ETSI GS NFV-IFA 036 V4.3.1 (2022-09)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for container cluster management and orchestration specification

Disclaimer

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

Reference

DGS/NFV-IFA036

Keywords

container, management, MANO, NFV,
orchestration, virtualisation

ETSI

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

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

Siret N° 348 623 562 00017 - 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:
http://www.etsi.org/standards-search

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

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

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

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

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.

© ETSI 2022.
All rights reserved.

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

Modal verbs terminology

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

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

1 Scope

The present document specifies requirements on Container Infrastructure Service (CIS) cluster management services and descriptors associated to CIS cluster management. The requirements apply to:

- CIS Cluster Management (CCM) service interfaces provided by the CCM function:
    - CIS cluster lifecycle management
    - CIS cluster configuration management
    - CIS cluster performance management
    - CIS cluster fault management
    - CIS cluster security management
- Service interfaces provided by the Container Infrastructure Service Management (CISM) function:
    - CIS instance management
    - Managed CIS Cluster Objects (MCCOs) management

2 References

2.1 Normative references

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

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

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

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

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

[2] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification".

2.2 Informative references

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

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

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

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

[i.2] ETSI GR NFV-IFA 029: " Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"".

[i.3] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.4] ETSI GS NFV-SOL 005: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point".

[i.5] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[i.6] CNI™: "The Container Network Interface Documentation".

NOTE: Available at https://www.cni.dev/docs/.

[i.7] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.8] ETSI GR NFV-IFA 038: "Network Functions Virtualisation (NFV) Release 4; Architectural Framework; Report on network connectivity for container-based VNF".

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

[i.10] ETSI GS NFV-IFA 014: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Network Service Templates Specification".

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] and the following apply:

CIS cluster: set of CIS instances, and one or multiple CISM instances managing them

NOTE: At minimum, the CIS cluster contains one CISM instance and one CIS instance.

CIS cluster enhancement capability: MCCO that provides additional capabilities to a CIS cluster

NOTE: Clause C.2 introduces various examples of CIS cluster enhancement capabilities.

CIS cluster management: management of one or more CIS clusters

NOTE: The CIS cluster management provides lifecycle management and FCAPS management of CIS clusters.

CIS cluster node: compute resource that runs a Container Infrastructure Service (CIS) instance or a Container Infrastructure Service Management (CISM) instance, or both

NOTE: The CIS cluster node can be either physical (e.g. a bare-metal server), or virtual (e.g. a virtual machine).

CIS cluster nodes network: network connecting part of or the whole set of CIS cluster nodes conforming the CIS cluster

CIS cluster storage: set of storage resources attached to one or multiple CIS clusters

daemon object: MCCO triggering a background process to run in the CISM

NOTE: Clause C.3 introduces examples of daemon objects.

hybrid CIS cluster: CIS cluster composed of a mixture of virtual and bare-metal CIS cluster nodes

managed CIS cluster object: abstract NFV object for CIS cluster management characterized by its configuration, state, requested and allocated infrastructure resources, and applicable operational policies

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:

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

BGP	Border Gateway Protocol
CCD	CIS Cluster Descriptor
CCEC	CIS Cluster Enhancement Capability
CCM	CIS Cluster Management
CCND	CIS Cluster Node Descriptor
CCNRD	CIS Cluster Node Resource Descriptor
CE	Customer Edge
CIDR	Classless Inter-Domain Routing
CNI™	Container Network Interface
DC	Data Centre
DHCP	Dynamic Host Configuration Protocol
FCAPS	Fault management, Configuration management, Account management, Performance management and Security management
IPAM	IP Address Management
L2NW	Layer 2 Network
LB	Load Balancer
LUN	Logical Unit Number
MCCO	Managed CIS Cluster Object
PV	Persistent Volume
RBAC	Role Based Access Control
SDN	Software-Defined Networking
ToR	Top of Rack

4 Overview and background

4.1 Problem statement

The present document focuses on the following issues to provide a complete standard solution for the introduction of containerized VNF management in NFV-MANO.

- Current industry solutions for OS container management expect that a cluster of worker machines (running either in virtual machines or on bare-metal servers) is provided for their use. In an NFV environment the cluster of worker machines is provided by the NFVI and the corresponding resources are allocated by NFV-MANO. The CISM is configured to use these worker machines for the deployment and management of the containerized workloads.

- In case that worker machines are bare-metal servers, current industry solutions typically handle the configuration of the worker machines to be used by the CISM manually, which is not an optimal solution.

- Containerized workloads of different VNFs might need to be provided with a certain level of separation or isolation. The correct mapping of isolation requirements between containerized workloads as defined via the NFV templates (e.g. containerized workloads of different VNFs, specified co-location or separation as defined in affinity/anti-affinity groups) is not addressed in the referenced documentation.

- With containerized workloads, bare-metal deployments become also an important deployment form. CIS instances for hosting the containerized workloads can not only be virtual machines as they can be allocated via the VIM, but also bare-metal servers. The architectural options supporting the allocation of physical resources for hosting the OS containers is unspecified.

- Open source solutions for OS container platforms, e.g. Kubernetes® provide capabilities for flexible management of cluster-wide capabilities and features.
  It is not practical to provide these capabilities only as part of the software images used during the CIS cluster creation. A mechanism that enables the cluster administrator to dynamically add or remove such features or capabilities on a running CIS cluster is still unspecified.

The present document introduces concepts and functionality to address these gaps.

4.2 Introduction

4.2.1 General principles for CIS clusters and their management

Current industry solutions for OS container management provide solutions for grouping the compute resources that containerized workloads are deployed on. The CISM as described in ETSI GS NFV-IFA 040 [1] provides the OS container management services to manage the containerized workloads represented by Managed Container Infrastructure Objects (MCIOs). The CISM depends on having a set of compute resources to deploy the CIS instances and the containerized workloads. The present document specifies the services for the management of these sets of compute resources and to make these resources available for the use by CISM.

In the scope of the present document and NFV-MANO, the term CIS cluster node is used for such a compute resource and in accordance with ETSI GR NFV-IFA 029 [i.2], and the term CIS cluster is used to refer to a set of resources including CIS instances and CISM instances using these compute resources as well as storage and network resources.

The functional requirements for the CIS Cluster Management (CCM) services and the CISM services specified in ETSI GS NFV-IFA 010 [2] shall apply.

- CIS cluster node:

  Each CIS cluster node in the role of a worker machine hosts a CIS instance as introduced in ETSI GR NFV-IFA 029 [i.2]. This includes the container runtime environment with the capabilities supporting the containerized workloads. The CISM schedules containerized workloads on the CIS instances of a CIS cluster. CIS cluster nodes can also be used as control nodes and then host the CISM.

  CIS cluster nodes can be realized as virtual machines or as bare-metal servers. See clause 4.2.5 for more details.

- CISM instances and CIS instances:

  CISM instances and CIS instances can be deployed using software images that provision the initial configuration. In this initial deployment, the CCM interacts directly or indirectly with infrastructure managers (e.g. the VIM) to allocate resources for the CIS cluster nodes, networks and storage, deploys the initial software and instantiates CISM and CIS instances. Scaling and upgrade of a CIS cluster are performed similarly. In addition, the CCM can deploy and configure additional CIS cluster capabilities (i.e. CIS Cluster Enhancement Capabilities (CCEC), see clause 4.2.14) that are delivered separately from the CIS cluster, and instantiated and configured separately.

- CIS cluster as an NS:

  CIS clusters can themselves, but need not, be deployed and managed as Network Services (NSs). A CCM deploying and managing CIS clusters where CIS cluster nodes are virtual machines consumes the interfaces exposed by VIM as defined in ETSI GS NFV-IFA 005 [i.3] or the interfaces exposed by an NFVO as defined in ETSI GS NFV-IFA 013 [i.5]. The latter case applies when CIS clusters are deployed and managed as NSs (see clause B.3). In that case the CIS and CISM functionality are provided by the constituent VNFs and the CCM plays the Element Management (EM) role with regards to these VNFs.

- Declarative descriptors:

  CIS clusters and CIS cluster nodes are described by declarative descriptors that describe resources, reference the initial software images, provide scaling limits, etc. CIS clusters and CIS cluster nodes can be modified or upgraded via CIS cluster LifeCycle Management (LCM) operations. More information on declarative descriptors for CIS clusters and CIS cluster nodes is available in clauses 6.2.1, 6.2.2 and 6.3.2, respectively.

  CCECs are also described by declarative descriptors. The CCM manages the provisioning of the CCECs together with the CISM instance of a CIS cluster and provides the necessary operations to the CCM Consumer. See clause 4.2.14.

4.2.2 Lifecycle Management for CIS clusters

A CIS cluster is composed of CIS instances and CISM instances hosted on one or multiple CIS cluster nodes. The number of CIS cluster nodes belonging to the CIS cluster is variable according to dynamic changes of compute resources consumed by the containerized workloads running on the CIS instances of the CIS cluster. Therefore, the CIS cluster has its own lifecycle and can be managed by NFV-MANO functional entities to match the dynamics in consuming compute resources in the CIS cluster.

Lifecycle management of CIS clusters includes the following aspects:

- Creating CIS cluster: A CIS cluster is newly created in the NFV-MANO domain.
- Modifying CIS cluster: A CIS cluster is modified, e.g. change of the CIS cluster information or configuration, scaling the CIS cluster (e.g. by addition or removal of resources of the CIS cluster), or modification of CIS cluster software.
- Deleting CIS cluster: A CIS cluster is deleted.
- Querying CIS cluster: The information of a CIS cluster is queried.
- Subscription/Notification related to CIS cluster management: Consumers of CIS cluster management services subscribe to receive notifications about changes related to CIS clusters. Notifications are sent to Consumers when their subscribed events occur.

Before a CIS cluster is created, the CCM creates an identifier that the Consumer and the NFVO can use in further operations on the CIS cluster and to identify the CIS cluster in placement decisions. The CCM also provides the Consumer with address information of the CISM services available in the new CIS cluster.

The Consumer can assign also a name to the CIS cluster.

4.2.3 Placement of CIS clusters and resources

The components of a CIS cluster (i.e. the CISM instances and CIS instances) are placed on CIS cluster nodes which provide compute resources for running the CISM instances and CIS instances. A CIS cluster node is either a virtual machine or a bare-metal server, and hosts a CISM instance, or a CIS instance or both. The CIS cluster is scaled out or scaled in with increased or decreased number of CIS cluster nodes belonging to that CIS cluster, in which the newly-added or deleted CIS cluster nodes, host CIS instances or CISM instances.

The CCM Consumer defines placement constraints for a CIS cluster during CIS cluster creation or update. The placement constraints can be defined in a similar way as for the placement of VNFs. The CCM Consumer can define affinity or anti-affinity with different scopes (the NFVI-PoP, zone, zone group or NFVI-node level). Also, constraints for specific geographic location can be defined in the same way as for a VNF. The placement and affinity/anti-affinity constraints are also further processed by the NFVO to determine the exact placement, e.g. one or a set of specific resource zones in the NFVI, during the resource granting exchange that the CCM can perform against the NFVO.

Such placement and affinity/anti-affinity constraints can be defined as strict or be interpreted as best effort.

The CCM Consumer defines whether a CIS cluster is requested to be deployed on physical or virtual CIS cluster nodes, i.e. bare-metal servers or virtual machines, and other requirements on the CIS cluster nodes, e.g. available hardware acceleration capabilities. A CIS cluster can also be "hybrid" and include both physical and virtual CIS cluster nodes. Clause 4.2.5 provides further considerations regarding hybrid CIS clusters.

It is the responsibility of the CCM to request the allocation of the infrastructure resources matching the placement constraints for the CIS cluster nodes, either by interacting directly or indirectly with the VIM or other infrastructure resource manager function (e.g. the entity responsible for the management of physical resources) or by providing infrastructure resources from an internal pool, e.g. in case of bare-metal servers available only for that CCM.

4.2.4 CIS cluster characteristics

A CIS cluster is characterized by a series of attributes which describe the CIS cluster in terms of deployment and operational behaviour requirements, and that are defined in the CIS Cluster Descriptor (CCD, refer to clause 6.2.1). The CIS cluster characteristics includes the following aspects:

- Size of the CIS cluster, i.e. the maximum and minimum number of CIS cluster nodes a CIS cluster can possess.
- Description of CIS cluster nodes to be used by the CIS cluster, refer to the information on the CIS cluster node in the CIS Cluster Node Descriptor (CCND) of clause 6.2.2.
- Scaling characteristics of the CIS cluster, e.g. allowed range of steps or levels applied for the scaling of the CIS cluster, represented by the minimum and maximum value of steps or levels.
- Affinity and anti-affinity rules associated to the CIS cluster, describe the relationship of affinity and anti-affinity between the components of the CIS cluster (i.e. CISM instances and CIS instances).
- Placement constraints for deploying the CIS cluster.
- Description related to CIS cluster networking aspects, refer to clause 4.2.6 for more information about CIS cluster networking and clause 6.2.1 for information on the network resources defined in the CCD in clause 6.2.1.
- CIS cluster storage description, refer to clause 4.2.7 for more information about CIS cluster storage aspects and clause 6.2.1 for information on the storage resources defined in the CCD.

During CIS cluster lifecycle, the CCM keeps track of CIS cluster runtime characteristics including but not restricted to the following information:

- Identification and name of the CIS cluster
- Information about how to consume the CISM service in the cluster and available CISM services
- Identifier of the CCD
- Current size of the CIS cluster, i.e. current number of CIS cluster nodes, CISM instances and CIS instances
- Placement information of the CIS cluster nodes, i.e. actual location, labels of the nodes, etc.
- Resource characteristics of the CIS cluster nodes, e.g. acceleration capabilities
- Status information of the CIS cluster, CIS instances, CISM instances and their resources
- Information about networks and storage part of or associated to the CIS cluster
- Information about the CCECs of the CIS cluster

The CCM provides means for its Consumer to query that information. There can be other runtime information related to the CIS cluster and its services that can be obtained via the CISM of the CIS cluster. The information includes but not be restricted to the following:

- Information of the namespaces associated to the CIS cluster, as specified in clause 6.7 of ETSI GS NFV-IFA 040 [1]
- Information about MCCOs instantiated on the CIS clusters (see clause 4.2.13)

4.2.5 Virtual and Bare-metal CIS clusters

4.2.5.1 Introduction

CIS clusters can be based on virtualised or physical compute resources. A CCM can be able to manage both virtual and bare-metal CIS clusters from the same pool of physical resources; or virtualised and physical compute resources can be used together in the same CIS cluster, i.e. a hybrid CIS cluster.

4.2.5.2 Virtual CIS clusters

Compute resources for virtual CIS clusters can be allocated via the standardized VIM interfaces, see ETSI GS NFV-IFA 005 [i.3]. In this case each CIS cluster node is a VM. The VMs can be deployed on the same or different physical servers as it is specified in the placement constraints.

The CIS Cluster Node Resource Descriptor (CCNRD) specifies the characteristics for the virtualised resource, i.e. the VM, and requirements on capabilities supported by the server hosting the VM, e.g. acceleration capabilities.

Clause B.2 illustrates the workflow to create a CIS cluster, which includes the case of using virtual compute resources.

4.2.5.3 Bare-metal CIS clusters

In case of bare-metal CIS clusters (bare-metal deployments), each CIS cluster node covers a bare-metal server, completely assigned to this role and the container platform (the CISM or CIS or combined) is executed on the operating system of this physical compute resource.

The allocation of the bare-metal servers can be done via other infrastructure management function. Such an infrastructure management function enables allocating bare-metal servers to a CIS cluster.

NOTE 1: A potential example of infrastructure management function is the "bare-metal service" of OpenStack®.

NOTE 2: The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. ETSI is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

NOTE 3: As an alternative, CCM implementations can include a functionality to manage a pool of pre-configured physical servers that can be dynamically assigned to CIS clusters, or there can be a separate function that manages a pool of hardware resources and can assign bare-metal servers from that pool to Consumers.

NOTE 4: Bare-metal servers provide a logical abstract layer that represents the physical resources.

The CCM is responsible to make sure the CIS cluster nodes match the requested capabilities according to the CCNRD, to deploy the necessary software for the CISM or CIS instance on the CIS cluster nodes as specified in the CIS cluster node descriptor, see clause 6.2.2, and to initiate the necessary configuration steps.

The CCNRD (see clause 6.2.3) specifies the hardware characteristics of the bare-metal server to be allocated.

Clause B.2 illustrates the workflow to create a CIS cluster, which includes the case of using bare-metal servers.

4.2.5.4 Hybrid CIS clusters

A CIS cluster can be "hybrid" and include both physical and virtual CIS cluster nodes. Physical CIS cluster nodes are typically fulfilled by the provisioning of bare-metal servers, as described in clause 4.2.5.3. Virtual CIS cluster nodes are typically fulfilled by the instantiation and provisioning of VMs on the NFVI.

For the creation of hybrid CIS clusters, pooling of CIS cluster nodes is performed against the VIM for VM (as in clause 4.2.5.2) and other infrastructure management functions for bare-metal servers, as indicated in clause 4.2.5.3. Depending on the capabilities of the infrastructure management functions for bare-metal servers, pooling of such servers is only done from existing installed servers. Whereas for the case of VM, more dynamic creation, update and termination of CIS cluster nodes and their pooling into the CIS cluster is typically supported.

Storage resources are also considered for pooling as described in clause 4.2.7.

A key aspect in hybrid CIS clusters concerns to the networking: the one or more pools of bare-metal servers and the one or more pools of VMs that are targeted for inclusion into the same CIS cluster are expected to have network connectivity:

- for the control plane to properly operate among CISM and CIS instances; and
- for the data plane to connect between sets of one or multiple OS containers, which is fulfilled by the primary container cluster internal network.

Clause 4.2.6.2 describes the concept of CIS cluster nodes network.

The capability to define requirements or characteristics of the CIS cluster nodes specific for bare-metal server or VM is supported by the CCNRD. In the case of a hybrid CIS cluster, information on the CIS cluster nodes to run CISM instances and/or CIS instances includes references to CCNRD for bare-metal server and VM.

4.2.6 Networking

4.2.6.1 Overview

Regarding CIS cluster networking, three types of networks are considered:

- the one or more networks connecting the set of CIS cluster nodes conforming the CIS cluster, referred hereafter as "CIS cluster nodes network";
- the one or more networks that serve the purpose to interconnect groups of one or more OS containers, e.g. Pod with OS containers, deployed on different CIS cluster nodes, referred hereafter as "container cluster network"; and
- the one or more networks that connect the CIS cluster to external networks outside the CIS cluster, which allows groups of one or more OS containers, deployed on the CIS cluster to be reachable from outside the CIS cluster and the applicable groups of one or more OS containers to also access networks outside the CIS cluster, referred hereafter as "cluster external network".

4.2.6.2 CIS cluster nodes network

The network that connects the CIS cluster nodes can be realized either as physical network or virtual network. When the CIS cluster is created by the CCM (see also clause B.2), 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.

In the case of bare-metal CIS cluster, connectivity between CIS cluster nodes can be performed either with physical network or virtual network with L2 and L3 connectivity. The CIS cluster nodes can be placed into one or more infrastructure provider networks pre-configured via a networking service such as a Software-Defined Networking (SDN) solution.

In the case of VM-based CIS cluster, a virtual network is created to connect the VMs which are setup as CIS cluster nodes. As an example with OpenStack®, the virtual network can either be a tenant (or self-service) network or an infrastructure provider network.

In the case of hybrid CIS cluster (bare-metal and VM), connectivity between CIS cluster nodes can be performed with either L2 or L3 infrastructure provider networks, which enable VMs either L2 or L3 connectivity which is mapped to existing L2 or L3 networks in the infrastructure, e.g. in the NFVI-PoP (or site, data center).

To provide access to the CISM of the CIS cluster, the CCM configures an IP address or DNS name representing the endpoints of CIS cluster control management (part of the CISM). The IP address to configure is the IP address of the CIS cluster node hosting the CIS cluster control management endpoint; such IP address is assigned as part of the CIS cluster nodes network configuration. In configurations with multiples CISM instances, the IP address to configure can also be an outside (other than a CIS cluster node) Load Balancer (LB)'s exposed IP address.

4.2.6.3 Overview of container cluster network

As introduced by ETSI GR NFV-IFA 038 [i.8], there are different types of container cluster networks:

- Primary container cluster internal network: network that is not exposed external to the CIS cluster and to which all OS containers deployed within the CIS cluster are connected through their primary network interface.
- Primary container cluster external network: a network that is exposed external to the CIS cluster to which OS containers deployed within the CIS cluster are connected indirectly via a primary network interface, through native capabilities of the underlying container infrastructure.
- Secondary container cluster internal network: a network that is not exposed external to the CIS cluster and to which OS containers deployed within the CIS cluster are connected via an additional network interface other than their primary network interface.
- Secondary container cluster external network: network that is exposed external to the CIS cluster to which OS containers deployed within the CIS cluster are connected directly via additional network interfaces other than the primer network interface.

Whether a CIS cluster contains secondary container cluster networks depends on the connectivity requirements of VNF and NS deployments and operational policies.

Table 4.2.6.3-1 summarizes the types of container cluster networks, their characteristics and dependencies on the CIS cluster nodes network and cluster external networks.

Table 4.2.6.3-1: Summary of container cluster networks

Type	External connectivity	Dependencies
Primary container cluster internal network	No	CIS cluster nodes network
Primary container cluster external network	Yes	CIS cluster nodes network, and cluster external network
Secondary container cluster internal network	No	CIS cluster nodes network
Secondary container cluster external network	Yes	CIS cluster nodes network, and cluster external network

Figure 4.2.6.3-1 illustrates examples on the types of container cluster networks and the CIS cluster nodes network.

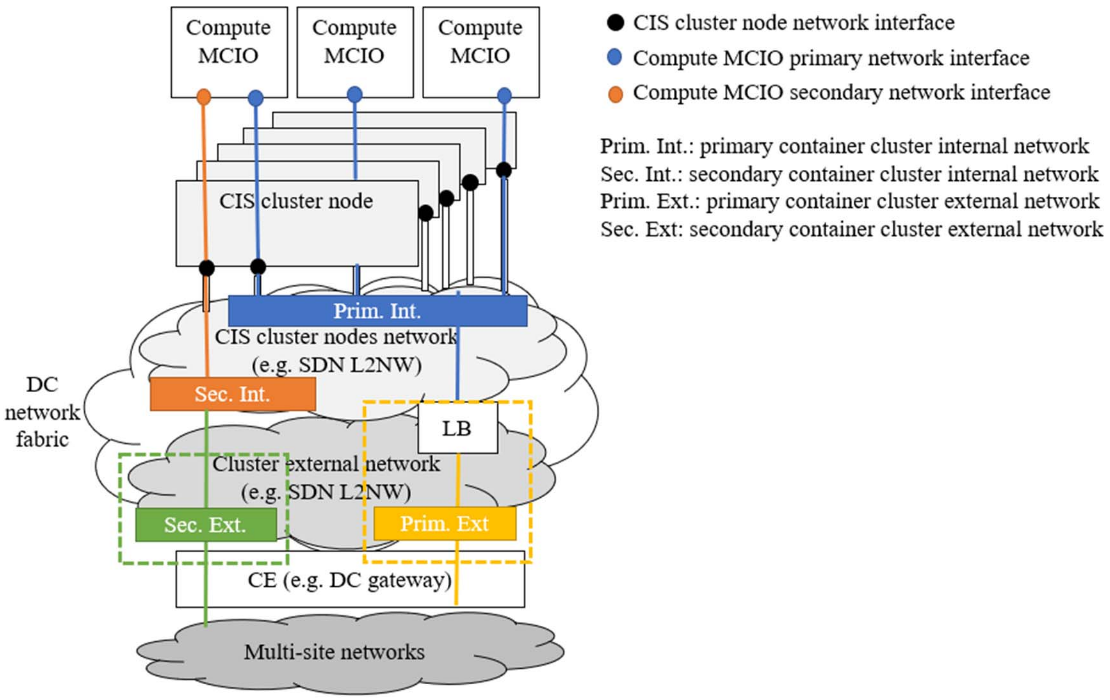
Compute MCIO
Compute MCIO
Compute MCIO
● CIS cluster node network interface
● Compute MCIO primary network interface
● Compute MCIO secondary network interface
Prim. Int.: primary container cluster internal network
Sec. Int.: secondary container cluster internal network
Prim. Ext.: primary container cluster external network
Sec. Ext: secondary container cluster external network
CIS cluster node
Prim. Int.
CIS cluster nodes network (e.g. SDN L2NW)
DC network fabric
Sec. Int.
LB
Cluster external network (e.g. SDN L2NW)
Sec. Ext.
Prim. Ext
CE (e.g. DC gateway)
Multi-site networks

Figure 4.2.6.3-1: Types of container cluster network on setup on CIS cluster

4.2.6.4 CIS cluster networking aspects

Following are key aspects to be considered by the CCM when configuring the CIS cluster for enabling connectivity for OS containers on a CIS cluster, and thus become parts of designing the networking aspects of CIS clusters:

1) IP address management, necessary to create an overall address space for the virtual networks (typically implemented as bridges) on each CIS cluster node.

2) Forwarding (routing or switching) of packets (frames) from/to the virtual networks/bridges of the CIS cluster nodes through the network connecting the CIS cluster nodes.

In addition, if the container cluster network (either primary or secondary) is to be enabled to have access external to the CIS cluster, then an additional key element is:

3) Forwarding of packets from/to the virtual networks/bridges of the CIS cluster nodes to external networks.

Table D.1-1 in clause D.1 lists solutions and examples for the set of aspects described above.

The connectivity of the groups of one or more OS containers to the container cluster network can be performed in different forms. The configuration and availability of the plugins that enable such mechanisms is part of the CIS cluster nodes configuration performed by the CCM. Table D.2-1 in clause D.2 provides a list of common solutions to enable the network interfaces for the groups of one or more OS containers.

4.2.6.5 Means for configuring CIS cluster networking

There are two means by which configuration aspects of CIS cluster networking can be performed:

- Static configuration: in this case, the CCM configures the networking aspects on the relevant CIS cluster nodes, including the CISM.

- Dynamic configuration: in this case, the CCM, by means of the CISM of the CIS cluster, requests setting daemon objects on the relevant CIS cluster nodes which upon actual container cluster network creation or modification requests perform the necessary configuration on the actual CIS cluster nodes and on the groups of one or more OS containers.

EXAMPLE: Certain network plugins can be deployed and configured by using daemon objects.

4.2.6.6 CIS cluster networking for primary container cluster networks

The present clause provides more details regarding the specific considerations for setting up the primary container cluster networks and the role of the CCM in their configuration.

The following steps illustrate how primary container cluster network is set up:

1) As described in clause 4.2.6.2, the CCM requests the infrastructure managers (e.g. VIM) the creation and/or configuration of the CIS cluster nodes network as part of the CIS cluster creation or updates. Requirements about the association of the CIS cluster nodes network with network interfaces of the CIS cluster nodes can be provided, e.g. bandwidth and capabilities of the interfaces. For further configuration steps, the CCM is expected to know what network interfaces are associated to what CIS cluster nodes networks.

2) The CCM administers the CIS cluster networking by requesting the CISM to apply the network configuration for the primary container cluster internal network. This typically involves applying the configuration provided via a manifest configuration file. The network configuration to provide is dependent on the type of container networking plugin of choice for the container infrastructure platform and it can include variables such as the type of overlay backend to use (e.g. VXLAN or IP-in-IP), the primary container cluster network Classless Inter-Domain Routing (CIDR), the association to CIS cluster node network interfaces, etc.

3) In the case that CIS cluster node creation steps have not installed necessary network plugin and plugin control executables, or that alternative plugins are to be used, then the CCM installs the necessary network plugin and plugin control executables. The installation of the executables can be performed in various ways depending on the networking plugin of choice for the container infrastructure platform (e.g. CCM login into CIS cluster nodes and installing the plugin, CCM requesting to the CISM to deploy the executable on CIS cluster nodes via some daemon object, etc.).

In addition, the following steps illustrate how to enable primary container cluster external networking:

4) Different sub-cases are considered:

   a) In the case of using an infrastructure provider load balancer solution, the CISM is configured with the appropriate infrastructure provider controller to enable the CISM to request the setup of the external load balancer. In this case, the CISM can directly interact with the infrastructure manager (e.g. VIM) for the setup and configuration of the load balancer.

   b) In the case of using actual external network reachability of CIS cluster nodes, the CIS cluster nodes network that has been created or configured on the step 1 is also configured to correspondingly route the traffic from/to external network of the CIS cluster. It is assumed that the setup of the relevant network resources in the NFVI-PoP or data center is either pre-provisioned or if the provisioning is dynamic and takes place during the CIS cluster lifecycle management, the following two cases regarding the management of the external connectivity with corresponding network resources referred as "NFVI-PoP network gateway" are possible:

      i) The NFVO is responsible for preparing the configuration and requesting, either directly or via the VIM, the NFVI-PoP network gateway, during the steps of resources granting established between the CCM and the NFVO.

      ii) The CCM is granted access to and becomes responsible for preparing the configuration and requesting, either directly or via the VIM, the NFVI-PoP network gateway.

NOTE: Clause E.1.2 of ETSI GS NFV-SOL 005 [i.4] provides additional information about the management models of NFVI-PoP network gateway (or also referred as Customer Edge (CE) or Data Centre (DC) gateway) in the context of multi-site network connectivity.

   c) In the case of using L7 load-balancing solution, an ingress controller is deployed on the CIS cluster which in addition can have dependency on some infrastructure provider LB (see point a)).

4.2.6.7 CIS cluster networking for secondary container cluster networks

The present clause provides more details regarding the specific considerations for setting up the secondary container cluster networks and the role of the CCM in their configuration.

The steps for setting up the corresponding networks are in addition to the steps for setting up the primary container cluster internal network in clause 4.2.6.6, as these steps are typically a pre-condition for enabling the setup of the artifacts and plugins for configuring the secondary container cluster networks. Also, these steps are only necessary when secondary container cluster networks are needed.

The following steps illustrate additional steps for setting up the secondary container cluster networks:

1) The CCM requests the CISM to install the network configuration for the secondary container cluster internal network. This typically involves applying the configuration provided via a manifest configuration file and the installation of network plugins and/or plugin control executables.

2) The actual creation of the secondary container cluster network takes place by the NFVO requesting to the CISM the creation of a secondary network definition resource. For a secondary container cluster internal network (i.e. without access to external networks), the network configuration properties conform to the L3 (IP configuration) of a CIS cluster nodes network without external access.

For enabling secondary container cluster external networking, the following applies:

3) The NFVO requests to the CISM the creation of a secondary network definition resource (as in step 2), but in this case the network configuration properties conform to the L3 (IP configuration) of a CIS cluster nodes network with external access.

4.2.7 Storage

The CCM is responsible for providing storage space as part of a CIS cluster based on the storage resource requirements in the CIS cluster descriptors. The CCM provides the storage to the CISM instances for use by containerized workloads according to the declarative descriptors for the storage MCIOs.

Containerized workloads might use persistent and/or ephemeral storage. NFV-MANO provides persistent storage resources which all CIS cluster nodes can access in two operational steps, pooling and provisioning:

- Pooling: Storage resources are pooled as virtualised resources or external storage, and inventoried, e.g. network file system, virtual volume created by the VIM, software defined storage.

- Provisioning: Pooled virtualised resources or external storage are split and provisioned as CIS cluster storage resources, e.g. persistent volumes. The amount of CIS cluster storage is expected to fulfil the demands of storage resources requested by the containerized workloads running on the CIS cluster.

With the CIS cluster provisioned storage, the containerized workloads can further make use of these storage resources by claiming them, a process by which provisioned storage resources are associated with the containerized workloads and managed as Storage MCIOs by the CISM.

The present clause describes how the CCM creates and manages persistent storage resources for the CIS cluster.

The CCM is responsible for the pooling of storage resources. The CCM requests storage resources (e.g. creating a storage resource pool by using AllocateStorageRequest defined in clause 7.5.1 of ETSI GS NFV-IFA 005 [i.3]) to an infrastructure manager after requesting granting to the NFVO with information related to profiles of storage, e.g. StorageClassName. After creating the storage resource pool, the CCM can access to the storage resource pool and retrieve information about the storage Logical Unit Number (LUN) and consumption of the created storage resource pool.

The CCM is also responsible for the provisioning of storage resources based on CIS cluster descriptors which describe information about capacity, type, name and placement control of storage resources to be provisioned. Based on information from the storage resource requirement described in the CIS cluster descriptors, the CCM configures on the applicable CIS clusters the set of provisioned storage resources (e.g. storage volume resources which abstract the pooled physical or virtual storage resources).

EXAMPLE: In Kubernetes® environment, the creation of one or more Persistent Volume (PV) is performed as part of the provisioning.

The CCM can also support dynamic provisioning of storage resource. For this case, the CCM configures the CIS cluster and the CISM to be capable for dynamic provisioning. On the one hand, in case of static provisioning, storage resources are independently provisioned in advance to execution of lifecycle of the relevant containerized workloads; on the other hand, in case of dynamic provisioning, storage resource provisioning is performed by the CISM as a part of lifecycle of the relevant containerized workload just before the containerized workloads are deployed.

In addition, the CCM provides information related to profiles of storage, e.g. storage classes, which are provisioned to the CIS cluster.

NFVO knows how many storage resources are consumed from the total NFVI capacity, how many storage resources are added into the CIS cluster and what profiles of storage CCM specifies. In addition, the NFVO can query the CISM or receive notifications from the CISM, via the CIS MCCO management interfaces, about the configured and provisioned storage resources into the CIS cluster which are exposed as managed objects by the CISM. NFVO can consider the retrieved information to fulfil placement constraints such as affinity/anti-affinity rules in the CIS cluster selection and VNF placement procedure (see clause 4.2.8) and track storage resource capacity consumption.

A new descriptor is introduced to contain the attributes needed for persistent volumes (e.g. storage class, size), so the CCM can provision the storage which can subsequently be used by the containerized workloads. In the case of dynamic provisioning, the amount of storage resources to be consumed by the relevant containerized workloads is determined just before the containerized workloads are deployed.

The CCM monitors consumption of storage resources provided by CIS cluster nodes, and the CCM notifies the shortage of storage resources when the consumption of storage resources is over the thresholds. The CCM Consumer can also set capacity thresholds associated to the storage resources of a CIS cluster.

NOTE: The present document supports the case that pooled and provisioned storage resources are consumed by only one CIS cluster.

4.2.8 CIS cluster selection and VNF placement

During VNF instantiation, NFV-MANO selects a CIS cluster, so that a specific CISM instance is indirectly selected for the instantiation of the containerized workloads for the VNF. Consequently, a VNFM requests creation of the MCIOs from a specified CISM instance.

NOTE: The present document version supports the case that only one CIS cluster is selected for deploying the one or more containerized workloads for the VNF.

An NFVO selects the CIS cluster according to NS and runtime information of relevant CIS clusters. The information regarding a CISM connection is transferred over the Or-Vnfm reference point using the "VimConnectionInfo" defined in clause 8.12.5 of ETSI GS NFV-IFA 007 [i.7].

At any time, but in particular latest during the VNF LCM granting exchange, the NFVO collects relevant CIS clusters information which is expected to be used for CIS cluster selection. The NFVO uses the interfaces exposed by the CISMs and a CCM in order to collect such information. CISM exposes information of the CIS cluster as logical entities of CISM and CIS instances, while the CCM exposes information of the CIS cluster as CIS cluster node entities. The NFVO performs the CIS cluster selection based on:

- the collected information from CISM and CCM;
- the location constraints information that the NFVO receives from the OSS/BSS as part of the NS LCM requests and the affinity/anti-affinity rules among NS constituents (e.g. VNF) at the NS level defined via the NSD of the NS to instantiate; and
- the resource requirements expressed in the VNFD of the VNFs to instantiate.

EXAMPLE 1: If a VNF expects to leverage SR-IOV capabilities, it is expected that the NFVO selects a CIS cluster that knows either all or a subset of the CIS cluster nodes have SR-IOV capable network interface cards which fulfil the amount and capacity of requested resources.

As specified by the "mcioConstraintParams" attribute of the "Vdu" information element in clause 7.1.6.2 of ETSI GS NFV-IFA 011 [i.9], specific types of constraints can be defined to influence the deployment of the containerized workloads for the VNF. As defined in the "mcioConstraints" attribute of the "GrantInfo" information element in clause 8.3.3 of ETSI GS NFV-IFA 007 [i.7], the value in the key-value pair indicates the value to be assigned to the MCIO constraint according to the specified list of possible enumeration values defined for the key in the key-value pair.

The values in the "mcioConstraints" key-value are determined based on the "tagging" (or also referred as "labeling") of the CIS cluster nodes.

CIS cluster node tags provide characterization information of each CIS cluster node. By referencing such tags, a CISM determines a CIS cluster node which can be used to deploy one or more of the containerized workloads for the VNF.

Regarding the values of the tags, these can be determined by the CCM Consumer based on certain operational policies or rules. However, the tags and values set to the CIS cluster nodes are expected to convey semantically the constraint scopes according to the "mcioConstraintParams".

Table 4.2.8-1 summarizes the minimum set of expected supported CIS cluster node tagging scopes.

Table 4.2.8-1: Summary of supported CIS cluster node tagging scopes

Scope	Correspondence with ETSI GS NFV-IFA 011 [i.9]	Description
NFVI-PoP	affinityNfviPop, antiAffinityNfviPoP, localAffinityNfviPop, localAntiAffinityNfviPop	To indicate in which NFVI-PoP the CIS cluster node is placed.
Zone	affinityZone, antiAffinityZone, localAffinityZone, localAntiAffinityZone	To indicate in which resource zone of the NFVI-PoP the CIS cluster node is placed.
ZoneGroup	affinityZoneGroup, antiAffinityZoneGroup, localAffinityZoneGroup, localAntiAffinityZoneGroup	To indicate in which resource zone group of the NFVI-PoP the CIS cluster node is placed.
NFVI-node	affinityNfviNode, antiAffinityNfviNode, localAffinityNfviNode, localAntiAffinityNfviNode	To indicate in which NFVI-node the CIS cluster node is placed. This applies in the case of VM-based CIS cluster nodes.
CIS-node	affinityCisNode, antiAffinityCisNode, localAffinityCisNode, localAntiAffinityCisNode	To differentiate among CIS cluster nodes, e.g. by using different node hostnames.
SSD device capability	nodeAdditionalCapabilitySsd	To indicate if the CIS cluster node has SSD devices(s).
DPDK driver capability	nodeAdditionalCapabilityDpdk	To indicate if the CIS cluster node has DPDK driver capability.
SR-IOV capability	nodeAdditionalCapabilitySriov	To indicate if the CIS cluster node has SR-IOV card(s).
GPU acceleration capability	nodeAdditionalCapabilityGpu	To indicate if the CIS cluster node has GPU acceleration device(s).
FPGA capability	nodeAdditiionalCapabilityFpga	To indicate if the CIS cluster node has FPGA device(s).
CPU pinning capability	nodeAdditionalCapabilityCpuPin	To indicate if the CIS cluster node has CPU pinning capability.
Logical NUMA capability	nodeCapabilityLogicalNuma	To indicate if the CIS cluster node has logical NUMA architecture capability.
Pooled nodes	nodePool	To indicate if the CIS cluster node belongs to a pool of CIS cluster nodes with same capabilities.

The CCM manages and is responsible for the CIS cluster node tagging. The timings to configure the CIS cluster node tags are the following:

- Creation of CIS cluster: the CCM takes care of management and configuration operation about tagging CIS cluster nodes. Concerning the management, the CCM collects information about which CIS cluster node is expected to be assigned with which tag. Concerning the configuration operation, the following two sub-cases are possible:

    - The CCM accesses the CIS cluster node and configures its tagging information. This case is relevant for CIS cluster node tagging of physical CIS cluster nodes.

  - The CCM can configure the tagging information on the CIS cluster node via day-0 configuration mechanisms (e.g. boot data) supported by the VIM. This case is relevant for CIS cluster node tagging of virtual (VM-based) CIS cluster nodes.

- Runtime of CIS cluster: once a CIS cluster is created and operating (i.e. CISM is fully operational), the CCM is still responsible for managing the tagging of CIS cluster nodes. However, concerning the configuration operation, the CCM invokes the CIS instance management service provided by the CISM, and the CISM further executes the operation.

The CCM determines the proper tagging of CIS cluster nodes based on:

- Specific information (or metadata) in the CCND based on the requested capabilities of the CIS cluster nodes. See example 2.

- Runtime information that the CCM obtains based on interactions with the NFVO, VIM or other infrastructure manager. See example 3.

EXAMPLE 2: If CIS cluster node is requested to have SSD drives, specific information can indicate the values of the tagging to use for the CIS cluster nodes, such as "disktype=ssd".

EXAMPLE 3: Based on the granting exchange with the NFVO, the CCM can learn that certain cluster resources have been assigned from resource zone "A", while others from resource zone "B", and tag the CIS cluster nodes accordingly with "resourcezone=A" and "resourcezone=B".

In addition to determining the VNF placement, the tag also has capability to affect relocation of containerized workloads of the VNF. For instance, the tag can show tainted situation that the CIS cluster node with the tag has malfunction and thereby the CISM can halt containerized workloads based on the tag and information associated with the VNF instances themselves and create new containerized workloads on another applicable CIS cluster node.

4.2.9 Relation of CIS cluster management and resource management

As stated in clause 4.2.2, the management of a CIS cluster includes the addition or removal of CIS cluster nodes in the CIS cluster. CIS cluster nodes are created or realized from a pool of infrastructure compute resources (either virtual machines or bare-metal servers) that can be managed by the VIM (in case of virtual machines) or other infrastructure resource manager function responsible for the management of physical resources (in case of bare-metal servers). Resource management (compute, storage and network) interface operations exposed by the VIM are consumed for this purpose (refer to clause B.2 workflow on creating a CIS cluster).

A CIS cluster may also be managed as an NS whose VNFs provide the CIS and CISM functionality. In that case, the CCM consumes the NS LCM interface operations exposed by an NFVO, which in turn interacts with a VNFM and a VIM to deploy the VNFs providing the CIS cluster functionality and allocate virtualised resources that are used by the CIS cluster respectively (refer to clause B.3 workflow on creating a CIS cluster as an NS). When requesting the creation of a CIS cluster, the CCM Consumer provides the identifier of the NSD of the corresponding NS as well as addressing information for accessing the NFVO where this NSD has been on-boarded.

Whichever method is used to create the CIS cluster, the allocated resources associated to the CIS cluster are either designated for containerized workloads to be deployed within their respective limits of namespace quota, or used by the used by the CISM. The relation of CIS cluster management and VM-based CIS cluster resource management is shown in figure 4.2.9-1 when the CCM interacts directly with the VIM. Figure 4.2.9-2 illustrates the relation between CIS cluster management and NS management when the CIS cluster is deployed and managed as an NS. In the latter case, the existing resource management functionality in NS management applies for CIS cluster management.

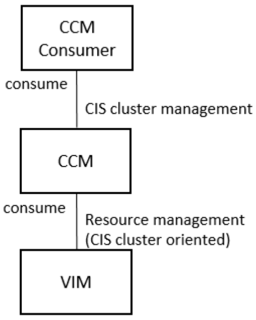

Figure 4.2.9-1: Relation of CIS cluster management and VM-based CIS cluster resource management

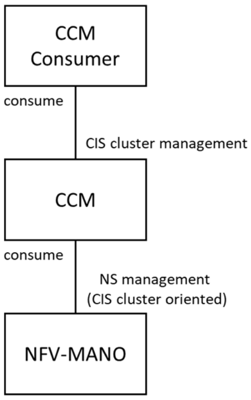

Figure 4.2.9-2: Relation of NS-based CIS cluster management and NS management

4.2.10 Relation of Network Services and CIS clusters

In general, a Network Service (NS) is agnostic to the infrastructure implementation of the NS, e.g. the specification of the NS is independent of whether its constituent VNFs are VM based, container based or a mix of both.

The relation between NSs and CIS clusters is twofold. On one hand, CIS clusters provide the infrastructure resources for hosting all or part of the constituents of NSs. On the other hand, CIS clusters where CIS cluster nodes are virtual machines can themselves, but need not, be deployed and managed as NSs.

In the first case the NSD does not convey information related to a CIS cluster or the CIS cluster nodes/storage resources belonging to the CIS cluster. Yet, it is expected in the context of container based VNF deployments, CIS clusters will be used for the deployment of such VNF and NS. In addition, the NSD contains information to associate VNF external CPs (belonging to the constituent containerized VNFs of the NS) to NS VL. Depending on the placement of NS constituents (e.g. if all or part of the NS are deployed using CIS cluster resources), NS VLs can be realized fully or partially as secondary container cluster internal/external networks.

The constituent containerized VNFs of an NS can be deployed in the same or different CIS clusters, as specified by affinity/anti-affinity rules. It is also possible that a single CIS cluster could be used for deploying multiple NS instances. The affinity and/or anti-affinity relationship between the constituent VNFs of the NS is extended to apply for the scope of the CIS cluster.

In the second case, the contents of the NSD for deploying the CIS cluster as an NS is designed to match the contents of the CCD (refer to clause 6.1) and thus conveys information related to a CIS cluster. An NS instance maps to a CIS cluster. The NS corresponding to the CIS cluster is independent from the NSs whose constituents are hosted in the CIS cluster resources. The latter NSs are overlaid on the former NS.

4.2.11 Relation of namespaces and CIS clusters

As stated in clause 4.4.2, a CIS cluster is logically divided into one or multiple namespaces. A namespace does not span multiple CIS clusters, but is valid within one CIS cluster. Namespaces in different CIS clusters are considered different namespaces even if they have identical names.

Compute/Storage/Network MCIOs are grouped into namespaces and each Compute/Storage/Network MCIO only belongs to one namespace. Both CIS cluster and namespace are regarded as mechanisms to isolate groups of constituent components of the containerized workload (represented by Compute/Storage/Network MCIOs) from each other in a viewpoint of multi-tenancy security. The CCM is not involved in namespace management.

As a part of CIS cluster management, when CIS cluster nodes are deployed in the form of virtual machines, the CCM requests directly or indirectly the VIM to allocate infrastructure resources to create new CIS cluster nodes for a CIS cluster. Infrastructure resources allocated to a CIS cluster and dedicated for containerized workload deployments are further managed by the CISM instance in charge of the CIS cluster. These infrastructure resources of the CIS cluster are consumed by the Compute/Storage/Network MCIOs which are grouped into namespaces to achieve logical isolation. Namespaces are managed by the CISM.

4.2.12 FCAPS management for CIS clusters

As in traditional Fault management, Configuration management, Account management, Performance management and Security management (FCAPS management) operations, configuration management, performance management and fault management related to CIS clusters are provided by the CCM to the CCM Consumer.

Configuration management for the CIS cluster is provided by the CCM to its Consumer during the lifecycle of the CIS cluster. The configuration management operations include transferring and applying configuration information to the CIS cluster, querying the configuration of the CIS cluster and subscribing/notifying the events in case of the change of CIS cluster configurations. The configuration information related to the CIS cluster can be either the configuration of the CIS cluster related object instances, e.g. CIS cluster node, CIS cluster storage, CIS cluster nodes network, CISM instance, CIS instance or a combination of the above.

Performance information on a given CIS cluster related object instance (e.g. CIS cluster node, storage or network) is provided by the CCM. The performance information results from performance information of the virtualised resources that is collected from the VIM or performance information of bare-metal resources that is collected from a management entity managing physical resources, and mapped by the CCM to this CIS cluster related object instance. Collection and reporting of performance information is controlled by a PM job that groups details of performance collection and reporting information. When new performance information is available, the CCM notifies the CCM Consumer using a notification.

Alarms related to CIS clusters are provided by the CCM and are visible to the CCM Consumer. Virtualised resource alarms or physical resource alarms collected by the CCM will be filtered and correlated by the CCM and mapped to the corresponding CIS cluster related object instances (e.g. CIS cluster node, storage or network), resulting in alarms on corresponding CIS cluster.

Depending on the specific deployment requirements for the CIS cluster, the CCM can construct CISM with high availability. CISM high availability can be achieved by providing redundancy of API servers and databases, which are parts of CISM. The CCM can perform configuration of a load balancer backed with the redundant API servers and clustering of the redundant databases based on CCD (see clause 6.2.1).

CISM is capable of (un-)cordoning CIS cluster nodes by performing tagging operations of CIS cluster nodes (see clause 4.2.8). Depending on the tagging values assigned, segregation or desegregation of a CIS cluster node can be realized.

CIS cluster management considers the following security aspects:

- Guarantee secure communication among CIS cluster nodes.
  The CCM configures security related information and artifacts, e.g. certificates, to CIS cluster nodes, based on the security information provided by entities responsible for security management.

- Authenticate and authorize invocating CISM capabilities from external and/or internal entities of CIS cluster.
  The CCM configures the CISM by using configuration files and declarative descriptors representing Role Based Access Control (RBAC) related information (see clause 6.3.5), based on the authorization and authentication information provided by entities responsible for security management, and issues credentials to entities responsible for the authorization management, so that Consumers (e.g. a VNFM) can access the service exposed by the CISM.

- Enable and configure the auditing of CIS cluster nodes.
  The CCM configures auditing related information to the CISM, based on the security information provided by entities responsible for security management.

NOTE: The mechanisms and solutions for providing the related security information and configuration to the CCM are not specified in the present document.

4.2.13 Managed CIS cluster object

A Managed CIS Cluster Object (MCCO) is an abstract NFV object for CIS cluster management. Depending on the applicability and functionality scope of an MCCO, the MCCO can serve two purposes:

- enhancing or increasing the set of CIS cluster capabilities (see examples in clause 4.2.14); and
- supporting CIS cluster management processes such as those related to fulfilment and assurance of CIS cluster (see examples in clause 4.2.15).

An MCCO is characterized by its configuration, state, requested and allocated infrastructure resources, and applicable operational policies. The desired state of an MCCO is specified in a declarative descriptor. The declarative description of an MCCO is interpreted by the CCM and, depending on the MCCO type or functionality, it can also be interpreted by the CISM when the MCCO is applied and further operated on a CIS cluster. More information about the declarative descriptors of an MCCO is available in clause 6.3.

Depending on its type, an MCCO instance can be instantiated and deployed as:

- a group of one or more OS containers running on a CIS instance;
- configuration objects on the CISM; or
- a combination of the above.

The CCM is responsible for the lifecycle management of the MCCO, e.g. installing and applying the MCCO instance to the CIS cluster by requesting to the CISM for the MCCO instantiation, deleting the MCCO instances from the CIS cluster by requesting to the CISM for the MCCO termination, etc.

NOTE: MCCO lifecycle management is independent of the CIS cluster lifecycle management. Installing and applying the MCCO instance to the CIS cluster establishes an association between the CIS cluster and the MCCO, while deleting the MCCO instance from the CIS cluster disassociates the CIS cluster and the MCCO.

In addition, since MCCO instances consume compute, network and/or storage resources of the CIS cluster, the CCM has also the responsibility to request granting for resources necessary for the deployment of MCCO instances. Clause 4.2.14 provides additional information about the responsibility of the CCM in handling MCCOs related to CIS cluster enhancement capabilities, and clause 4.2.15 provides additional information about the responsibility of the CCM in handling MCCOs related to daemon objects.

Clause C.1 documents examples of MCCOs and their management using open source solutions.

4.2.14 CIS cluster enhancement capability

In order to address the demands of additional CIS cluster capabilities for the deployment of containerized workloads or for operating the CIS clusters, e.g. supporting secondary container cluster networking, CIS clusters can support providing additional capabilities to their baseline capability set. A CIS Cluster Enhancement Capability (CCEC) can be applied to a CIS cluster and thereby advanced features for CIS clusters can be realized. The CCEC is regarded as a specific type of MCCO.

Extending the capability set of CIS clusters can be done statically by design or dynamically at runtime:

- Statically: CIS cluster descriptors contain or refer to MCCO declarative descriptors corresponding to the set of CCECs that are applied at creation time of the CIS cluster.
- Dynamically: the CIS cluster can be updated at runtime by applying (e.g. installing) MCCO declarative descriptors of the CCEC or by removing (e.g. uninstalling) applied CCECs.

Extending the capability set of CIS clusters is expected to be implemented by two elements:

- MCCO declarative descriptors, which define the type of CCEC, the value name for the "kind" if the CCEC is exposed as new API objects, and how to make a specific CCEC inventoried and operational via CISM service interfaces, and
- CCEC controllers, which watch status of the CCEC and operate relevant resources in a CIS cluster.

NOTE: The "kind" of a CCEC is used to differentiate the type of objects that are exposed through the CISM interfaces, and which are made available as CIS cluster capabilities to CISM Consumers.

Applying CCECs, and thus extending the capability set of a CIS cluster, impacts cluster-wide features on a CIS cluster. Furthermore, multiple CCECs can be applied to a CIS cluster. Therefore, avoiding conflicts among multiple CCECs is expected to be addressed. Although conflicts among multiple CCECs are cluster-widely detected on the CIS cluster, depending on configuration of CCECs, applicability of CCECs can be limited within a specific namespace or multiple namespaces of the CIS cluster.

The CCM has the following responsibilities to manage CCECs:

- Requests a granting operation to the NFVO for granting resources used by the CCEC:
  - retrieve information about necessary virtualised resources from the associated MCCO declarative descriptor for CCEC; and
  - send a request regarding resources to be granted to the NFVO.
- Manages lifecycle of the CCEC based on the requirements and behavioural description of the CCEC defined in the associated MCCO declarative descriptor. The CCM interacts with the CISM or directly with the CIS cluster nodes depending on the type and form of lifecycle management of the CCEC. In the case of lifecycle management of CCEC that leverage other capabilities of the CISM, such as using daemon objects or using the capability to CISM resource API, it is expected that the CCM will interact with the CISM. Management lifecycle actions include:
  - Install and apply the CCEC to the CIS cluster;
  - Modify configurations of the CCEC in the CIS cluster; and
  - Delete the CCEC from the CIS cluster.
- Handles CCEC related information:
  - Keep track of the relation between the kind of CCEC and the CIS cluster; and
  - Receive/respond queries from other entities, e.g. the NFVO, regarding information related to the CCEC.

4.2.15 Daemon object for CIS cluster nodes

Daemon objects are used to deploy MCCO instances having same functionality onto all applicable CIS cluster nodes. The following use cases are some examples for using daemon objects; running an MCCO instance to collect logs on every CIS cluster node, running an MCCO instance to monitor status of every CIS cluster node, and running an MCCO instance to dynamically configure routing information on every CIS cluster node. The daemon object is used by the CISM to control a set of daemon processes running simultaneously across a CIS cluster. The daemon object is regarded as a specific type of MCCO.

The daemon object has the following characteristics:

- In order to perform the functionality, MCCO instances based on the daemon object can consume compute, network and/or storage resources of the same resource pool used for the deployment of VNF instances. Therefore, infrastructure resources consumed by the daemon object are expected to be granted by the NFVO.
- When CIS cluster nodes are added to the CIS cluster, MCCO instances based on the daemon object are added to them. When CIS cluster nodes are removed from the cluster, those MCCO instances are garbage collected. Deleting the daemon object is expected to clean up the MCCO instances instantiated based on the daemon object across the CIS cluster. Therefore, the daemon object is associated to cluster-wide features.

The CCM has the following responsibilities to manage daemon objects:

- Requests a granting operation to the NFVO for granting resources used by the daemon object:
    - retrieve information about necessary virtualised resources from the associated MCCO declarative descriptor for daemon object; and
    - send a request regarding resources to be granted to the NFVO.
- Manages lifecycle of the daemon object by interacting with the CISM, based on the requirements and behavioural description of the daemon object defined in the associated MCCO declarative descriptor. Management lifecycle actions include:
    - install and apply the daemon object to the CIS cluster;
    - modify configurations of the daemon object in the CIS cluster; and
    - delete the daemon object from the CIS cluster.
- Handles daemon object related information:
    - Keep track of which daemon objects are deployed on the CIS cluster.
    - Receive/respond queries from other entities, e.g. the NFVO, regarding information related to the daemon object.

4.3 Framework

4.3.1 Overview

The CCM and CISM functions provide one or more management capabilities which can be invoked by using one or more management service interfaces.

The services for the management and orchestration of CIS clusters and its constituents are exposed via management service interfaces by the CCM and CISM functions as specified in the present document. The management service interfaces can be consumed by:

- other NFV-MANO functional entities; and/or
- consumers outside NFV-MANO.

4.3.2 CCM function and CCM services

The CCM function offers management services for the CIS clusters, which are exposed by the container cluster management service interfaces.

4.3.3 CISM function and CISM services

The CISM function offers OS container management services as described in ETSI GS NFV-IFA 040 [1]. In addition, the CISM function offers services for the management of the CIS instances, cluster storage and MCCOs.

4.4 Relationship among key concepts

4.4.1 Deployment example of CIS clusters

In an environment that has multiple CIS clusters, each CIS cluster has one or more instances of the CISM which manages workloads deployed in its CIS cluster (see note). The CISM instance is also responsible for managing the CIS instances. A CIS cluster has at least one CIS cluster node hosting a CIS instance and one CISM instance for the management.

Figure 4.4.1-1 shows an example of several VNFs deployed in different CIS clusters.

NOTE: A CIS cluster can have multiple CISM instances for reliability purpose of the CIS cluster.

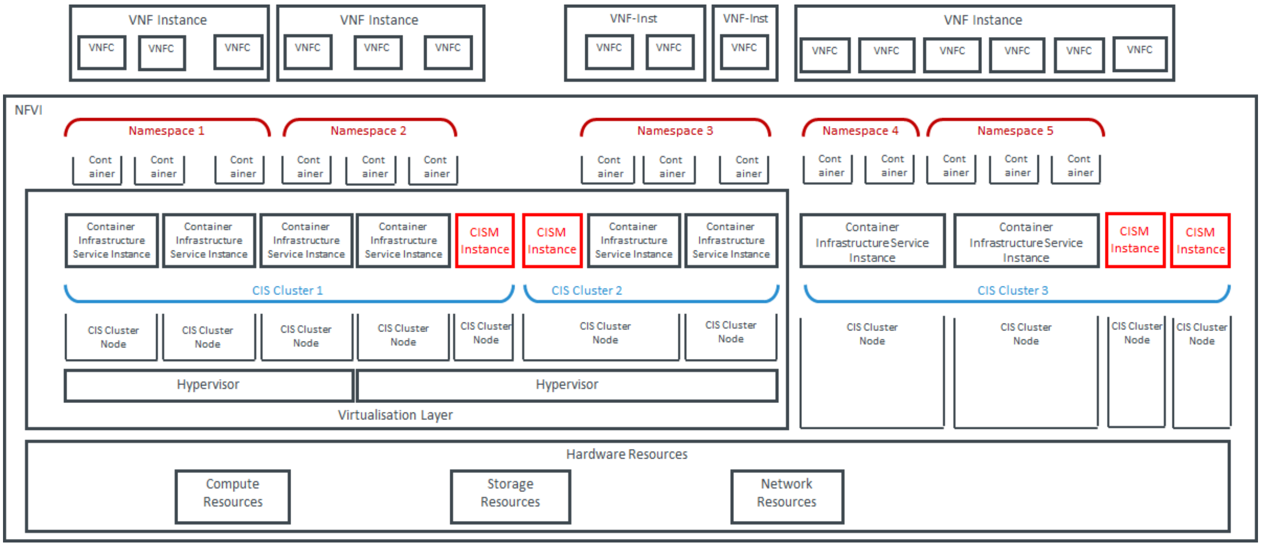

Figure 4.4.1-1: Deployment example with VNFs, CIS clusters and namespaces

4.4.2 Managed object view of key concepts in a CIS cluster

From the viewpoint of managed NFV objects, the relationship among CIS cluster node, CISM instance, CIS instance and namespace in a CIS cluster is shown in figure 4.4.2-1.

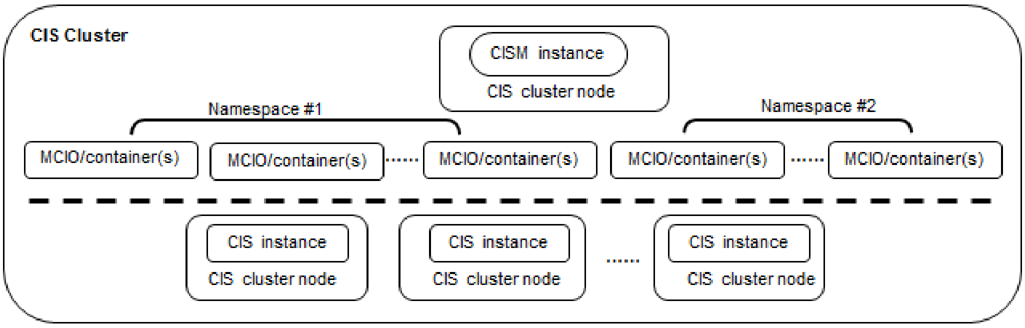

Figure 4.4.2-1: Relationship among CIS cluster node, CISM instance, CIS instance and namespace

A CIS cluster is generally composed of a group of CIS cluster nodes hosting at least one CISM instance and one CIS instance. The CISM instance schedules containerized workloads to corresponding CIS instances in the CIS cluster.

A CIS cluster can be logically divided into one or multiple namespaces. A namespace (see ETSI GS NFV-IFA 040 [1]) provides a mechanism to isolate groups of containerized workloads from others from a viewpoint of multi-tenancy security, and it also provides access control to these groups of containerized workloads. Resources in the CIS cluster nodes of a CIS cluster can be grouped into a namespace and can only belong to that namespace. Those resources are allocated to MCIOs grouped in the namespace.

The CISM instance provides service interfaces for namespace management and CIS instance management in the scope of the CIS cluster to its northbound Consumers. The CISM instance can also enforce resource limits (i.e. namespace quota) on a namespace as requested by its northbound Consumer.

NOTE: A CIS cluster has a default namespace that is not manageable.

5 Service requirements

5.1 CCM Service requirements

5.1.1 Introduction

Clause 5.1 in the present document specifies the set of requirements applicable to interfaces exposing CIS cluster management and orchestration services offered by the CCM function.

5.1.2 General CCM service requirements

Table 5.1.2-1 specifies requirements applicable to the services provided by the CCM.

Table 5.1.2-1: CCM service requirements

Identifier	Requirement
CcmSvc.001	The CCM shall provide a CIS cluster lifecycle management service.
CcmSvc.002	The CCM shall provide a CIS cluster fault management service.
CcmSvc.003	The CCM shall provide a CIS cluster configuration management service.
CcmSvc.004	The CCM shall provide a CIS cluster performance management service.
CcmSvc.005	The CCM shall provide a CIS cluster security management service.
CcmSvc.006	The services provided by the CCM shall support access control (e.g. RBAC).

5.1.3 CIS cluster lifecycle management service interface requirements

Table 5.1.3-1 specifies the requirements applicable to the interface of the CIS cluster management service produced by the CCM.

Table 5.1.3-1: CIS cluster management service interface requirements

Identifier	Requirement
CcmClMgt.001	The CIS cluster lifecycle management service interface produced by the CCM shall support creating a CIS cluster. See note 1.
CcmClMgt.002	The CIS cluster lifecycle management service interface produced by the CCM shall support querying information about a CIS cluster. See note 3.
CcmClMgt.003	The CIS cluster lifecycle management service interface produced by the CCM shall support modifying a CIS cluster. See note 2.
CcmClMgt.004	The CIS cluster lifecycle management service interface produced by the CCM shall support deleting a CIS cluster.
CcmClMgt.005	The CIS cluster lifecycle management service interface produced by the CCM shall support sending notifications in the event of changes to a CIS cluster.
NOTE 1: The creation of CIS cluster includes the management of the necessary resources and placement constraints, the creation, allocation, setup of the CIS cluster nodes networks according to the requirements and configuration of connectivity of CIS cluster nodes to such networks and pooling and provisioning of the CIS cluster storage. Before a CIS cluster is created, the CCM shall create an identifier that the Consumer and the NFVO can use in further operations on the CIS cluster and to identify the CIS cluster in placement decisions. The CCM shall also provide the Consumer with address information of the CISM services available in the CIS cluster. NOTE 2: Modifying a CIS cluster includes: scaling (i.e. resize) the CIS cluster, installing and applying CIS cluster artefacts (e.g. executables or plugins), modifying the network-related configuration of the CIS cluster and CIS cluster nodes, modifying the storage-related configuration of CIS cluster, modification (e.g. update/upgrade) of CIS cluster software. NOTE 3: Information about a CIS cluster includes, but is not limited to: CIS cluster level information such as location of the CIS cluster, number of CIS cluster nodes; CIS cluster node level information such as types of CIS cluster nodes (if it is a CISM, CIS, or both) composing the CIS cluster, resources used by the CIS cluster node, the capabilities supported by the CIS cluster node, the configuration of the CIS cluster node, the placement information of the CIS cluster nodes, CIS cluster storage resource related information, CIS cluster networking resource related information, CISM instance information. See clauses 4.2.2 and 4.2.4 for more runtime information that can be queried.	

5.1.4 CIS cluster fault management service requirements

Table 5.1.4-1 specifies the requirements applicable to the interface of the CIS cluster fault management service produced by the CCM.

Table 5.1.4-1: CIS cluster fault management service interface requirements

Identifier	Requirement
CcmFltMgt.001	The CIS cluster fault management service interface produced by the CCM shall enable its Consumers to collect CIS cluster fault information. See note 1.
CcmFltMgt.002	The CIS cluster fault management service interface produced by the CCM shall support sending notifications in event of a change in alarm information on a CIS cluster. See note 2.
CcmFltMgt.003	The CIS cluster fault management service interface produced by the CCM shall support sending notifications in event of the creation of an alarm on a CIS cluster.
CcmFltMgt.004	The CIS cluster fault management service interface produced by the CCM shall support sending notifications in event of the clearance of an alarm on CIS cluster.
CcmFltMgt.005	The CIS cluster fault management service interface produced by the CCM shall support acknowledgement of an alarm.
CcmFltMgt.006	The CIS cluster fault management service interface produced by the CCM shall support sending notifications in event of rebuilt.
CcmFltMgt.007	The CIS cluster fault management service interface produced by the CCM shall support managing subscriptions to the notifications related to alarms.
NOTE 1: Fault information on a given CIS cluster can include the information related to the alarm (e.g. alarm created, alarm cleared, etc.), alarm causes and identification of this CIS cluster and fault information concerning the infrastructure resources supporting the CIS cluster related object instances. NOTE 2: Possible changes of alarm information include change state information, perceived severity, etc.	

5.1.5 CIS cluster configuration management service requirements

Table 5.1.5-1 specifies the requirements applicable to the interface of the CIS cluster configuration management service produced by the CCM.

Table 5.1.5-1: CIS cluster configuration management service interface requirements

Identifier	Requirement
CcmCfgMgt.001	The CIS cluster configuration management service interface produced by the CCM shall support transferring and applying CIS cluster configurations provided by the CCM Consumer (see notes 1 and 2).
CcmCfgMgt.002	The CIS cluster configuration management service interface produced by the CCM shall support querying the information about CIS cluster configurations.
CcmCfgMgt.003	The CIS cluster configuration management service interface produced by the CCM shall support sending notifications in the event of CIS cluster configuration changes.
CcmCfgMgt.004	The CIS cluster configuration management service interface produced by the CCM shall support managing subscriptions to the notifications related to configuration management.
NOTE 1: Applying CIS cluster configurations encompasses the deletion and modification of configurations. NOTE 2: The configuration information related to the CIS cluster can be either the configuration of the CIS cluster related object instances, e.g. CIS cluster node, CIS cluster storage, CIS cluster nodes network, CISM instance, CIS instance or a combination of the above.	

5.1.6 CIS cluster performance management service requirements

Table 5.1.6-1 specifies the requirements applicable to the interface of the CIS cluster performance management service produced by the CCM.

Table 5.1.6-1: CIS cluster performance management service interface requirements

Identifier	Requirement
CcmPerfMgt.001	The CIS cluster performance management service interface produced by the CCM shall support controlling the collection and reporting of CIS cluster performance information, resulting from infrastructure resources (VMs or bare-metal servers) performance information, on the CIS cluster(s) it manages (see note 1).
CcmPerfMgt.002	The CIS cluster performance management service interface produced by the CCM shall support sending notifications in the event of the availability of CIS cluster performance information.
CcmPerfMgt.003	The CIS cluster performance management service interface produced by the CCM shall support creating a PM job specifying the CIS cluster performance information to be collected.
CcmPerfMgt.004	The CIS cluster performance management service interface produced by the CCM shall support deleting one or more PM job(s).
CcmPerfMgt.005	The CIS cluster performance management service interface produced by the CCM shall support querying the information about one or more PM job(s).
CcmPerfMgt.006	The CIS cluster performance management service interface produced by the CCM shall support managing the thresholds on specified CIS cluster performance information (see note 2).
CcmPerfMgt.007	The CIS cluster performance management service interface produced by the CCM shall support sending notifications in the event of a threshold defined for a specified metric of a CIS cluster being crossed.
CcmPerfMgt.008	The CIS cluster performance management service interface produced by the CCM shall support managing subscriptions to the notifications related to performance management.
CcmPerfMgt.009	The CIS cluster performance management service interface produced by the CCM shall support sending notifications in the event of shortage of capacity in the CIS cluster (see note 3).
NOTE 1: The collection of performance information on a given CIS cluster controlled by the PM Job in the CCM results from collected performance information of the infrastructure resources that are mapped to this CIS cluster related object instance (e.g. CIS cluster node, storage or network). NOTE 2: Management of thresholds include creation, deletion and query of the thresholds on specified CIS cluster performance information. NOTE 3: CIS cluster capacity shortage can be the shortage of storage, compute, etc.	

5.1.7 CIS cluster security management service requirements

Table 5.1.7-1 specifies the requirements applicable to the interface of the CIS cluster security management service produced by the CCM.

Table 5.1.7-1: CIS cluster security management service interface requirements

Identifier	Requirement
CcmSecMgt.001	The CIS cluster security management service interface produced by the CCM shall support configuration of security related information and artifacts for secure communication among CIS cluster nodes. See note.
CcmSecMgt.002	The CIS cluster security management service interface produced by the CCM shall support configuration of authorization and authenticate invocating CISM capabilities from external and/or internal entities of the CIS cluster by using configuration files and declarative descriptors representing RBAC. See note.
CcmSecMgt.003	The CIS cluster security management service interface produced by the CCM shall support configuration of auditing related information for auditing of CIS cluster nodes.
NOTE: The security information for the configuration is provided by entities responsible for security management.	

5.2 Service requirements of the CISM

5.2.1 Introduction

The requirements applicable to interfaces exposing OS container management and orchestration services offered by the CISM function are specified in ETSI GS NFV-IFA 040 [1]. In addition, requirements applicable to the following interfaces exposing CIS instance management services are specified in the present document:

- CIS instance management service
- CIS MCCO management service

5.2.2 General CISM service requirements

Table 5.2.2-1 specifies requirements applicable to the services provided by the CISM in addition to those listed in ETSI GS NFV-IFA 040 [1].

Table 5.2.2-1: CISM service requirements

Identifier	Requirement
CismSvc.101	The CISM shall provide a CIS instance management service. See note.
CismSvc.102	The CISM shall provide a CIS MCCO management service.
CismSvc.103	The services provided by the CISM shall support access control (e.g. RBAC).
NOTE: CISM service requirements CismSvc.001 to 005 are listed in ETSI GS NFV-IFA 040 [1], clause 6.2.	

5.2.3 CIS instance management service interface requirements

Table 5.2.3-1 specifies the requirements applicable to the interface of the CIS instance management service produced by the CISM.

Table 5.2.3-1: CIS instance management service interface requirements

Identifier	Requirement
CismCisInsMgt.001	The CIS instance management service interface produced by the CISM shall support instantiating a CIS instance. See note 1.
CismCisInsMgt.002	The CIS instance management service interface produced by the CISM shall support querying information about a CIS instance. See note 2.
CismCisInsMgt.003	The CIS instance management service interface produced by the CISM shall support modifying a CIS instance. See note 1.
CismCisInsMgt.004	The CIS instance management service interface produced by the CISM shall support deleting a CIS instance. See note 3.
CismCisInsMgt.005	The CIS instance management service interface produced by the CISM shall support sending notifications in the event of changes to a CIS instance.
NOTE 1: The instantiation and modification of CIS instances includes enabling setting up the values of various CIS instance characteristics such as name, capacity, metadata, labels/tags. NOTE 2: Information about a CIS instance includes, but is not limited to: name of the CIS instance, capacity of the CIS instance and capacity allocated for workloads scheduling, metadata of the CIS instance including labels/tags. NOTE 3: The deletion of CIS instances implies the removal of the CIS instance as an object managed by the CISM.	

5.2.4 CIS MCCO management service interface requirements

Table 5.2.4-1 specifies the requirements applicable to the interface of the CIS MCCO management service produced by the CISM.

Table 5.2.4-1: CIS MCCO management service interface requirements

Identifier	Requirement
CismMccom.001	The CIS MCCO management service interface produced by the CISM shall support instantiating (i.e. installing/applying) MCCOs.
CismMccom.002	The CIS MCCO management service interface produced by the CISM shall support querying information about MCCOs.
CismMccom.003	The CIS MCCO management service interface produced by the CISM shall support modifying MCCOs.
CismMccom.004	The CIS MCCO management service interface produced by the CISM shall support terminating (deleting) MCCO.
CismMccom.005	The CIS MCCO management service interface produced by the CISM shall support sending notifications in the event of changes to MCCOs.
NOTE: In case that an MCCO is related to networking or storage (see clause 6.3.4), configuration for them is realized by invoking the CIS MCCO management service interfaces operating the MCCO.	

6 NFV object modelling for CIS cluster management

6.1 Overview

The present document introduces declarative descriptors for the CIS cluster and its constituents. Where possible, e.g. resource descriptors, the definition of these descriptors can be based on other NFV descriptors and information elements as specified in ETSI GS NFV-IFA 014 [i.10] and ETSI GS NFV-IFA 011 [i.9] and also can re-use some information elements defined in the reference specifications.

The first group of descriptors and information elements relates to the initial deployment of CIS clusters and their lifecycle management. These descriptors and information elements specify e.g. the resources for the CIS clusters and nodes, networks and storage, software images for initial deployment of CISM and CIS instances:

- CIS Cluster Descriptor (CCD)
  The CCD describes cluster characteristics as described in clause 4.2.4.

- CIS Cluster Node Descriptor (CCND)
  The CCND is referenced from the CCD and describes characteristics of CIS cluster nodes. It references a CCNRD for the node's resource characteristics and additionally includes necessary information for the basic creation of the CIS cluster. e.g. manifests, software images.

- CIS Cluster Node Resource Descriptor (CCNRD)
  The CCNRD is referenced from the CCND and describes resource characteristics of CIS cluster nodes, e.g. virtual machine/bare-metal server, resource requirements.

Another group of descriptors is used to deploy and configure additional cluster capabilities, e.g. CIS cluster enhancement capabilities, or daemon objects.

- MCCO declarative descriptor
  The MCCO declarative descriptor describes characteristics of managed CIS cluster objects and their lifecycle management. Examples are the CCEC (see clause 4.2.14) and daemon objects (see clause 4.2.15).

The CCD and CCND provide the main input for the CCM to determine what to request from infrastructure managers (e.g. VIM). When the CCM has a direct access to the VIM, the contents of the CCD and CCND can typically be mapped to virtualised resource descriptors as defined in ETSI GS NFV-IFA 005 [i.3]). When CIS clusters are themselves deployed and managed as NSs, an appropriate NSD and a set of VNF packages referenced from this NSD are on-boarded by the CCM Consumer to the NFVO used to instantiate these NSs. It is the responsibility of the CCM Consumer to ensure that their contents match the requirements specified in the CCD and its referenced CCNDs. For example, the boot images referenced in a CCND shall also be referenced in the VNFDs of the constituent VNFs.

The relationships among the CCD, CCND, CCNRD and MCCO declarative descriptor in the present clause are illustrated in figure 6.1-1. The CCD, CCND and CCNRD describes the CIS cluster related managed objects used for the creation of a CIS cluster. As described in clause 4.2.14, the CCD can contain or reference to the MCCO declarative descriptors corresponding to the set of MCCOs that are applied at the instantiation time of the CIS cluster. On the other hand, an MCCO can be applied to a CIS cluster by instantiating the object based on its declarative descriptor. The relationships among the NSD, VNFD and CCD are illustrated in clause 6.4.

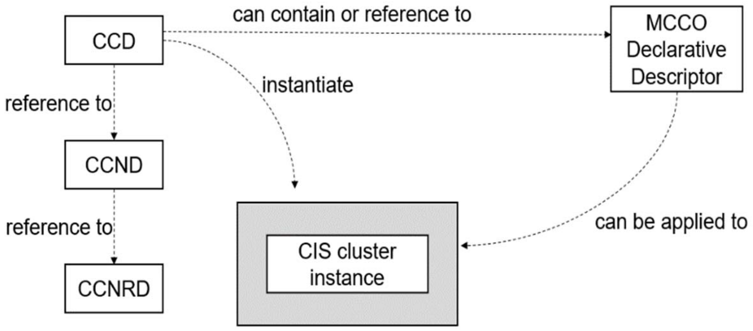

Figure 6.1-1: CCM related declarative descriptors relationship

6.2 Descriptors for the CIS cluster LCM

6.2.1 CIS Cluster Descriptor (CCD)

A CIS cluster descriptor is an NFV template that describes the desired infrastructure resource (compute, storage and network) characteristics for a CIS cluster. It is interpreted by the CCM for the allocation of those resources and their preparation for the further steps in CIS cluster LCM operations. During CIS cluster creation, the CCM uses the information of the CCD to allocate virtual resources or physical resources, and prepares the resources for the instantiation of the CISM and CIS instances. Since this preparation typically includes software installation and configurations, the CCD also contains necessary information for this step which can be complemented with run-time information.

NOTE: While the format of the CCD is specified during the protocol design phase, and some parts are profiled and just mapped to descriptors or files from the existing solutions such as Kubernetes®, the present document provides an introduction on the high-level information and structure of the CCD. Since the present document mainly specifies the requirements for a service interface, no full specification of information elements is provided.

The CCD provides the following information:

- Common metadata:
  - Unique identification of the descriptor
  - Information of the provider of the descriptor
  - Versioning information
- Information on the CIS cluster node(s) to run CISM instances:
  - Reference to a CCND
  - Initial, minimum and maximum number of CISM instances
- Information on the CIS cluster nodes to run CIS instances:
  - Reference to a CCND
  - Initial, minimum and maximum number of CIS instances
- Additional scaling information, e.g. rules
- Additional placement rules for the CIS cluster nodes hosting the CISM instances and CIS instances:
  - Affinity/anti-affinity between cluster resources in the CIS cluster
  - Affinity/anti-affinity with respect to other CIS clusters or resources
- Information on the storage resources:
  - Reference to MCCO declarative descriptor for persistent storage including the description of storage class, size, etc.
  - Capacity, type, name and placement control of storage resources
  - Affinity/anti-affinity between storage resources
- Information on the network resources:
  - Network resources requirements for the CIS cluster nodes networks
  - Networking information for the primary and secondary container cluster, internal and external networks
- Scripts and configuration files for the setup of the CISM instance, e.g. installer script

- Requirements (e.g. types and versions) related to cloud provider in support of the interaction between CISM's cloud provider controllers and underlying infrastructure managers for handling capabilities such as those related to dynamic networking and storage provisioning

6.2.2 CIS Cluster Node Descriptor (CCND)

A CIS cluster node descriptor is an NFV template that describes the desired characteristics for a CIS cluster node. It is referenced from the CCD and interpreted by the CCM for the allocation of the resources of a CIS cluster node and their preparation for the further steps in LCM operations. In particular during cluster creation, the CCM uses the information of the CCND to request the creation of a virtual machine or allocate a bare-metal server for a CIS node, and prepares the node resources for the instantiation of a CISM or CIS instance. Since this preparation typically includes software installation and configuration, the CCND contains also necessary information for this step which can be complemented with run-time information.

NOTE: The format of the CCND is specified during the protocol design; the present document provides only an introduction on the high-level information of the CCND. Since the present document mainly specifies the requirements for a service interface, no full specification of information elements is provided.

The CCND provides the following information:

- Common metadata:
  - Unique identification of the descriptor
- Information characteristics of the CIS cluster node:
  - Reference to a CIS Cluster Node Resource Descriptor (CCNRD)
  - Flavour of CIS node, e.g. CISM or flavour of CIS instance, e.g. associated to different resource capabilities
  - Boot image and scripts, etc. to use for installation
  - Information of the software to be installed on the CIS cluster node, e.g. the name and version of the components that CISM instance and/or CIS instance contain, as well as any relevant version dependencies

6.2.3 CIS Cluster Node Resource Descriptor (CCNRD)

A CIS cluster node resource descriptor is an NFV template that describes the desired resource characteristics for a CIS cluster node. It is referenced from the CCND and interpreted by the CCM for the allocation of the resources of a CIS cluster node.

NOTE 1: The format of the CCNRD is specified during the protocol design; the present document provides only an introduction on the high-level information of the CCNRD. Since the present document mainly specifies the requirements for a service interface, no full specification of information elements is provided.

The CCNRD provides the following information:

- Common metadata:
  - Unique identification of the descriptor
- Information characteristics of the CIS cluster node:
  - Machine type, e.g. VM or bare-metal

NOTE 2: In case of VM machine type, the CCNRD properties below specify the characteristics for the virtual resource; in case of bare-metal machine type, the CCNRD properties below specify the hardware characteristics for the bare-metal server.

  - CPU requirements, e.g. CPU architecture, clock speed, number of virtual CPUs
  - Memory and local disk requirements

- Requirements for network interfaces
- Additional resource capabilities, e.g. acceleration support

NOTE 3: The way to describe hardware requirements for the servers a VM is running on and the way to describe hardware requirements for bare-metal servers are the same.

6.3 MCCO declarative descriptor

6.3.1 Commonality

An MCCO declarative descriptor contains information relevant to MCCO instances to be installed. The information relevant to an MCCO instance includes:

- name: indicates the name of the MCCO instance;
- type: indicates the type of the MCCO instance; and
- additional metadata: indicates the general additional information of the MCCO instance.

The type of an MCCO instance represents to which feature the MCCO instance belongs, such as CCEC, daemon object, network related objects, storage related objects, etc., which are further described in the subsequent clauses.

In addition, when deploying CCEC, daemon object and other CIS cluster administrative components, workloads might be deployed at the same time, which consume CIS cluster resources, i.e. compute, network and storage. Since the workloads themselves are deployed based on OS containers, OsContainerDesc information element described in ETSI GS NFV-IFA 011 [i.9] is leveraged for the specification of the relevant declarative descriptors in order to represent requirements of the workloads.

6.3.2 CCEC

There are two sorts of declarative descriptors related to CCEC: one is the MCCO declarative descriptor to describe the definition of the CCEC and the other is the MCCO declarative descriptor for a CCEC controller to represent resources and properties for the controller. The MCCO declarative descriptor includes:

- name: indicates the name of the CCEC;
- scope: indicates whether the CCEC is applicable only for a specific namespace, multiple namespaces or the whole CIS cluster; and
- versioning information: indicates a list of versions supported by the CCEC.

6.3.3 Daemon object

To deploy MCCO instances onto applicable CIS cluster nodes by a daemon object, an MCCO declarative descriptor for the daemon object represents:

- the resources to be consumed by the MCCO instances;
- the necessary information for the instantiation of the MCCO instances; and
- the selection of applicable CIS cluster nodes to deploy the MCCO instances on.

The CIS cluster node selection is performed based on the CIS cluster node tagging, which is described in clause 4.2.8 of the present document, as well as VNF placement constraints.

6.3.4 MCCOs with a specific scope of applicability

6.3.4.1 Networking

By leveraging the secondary container cluster network specific CCEC, e.g. NetworkAttachmentDefinition, deployment of an MCCO to represent configurations for secondary container cluster networks is enabled. As mentioned in clause 6.3.2 of the present document, there are two sorts of declarative descriptors:

- An MCCO declarative descriptor to enable secondary container cluster networks: the declarative descriptor is used for defining the MCCO which represents configuration for secondary container cluster networks.
- An MCCO declarative descriptor for CCEC controller: the declarative descriptor is used for a daemon object which deploys MCCO instances responsible for configuring secondary container cluster network related behaviour of each CIS cluster node to attach an interface connected with an appropriate secondary container cluster network to a VNFC instance.

6.3.4.2 Storage

The MCCO declarative descriptor related to storage aspect of a CIS cluster specifies the MCCO instances to represent configurations to provision pooled virtualised resources or external storage as CIS cluster storage resources. When containerized workloads demand storage resources, following the claim of the demanding, the configuration is expected to be consumed to associate relevant CIS cluster storage resources with the containerized workload.

6.3.5 RBAC for access control to CISM

To realize RBAC for access control to CISM service interfaces, there are three types of MCCO and their declarative descriptors to define roles, to create accounts, and to bind between the roles and the accounts.

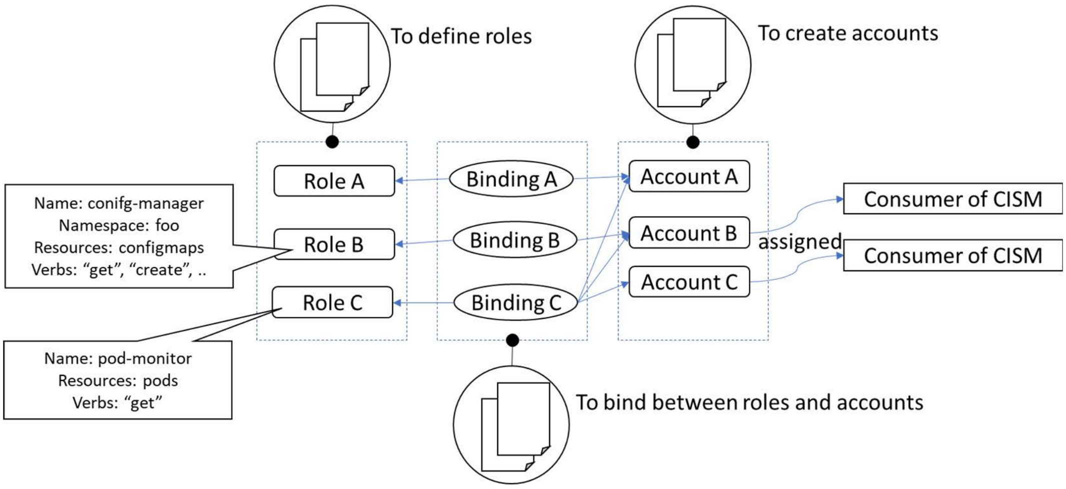

Figure 6.3.5-1: Overview of relationship among declarative descriptors related to RBAC

Firstly, declarative descriptors are used to define the roles that represent which resources or information an entity bound to the role can access and how the entity can access the resources or information, e.g. get, watch, list, etc. In addition, the declarative descriptor can refer to two scopes: the first scope is associated to and affects a namespace and the second scope influences the whole CIS cluster.

Secondly, declarative descriptors are used to create the accounts that can be assigned to Consumers of CISM service interfaces.

Thirdly, the declarative descriptor that binds the roles and the accounts defines specific references to the roles and the accounts to be bound. The declarative descriptor also has two scopes: the first scope is used for binding the roles associated to a certain namespace and the second scope is used for binding the roles affecting the whole CIS cluster.

6.4 Relationship of NFV templates and CIS cluster descriptors

6.4.1 Introduction

For the relationships between NFV templates (e.g. NSD, VNFD) and CIS cluster descriptors, there are two scenarios (types of NS usage) to be considered:

- In case the workloads are deployed in a CIS cluster, whether the workloads' descriptors are related to the CCD.
- In case a CIS cluster is deployed as an NS, there is a direct mapping relationship between the NSD and the CCD.

6.4.2 Relationship of workload related descriptors to the CCD

As described in clause 4.2.8, the NFVO dynamically selects the CIS cluster for the deployment of workloads. Therefore, there is no direct reference from an NSD or the VNFDs to a CCD. The NFVO calculates the resource needs and placement constraints from the NSD and VNFDs, and finds a CIS cluster (created from a CCD and its resource related descriptors), with available resources that match all constraints.

6.4.3 Relationship of the NSD and CCD in case a CIS cluster is deployed as NS

In this case, an NSD and a CCD describe the same CIS cluster from a different perspective. As outlined in the use case in clause B.3, the NSD and CCD are onboarded independently. When the CCM creates the CIS cluster, it sends an instantiate NS request to the NFVO (NFVO_B in clause B.3). For a successful CIS cluster creation, the resource description in the NSD and its constituents shall match the resource description in the CCD and its constituents.

There are several possible options to achieve this (not a complete list):

a) The NSD and CCD are created independently, the OSS specifies the NSD id and CCD id and additional parameters when requesting to create a CIS cluster. This implies that the OSS knows/is aware of the relationship between the NSD and CCD. After NS instantiation, the CCM checks whether the resources of the NS instance are appropriate for the CIS cluster.

b) The CCM dynamically creates the NSD and its constituents from the CCD. In this case, the CCM also onboards the NSD and VNF packages.

It is out of scope for the present document to further specify these options, but figure 6.4.3-1 illustrates the mapping of the main relevant descriptors for the CIS cluster nodes. Similar mapping can be done for CIS cluster storages and networks.

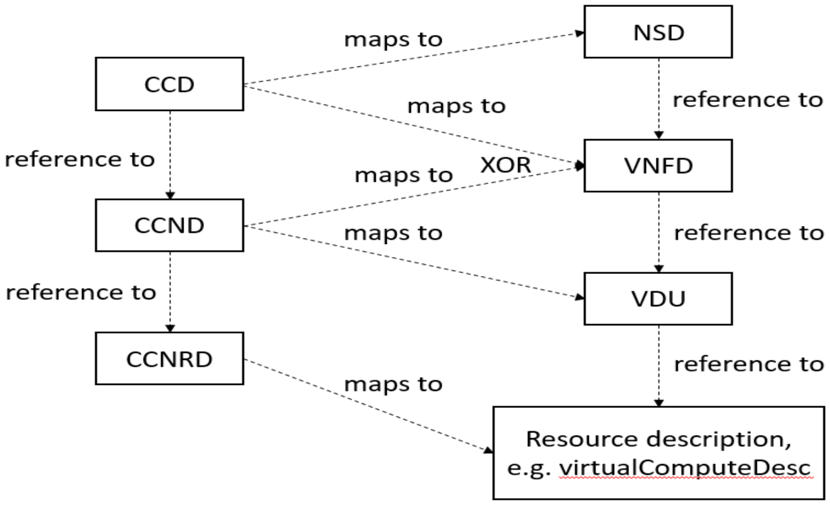

Figure 6.4.3-1: Mapping of the CCD and NSD compute resources in case a CIS cluster is deployed as NS

NOTE 1: The MCCO declarative descriptor is independent of such mapping between CCD and NSD.

NOTE 2: The VNFD can be mapped from the CCD or the CCND according to different implementations:

- VNFD maps to CCD: in this case, a VNF is able to realize from a resource perspective a whole CIS cluster.
- VNFD maps to CCND: in this case, a VNF is realized by a single VNFC instance that realizes from a resource perspective a single CIS cluster node.

Annex A (informative): Overview of services related to OS container and CIS cluster management

The services necessary for management of containerized workloads in an NFV environment are described in the present document and in ETSI GS NFV-IFA 040 [1]. Table A-1 illustrates the relation of documents, function names, services and objects.

Table A-1: Relation of OS container related services and documents

Function	CIR	CISM		CCM
Service area	Image Mgmt related services	Workload Mgmt related services	Node Mgmt related services	Cluster related services
Scope	• Store images and provide them to other functions	• Life cycle management for workloads • Manage namespaces in a CIS cluster • Manage namespace quota as resource limit	• Life cycle management for CIS instances in a CIS cluster • Management of Managed CIS Cluster Objects	• Life cycle management for CIS clusters • Life cycle management for CISM instances in a CIS cluster • Allocation of instantiated infrastructure-resources for CIS cluster nodes • FCAPS of CIS cluster
Services	OS container image management service	OS container workload management service, OS container compute management service, OS container storage management service, OS container network management service, OS container configuration management service	CIS instance management service, CIS MCCO management service	CIS cluster lifecycle management service, CIS cluster fault management service, CIS cluster configuration management service, CIS cluster performance management service, CIS cluster security management service
Descriptors	n/a	MCIO declarative descriptor	MCCO declarative descriptor	CCD, CCND, CCNRD
Objects	OS container image	MCIO MCIOP Namespace Namespace quota	CIS instance object, MCCO	CIS cluster object, CIS cluster node object, CISM instance object
	ETSI GS NFV-IFA 040 [1]		ETSI GS NFV-IFA 036 (the present document)	

Annex B (informative):
Workflows

B.1 Introduction

The present annex describes examples of end-to-end workflows concerning the operations for managing CIS clusters or the lifecycle of NS/VNF utilizing the CIS clusters.

All workflows are illustrated by use case description with sequence charts. The sequenced messages in the charts are numbered and are complemented by step descriptions with corresponding numbers.

B.2 Create a CIS cluster

B.2.1 Introduction

In this workflow example, the CCM creates the CIS cluster in a similar way as a VNFM would instantiate a VNF, but in the information flow in the present clause, the CIS cluster is not considered to be a VNF or NS. Clause B.3 shows a workflow where CCM creates the CIS cluster as an NS.

B.2.2 Actors

Table B.2.2-1: Create a CIS cluster, actors and roles

#	Actor	Description
1	Consumer	Either the OSS or other management system (e.g. NFVO) responsible for initiating the management of the CIS clusters
2	NFVO	NFV Orchestrator of the NFV system that is expected to orchestrate VNFs deployed in that CIS cluster
3	CCM	CIS Cluster Management function to manage the new CIS cluster for the Consumer
4	CISM	Container Infrastructure Service Management Function that deploys containerized workloads in the cluster
5	VIM	Virtualised Infrastructure Manager responsible for the virtualised resources that can be used for the CIS cluster

B.2.3 Pre-Conditions

Table B.2.3-1: Create a CIS cluster, pre-conditions

#	Pre-condition	Description
1	NFV-MANO (VIM, NFVO and VNFM) and CCM are running	
2	Necessary connectivity between OSS, NFV-MANO and CCM is available	
3	For the case of bare-metal CIS clusters, a pool of physical resources is available, either managed by CCM itself or by another entity	
4	NFVO is subscribed to receive notifications from the CCM	
5	CCD with its referenced CCNDs and software images are available to the CCM	

B.2.4 Post-Conditions

Table B.2.4-1: Create a CIS cluster, post-conditions

#	Post-condition	Description
1	The CIS cluster is created using resources according the request and can be used to deploy containerized workloads.	
2	The CISM instance(s) are providing their service and can be used to deploy containerized workloads.	
3	The Consumer and NFVO are notified of the successful cluster creation and provided with the necessary information about the CIS cluster and the CISM instances.	With this information, the Consumer can query for additional information about the CIS cluster (e.g. capacity of the CIS cluster) from the CCM and the CISM instance associated to the CIS cluster.

B.2.5 Description

Figure B.2.5-1 illustrates the flow for creation of a CIS cluster.

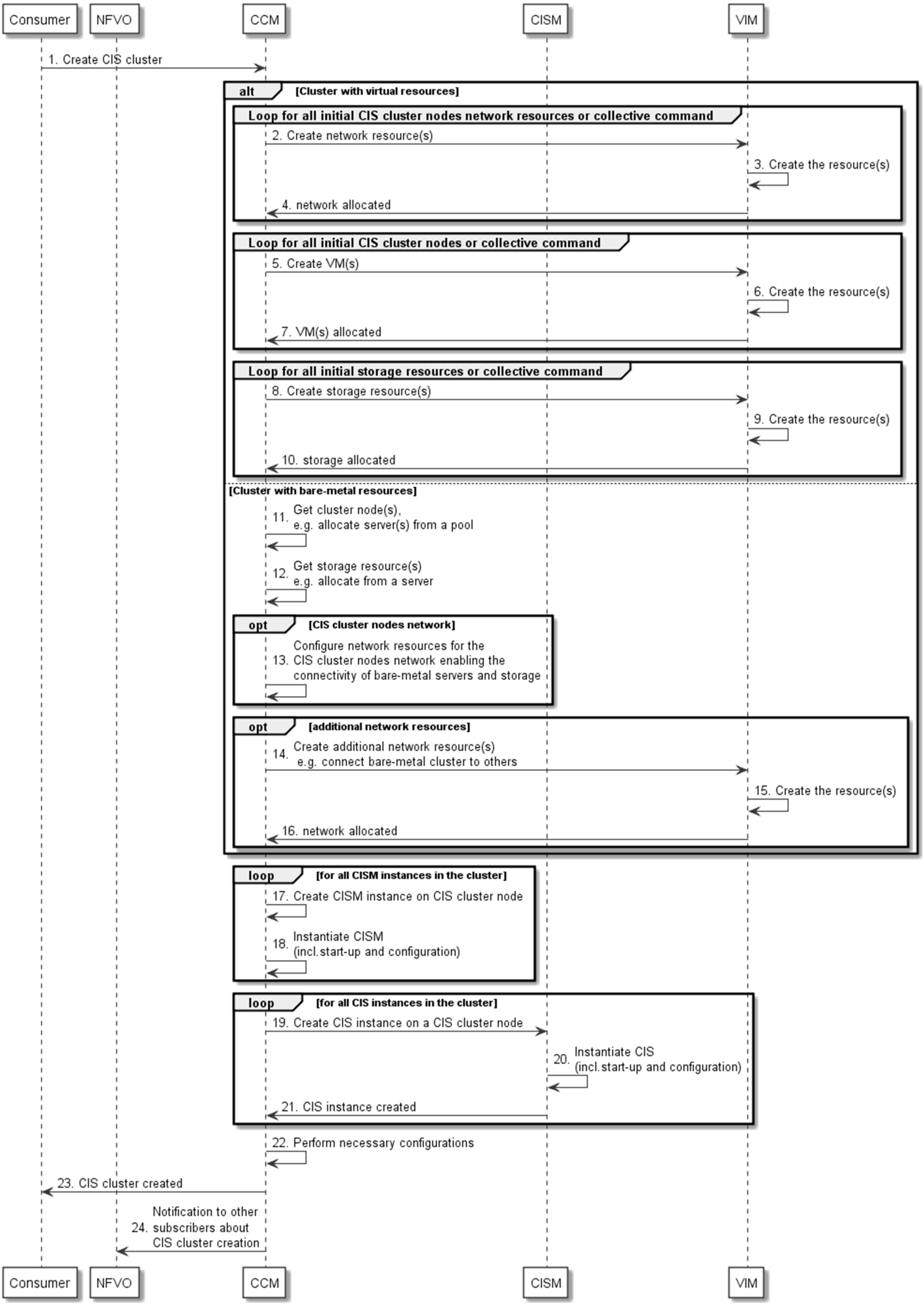
Consumer
NFVO
CCM
CISM
VIM
1. Create CIS cluster
alt [Cluster with virtual resources]
Loop for all initial CIS cluster nodes network resources or collective command
2. Create network resource(s)
3. Create the resource(s)
4. network allocated
Loop for all initial CIS cluster nodes or collective command
5. Create VM(s)
6. Create the resource(s)
7. VM(s) allocated
Loop for all initial storage resources or collective command
8. Create storage resource(s)
9. Create the resource(s)
10. storage allocated
[Cluster with bare-metal resources]
11. Get cluster node(s), e.g. allocate server(s) from a pool
12. Get storage resource(s) e.g. allocate from a server
opt [CIS cluster nodes network]
13. Configure network resources for the CIS cluster nodes network enabling the connectivity of bare-metal servers and storage
opt [additional network resources]
14. Create additional network resource(s) e.g. connect bare-metal cluster to others
15. Create the resource(s)
16. network allocated
loop [for all CISM instances in the cluster]
17. Create CISM instance on CIS cluster node
18. Instantiate CISM (incl.start-up and configuration)
loop [for all CIS instances in the cluster]
19. Create CIS instance on a CIS cluster node
20. Instantiate CIS (incl.start-up and configuration)
21. CIS instance created
22. Perform necessary configurations
23. CIS cluster created
24. Notification to other subscribers about CIS cluster creation
Consumer
NFVO
CCM
CISM
VIM

Figure B.2.5-1: Create a CIS cluster

1) The Consumer triggers creation of a CIS cluster. The Consumer can be the OSS, the NFVO or another entity managing the infrastructure for a Service Provider. The Consumer provides the necessary information for the desired CIS cluster, e.g. resource requirements, affinity constraints via a CCD. Additional information such as initial number of nodes and placement constraints can be part of the parameters of the command.

Steps 2 to 10 describe the resource management in case of a virtual CIS cluster, first the compute resources then storage and network. There can be loops or collective operations.

NOTE 1: The order of resource allocation can vary and some steps can be executed in parallel.

NOTE 2: Before the CCM interacts with the VIM for resource management (in case of VM resources) related to a CIS cluster, the CCM requests the NFVO to grant the process of resource management.

2) The CCM requests the network resources for the CIS cluster nodes networks from the VIM (e.g. Allocate Virtualised Network Resource operation, see ETSI GS NFV-IFA 005 [i.3]).

3) The VIM creates the network resources and allocates them for the CIS cluster.

4) The VIM confirms the creation and provides the CCM with the resource information.

5) The CCM requests VM resources from the VIM (e.g. Allocate Virtualised Compute Resource operation see ETSI GS NFV-IFA 005 [i.3]).

6) The VIM creates the VM and allocates it for the CIS cluster.

7) The VIM confirms the VM creation and provides the CCM with the resource information.

8) The CCM requests virtualised storage resources from the VIM (e.g. Allocate Virtualised Storage Resource operation, see ETSI GS NFV-IFA 005 [i.3]).

NOTE 3: These storage resources are for use for the whole cluster.

9) The VIM creates the storage resources and allocates them for the CIS cluster.

10) The VIM confirms the creation and provides the CCM with the resource information.

Steps 11 to 16 describe the resource management in case of a bare-metal CIS cluster. There can be loops or collective operations.

NOTE 4: The order of resource allocation can vary and some steps can be executed in parallel.

NOTE 5: Before the CCM internally performs resource management (in case of bare-metal servers) related to a CIS cluster, the CCM requests the NFVO to grant the process of resource management.

11) The CCM can have internally a pool of resources from which it allocates servers or can use a separate entity to manage a server pool.

12) The CCM can get storage resource e.g. by allocating storage from a storage server.

13) In some cases, separate network resources are necessary (which are not managed by the VIM) for the realization of the CIS cluster nodes networks enabling the connectivity of the bare-metal servers allocated for the CIS cluster. CCM executes necessary configuration e.g. using SDN.

14) In some cases of mixed environments (e.g. with VM-based VNFs hosted on the NFVI) additional network resources from the VIM provide the connectivity between the bare-metal CIS cluster and other clusters or infrastructure networks. CCM requests these resources from the VIM.

15) The VIM creates the network resources and allocates them for the CIS cluster.

NOTE 6: This includes the necessary resources to enable the CCM to connect to the CIS cluster.

16) The VIM confirms the creation and provides the CCM with the resource information.

Steps 17 to 22 describe the instantiation of CISM and CIS instances on the previously allocated resources.

NOTE 7: The order of the steps can vary and some steps can be executed in parallel.

17) The CCM instantiates CISM instance(s) on some CIS cluster nodes according to the information in the CIS cluster descriptors (CCD and CCND) and in the parameters of the command. In case of VMs, this can be done e.g. by deploying an image, in case of bare-metal servers e.g. by installing a boot image.

NOTE 8: A CISM instance can also share its software image with a CIS instance.

18) The CCM starts the software of the CISM instance(s) and executes necessary configuration.

NOTE 9: This includes to establish necessary peering (e.g. communication configuration) between CCM, CISM and CIS instances.

19) The CCM requests the CISM (see CismCisInsMgt.001) to instantiate the CIS instances on the remaining CIS cluster nodes according to the information from CCND and parameters of the command.

NOTE 10: The instantiation steps (step 18 and step 19) include all necessary initial configuration for the corresponding CIS cluster nodes.

20) The CISM performs the main steps for instantiation, configuration and networking of the CIS instance.

21) The CISM acknowledges the CIS instance's instantiation.

22) Finally, additional configuration can be performed, e.g. for the CIS cluster nodes network and for cluster external networks and interfaces of the CIS cluster.

NOTE 11: The final configuration step (step 22) include all necessary activities regarding enabling the connectivity of the CIS cluster towards NFV-MANO entities.

23) The CCM notifies the Consumer about the successful CIS cluster creation providing necessary information about the CIS cluster and the CISM instance, e.g. capabilities and a CIS cluster identification.

24) The CCM also sends notification to other subscribers about the successful CIS cluster creation providing similar information.

B.3 Create a CIS cluster as an NS

B.3.1 Introduction

In this workflow example, the CCM creates the CIS cluster as an NS. The CCM plays the role of an OSS. The NS provides the functionality of a CIS cluster. In this example the NS contains two types of VNFs, one provides the CISM functionality and the other one provides the CIS functionality. The contents of the NSD and the selected instantiation level determines how many CISM and CIS instances are instantiated when the NS is instantiated.

Many other arrangements are possible but not covered by this example, e.g. the NS can be designed with a single VNF that provides both the CIS cluster and CISM functionality.

The present procedure describes the deployment of the NS providing the functionality of the CIS cluster. The deployment of VNFs on the CIS cluster is expected to be also performed by deploying other NSs including the corresponding VNFs. Therefore, it is envisioned that two kinds of NSs are deployed: an "underlay" NS providing the CIS cluster functionality and an "overlay" NS providing the deployment of actual containerized VNFs. The two NSs are completely independent of each other (i.e. no nesting NS relationship is established between the two NS instances, accounting of resources usage by each NS is independent, etc.), and in fact, these can be managed by different NFV-MANO stack instances as indicated in clause B.3.2.

B.3.2 Actors

Table B.3.2-1 describes the actors and roles involved in the creation of a CIS cluster. It does not preclude that a functional block instance can play multiple roles (e.g. the NFVO-A and NFVO-B roles can be played by the same NFVO instance).

Table B.3.2-1: Create a CIS cluster, actors and roles

#	Actor	Description
1	Consumer	Either the OSS or other management system (e.g. NFVO) responsible for initiating the management of the CIS clusters.
2	NFVO-A	NFV Orchestrator of the NFV system that is expected to orchestrate VNFs deployed in the CIS cluster.
3	VNFM-A	VNFM that is expected to manage the lifecycle of the VNFs deployed in the CIS cluster.
4	CCM	CIS Cluster Management function to manage the new CIS cluster for the Consumer.
5	CISM	Container Infrastructure Service Management function that deploys containerized workloads in the CIS cluster.
6	VIM	Virtualised Infrastructure Manager responsible for the virtualised resources that can be used for the CIS cluster.
7	NFVO-B	NFV Orchestrator of the NFV system that is expected to deploy and manage the NS that provides the CIS cluster functionality.
8	VNFM-B	VNFM that is expected to manage the lifecycle of the VNFs that provide the CIS cluster functionality.

B.3.3 Pre-Conditions

Table B.3.3-1 describes the pre-conditions for creating a CIS cluster.

Table B.3.3-1: Create a CIS cluster, pre-conditions

#	Pre-condition	Additional description
1	NFVO-A, NFVO-B, VNFM-A, VNFM-B, VIM and CCM are running.	
2	CCD with its referenced CCNDs etc are available to the CCM.	
3	The NSD for deploying the "CIS cluster NS" and the VNF packages it refers have been on-boarded on NFVO-B.	The NSD includes VLDs enabling the creation of network resources for primary and secondary container cluster networks.
4	Necessary connectivity between OSS, NFV-MANO functional blocks and CCM is available.	
5	The NFVO-A is subscribed to receive notifications from the CCM.	
6	The CCM is subscribed to receive notifications from the NFVO-B.	
7	Configuration data for the installation of the CISM and CIS instances are available to the CCM.	

B.3.4 Post-Conditions

Table B.3.4-1 describes the post-conditions after creating a CIS cluster.

Table B.3.4-1: Create a CIS cluster, post-conditions

#	Post-condition	Additional description
1	The CIS cluster is created as an NS instance according to the request and can be used to deploy containerized workloads.	
2	The CISM instance(s) are providing their service and can be used to deploy containerized workloads.	
3	The Consumer and NFVO-A are notified of the successful cluster creation and provided with the necessary information about the CIS cluster and the CISM instances.	

B.3.5 Description

Figure B.3.5-1 illustrates the flow for creation of a CIS cluster.

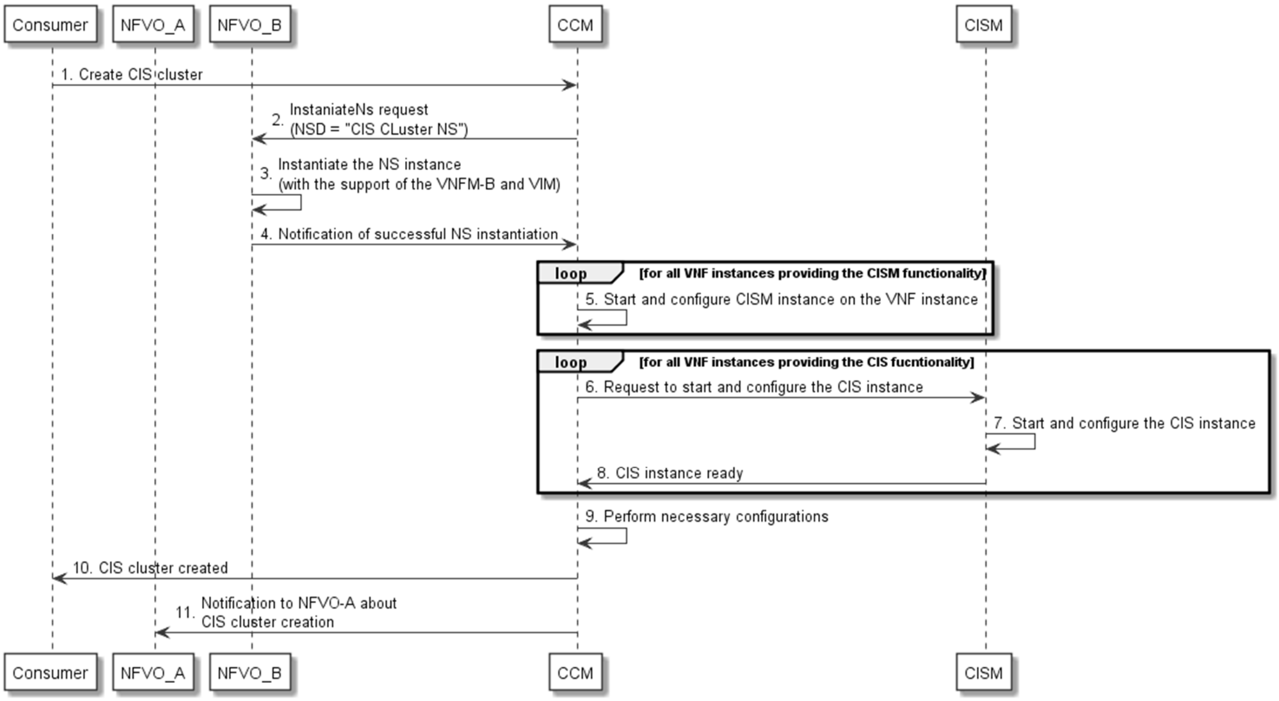
Consumer
NFVO_A
NFVO_B
CCM
CISM
1. Create CIS cluster
2. InstaniateNs request (NSD = "CIS CLuster NS")
3. Instantiate the NS instance (with the support of the VNFM-B and VIM)
4. Notification of successful NS instantiation
loop [for all VNF instances providing the CISM functionality]
5. Start and configure CISM instance on the VNF instance
loop [for all VNF instances providing the CIS fucntionality]
6. Request to start and configure the CIS instance
7. Start and configure the CIS instance
8. CIS instance ready
9. Perform necessary configurations
10. CIS cluster created
11. Notification to NFVO-A about CIS cluster creation
Consumer
NFVO_A
NFVO_B
CCM
CISM

Figure B.3.5-1: Create a CIS cluster

1) The Consumer triggers the creation of a CIS cluster. The Consumer can be the OSS or another entity managing the infrastructure for a Service Provider. The Consumer provides the necessary information for the desired CIS cluster, e.g. resource requirements, affinity constraints via the CCD as well as the identifier of the supporting NSD and the identifier of the NFVO where this NSD has been on-boarded (i.e. NFVO-B). Additional information such as initial number of nodes and placement constraints can be part of the parameters of the command.

2) The CCM requests the instantiation of an instance of the "CIS cluster NS" from the NFVO-B according to the information in the cluster descriptors (CCD and CCND) and in the parameters of the command, using the InstantiateNs operation as defined in ETSI GS NFV-IFA 013 [i.5].

3) The NFVO-B with the support of a VNFM and a VIM proceeds to the instantiation of the NS instance. This includes requesting the allocation of the necessary infrastructure resources to the CISM VNF and CIS VNF instances.

4) The NFVO-B notifies the CCM upon successful instantiation of the NS.

5) The CCM starts the software of the CISM instance(s) on the VNF instances providing the CISM functionality and executes necessary configuration.

NOTE 1: This includes to establish necessary peering (e.g. communication configuration) between CCM, CISM and CIS instances.

6) The CCM requests the CISM (see CismCisInsMgt.001) to start the CIS instances on the remaining VNF instances providing the CIS functionality according to the information from CCND and parameters of the command.

NOTE 2: The instantiation steps (step 3, step 5 and step 6) include all necessary initial configuration for the corresponding CIS cluster nodes.

7) The CISM performs the main steps for starting, configuration and networking of the CIS instance.

8) The CISM acknowledges the completion of the CIS instance instantiation.

9) Finally, additional configuration can be performed, e.g. for the CIS cluster nodes network and for cluster external networks and interfaces of the CIS cluster.

NOTE 3: The final configuration step (step 9) include all necessary activities regarding enabling the connectivity of the CIS cluster towards NFV-MANO entities.

10) The CCM notifies the Consumer about the successful CIS cluster creation providing necessary information about the CIS cluster and the CISM instance, e.g. capabilities and a CIS cluster identification.

11) The CCM also sends notification to other subscribers about the successful CIS cluster creation providing similar information.

B.4 Instantiation of a containerized VNF

B.4.1 Introduction

This workflow example illustrates the instantiation of a containerized VNF including the creation of a CIS cluster if necessary.

B.4.2 Actors

Table B.4.2-1: Instantiate containerized VNF, actors and roles

#	Actor	Description
1	OSS	The OSS of the service provider triggers the instantiation of a VNF, and if necessary, of the CIS cluster.
2	NFVO	The NFV Orchestrator is responsible to orchestrate the instantiation of the containerized VNF.
3	VNFM	The VNF Manager is responsible for the lifecycle management of the VNF to be instantiated.
4	CISM	The Container Infrastructure Service Management Function deploys the containerized workloads.
5	CCM	The CIS Cluster Management function creates a new CIS cluster if it is necessary for the VNF instantiation.

B.4.3 Pre-Conditions

Table B.4.3-1: Instantiate containerized VNF, pre-conditions

#	Pre-condition	Description
1	NFV-MANO and CCM are running.	
2	NSD and VNF Package (with its VNFD) of the VNF instance to be instantiated are on-boarded.	
3	For the case of bare-metal CIS clusters, a pool of physical resources is available, either managed by CCM itself or by another entity.	

B.4.4 Post-Conditions

Table B.4.4-1: Instantiate containerized VNF, post-conditions

#	Post-condition	Description
1	The new VNF instance is available and connected as per the NS requirements.	
2	In the case the VNF instance could not be instantiated on an existing CIS cluster, an additional CIS cluster has been created.	

B.4.5 Description

Figure B.4.5-1 illustrates the flow for instantiation of the containerized VNF.

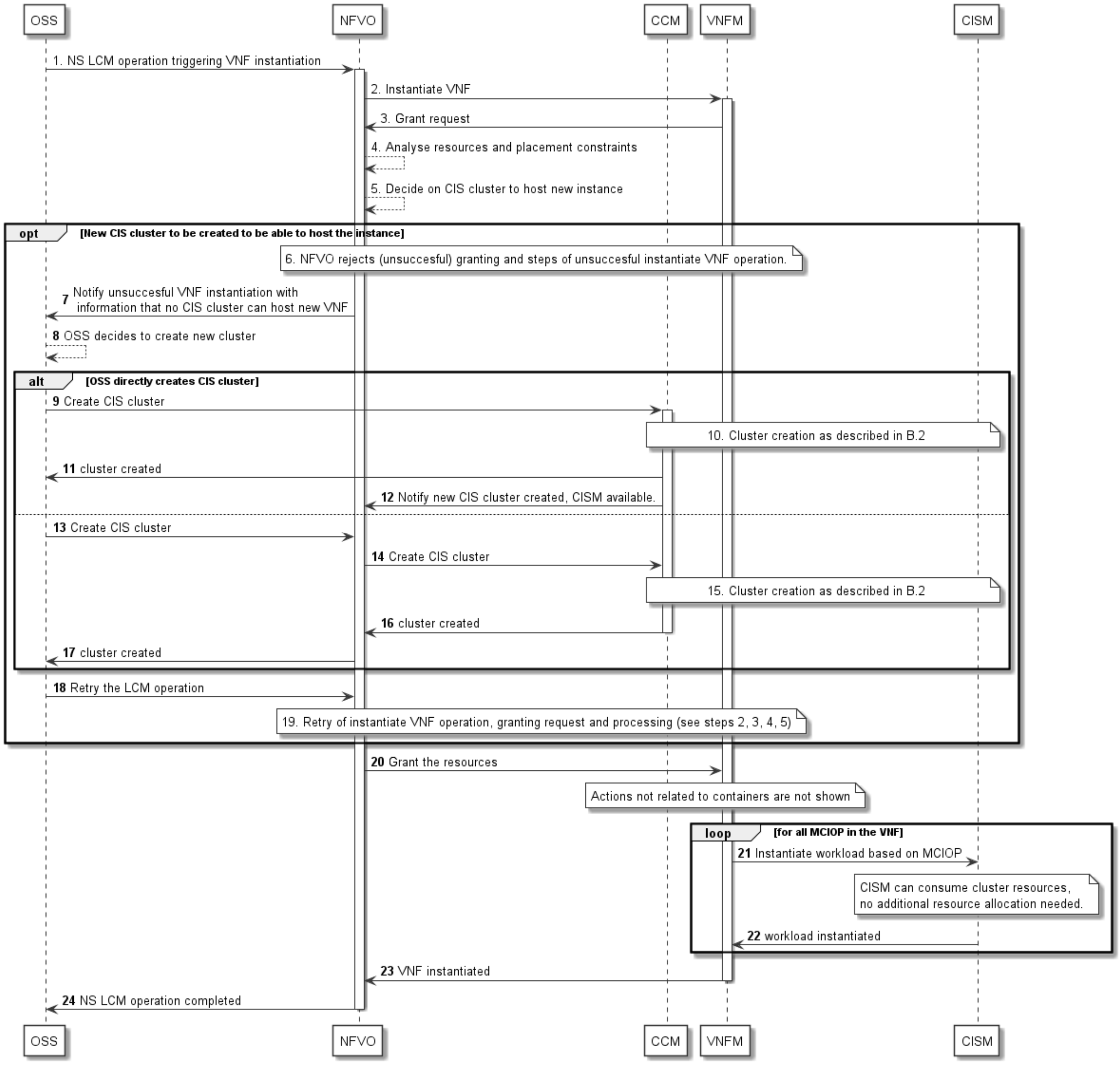
OSS
NFVO
CCM
VNFM
CISM
1. NS LCM operation triggering VNF instantiation
2. Instantiate VNF
3. Grant request
4. Analyse resources and placement constraints
5. Decide on CIS cluster to host new instance
opt
[New CIS cluster to be created to be able to host the instance]
6. NFVO rejects (unsuccesful) granting and steps of unsuccesful instantiate VNF operation.
7 Notify unsuccesful VNF instantiation with information that no CIS cluster can host new VNF
8 OSS decides to create new cluster
alt
[OSS directly creates CIS cluster]
9 Create CIS cluster
10. Cluster creation as described in B.2
11 cluster created
12 Notify new CIS cluster created, CISM available.
13 Create CIS cluster
14 Create CIS cluster
15. Cluster creation as described in B.2
16 cluster created
17 cluster created
18 Retry the LCM operation
19. Retry of instantiate VNF operation, granting request and processing (see steps 2, 3, 4, 5)
20 Grant the resources
Actions not related to containers are not shown
loop
[for all MCIOP in the VNF]
21 Instantiate workload based on MCIOP
CISM can consume cluster resources, no additional resource allocation needed.
22 workload instantiated
23 VNF instantiated
24 NS LCM operation completed

Figure B.4.5-1: Instantiate containerized VNF

1) The OSS sends an NS LCM request that implies the instantiation of a VNF.

NOTE 1: The VNF instantiation can be triggered e.g. by Instantiate NS, Update NS, Scale NS, or other operation.

2) NFVO requests the VNFM to instantiate the VNF.

3) The VNFM requests the NFVO to grant resources for the new VNF instance.

4) The NFVO analyses the resources for the new VNF instance and the given placement constraints, e.g. anti-affinity.

5) The NFVO selects a CIS cluster for the deployment of the containerized workloads of the VNF.

Steps 6 to 17 show the case when a new CIS cluster needs to be created, so the VNF can be instantiated.

6) In this case, first the NFVO interacts with the VNFM to reject (unsuccessful) the granting and the VNFM rolls back the Instantiate VNF operation.

NOTE 2: Details of the grant process, e.g. roll-back in case of FAILED_TEMP, are out of scope of the present document.

7) The NFVO notifies the OSS the unsuccessful VNF instantiation with information that there is no CIS cluster available that can host the new VNF instance. The NS LCM operation is rejected with a temporary failure, i.e. FAILED_TEMP.

8) The OSS decides that a new CIS cluster is to be created, so the VNF can be instantiated.

Steps 9 to 12 and steps 13 to 17 show two alternatives to trigger the CIS cluster creation.

Alternative 1:

9) The OSS triggers creation of a new CIS cluster.
In this first alternative, the OSS directly sends a create CIS cluster command to the CCM.

10) The CCM creates the new cluster based on the information given by the OSS, as described in clause B.2.

11) The CCM returns all necessary information about the newly created cluster to the OSS.

12) In this alternative NFVO is subscribed at CCM to be notified of the CIS cluster creation. The notification contains the necessary information for the NFVO to make use of the new cluster in subsequent LCM operations.

Alternative 2:

13) This second alternative illustrates that the OSS triggers the NFVO to create the new CIS cluster.

14) The NFVO requests the CCM for creation of a new CIS cluster.

15) The CCM creates the new cluster as described in clause B.2 (same as step 5).

16) The CCM returns all necessary information about the newly created CIS cluster to the NFVO.

17) The NFVO returns all necessary information about the newly created CIS cluster to the OSS.

18) OSS retries the LCM operation which was in state FAILED_TEMP.

NOTE 3: For details about retry of LCM operations after FAILED_TEMP, see ETSI GS NFV-SOL 005 [i.4], clause 6.3.7.

19) NFVO retries the Instantiate VNF operation with the VNFM and NFVO re-evaluates the grant request, i.e. resources, placement constraints and CIS cluster decision (see steps 2, 3, 4 and 5).

NOTE 4: The flow here does not show the option of a loop of multiple re-tries in case the re-evaluation in step 19 fails.

20) NFVO confirms the granted resources.

21) For each MCIOP, the VNFM requests the CISM instance of the given CIS cluster to instantiate the workload.

NOTE 5: CISM can consume the resources of the CIS cluster within the limits of the namespace quota. No further resource allocation needs to be done in this step.

22) CISM returns success to VNFM.

23) VNFM returns success of the VNF instantiation to NFVO.

24) NFVO returns success to OSS.

B.5 Deploy daemon object on a CIS cluster

B.5.1 Introduction

In this workflow example, the CIS cluster administrator deploys a daemon object (see clause 4.2.15) on a CIS cluster.

B.5.2 Actors

Table B.5.2-1: Deploy daemon object on a CIS cluster, actors and roles

#	Actor	Description
1	Consumer	Either the OSS or other management system responsible for the management of the CIS clusters
2	NFVO	NFV Orchestrator of the NFV system. During CIS cluster management, the NFVO is mainly involved in the granting process
3	CCM	CIS Cluster Management function that manages the CIS cluster for the Consumer
4	CISM	Container Infrastructure Service Management function that deploys containerized workloads in the cluster
5	CIS	CIS instance that runs MCCO instances

B.5.3 Pre-Conditions

Table B.5.3-1: Deploy daemon object on a CIS cluster, pre-conditions

#	Pre-condition	Description
1	NFV-MANO (VIM, NFVO and VNFM) and the CCM are running	
2	The CIS cluster is created (see workflow in clause B.2), and the CISM is able to manage workloads in the cluster	This includes all resources specified in the CCD and CCNDs, and at least a primary container cluster network.
3	Necessary connectivity between the OSS, NFV-MANO and CCM is available	
4	The MCCO declarative descriptor describing the daemon object is onboarded to the CCM	

B.5.4 Post-Conditions

Table B.5.4-1: Deploy daemon object on a CIS cluster, post-conditions

#	Post-condition	Description
1	The daemon object is instantiated on all applicable CIS cluster nodes.	
2	The Consumer and other subscribers are notified with the successful instantiation of the daemon object.	

B.5.5 Description

Figure B.5.5-1 illustrates the flow to deploy a daemon object on a CIS cluster.

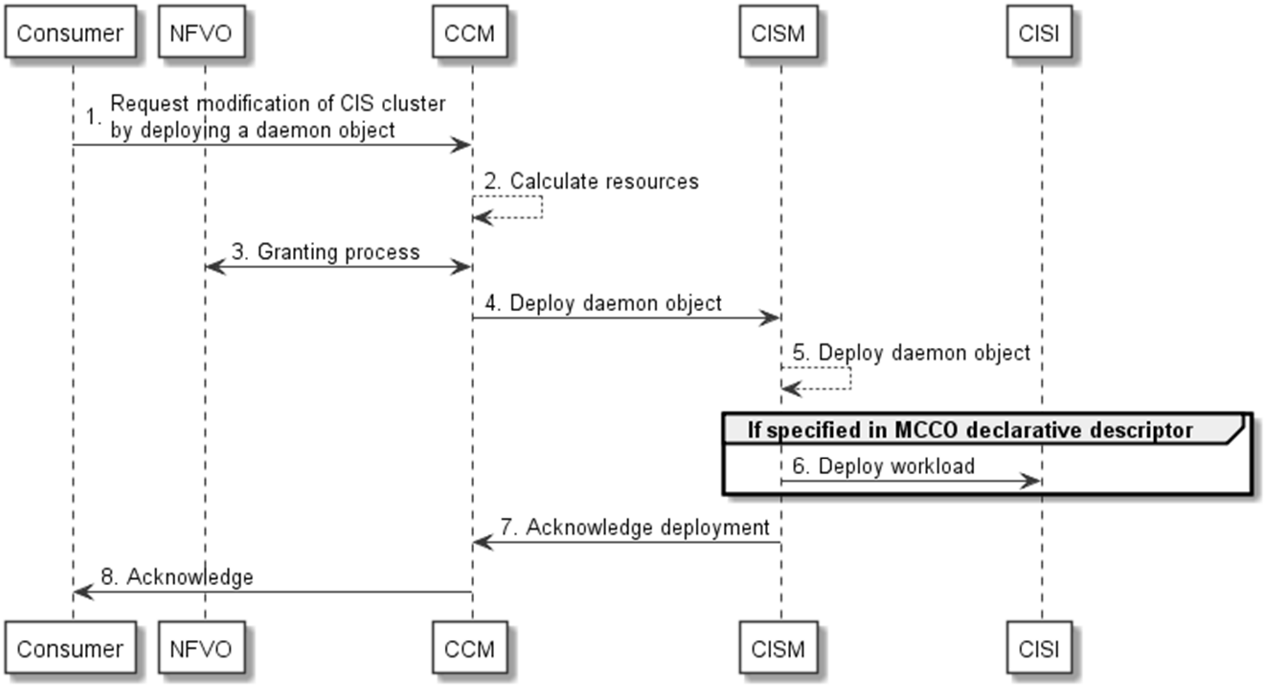

Figure B.5.5-1: Deploy daemon object on a CIS cluster

1) The Consumer requests the CCM to modify a CIS cluster, with an indication to deploy a daemon object to the CIS cluster, specifying the identification of the onboarded MCCO declarative descriptor that describes the daemon object and an identification of the CIS cluster.

2) The CCM parses the MCCO declarative descriptor and calculates necessary resource requirements for deploying the daemon object.

3) The CCM executes granting process with the NFVO.

4) After successful granting, the CCM requests the CISM of the CIS cluster to deploy the daemon object.

5) The CISM deploys the daemon object.

6) Depending on the content of the MCCO declarative descriptor, the CISM deploys workloads on the CIS instances that match filter criteria in the MCCO declarative descriptor, and/or executes necessary actions, e.g. to install and apply CCECs to the CIS cluster.

7) The CISM confirms successful deployment of the daemon object to the CCM.

8) After successful deployment of the daemon object, the CCM notifies the Consumer and all subscribers.

B.6 Scaling out a CIS cluster

B.6.1 Introduction

This workflow demonstrates the scaling out of a cluster. Several steps are similar to the instantiation use cases, see clauses B.2 and B.3, and will not be illustrated in all details. The use case concentrates on the scaling out of compute resources, i.e. CIS cluster nodes, be it nodes for CIS instances or CISM instances. Scaling out of storage and network resources requires different configuration steps, but the general flow is similar.

B.6.2 Actors

Table B.6.2-1: Scaling out a CIS cluster, actors and roles

#	Actor	Description
1	Consumer	Either the OSS or other management system (e.g. NFVO) responsible for initiating the management of the CIS clusters.
2	NFVO	NFV Orchestrator of the NFV system that is expected to orchestrate VNFs deployed in that CIS cluster.
3	CCM	CIS Cluster Management function to manage the CIS cluster for the Consumer.
4	CISM	Container Infrastructure Service Management Function that deploys containerized workloads in the cluster.
5	VIM	Virtualised Infrastructure Manager responsible for the virtualised resources that can be used for the CIS cluster.

B.6.3 Pre-Conditions

Table B.6.3-1: Scaling out a CIS cluster, pre-conditions

#	Pre-condition	Description
1	NFV-MANO (VIM, NFVO and VNFM) and CCM are running	
2	Necessary connectivity between OSS, NFV-MANO and CCM is available	
3	For the case of bare-metal CIS clusters, a pool of physical resources is available, either managed by CCM itself or by another entity	
4	NFVO is subscribed to receive notifications from the CCM	
5	CCD with its referenced CCNDs and software images are available to the CCM	
6	The CIS cluster to be scaled out is available and its CISM function is running	

B.6.4 Post-Conditions

Table B.6.4-1: Scaling out a CIS cluster, post-conditions

#	Post-condition	Description
1	The CIS cluster is scaled out according to the request and the additional capacity can be used to deploy containerized workloads via the CISM.	
2	The Consumer and NFVO are notified of the successful scale out.	

B.6.5 Description

Figure B.6.5-1 illustrates the flow for scaling out a CIS cluster.

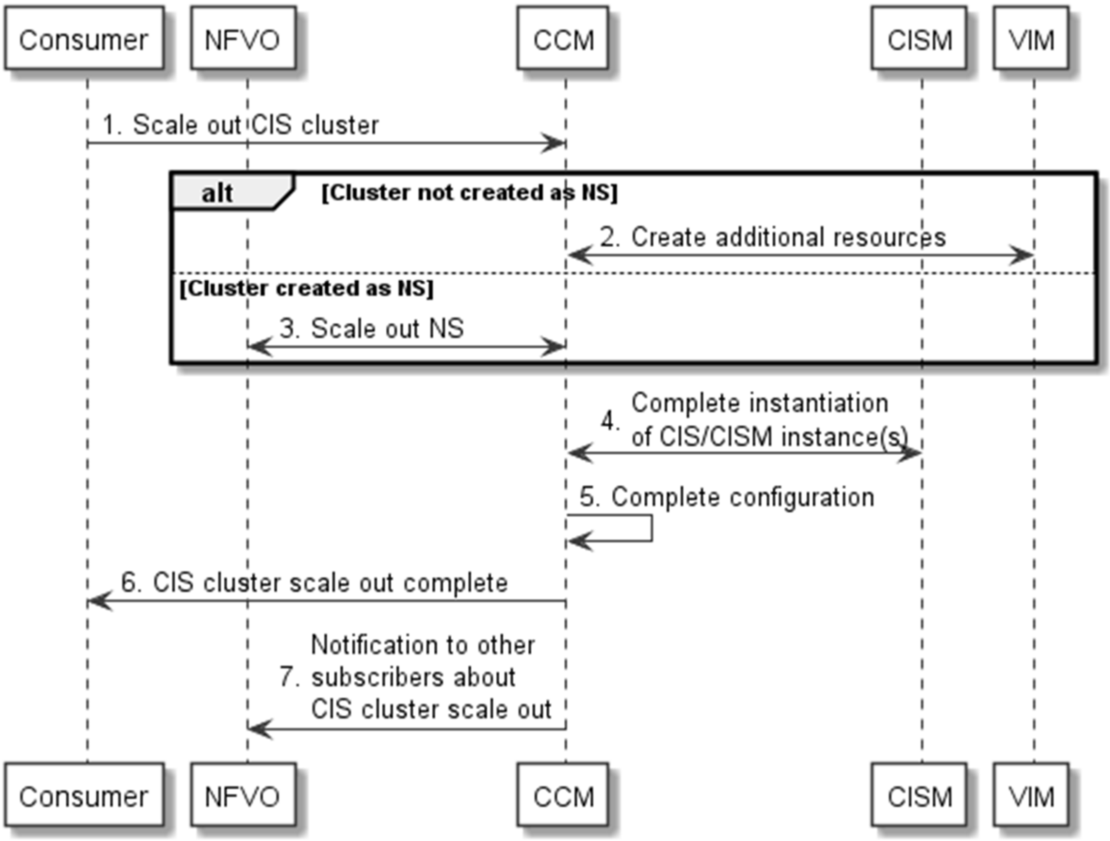
Consumer
NFVO
CCM
CISM
VIM
1. Scale out CIS cluster
alt
[Cluster not created as NS]
2. Create additional resources
[Cluster created as NS]
3. Scale out NS
4. Complete instantiation of CIS/CISM instance(s)
5. Complete configuration
6. CIS cluster scale out complete
7. Notification to other subscribers about CIS cluster scale out
Consumer
NFVO
CCM
CISM
VIM

Figure B.6.5-1: Scale out a CIS cluster

1) The Consumer triggers scaling out of a CIS cluster. The Consumer can be the OSS, the NFVO or another entity managing the infrastructure for a Service Provider. The Consumer provides the necessary information for the desired new size of the CIS cluster, e.g. requirements of the desired additional resources.

NOTE 1: The Consumer decides on the scaling out using performance data, expected load changes or other inputs which is outside the scope of the present document.

2) In the case the CIS cluster was not created as an NS, the CCM creates the desired additional CIS cluster resources as it is described in clause B.2.5, steps 2 to 16.

NOTE 2: In this case, this includes that the CCM requests the NFVO to grant the process of resource management.

3) In the case the CIS cluster was created as an NS, the CCM uses an NS scale out operation with similar steps as in the CIS cluster creation described in clause B.3.5, steps 2 to 4.

NOTE 3: The steps 2 and 3 includes the necessary resources for the connectivity of additional resources.

4) The CCM completes the instantiation of additional CIS and/or CISM instances.

NOTE 4: In the case the CIS cluster was not created as an NS, these actions are similar to steps 17 to 21 in clause B.2.5, in case of a CIS cluster that was created as an NS, the steps are similar to steps 5 to 8 in clause B.3.5.

NOTE 5: This step includes operations on the additional CIS and/or CISM instances that are executed by the CISM, which is also aware of any MCCOs (e.g. representing daemon objects) applied in the CIS cluster and triggers necessary actions.

5) Finally, additional configuration can be performed, e.g. for the CIS cluster nodes network and for cluster external networks and interfaces of the CIS cluster.

6) CCM notifies the Consumer about the successful CIS cluster scaling providing necessary information e.g. the new CIS cluster capacity.

7) CCM also sends notification to other subscribers about the successful scaling of the CIS cluster providing similar information.

B.7 Instantiation of a NS containing containerized VNFs

B.7.1 Introduction

This workflow demonstrates several aspects that can occur during NS instantiation. The well-known actions necessary for typical NS and VNF instantiation are not illustrated in detail, as well as the steps necessary for a CIS cluster LCM action if contained within the flow. The focus of the workflow is on the NFVO actions that are part of CIS cluster selection and illustrates triggers for CIS cluster LCM operations if no appropriate cluster can be found.

There can be different scenarios how a Consumer manages CIS clusters (e.g. directly interfacing with CCM or via a NFVO (e.g. using policies), or whether the Consumer uses NSs to deploy CIS cluster (see clause B.3). The description of this workflow tries to be independent of such differences.

B.7.2 Actors

Table B.7.2-1: Instantiation of a NS containing containerized VNFs, actors and roles

#	Actor	Description
1	Consumer	Either the OSS or other management system (e.g. NFVO) responsible for initiating the NS instantiation and the management of the CIS clusters. See note 1.
2	NFVO	NFV Orchestrator of the NFV system that is expected to orchestrate NSs and VNFs and also during the CIS cluster LCM is responsible for the granting process. See note 2.
3	VNFM	VNF Manager that is expected to execute the LCM for the VNF(s).
4	CCM	CIS Cluster Management function to manage CIS clusters for the Consumer. See note 3.
5	CISM	Container Infrastructure Service Management Function that deploys containerized workloads in the cluster.
NOTE 1: Depending on the workflows of the operator, the roles can be split and different Consumers can be responsible for NS LCM or CIS cluster LCM. This is not illustrated in the present use case. NOTE 2: There can be multiple NFVOs for multiple administrative domains involved, either for nested NSs or for multiple CIS clusters or CCMs. Multiplicity and multiple administrative domains are not illustrated in the present use case. NOTE 3: There can be multiple CCMs in an NFV system, responsible for CIS cluster management in different administrative domains. Multiple CCMs are not illustrated in the present use case.		

B.7.3 Pre-Conditions

Table B.7.3-1: Instantiation of a NS containing containerized VNFs, pre-conditions

#	Pre-condition	Description
1	NFV-MANO (VIM, NFVO and VNFM) and CCM are running.	
2	Connectivity between OSS, NFV-MANO and CCM is available.	
3	For the case of bare-metal CIS clusters, a pool of physical resources is available, managed via other infrastructure management function.	
4	NFVO is subscribed to receive notifications from the CCM.	
5	NSD and constituent descriptors and VNF packages are onboarded.	
6	Appropriate CCD(s) and constituent descriptors are onboarded.	

B.7.4 Post-Conditions

Table B.7.4-1: Instantiation of a NS containing containerized VNFs, post-conditions

#	Post-condition	Description
1	The NS is successfully instantiated. If necessary, new CIS cluster(s) have been created or existing ones have been scaled to accommodate the instantiation.	
2	The Consumer and NFVO are notified of the NS and CIS cluster LCM operations.	

B.7.5 Description

Figure B.7.5-1 illustrates the flow for scaling out or creating a new CIS cluster to accommodate the instantiation of an NS. The flow is simplified in several ways:

- Details of CIS cluster LCM operations are not shown, since they are identical to the use cases in clause B.2, B.3 or B.6.
- Details of instantiation of containerized VNFs are not shown, since they are shown in the use case in clause B.4.
- Details of the general flow of NS instantiation are not shown. Relevant use cases and flows are documented in annex D of ETSI GS NFV-IFA 010 [2].

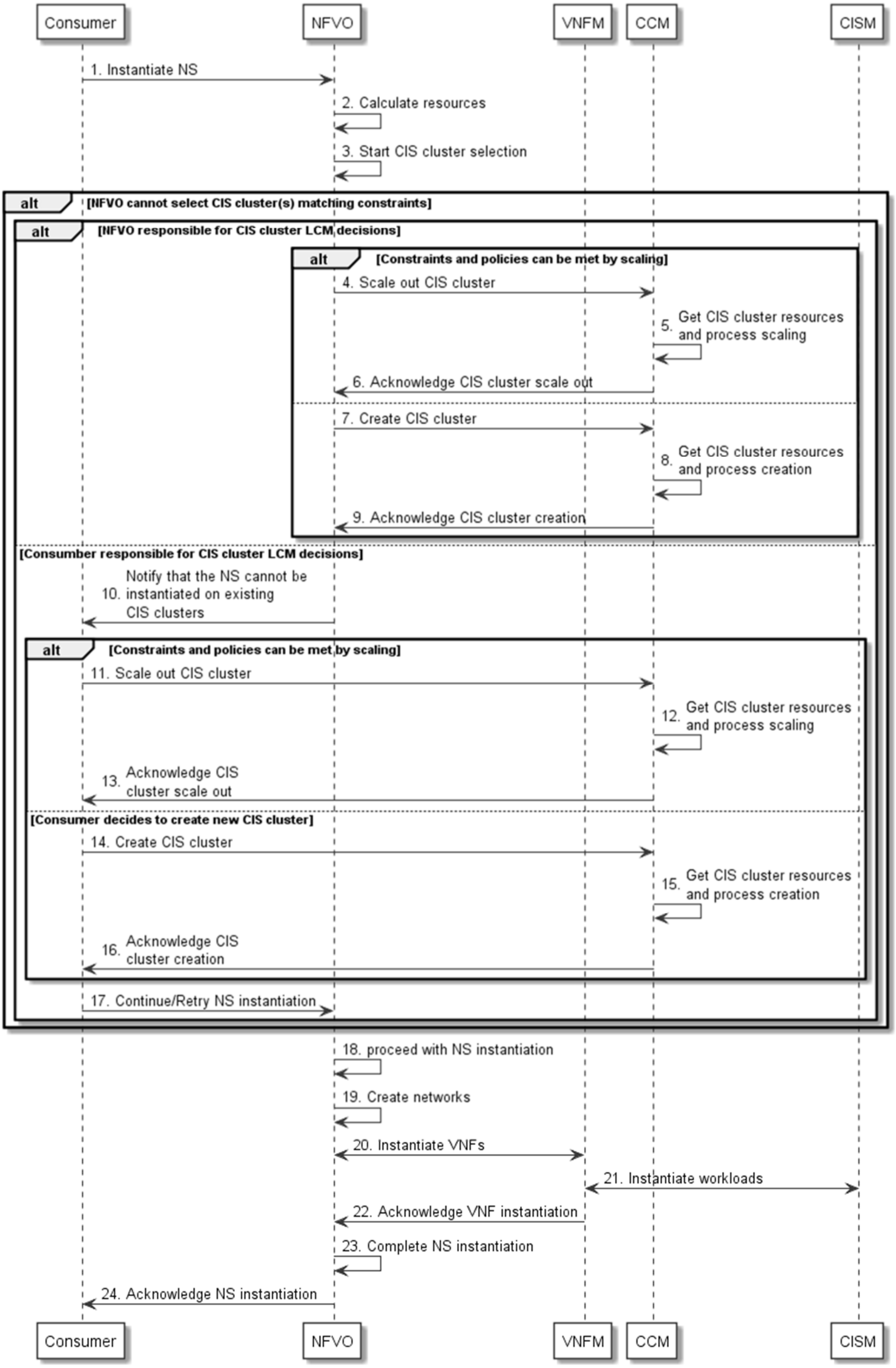
Consumer
NFVO
VNFM
CCM
CISM
1. Instantiate NS
2. Calculate resources
3. Start CIS cluster selection
alt [NFVO cannot select CIS cluster(s) matching constraints]
alt [NFVO responsible for CIS cluster LCM decisions]
alt [Constraints and policies can be met by scaling]
4. Scale out CIS cluster
5. Get CIS cluster resources and process scaling
6. Acknowledge CIS cluster scale out
7. Create CIS cluster
8. Get CIS cluster resources and process creation
9. Acknowledge CIS cluster creation
[Consumer responsible for CIS cluster LCM decisions]
10. Notify that the NS cannot be instantiated on existing CIS clusters
alt [Constraints and policies can be met by scaling]
11. Scale out CIS cluster
12. Get CIS cluster resources and process scaling
13. Acknowledge CIS cluster scale out
[Consumer decides to create new CIS cluster]
14. Create CIS cluster
15. Get CIS cluster resources and process creation
16. Acknowledge CIS cluster creation
17. Continue/Retry NS instantiation
18. proceed with NS instantiation
19. Create networks
20. Instantiate VNFs
21. Instantiate workloads
22. Acknowledge VNF instantiation
23. Complete NS instantiation
24. Acknowledge NS instantiation
Consumer
NFVO
VNFM
CCM
CISM

Figure B.7.5-1: Instantiation of a NS containing containerized VNFs

1) The Consumer decides to instantiate an NS and requests to the NFVO to create NS identifier and instantiate NS as described in ETSI GS NFV-IFA 013 [i.5].

2) The NFVO analyses the NSD, constituent descriptors and referenced packages and placement constraints and calculates the resources needed for the instantiation of the NS.

3) The NFVO analyses the need for CIS cluster(s) and tries to select the CIS cluster(s) for all containerized VNFs in the NS. In case that one or more CIS cluster(s) can be selected, the flow continues in step 18.

Steps 4 to 9 describe the case that NFVO is the entity responsible to take decisions on CIS cluster LCM.

4) In case the NFVO, based on current runtime information and policies, decides that the placement constraints can be met and sufficient resources can be provided by scaling out existing CIS cluster(s), the NFVO requests the CCM to scale out one or more CIS cluster(s).

5) The CCM allocates resources and scales out one or more CIS cluster(s) as shown in the flow in clause B.6.

6) The CCM acknowledges to the NFVO the successful CIS cluster scaling.

7) In case the NFVO, based on current runtime information and policies, decides to create additional CIS cluster(s), the NFVO requests the CCM to create one or more CIS cluster(s).

8) The CCM allocates resources and creates one or more CIS cluster(s) as shown in the flow in clause B.2 or B.3.

9) The CCM acknowledges to the NFVO the successful CIS cluster creation.

Steps 10 to 17 describe the case that the Consumer is responsible to make decisions on CIS cluster LCM.

10) The NFVO notifies the Consumer that the NS instantiation cannot be executed and provides the Consumer with information about the reason why no CIS cluster could be selected.

11) In case the Consumer, based on current runtime information and policies, decides that placement constraints can be met and sufficient resources can be provided by scaling out existing CIS cluster(s), the Consumer requests the CCM to scale out one or more CIS cluster(s).

12) The CCM allocates resources and scales out one or more CIS cluster(s) as shown in the flow in clause B.6.

13) The CCM acknowledges to the Consumer the successful CIS cluster scaling.

14) In case the Consumer, based on current runtime information and policies, decides to create additional CIS cluster(s), the Consumer requests the CCM to create one or more CIS cluster(s).

15) The CCM allocates resources and creates one or more CIS cluster(s) as shown in the flow in clause B.2 or B.3.

16) The CCM acknowledges to the Consumer the successful CIS cluster creation.

17) The Consumer continues/retries the NS instantiation.

18) Now the CIS cluster(s) and required resources are available and the NFVO can proceed with the NS instantiation.

19) The NFVO together with other management functions, e.g. VIM, creates the networks for the NS.

20) The NFVO requests the VNFM to instantiate the constituent VNFs as shown in the flow in clause B.4.

21) For the containerized VNFs, the VNFM requests the CISM to instantiate the MCIOs.

22) The VNFM acknowledges to the NFVO the VNF instantiation.

NOTE: Granting procedure is not shown.

23) The NFVO completes the NS instantiation.

24) The NFVO acknowledges to the Consumer the NS instantiation.

Annex C (informative): Examples

C.1 Examples of MCCO and their management using open source solutions

C.1.1 Introduction

The subsequent clauses describe examples of MCCO by using an open source solution, e.g. Kubernetes®.

C.1.2 An example for CCEC

In case of using Kubernetes®, CCEC can be mapped to Custom Resource Definition. Figure C.1.2-1 illustrates the overview of applying MCCO for CCEC with CISM, CCM and CIS nodes.

NOTE: In figure C.1.2-1, for the sake of simplicity, Custom Resource Controller is omitted.

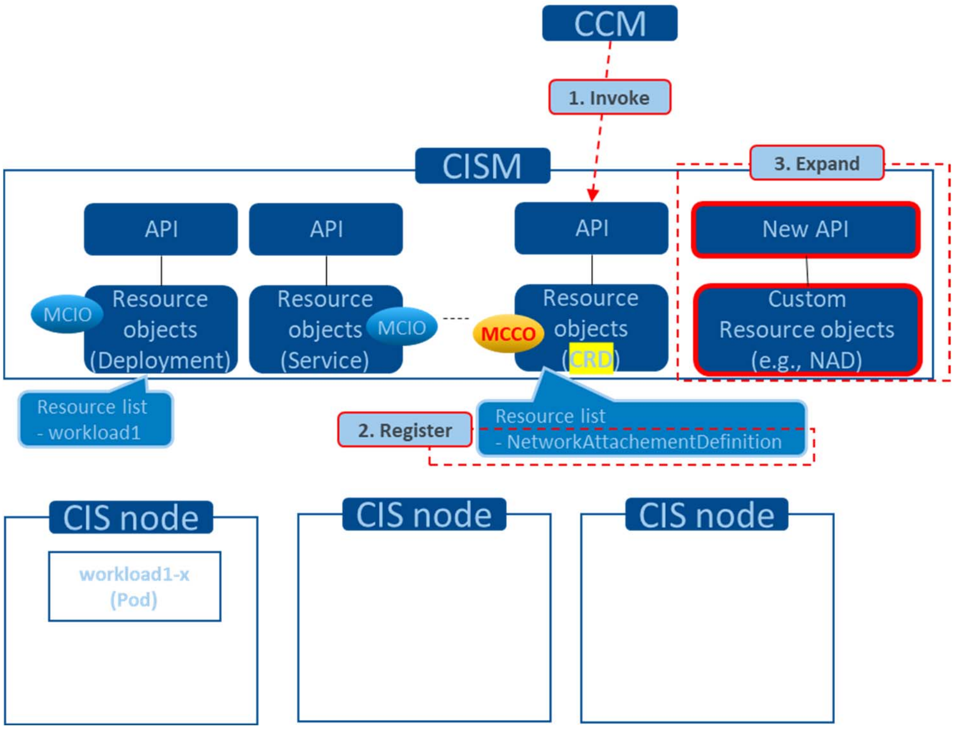

Figure C.1.2-1: Overview of applying MCCO for CCEC

C.1.3 An example for daemon object

In case of using Kubernetes®, daemon object can be mapped to DaemonSet. Figure C.1.3-1 illustrates the overview of applying MCCO to CIS nodes (represented in figure C.1.3-1 as "workload2-ds-x" in each of the CIS nodes) by using a daemon object and the role of the CCM and CISM in this process.

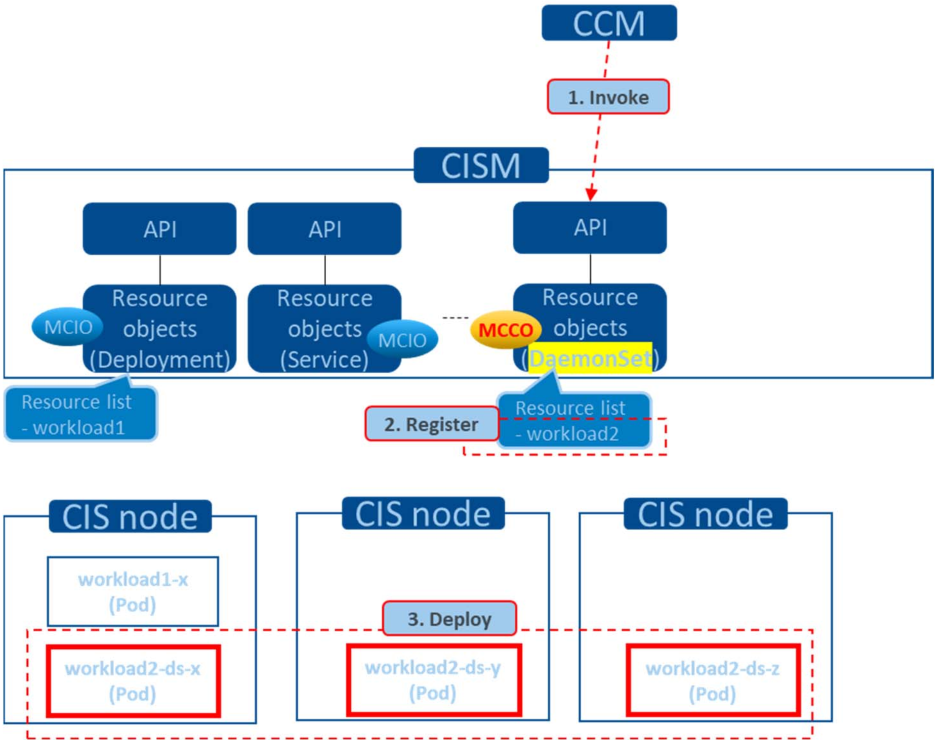

Figure C.1.3-1: Overview of applying MCCO by daemon object

C.2 CIS cluster enhancement capability

C.2.1 Introduction

CCEC is the NFV feature which can be mapped to the open source solution mechanism related to CustomResourceDefinition (CRD) in Kubernetes®. In the present clause C.2, mapping examples between the NFV concept and the open source solution are illustrated.

C.2.2 Example

NFV objects/elements related to CIS cluster enhancement capability enable diverse use cases for CIS cluster management. Example of such use cases include:

- cluster networking and enabling secondary container cluster networks;
- logging information across CIS clusters;
- automation of configuration dedicated to a specific application; and
- enabling Sidecar/Service-mesh oriented-application deployment.

NOTE: The example presented in the present clause does not aim to specify which open source solution to utilize, but to provide information in order for the readers to understand the concept of the feature.

In case of using Multus Container Network Interface (CNI™), CCEC elements and related elements for using the defined enhancement capability can be mapped as seen in table C.2.2-1.

Table C.2.2-1: Mapping for case of using Multus CNI™

ETSI NFV	Open source solution
MCCO declarative descriptor for CCEC	Kubernetes® manifest with the kind "CRD" to define the custom resource "NetworkAttachmentDefinition".
CCEC controller	Kubernetes® Pod (which image is ghcr.io/k8snetworkplumbingwg/multus-cni; precisely, which is expected to be deployed via DaemonSet and whose name might be "kube-multus-ds-xxxx") to watch the status of the custom resource "NetworkAttachmentDefinition".
CCEC resource	The custom resource "NetworkAttachmentDefinition", which is managed as a resource object in database of a relevant Kubernetes® cluster.
MCCO declarative descriptor for CCEC resource	Kubernetes® manifest with the kind "NetworkAttachmentDefinition" to define relevant information to be utilized by Multus CNI™.

C.3 Daemon object

C.3.1 Introduction

Daemon object is the NFV feature which can be mapped to the open source solution mechanism related to DaemonSet in Kubernetes®. In the present clause C.3, mapping examples between the NFV concept and the open source solution are illustrated.

C.3.2 Example

NFV objects/elements related to daemon objects enable diverse use cases for CIS cluster management. Example of such use cases include:

- monitoring status of each CIS cluster node;
- logging information on each CIS cluster node; and
- dynamically configuring routing information on each CIS cluster node.

NOTE: The example presented in the present clause does not aim to specify which open source solution to utilize, but to provide information in order for the readers to understand the concept of the feature.

In case of using Fluentd®, daemon object elements and related elements can be mapped as seen in table C.3.2-1.

Table C.3.2-1: Mapping for case of using Fluentd®

ETSI NFV	Open source solution
MCCO declarative descriptor for daemon object	Kubernetes® manifest with the kind "DaemonSet" to deploy Kubernetes® Pods including the container image for Fluentd®.
MCCO instantiated as the daemon object	Kubernetes® DaemonSet, which is a resource object created in a control plane based on the above manifest.
MCCO instance deployed on each CIS cluster node based on the daemon object	Kubernetes® Pod (which image is quay.io/fluentd_elasticsearch/fluentd; precisely, which are deployed via the DaemonSet and whose name might be "fluentd-elasticsearch-ds-xxxx") to collect data related to each CIS cluster node.

Annex D (informative): Cluster networking

D.1 CIS cluster networking aspects solutions

Table D.1-1 lists solutions and examples for the set of CIS cluster networking aspects described in clause 4.2.6.4.

Table D.1-1: Solutions and examples of CIS cluster networking aspects

Aspect	Solution	Description	Examples
IP address management	Dynamic IP address allocation	IP addresses are allocated by a Dynamic Host Configuration Protocol (DHCP) server running on the CIS cluster nodes network. Thus, to enable such solution, the availability of a DHCP server is pre-condition for the setup on the CIS cluster nodes.	CNI™'s dhcp IP Address Management (IPAM) [i.6]
	Local IP address range allocation	IP addresses are allocated out of a specified address range. Uniqueness of addresses are only ensured from the range of IP addresses pre-allocated to the CIS cluster node. For enabling such a solution, the CCM configures on the CIS cluster nodes the address ranges of use for each of the CIS cluster nodes.	CNI™'s host-local IPAM [i.6]
	Static IP address allocation	IP address is allocated statically to the groups of one or more OS containers. For enabling such a solution, the CCM configures the applicable network plugin executables on the CIS cluster nodes with the appropriate "static" setting. IP address for the group of one or more OS containers can be set during the containerized workload management via the CISM.	CNI™'s static IPAM [i.6]
Packet forwarding within the CIS cluster	Overlay network	A network layered on top of another network (underlay network), typically created by encapsulating (tunnelling) packets among endpoints of the underlay network, and devices connected to the endpoints become then part of the overlay network. For enabling such a solution, the CCM configures the applicable network plugin executables on the CIS cluster nodes along with their associated particular overlay format configuration.	VXLAN, IP-in-IP. (Flannel)
	Non-overlay network with L3 routing	Routing peering is established among CIS cluster nodes and network devices which become part of the CIS cluster nodes network. Additional routing protocols enable the exchange of routing information enabling then packets to get routed among the network devices. Routing protocol can run on both CIS cluster nodes and underlay network nodes (e.g. in the NFVI), i.e. routing peering can be established with CIS cluster nodes, route reflectors and network nodes (e.g. Top of Rack (ToR) routers). For enabling such a solution, the CCM configures the applicable network plugin executables on the CIS cluster nodes along with the corresponding L3 routing and peering information.	Border Gateway Protocol (BGP) peering with the CIS cluster nodes network: virtual network (Calico), physical network (Calico, MetalLB)
	L2 underlay	CIS cluster nodes belong either to the same L2 physical network or same VLAN, and L2 bridging or direct mode configuration on the CIS cluster node enables packets to/from groups of one or more OS containers to be forwarded among groups of one or more OS containers allocated on different CIS cluster nodes.	CNI™'s bridge, macvlan, etc., [i.6]
Packet forwarding external to the CIS cluster	L3 site (DC) routing	CIS cluster nodes have connectivity via the NFVI network to DC gateway routing devices which route between external networks and the container cluster networks.	Kubernetes® Service with external IP Kubernetes® Service NodePort
	L3/L4 Load-balancing	Infrastructure-provided load balancing devices route between the container cluster network and the external network using layer 3 and 4 information, such as IP addresses and transport ports.	Kubernetes® Service LoadBalancer

Aspect	Solution	Description	Examples
	L7 Load-balancing	Application load balancers route L7 application traffic between the container cluster network and the external network.	Kubernetes® Ingress

D.2 Common solutions for OS container network interfaces

Table D.2-1 provides a list of common solutions to enable the network interfaces for the groups of one or more OS containers.

Table D.2-1: Common solutions for OS container network interfaces

Solution	Description	Exemplary use cases	Examples
Bridging	Groups of one or more OS containers are connected to a bridge (virtual switch) residing on the CIS cluster node. Groups of one or more OS containers get a virtual interface. The bridge can act as a gateway if provided an IP address, or bridge at L2 with the CIS cluster node's network interface.	Enable connectivity among groups of one or more OS containers on the same CIS cluster node and across CIS cluster nodes.	CNI™'s bridge [i.6]
Host interface	The groups of one or more OS containers use directly a CIS cluster node's network interface.	Enable use of devices with DPDK.	CNI™'s host-device [i.6]
Virtual interface	The groups of one or more OS containers get a virtual interface linked point-to-point to a CIS cluster node's node interface, or a virtual sub-interface associated to the CIS cluster node's node interface either with the same or distinct MAC address as the CIS cluster node's network interface.	Enable connectivity among groups of one or more OS containers on the same CIS cluster node and across CIS cluster nodes.	CNI™'s ptp, macvlan, ipvlan [i.6]

Annex E (informative): Change History

Date	Version	Information about changes
October 2019	0.0.1	First draft, introducing the document skeleton (NFVIFA(19)000845r1)
December 2019	0.0.2	NFVIFA(19)000846 IFA036 Scope Approved IFA#170 NFVIFA(19)000893 IFA036-Remove Annex -Authors and contributors Approved IFA#173 NFVIFA(19)000945r3 IFA036 Problem Statement Approved IFA#177
August 2020	0.0.3	NFVIFA(20)000469r4 IFA036 Scope update NFVIFA(20)000520r3 IFA036 4.x Relationship among key concepts NFVIFA(20)000522r3 IFA036 Clause 4.2 Introduction NFVIFA(20)000523r2 IFA036 Clause 4.3 Framework NFVIFA(20)000524r1 IFA036 Annex on container related services NFVIFA(20)000525r3 IFA036 Clause 3.1 Term Definitions
October 2020	0.0.4	NFVIFA(20)000558r2 IFA036 Clause 3.1 Term Definitions of CCM NFVIFA(20)000603r1 IFA036 Fix typos in Version 003 NFVIFA(20)000609r5 IFA036 Clause 5.1 Requirements of CCM NFVIFA(20)000625r1 IFA036 5.x Service interface requirements for CIS instance management
January 2021	0.0.5	NFVIFA(20)000730r1 IFA036 4.2.2 Lifecycle management for CIS cluster NFVIFA(20)000688r1 IFA036 Enhance Clause 4 to cover input from discussion papers NFVIFA(20)000697r1 IFA036 Update for Annex A
February 2021	0.0.6	NFVIFA(20)000895r5 IFA036 Annex B Flow for Create CIS Cluster NFVIFA(21)000027r3 IFA036 4.2.3 Placement of CIS clusters and resources NFVIFA(21)000028r2 IFA036 4.2.4 CIS cluster characteristics
April 2021	0.0.7	NFVIFA(21)000151r3 IFA036 Preconditions etc for flow in B.2 NFVIFA(21)000169r4 IFA036 Annex B Flow for Instantiation of a containerized VNF NFVIFA(21)000295r2 FEAT17 IFA036 CIS cluster selection and VNF placement
June 2021	0.0.8	NFVIFA(21)000394r1 IFA036 4.2.8 Relation of CIS cluster management and resource management NFVIFA(21)000395r1 IFA036 4.2.9 Relation of Network Services and CIS cluster NFVIFA(21)000396r2 IFA036 4.2.10 Relation namespace and CIS cluster NFVIFA(21)000406r2 IFA036 4.2.11 FCAPS management for CIS clusters
September 2021	0.0.9	NFVIFA(21)000294r2 IFA036 Clause 4.2.5 Adding cluster networking NFVIFA(21)000616r1 IFA036 some small fixes NFVIFA(21)000449r4 FEAT17 IFA036 4.2.6 Cluster storage NFVIFA(21)000709r3 FEAT17 IFA036 Enhanced CIS Cluster Capability NFVIFA(21)000744r2 FEAT17 IFA036 Daemon workload NFVIFA(21)000791r1 IFA036 Clause 5.1.3 Updating requirements considering networking
November 2021	0.0.10	NFVIFA(21)000795r2 IFA036 Extend Overview NFVIFA(21)000867r1 IFA036 Clause 6 Overview and skeleton NFVIFA(21)000910r2 IFA036 6.2 CIS cluster related descriptors NFVIFA(21)000919r1 IFA036 start resolve editors notes NFVIFA(21)000925r3 IFA036 Clause 3, 4.2, Annex MCCO description and definition of CCEC NFVIFA(21)000934r3 FEAT17 IFA036 Clause 5.1 Updating requirements of CIS cluster storage
November 2021	0.0.11	NFVIFA(21)000922r3 IFA036 Annex Workflow Daemon Workload NFVIFA(21)000946 IFA036 Abbreviations and more NFVIFA(21)000947r3 IFA036 Add clause 6.2.2 on CCND
December 2021	0.0.12	NFVIFA(21)000957r2 FEAT17 IFA036 skeleton for clause 6.3 NFVIFA(21)0001004r2 FEAT17 IFA036 Clause 4.2.5 Addressing ENs networking NFVIFA(21)0001005 FEAT17 IFA036 Clauses 4.2.3 4.2.8 and new Addressing ENs placement and hybrid CIS cluster NFVIFA(21)0001006r1 FEAT17 IFA036 Clause 4.2.7 Addressing ENs CIS cluster selection NFVIFA(21)0001007 FEAT17 IFA036 Clause 4.2.12 4.2.13 and 4.2.14 Addressing ENs about MCCO CCEC and daemon object NFVIFA(21)0001008r1 FEAT17 IFA036 Clause 5.1.3 and 5.2.3 Reqs about placement and CIS selection NFVIFA(21)0001016r1 FEAT17 IFA036 Clause 5.2 CISM MCCO management service requirements

Date	Version	Information about changes
		NFVIFA(21)0001023r1 FEAT17 IFA036 contents for MDD Commonality NFVIFA(21)0001024 FEAT17 IFA036 contents for MDD CCEC & Daemon object NFVIFA(21)0001026 FEAT17 IFA036 contents for MDD specific MCCO NFVIFA(21)0001027 FEAT17 IFA036 security aspect for clause 4.2.11 NFVIFA(21)0001046 IFA036 clause 2 3 ENs resolution NFVIFA(21)0001047r1 IFA036 clause 4.1 EN s resolution NFVIFA(21)0001048 IFA036 clause 4.2.1 EN s resolution NFVIFA(21)0001049 IFA036 clause 4.2.4 ENs resolution NFVIFA(21)0001050r1 IFA036 clause 4.2.9 ENs resolution
January 2022	0.0.13	NFVIFA(21)0001040r2 IFA036 5.1 Add CIS cluster configuration management requirements NFVIFA(21)0001041r2 IFA036 5.1 Add CIS cluster performance management requirements NFVIFA(21)0001042r3 IFA036 5.1 Add CIS cluster fault management requirements NFVIFA(22)000011 IFA036 D.1 ENs' resolution
February 2022	0.0.14	NFVIFA(22)000029r1 IFA036 Clarify CIS Cluster Identification NFVIFA(22)000030r1 IFA036 Resolve EN on runtime characteristics NFVIFA(22)000031 IFA036 Two small changes NFVIFA(22)000032 IFA036 Remove an Editors Note in Clause 4.2.1 NFVIFA(22)000033 IFA036 Remove some Editors Notes in Clause 6.1 NFVIFA(22)000034 IFA036 Update table in Annex A
February 2022	0.0.15	NFVIFA(22)000055r2 IFA036 5.1.5 EN's resolution NFVIFA(22)000056r1 IFA036 5.1.6 EN's resolution NFVIFA(22)000057r1 IFA036 4.2.11 EN's resolution NFVIFA(22)000058r1 IFA036 5.1.2 EN's resolution NFVIFA(22)000059r1 IFA036 typo corrections NFVIFA(22)000060r1 FEAT17 IFA036 4.2.6 Cluster storage EN resolution NFVIFA(22)000064r1 FEAT17 IFA036 RBAC declarative descriptors NFVIFA(22)000065 FEAT17 IFA036 Clarification on clause 6 NFVIFA(22)000066r1 FEAT17 IFA036 EN resolution in clause 4.2.7 NFVIFA(22)000084r1 FEAT17 IFA036 Clause 4.2.11 FM-related EN resolution NFVIFA(22)000016r4 IFA036 - VNF-based CIS clusters Some editorial corrections
March 2022	0.0.16	NFVIFA(22)000010r1 IFA036 B.2.1 ENs resolution NFVIFA(22)000113r2 IFA036 4.2.4 EN s resolution NFVIFA(22)000114r1 IFA036 5.1.3 EN s resolution NFVIFA(22)000115r1 IFA036 5.2.3 EN s resolution NFVIFA(22)000116r1 IFA036 6.1 EN s resolution NFVIFA(22)000117r1 IFA036 6.2.2 EN s resolution NFVIFA(22)000118r1 IFA036 B.1 EN s resolution NFVIFA(22)000119r1 IFA036 B.2.5 EN s resolution NFVIFA(22)000120r1 IFA036 1 EN s resolution NFVIFA(22)000135r1 IFA036 Annex A EN s resolution NFVIFA(22)000137r1 IFA036 4.2.7 EN fix terminology usage MCIO/Workload NFVIFA(22)000138r1 IFA036 Fix more terminology issues
April 2022	0.0.17	NFVIFA(22)000136r2 IFA036 Annex B.2 EN s resolution NFVIFA(22)000267r1 FEAT17 IFA036 Clause 4.2.6 Storage-related EN resolution NFVIFA(22)000281 FEAT17 IFA036 Multiple clauses Various EN handling NFVIFA(22)000284 IFA036 5.1.2 EN's resolution
May 2022	0.0.18	NFVIFA(22)000242r3 IFA036 6 EN s resolution NFVIFA(22)000285r4 IFA036 6.1 EN s resolution NFVIFA(22)000301 IFA036 Align B3 to 136r2 NFVIFA(22)000300r1 IFA036 Annex B.6 Scaling out a CIS cluster
June 2022	0.0.19	NFVIFA(22)000316r2 IFA036 Bare Metal CIS clusters NFVIFA(22)000317r1 IFA036 CCNRD for bare metal NFVIFA(22)000340 IFA036 Update Clause 4.2.1 NFVIFA(22)000341 IFA036 Change order of clauses in clause 4.2 NFVIFA(22)000342 IFA036 Update Clause 4.3 NFVIFA(22)000343 IFA036 Remaining Editor s Notes NFVIFA(22)000344r1 IFA036 Annex B7 NS Instantiation Work Flow

Date	Version	Information about changes
July 2022	0.0.20	NFVIFA(22)000438r1 IFA036 review clause 4.1 editorial clean-up NFVIFA(22)000459 IFA036 update clause 4.2.1 NFVIFA(22)000464r1 IFA036 review on removing IFA035 reference NFVIFA(22)000465r1 IFA036 review CIS cluster assurance management service requirements handling NFVIFA(22)000466r1 IFA036 review clause 4.2.1 editorial clean-up NFVIFA(22)000467r1 IFA036 review clause 4.2.2 editorial clean-up NFVIFA(22)000474r1 IFA036 review clause 4.2.5.4 EN resolution NFVIFA(22)000478 IFA036 review clause 4.2.9 editorial clean-up NFVIFA(22)000489r1 IFA036 review clause 6 editorial clean-up
July 2022	0.0.21	NFVIFA(22)000437r2 IFA036 review clause 3 definition improvement NFVIFA(22)000499r1 IFA036 review alignment on usage of CIS cluster creation NFVIFA(22)000500 IFA036 review handling of abbreviation first occurrence NFVIFA(22)000524 IFA036 review informative reference supplement NFVIFA(22)000527 IFA036 definition addition of hybrid CIS cluster NFVIFA(22)000528r2 IFA036 addition and clarification of security aspects NFVIFA(22)000532 IFA036 Inconsistency on bare metal and other corrections NFVIFA(22)000529r2 FEAT17 IFA036 editorial changes and clarification
July 2022	0.0.22	NFVIFA(22)000530r1 FEAT17 IFA036 consistency on Cluster nodes network NFVIFA(22)000531r2 FEAT17 IFA036 modification for requirements on storage NFVIFA(22)000535 IFA036 review aligning notations on referencing annexes NFVIFA(22)000536r1 IFA036 review MCCO management related description improvement NFVIFA(22)000537r1 IFA036 review clause B.5 daemon object workflow improvement NFVIFA(22)000538r1 IFA036 review storage related description improvement NFVIFA(22)000559 FEAT17 IFA036 Additional CIS security alignment Editorial corrections and consistent formatting, consistent wording in flow diagrams

History

Document history		
V4.3.1	September 2022	Publication