ETSI GR NFV-IFA 043 V5.1.1 (2024-05)

Network Functions Virtualisation (NFV) Release 5; Architectural Framework; Report on enhanced container networking

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-IFA043

Keywords

autonomic networking, container, network management, NFV

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document investigates the aspects of NFV that have an impact on enhanced container networking, including but not limited to:

- telecom specific use cases (e.g. connectivity for containers realizing vRAN, etc.) and solutions for container networking that could be applied to NFV-MANO;
- enhancements to OS container multiple network support; and
- support of network policies for container networking.

The present document also documents potential solutions, and where applicable, it also provides recommendations for enhancements to the NFV architectural framework and its functionality aiming to provide further support to address enhanced container networking.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ETSI GR NFV 003 (V1.8.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GR NFV-IFA 038 (V4.1.1): "Network Functions Virtualisation (NFV) Release 4; Architectural Framework; Report on network connectivity for container-based VNF".

[i.3] ETSI GS NFV-SOL 018 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; Profiling specification of protocol and data model solutions for OS Container management and orchestration".

[i.4] ETSI GS NFV-IFA 036 (V4.3.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Specification of requirements for the management and orchestration of container cluster nodes".

[i.5] ETSI GS NFV-IFA 040 (V4.1.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

[i.6] ETSI GS NFV-IFA 007 (V4.2.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.7] ETSI GS NFV-SOL 003 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point".

[i.8] ETSI GS NFV-IFA 008 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.9] ETSI GS NFV-IFA 011 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.10] ETSI GR NFV-IFA 046 (V5.1.1): "Network Functions Virtualisation (NFV) Release 5; Architectural Framework; Report on NFV support for virtualisation of RAN".

[i.11] Kubernetes® Network Plugins.

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.1] apply.

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI GR NFV 003 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

SNCP	Secondary Network Configuration Profile

4 Overview

4.1 Problem statement

ETSI GR NFV-IFA 038 [i.2] studies, as part of the ETSI NFV Release 4, the management of network connectivity and its associated virtualised network resources for container-based VNFs by the NFV-MANO Architectural Framework. OS container multiple networks provide the network connectivity between containerized VNFs via the secondary container cluster internal/external networks as described in ETSI GR NFV-IFA 038 [i.2].

The present document extends beyond the use cases introduced in ETSI GR NFV-IFA 038 [i.2] by further considering additional issues and/or enhancements in the following areas, such as (not exhaustive list):

- operation and management for container network;
- security and isolation of container networks;
- secondary container cluster networks spanning multiple clusters and sites;
- impact of hybrid deployment on container networks; and
- applicability of container networks for actual telco use cases and protocols.

4.2 Introduction

The present document investigates aspects of enhanced container network for new use cases and solutions different from the use cases in ETSI GR NFV-IFA 038 [i.2]. In more detail, the present document further studies on the following technical scenarios:

- The telecom specific use cases (e.g. connectivity for containers realizing vRAN, etc.) and solutions for container networking that could be applied by NFV-MANO.
- The new scenarios and solutions of cluster networking derived from the open source communities, e.g. Kubernetes®, which are applicable to the enhanced container network in the NFV framework.
- The use cases related to lifecycle management of OS container multiple networks, especially for modifying OS container multiple networks, such as the increase or decrease in number of the network objects of multiple networks, etc.
- The use cases for effective isolation of container networks. In this case, network isolation is expected to be in place to block access to unallowed networks. One certain case is that network policies can be used to limit the connectivity of the groups of one or more OS container (such as a Pod in the case of Kubernetes®) and data flows to ensure effective isolation of networks for different tenants.

4.3 Network policy

Clause 6.8 of ETSI GR NFV-IFA 038 [i.2] introduces the concept of network policy, and relevant parameters of network policy of secondary container cluster internal/external network defined in a Secondary Network Configuration Profile (SNCP).

A namespace provides a mechanism to isolate its grouped elements from others, as specified in clause 5.2.3 in ETSI GS NFV-IFA 040 [i.5]. Namespaces for container resource isolation can be used in CIS cluster, including container network resources.

In general, groups of one or more OS containers in different namespaces are not allowed to communicate with each other. However, in specific scenarios, some applications need the groups of one or more OS containers in different namespaces to communicate with each other; and a network policy can serve for this case.

Network policies can be used to control traffic flow at the IP address or port level (OSI layer 3 or 4) of groups of one or more OS containers. For example, the groups of one or more OS containers can be rejected from other namespace to access, be allowed from other namespace to access the specified application, or be restricted to access between applications in the same namespace, and so on. In Kubernetes®, network policies are considered to be used for particular applications in a CIS cluster, and network policies are implemented by the network plugin [i.11], e.g. Calico. To use network policies, a feasible networking solution needs to be considered for supporting network policy, and a network policy controller is needed for creating a network policy resources and performing network policy rules.

A network policy specifies how a group of one or more OS containers is allowed to communicate with other groups of one or more OS containers which can be inside the same or different namespaces based on setting rules of ingress and egress. The network policy establishes the rules for a selected group of one or more OS containers and contains the following three elements:

- Which other groups of one or more OS containers are allowed, with the exception that a group of one or more OS containers cannot block access to itself.
- Namespaces that are allowed.
- IP blocks that are allowed.

There are two sorts of isolation for a group of one or more OS containers: isolation for egress, and isolation for ingress. They are independent and both relevant for a connection from one group of one or more OS containers to another. The network policy controller manages connections for the groups that can be established. For allowing the connectivity from a source group to a destination one to be allowed, both the egress policy on the source group and the ingress policy on the destination group are needed.

A network policy controller is configured according to the network policy rules to control traffic which is allowed to/from the groups of one or more OS containers via matching the namespace selectors, the selectors for the groups of one or more OS containers and IP blocks.

When a selected group of one or more OS containers is set to be "Egress" in its policy types, the only allowed connections from the group are those allowed by the egress list of some network policies that applies to the group for egress. Similarly, when a selected group of one or more OS containers is set to be "Ingress" in its policy types, the only allowed connections into the group are those from the group's node and those allowed by the ingress list of some network policies that applies to the group of one or more OS containers for ingress.

Figure 4.3-1 illustrates an example of connectivity between groups of one or more OS containers in different namespaces. For simplicity, in the figure, the alternative term "Pod" is used for referring to the group of one or more OS containers.

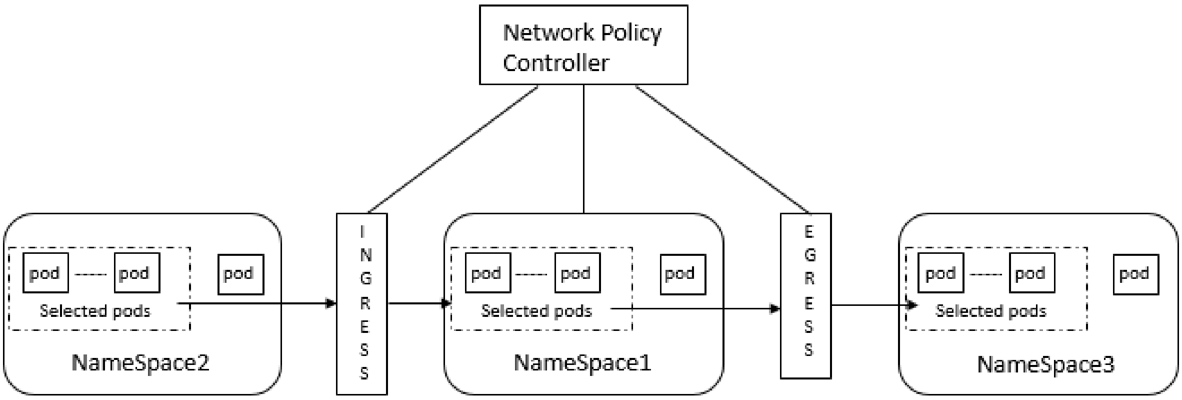

Figure 4.3-1: Example of connectivity between groups of one or more OS containers in different namespaces

5 Use cases

5.1 Overview

Clause 5 documents various use cases related to network connectivity for container-based VNFs. Firstly, clause 5.2 describes a use case related to pre-configure secondary container cluster networks. Secondly, clause 5.3 describes use cases related to re-configure secondary container cluster networks, which includes adding new secondary container cluster networks and deleting existing secondary container cluster networks. Finally, clause 5.4 describes a use case about connectivity for hybrid VM/container-based VNFs deployed on multiple CIS clusters.

5.2 Pre-configure secondary container cluster networks

5.2.1 Introduction

The secondary container cluster internal/external networks can be dynamically configured and associated with VLs when an NS is instantiated, as defined in ETSI GR NFV-IFA 038 [i.2]. Another case is that secondary container cluster internal/external networks can be statically pre-configured in CIS clusters based on the planning of multiple networks, and then simply be assigned to associated VLs when an NS is instantiated.

5.2.2 Actors and roles

Table 5.2.2-1 describes the use case actors and roles involved in the pre-configuration of secondary container cluster internal/external networks for an NS instantiation.

Table 5.2.2-1: Pre-configure secondary container cluster networks actors and roles

#	Actor and role	Description
1	CCM	Responsible for the lifecycle management of the CIS clusters.
2	NFVO	Responsible for orchestrating the configuration of secondary container cluster internal/external networks.
3	CISM	Responsible for performing operations of pre-configuring the secondary container cluster internal/external networks.

5.2.3 Pre-conditions

Table 5.2.3-1 describes the pre-conditions for pre-configuring secondary container cluster internal/external networks.

Table 5.2.3-1: Pre-configure secondary container cluster networks pre-conditions

#	Pre-condition	Description
1	NFVO, CISM and CCM are running.	
2	The CIS clusters to be configured are available.	
3	The NSD is available.	

5.2.4 Post-conditions

Table 5.2.4-1 describes the post-conditions after pre-configuring secondary container cluster internal/external networks.

Table 5.2.4-1: Pre-configure secondary container cluster networks post-conditions

#	Post-condition	Description
1	The NS instance is created successfully.	
2	The pre-configured secondary container cluster internal/external networks are available and fulfil the connectivity of assigned NS/VNF VLs.	

5.2.5 Flow description

Table 5.2.5-1 describes the use case flow for pre-configuring secondary container cluster internal/external networks.

Table 5.2.5-1: Pre-configure secondary container cluster networks flow description

#	Actor/Role	Action/Description
Begins when	NFVO	Based on the network planning of multiple networks (e.g. SNCP), the NFVO pre-configures the secondary container cluster internal/external networks in the CIS clusters. SNCPs are included as artefacts in the NSD file structure as described in clause 7.1.4 in ETSI GR NFV-IFA 038 [i.2].
Step #1	NFVO<->CCM	The NFVO requests to the CCM to provide the available CIS clusters as defined in ETSI GS NFV-IFA 036 [i.4] according to the requirements of virtual resources for NS to be instantiated. The CCM returns the information of the CIS clusters to the NFVO.
Step #2	NFVO->CCM	The NFVO requests the CCM to perform the operation of pre-configuring secondary container cluster internal/external networks based on the SNCPs (see note).
Step #3	CCM<->CISM	As specified in ETSI GS NFV-IFA 036 [i.4], the CCM requests the CISM to install the network configuration for the secondary container cluster networks via the manifest configuration files. The CISM returns the information regarding the created network attachment definition resources to the CCM.
Step #4	CCM->NFVO	The CCM returns the information of the pre-configured secondary container cluster internal/external networks to the NFVO.

#	Actor/Role	Action/Description
Ends when	NFVO	The NFVO performs the procedures of instantiating the NS. For the operation related VLs, the NFVO directly associates (e.g. by matching NS/VNF VL requirements to pre-configured networks) the pre-configured secondary container cluster internal/external networks with NS VLs and VNF VLs instead of initiating the operation of creating secondary container cluster internal/external networks, and then the NFVO continues the follow-up procedures to instantiate the NS as defined in ETSI GR NFV-IFA 038 [i.2].
NOTE: More information about SNCPs and their relation to NFV descriptors and CIS clusters is provided in clause 7.1 in ETSI GR NFV-IFA 038 [i.2].		

5.3 Re-configure secondary container cluster networks

5.3.1 Introduction

For an existing NS instance or containerized VNF instance, secondary container cluster internal/external networks have been configured to provide multiple networks. The relevant use cases and solutions have been described in ETSI GR NFV-IFA 038 [i.2].

For customer's further requirements, like 5G vertical customers, it might be needed to update existing NS instances, e.g. to enable additional connectivity for the customer to connect to the network operator's network. This can further imply to re-configure secondary container cluster networks while the NS instance or VNF instance is running, in the case that network connectivity is either fully or partially fulfilled with secondary container cluster networks. Another possible outcome to fulfil connectivity requirement could be to delete unused secondary container cluster networks, if needed.

5.3.2 Actors and roles

Table 5.3.2-1 describes the use case actors and roles involved in re-configuring secondary container cluster internal/external networks to update the multiple networks, e.g. by adding new secondary container cluster networks or deleting existing secondary container cluster networks.

Table 5.3.2-1: Re-configure secondary container cluster networks actors and roles

#	Actor and role	Description
1	OSS/BSS	Responsible for triggering the operation of NS update.
2	NFVO	Responsible for initiating the operation of updating multiple networks to add new secondary container cluster networks or delete existing ones. Responsible for lifecycle management of the NS, containerized VNF and multiple networks.
3	VNFM	Responsible for the lifecycle management of containerized VNF/VNFC.
4	CISM	Responsible for managing the re-configuration of the secondary container cluster internal/external networks to update the set of multiple networks.
5	CISI	Responsible for setting up (e.g. configure relevant CIS cluster resources) the secondary container cluster internal/external networks.

5.3.3 Pre-conditions

Table 5.3.3-1 describes the pre-conditions for re-configuring secondary container cluster internal/external networks to update the multiple networks, e.g. by adding new secondary container cluster networks or deleting existing secondary container cluster networks.

Table 5.3.3-1: Re-configure secondary container cluster networks pre-conditions

#	Pre-condition	Description
1	OSS/BSS, NFVO, VNFM, VIM are running, and a NS instance or container VNF instance has been created.	
2	The multiple networks for NS instance or containerized VNF instances have been created, the network connectivity has been implemented between groups of one or multiple OS containers (e.g. Pods) via the multiple networks.	The multiple networks is implemented by the multiple secondary container cluster internal/external networks.

5.3.4 Post-conditions

Table 5.3.4-1 describes the post-conditions after re-configuring secondary container cluster internal/external networks to update the multiple networks.

Table 5.3.4-1: Re-configure secondary container cluster networks post-conditions

#	Post-condition	Description
1	The secondary container cluster internal/external networks have been re-configured.	
2	The NS instance or containerized VNF instance has been updated successfully.	The containerized VNF/VNFC can connect to the new (in case of adding) secondary container cluster networks.

5.3.5 Flow description

Table 5.3.5-1 describes the use case flow for re-configuring secondary container cluster internal/external networks to update the multiple networks.

Table 5.3.5-1: Re-configure secondary container cluster networks flow description

#	Actor/Role	Action/Description
Begins when	OSS/BSS	The OSS/BSS is ready to trigger an NS update to request changing the external VNF connectivity of NS instance or changing internal VNF connectivity of a containerized VNF instance.
Step #1	OSS/BSS->NFVO	The NFVO analyses the request received from the OSS/BSS, and determines that it concerns to updating the multiple networks. Then the NFVO decides to re-configure the secondary container cluster internal/external networks.
Step #2	NFVO->CCM	The NFVO requests the CCM to add/delete/modify CIS cluster nodes networks serving as secondary container cluster networks according to the necessary updates.
Step #3	CCM->NFVO	The CCM performs the necessary updates regarding the CIS cluster nodes networks, also interacting with the infrastructure management functions regarding the resource fulfilment parts for the networks. Once completed, it provides back to the NFVO the information about the CIS cluster nodes networks and the corresponding secondary container cluster networks.
Step #4	NFVO->CISM	The NFVO requests to perform the operation of re-configuring network attachment definition resources corresponding to the secondary container cluster internal/external networks based on the SNCPs.
Step #5	CISM<->CISI	The CISM performs the operation of re-configuring the network attachment definition resources for the corresponding secondary container cluster internal/external networks based on the SNCPs via interaction with the CISI.
Step #6	CISM->NFVO	The CISM returns the information of the re-configured network attachment definition resources of the corresponding secondary container cluster internal/external networks to the NFVO.
Step #7	NFVO->VNFM	The NFVO performs the procedures of updating the NS instance if the container networks which are added or deleted are used for connection between containerized VNFs, or updating the containerized VNF instance if the container networks which are added or deleted are used for connection between VNFCs belonging to the same containerized VNF, and requests VNFM to update VNF instance. The NFVO sends to the VNFM the information about the network attachment definition resources to be used for updating the connectivity of the VNF/VNFC to the NS/VNF VLs that are fulfilled with the updated secondary container cluster networks.

#	Actor/Role	Action/Description
Step #8	VNFM->CISM	The VNFM performs the procedures of updating the containerized VNF instance, and requests CISM to update the containerized workloads realizing the VNFC instances. For updating the containerized workloads, the CISM creates new groups of one or multiple OS containers (e.g. Pods) and connects them to the container networks, or deletes unused groups of one or multiple OS containers.
Step #9	CISM ->VNFM	CISM informs VNFM that the containerized workloads are updated successfully.
Step #10	VNFM->NFVO	The VNFM informs NFVO that the VNF instance is updated successfully after the VNFM has updated/created/deleted the set of relevant VNFC instances.
Step #11	NFVO ->OSS/BSS	The NFVO informs OSS/BSS that the NS instance or VNF instance has been updated successfully after the VNFM has implemented the operation of updating VNF instance and secondary container cluster internal/external networks have been re-configured.
Ends when	OSS/BSS	The OSS/BSS confirms that NS instance has been updated successfully.

5.4 Connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters

5.4.1 Introduction

As documented in clause 4.3 of ETSI GR NFV-IFA 038 [i.2], it is expected that interconnectivity can be established between various forms of VNFs, regardless of whether they are container-based, VM-based or hybrid (i.e. a mix of VM and container-based VNFC). However, ETSI GR NFV-IFA 038 [i.2] does not describe use cases about:

- Establishing connectivity between VM-based VNF or VNFC instances and container-based VNF or VNFC instances, or even to PNF instances.
- Establishing connectivity for container-based VNF or VNFC instances deployed across multiple CIS clusters.

NOTE 1: ETSI GR NFV-IFA 038 [i.2] reports about use cases and solutions to establish connectivity across CIS cluster nodes within the same CIS cluster.

The present use case illustrates the intent by the network operator (or on its behalf the OSS/BSS and NFV-MANO) to establish connectivity for hybrid VM/container-based deployments possibly across different CIS clusters. Figure 5.4.1-1 illustrates a possible scenario. For simplicity, all the depicted VNF and PNF instances are assumed to be constituents of the same NS instance. This complex networking scenario is common in environments where a mix of technologies are employed for deploying the network, in addition to also handling connectivity to parts of the network that are not virtualised. A specific example of this is the deployment of vRAN, where some NFs are virtualised, like the Centralized Unit (CU) and Distributed Unit (DU), while others are not, like the Radio Unit (RU). More information about vRAN is available in the ETSI GR NFV-IFA 046 [i.10].

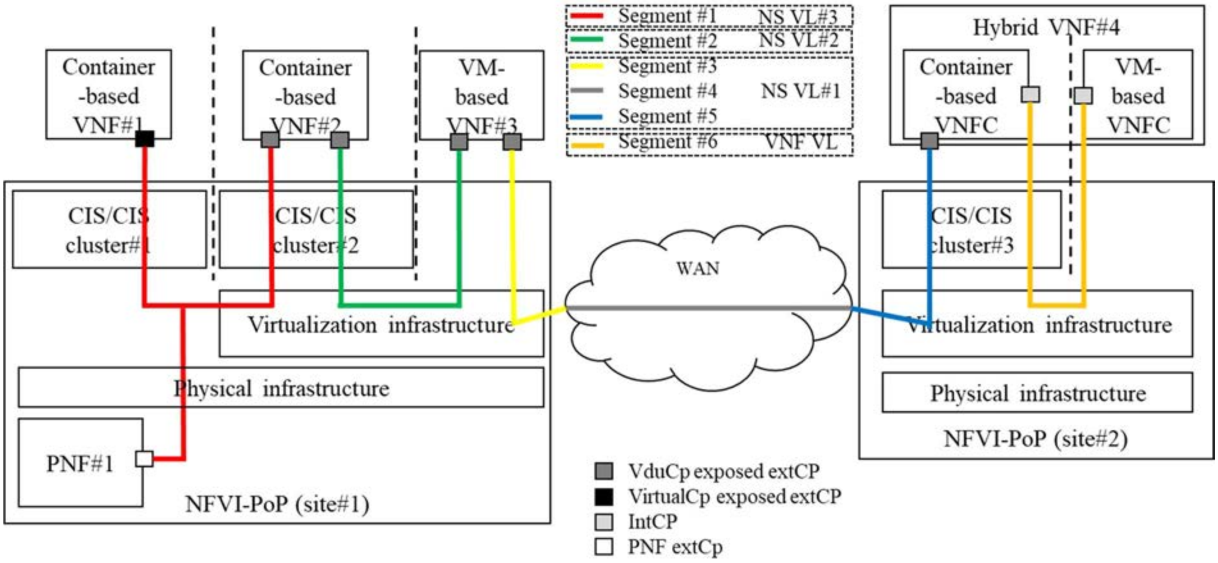

Figure 5.4.1-1: Example of scenario depicting hybrid VM/container-based deployments across different CIS clusters

The different network segments involved in this scenario are:

- Segment #1: connectivity between two container-based VNF instances deployed on different CIS clusters and a PNF, residing on the same NFVI-PoP (see red line on the left hand-side). One of the CIS clusters is deployed on bare-metal, and the other one on virtualisation infrastructure (i.e. VM-based). The PNF instance is depicted as part of the NFVI-PoP, but this does not mean that the PNF is instantiated with resources from the NFVI, nor that it is part of the NFVI. However, it is assumed that the PNF instance is or can be connected to the network fabric in the NFVI-PoP. At VL level, this segment corresponds to an NS VL, indicated as NS VL#3 in figure 5.4.1-1.

- Segment #2: connectivity between a container-based VNF on a VM-based CIS cluster with a VM-based VNF over a common virtualisation infrastructure, residing on the same NFVI-PoP (see green line on the left hand-side). At VL level, this segment corresponds to an NS VL, indicated as NS VL#2 in figure 5.4.1-1.

- Segment #3: connectivity from a VM-based VNF towards the WAN/transport network (see yellow line in the middle).

- Segment #4: multi-site connectivity across the WAN/transport network.

- Segment #5: connectivity from the WAN/transport network towards an external connection point of a hybrid VNF exposed by a container-based VNFC (see blue line on the right hand-side). At VL level, segments #3, #4 and #5 correspond to an NS VL, indicated as NS VL#1 in figure 5.4.1-1.

- Segment #6: connectivity between VNFC components of the same VNF (i.e. the hybrid VNF), one based on containers deployed on a VM-based CIS cluster, and a VM-based VNFC. This would correspond to a VNF internal VL, indicated simply as VNF VL in figure 5.4.1-1.

NOTE 2: The use of the term "segment" does not imply the use of some form of network segmentation technology. The term "segment" is used only to reflect portions of connectivity.

5.4.2 Actors and roles

Table 5.4.2-1 describes the use case actors and roles involved in the use case.

Table 5.4.2-1: Connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters actors and roles

#	Actor and role	Description
1	CCM	Responsible for lifecycle management of the CIS clusters, including their CIS cluster nodes networks.
2	NFVO	Responsible for orchestrating the connectivity for the VNFs/NSs.
3	VNFM	Responsible for the lifecycle management of the VNFs.
4	VIM	Responsible for the virtualised resource management, including virtualised networks in the NFVI.
5	CISM	Responsible for the containerized workload management and creation of network attachment definition resources for secondary container cluster networks.
6	WIM	Responsible for the management of multi-site connectivity services.

5.4.3 Pre-conditions

Table 5.4.3-1 describes the pre-conditions for the use case.

Table 5.4.3-1: Connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters pre-conditions

#	Pre-condition	Description
1	NFVO, CCM, VIM, CISM and WIM are running.	
2	The CIS clusters are available.	
3	The NSD and referenced VNF Packages (with corresponding VNFD) are onboarded.	The NSD is used for the deployment of the NS referencing all the relevant VNFs to deploy and PNF to connect.
4	The PNF is available and connected physically to the network fabric in the NFVI-PoP.	

5.4.4 Post-conditions

Table 5.4.4-1 describes the post-conditions for the use case.

Table 5.4.4-1: Connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters post-conditions

#	Post-condition	Description
1	The NS instance is created successfully.	All the NS constituents (e.g. VNF and PNF) are connected via the one or more NS VL.

5.4.5 Flow description

Table 5.4.5-1 describes the use case flow.

NOTE: For simplicity and to ease the use case flow, the use case assumes the setup of the connectivity for a scenario as depicted in figure 5.4.1-1 in terms of deriving the number of NS VL and necessary network segments established through the virtual networks and primary/secondary container cluster networks.

Table 5.4.5-1: Connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters flow description

#	Actor/Role	Action/Description
Begins when	NFVO (with VNFM)	The NFVO receives the request to instantiate an instance of the NS based on the onboarded NSD. The NFVO processes the request and determines which VNF instances to deploy and the set of NS VL needed for establishing the connectivity between the NS constituents. The following set of NS VL are derived: • NS VL#1 to connect between VNF#3 and VNF#4 across different sites (this corresponds to the segments #3, #4 and #5 in figure 5.4.1-1). • NS VL#2 to connect between VNF#3 and VNF#2 within site#1 (this corresponds to the segment #2 in figure 5.4.1-1). • NS VL#3 to connect between VNF#1, VNF#2 and PNF#1 (this corresponds to the segment #1 in figure 5.4.1-1). In addition, the NFVO determines that the VNF#4 has an internal VL (this corresponds to the segment #6 in figure 5.4.1-1) to be established between a container-based VNFC and a VM-based VNFC, e.g. by learning through VNF LCM granting procedures (see note 1). The corresponding types of VNF external CP connectivity are determined, e.g. VNF#1 uses a VirtualCP for external connectivity. See note 2.
Step #1	NFVO->WIM	The NFVO requests the WIM to instantiate an MSCS to establish service connectivity between site#1 and site#2.
Step #2	NFVO->VIM	For the instantiation of the VNF#4 internal VL, the NFVO requests the VIM managing resources in the site#2 to create a virtualised network able to interconnect VMs conforming the CIS cluster#3 with other VMs that can be instantiated on the virtualised infrastructure (for creating VM-based VNFC).
Step #3	NFVO->CCM	For the instantiation of the VNF#4 internal VL, in addition, the NFVO requests the CCM to create a CIS cluster nodes network (see note 3) to be used as a secondary container cluster external network with connectivity to the virtual network created in the step #2. For the instantiation of the network segment in the site#2 towards the NS VL#1, the NFVO requests the CCM to create a CIS cluster nodes network to be used as a secondary container cluster external network; this secondary container cluster external network has connectivity, and it can be routed/forwarded by the NFVI-PoP network gateway in site#2.
Step #4	NFVO->CISM	The NFVO requests the CISM of CIS cluster#3 to create the necessary network attachment definition resources and associate them to the secondary container cluster external networks created in the step #3.
Step #5	NFVO->VNFM	The NFVO requests the VNFM to instantiate the hybrid VNF#4. The NFVO provides via the external VL information references to the externally managed VL and to the network attachment definition resources for the VNFM to make use of the instantiated networks for the internal and external connectivity. See note 4.
Step #6	NFVO->VIM	For the instantiation of the NS VL#1, the NFVO requests the VIM managing resources in the site#1 to create a virtualised network able to interconnect VMs to be deployed on the virtualised infrastructure; this virtualised network has connectivity, and it can be routed/forwarded by the NFVI-PoP network gateway in site#1.
Step #7	NFVO->VIM	For the instantiation of the NS VL#3, the NFVO requests the VIM managing resources in the site#1 to create a virtualised network to be associated to an infrastructure network in the NFVI. This infrastructure network provides connectivity to the PNF#1 and external connectivity to the CIS cluster#1 (possibly with some load balancing network device).
Step #8	NFVO->VIM	For the instantiation of the NS VL#2, the NFVO requests the VIM managing resources in the site#1 to create a virtualised network able to interconnect VMs conforming the CIS cluster#2 with other VMs that can be instantiate on the virtualised infrastructure (for creating VM-based VNFC).
Step #9	NFVO->CCM	For the instantiation of the NS VL#2, in addition, the NFVO requests the CCM to create a CIS cluster nodes network to be used as a secondary container cluster external network with connectivity to the virtual network created in the step #8. As part of the instantiation of the NS VL#3, the NFVO requests the CCM to create a CIS cluster nodes network to be used as a secondary container cluster external network with connectivity towards, at least one, infrastructure network in the NFVI of site#1.

#	Actor/Role	Action/Description
Step #10	NFVO->CISM	The NFVO requests the CISM of CIS cluster#2 to create the necessary network attachment definition resources and associate them to the secondary container cluster external networks created in the step #9.
Step #11	NFVO->VNFM	The NFVO requests the VNFM to instantiate VNF#3. The NFVO provides the necessary external VL information to connect to NS VL#1 and NS VL#2.
Step #12	NFVO->VNFM	The NFVO requests the VNFM to instantiate VNF#2. The NFVO provides via the external VL information references to the network attachment definition resources for the VNFM to make use of the instantiated networks for external connectivity of the VNFs.
Step #13	NFVO->VNFM	The NFVO requests the VNFM to instantiate VNF#1. The NFVO provides via the external VL information references to the L3 network configuration for the Virtual CP to be instantiated; such configuration enables the connectivity to the infrastructure network created in step 7.
Ends when	NFVO	The NFVO completes the NS instantiation after all NS constituents have been instantiated and connected.
NOTE 1: VNF and CIS cluster LCM granting procedures are not illustrated. NOTE 2: For simplicity in the use case description, no VNF internal VLs are derived for deploying VNF#1, VNF#2 and VNF#3, as these cases are already supported by referenced ETSI NFV specifications. NOTE 3: For the creation of the CIS cluster nodes network, the CCM would further interact with infrastructure managers (including VIM) to create the corresponding virtualised networks in the NFVI. This case is applicable to multiple steps, and it is not represented as a specific step to simplify the use case flow. NOTE 4: For the instantiation of the VNF instances, the VNFM further interacts with VIM and CISM to instantiate the virtualised resources and containerized workloads for the VNFs, respectively. These steps are not represented, for simplicity, in the use case flow. NOTE 5: Response steps are not described in order to simplify the use case flows. NOTE 6: Several steps in the use case flow can be performed in parallel.		

6 NFV support for enhanced container networking

6.1 Overview

Clause 6.2 documents various potential solutions related to enhanced network connectivity for container-based VNFs, including solutions to add additional secondary container cluster network, to delete a secondary container cluster network, or to pre-configure secondary container cluster networks, etc. Clause 6.2 also documents solutions to cover aspects of connectivity for hybrid VM/container-based VNFs.

Subsequently, clause 6.3 further elaborates on the potential architectural enhancements, including enhancements related to NFV descriptors and other artifacts, enhancements related to NFV-MANO functional aspects and enhancements related to NFV-MANO interfaces.

6.2 Potential solutions

6.2.1 Solution for adding additional secondary container cluster network

6.2.1.1 General description

When an NS instance already exists and there is a need to update it, the network operator, via the OSS/BSS, can initiate an NS update operation. The network operator might want to update the existing multiple networks in support of the NS instance, e.g. by adding additional secondary container cluster networks. The operation of NS update can be used for updating the existing created multiple networks. The operation of updating multiple networks includes adding one or more secondary container cluster networks for multiple networks, deleting one or more secondary container cluster networks for multiple networks and modifying network connectivity for multiple networks which has already been described in clause 5.1.4 of ETSI GR NFV-IFA 038 [i.2].

6.2.1.2 Pre-requisite

Following are the pre-requisites to trigger the adding additional secondary container cluster network:

- The manifest (e.g. SNCP) is updated, in which the network attributes of secondary container cluster internal/external networks are changed (e.g. the network attributes of a new secondary container cluster network is added).
- The information in the NSD includes the attributes of a new external VL which is mapping to a new secondary container cluster network, and the attributes of an external CP of the VNF instance connected to this new external VL.
- The NSD file structure including the updated NSD and the updated artifacts (e.g. SNCPs) is successfully on-boarded.

6.2.1.3 Procedure

The procedure for adding additional secondary container cluster network is used for extending external network connectivity between container-based VNF instances inside a NS instance, which is described as it follows.

For the operation of updating multiple networks to add a new secondary container cluster network, the network operator, via the OSS/BSS invokes the Update NS operation with the update information by using the NS LCM interface over the Os-Ma-nfvo reference point. The information includes the attributes of a new external VL which is mapping to a new secondary container cluster network, and the attributes of an external CP of the VNF instance connected to this new external VL.

The NFVO analyses the request message received from the OSS/BSS, and determines that it needs to add a new external virtual link connected to the existing VNF instance, or connected to the new VNF instance, if a new VNF is also determined to be instantiated. Then the NFVO decides to re-configure the multiple networks to add a new secondary container cluster network.

For creating a new NS VL instance, the NFVO can inject the specific attributes of the new external VL described in the NSD into the CISM to update the respective multiple networks configuration profiles of the secondary container cluster internal/external network. If new secondary container cluster networks are necessary, first the NFVO requests the CCM to create the CIS cluster nodes networks, which realize the secondary container cluster internal/external networks. The CISM will create the network attachment definition resources enabling the connectivity to the new secondary container cluster network.

After the secondary container cluster internal/external networks re-configured successfully by the CISM, the NFVO will request to perform necessary VNF lifecycle management operations to the VNFM specified in ETSI GS NFV-IFA 007 [i.6]. For example the NFVO requests the instantiate VNF operation in case that new container-based VNF instances need to be added into the NS instance to connect to the new secondary container cluster network, or the NFVO requests to change external VNF connectivity to add a new external CP of the existing VNF instance which is used to connect with the new secondary container cluster network. The VNFM performs the operation to associate the external CP of the VNF instance and connect to the new external VL.

The VNFM can inject specific references attributes of network attachment definition resources for the secondary container cluster network associated with the new VNF external VL to the CISM and indicate the respective SNCP(s).

The CISM re-populates annotations' placeholder of the declarative descriptor of MCIO with information about network attachment definition resources to update the existing secondary container cluster internal/external networks.

During the process of the VNF lifecycle management operation for container-based VNFs, according to the MCIO declarative descriptor, when the MCIO is created, the CNI™ Plugin connects the network interface of the group of one or more OS container to the new secondary container cluster internal/external network. The updating operation of secondary container cluster internal/external networks is completed when all the connect points of VNF instances have connected to the updated secondary container cluster internal/external networks.

6.2.2 Solution for deleting a secondary container cluster network

6.2.2.1 General description

Same description as in clause 6.2.2.1 applies for the present proposed solution.

6.2.2.2 Pre-requisite

Following are the pre-requisites to trigger the deletion of a secondary container cluster network:

- The manifest (e.g. SNCP) is updated, in which the network attributes of secondary container cluster internal/external networks are changed (e.g. the network attributes of an existing secondary container cluster network is deleted).

6.2.2.3 Procedure

The procedure for deleting a secondary container cluster network is used for changing external network connectivity between container-based VNF instances inside a NS instance, which is described as it follows.

For the operation of updating multiple networks to delete an existing secondary container cluster network, the network operator, via the OSS/BSS, invokes the Update NS operation with the update information by using the NS LCM interface over the Os-Ma-nfvo reference point. The information includes which existing external VL and which external CP of the VNF instances are to be removed.

The NFVO analyses the request message received from the OSS/BSS, and determines that it needs to delete an existing external VL connected to the VNF instance. Then the NFVO decides to re-configure the multiple networks to remove a secondary container cluster network associated to the external VL to be deleted.

For deleting unnecessary network connections, the NFVO requests the VNFM to perform some necessary VNF lifecycle management operations specified in ETSI GS NFV-IFA 007 [i.6]. For example, the NFVO requests the change external VNF connectivity operation to disconnect the external CP that is connected to a particular external VL. The VNFM performs the operation to disconnect the external CP of the VNF instance connected to the existing external VL as requested. Meanwhile, the VNFM can also perform lifecycle management of the VNFC instances that were connected to the external VL, and if the VNFC instances are no longer needed, to terminate the associated containerized workloads. In this case, during the process of the VNF lifecycle management operation for container-based VNFs, according to the MCIO declarative descriptor, the VNFM can request the CISM to terminate the unnecessary MCIO (e.g. a group of one or more OS container), and the CNI™ Plugin disconnects the network interface of the group of one or more OS container to the secondary container cluster network which needs to be deleted.

If no VNF external CPs are connected to the existing NS VL, and depending on operational policies, the NFVO can perform the operation of deleting NS virtual link. This can be considered when no network interface of the group of one or more OS container keep a connection with the existing secondary container cluster network. In such a case, the CCM performs, based on the request from the NFVO, the operation of deleting the CIS cluster nodes network realizing the secondary container cluster network that is no longer used.

6.2.3 Solution for pre-configuring secondary container cluster networks

6.2.3.1 General description

The secondary container cluster internal/external networks can be created dynamically. When the NFVO performs the NS lifecycle management operation, the NFVO requests the CCM to configure the CIS cluster nodes networks that realize such secondary container cluster networks. The detailed solution is achieved in ETSI GR NFV-IFA 038 [i.2]. Meanwhile, there is another way that the secondary container cluster internal/external networks can be created, and that is pre-configured by the CCM (e.g. created at the time when the CIS cluster is created). In such a scenario, the NFV-MANO can use the already created secondary container cluster internal/external networks as internal VLs for a VNF instance and/or VLs for the NS instance when the NFVO performs the NS lifecycle management.

6.2.3.2 Pre-requisite

The NFVO has the capability to trigger the CCM to pre-configure the secondary container cluster internal/external networks in a CIS cluster.

The network plugins/plugin control executables have been installed by the CCM into the CIS cluster.

6.2.3.3 Procedure

The procedure for pre-configuring secondary container cluster network is described as it follows.

The NFVO uploads the manifest configuration files (e.g. SNCP) to the CCM. Then the NFVO requests the CCM to perform the operation of pre-configuring CIS cluster networks that realize the secondary container cluster networks based on the manifest configuration files and the operator policies.

The CCM performs the operation on the indicated CIS cluster. As specified in ETSI GS NFV-IFA 036 [i.4], the CCM requests the CISM to install the network configuration for the secondary container cluster networks via the manifest configuration files. The CISM performs the creation of the network attachment definition resources for the secondary container cluster networks.

The CISM returns the information regarding the created network attachment definition resources to the CCM. The CCM returns the information of the pre-configured CIS cluster nodes networks to the NFVO.

In order to proceed with the NS instantiation with container-based VNFs, the OSS/BSS sends to the NFVO an "InstantiateNsRequest" to trigger the NS instantiation operation. Based on the NS VL connectivity requirements expressed in the NSD (e.g. with additional secondary container cluster internal/external network associated properties), and the information of the created secondary container cluster internal/external networks which have been pre-configured by the CCM successfully, the NFVO performs the operation to associate the necessary VLs described in VLD with the created the secondary container cluster internal/external networks, which can be regarded as the creation operation of the NS VLs.

The NFVO requests the instantiation of the VNF and includes references to the previously network attachment definition resource(s). The VNFM injects specific references attributes of network attachment definition resources to the CISM.

The CISM populates annotations' placeholder of the declarative descriptor of MCIO with information about the network attachment definition resources used to connect to the secondary container cluster external networks.

During the process of the VNF instantiation operation for container-based VNFs, according to the MCIO declarative descriptor, when the MCIO is created, the CNI™ Plugin connects the network interface of the group of one or more OS container to the secondary container cluster external networks.

6.2.4 Solution for mapping NS and VNF VL abstractions, primary/secondary container cluster networks, and CIS cluster nodes networks

6.2.4.1 General description

The present solution aims at addressing the following key issue identified from the use case "on connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters" introduced in clause 5.4.

Key issue: For NFV-MANO to process the connectivity requirements between VNF and constituents in VNFs, it makes use of the VNFD and the runtime information. The referenced specifications potentially lack expressiveness regarding how to map between the NS and VNF VL abstractions and the primary/secondary container cluster networks, and between the primary/secondary container cluster networks and the CIS cluster nodes networks.

6.2.4.2 Background

ETSI NFV-MANO specifications provide means to map between the NS and VNF VL abstractions and the underlying network resources realizing such VL. For instance, ETSI GS NFV-IFA 007 [i.6] specifies the "ExtManagedVirtualLinkInfo"; the information element defines an attribute "networkResource" of content type "ResourceHandle". The resource handle has a reference to the virtual network resource or network MCIO that is provided by the infrastructure management function (VIM or CISM, respectively). This provides a way to map between the VL level abstraction and the underlying network resource realization.

Also, according to the protocol and data model of CISM API specified in ETSI GS NFV-SOL 018 [i.3], the "resourceId" in the ResourceHandle is mapped to the "k8s.cni.cnf.io/networks" field, which indicates a list of identifiers of Network Attachment Definitions (NADs) representing secondary container cluster external networks which are attached to the group of one or more OS containers (i.e. a Pod) through respective interfaces. The "ExtVirtualLinkInfo" data type specified in clause 5.5.3.2 of ETSI GS NFV-SOL 003 [i.7] includes the attribute "extNetAttDefResource", which corresponds to the network attachment definition resources that provide the specification of the interface to attach connection points to this VL.

6.2.4.3 Solution description

The solution considers how to map the different abstractions and resources for both primary and secondary container cluster networks.

Primary container cluster networks:

When the NS VL corresponds to a primary container cluster network, the runtime information contains:

- The VL runtime information contains a resource handle that references the network resource, a virtual network resource in the case of VM-based CIS cluster, or an infrastructure provider network resource (physical network) in case of a bare-metal CIS cluster. In the case of hybrid CIS cluster, the resource handle references the virtual network resource, which in turn is mapped by the VIM to a corresponding infrastructure provider network that connects the bare-metal CIS cluster nodes.

- The CIS cluster nodes network runtime information maintained by the CCM contains a resource handle that references the same information indicated in the previous listed item.

- The NFVO maps the VL runtime information to the CIS cluster nodes network runtime information by using additional attributes in the VL runtime information objects.

Secondary container cluster networks:

When the NS/VNF VL corresponds to a secondary container cluster network, the runtime information contains:

- The VL runtime information contains a resource handle that references the network resource, a virtual network resource in the case of VM-based CIS cluster, or an infrastructure provider network resource (physical network) in case of a bare-metal CIS cluster. In the case of hybrid CIS cluster, the resource handle references the virtual network resource, which in turn is mapped by the VIM to a corresponding infrastructure provider network that connects the bare-metal CIS cluster nodes.

- The CIS cluster nodes network runtime information maintained by the CCM contains a resource handle that references the same information indicated in the previous listed item.

- The VL runtime information contains information of network attachment definition resources providing the specification of interfaces to attach connections points to the VL.

- The NFVO maps the VL runtime information to the CIS cluster nodes network runtime information by using additional attributes in the VL runtime information objects.

Currently, secondary container cluster networks for a VNF are only modelled by the "ExtManagedVirtualLinkInfo", and not by "VnfVirtualLinkResourceInfo".

Figure 6.2.4.3-1 illustrates a possible extension to the "ResourceHandle" (in red) to map to information available at the CIS cluster level, enabling the NFVO to map the VL runtime information to the CIS cluster nodes network.

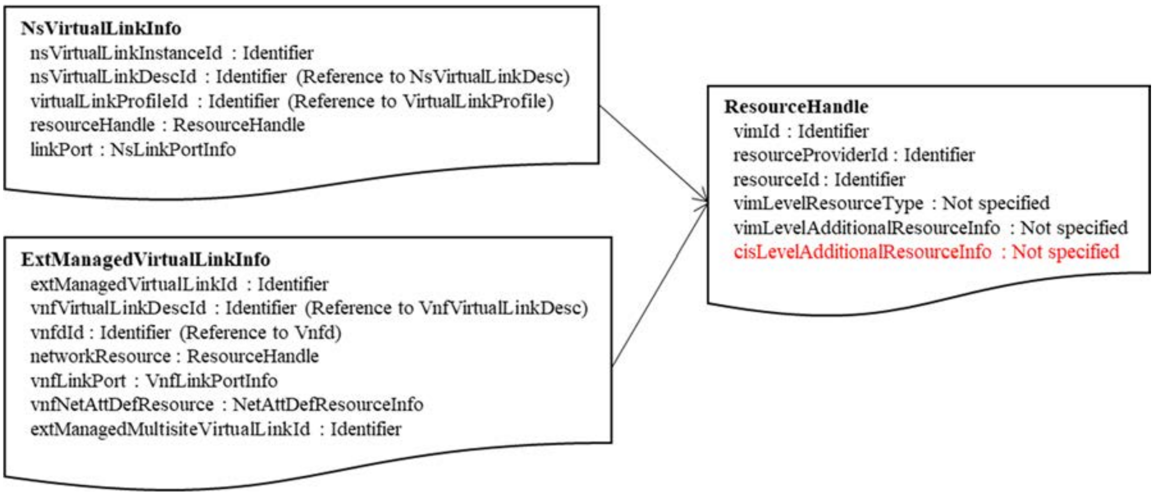
NsVirtualLinkInfo
nsVirtualLinkInstanceId : Identifier
nsVirtualLinkDescId : Identifier (Reference to NsVirtualLinkDesc)
virtualLinkProfileId : Identifier (Reference to VirtualLinkProfile)
resourceHandle : ResourceHandle
linkPort : NsLinkPortInfo
ExtManagedVirtualLinkInfo
extManagedVirtualLinkId : Identifier
vnfVirtualLinkDescId : Identifier (Reference to VnfVirtualLinkDesc)
vnfdId : Identifier (Reference to Vnfd)
networkResource : ResourceHandle
vnfLinkPort : VnfLinkPortInfo
vnfNetAttDefResource : NetAttDefResourceInfo
extManagedMultisiteVirtualLinkId : Identifier
ResourceHandle
vimId : Identifier
resourceProviderId : Identifier
resourceId : Identifier
vimLevelResourceType : Not specified
vimLevelAdditionalResourceInfo : Not specified
cisLevelAdditionalResourceInfo : Not specified

Figure 6.2.4.3-1: Example of extending the resource handles to map information at the CIS level

6.2.5 Solution for interworking between VM-based and bare-metal CIS clusters with NFV-MANO

6.2.5.1 General description

The present solution aims at addressing the following key issue identified from the use case "on connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters" introduced in clause 5.4.

Key issue: When connectivity is expected to be enabled between VM-based and bare-metal CIS clusters, different kinds of network interfaces are involved at the CIS cluster infrastructure level. Which information and how NFV-MANO can determine that there is connectivity or there can be connectivity enabled between the two kinds of CIS clusters?

6.2.5.2 Background

As specified in clause 4.2.6.2 of ETSI GS NFV-IFA 036 [i.4], a CIS cluster can be hybrid (i.e. based on bare-metal and VM) and the connectivity between the CIS cluster nodes in this case can be performed with L2/L3 infrastructure provider networks, which enable VMs to connect to existing L2/L3 networks in the infrastructure supporting the bare-metal CIS cluster nodes.

6.2.5.3 Solution description

The solution is based on the following principles:

- CIS cluster nodes networks for respective CIS clusters are not shared to maintain proper network isolation between the CIS clusters, e.g. a CIS cluster nodes network for a VM-based CIS cluster uses a virtualised network mapped (or realized) by an infrastructure provider network, and the CIS cluster nodes network for the bare-metal CIS cluster is realized by another infrastructure provider network.

In this case, a forwarding/routing network device provides the connectivity between the two CIS cluster nodes networks.

The solution considers that the following information is maintained:

- information about the infrastructure provider networks that are established in the NFVI-PoP;
- information about which infrastructure provider networks the NFVI nodes are connected and through which network interfaces;
- information about the capability in the NFVI-PoP of forwarding/routing traffic between the infrastructure provider networks; and

- information about which vNICs of the virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks.

Table 6.2.5.3-1 provides different sub-solutions regarding the entities that maintain and expose such information.

Table 6.2.5.3-1: Sub-solutions

Information	Who maintains and provides the information	
	Sub-solution A	Sub-solution B
Information about the infrastructure provider networks that are established in the NFVI-PoP.	VIM	PIM
Information about to which infrastructure provider networks the NFVI nodes are connected and through which network interfaces	VIM	PIM
Information about the capability in the NFVI-PoP of forwarding/routing traffic between the infrastructure provider networks	VIM	PIM
Information about which the vNICs of the virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks	VIM	VIM

Exposing such sets of information is expected, since the consumer determines, when requesting to the CCM to create a CIS cluster nodes network, the reference to the infrastructure provider network to be used for the CIS cluster nodes network.

6.2.6 Solution of networking for a hybrid VNF

6.2.6.1 General description

The present solution aims at addressing the following key issue identified from the use case "on connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters" introduced in clause 5.4.

Key issue: When a VNF is realized by both VM-based as well as container-based VNFC, information about the mapping of internal VL information of a VNF to virtualised network resources and primary/secondary container cluster networks is not provided according to the referenced specifications.

6.2.6.2 Background

ETSI NFV-MANO specifications provide means for defining the internal VLs of a VNF, i.e. VLs for the internal (within the VNF) connectivity of VNFC. In particular, at the runtime level, ETSI GS NFV-IFA 007 [i.6] and ETSI GS NFV-IFA 008 [i.8] relevant runtime information element such as "VnfVirtualLinkResourceInfo", "ExtVirtualLinkInfo", "VnfLinkPortInfo", "ExtLinkPortInfo", "VnfcResourceInfo", "VnfCpInfo", "VnfExtCpInfo", "VirtualCpInfo" and "NetAttDefResourceInfo".

In the case of a VNF only based on VM technology, i.e. all its VNFCs are VM-based, if there are multiple VNFC instances to connect, and these need internal VNF connectivity, they can be connected to one or more VNF internal VL. The connectivity of the VNFC CPs is performed via the VNF link ports. When a VNF exposes an external CP, then, the typical mechanism is to connect the VNFC CP exposed as an external CP directly to an external VL via an external link port.

In the case of a VNF only based on container technology, i.e. all its VNFCs are based on groups of one or more OS containers (e.g. a Pod in the case of Kubernetes®), the network connectivity varies as follows:

- All VNFC instances are connected by default to a primary container cluster network. VNFC CPs carry information about the L2/L3 of connectivity to such a network. However, as specified by ETSI GS NFV-IFA 011 [i.9], clause 7.1.6.4.2, "VduCpd" corresponding to CP connecting to the primary container cluster network, the reference to a "VnfVirtualLinkDesc" for realizing a VNF internal VL need not be presented, and in clause 7.1.6.2.2, providing connectivity requirements for VNFC CP via "VduCpd" is not needed in the case of connecting only to the primary container cluster network.

- For VNFC instances that, in addition to the primary container cluster network, are connected to a secondary container cluster network, "VduCpd" are provided to indicate the requirements of connectivity to this additional network. At runtime, the representation of connectivity to the secondary container cluster networks is performed via the network attachment definition resources. As specified in ETSI GS NFV-IFA 008 [i.8], a VNFC CP (whose runtime information is provided by the "VnfcCpInfo" information element), references a "NetAttDefResourceInfo", which in turn references to a resource handle for the resource in scope of the CISM. As specified by ETSI GS NFV-IFA 007 [i.6] and ETSI GS NFV-IFA 008 [i.8], in the case of secondary container cluster networks, the internal VLs are modelled as externally-managed VL, that is, necessary mapping information between the VL and the network attachment definition resources are present in the "ExtManagedVirtualLinkInfo".

In the case of a hybrid VNF, where some of the VNFC are based on VM technology, and other VNFCs are based on OS containers and there is a need to interconnect both types of VNFCs through common networks, the current design-time and runtime modelling is not precise to indicate the scope of the VNF internal VL, and the relationship of the VNF internal VL with the network attachment definition resources.

6.2.6.3 Solution description

The solution considers how to map the different abstractions and resources for both primary and secondary container cluster networks, and in the case of hybrid VNFs where VM-based and container-based VNFC instances share common network connectivity.

Figure 6.2.6.3-1 illustrates an example of this case and solution.

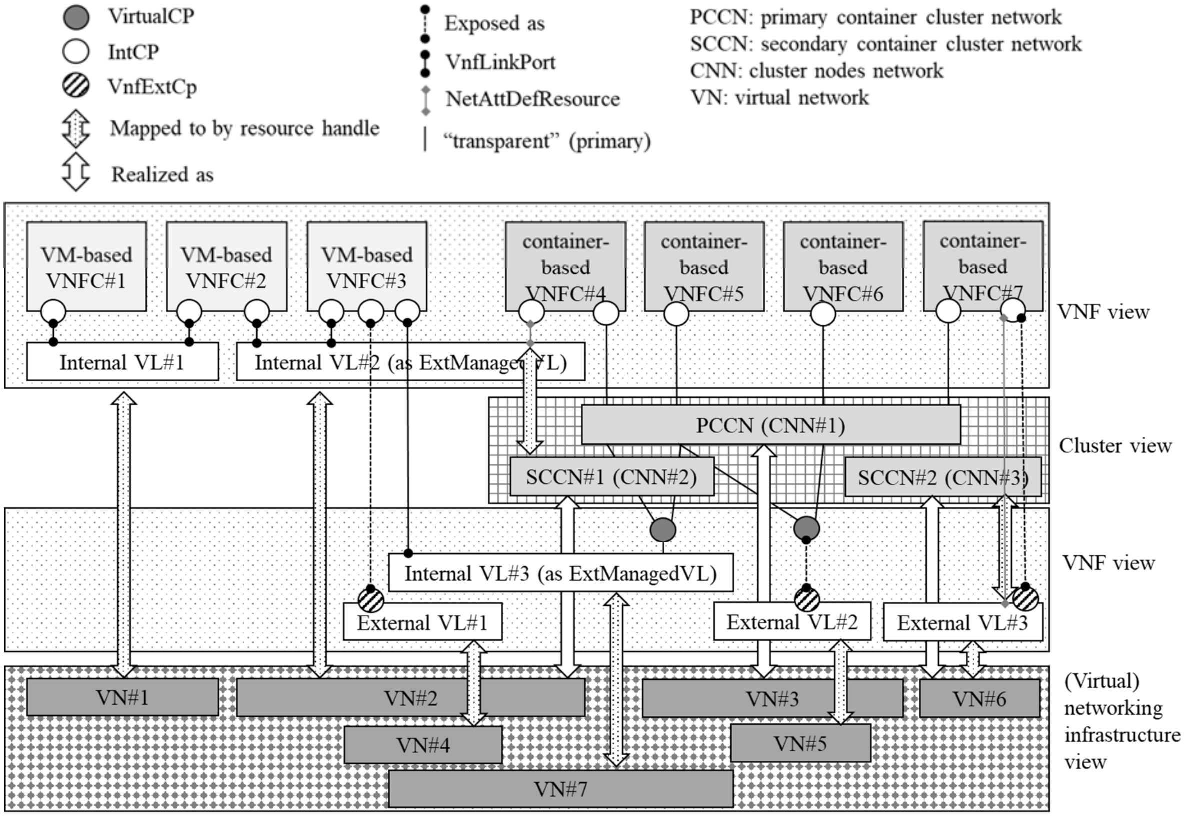

Figure 6.2.6.3-1: Example of networking in a hybrid VNF

Views:

Figure 6.2.6.3-1 represents three different views:

- VNF view: it represents the abstraction view at the VNF level, as provided by the VNFM;
- Cluster view: it represents the abstraction view at the cluster level concerning the networking part, as provided by the CCM and CISM; and

- (Virtual) networking infrastructure view: it represents the network infrastructure view, as provided by the VIM or other infrastructure managers.

VL and container cluster network realizations:

In the example of figure 6.2.6.3-1, internal and external VLs are realized as follows:

- Internal VL#1: the VL is realized by a virtual network, VN#1. The VL object maps 1:1 to the underlying virtual network resource via a corresponding resource handle.
- Internal VL#2: see "Hybrid networking" below.
- Internal VL#3: see "Hybrid networking" below.
- External VL#1: the VL is realized by a virtual network, VN#4. The VL object maps 1:1 to the underlying virtual network resource via a corresponding resource handle.
- External VL#2: the VL is realized by a virtual network, VN#5. The VL object maps 1:1 to the underlying virtual network resource via a corresponding resource handle.
- External VL#3: the VL is realized by a virtual network, VN#6. The VL object maps 1:1 to the underlying virtual network resource via a corresponding resource handle.
- Primary Container Cluster Network (PCCN): it is mapped to a CIS cluster nodes network (CNN) #1. The network is realized by a virtual network, VN#3.
- Secondary Container Cluster Network (SCCN) #1: see "Hybrid networking" below.
- SCCN#2: it is mapped to a CCN#3. The network is realized by the virtual network VN#6, which in turn realizes the External VL#3.

Hybrid networking: The internal VL#2 which connects VM-based and container-based VNFC instances needs to be capable to express the connectivity offered to both types of VNFCs. The VL is realized by a virtual network, VN#2. At the same time, the SCCN#1 is also realized by the VN#2. To represent this duality, the ExtManagedVirtualLinkInfo refers to links ports and to network attachment definition resources. The "networkResource" resource handle of the VL maps to the underlying virtual network, VN#2.

The internal VL#3 which connects also VM-based and container-based VNFC instances, in the latter case via a Virtual CP, needs to also be capable to express the connectivity offered to both types of VNFCs. The VL is also realized by a virtual network, VN#7. The ExtManagedVirtualLinkInfo is capable of referring, either directly or indirectly, to a port offering the external connectivity of the Virtual CP outside the PCCN. The "networkResource" resource handle of the VL maps to the underlying virtual network, VN#7.

6.2.7 Solution for NFV-MANO responsibilities of networking in scenarios of mixed VM-based and container-based deployments

6.2.7.1 General description

The present solution aims at addressing the following key issue identified from the use case "on connectivity for hybrid VM/container-based VNF deployments on multiple CIS clusters" introduced in clause 5.4.

Key issue: In the scenario of having a mix of VM-based vs. container-based deployment, virtualised network resources, as well as container cluster networks are involved. Referenced specifications do not clearly describe the responsibilities and roles of the set of NFV-MANO functional blocks/functions in the management of the respective networks. For instance, if a virtualised network is to be reused for both connectivity of VM-based VNFCs as well as VM-based CIS cluster nodes, would the NFVO request the creation of the whole network, or would some steps be delegated to the CCM when creating the CIS cluster nodes network?

6.2.7.2 Background

According to ETSI GS NFV-IFA 036 [i.4], the CCM is responsible for provisioning the CIS cluster nodes networks. Based on the request, the CCM requests the infrastructure managers (e.g. VIM) the creation and/or setup of the network resources that realize the CIS cluster nodes network. More information is available in clause 4.2.6.2 of ETSI GS NFV-IFA 036 [i.4]. Furthermore, the CCM does not have visibility at the VNF-level, only at the CIS cluster level; hence, the CCM cannot determine whether a VNF is being realized fully as container-based, or hybrid.

The NFV-MANO supports the delegation of virtualised networks management between some of its functional blocks and functions. For instance, the NFVO can request the creation of virtualised networks for a VNF. The information of the already created virtualised networks can be provided to the VNFM, when such virtualised networks are to be used as VNF internal VL. In this case, the VNFM does not interact with the VIM to request the creation of the network, since the network has already been created. This feature is specified in the NFV-MANO framework as "externally managed VL".

6.2.7.3 Solution description

The solution considers defining the responsibilities and mechanisms of creating virtualised networks to be used for the connectivity in case of VM-based and container-based deployments.

In order to avoid potential conflicts in terms of management of the virtualised networks in those cases, different sub-options can be considered:

- Option A: a single entity is responsible for setting up the virtualised network that is being used in the hybrid VM-based and container-based deployment scenario.
- Option B: use multiple virtualised networks setting a boundary of interconnectivity between them.

Option A:

This option considers that connectivity for the mixed scenario can be realized by a single virtualised network. In such a case, there is no need to set up additional interconnectivity devices (e.g. routers).

In this option, as the NFVO has a global view of the network requirements in mixed scenarios by processing the NS/VNF LCM requests as well as the corresponding NSD/VNFDs, it is responsible for setting up the network resources by requesting the infrastructure managers (e.g. VIM for a case of virtualised networks). This virtualised network provides both connectivity to CIS cluster nodes, where containerized workloads can be deployed, as well as to VM that can potentially be created within the NFVI. The NFVO interacts with the CCM for setting up the CIS cluster, including its CIS cluster nodes networks, but provides to the CCM information about the already created virtualised networks.

NOTE: This is similar concept to the externally-managed VL.

Further, the NFVO, when applicable, can also provide references to the virtualised networks to be used by a VNF in a hybrid scenario by using the feature of externally-managed VLs.

In summary, in this option, the NFVO has full responsibility of setting up the virtualised networks which are used for the hybrid scenario.

Taking as an example the illustration in figure 6.2.7.3-1, the VN#3 would be setup completely by the NFVO and its information be passed to the CCM when requesting to setup the CIS cluster nodes network CNN#2 for the secondary container cluster network #1.

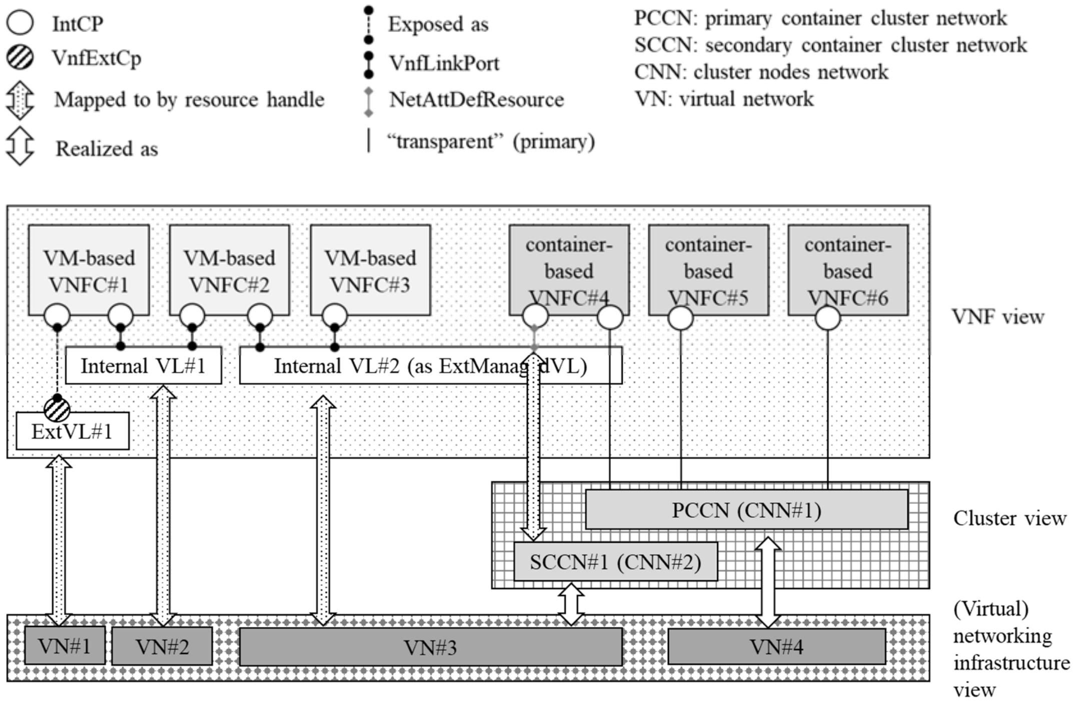

Figure 6.2.7.3-1: Example of networking in a hybrid VNF with single virtual network

Option B:

In this option, virtualised networks are provisioned to match the boundaries of the VM-based deployment and container-based deployment parts.

For the virtualised network to be used as CIS cluster nodes network and correspondingly for interconnecting container-based VNFC, the CCM is responsible for setting it up by requesting the corresponding infrastructure manager.

For the virtualised network to be used to interconnect VM-based VNFC, the NFVO is responsible for it by requesting also to the corresponding infrastructure manager. In this case, the NFVO needs to consider setting up the virtualised network with the capability to interconnect to the other virtualised network used for the CIS cluster.

Taking as an example the illustration in figure 6.2.7.3-2, the VN#4 would be set up by the CCM and the VN#3 would be set up by the NFVO. The NFVO needs to request setting up the VN#3 indicating that the network needs to be interconnected to VN#4.

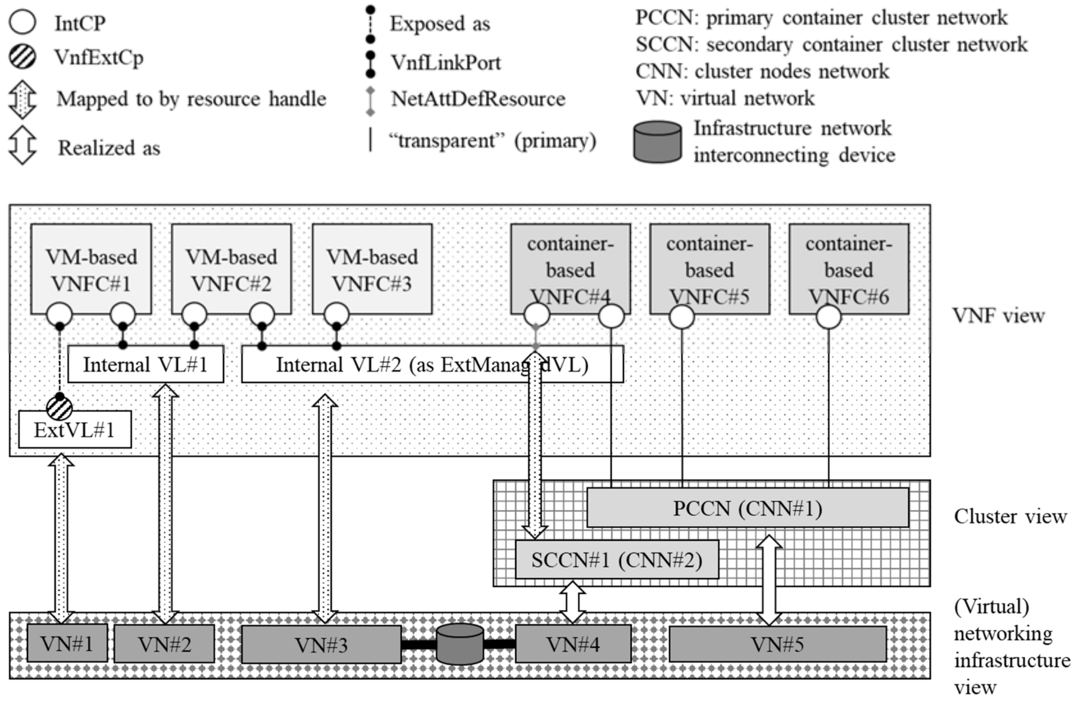

Figure 6.2.7.3-2: Example of networking in a hybrid VNF with multiple virtual networks

6.3 Potential architectural enhancements

6.3.1 Enhancements related to NFV descriptors and other artifacts

All solutions described in clause 6.2 have no impacts on NFV descriptors and other artifacts.

NOTE: There are no additional enhancements beyond recommendations from ETSI GR NFV-IFA 038 [i.2].

6.3.2 Enhancements related to NFV-MANO functional aspects

As documented in clause 6.2.4, there is a lack of expressiveness regarding how to map between the NS and VNF VL abstractions and the primary/secondary container cluster networks, and between the primary/secondary container cluster networks and the CIS cluster nodes networks. As suggested by the solution description in clause 6.2.4.3, the following enhancements are derived related to NFV-MANO functional aspects:

- For the case of primary and secondary container cluster networks:
    - Enh632.001: The NFVO is expected to be capable of mapping the runtime information of VL to the CIS cluster nodes network.

As documented in clause 6.2.5, there is lack of information about how NFV-MANO can determine that there is connectivity between VM-based and bare-metal CIS cluster. As suggested by the solution description in clause 6.2.5.3, the following enhancements are derived related to NFV-MANO functional aspects:

- Enh632.002: The NFV-MANO framework is expected to support that CIS cluster nodes networks of VM-based and bare-metal CIS clusters are not shared to maintain network isolation, and that connectivity between is performed via forwarding/routing network devices available in the NFVI.

- Enh632.003: The PIM is expected to be capable of holding information about infrastructure provider networks, the NFVI nodes that are connected to these infrastructure provider networks, and information about the forwarding/routing capabilities in the NFVI-PoP between infrastructure provider networks.

- Enh632.004: The VIM is expected to be capable of holding information about which vNICs of virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks.

As documented in clause 6.2.6, there is lack of information about the connectivity when a VNF is realized by both VM-based and container-based VNFC, about how the internal VL information maps to virtualised network resources and primary/secondary container cluster networks. As suggested by the solution description in clause 6.2.5.3, the following enhancements are derived related to NFV-MANO functional aspects:

- Enh632.005: The NFVO is expected to be capable of determining when a virtual network resource is to be used to realize an internal VL that connects both VM-based and container-based VNFC instances of a VNF instance.

As documented in clause 6.2.7, the responsibility between NFVO and CCM for virtual network resources to be reused for both VM-based VNFC and well as VM-based CIS cluster nodes is unclear. As suggested by the solution description in clause 6.2.7.3, the following enhancements are derived related to NFV-MANO functional aspects:

- For the case that no strict isolation requirements are to be considered regarding the networking of CIS clusters vs. other components in the NFVI:
    - Enh632.006: The NFVO is expected to take responsibility of setting up the virtual network resource for the CIS cluster nodes network serving as secondary container cluster network, which is used also as virtual network for the VL connecting VM-based VNFC.
    - Enh632.007: The CCM is expected to be capable of reusing, as externally managed resource, existing virtual network resources to assign to CIS cluster nodes networks serving as secondary container cluster networks.
- For the case that stricter isolation requirements are to be considered regarding the networking of CIS clusters vs. other components in the NFVI:
    - Enh632.008: The CCM is expected to take responsibility of setting up the virtual network resource for the CIS cluster nodes network serving as secondary container cluster network.
    - Enh632.009: The VIM is expected to be capable of setting up virtual network resources that are to be explicitly connected (forwarded/routed) to other existing virtual network resources, and creating the necessary network resources enabling such a connectivity.

6.3.3 Enhancements related to NFV-MANO interfaces

As documented in clause 6.2.4, there is a lack of expressiveness regarding how to map between the NS and VNF VL abstractions and the primary/secondary container cluster networks, and between the primary/secondary container cluster networks and the CIS cluster nodes networks. As suggested by the solution description in clause 6.2.4.3, the following enhancements are derived related to NFV-MANO interfaces:

- For the case of primary and secondary container cluster networks:
    - Enh633.001: The CCM is expected to provide resource level information (via a "resource handle") to reference the virtual network resource (in case of VM-based or hybrid CIS cluster) or infrastructure provider network (in case of bare-metal CIS cluster) that realizes the CIS cluster nodes network.
- Only for the case of secondary container cluster networks:
    - Enh633.002: In case of a secondary container cluster network that realizes an NS VL, the NFVO is expected to provide information about the network attachment definition resources providing the specification of interface to attach connection points to the NS VL.

As documented in clause 6.2.5, there is lack of information about how NFV-MANO can determine that there is connectivity between VM-based and bare-metal CIS cluster. As suggested by the solution description in clause 6.2.5.3, the following enhancements are derived related to NFV-MANO interfaces:

- Enh633.003: The PIM resource management interfaces supporting to provide information about infrastructure provider networks, the NFVI nodes that are connected to these infrastructure provider networks, and information about the forwarding/routing capabilities in the NFVI-PoP between infrastructure provider networks.
- Enh633.004: The VIM is expected to provide information about which vNICs of virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks.

As documented in clause 6.2.6, there is lack of information about the connectivity when a VNF is realized by both VM-based and container-based VNFC, about how the internal VL information maps to virtualised network resources and primary/secondary container cluster networks. As suggested by the solution description in clause 6.2.5.3, the following enhancements are derived related to NFV-MANO interfaces:

- Enh633.005: The ExtManagedVirtualLinkData to enable for a single internal VL both, references to link ports enabling connectivity to VM-based VNFCs and network attachment definition resource definitions enabling the connectivity of container-based VNFCs.

- Enh633.006: The ExtManagedVirtualLinkInfo to define, unambiguously, that both link ports and network attachment definition resource can be referenced and present at the same time, to indicate that a single internal VL is providing connectivity for both VM-based and container-based VNFCs.

- Enh633.007: The ExtVirtualLinkInfo and ExtManagedVirtualLinkInfo to enable referencing load-balancing resources and relevant connectivity information (to which networks are connected) that provide the connectivity for Virtual CPs connecting to such VLs.

As documented in clause 6.2.7, the responsibility between NFVO and CCM for virtual network resources to be reused for both VM-based VNFC and well as VM-based CIS cluster nodes is unclear. As suggested by the solution description in clause 6.2.7.3, the following enhancements are derived related to NFV-MANO interface:

- For the case that no strict isolation requirements are to be considered regarding the networking of CIS clusters vs. other components in the NFVI:

  - Enh633.008: The CIS cluster lifecycle management interface is expected to support providing information, as externally managed resource, of existing virtual network resources to assign to secondary container cluster networks.

- For the case that stricter isolation requirements are to be considered regarding the networking of CIS clusters vs. other components in the NFVI:

  - Enh633.009: The Virtualised Network Resources Management Interface is expected to support providing information of virtual network resources that are to be explicitly connected (forwarded/routed) to other existing virtual network resources.

7 Recommendations for future work

7.1 Overview

The present clause 7 documents recommendations about potential enhancements, changes, or clarifications to existing ETSI NFV specifications. The recommendations are derived based on the gap analysis performed in the documentation of the potential solutions and the evaluation of solutions documented in clause 6.

The recommendations are categorized and elaborated as follows:

- architecture and framework aspects (refer to clause 7.2);

- functional aspects (refer to clause 7.3);

- descriptors and other information/data model artefacts (refer to clause 7.4);

- interfaces and associated information/data model (refer to clause 7.5); and

- other recommendations, if any (refer to clause 7.6).

Finally, clause 7.7 describes gaps identified in the present document for which no recommendations are further derived.

7.2 Recommendations related to the NFV architectural framework

The present clause provides recommendations focusing on enhancements to the NFV architectural framework, potentially by identifying potential new functions or functional blocks, and interactions among functional blocks, or identifying general functionality expected at an architecture level.

Table 7.2-1 provides the recommendations related to the NFV architectural framework.

Table 7.2-1: Recommendations related to the NFV architectural framework

Identifier	Recommendation description	Comments and/or traceability
ifa043.arch.001	It is recommended that a recommendation is specified for the NFV architectural framework to maintain network isolation between CIS cluster nodes networks of VM-based and bare-metal CIS clusters.	Refer to Enh632.002.

7.3 Recommendations related to functional aspects

The present clause provides recommendations focusing on functional aspects of the functional blocks of the NFV architectural framework identifying specific new or extended functionality of the NFV architectural framework functional blocks and functions.

Table 7.3-1 provides the recommendations related to functional aspects.

Table 7.3-1: Recommendations related to functional aspects

Identifier	Recommendation description	Comments and/or traceability
ifa043.func.001	It is recommended that a requirement be specified for the NFVO to support mapping the runtime information of VL to the CIS cluster nodes networks.	Refer to Enh632.001.
ifa043.func.002	It is recommended that a requirement be specified for the PIM to hold inventory information about infrastructure provider networks, the NFVI nodes that are connected to these networks, and information about the forwarding/routing capabilities in the NFVI-PoP between such networks.	Refer to Enh632.003.
ifa043.func.003	It is recommended that a requirement be specified for the VIM of holding information about which vNICs of virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks.	Refer to Enh632.004.
ifa043.func.004	It is recommended that a requirement be specified for the NFVO to support determining when a virtual network resource is to be used to realize an internal VL that connects both VM-based and container-based VNFC instances of a VNF instance.	Refer to Enh632.005.
ifa043.func.005	It is recommended that a requirement be specified for the NFVO to support setting up the virtual network resource for the CIS cluster nodes network serving as a secondary container cluster network, which is also to be used for the internal VL of a VNF connecting VM-based VNFC instances.	Refer to Enh632.006. This recommendation applies for the case that no strict isolation requirements are considered regarding the networking of CIS clusters vs. other components in the NFVI.
ifa043.func.006	It is recommended that a requirement be specified for the CCM to support reusing, as externally managed resource, existing virtual network resources to assign to CIS cluster nodes networks serving as secondary container cluster networks.	Refer to Enh632.007. This recommendation applies for the case that no strict isolation requirements are considered regarding the networking of CIS clusters vs. other components in the NFVI.

Identifier	Recommendation description	Comments and/or traceability
ifa043.func.007	It is recommended that further clarification be specified for the CCM to support setting up the virtual network resource for the CIS cluster nodes network serving as a secondary container cluster network.	Refer to Enh632.008. This recommendation applies for the case that stricter isolation requirements are considered regarding the networking of CIS clusters vs. other components in the NFVI.
ifa043.func.008	It is recommended that a requirement be specified for the VIM to support setting up virtual network resources to be explicitly connected to other virtual network resources and creating the necessary network resources enabling such a connectivity.	Refer to Enh632.009. This recommendation applies for the case that stricter isolation requirements are considered regarding the networking of CIS clusters vs. other components in the NFVI.

7.4 Recommendations related to NFV descriptors and other artifacts

The present clause provides recommendations focusing on NFV descriptors, packaging and other artifacts.

No recommendations are derived.

7.5 Recommendations related to interfaces and information model

The present clause provides recommendations focusing on interfaces and associated information.

Table 7.5-1 provides the recommendations related to interfaces and associated information.

Table 7.5-1: Recommendations related to interfaces and information model

Identifier	Recommendation description	Comments and/or traceability
ifa043.if.001	It is recommended that a requirement be specified for the CIS cluster lifecycle management service interface produced by the CCM to support providing resource level information to reference the virtual network resource or infrastructure provider network that realizes the CIS cluster nodes network.	Refer to Enh633.001. Resource level information can be modelled as a "resource handle", as specified in other referenced specifications. This case is applicable for CIS cluster nodes networks that serve as primary and secondary container cluster networks.
ifa043.if.002	It is recommended that a requirement be specified for the NS LCM interface produced by the NFVO to provide information about the network attachment definition resources providing the specification of interfaces to attach connections points to the NS VLs.	Refer to Enh633.002.
ifa043.if.003	It is recommended that a requirement be specified for the resource management interfaces produced by the PIM to provide information about infrastructure provider networks, the NFVI nodes that are connected to these infrastructure provider networks, and information about the forwarding/routing capabilities in the NFVI-PoP between infrastructure provider networks.	Refer to Enh633.003.

Identifier	Recommendation description	Comments and/or traceability
ifa043.if.004	It is recommended that a requirement be specified for the virtualised resource management interfaces produced by the VIM to provide information about which vNICs of virtualised compute resources (i.e. VMs) are connected to which infrastructure provider networks.	Refer to Enh633.004.
ifa043.if.005	It is recommended that a requirement be specified for the VNF lifecycle management interface produced by the VNFM to enable externally managed VL input and runtime information to reference for a single VL both link ports enabling connectivity to VM-based VNFCs and network attachment definition resources to enable the connectivity of container-based VNFC, together.	Refer to Enh633.005 and Enh633.006. Updates to the NS lifecycle management interface produced by the NFVO are expected to be also considered to align the functionality to the VNF LCM interface.
ifa043.if.006	It is recommended that a requirement be specified for the VNF lifecycle management interface produced by the VNFM to enable referencing load-balancing resources and relevant connectivity information (to which networks are connected) that provide the connectivity for Virtual CPs.	Refer to Enh633.007. Updates to the NS lifecycle management interface produced by the NFVO are expected to be also considered to align the functionality to the VNF LCM interface.
ifa043.if.007	It is recommended that a requirement be specified for the CIS cluster lifecycle management interface produced by the CCM to support providing information, as externally managed resource, of existing virtual network resources to assign to secondary container cluster networks.	Refer to Enh633.008.
ifa043.if.008	It is recommended that a requirement be specified for the Virtualised Network Resources Management Interface produced by the VIM to support providing information of virtual network resources that are to be explicitly connected (forwarded/routed) to other existing virtual network resources.	Refer to Enh633.009.

7.6 Other recommendations

The present clause provides recommendations for categories other than those documented in the previous clauses.

No other recommendations are derived.

7.7 Gaps without recommendations

The present clause lists the gaps identified in potential solutions for which recommendations are not derived.

NOTE: The purpose of the present clause is to track gaps from which normative work is not foreseen.

No gaps without recommendations are derived.

Annex A: Change history

Date	Version	Information about changes
October 2021	0.0.1	First draft, implementing contributions: • NFVIFA(21)000786r1_FEAT19_IFA043_Skeleton • NFVIFA(21)000787r1_FEAT19_IFA043_Scope
December 2021	0.0.2	Implementation of approved contributions from IFA#263 and IFA#266: • NFVIFA(21)000961r2_FEAT19_IFA043_Clause_4_1_Problem_statement • NFVIFA(21)000962r2_FEAT19_IFA043_Clause_4_2_Introduction
April 2022	0.0.3	Implementation of approved contributions from IFA#279: • NFVIFA(22)000159r4_IFA043_Clause_5_x_Use_Case_CCM_pre-configures_cluster_networ
December 2022	0.0.4	Implementation of approved contributions from IFA#313 and IFA#315: • NFVIFA(22)000897_FEAT19_IFA043_Clause_4_x_Network_policy • NFVIFA(22)000898r4_FEAT19_IFA043_Clause_5_x_Use_Case_re-configure_secondary_con
June 2023	0.1.0	Implementation of approved contributions from IFA#332 and IFA#337: • NFVIFA(23)000291r1_FEAT19a_IFA043_Clause_5_2_5_Editor_s_note_resolution • NFVIFA(23)000283r3_FEAT19a_IFA043_Clause_6_2_x_Solution_for_adding_adding_addit • NFVIFA(23)000284r3_FEAT19a_IFA043_Clause_6_2_x_Solution_for_CCM_pre-configuring • NFVIFA(23)000436r3_FEAT19a_IFA043_Clause_6_2_y_Solution_for_deleting_a_secondar • NFVIFA(23)000450r1_FEAT19a_IFA043_Adding_use_case_about_hybrid_deployments
September 2023	0.2.0	Implementation of approved contributions from IFA#350: • NFVIFA(23)000649r1_FEAT19a_IFA043_Remove_redundant_automation_contents • NFVIFA(23)000650r1_FEAT19a_IFA043_Clause_6_1_overview • NFVIFA(23)000651_FEAT19a_IFA043_Remove_hanging_clauses • NFVIFA(23)000652_FEAT19a_IFA043_Clause_5_1_overview • NFVIFA(23)000656r1_FEAT19a_IFA043_Clause_6_3_Skeleton_on_potential_architectura • NFVIFA(23)000657r1_FEAT19a_IFA043_Clause_6_2_Solution_for_mapping_NS_and_VNF_VL • NFVIFA(23)000658r1_FEAT19a_IFA043_Clause_6_2_Solution_for_interworking_between_ • NFVIFA(23)000662r1_FEAT19a_IFA043_Clause_6_2_Solution_of_network_for_hybrid_VNF • NFVIFA(23)000663_FEAT19a_IFA043_Clause_6_2_Solution_for_NFV-MANO_responsibili
December 2023	0.3.0	Implementation of approved contributions from IFA#362: • NFVIFA(23)000786r1_FEAT19a_IFA043_Clause_6_3_1_Enhancements_NFV_descriptors_and • NFVIFA(23)000787r1_FEAT19a_IFA043_Clause_6_3_2_Enhancements_NFV-MANO_functional • NFVIFA(23)000788r1_FEAT19a_IFA043_Clause_6_3_3_Enhancements_NFV-MANO_interfaces • NFVIFA(23)000797_FEAT19a_IFA043_Clause_6_3_Hybrid_UC_enhancements • NFVIFA(23)000805_FEAT19a_IFA043_Clause_7_Hybrid_UC_recommendations
February 2024	0.4.0	Implementation of approved contributions from IFA#368 and IFA#369: • NFVIFA(24)000069r1_FEAT19a_IFA043_Editorial_review • NFVIFA(24)000077_FEAT19a_IFA043_editorial_clean-up • NFVIFA(24)000057r1_FEAT19a_IFA043_Clause_5_2_5_Editor_s_note_resolution • NFVIFA(24)000059r3_FEAT19a_IFA043_Clause_6_2_Editor_s_note_resolution

Date	Version	Information about changes
		• NFVIFA(24)000060r1_FEAT19a_IFA043_Clause_6_3_Editor_s_note_resolution • NFVIFA(24)000061r1_FEAT19a_IFA043_Clause_7_Editor_s_note_resolution • NFVIFA(24)000073r1_FEAT19a_IFA043_Multiple_clauses_Technical_review Rapporteur actions: • Decapitalize "During" in NFVIFA(24)000073r1.
May 2024	5.1.1	First published version.

History

Document history		
V5.1.1	May 2024	Publication