ETSI GS NFV-IFA 033 V4.1.1 (2020-08)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification

Disclaimer

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

Reference

DGS/NFV-IFA033

Keywords

cyber security, interface, management, MANO, NFV, orchestration, security, virtualisation

ETSI

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

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

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

Important notice

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

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

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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

Modal verbs terminology

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

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

1 Scope

The present document specifies the requirements applicable to the interfaces supported over the Sc-Or, Sc-Vnfm, Sc-Vi reference points as well as the operations invoked over these interfaces. The purpose of the interfaces is to support security monitoring and management as specified in ETSI GS NFV-SEC 013 [i.3].

2 References

2.1 Normative references

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

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

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[2] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[3] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

2.2 Informative references

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

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

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

[i.1] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

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

[i.3] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.4] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification".

[i.5] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.6] ETSI GS NFV-SOL 003: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.2] and ETSI GS NFV-IFA 026 [i.4] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GR NFV 003 [i.2].

HMEE	Hardware Mediated Execution Enclave
HSM	Hardware Security Module
PSF	Passive, Semi-Active or Fully-Active
SF	Semi-Active or Fully-Active
SM	Security Manager
TPM	Trusted Platform Module

4 Overview of interfaces for the Sc-Or, Sc-Vnfm and Sc-Vi reference points

4.1 Introduction

4.1.1 Reference architecture

The Sc-Or, Sc-Vnfm and Sc-Vi reference points are specified in ETSI GS NFV-IFA 026 [i.4].

4.1.2 NFVO as a proxy for getting information from other functional blocks

The Security Manager has requirements for getting information which originates from the NFVO, VIM, VNFM or OSS/BSS. As a general principle, the information originated from either the VIM, VNFM or OSS/BSS is sent to the NFVO from the originated entity, then the information is sent from the NFVO to the SM in which the NFVO acts as a proxy.

This principle is reflected by the present document in the following ways:

- The present document defines a reference point between the NFVO and the SM.
- The present document does not define a reference point between the OSS/BSS and the SM (NFVO as a proxy).
- The present document does not define a reference point between the VNFM and the SM (NFVO as a proxy).
- The present document defines a reference point between the VIM and the SM, and only one interface including a reduced set of operations compared to Or-Vi and Vi-Vnfm reference point is specified for this reference point.

4.1.3 Interfaces on the Sc-Or reference point

The Sc-Or reference point is used for exchanges between the SM and the NFVO, and supports the interfaces defined in Table 4.1.3-1.

Table 4.1.3-1: Interfaces on the Sc-Or reference point

Numbering	Name	Description	Produced by / consumed by
Sc-Or.NsLcm	NS Lifecycle Management	NS Lifecycle Management, derived from the NS LCM interface on the Os-Ma-nfvo reference point. This interface supports notification operations. For a Passive Security Manager there is no further action. Where the Semi-Active or Fully-Active Security Managers needs to take further action, it is done over the Security Policy Enforcement interface.	Produced by the NFVO, consumed by the SM.
Sc-Or.StatusInfo	Status Information Management	This interface supports request/response operations for getting status information such as lists of VNF and run-time information about an NS instance.	Produced by the NFVO, consumed by the SM.
Sc-Or.SecEnforce	Security Policy Enforcement	This interface support request/response operations for Fully-Active or Semi-Active SMs to e.g. request changes to active VNFs to enforce security policies.	Produced by the NFVO, consumed by the SM.
Sc-Or. SecurityVnfMgmt	Security VNF Management	This interface supports request/response operations for management of the VNFs required for security purposes.	Produced by NFVO, consumed by the SM.

4.1.4 Interfaces on the Sc-Vi reference point

The Sc-Vi reference point is used for exchanges between the SM and the VIM, and supports the interface shown in Table 4.1.4-1.

Table 4.1.4-1: Interfaces on the Sc-Vi reference point

Numbering	Name	Description	Produced by / consumed by
Sc-Vi.Telem	Telemetry Information Management	This interface supports notifications and request/response operations of telemetry information as seen by the VIM.	Produced by the VIM, consumed by the SM.

4.2 Relation to other NFV Group Specifications

Information about the reference points in the ETSI NFV architecture can be found in ETSI GS NFV 002 [i.1] and the security monitoring architecture can be found in ETSI GS NFV-IFA 026 [i.4].

5 Reference point and interface requirements

5.1 Introduction

This clause defines or references requirements applicable to interfaces in the context of the Sc-Or and Sc-Vi reference points, in order to support security monitoring and management as specified in ETSI GS NFV-SEC 013 [i.3].

Requirements are labelled according to whether they are applicable to Passive, Semi-Active or Fully-Active security monitoring, using the definitions from ETSI GS NFV-IFA 026 [i.4]. The right-most column of all tables in clause 5 is entitled "PSF" and is used to list the type of SMs to which the requirement applies. "S" and "F" indicate that it applies to "Semi-Active" or "Fully-Active", while "SF" indicates that it applies to Semi-Active and Fully-Active (this is therefore a conditional requirement). If the requirement applies to all types of SM (written as "All") then the requirement is considered to be a mandatory requirement, unless it is otherwise stated in the text of the requirement.

5.2 Reference point requirements

5.2.1 Sc-Or reference point requirements

Table 5.2.1-1 specifies requirements applicable to the Sc-Or reference point.

Table 5.2.1-1: Sc-Or reference point requirements

Numbering	Requirement	PSF (see clause 5.1)
Sc-Or.001	The Sc-Or reference point shall support the NS Lifecycle Management interface produced by the NFVO.	All
Sc-Or.002	The Sc-Or reference point shall support the Status Information Management interface produced by the NFVO.	All
Sc-Or.003	The Sc-Or reference point shall support the Security Policy Enforcement interface produced by the NFVO.	SF
Sc-Or.004	The Sc-Or reference point shall support the Security VNF Management interface produced by the NFVO.	All

5.2.2 Sc-Vi reference point requirements

Table 5.2.2-1 specifies requirements applicable to the Sc-Vi reference point.

Table 5.2.2-1: Sc-Vi reference point requirements

Numbering	Requirement	PSF (see clause 5.1)
Sc-Vi.001	The Sc-Vi reference point shall support the Telemetry Information Management interface produced by the VIM.	All

5.3 Interface requirements

5.3.1 Interface requirements for NS Lifecycle Management

This clause specifies requirements applicable to NS Lifecycle Management interface produced by the NFVO over the Sc-Or reference point. The consumer of the interface is the Security Manager. The requirements applicable to the Semi-Active and Fully-Active Security Manager can be met by a combination of operations provided by this interface with operations provided by other interfaces, i.e. a notification received on the NS Lifecycle Management interface may trigger subsequent operations on the Security Policy Enforcement interface over Sc-Or reference point.

Table 5.3.1-1 specifies requirements applicable to the NS Lifecycle Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.1-1: NS Lifecycle Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.NsLcm.001	The NS Lifecycle Management interface shall support providing reports on NSs including information on their constituent VNFs and PNFs. See note 1.	R1.3.70	All
Sc-Or.NsLcm.002	The NS Lifecycle Management interface shall support the delivery of the package/artefact integrity information (e.g. checksum).	R2.1.250	All
Sc-Or.NsLcm.003	The NS Lifecycle Management interface shall support providing notifications of all unauthorized attempts to change VNFs (including on-boarding, instantiation, modification and termination).	R1.3.110 See note 2.	All

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.NsLcm.004	The NS Lifecycle Management interface shall support providing details of topology changes including migration, scale-in and scale-out of VNFs.	R1.3.220 See note 2.	All
Sc-Or.NsLcm005	The NS Lifecycle Management interface shall support providing VNF lifecycle management event information when a VNF is created.	R2.1.150 See note 2. (The NFVO would know about the end result. The VNFM knows more detail e.g. changes of affected VNFs, intermediate steps for each VNF that is touched.)	All
Sc-Or.NsLcm.006	The NS Lifecycle Management interface shall support providing the following information as part of the NS LCM notification related to a VNF instantiation event: • Source of request (see note 3). • VNF Package Identifier • VNFD Identifier. • Integrity check of VNF package/artefact. • VNF instance identifier. • Connectivity information (including connections to PNFs) as known by NFV-MANO.	R2.1.210 See note 2.	All
Sc-Or.NsLcm.007	The NS Lifecycle Management interface shall support providing the following information relating to a VNF modification event (see note 4) and VNF termination event: • Source of request (see note 3). • VNF instance identifier • Details of the change.	R2.1.160 (modification) and R2.1.170 (termination). R2.1.220 (modification) and R2.1.230 (termination). See note 2 (anything at resource level is not seen by the NFVO).	All
Sc-Or.NsLcm.008	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.2	All
NOTE 1: PNF information is limited to a description of their connection points, information about the virtual links they are attached to, and information about the network forwarding paths in which they are involved, if any. Additional information about PNFs is out of scope of ETSI NFV specifications. NOTE 2: These requirements are based on an underlying requirement (from ETSI GS NFV-IFA 026 [i.4]) for information that was originally stored or created by the VNFM. As described in clause 4.1.2, this information is being sent to the SM over the Sc-Or reference point. NOTE 3: The source of the event is e.g. application layer OSS/BSS, VNF, EMS, auto healing function. NOTE 4: Modification is any change to a VNF: - configuration; - run-time images or code version; - location (physical or logical); - host resources; - NFV layer communications peering relationships; - identification of the VNF instance (i.e. the identity generated during the instantiation); - changes to 1 or more VNFC instances within a VNF; - load balancing.			

5.3.2 Interface requirements for Status Information Management

Table 5.3.2-1 specifies requirements applicable to the Status Information Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.2-1: Status Information Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.StatusInfo.001	The Status Information Management interface shall support providing the VNF instantiation state and operation state for all active VNFs. See note.	R2.1.320	All
NOTE: For more details on instantiation state see ETSI GS NFV-IFA 007 [i.5], clause 7.2.2 (INSTANTIATED, NOT_INSTANTIATED). For more details on operational states see: - ETSI GS NFV-IFA 007 [i.5], clause 7.2.11 (STARTED, STOPPED). - ETSI GS NFV-IFA 007 [i.5], clause 8.5.3 "vnfState" attribute in "InstantiatedVnfInfo". - ETSI GS NFV-SOL 003 [i.6], clauses 5.5.4.3 to 5.5.4.7 and 5.6.2.			

5.3.3 Interface requirements for Security Policy Enforcement

Table 5.3.3-1 specifies requirements applicable to the Security Policy Enforcement interface produced by the NFVO over the Sc-Or reference point. Any additional aspects of security policy management (beyond those listed below) are out of scope of the present document. Details are in ETSI GS NFV-IFA 026 [i.4] and ETSI GS NFV-SEC 013 [i.3].

Table 5.3.3-1: Security Policy Enforcement interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.SecEnforce.001	For Semi-Active and Fully-Active Security Managers, the Security Policy Enforcement interface shall support the provision of security policy instructions (e.g. immediately terminate one or more VNFs of a network service).	Derived from R2.1.30 (subset) R2.1.40 (subset)	SF
Sc-Or.SecEnforce.002	For Semi-Active Security Managers, the Security Policy Enforcement interface shall support terminating a VNF. The termination request shall be able to specify: • whether another VNF may be created to replace the VNF being terminated. • whether it wants a snapshot of the VNF to be made for later analysis.	R2.1.260 (re-phrased as interface requirement)	S
Sc-Or.SecEnforce.003	For Fully-Active Security Managers, the Security Policy Enforcement interface shall support terminating a VNF. The termination request shall be able to specify: • whether another VNF may be created to replace the VNF being terminated. • whether it wants a snapshot of the VNF to be made for later analysis. • whether the VNF package and VNFD shall be disabled. • whether all other VNFs running on the same host should be terminated. See note. • whether NFV-MANO shall actively erase the resources used by all HMEEs, TPMs, HSMs or other storage used by the terminated VNF.	R2.1.270 (re-phrased as interface requirement)	F

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.SecEnforce.004	For Semi-Active and Fully-Active Security Managers, the Security Policy Enforcement interface shall support terminating the use of a specific host: • The termination request shall allow the SM to specify whether VNFs running on the host may be migrated or shall be terminated. • The termination request shall allow the SM to specify whether to quarantine the host along with the hosted VNFs.	R2.1.290 (for S) R2.1.300 (for F)	SF
Sc-Or.SecEnforce.005	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.2	All
NOTE: Requirement is met by determining all the other VNFs on the same host and terminating each of them.			

5.3.4 Interface requirements for Security VNF Management

Table 5.3.4-1 specifies requirements applicable to the Security VNF Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.4-1: Security VNF Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Or.SecurityVnfMgmt.001	The Security VNF Management interface shall support creating/instantiating, modifying or terminating security VNFs to be inserted into or removed from a network service.	Derived from R2.1.310 (uses the term creating) and R1.2.100 and R1.2.120 (uses the term instantiating).	SF
Sc-Or.SecurityVnfMgmt.002	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.2.	All

5.3.5 Interface requirements for Telemetry Information Management

Table 5.3.5-1 specifies requirements applicable to the Telemetry Information Management interface produced by VIM over the Sc-Vi reference point.

Table 5.3.5-1: Telemetry Information Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [i.4]	PSF (see clause 5.1)
Sc-Vi.Telem.001	The Telemetry Information Management interface shall support querying and notifying telemetry information which includes: NFVI system configurations (including capacity, images, compute flavour), policies and packet headers.	Covers part of R3.140.	All
Sc-Vi.Telem.002	The Telemetry Information Management interface shall support providing location information from the VIM, e.g. HostID, ZoneID and physical location.	R2.1.160 and R2.1.210	All

5.4 Security requirements

Table 5.4-1 specifies the requirements relating to security in the realization of interface operations over Sc-Or and Sc-Vi reference point. Each requirement applies to all interfaces except where it is stated otherwise.

Table 5.4-1: Security requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA026 [i.4]	PSF (see clause 5.1)
Security.001	Each set of SM to NFV-MANO interfaces on the reference points Sc-Or and Sc-Vi (for the same SM) shall use independent integrity and confidentially protection from all other SM to NFV-MANO interface sets. This is a requirement about having independent cryptographic keys from the interfaces not defined in the present document.	Clause 5.3	All
Security.002	All interfaces shall enable NFV-MANO to ensure that VNF lifecycle management events are sent to the correct one or more SMs subject to the trust domain separation model being implemented by a network.	Clause 5.3	All
Security.003	All interfaces shall support identification of parties to enable NFV-MANO to reject instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain.	Clause 5.3	All
Security.004	Traffic of the SM shall be isolated and separated from other traffics in data/control planes etc.	R.1.1.160	All
Security.005	The Telemetry Information Management interface shall support relevant additional data security policies and authorized access such as telemetry source and destination authentication, telemetry data integrity and confidentiality, opportunistic encryption, trusted time, and synchronization across multiple NFVI systems.	R.1.3.160	All
Security.006	All interfaces shall enable the NFVO/VNFM/VIM to support separate independent security associations and keys for each SM on each logical interface.	R.2.1.70	All
Security.007	The identification and authentication over all interfaces shall enable the NFVO/VNFM/VIM to ensure that only lifecycle management events applicable to a specific SM(s) are sent to that SM(s).	R.2.1.80	All

6 Interfaces over Sc-Or reference point

6.1 Introduction

This clause defines the interfaces exposed by the NFVO towards the SM over the Sc-Or reference point.

6.2 NS Lifecycle Management Interface

This interface allows the SM to subscribe to notifications relating to NS lifecycle management operations from the NFVO. The requirements for this interface are specified in table 5.3.1-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Subscription/Notification (refer to clauses 7.3.11 to 7.3.14 of ETSI GS NFV-IFA 013 [3]).

NOTE: The Subscription/Notifications operations in clauses 7.3.11 to 7.3.14 of ETSI GS NFV-IFA 013 [3] enable Sc-Or.NsLcm.006 to be met as follows:

- The Subscription/Notifications operations in clauses 7.3.11 to 7.3.14 return the information as shown in clause 8.3.2.2 of ETSI GS NFV-IFA 013 [3].
- This gives the appropriate identifiers in order to use the QueryNS operation to retrieve all the information required by Sc-Or.NsLcm.006. Specifically, QueryNS returns NSInfo which contains VnfInfo, which meets Sc-Or.NsLcm.006 as follows:
  - VNF Package Identifier = vnfinfo.onboardedVnfPkgInfoId.
  - VNFD Identifier = vnfinfo.vnfdId.
  - VNF instance identifier = vnfinfo.vnfInstanceId.
  - Connectivity information (including connections to PNFs) as known by NFV-MANO = vnfinfo.extVirtualLinkInfo.
  - Integrity check of VNF package/artefact = use onboardedVnfPkgInfoId to get to VnfPkgInfo, which has a checksum (and also the VNF Package has a SoftwareImageInformation element with a checksum).

6.3 Status Information Management Interface

This interface allows the SM to query status information from the NFVO. The requirements for this interface are specified in table 5.3.2-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Query NS (refer to clause 7.3.6 of ETSI GS NFV-IFA 013 [3]).

6.4 Security Policy Enforcement Interface

This interface allows (Fully-Active or Semi-Active) SMs to request changes to active VNFs to enforce security policies. The requirements for this interface are specified in table 5.3.3-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Update NS (refer to clause 7.3.5 of ETSI GS NFV-IFA 013 [3], see note 1).
- Update VNF Package Info (refer to clause 7.7.16 of ETSI GS NFV-IFA 013 [3], see note 3).

NOTE 1: Update NS is used as follows:

- To meet Sc-Or.SecEnforce.002 and .003 (terminating VNF), with updateType = RemoveVnf and a removeVnfInstanceId attribute set to the appropriate identifier (see note 2).
- To meet Sc-Or.SecEnforce.002 and .003 (create snapshot), with updateType = CreateSnapshot.
- To meet Sc-Or.SecEnforce.002 and .003 (whether another VNF may be created) by sending one UpdateNS request to kill the VNF instance and sending another UpdateNS request to recreate it if required.

NOTE 2: According to ETSI GS NFV-IFA 013 [3], note 1 of table 7.3.5.2-1, a VNF instance is only terminated by the NFVO if it is no longer used by any NS. As a consequence, in order to terminate a VNF instance, the SM has to send an UpdateNS request to each NS where this VNF instance is a part.

NOTE 3: Update VNF Package Info is used as follows:

- To meet Sc-Or.SecEnforce.003 (disabling a VNF Package).

NOTE 4: An explanation of how to meet Sc-Or.SecEnforce.004 is not given in the present document.

6.5 Security VNF Management Interface

This interface allows the SM to manage security-related VNFs from the NFVO. The requirements for this interface are specified in table 5.3.4-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Update NS (refer to clause 7.3.5 of ETSI GS NFV-IFA 013 [3]).

NOTE: It is assumed that the VNFD of the security-related VNF is referenced from the NSD.

7 Interfaces over Sc-Vnfm reference point

7.1 Introduction

The present document does not define any interfaces over the Sc-Vnfm reference point.

8 Interfaces over Sc-Vi reference point

8.1 Introduction

This clause defines the interfaces exposed by the VIM towards the SM over the Sc-Vi reference point.

8.2 Telemetry Information Management interface

8.2.1 Description

This interface allows the SM to query or subscribe to notifications related to telemetry information from the VIM. The requirements for this interface are specified in table 5.3.5-1.

The following operations are defined for this interface, and these operations shall follow the specifications from ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2], except that the producer is the VIM and the consumer is the SM.

The interface supports the following Query operations derived from interfaces in ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2]:

- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.2 Query Compute Capacity operation
- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.5 Query Compute Resource Zone operation
- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.6 Query NFVI-PoP Compute Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.4.2 Query Network Capacity operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.4.5 Query NFVI-PoP Network Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.5.3 Query NFP operation
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4.5 Query NFVI-PoP Storage Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4.6 Query Storage Resource Zone operation
- From ETSI GS NFV-IFA 005 [1], clause 7.9.3.3 Query Storage Resource Quota operation

- From ETSI GS NFV-IFA 005 [1], clause 7.10.3 Query Compute Host Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.2.2 Query Images operation
- From ETSI GS NFV-IFA 006 [2], clause 7.2.3 Query Image operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.1.3 Query Virtualised Compute Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.3.4 Query Virtualised Compute Resource Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.4.3 Query Compute Flavour operation
- From ETSI GS NFV-IFA 006 [2], clause 7.4.1.3 Query Virtualised Network Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.4.3.4 Query Virtualised Network Resource Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.5.1.3 Query Virtualised Storage Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.5.3.4 Query Virtualised Storage Resources Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.7.3 Query PM Job operation
- From ETSI GS NFV-IFA 006 [2], clause 7.7.8 Query Threshold operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.1.2 Query Compute Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.2.2 Query Network Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.3.2 Query Storage Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.9.1.2 Query Compute Resource Quota operation
- From ETSI GS NFV-IFA 006 [2], clause 7.9.2.2 Query Network Resource Quota operation
- From ETSI GS NFV-IFA 006 [2], clause 7.9.3.2 Query Storage Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.10.4 Query Policy operation
- From ETSI GS NFV-IFA 006 [2], clause 7.10.10 Query Subscription Info operation

The interface supports subscription/notification operations derived from the following interfaces in ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2]:

- From ETSI GS NFV-IFA 005 [1], clause 7.3.4 Virtualised Compute Resources Capacity Management Interface
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4 Virtualised Storage Resources Capacity Management Interface
- From ETSI GS NFV-IFA 005 [1], clause 7.11.1 Compute Host Capacity Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.3.2 Virtualised Compute Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.3.3 Virtualised Compute Resources Information Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.4.2 Virtualised Network Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.4.3 Virtualised Network Resources Information Management Interface

- From ETSI GS NFV-IFA 006 [2], clause 7.5.2 Virtualised Storage Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.5.3 Virtualised Storage Resources Information Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.6 Virtualised Resources Fault Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.7 Virtualised Resources Performance Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.8.4 Virtualised Resources Reservation Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.9.4 Virtualised Resources Quota Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.10 Policy Management Interface

History

Document history		
V4.1.1	August 2020	Publication