployed as two NS instances:

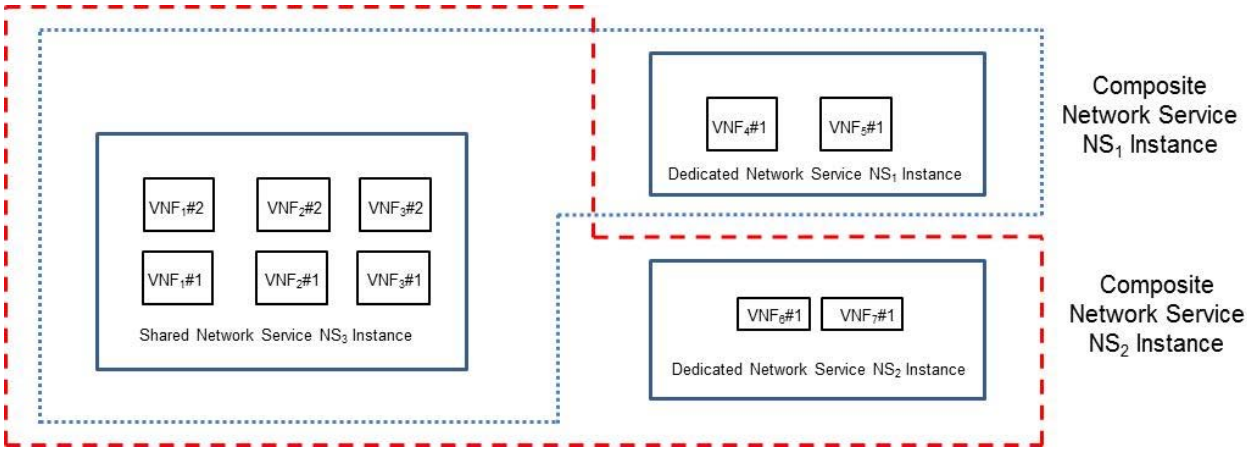
- a shared network service NS_3 instance, which is made of instances of VNF_1, VNF_2 and VNF_3 in 1:1:1 proportion - therefore, they have to be scaled together;
- a dedicated network service NS_1 instance, which is composed of instances of VNF_4 and VNF_5 of which only VNF_4 needs to be scaled.

Figure 6.1 displays different instantiation levels depending on the workload situations:

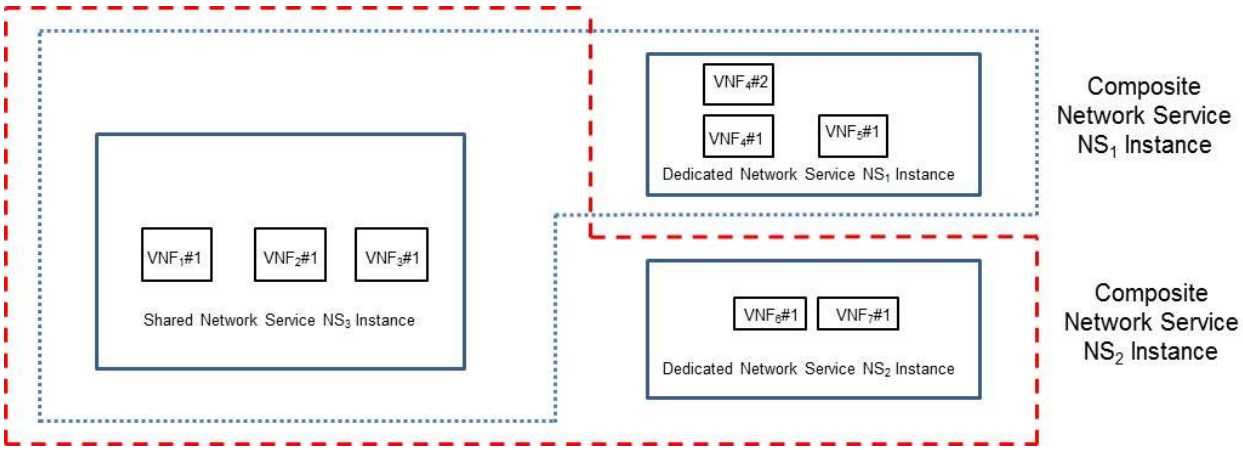
- Figure 6.1a shows the initial deployment before any scaling process;
- in Figure 6.1b, only the shared network service NS_3 instance is scaled out, i.e. in addition to the three "#1" instances of VNF_1, VNF_2 and VNF_3, three new "#2" instances have been created;
- in Figure 6.1c, the dedicated network service NS_1 instance is scaled out, i.e. in addition to the two "#1" instances of VNF_4 and VNF_5, one new "#2" instance of VNF_4 has been created;
- Figure 6.1d shows the case where the shared network service NS_3 instance and the dedicated network service NS_1 instance are both scaled out.



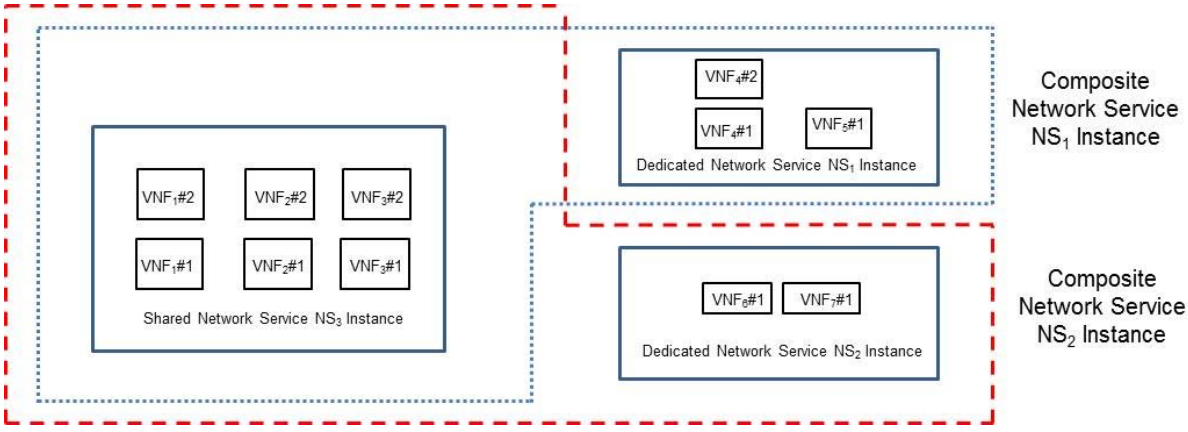
a) Before any scaling process



b) Scaling out a shared network service instance



c) Scaling out a dedicated network service instance



d) Scaling out shared and dedicated network service instances

Figure 6.1: Scaling out examples of a composite network service instance

In all these cases, the scaling out operations have to respect the resiliency considerations put in place during the design and deployment of the network service instances which were sketched out in clause 5.2:

- operations rules defined for the NS have to be respected when deploying and running the new VNF instance(s) - anti-affinity constraint is an example of deployment rules that the NFVO follows a priori;

- the virtualised resources newly allocated as part of the scaling operations need the reliability/availability characteristics appropriate for the target resiliency class - that is, the new VNF instance(s), as well as the virtual links scaled for the new VNF instance(s) have to follow the same design, e.g. redundancy configuration such as single/dual home, link aggregation, etc.;

- after scaling the network service instance(s) has(have) to maintain the same level of performance characteristics (e.g. E2E delay), resiliency, and other characteristics to continue to satisfy the requirements of the composite network service instance.

In addition to these precautions, service continuity has to be ensured by the vendor (e.g. providing appropriate scripts) when new VNF instances are created or existing ones are taken away. An increase (scaling out) or decrease (scaling in) of resources allocated to the network services should not result in any service interruption for the users of the network slice depending on these NSs during expansion or contraction.

The resiliency practices described above have to be applied to both shared and dedicated network services. Special care has to be taken to load balance in the newly created VNF instance(s) to the traffic incoming from (or going to) another network service in the case of scaling out. Workload reassignment may also be needed in the remaining VNF instance(s) in the case of scaling in. Stateful traffic distribution during scaling out also has to apprehended with attention, e.g. on-going sessions should be connected to the same VNF instance(s).

NOTE 1: The need, or not, of special considerations for load balancing traffic and processing of stateful traffic after creation/removal of VNF instances (NS scaling out/in) in the case of shared NS(s) is for further study.

Finally, scaling procedure failures have to be examined beforehand, and measures taken to ensure that there is no loss of service to existing network slices users and to avoid impact on agreed SLAs for the related usage scenarios, e.g. eMBB, uRLLC, mMTC. The origins of scaling failures for a network service are numerous:

- violation of the forwarding graph dependencies in one (or several) VNF(s) of the network service;

- violation of the dependencies in a nested network service (e.g. how two nested NSs are linked to each other);

- unprotected new network service instance (e.g. failure to scale out a new pair of VNFs);

- malfunction of old/new network service instance; etc.

NOTE 2: In case the composite network service NS_2 shown in Figure 6.1 has to be scaled out, if the two composite network services NS_1 and NS_2 do not have the same priority (e.g. one of them is more critical than the other), the higher priority composite network service needs to be served first, i.e. the scaling out process will start with its VNFs.

6.1.2 Migration

VNFs composing network services rely on virtualised resources (compute, storage, …) which are created on physical resources. It may be necessary to move these virtualised resources from one set of physical resources to another. Such relocation process is useful in diverse cases:

- maintenance purposes, e.g. NFVI software/hardware modification, servers addition/removal;

- service restoration following failures;

- failure prevention through a deep analysis of appropriate KPIs.

As of the type of migration, there are two possible ways to execute it:

- offline (or cold) migration, e.g. suspending the guest virtual machine (VM) and moving an image of the memory representing the VM to the destination host; the VM is then resumed on the destination host and the memory used by the VM on the source host is freed;

- live (or hot) migration, e.g. migrating an active VM from one physical host to another. In this case the VM is not suspended at the time the copying of its memory image starts. Rather changes in the active image are copied as well until at the destination the image has been recreated completely and the changes can be delivered in a single copy cycle. At this point, the VM is suspended at the source location and the last changes are copied to the destination. By that the VM is then completely recreated and activated at the new location.

As a result of such a process "live migration" still may cause a detectable interruption of the VM which could create inconsistency in the VNF if not considered and handled properly.

NOTE: Considering the high bandwidth needed for live migration, higher priority (composite) network services should be satisfied first when migration is envisaged - in addition, when there is not enough bandwidth, lower priority (composite) network services may be offline/cold migrated.

As in the case of scaling out described previously, relocating virtualised resources, e.g. from one physical node to another physical node, has to follow resiliency practices:

- resiliency class requests for the virtualised resources reliability, e.g. migrate the virtualised storage resource to a specific resource zone or to a specific host;
- operations rules, e.g. need for maintaining anti-affinity during and after the migration operation;
- isolation feature - containment capability has to be preserved after the migration process;
- service continuity - guests do not experience any downtime due to changes, e.g. made to any of the hosts.

As failures of the migration process within a DC (local migration) or across DCs (wide area migration) may happen, backup and restore procedures are needed. These should take into account the initial situation before the migration, e.g. the forwarding graph dependencies in network services VNFs, the dependencies of (nested) network services.

6.2 Restoration

Following the initial phase of a slice (subnet) lifecycle, i.e. its resiliency-oriented creation (clause 5.2), clause 6.1.1 has described the dynamic provisioning/deprovisioning of resources granted to VNFs which are the constituents of the NSs used by composite NS instances (i.e. scaling). Migration, i.e. the relocation process of virtualised resources, was described in clause 6.1.2. The present clause tackles failures encountered at the network service level during composite NS instance operations.

Numerous challenges can occur in the different layers of an NFV system:

- hardware/software failures among the compute/storage resources;
- loss of connectivity both locally or in a wide-area perimeter;
- overload due to unusual high traffic demand (caused by a legitimate event or attacks);
- failure of scaling or migration processes;
- system misconfiguration;
- etc.

As far as these challenges are handled/mitigated at their level and do not impact the VNFs (e.g. thanks to an intra-VNF redundancy design, automatic VMs migration, presence of defense mechanisms), they are not considered in the present document which rather focuses on failures at the VNF level thus perturbating the network services composing the slices or slice subnets.

As resources are needed to restore network services, the different situations include:

- the requested resources are available - the present clause deals with this situation;
- the desired resources are insufficient - the next clause 6.3 will handle this case.

When anomalies occur, the affected VNFs should fully resume their services. The present clause is about restoration of all impacted VNFs/NSs supporting the slices (slice subnets) to their normal operations as before the failure(s) when there is no need for conflict mitigation in the resource allocation. Clause 6.3 will deal with the situations where lack of resources leads to the choice of not re-instantiating some network services after their failure(s). It is assumed in the present document that such situations lead to the decision of leaving some slices (slice subnets) unavailable or degraded. In such situations, a further step consists of restoring the complete/original configuration of the NS instances when resources become available, e.g. bringing up again the slices (slice subnets) which were not re-instantiated earlier. It is noteworthy that such procedure is an integral part of the service provider policy and SLA management.

Surveillance of network service operations corresponds to - among others - monitoring the functioning of its VNFs, e.g. via heartbeat or watchdog mechanisms for failure detection. This process detects VNF(s) failure whose impact on the network service(s) and, consequently, on the slices (slice subnets) strongly depends on deployment choices such as VNF redundancy:

- if there is no impact, e.g. because redundancy has helped to mask the VNF(s) failure, the restoration of failed VNF(s) is to be done in order to get back to the original normal operation;
- if the related network service(s) is(are) impacted by the VNF(s) failure, the immediate restoration of failed VNF(s) has to minimize the repercussion on the service delivery, e.g. through the respect of SLA commitment.

On the long term, in the ideal case, data collection in time/space coupled with anomaly analytics (trend identification using, e.g. resource usage, logs in conjunction with correlation analysis) leads to failure prediction, and triggering proactive control functions that apply predefined actions to prevent VNF(s) failure to occur.

Whatever the impact cited above, re-instantiating the failed VNF instances needs to respect the resiliency expectations expressed during these VNF instances creation:

- correct allocation of resiliency class for compute, storage and networking resources;
- application of appropriate policies (e.g. use of anti-afffinity rules for redundant elements) driven by principles such as the isolation of network slices (slice subnets) following network service failures;
- respect of network services dependency.

NOTE: The isolation aspect is related to failure containment, i.e. firstly preventing the failure of one network service propagating to other network services and secondly to other slices (slice subnets).

As for service continuity, two categories of services can be considered:

- For stateless services, service continuity means that the service functionality remains available following a VNF instance failure (i.e. another VNF instance is available to serve new requests), but ongoing requests/sessions can be lost. Thus, users are able to obtain the service they were using before the failure happened afterward on a retry. This means that redundancy needs to be used only to the extent so that the functionality and the configurations can be restored fast enough to serve the users' retry. Depending on the re-instantiation time of the failed VNF(s), this may require no other redundancy than for handling the traffic volume or some pre-instantiated spare VNF instance(s) that can take on traffic from the failed instance(s) right after the failure. The QoS may be thus degraded, but the service is ensured as long as at least one VNF instance is available to meet the demands.
- In case of stateful services, the service state may or may not be externalised. If the state cannot be externalised, then VNF instances have to be used in redundancy to back up each other in such a way that if an instance fails, the backing up standby instance is able to take over the service from the state the failed instance has left of. Among others, this needs guarantees that instances backing up each other never fail together.. If the state can be externalised then the VNF(s) themselves provide stateless services (see previous case); however, the service providing the state storage needs to follow still the principles of stateful services. Here, the resiliency evaluation of VNF instance needs to consider the state storage availability, including the related connectivity.

Restoration priority

As indicated above, this clause tackles network services restoration for situations in which the NFV system is not experiencing any resource shortage issue. Nevertheless, in case of multiple VNF failures, restoration priority at the NS/VNF level may prove to be useful. Different situations can be envisioned:

- if several network service instances chained together are impacted by the failure, some particular instances may need to be restored before others if sequential constraints are present;
- if both shared network service(s) and dedicated network service(s) are impacted by the failure, VNFs composing the shared network service(s) have to be restored first to minimize the global service unavailability;
- if different slices (slice subnets) are impacted by the failure, the VNFs which are part of higher priority slice (or slice subnet) related NSs will be restored first.

Handling of the restoration procedures has to take into consideration the NS instance priority attribute, therefore NFVO would prioritize accordingly the restoration of NS instances that have different levels of priority.

Congestion

If the original challenge leading to a failure of VNFs composing the network service(s) is overload due to high traffic demand, mechanisms are needed to control the situation before any restoration can be processed. For instance, in case of malicious traffic, detection procedures should identify such traffic and initiate mitigation, e.g. determining and isolating the source of the attack.

Congestion is not only characterized by a sudden increase of external traffic. In a network service composed of VNFs, it could happen that some of them are strongly needed by a huge number of other VNFs. In such a situation, if the former VNF instance fails and is replaced, all the latter VNF instances will try to re-establish the lost connection instantaneously creating a traffic surge. This surge of traffic represents a significant traffic storm. Overload control has then to be implemented in order to prevent the failure of the newly replaced VNF instance.

6.3 Resource reallocation

The present clause deals with the case of lack of resources leading to the re-instantiation of only a subset of impacted VNFs, i.e. some NSs and not all of them, after failures occur. VNFs which benefit from this restoration procedure are characterized by their importance through the role they play in the building of slice (or slice subnet) related network services. Examples include those network services which compose the high priority slices (or slice subnets).

ETSI GS NFV-REL 001 [i.7] has identified two ways of tackling the resources limitation scenario in case of hardware failure:

- *regression* means that the failed VNF instances are restored using only the available free hardware capacity, which is less than what is needed to restore all failed VNF instances;
- *pre-emption* means that some healthy running VNF instances are suspended to provide room for the restoration of failed VNF instances.

NOTE 1: Although priority is not needed for the use of regression, the two methods described above can be used in combination depending on priorities.

NOTE 2: In some situations, if two (composite) network services of the same importance (i.e. they have the same priority) are using a common infrastructure, and if they are both already scaled out, a way to tackle resources limitation may consist of scaling in the two (composite) network services, resulting in a degraded mode functioning of these two (composite) network services.

Figure 6.2 shows a system managed by a common NFVO consisting of two different infrastructures INF_1 and INF_2 providing resources to three composite network service instances. The 1st composite network service instance uses a network service NS_1 instance and a network service NS_3 instance. The latter is shared with the 2nd composite network service instance which also builds on a second network service NS_2 instance. As for the 3rd composite network service instance, it relies on a single network service NS_4 instance. The different network services comprise the following VNFs:

- VNF_4 and VNF_5 for NS_1;
- VNF_6 and VNF_7 for NS_2;
- VNF_1, VNF_2 and VNF_3 for NS_3;
- VNF_8, VNF_9, VNF_{10} and VNF_{11} for NS_4.

The first infrastructure INF_1 is used by the NS_3 and NS_4 instances, while the NS_1 and NS_2 instances rely on the second infrastructure INF_2. For the purpose of the present clause, it is assumed that the 1st composite network service instance has a higher priority than the 2nd and the 3rd composite network service instances.

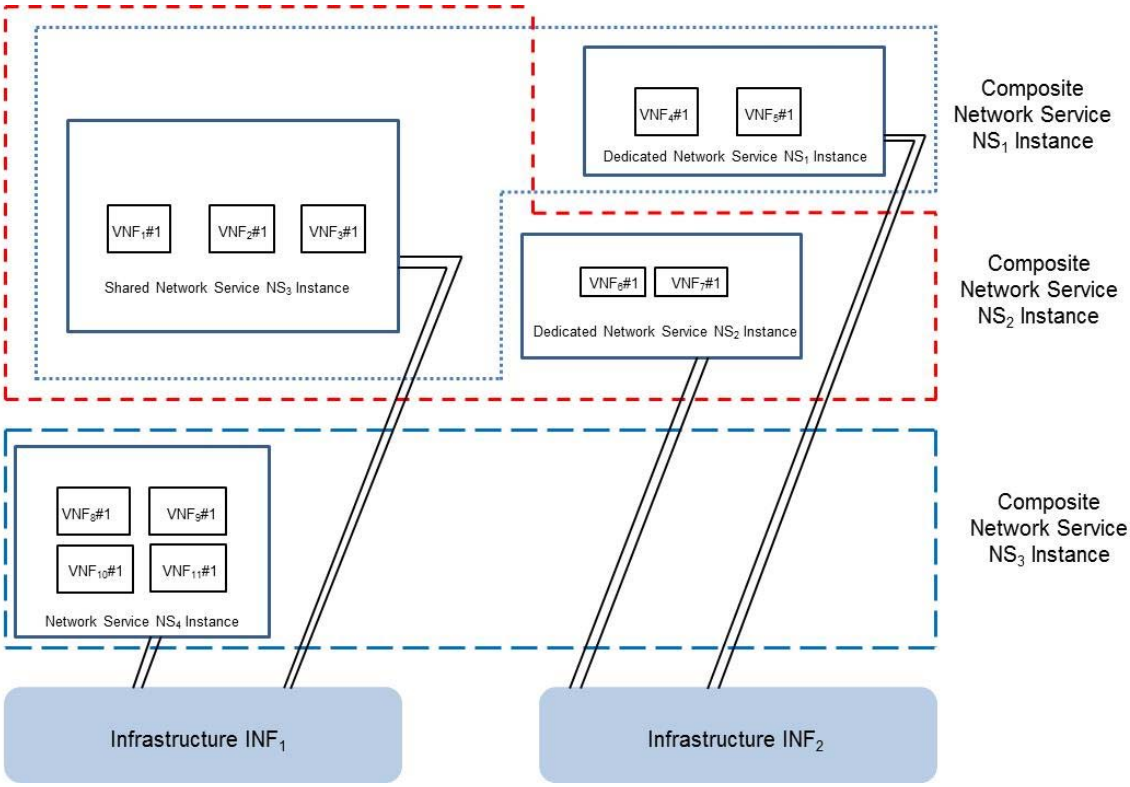


Figure 6.2: Composite network services running on two distinct infrastructures

If a failure hits INF_1 causing the loss of all VNFs running on it (Figure 6.3), the regression procedure is started by moving to INF_2, firstly, all VNFs belonging to NS_3 because the 1st composite network service instance is more crucial than the 3rd composite network service instance. After the successful re-instantiation of VNFs composing NS_3, the restart of those VNFs included in NS_4 is launched, but the process is aborted. Actually, in this example, the lack of resources would only permit to launch instances for VNF_8 and VNF_9 (and not for VNF_{10} and VNF_{11}), i.e. not all composite network services running before the failure are operational after the termination of the overall restoration procedure. Consequently, the 3rd composite network service instance is unavailable after the overall restoration procedure stops due to lack of resources.

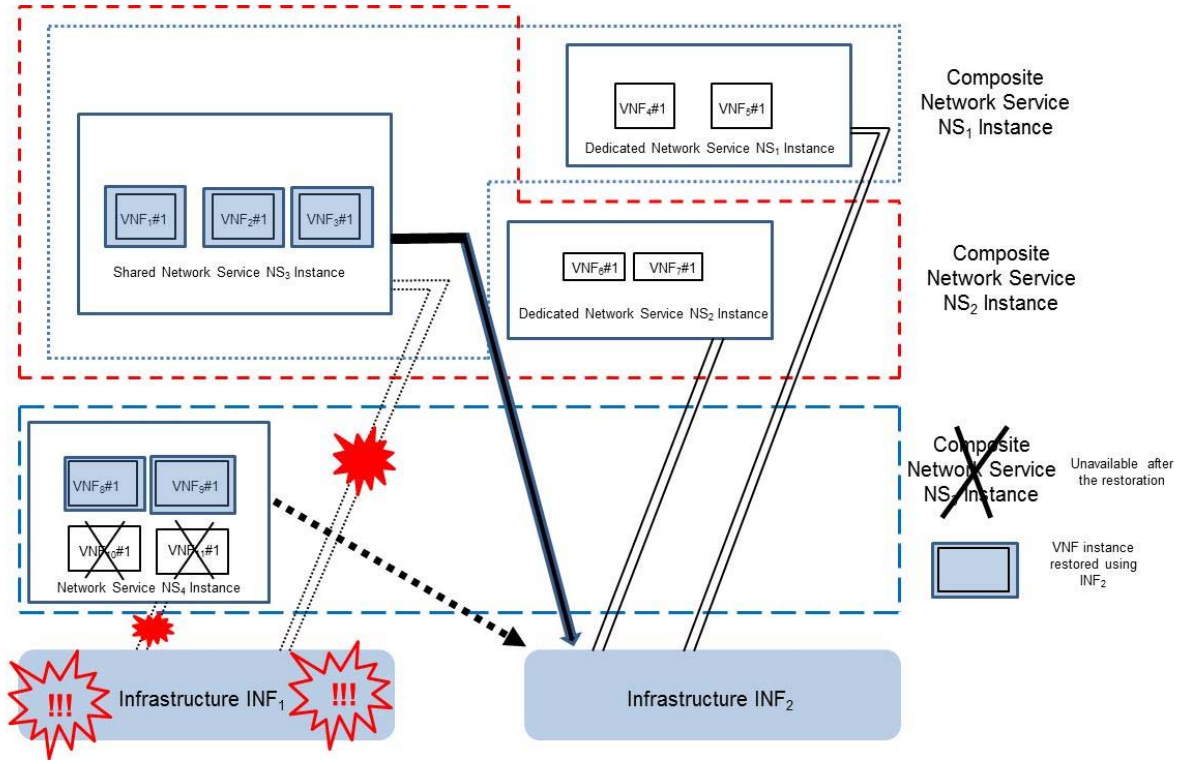


Figure 6.3: Regression following an infrastructure failure

Another scenario can occur: INF_2 does not have enough resources to host the three VNFs (i.e.VNF_1, VNF_2 and VNF_3) belonging to NS_3. Figure 6.4 shows that the overall restoration then follows two steps in this case:

- as in the previous scenario, regression is started by moving to INF_2 all VNFs belonging to NS_3 - in this example, as INF_2 can only provide resources to VNF_1 and VNF_2, the next step is necessary;
- considering that the 1st composite network service instance has a higher priority than the 2nd composite network service instance, pre-emption is then launched in order to suspend the two VNF_6 and VNF_7 running instances - the freed resources are thus used to re-instantiate VNF_3.

In this second scenario, the 2nd composite network service instance, together with the 3rd composite network service instance, are unavailable after the overall restoration procedure stops due to lack of resources.

NOTE: As suspending running VNFs (i.e. some network services) to leave room for other VNFs (i.e. other network services) is an important matter, strict slice (or slice subnet) - mapped to composite network service as indicated in clause 4.3 - management policies have to be defined a priori, e.g. through SLA between all involved stake holders.

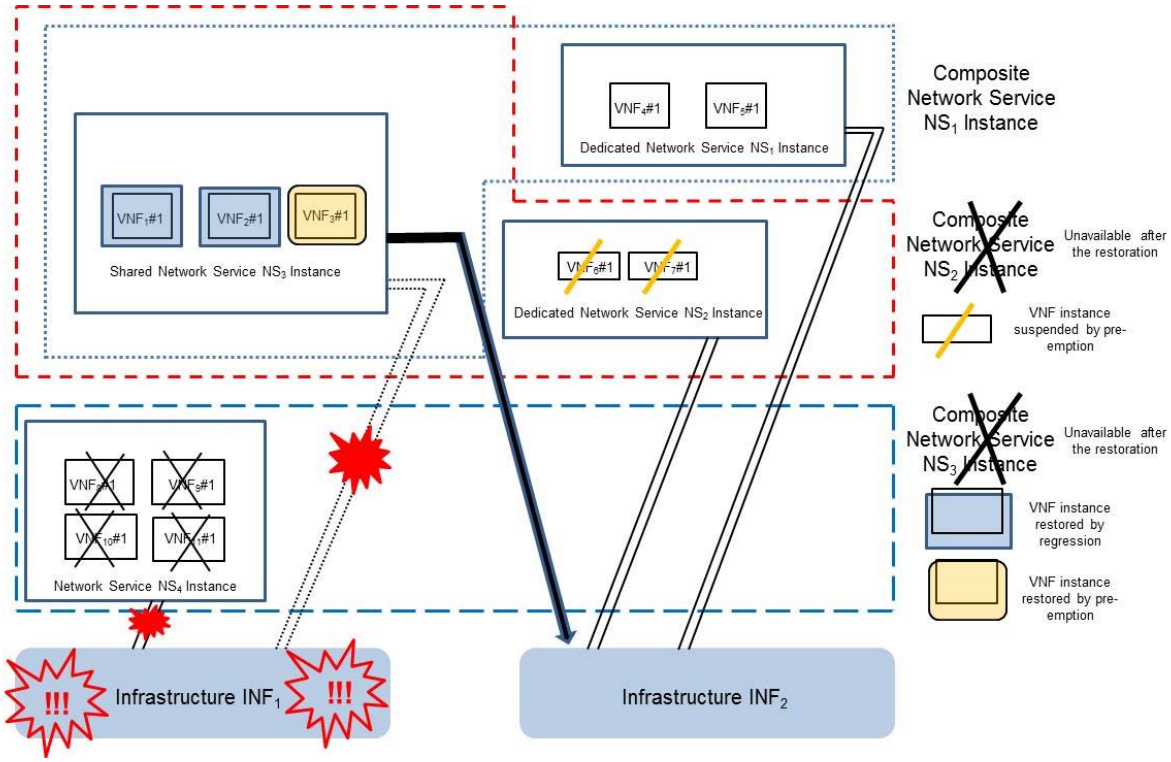


Figure 6.4: Regression and pre-emption following an infrastructure failure

Besides the reinstantiation procedure sketched earlier, all rules described in the previous clause 6.2 for VNFs restoration need obviously to be respected (e.g. use of appropriate VNFs deployment flavours, allocation of proper resiliency class for compute/storage/networking resources, overload control in case of congestion, etc.).

In a long run, the process described in this clause needs to be followed by the recovery procedure, i.e. bringing back all slices (slice subnets) to operations after the failure situation has been fixed.

Case of high scale disturbance

In scenarios such as large-scale disasters, situations may include the loss of entire data centers. Local redundancy designed for slices (or slice subnets) robustness, as shown above with the presence of a second infrastructure used for regression/pre-emption, is then useless. For the critical slices (or slice subnets) for which geo-redundancy is implemented from the start, the mechanisms described above may still apply.

For instance, as geo-redundancy relies on different geographic data centers, the use of regression allows, to a certain extent (i.e. if constraints allow it), to re-instantiate in a remote location the impacted network services. If needed, pre-emption pursues the restoration by suspending the less prioritized tasks in order to leave room in the remote data centers for running the VNFs/network services impacted by the disaster.

In such extreme disaster situations, service continuity requirement could be violated, as well as unavailability tolerance should be accepted by the customers, except for emergencies services, and new critical use cases planned for 5G, e.g. ultra Reliable and Low Latency communications.

7 NFV software modification and their impacts on network slice resiliency

7.1 Introduction

As shown in Figure 4.2, network slices or network slice subnets can be mapped to network services from a resource management viewpoint. VNFs, together with PNFs and virtual links used for connectivity, are the constituents of such network services. This clause 7 considers NFV software modification and its impact of this life cycle process on the overall resiliency of network slices (or network slice subnets). Three kinds of software are considered for the modification process in an NFV environment: VNF, NFVI, and MANO. Clause 7.2 considers VNF software, while the subsequent clause 7.3 analyses the NFVI software. As stated in the introduction, as NFV-MANO resiliency is considered in [i.11], the present document does not cover NFV-MANO faults/failures. Consequently, the NFV-MANO software modification is not considered here, and may be the subject of a further study.

Two types of software modification are defined in ETSI GS NFV-REL 006 [i.10]:

- update is the software modification process for bug fixes or enhancements without adding, modifying or removing functionality, interfaces or protocols;
- upgrade is the software modification process aimed at adding, modifying or removing functionality, interfaces or protocols.

This distinction is not relevant for the present document which does not make difference between these two types for their implication on network slices (or network slice subnets) resiliency.

ETSI GS NFV-REL 006 [i.10] has also identified different software modification related tasks which can be grouped into two main phases:

- preparation, which is composed of:
  - downloading the new software;
  - testing it on the network operator's premises (if needed);
  - on-boarding it into the NFV system; and
  - any other prerequisite necessary to carry out the deployment plan (e.g. checking for resources availability);
- deployment, which consists of deploying the new software in the live NFV system, i.e. instantiation of entities with the new software version to replace entities of the old software version.

From a resiliency perspective, the second phase is to be apprehended with care in order to fulfill service availability and service continuity for the network slices (or network slice subnets) impacted by the software modification.

The deployment phase also needs to consider exception handling. Actually, whenever a problem occurs while the software modification is in progress, or if the new software turns out to be unsatisfactory after the software modification, it is necessary to revert back from the newly deployed software to the old software and to remove the newly deployed software in a graceful manner with minimal service impact. Note that this process may need to be initiated for certain conditions, e.g. degraded performance (beyond acceptable limits) even if the new software is operating correctly.

Losing session data for some stateful services by an abrupt removal of the new software may be justified by the fact that this prevents fault propagation and further service degradation. For instance, an abrupt removal is preferable if the VNF is part of a network service shared by two slices (or slice subnets). In other cases, the new software can remain until the completion of the services as part of a graceful rollback process. It is noteworthy that for compatibility purposes, restoring an older software version may require special care as even if the new software to be removed is backward compatible, this does not guarantee that the old software to be restored is forward compatible with the new software to be removed.

NOTE: Any failure during the VNF software or NFVI resource software modification process may impact the final (composite) network service(s) provided by the VNF system - such situation has to be handled as it is detailed in ETSI GS NFV-REL 006 [i.10].

7.2 VNF software

Two types of VNF software architectures have to be considered: stateless, and stateful. The second type is obviously more complex, as session data and affinity of session connections have to be taken into consideration during the update/upgrade process.

Stateless case

For a stateless VNF, a method proposed in ETSI GS NFV-REL 003 [i.8] consists of deploying a new software version instance and using simultaneously the old and new software version instances. Since the VNF is stateless, after the new software version instance has started, all traffic will be directed to it. The old software version instance(s) will then be terminated once it (they) has (have) finished processing its (their) current load. This method thus realize the upgrade process while respecting service continuity.

Stateful case

For VNF software modification, different methods can be used according to the diverse deployment options [i.10]:

- network service level active-standby VNF redundancy;
- active-active configurations;
- VNF including internal resiliency mechanisms, e.g. VNFC redundancy.

The methods sketched earlier for software modification rely on the creation of VNF instances using the new software. In situations where resources may be limited, e.g. in a PoP, it is thus recommended to avoid scaling out VNFs hosted by the infrastructure, but not concerned by the upgrade especially if such VNFs support low priority network services. This requires the awareness of MANO of initiated/ongoing VNF upgrades.

Network slices or network slice subnets can be mapped to composite network services. These network services may in turn be formed of shared and dedicated network services. An elementary precaution is to ensure that the update/upgrade of any VNF which is part of a shared network service will still be compatible with all the composite network services using the related network service.

7.3 NFVI resource software

The NFVI represents the hardware and software composing the environment in which VNFs are deployed, managed, and executed. It is formed of physical hardware resources for computing, storage and networking, and software resources providing the virtualisation layer and the virtualised resources (e.g. hypervisors, VMs, VLANs, virtual disks, etc.).

The software modification of NFVI resource thus includes change of:

- physical equipment firmware;
- host OS and/or hypervisor software (including VMs);
- software providing virtual networks/storage.

The present clause examines how care taken at the changes in NFVI layer helps to prevent adverse effect of the NFVI software modification on the network slices (or slice subnets) through their hosted network services and VNFs.

To avoid VNF service disruption (which may impact the related network service) during NFVI software modification, the approach proposed in ETSI GS NFV-REL 006 [i.10] requires a facility for VNFs to prepare for upcoming unavailability of NFVI resources, and take appropriate actions in a more graceful fashion than the operations performed under failure conditions. This takes the form of a *notice period* of upcoming software modifications, and a time bound opportunity for services to react on their own in preparation for the NFVI software modification. Such preparation includes blocking the traffic directed to the impacted virtualised resource and evacuating it before the shutdown, scaling out in order to increase redundancy in the pool of redundant servers, etc.

The notice period is considered at the level of individual vitualised resources, but also for their groups, as instances in the group collaborate in maintaining their services - therefore, for service continuity, it is essential to maintain the group functional.

Accordingly, the approach is based on the knowledge at the NFVI layer of *constraints* of the hosted VNFs with respect to the virtualised resources and their groups. The grouping of virtualised resources relevant and known to both the NFVI and the VNF layer uses anti-affinity groups.

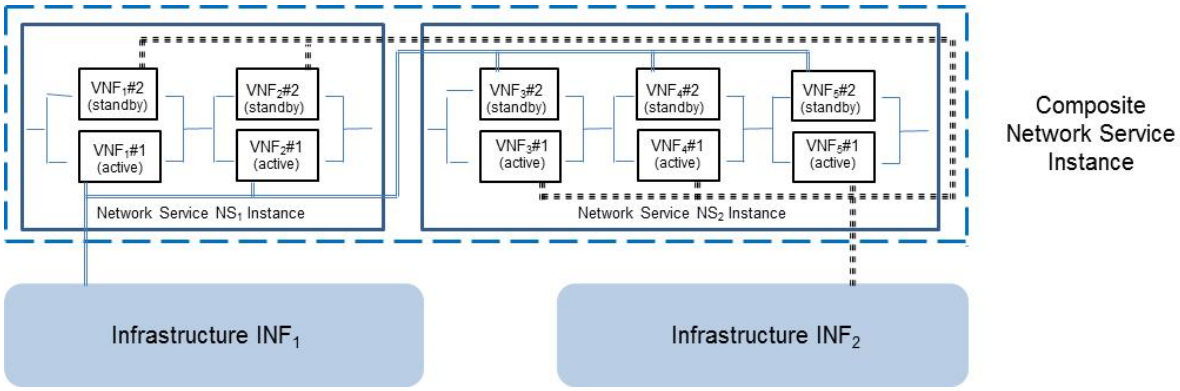
The constraints can be expressed at the time when the virtualised resources and their groups are requested from the NFVI layer; or later when their manager entity is notified about the upcoming NFVI software modification, i.e. the manager entity can provide the constraints to the NFVI layer on demand. The constraint could include:

- *notice period* or *lead time* requested for the notification as preparations may need time;
- whether the notification is requested before a (group of) virtualised resource(s) is impacted;
- for an anti-affinity group, the minimum number of virtualised resources that have to be available and/or maximum number of virtualised resources that can be impacted simultaneously;
- upper limit of the interruption time at which virtualised resource live migration is feasible (undetectable for the VNF), otherwise offline migration is preferred.

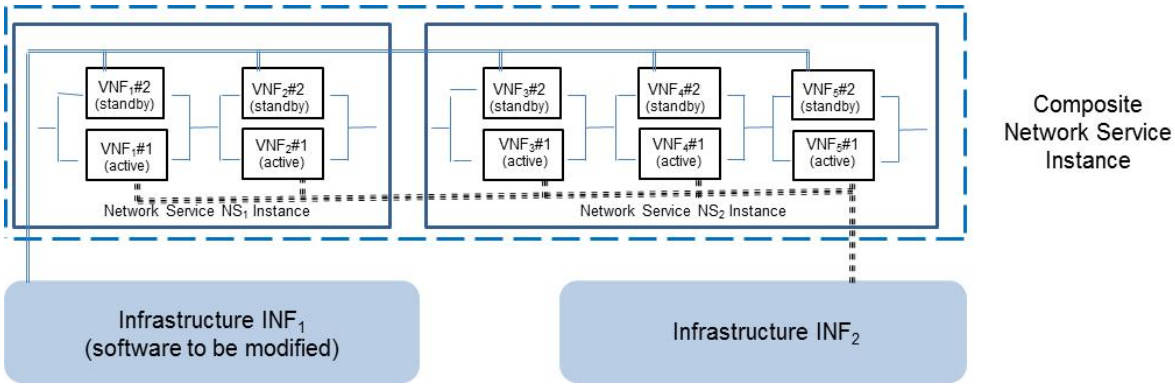
NOTE: The informative Annex C of ETSI GS NFV-REL 006 [i.10] provides an example of the coordination flow for NFVI software modification.

Figure 7.1a shows an example of such VNF combinations. The composite network service is made of two network services. The first one (NS_1) is composed of two VNFs (VNF_1 and VNF_2), while the second one (NS_2) is formed of three VNFs (VNF_3, VNF_4 and VNF_5). All five VNFs run in a redundant manner, i.e. there are two instances for VNF_1 (resp. VNF_2, VNF_3, VNF_4 and VNF_5) operating as active and standby. The two infrastructures (INF_1 and INF_2), considered for simplicity purposes as two servers, allow the deployment of the VNF instances using anti-affinity rules, i.e. the active VNF_1 and VNF_2, together with the standby VNF_3, VNF_4 and VNF_5, run on INF_1, while the active VNF_3, VNF_4 and VNF_5, together with the standby VNF_1 and VNF_2, run on INF_2.

If the INF_1 software is to be modified, all active roles of instances currently running on it, i.e.VNF_1 and VNF_2 instances, have to be moved to instances of INF_2 first. In this example, it also means the moving of the standby roles of VNF_1 and VNF_2 instances to INF_1 (Figure 7.1b). Note that this role transfer is not handled by NFV-MANO as redundancy is not visible to it, by rather by an application-related function such as OSS.



a) Original resource allocation



b) Resource allocation for INF_1 software modification

Figure 7.1: Composite network service using two meshed network services based on redundant VNFs

As for the lead time, ensuring the maximum lead time imposed by the constraints sketched above should be sufficient for preparing operations such as migration in a comfortable time window.

8 Recommendations

8.1 Design time recommendations

To meet the availability/reliability requirements of a network slice (or network slice subnet) instance, it is recommended that the non-functional aspects of the supporting network service instances have to be designed and deployed with the following considerations:

- create the proper NS design, e.g. NS deployment flavour, by choosing appropriate VNFs deployment flavours, and defining VL flavours;
- specify the appropriate resiliency class of resources (e.g. compute, storage, networking);
- assign and apply the proper policies (e.g. priority/pre-emption rules).

If network slices (or network slice subnets) are composed of both shared and dedicated network services, it is recommended that the shared network service instance has the resiliency level at least of the most demanding, in terms of reliability/availability, dedicated network service instances.

For isolation purposes, it is recommended to choose appropriate placement strategies during instantiation, resulting in the avoidance of impact of the overload of one network slice (or network slice subnet) instance on another network slice (or network slice subnet) instance.

For isolation purposes, it is recommended to choose appropriate placement strategies during instantiation, resulting in the avoidance of propagation of the failure of one network slice (or network slice subnet) instance to another network slice (or network slice subnet) instance.

For proper NSs (supporting network slices, or network slice subnets) resiliency design, it is recommended that their VNFs provide an absolute availability value - based on an availability of NFVI and MANO of 100 % - for each DF, in addition to the supply of these DFs. It is also recommended that this absolute availability is maintained throughout the different scale levels of these VNFs, that is, it is characterized by the minimum absolute availability value a given VNF DF can sustain.

For building network slices (network slice subnets), it is recommended that the VNFs documentation includes information (e.g. DF redundant capability) based on which a service provider can design the corresponding resilient NSs.

It is recommended to standardize the evaluation of VNF absolute availability, that is, considering 100 % NFVI and MANO availability, so that it is repeatable and comparable for performing the test by vendors and by service providers.

8.2 Run time recommendations

Network slices (or network slice subnets) may rely exclusively on dedicated network services, or be supported by both shared and dedicated network services. It is then recommended that scaling out operations respect resiliency considerations put in place during the design and deployment of the network service instances:

- operations rules (e.g. anti-affinity) defined for the NSs are respected when deploying and running the new VNF instance(s) - note that such rules are followed, a priori, by the NFVO;
- virtualised resources newly allocated as part of the scaling operations have the reliability/availability characteristics appropriate for the target resiliency class, e.g. virtual links scaled for the new VNF instance(s) follow the same redundancy configuration (link aggregation, etc.);
- after scaling, the resiliency level of the network service instances has to be maintained to continue to satisfy the requirements of the supported network slice (network slice subnet) instance.

In case virtualised resources used by the NSs supporting the network slices (or network slice subnets) have to be relocated, it is recommended that:

- resiliency classes of resources are ensured;
- operations rules are maintained during and after the operation;
- containment capability has to be preserved after the migration process;
- service continuity is respected, i.e.no downtime experienced due to changes.

When re-instantiating failed VNFs of the NSs supporting the network slices (or network slice subnets), the resiliency expectations expressed during the instantiation of these VNFs are to be respected. It is thus recommended to apply appropriate policies driven by principles such as the isolation of network slices (network slice subnets) following network service failures.

As for service continuity during network slices (or network slice subnets) restoration following a failure, the following recommendations are provided:

- for stateless services, it is recommended to provide redundancy in terms of capacity for handling additional traffic volume or some pre-instantiated spare VNF instance(s) that can take on traffic from the failed instance(s) right after the failure;
- for stateful services with externalised service state;
- it is recommended to provide redundancy in terms of capacity for handling additional traffic volume or some pre-instantiated spare VNF instance(s) that can take on traffic from the failed instance(s) right after the failure;
- for stateful services without externalised service state, it is recommended that VNF instances using shared data are running in redundancy to back up each other; if an instance fails, the backing up instance which may be another active instance or a standby instance is thus able to take over the service from the state the failed instance has left of.

As restoration priority at the NS/VNF level is needed in case of multiple VNF failures happening in network slices (or network slice subnets), it is recommended that:

- if several network service instances chained together by sequential constraints and several of them are impacted by the failure, then some particular instances have to be restored before others as defined by the sequential constraints;
- if different network slices (network slice subnets) are impacted by the failure, the VNFs which are part of higher priority network slices (or network slice subnets) related NSs have to be restored first;
- if both shared network service(s) and dedicated network service(s) are impacted by the failure, VNFs composing the shared network service(s) have to be restored first to minimize the global service unavailability.

If the original challenge leading to a failure of VNFs composing the NSs of the network slices (or network slice subnets) is overload/congestion due to high traffic demand, it is recommended that NFVO analyses and controls the situation before any restoration can be processed.

If after failures, the lack of resources would lead to the re-instantiation of only a subset of VNFs, then the VNFs that are part of NSs related to higher priority network slices (or network slice subnets) have to be re-instantiated first. It is then recommended to apply regression and/or pre-emption methods as detailed in clause 6.3 to achieve this.

8.3 Software modification recommendations

8.3.1 VNF software

For stateless VNFs composing the NSs of the network slices (or network slice subnets), it is recommended to use simultaneously the old and new software version instances deployed either at the VNF or VNFC levels: all new traffic will be directed to the new software, and the old software will be terminated once it has finished processing its current load.

For stateful VNFs composing the NSs of the network slices (or network slice subnets):

- in VNF active-standby configurations, it is recommended that the standby VNF is upgraded first, followed by the switch of connections from the old VNF version instance to the new VNF version instance and the upgrade of the remaining old VNF version instance - it is noteworthy that there is no VNF redundancy in case of failure while the upgrade process is under way;
- in VNF active-active configurations, it is recommended to deploy a new software version in additional active instance(s) and to use simultaneously the old and new software version instances - all new traffic will be directed to the new software, and the old software will be terminated once it has finished processing its current load.

In situations where resources are limited, e.g. in a PoP, it is recommended to avoid scaling out VNF instances which are not concerned by the upgrade if such VNFs participate in low priority network slices (or slice subnets).

8.3.2 NFVI resource software

As detailed in clause 7.3, the knowledge at the NFVI layer of constraints of the hosted VNFs with respect to the virtualised resources and their groups helps to avoid service disruption during NFVI software modification. For VNFs composing the NSs of the network slices (or network slice subnets), it is recommended that they provide their constraints in a timely manner to the NFVI software modification manager to be aware of the constraints and relationships. It is also recommended that the NFVI software modification manager takes into account these constraints.

Annex A:
Authors & contributors

The following people have contributed to the present document*:*

Rapporteur:
Chidung Lac, Orange

Other contributors:
Cristina Badulescu, Ericsson

Pradeepsunder Ganesh, Intel

Ulrich Kleber, Huawei

Gerald Kunzmann, NTT DOCOMO

Shaoji Ni, Huawei

Maria Toeroe, Ericsson

History

Document history		
V3.1.1	June 2019	Publication