



Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options

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.

ReferenceDGS/NFV-IFA009

Keywordsarchitecture, management, NFV, orchestration

ETSI

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

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

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

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

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	7
4 NFV Architecture Framework - Release 1	7
4.0 introduction	7
4.1 Functional Blocks.....	7
4.2 Reference Points.....	9
4.3 Interfaces	9
5 Key rationales driving clarification of Architectural Options	9
6 Architectural Options	10
6.1 Overview	10
6.2 Architectural options related to VNFM.....	11
6.2.1 Architectural Option with generic VNFM	11
6.2.1.1 Overview	11
6.2.1.2 Resource management	11
6.2.1.3 VNF management	12
6.2.1.4 Cross-domain operation	12
6.2.1.5 FCAPS management	12
6.2.2 Architectural Option with Multiple VNFM(s).....	12
6.2.2.0 Introduction.....	12
6.2.2.1 Overview	12
6.2.2.2 Resource management	13
6.2.2.3 VNF management	13
6.2.2.4 Cross-domain operation	13
6.2.2.5 FCAPS management	13
6.3 Architectural options related to VNF related resource management.....	14
6.3.1 Architectural option where VNF related resource management done by VNFM.....	14
6.3.1.1 Introduction.....	14
6.3.1.2 Resource management	14
6.3.1.3 VNF management	14
6.3.2 Architectural option where VNF related resource management done by NFVO	15
6.3.2.1 Introduction.....	15
6.3.2.2 Resource management	15
6.3.2.3 VNF management	16
6.4 Architectural Options related to the split of NFVO.....	16
6.4.1 Use Case #1- Network Service Orchestrator and Resource Orchestrator	16
6.4.1.1 Description	16
6.4.1.2 Network Service Orchestration	17
6.4.1.3 Resource Orchestration	17
6.4.2 Use Case #2- Service Control and Virtual Network Platform Control	17
6.4.2.1 Description	17
6.4.2.2 Service Control Functions.....	19
6.4.2.3 Virtual Network Platform Control Functions.....	19
6.4.3 Use Case #3- Network Services offered by a separate admin domain.....	19
6.4.3.1 Description	19
6.4.3.2 Umbrella NFVO.....	20

6.4.3.3	NFVO in admin domain.....	21
6.5	Architectural options related to EM functions deployment.....	21
6.5.1	Introduction.....	21
6.5.2	Non-MANO related options	21
6.5.3	MANO related options.....	21
6.5.3.1	Overview	21
6.5.3.2	EM functions as VNFCs	21
6.5.3.3	EM functions as VNFs	21
6.5.3.4	EM functions as other Virtualised elements.....	22
6.6	Architectural options related to VNF lifecycle operation granting	22
6.6.1	Architectural option with bulk granting.....	22
6.6.1.1	Introduction.....	22
6.6.1.2	Pre-requisite conditions for applying bulk granting	23
6.6.1.3	Permission of bulk granting by the NFVO.....	23
6.6.1.4	Revocation of bulk granting by the NFVO	23
6.6.1.5	Co-existence with the existing NS level policies at the NFVO.....	23
6.6.1.6	Evaluation on bulk granting	24
Annex A (informative): Operational Flows.....		25
A.1	Architectural option related to VNF related resource management.....	25
A.1.1	VNF related resource management done by VNFM	25
A.1.2	VNF related resource management done by NFVO.....	26
A.2	Architectural option related to bulk granting	26
A.2.1	Permitting bulk granting in pull mode.....	26
A.2.2	Permitting bulk granting in push mode	27
Annex B (informative): Bibliography.....		29
Annex C (informative): Authors & contributors.....		30
History		31

Intellectual Property Rights

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document is an informative architectural study that identifies different viable architectural and functional options for the partitioning/distribution/consolidation of functionality amongst NFV-MANO functional blocks defined in NFV architectural document ETSI GS NFV 002 [i.2] and further refined in NFV-MANO architectural framework ETSI GS NFV-MAN 001 [i.4], as well as the potential impact in each case on reference points, on interfaces associated with the reference points, and on information elements exchanged over those interfaces.

2 References

2.1 Normative references

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

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

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

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

Not applicable.

2.2 Informative references

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

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

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

- [i.1] ETSI GS NFV 001 (V1.1.1): "Network Functions Virtualisation (NFV); Use Cases".
- [i.2] ETSI GS NFV 002 (V1.1.1): "Network Functions Virtualisation (NFV); Architectural Framework".
- [i.3] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".
- [i.4] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.3] and the following apply.

A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI GS NFV 003 [i.3].

bulk granting: action of giving permission to the VNFM for performing associated VNF lifecycle management operations without asking explicit granting from the NFVO

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.3] apply.

An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GS NFV 003 [i.3].

4 NFV Architecture Framework - Release 1

4.0 introduction

The present document references the NFV-MANO functional blocks, reference points, interfaces and information elements defined in ETSI GS NFV-MAN 001 [i.4].

4.1 Functional Blocks

The NFV-MANO functional blocks and reference points are illustrated in figure 4.1-1, representing the main architectural diagram in ETSI GS NFV-MAN 001 [i.4].

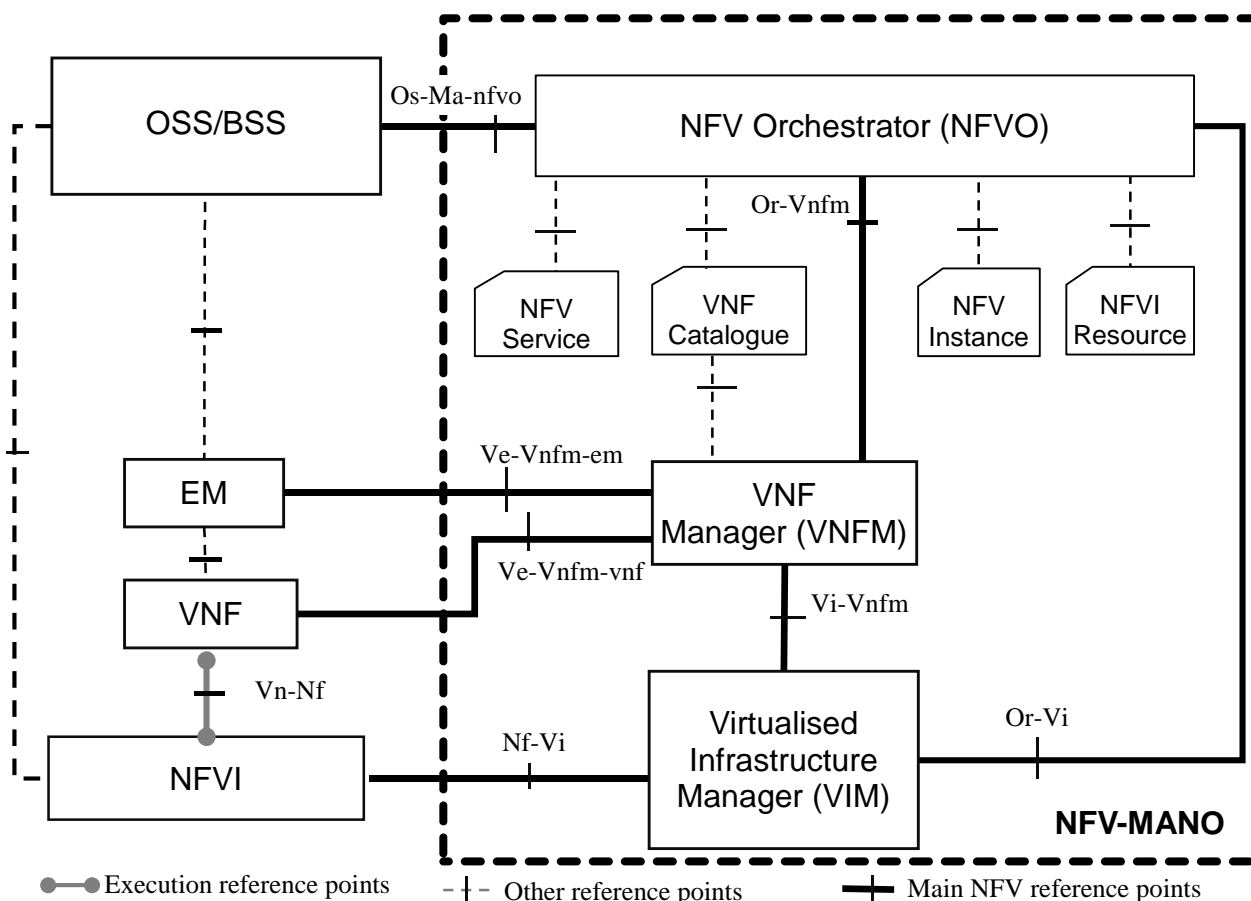


Figure 4.1-1: The NFV-MANO architectural framework with reference points

The following NFV-MANO functional blocks are the main focus of the present document with respect to potential composition or de-composition in order to realize a specific architectural option:

- NFV Orchestrator (NFVO) is a functional block with two main responsibilities:
 - the orchestration of NFVI resources across multiple VIMs, fulfilling the Resource Orchestration (RO) functions described in clause 4.2 of ETSI GS NFV-MAN 001 [i.4];
 - the lifecycle management of Network Services (NS), fulfilling the Network Service Orchestration functions described in clause 4.4 of ETSI GS NFV-MAN 001 [i.4].
- VNF Manager (VNFM) is a functional block with the main responsibility for the lifecycle management of VNF instances as described in clause 4.3 of ETSI GS NFV-MAN 001 [i.4].
- Virtualised Infrastructure Manager (VIM) is a functional block with the main responsibility for controlling and managing the NFVI compute, storage and network resources.

The following functional blocks may also be considered in order to provide a more complete architectural option:

- OSS/BSS is a functional block representing the combination of the operator's other operations and business support functions that are not otherwise explicitly captured in the architectural diagram.
- EM is a functional block with the main responsibility for FCAPS management functionality for a VNF.
- NFVI is a functional block representing all the hardware (e.g. compute, storage, and networking) and software (e.g. hypervisors) components that together provide the infrastructure resources where VNFs are deployed.

VNF is a functional block representing the Virtualised Network Function.

4.2 Reference Points

The following reference points illustrated in figure 4.1-1 are explored in the present document:

- Os-Ma-nfvo, a reference point between OSS/BSS and NFVO.
- Ve-Vnfm-em, a reference point between EM and VNFM.
- Ve-Vnfm-vnf, a reference point between VNF and VNFM.
- Or-Vnfm, a reference point between NFVO and VNFM.
- Or-Vi, a reference point between NFVO and VIM.
- Vi-Vnfm, a reference point between VIM and VNFM.

The following reference points not illustrated in figure 4.1-1 are explored in the present document:

- reference point between NFVO and NFVO;
- reference point between NSO and RO.

4.3 Interfaces

The following interfaces are discussed in the present document:

- Virtualised resources capacity management.
- VNF lifecycle management.
- VNF lifecycle change notification.
- Network Service lifecycle management.
- Network Service lifecycle change notification.
- VNF lifecycle operation granting.
- Interfaces related to bulk granting (such as Bulk granting command, Request/Revoke/Update bulk granting).
- Interfaces related to new identified reference points.

For additional details applicable to each interface (e.g. specific operations) see ETSI GS NFV-MAN 001 [i.4].

5 Key rationales driving clarification of Architectural Options

The NFV-MANO architectural framework ETSI GS NFV-MAN 001 [i.4] describes functional blocks, reference points, interfaces associated with the reference points, information elements exchanged over those reference points and a number of operational flows.

The deliberate and stated intent of ETSI GS NFV-MAN 001 [i.4] was to create an NFV management architecture framework that would allow for multiple possible architectural options to emerge.

There are some key rationales for continuing to study in more detail the NFV-MANO architecture framework, in order to identify, clarify and document the most viable architectural options, and the impact of pursuing the different architectural options identified.

A non-exhaustive list of key rationales driving the need for further analysis and clarification of the different architectural options includes:

- distribution of functionality between NFVO, VNFM and VIM;
- in operational flows, the existence of several alternatives for some operations;
- the potential processing of VNFD content by various functional blocks;
- the multiple possible interpretations of ownership and access paths to information managed by the different NFV-MANO functional blocks;
- the different roles that functional blocks play in policy administration and management;
- the different roles that functional blocks play in resource reservation;
- the need to and the effect of placing different functional blocks in different administrative domains;
- the presence of a single or multiple (identical and/or different) functional blocks (e.g. VIMs, VNFMs).

6 Architectural Options

6.1 Overview

The premise for describing viable architectural options is that NFV-MANO functional blocks can be partitioned/distributed/consolidated, in order to optimize specific operational flows and exchanges of information elements, and support placement of the resulting functional blocks in different administrative domains.

The present document proposes to describe viable architectural options based on the following guiding principles:

- The potential of placement of functions in different administrative domains needs to be taken into consideration.
- While a large number of architectural options can be derived because of the potential partitioning/distribution/consolidation of functionality amongst NFV-MANO functional blocks, a particular option is recommended in the present document if it adds identifiable benefits.

The following architecture options are studied in the present document:

- Architectural options related to VNFM, either using a generic VNFM or multiple VNFMs.
- Architectural options related to VNF related resource management, depending whether VNF-related Resource Management is done in direct or indirect mode.
- Architectural Options related to the split of NFVO, where the NFV Orchestrator functionality could be further de-composed into several components (e.g. Resource Orchestration (RO) functions and Network Services Orchestration (NSO) functions).
- Architectural options related to EM functions deployment in the scope of NFV.
- Architectural options related to VNF lifecycle operation granting, studying the bulk granting option.

6.2 Architectural options related to VNFM

6.2.1 Architectural Option with generic VNFM

6.2.1.1 Overview

This architectural option describes the implication of using a generic VNFM that can serve multiple VNFs of different types and/or originating from different providers. It is assumed that the operation of generic VNFM has no dependency on the VNF(s) it manages, but it should be able to accommodate the VNF-specific scripts defined in the VNF package. There may be multiple generic VNFMs which each managing a subset of the VNFs, depending on administrative criteria. The orchestrator needs to be able to handle multiple generic VNFMs in this case.

In this architectural option, it is assumed that:

- Standard interfaces are exposed by the VIM and the NFVO at the Vi-Vnfm and Or-Vnfm reference points (respectively).
- Standard interfaces are exposed by the VNF and the EM, at the Ve-Vnfm-vnf and Ve-Vnf-em reference points (respectively).
- The VNFM provides VNF lifecycle management procedures for each VNF it manages.
- The VNFM can be delivered by a provider that is different from the VNF providers.

Figure 6.2.1.1-1 illustrates such an architectural option.

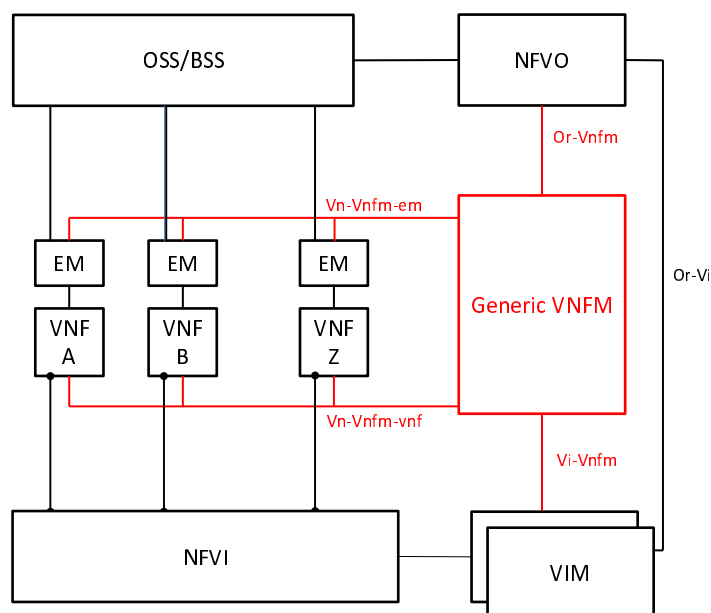


Figure 6.2.1.1-1: Architectural option with a generic VNFM.

6.2.1.2 Resource management

The VNFM requests resources required for the VNFs it manages via the interfaces exposed by the Vi-Vnfm and/or Or-Vnfm reference points. The VNFM needs to be able to interface with one or multiple VIMs.

6.2.1.3 VNF management

A VNFM can manage the lifecycle of multiple types of VNFs (potentially from different providers). Management of the lifecycle of simple VNFs typically relies on standard basic management capabilities. Life cycle management aspects that are specific to a VNF are captured by the VNF provider within scripts included in the VNF package. In order to fulfil its responsibilities in supporting VNF lifecycle management, a generic VNFM is expected to be capable of interpreting and executing such scripts.

NOTE: To enable independence between the generic VNFM and the VNF, the scripts are expected to be written in a VNF-independent, Provider-independent language that all generic VNFMs support. Until such a universal language is specified, an implementation of a generic VNFM may support one or more languages, and as a consequence would only be able to support VNF Packages that use these particular language(s). In some cases, where this is an issue, the VNF Package may be adapted to use a language supported by a particular implementation of a generic VNFM.

In addition, VNF lifecycle management functionality that may be necessary, but cannot be supported by a generic VNFM via the scripting language is assumed to be included in the VNF itself and is not visible to the generic VNFM, hence is out-of-scope for the present document. It is recommended that during the VNF Package validation the NFVO can detect whether the VNF Package can be managed by a generic VNFM, or requires a specific VNFM (e.g. via an indication in the VNF Package).

6.2.1.4 Cross-domain operation

The VNFM can reside in the same or different administrative domain as the VNFs it manages.

6.2.1.5 FCAPS management

The nature of the VNFM does not have any impact on the FCAPS management functionality for the VNF it manages. FCAPS management of a VNF is performed by an EM as per ETSI GS NFV-MAN 001 [i.4], clause 5.5.1.

6.2.2 Architectural Option with Multiple VNFMs

6.2.2.0 Introduction

The NFV Architectural Framework [i.2] allows for one or more VNF Managers (VNFM) attached to a single NFVO. This architectural option describes the impacts of a deployment using multiple VNFMs. Multiple VNFMs may be required to capsule application/VNF specific information and/or lifecycle operations within a single administrative domain. Multiple VNFMs may also be required in a scenario in which a VNFM handles VNFs with complex or advanced lifecycle management procedures and thus may be specific to those VNFs.

6.2.2.1 Overview

In this architectural option, it is assumed that:

- The VNFM integrates specific functionality which enables handling a single or set of defined VNFs.
- The VNFM can be delivered by the VNF provider.
- Towards the rest of NFV-MANO architectural framework functional blocks, the Vi-Vnfm and Or-Vnfm reference points become the main integration points of multiple VNFMs.

Figure 6.2.2.1-1 illustrates such an architectural option.

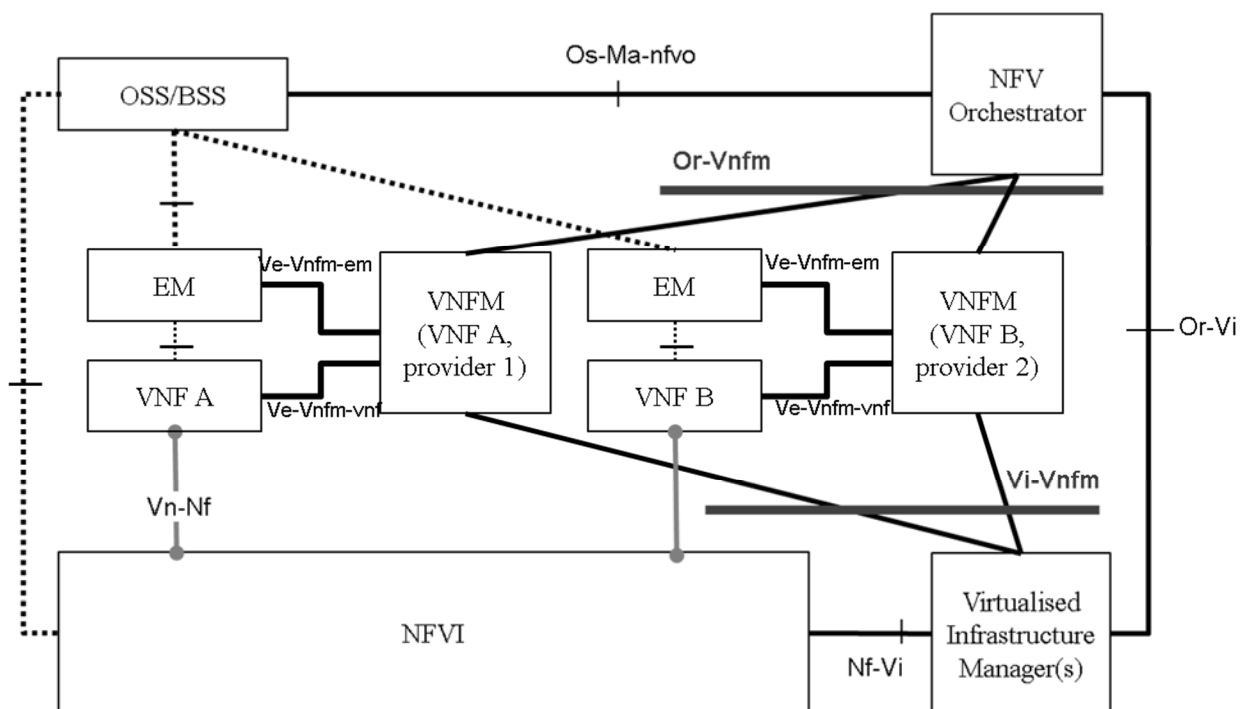


Figure 6.2.2.1-1: Architectural option with multiple VNFM.

6.2.2.2 Resource management

The VNFM requests resources required for the VNFs it manages via the interfaces exposed by the Vi-Vnfm and Or-Vnfm reference points. These reference points also become the main integration points of the VNFM towards the rest of NFV-MANO functional blocks. In the case VNFM from different vendors are used, the Vi-Vnfm and Or-Vnfm reference points are multi-vendor reference points.

6.2.2.3 VNF management

The VNFM may only manage the lifecycle of one or multiple VNFs, whose lifecycle procedures have been integrated with the VNFM and can be coupled with the functionality of the VNF(s). Thus it is likely that the VNFM will be provided by the same vendor as VNFs that the VNFM manages. In a deployment in which VNFs are supplied by multiple vendors there may be multiple VNFM in which each manages one or a subset of the VNFs from the same vendor. The orchestrator needs to be able to handle multiple VNFM in this case.

6.2.2.4 Cross-domain operation

The VNFM resides in the same administrative domain as the VNFs it manages.

6.2.2.5 FCAPS management

The VNF FCAPS are handled by the subsystem formed by VNF, VNFM and EM if applicable.

6.3 Architectural options related to VNF related resource management

6.3.1 Architectural option where VNF related resource management done by VNFM

6.3.1.1 Introduction

The NFV Management and Orchestration architecture enables both the NFVO and the VNFM to manage the Virtualised resources needed for lifecycle management of the VNFs.

This architectural option describes the case where the VNFM is the functional block to manage the virtualised resources needed for the lifecycle management of the VNF, except resource reservations requests.

In this architectural option, it is assumed that:

- Standard interfaces are exposed by the VIM and the NFVO at the Vi-Vnfm and Or-Vnfm reference points (respectively).
- The VNFM provides VNF lifecycle management procedures.

Figure 6.3.1.1-1 illustrates such an architectural option.

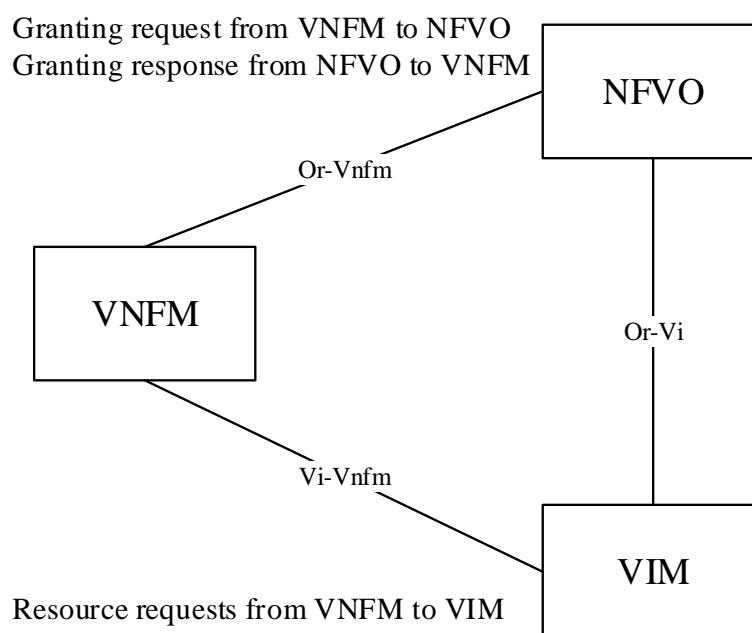


Figure 6.3.1.1-1: Architectural option with resource management done by VNFM

Simplified flows corresponding to this architectural option are shown in clause A.1.1.

6.3.1.2 Resource management

The VNFM requests resources required for the VNFs it manages via the Virtualised Compute/Storage/Network Resource Management interfaces exposed by the VIM on the Vi-Vnfm reference point.

6.3.1.3 VNF management

The VNFM provides VNF lifecycle management procedures.

As part of the processing of the VNF LCM operation, VNFM requests to the NFVO granting for every VNF LCM operation, except query operation, whether requesting new resources or freeing allocated resources.

No resource operation is issued by the VNFM before receiving a successful granting response. In the case of bulk granting the VNFM may perform resource operations independently after receiving an initial granting response (see clause 6.6).

6.3.2 Architectural option where VNF related resource management done by NFVO

6.3.2.1 Introduction

The NFV Management and Orchestration architecture enables both the NFVO and the VNFM to manage the Virtualised resources needed for lifecycle management of the VNFs.

This architectural option describes the case where the NFVO is the only functional block to manage the virtualised resources needed for the lifecycle management of the VNF.

In this architectural option, it is assumed that:

- Standard interfaces are exposed by the VIM and the NFVO at the Or-Vi and Or-Vnfm reference points (respectively).
- The VNFM provides VNF lifecycle management procedures.

Figure 6.3.2.1-1 illustrates such an architectural option.

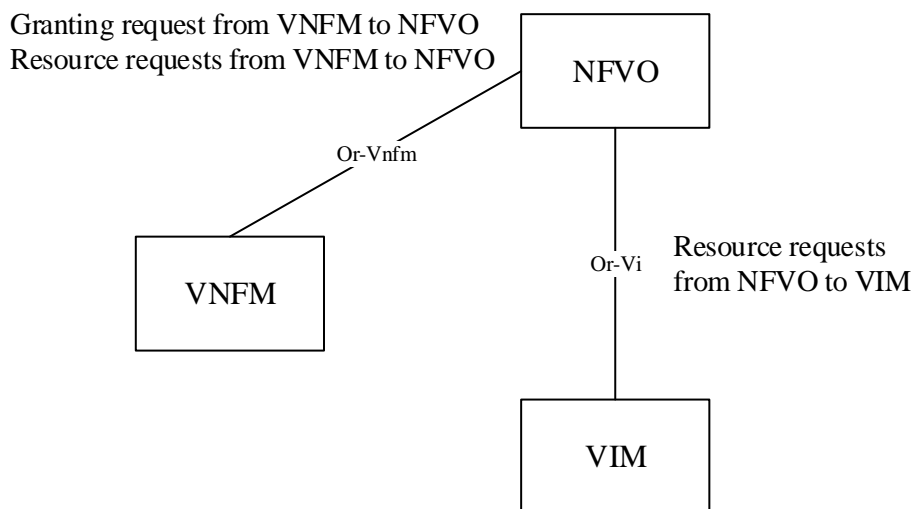


Figure 6.3.2.1-1: Architectural option with resource management done by NFVO

Simplified flows corresponding to this architectural option are shown in clause A.1.2.

6.3.2.2 Resource management

The VNFM requests resources required for the VNFs it manages via the Virtualised Resource Management interfaces exposed by the NFVO on the Or-Vnfm reference point.

The VNFM invokes Resource Management operations towards the NFVO, which in turn invokes them towards the VIM.

In this architectural option, the VNFM never communicates with the VIM for management of Virtualised resources.

6.3.2.3 VNF management

The VNFM provides VNF lifecycle management procedures and exposes the VNF lifecycle management interface.

As part of the processing of the VNF LCM operation, VNFM requests to the NFVO granting for every VNF LCM operation, except query operation, whether requesting new resources or freeing allocated resources.

No resource operation is issued by the VNFM before receiving a successful granting response

6.4 Architectural Options related to the split of NFVO

6.4.1 Use Case #1- Network Service Orchestrator and Resource Orchestrator

6.4.1.1 Description

This Use Case addresses a Network Operator offering of infrastructure to different departments within the same operator, as well as facilitating the offering this infrastructure to a different network operator like in cases of network sharing agreements.

In this Use Case, an administrative domain is regarded as one or more Datacentres and VIMs, providing an abstracted view of the resources hosted in it. Resource offering, whether internal or external, is based on administrative domains.

This use case is focusing on these administrative domains and does not explore whether the VNFMs and NSO might also be part of another domain.

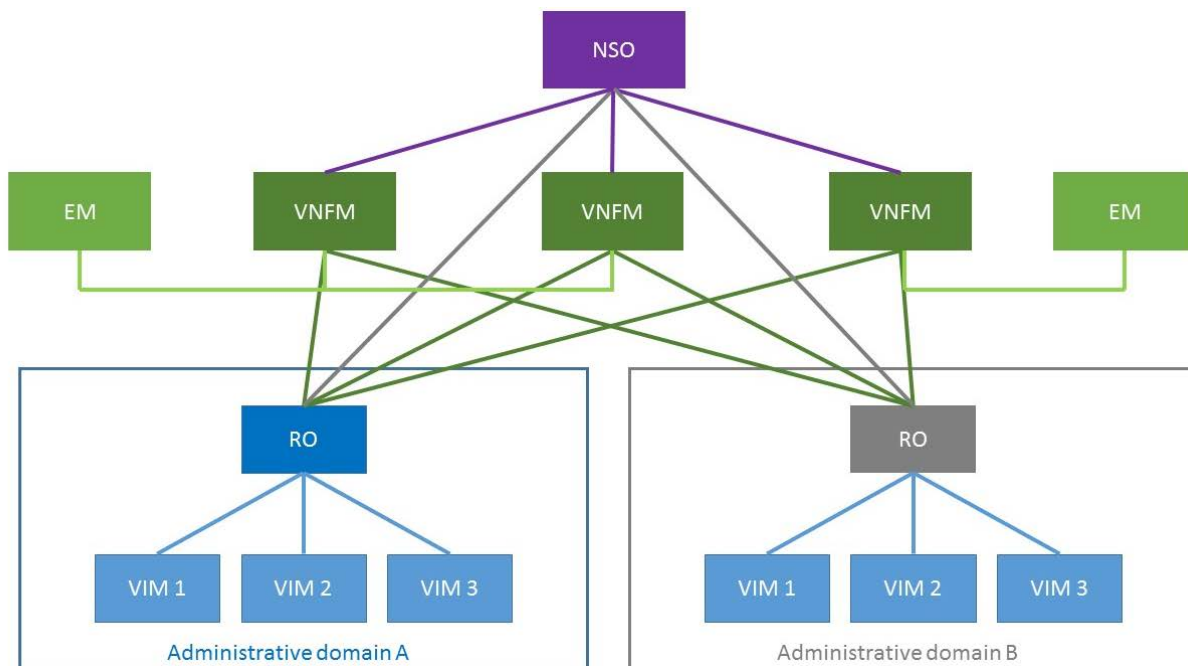


Figure 6.4.1.1-1: Infrastructure provided using multiple administrative domains

This use case aligns with the Use Case #1, NFVIaaS, as depicted in ETSI GS NFV 001 [i.1], where a service is orchestrated out of VNFs that can run on infrastructure provided and managed by another Service Provider. This infrastructure would be in a separate administrative domain managed by the other Service Provider.

This resources sharing implies the separation of some functionalities:

- on one side the Network Service Orchestration functionality,
- on the other side the Resource Orchestration functionality.

The separation of these functionalities requires to group a number of functions as elaborated hereafter in clauses 6.4.1.2 and 6.4.1.3.

6.4.1.2 Network Service Orchestration

The Network Service Orchestration is managing the lifecycle of network services.

It includes the management of the Network Services templates and VNF Packages (e.g. on-boarding new Network Services and VNF Packages).

The Network Service Orchestration provides the management of the instantiation of VNFs, in coordination with VNF Managers. It is also responsible to establish the connectivity between VNFs and PNFs parts of a Network Service, i.e. VNF FGs and VLs by calling the respective Resource Orchestrators. A VNF can use the resources of a given admin domain, but will not span across multiple admin domains.

The Network Service Orchestration is in charge of the granting VNF lifecycle management operations from VNF Managers, as those may impact Network Services.

The Network Service Orchestration is unaware of resources status in each administrative domain. It is only aware of the resource capacity exposed by the various Resource Orchestrators.

6.4.1.3 Resource Orchestration

The Resource Orchestration provides an overall view of the resources present in the administrative domain to which it provides access and hides the interfaces of the VIMs present below it. The regions/NFVI-Pop and resource groups defined by the various VIMs in the administrative domain are visible at the RO interface.

The Resource Orchestrator provides a proxy gateway for the VIM underneath it and acts as a bridge for some routing aspects also. WHEN providing resource management in indirect mode, ALL requests for resources from the VNFMs GO through the Resource Orchestrator to access the VIMs in each admin domain. Direct mode from the VNFMs to the VIMs in each admin domain is not possible.

The Resource Orchestration has a resource view and is aware of the resource usage and availability in the NFV infrastructure. The Resource Orchestrator is also providing the fault and performance management hiding the corresponding interfaces of the VIMs present below it.

The Resource Orchestration is aware of the logical grouping of the resource requirements, e.g. per the VNF.

Resource requirements per VNF are part of the granting info. Granting may also be needed at NSO level for validation against NS and capacity maintained by NSO for each RO.

The Resource Orchestration is not able to take decisions based on VNF instances or on Network Service instances, and needs to be instructed by either the relevant VNFM or the relevant Network Service Orchestration.

The Resource Orchestration is constantly updated with the latest infrastructure resources organization, availability and utilization from the various VIMs in the administrative domain.

6.4.2 Use Case #2- Service Control and Virtual Network Platform Control

6.4.2.1 Description

Network resources are more and more often not exclusively used by the operator. Enterprises and other operators can deploy certain services based on a service catalogue within the network of a hosting operator. For that, they can use predefined network service templates, create new ones, use certain orchestration functions or could even deploy their own (black-box) services.

This Use Case addresses a Network Operator offering of infrastructure and applications to different departments within the same operator, as well as facilitating the offering of these services to a different network operator like in cases of network sharing agreements, or hosting services. A typical example for making use of this scenario is an IMS-based business communication suite , offered to an enterprise.

As NFV solutions start to be deployed, the nature of the various types of network services point into optimizations of the network, compared to legacy plans; and organizational issues, business agreements and legacy features start to demand solutions to help optimizing the management of the network and the services offered to their customers.

As an example, in case of global operators, the number of services offered may be of a completely different nature: Enterprise services can be offered on a global or national basis, or Public (i.e. for consumer) services can be offered on a local, regional or national basis, all of them supported by a set/subset of network functions and demanding proper infrastructure supporting the different services.

In this Use Case as depicted in figure 6.4.2.1-1, a Virtual Network Platform is regarded as one or more Datacentres, VIMs and VNFMs (together with their related VNFs) allowing distinct specific sets of network functions to be hosted on each. For example, local (e.g. Germany, Italy) operations or regional (e.g. east, west, central) operations could be regarded as Virtual Network Platforms:

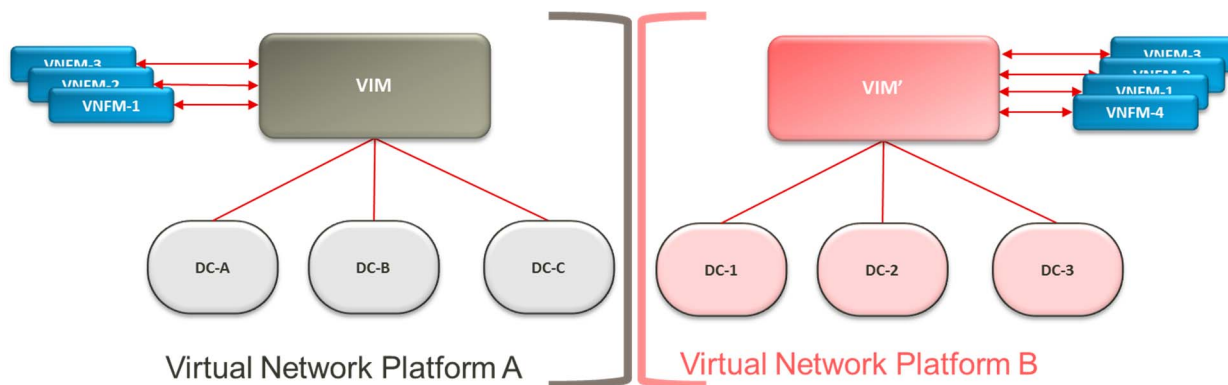


Figure 6.4.2.1-1: Virtual Network Platform as one or more Datacentres, VIMs and VNFMs

As an example, Enterprise Services department may be in need to deploy a Service in Platform A and Platform B due to one particular service nature. At the same time Consumer Services department may need to deploy a service in Platform A, e.g. due to latency requirements and a different service in Platform B.

Both organizations, Enterprise Service and Consumer Services, will be sharing resources in both domains, without having to be aware of the type of service and the resources the other is consuming.

The Use Case can increase in complexity as platforms grow in number and organizational borders between them appear; e.g. Platform A can be located in one country and Platform B in a different one, with Consumer services departments completely separated from each other and also separated from the Enterprise Services organization. This more complex scenario is depicted in figure 6.4.2.1-2.

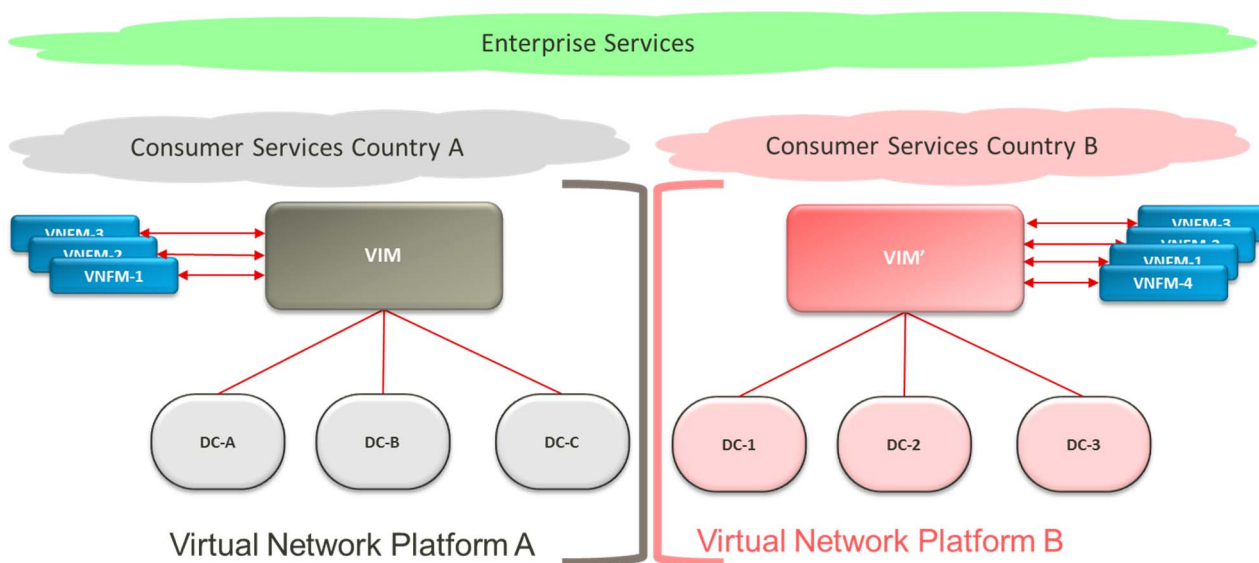


Figure 6.4.2.1-2: Virtual Network Platforms located in different countries providing customer services

This use case aligns with the Use Case #3, VNPaaS, as depicted in ETSI GS NFV 001 [i.1], where a service is orchestrated out of existing functions and managed by the third party within the limits of the Virtual Network Platform operator.

This resources sharing implies the separation of some functionalities:

- on one side the Service Control functionality,
- on the other side, the Virtual Network Platform Control functionality.

The separation of these functionalities requires to group a number of functions as elaborated hereafter in clauses 6.4.2.2 and 6.4.2.3.

6.4.2.2 Service Control Functions

The Service Control is able to manage a set of network services made up of virtual network functions residing in one or different platform domains. Each network service is defined by a Network Service Template, i.e. a collection of one or more VNF instance(s).

The Service Control can collect information, from all the connected platform domains, concerning the VNFs and VNF Templates available and of use by the different Network Services.

The Service Control is able to request installation of all network functions belonging to a network service as an atomic operation, using the Network Service Template and additionally, VNF(s) capacity figures and configuration.

The Service Control is unaware of resources status in each platform.

The Service Control can manage different Network Service Templates for the same Network Service (e.g. adapted to service forecast and used for deployment and scaling in/out).

6.4.2.3 Virtual Network Platform Control Functions

The Virtual Network Platform Control continuously monitors the utilization of each installed VNF and the resource availability in the NFV infrastructure.

The Virtual Network Platform Control has a VNF view: being aware of their instances location, performance and related events and is able to answer to any VNF installation or scaling request from a resource availability perspective.

The Virtual Network Platform Control is not able to take decisions based on the Network Service the VNF instances belong to, and needs to be instructed by the relevant Service Control Functionality.

The Virtual Network Platform Control is constantly updated with the latest infrastructure resources organization, availability and utilization.

6.4.3 Use Case #3- Network Services offered by a separate admin domain

6.4.3.1 Description

This Use Case addresses a Network Operator offering Network Services to different departments within the same operator, as well as facilitating the offering these Network Services to a different network operator like in cases of network sharing agreements.

In this Use Case, an administrative domain is regarded as one or more Datacentres, VIMs, VNFM(s) (together with their related VNFs) and NFVO, allowing distinct specific sets of network services to be hosted and offered on each.

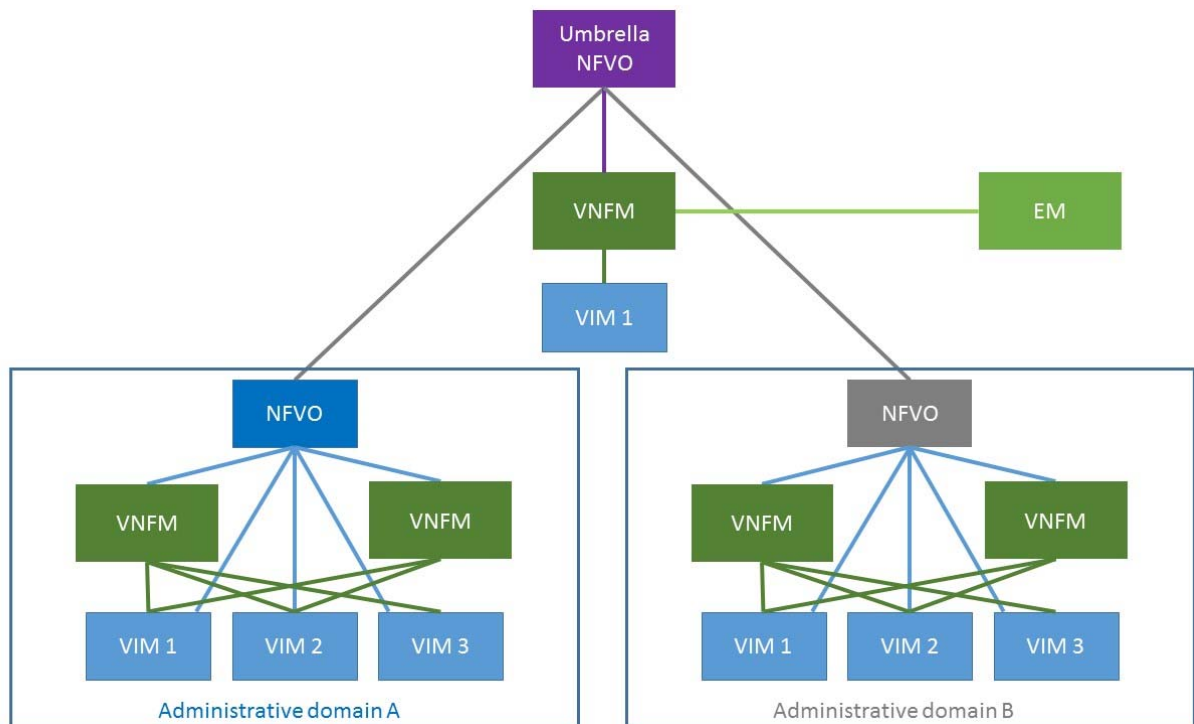


Figure 6.4.3.1-1: Network services provided using multiple administrative domains

Figure 6.4.3.1-1 is presenting 2 separate admin domains, each one offering a set of Network Services. This use case is not creating any new functional block out the NFVO, but introducing a new reference point between NFVOs.

This use case is a variant the Use Case #1VNPaaS, as depicted in ETSI GS NFV 001 [i.1], where VNFs offered as a service are grouped in Network Services being offered.

For instance, a CPM Network Service can be deployed on top of a vIMS network service provided in a different admin domain.

This use case requires composition of Network Services, so a top Network Service (like CPM in the example above) can include another Network Service (vIMS in the example). A Network Service containing other Network Services might also contain VNFs, as shown above in figure 6.4.3.1-1.

Note that it is only one possible use case for network service composition.

The NFVO in each admin domain will provide visibility of the Network Services specific to this admin domain.

For sake of simplicity, the NFVO sitting above the 2 admin domains is called in the present document an umbrella NFVO.

The separation of functionality between the umbrella NFVO functionality on one hand and on another, the NFVO of each admin domain is detailed hereafter in clauses 6.4.3.2 and 6.4.3.3.

6.4.3.2 Umbrella NFVO

The umbrella NFVO is providing the lifecycle management of umbrella network services defined in this NFVO. It does not provide the lifecycle management of the network services offered in each admin domain and managed by the NFVO of each admin domain.

It includes the management of the Network Services templates for the Network Services managed and VNF Packages managed by this NFVO (e.g. on-boarding new Network Services and VNF Packages).

The umbrella NFVO provides the management of the instantiation of VNFs for the ones directly part of the Network Services it manages, in coordination with VNF Managers as well as requesting the instantiation/ scaling and termination of the Network Services managed by different admin domains.

The umbrella NFVO is unaware of resources status in each administrative domain.

6.4.3.3 NFVO in admin domain

In each admin domain, the NFVO is providing standard NFVO functionalities, with a scope limited to the network services, VNFs and resources that are part of its admin domain.

It includes providing the lifecycle management of network services that are part of this admin domain.

It covers the management of the Network Services templates and VNF Packages specific to this admin domain (e.g. on-boarding new Network Services and VNF Packages).

The NFVO in the admin domain is in charge of the validation and authorization of NFVI resource requests from VNF Managers in this admin domain.

The NFVO of the admin domain provides the management of the instantiation of VNFs, specific to the admin domain, in coordination with VNF Managers.

6.5 Architectural options related to EM functions deployment

6.5.1 Introduction

The following clauses describe several options to deploy Element Management (EM) functions.

EM providers may follow either of these options or combinations of them.

6.5.2 Non-MANO related options

Non-MANO related options for deploying EM functions are outside the scope of ETSI NFV specifications. These include for example the case where EM functions are deployed in the form of dedicated software modules that are running on bare metal or in virtualisation containers outside the NFVI and are not visible to the NFV MANO functions, as well as the case where EM functions are subsumed in other OSS functions.

In such cases, the deployment of EM functions instances is independent from the deployment of VNF instances.

6.5.3 MANO related options

6.5.3.1 Overview

The functional behaviour of EM, EM internal architecture and details of interaction between EM and managed VNF(s) are out of scope of ETSI NFV. However, NFV may bring new opportunities for automated deployment and LCM of EM(s).

6.5.3.2 EM functions as VNFCs

The EM functions software is implemented in the form of VNFCs. In this deployment option, EM functions are embedded in the VNF and deployed at VNF instantiation time. There is at least one "EM" VNFC instance per VNF instance. MANO functions do not identify such "EM" VNFCs as being different from the other ones.

6.5.3.3 EM functions as VNFs

The EM functions software is implemented in the form of one or more VNFs. Such "EM" VNFs have to be included in the NS at design time together with the VNFs they manage. There might be one or several of such "EM" VNF for one, several or all VNFs in the NS. In this deployment option, EM functions are embedded in the NS and deployed at NS instantiation time. Within an NS, a dedicated forwarding graph will typically be defined to connect such "EM" VNFs to the VNF they manage. MANO functions do not identify such "EM" VNFs as being different from the other ones.

6.5.3.4 EM functions as other Virtualised elements

The EM functions software is implemented in the form of one or more software elements that are not VNF or VNFCs. Such elements can be included in the VNF Package, in which case they are similar to a VNFC except that they are explicitly identified as management plane elements and are associated to a specific type of descriptor to be defined. These elements can also be included at the NS level, in which case they are similar to a VNF except that they are explicitly identified as management plane elements and are associated to a specific type of descriptor to be defined.

6.6 Architectural options related to VNF lifecycle operation granting

6.6.1 Architectural option with bulk granting

6.6.1.1 Introduction

VNF Lifecycle Operation Granting is one basic functional mechanism over Or-Vnfm reference point in which the NFVO gives the permission to the VNFM for performing a VNF lifecycle management (LCM) operation and resource management operations necessary to complete it, if any apply. As the VNFM has to send a Grant Request to the NFVO for each VNF LCM operation to be performed, it can result in a high traffic exchange between the VNFM and the NFVO.

Bulk granting encompasses functionalities to permit the VNFM to perform multiple VNF LCM operations for one or multiple VNFs without asking explicit granting from the NFVO each time, provided that the needed conditions are met. Both the NFVO and the VNFM perform functionality related to management of bulk granting. The NFVO is responsible for determining whether bulk granting can be performed by the VNFM, with the assistance of policies configured inside the NFVO.

In this architectural option, it is assumed that:

- Standard interfaces are exposed by the VNFM and the NFVO at the Or-Vnfm reference point.
- The VNFM provides VNF lifecycle management procedures.

Figure 6.6.1.1-1 illustrates such an architectural option.

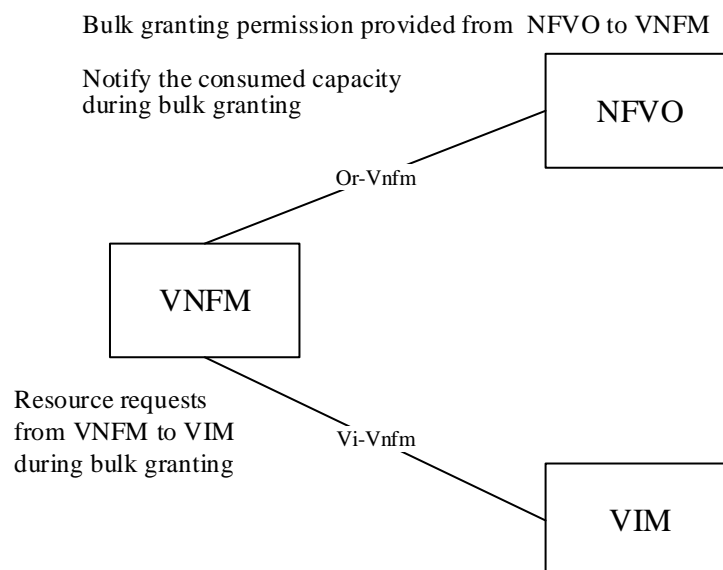


Figure 6.6.1.1-1: Architectural option with bulk granting

6.6.1.2 Pre-requisite conditions for applying bulk granting

Bulk granting is applied under certain conditions which align with the operator's policies in deploying and performing VNF lifecycle operations in the network. The following conditions are required as pre-requisite to bulk granting:

- The capacity information maintained at the NFVO, is per VNF or group of VNFs managed by this VNFM. If the capacity information for this VNF is per NS or group of VNFs spanning multiple VNFMs, the NFVO would decide whether this would prevent or not bulk granting.
- Policies applicable to bulk granting are in scope to the VNF. For instance, affinity/ anti-affinity policies across VNFs managed by different VNFMs would prevent bulk granting.
- Based on the policies or consistency aspects of the Network Service, the NFVO can decide whether this would prevent bulk granting.

6.6.1.3 Permission of bulk granting by the NFVO

The NFVO provides the permission of bulk granting to the VNFM in one of the following way:

- In Pull mode: The VNFM sends a request for bulk granting to the NFVO. The NFVO checks its permitted allowance for this VNFM and its internal policies (e.g. VNF dependencies, affinity/anti-affinity rules) and returns an acknowledgement including the granting granularity and permitted capacity in which the NFVO allows the VNFM to perform VNF lifecycle management. The granting granularity includes the range of VNFs granted to the VNFM, e.g. a single VNF, group of VNFs or all VNFs belonging to the VNFM. This will also include the LCM operation(s) granted for each of the identified VNF(s) e.g. Instantiation, Scale-out, etc.
- In Push mode: Based on its internal policies and the consumed capacity for VNF LCM operations based in received LCM Notifications, the NFVO directly sends the Bulk Granting command to the VNFM. The Bulk Granting command includes the granting granularity in which the NFVO allows VNFM to perform VNF lifecycle management operations and the permitted capacity allowed by the NFVO.

NOTE: The relationship between bulk granting, resource reservation and quota is not described in the present document.

6.6.1.4 Revocation of bulk granting by the NFVO

The NFVO is aware of the consumed capacity for VNF LCM operations performed by the VNFM during bulk granting by the means of VNF LCM Change Notifications containing consumed capacity information (see clause A.2). When the consumed capacity reaches the upper limit of capacity determined by the permitted allowance, or triggered by events according to the operator's policy, the NFVO can revoke bulk granting for the VNFM, or update bulk granting with a new permitted allowance. The NFVO can also revoke bulk granting when it decides that the VNFM grants of certain LCM operations like VNF scaling should be kept not any longer based on the NS scaling policies within the NFVO.

The NFVO decides based on policies/rules, indicators and constraints whether an update bulk granting with a new permitted allowance will be made. This ensures that the corresponding update is necessary and will not lead to a resource overload situation in the NFV ecosystem.

6.6.1.5 Co-existence with the existing NS level policies at the NFVO

Bulk granting is not just related with capacity management but also have to deal with the NS level policies at the NFVO. The NS level policies may include VNFs being managed by different VNFMs. Such policies may include VNF dependencies, affinity and anti-affinity rules etc. In case that such policies exists, the NFVO may decide to reject the Grant request. Alternatively, in case of affinity and anti-affinity rules, the NFVO may provide the VNFM the needed information, i.e. location constraints (e.g. the identifier of the host, site or geography area) queried from the VIM, or affinity groups, which is further used by the VNFM to communicate with the VIM in the VNF LCM operations.

6.6.1.6 Evaluation on bulk granting

Compared with the granting mechanism applied for each VNF LCM operation, management of bulk granting improves the efficiency of interaction between the NFVO and the VNFM:

- Reduce the interface calls (i.e. Grant Request/Grant ACK) over Or-Vnfm reference point during VNF LCM operations.
- Reduce the risk of NFVO as a single point of failure.
- Reduce the VNFM's overall response time on LCM request from the sender.

Annex A (informative): Operational Flows

A.1 Architectural option related to VNF related resource management

A.1.1 VNF related resource management done by VNFM

Figure A.1.1-1 illustrates a simple operational flow of a VNF LCM request where resource management is done by VNFM.

For sake of clarity, this flow has been simplified and a complete flow would have more interactions.

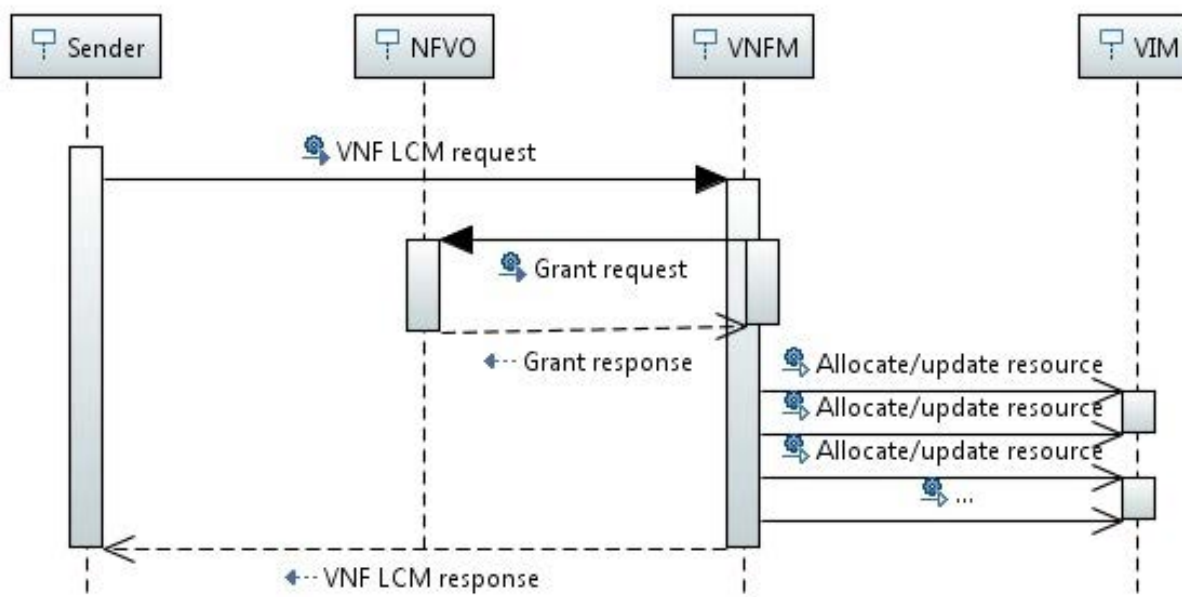


Figure A.1.1-1: Operational flow where resource management is done by VNFM

The main steps for the VNF LCM request are:

- 1) The sender (i.e. NFVO, EM, VNFM itself in case of auto-scale, etc.) issues a VNF LCM request to the VNFM using one of the operations of the VNF Lifecycle Management interface exposed by the VNFM.
- 2) The VNFM starts processing the request. If the request is not a query operation, the VNFM issues a Grant request to the NFVO using the operation Grant Lifecycle Operation of the VNF Lifecycle Operation Granting interface exposed by the NFVO. The grant request may be skipped in case bulk granting is used. For details see clause 6.6.
- 3) The NFVO processes the request and returns the response to the VNFM.
- 4) If the response is not successful, the VNFM cancels the VNF LCM request and return the failure to the Sender.
- 5) If the response is successful, the VNFM issues the needed resource requests to the VIM using the Virtualised Compute/Storage/Network Resource Management interfaces exposed by the VIM.
- 6) The VIM returns the responses back to the VNFM.
- 7) After completing the resource requests, the VNFM notifies the successful VNF LCM using the VNF Lifecycle Change Notification interface and reports back the response to the Sender.

A.1.2 VNF related resource management done by NFVO

Figure A.1.2-1 illustrates a simple operational flow of a VNF LCM request where resource management is done by NFVO. For sake of clarity, this flow has been simplified and a complete flow would have more interactions.

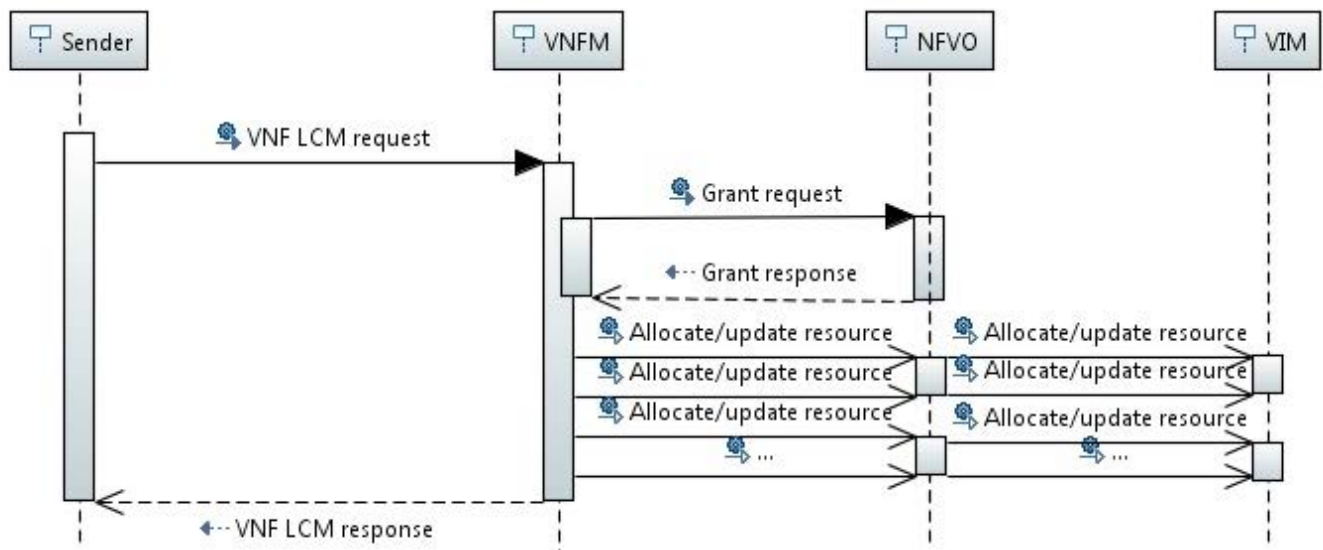


Figure A.1.2-1: Operational flow where resource management is done by NFVO

The main steps for the VNF LCM request are:

- 1) The sender (i.e. NFVO, EM, VNFM itself in case of auto-scale, etc.) issues a VNF LCM request to the VNFM using one of the operations of the VNF Lifecycle Management interface exposed by the VNFM.
- 2) The VNFM starts processing the request. If the request is not a query operation, the VNFM issues a Grant request to the NFVO using the operation Grant Lifecycle Operation of the VNF Lifecycle Operation Granting interface exposed by the NFVO.
- 3) The NFVO processes the request and returns the response to the VNFM.
- 4) If the response is not successful, the VNFM cancels the VNF LCM request and return the failure to the Sender.
- 5) If the response is successful, the VNFM issues the needed resource requests to the NFVO using the Virtualised Compute/Storage/Network Resource Management interfaces exposed by the NFVO.
- 6) The NFVO processes each of the resource requests and issues them in turn to the VIM using the Virtualised Compute/Storage/Network Resource Management interfaces exposed by the VIM.
- 7) The NFVO receives responses from the VIM and returns the responses back to the VNFM.
- 8) After completing the resource requests, the VNFM notifies the successful VNF LCM using the VNF Lifecycle Change Notification interface and reports back the response to the Sender.

A.2 Architectural option related to bulk granting

A.2.1 Permitting bulk granting in pull mode

Figure A.2.1-1 provides an example call flow for implementing management of bulk granting in pull mode.

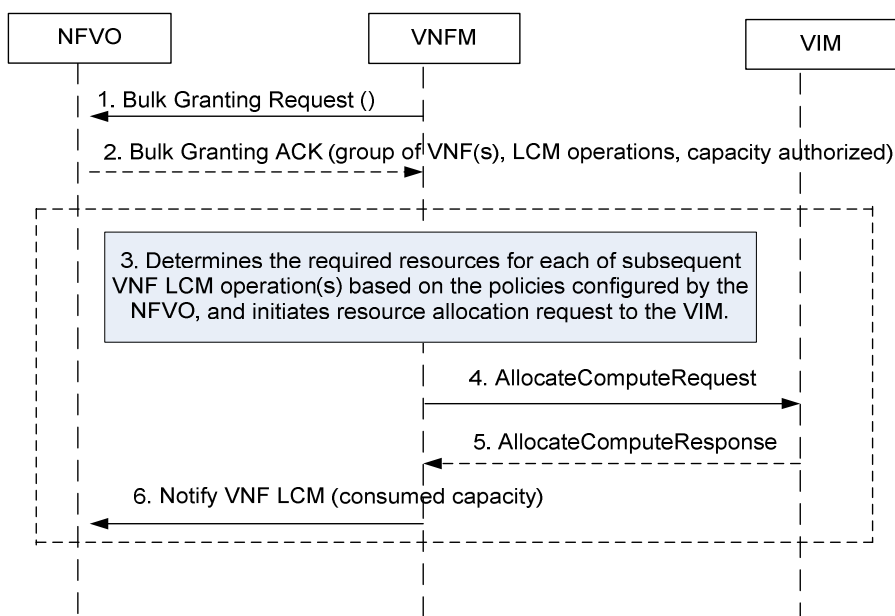


Figure A.2.1-1: Call flow of management of bulk granting in Pull mode

Pre-Condition: The VNFM is configured to request bulk granting.

- 1) The VNFM sends the Bulk Granting Request to the NFVO, to request for the permission of bulk granting.
- 2) The NFVO checks the related policies (e.g. VNF dependencies, affinity/anti-affinity rules) as specified in the VNFD and available capacity in the NFVI PoP. Based on the internal policies NFVO takes the decision and responds back with the Bulk Granting ACK message to the VNFM. The Bulk Granting ACK message includes, not limited to, the granting granularity the NFVO permitted to the VNFM, e.g. the identifier of the VNF(s), the related LCM operation(s) that can be granted for them and the capacity authorized for this VNF.

Step 3 to 6 repeat for each of subsequent VNF LCM operation:

- 3) For each subsequent VNF LCM operation related to the permitted VNF(s) received by the VNFM in Step 2, the VNFM checks if the LCM operation is in the scope of permission, based on the granting policy received from the NFVO. The VNFM determines the required resource for the LCM operation and decides to initiate resource allocation request to the VIM.
- 4) The VNFM sends AllocateComputeRequest message to the VIM for the VNF LCM operation.
- 5) The VIM responds AllocateComputeResponse message to the VNFM.
- 6) The VNFM sends a notification of VNF LCM to the NFVO. The notification message includes the consumed capacity during the VNF LCM operation.

A.2.2 Permitting bulk granting in push mode

Figure A.2.2-1 provides another example call flow for implementing management of bulk granting in push mode.

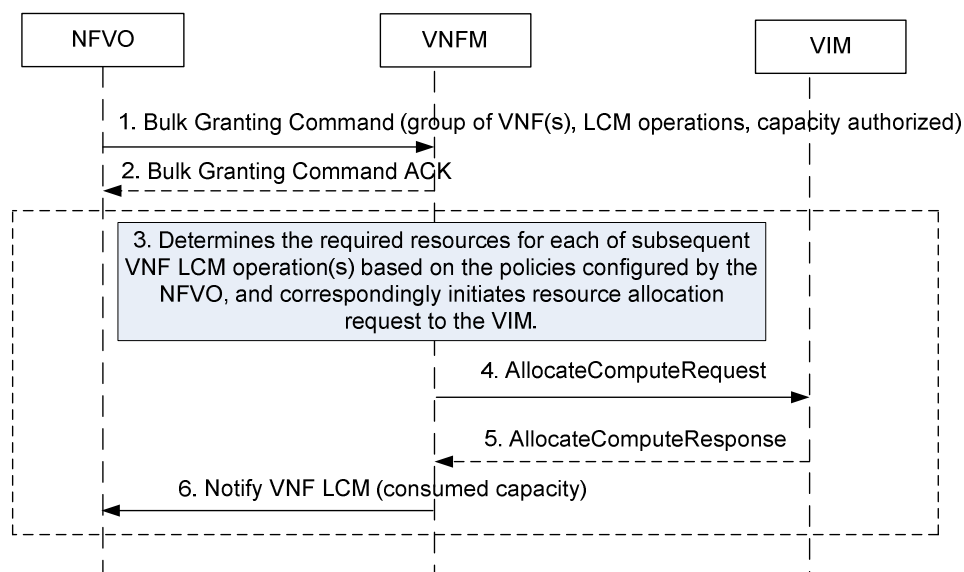


Figure A.2.2-1: Call flow of management of bulk granting in push mode

Compared with bulk granting in Pull mode, the main difference in Push mode is that bulk granting is directly initiated by the NFVO via a Bulk Granting Command, in which the granting granularity the NFVO permitted to the VNFM, e.g. the identifier of the VNF(s), the related LCM operation(s) that can be granted for them and the capacity authorized for this VNF are included.

Annex B (informative): Bibliography

ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV); Management and Orchestration; Functional Requirements Specification" .

ETSI GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture".

Annex C (informative): Authors & contributors

The following people have contributed to the present specification:

Rapporteur:

Peter Wörndle, Ericsson

Michael Brenner, ClearPath Networks

Other contributors:

Bruno Chatras, ORANGE

Joan Triay, DOCOMO Communications Lab

Kazuaki Obana, DOCOMO Communications Lab

Xia Haitao, Huawei

Amanda Xiang, Huawei

Marc Flauw, Hewlett-Packard Enterprise

Susana Sabater, Vodafone

Uwe Rauschenbach, Nokia Networks

Dmytro Gassanov, NetCracker

Chu Junsheng, ZTE Corporation

Michael Klotz, Deutsche Telekom AG

History

Document history		
V1.1.1	July 2016	Publication