ETSI GS NFV-IFA 040 V4.5.1 (2023-09)

GROUP SPECIFICATION

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

Disclaimer

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

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 the NFV object model for OS container management and orchestration. The present document also specifies requirements on the list of services to be offered by architectural elements providing the Container Infrastructure Service Management (CISM) and Container Image Registry (CIR) functions described in ETSI GR NFV-IFA 029 [i.2] and on the interfaces for exposing these services to NFV-MANO and other consuming entities.

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 010: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification".

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

[i.4]   ETSI GS NFV 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architectural Framework Specification".

[i.5]   ETSI GR NFV-IFA 038: "Network Functions Virtualisation (NFV) Release 4; Architectural framework; Report on network connectivity for container-based VNF".

3   Definition of terms, symbols and abbreviations

3.1   Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] apply.

3.2   Symbols

Void.

3.3   Abbreviations

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

4   Overview and framework for OS container management and orchestration

4.1   Introduction

The NFV-MANO architectural framework described in ETSI GS NFV 006 [i.4] identifies the following functional blocks/entities:

- NFV Orchestrator (NFVO);

- VNF Manager (VNFM); and

- Virtualised Infrastructure Manager (VIM).

ETSI GR NFV-IFA 029 [i.2] identifies the following functions required for the management and orchestration of OS containers:

- Container Infrastructure Service Management (CISM); and

- Container Image Registry (CIR).

The CISM is responsible for maintaining the containerized workloads as Managed Container Infrastructure Objects (MCIOs).

The CIR is responsible for storing and maintaining information of OS container software images.

The functional requirements for the CISM and the CIR specified in ETSI GS NFV-IFA 010 [1] shall apply.

The requirements for the VNF Package and the information elements for the VNFD to support OS container management and orchestration specified in ETSI GS NFV-IFA 011 [2] shall apply.

The present document specifies the requirements on the list of services to be provided by the CISM and the CIR, and on the management services interfaces to expose these services to other NFV-MANO functional entities and/or external entities outside NFV-MANO.

4.2   Framework

4.2.1   Overview

The CISM and CIR 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 OS containers are exposed via management service interfaces by the CISM and CIR 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.

The CISM and CIR functions produce the management service interfaces, which are invoked by consumers within an NFV-MANO functional entity and/or within an external entity outside NFV-MANO.

4.2.2   CISM function and CISM services

The CISM function offers multiple types of CISM services, i.e. OS container management services or other services, which are exposed by the OS container management service interfaces or other service interfaces respectively. More than one instance of an OS container management service interface is possible to cater for the possibility to expose different versions of a type of OS container management service interface. Other services than the OS container management services that may be offered by the CISM are not specified in the present document.

Figure 4.2.2-1 illustrates an example of the relationship between the different concepts introduced in the present clause.

The CISM function acts as the producer of three specific instances of OS container management services and their associated OS container management service interfaces plus one instance of another CISM service and its associated service interface. In this example, the types of CISM services are: "OS container management service A", "OS container management service B", "CISM service C", and "OS container management service D". The instance of "OS container management service D" is available and accessible via the same type of OS container management service interface, but through different interface instances providing different API endpoints. As an example, the API endpoints can provide different paths indicating the support of different versions of the same type of OS container management service interface. The example in figure 4.2.2-1 also shows three consumer instances, namely "NFV-MANO functional entity X", "NFV-MANO functional entity Y", and "external entity Z". Each consumer instance may access one or more CISM services via their respective service interfaces.
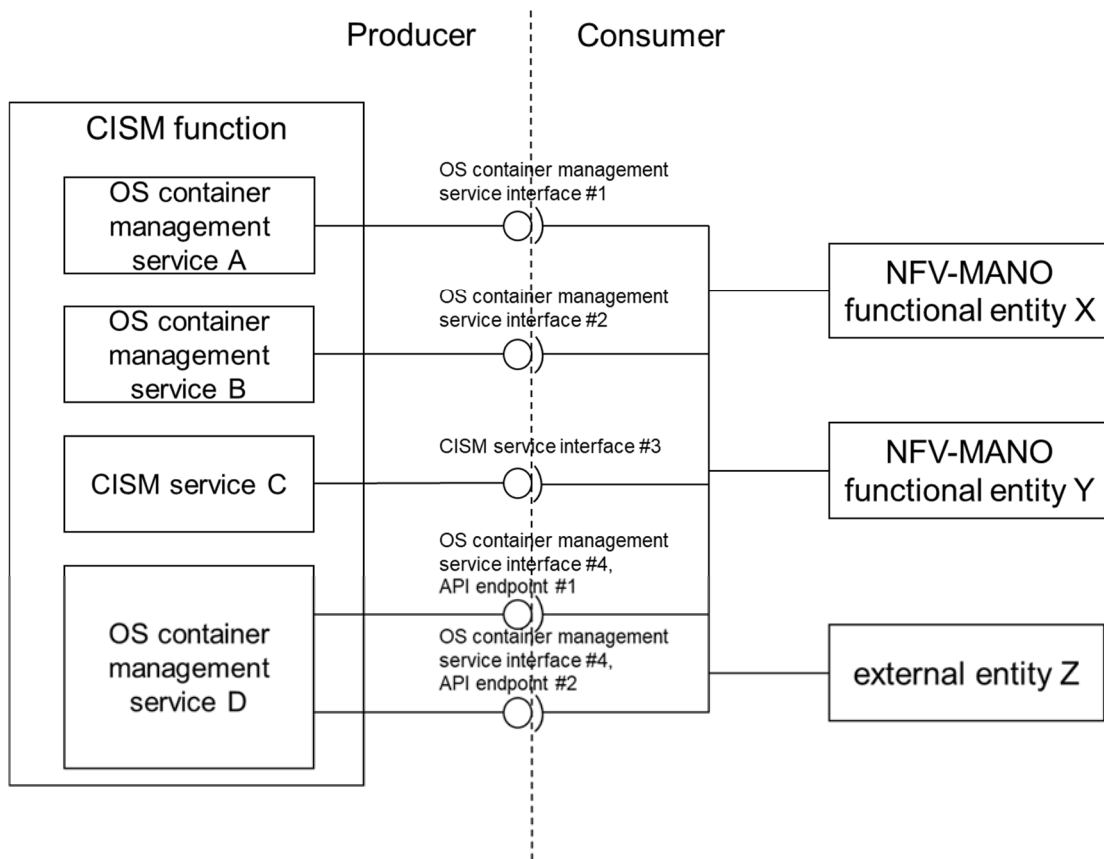
**Figure 4.2.2-1: Example of CISM function, CISM services, OS container
management service interfaces, and consumers**

4.2.3   CIR function and CIR services

The CIR function offers multiple types of OS container image management services, which are exposed by the OS container image management service interfaces. More than one instance of an OS container image management service interface is possible to cater for the possibility to expose different versions of a type of OS container image management service interface.

Figure 4.2.3-1 illustrates an example of the relationship between the different concepts introduced in the present clause.

The CIR function acts as the producer of three specific instances of OS container image management services and their associated OS container image management service interfaces. In this example, the types of CIR services are: "OS container image management service A", "OS container image management service B", and "OS container image management service C". The instance of "OS container image management service C" is available and accessible via the same type of OS container image management service interface, but through different interface instances providing different API endpoints. As an example, the API endpoints can provide different paths indicating the support of different versions of the same type of OS container image management service interface. The example in figure 4.2.3-1 also shows three consumer instances, namely "NFV-MANO functional entity X", "NFV-MANO functional entity Y", and "external entity Z". Each consumer instance may access one or more OS container image management services via their respective OS container image management service interfaces.
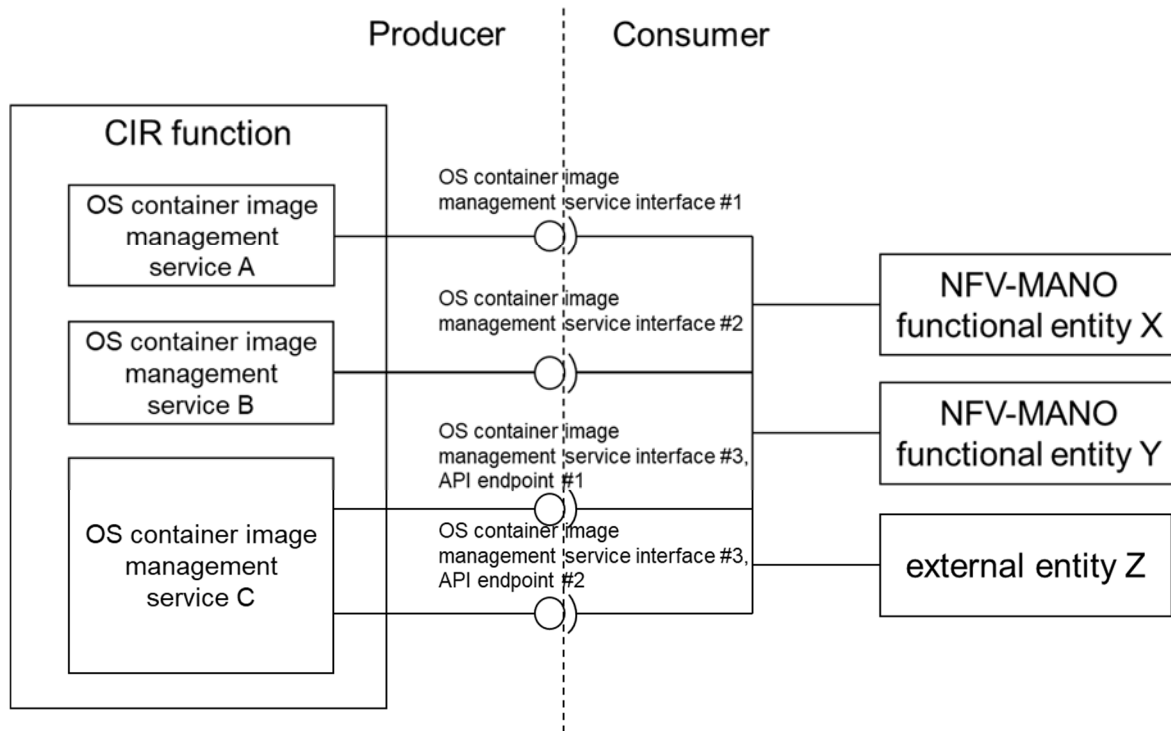
**Figure 4.2.3-1: Example of CIR function, OS container image management services,
OS container image management service interfaces, and consumers**

5   OS container NFV object model

5.1   Introduction

Clause 5 of the present document specifies the NFV object model for OS container management and orchestration. It describes and specifies abstract NFV objects related to OS container management and orchestration. It also specifies the relationship of these abstract NFV objects to the information models of NFV-MANO. The terms for these abstract NFV objects are used in the subsequent clauses of the present document to specify generic requirements on the services and management service interfaces exposed by the CISM and the CIR. The abstract NFV objects are also expected to be used in specifications profiling APIs of de-facto standard solutions, to map the abstract NFV objects to objects of the specific de-facto standard solution.

Some of the abstract NFV objects for OS container management and orchestration have been introduced in ETSI GR NFV-IFA 029 [i.2], but are formally specified in the present document.

5.2   Managed objects

5.2.1   Managed Container Infrastructure Object

5.2.1.1   Purpose

A Managed Container Infrastructure Object (MCIO) is an abstract NFV object for OS container management and orchestration, introduced by ETSI GR NFV-IFA 029 [i.2]. It is an object managed and exposed by the CISM, characterized by the desired and actual state of a containerized workload, including its requested and allocated infrastructure resources and applicable policies. The desired state of an MCIO is specified in a declarative descriptor which may include references to OS container images. This declarative descriptor is interpreted by the CISM.

Different types of MCIOs with different requested infrastructure resources exist. An MCIO is created by the CISM by allocating its requested infrastructure resources on Container Infrastructure Service (CIS) instances. Dependent on its type, the creation of an MCIO may include the deployment of an OS container image. MCIOs are lifecycle managed via change requests on their desired state, utilizing a modified declarative descriptor sent to the CISM, which adapts the infrastructure resource allocations according to the changed infrastructure resource requests.

5.2.1.2   Relationship to the existing NFV-MANO information model

Dependent on its type, an MCIO is represented by a corresponding object in the existing NFV-MANO information model. An MCIO requesting compute and/or storage infrastructure resources is mapped to a VNF Component (VNFC). An MCIO requesting network infrastructure resources for VNF external connectivity is mapped to an applicable sub-class of a Connection Point (CP). Figure 5.2.1.2-1 illustrates the mapping of an MCIO to the existing NFV-MANO logical objects.

NOTE 1: There is no MCIO type equivalent to an internal Virtual Link (VL).
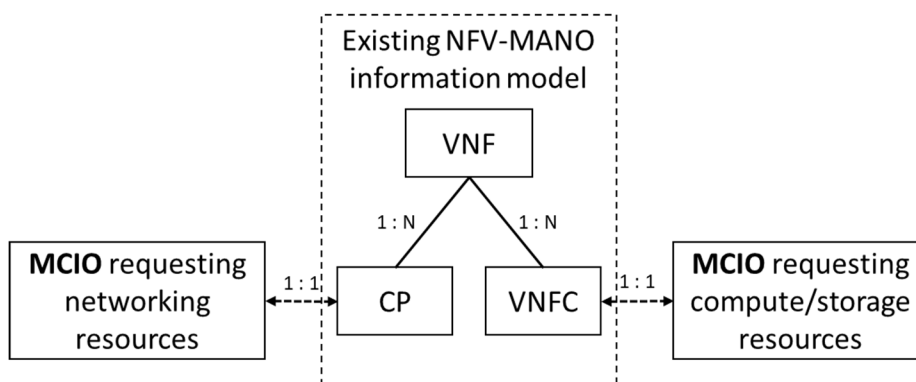
Figure 5.2.1.2-1: MCIO logical model mapping

Properties of an MCIO described in declarative descriptors and relevant being exposed to NFV-MANO are mirrored in attributes of the descriptors of the corresponding objects of the existing NFV-MANO information model. Properties of an MCIO requesting compute and/or storage infrastructure resources are described in attributes of the VDU information element of the VNF Descriptor. Properties of an MCIO requesting network infrastructure resources for VNF external connectivity are described in attributes of applicable sub-classes of the CPD information element of the VNF Descriptor. Figure 5.2.1.2-2 illustrates the specification of an MCIO's properties in enhanced NFV-MANO descriptor objects.

NOTE 2: Properties of MCIO's requesting network infrastructure resources cannot be used to specify requirements on the network infrastructure resources to be used for internal VLs.

NOTE 3: The declarative descriptor of an MCIO cannot be used to specify requirements equivalent to those specified for a VduCP that is not re-exposed as an external CP.
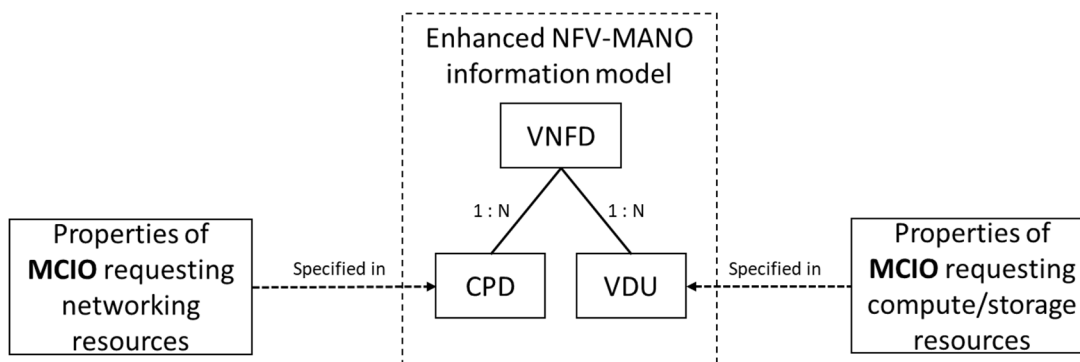
Figure 5.2.1.2-2: MCIO's properties specification

The above defined relationships in between the MCIO, their descriptors, and the NFV IM enables the interoperability of containerized workloads management with NFV management and orchestration. On the one hand, the information contained in NFV descriptors, artefacts and the VNF and NS runtime information held by NFV-MANO, that relates to MCIOs, enable the VNFM and NFVO of NFV-MANO to process relevant resources requirements, and perform the lifecycle, fault and performance management of VNF or VNF components, when these are realized by a set of OS containers. On the other hand, the mapped MCIO, their descriptors and the produced services by the CISM enable the VNFM and NFVO to request the relevant management of the containerized workloads to be deployed and managed on CIS instances.

NOTE 4: While the NFVO and VNFM do not manage individual OS containers, resources information related to OS containers such as images or resource requests can be exchanged and/or visible to the NFVO and VNFM for other purposes such as resources granting, capacity management, namespace management, etc.

5.2.2 Managed Container Infrastructure Object Package

5.2.2.1 Purpose

A Managed Container Infrastructure Object Package (MCIOP) is a hierarchical aggregate of information objects for OS container management and orchestration, introduced by ETSI GR NFV-IFA 029 [i.2]. The aggregate of information objects includes declarative descriptors and configuration files for one or multiple Managed Container Infrastructure Objects (MCIOs).

Configuration files typically specify values for parameters defined in the declarative descriptors. The MCIO configurable parameters are represented by key-value pairs. All the keys corresponding to MCIO configurable parameters are specified in the configuration files. The configuration files may contain values for some of the parameters. The other values are not specified in the configuration files but injected during the related containerized workload management. Furthermore, the values provided in the configuration files may also be overwritten by injecting values.

The MCIOP, representing aggregated containerized workloads, is used to instantiate and maintain containerized workloads and provide a higher abstraction level than individual MCIO declarative descriptors used by the CISM, declaring the relationships among the MCIOs, as addressed in ETSI GR NFV-IFA 029 [i.2].

5.2.2.2 Relationship to the existing NFV-MANO information model

The VNF Package contains both the VNFD and one or multiple MCIOPs. The VNFD and its constituent VDUs are the descriptor objects to instantiate the VNF and its constituent VNFCs. In this context, both the containerized VNF and the containerized VNFCs are regarded as containerized workloads. A containerized workload uses MCIOs during its lifecycle, which are created and maintained by using the declarative descriptors and configuration files for the respective MCIO in the MCIOP.

The relationship between an MCIOP and the existing NFV-MANO information model is shown in figure 5.2.2.2-1. The VNFD of a containerized VNF has references to one or multiple MCIOPs which contain declarative descriptors and configuration files for MCIOs consumed by the containerized VNF.
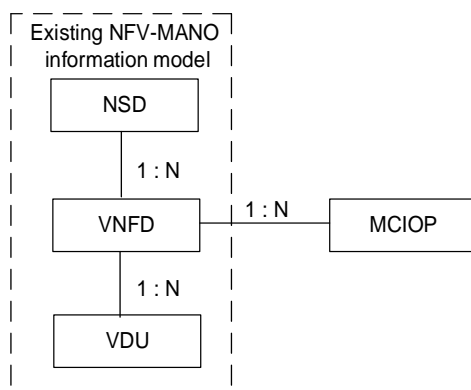

Figure 5.2.2.2-1: MCIOP logical model mapping

5.2.3   Namespace

A namespace is an abstract NFV object for OS container management and orchestration. It is an object managed and exposed by the CISM, representing a logical grouping for a particular set of identifiers, resources, policies and authorizations within the scope of a cluster of CIS instances. A namespace provides a mechanism to isolate its grouped elements from others and provides access control to them. All resources grouped into a namespace can only belong to one namespace.

MCIOs are created by the CISM by allocating infrastructure resources within the scope of a namespace. Only entities with granted access to a namespace can request lifecycle management of MCIOs within the scope of this namespace.

5.2.4   Namespace quota

A namespace quota is an abstract NFV object managed and exposed by the CISM, representing an upper limit of infrastructure resources. Namespace quota are used to specify the overall amount of infrastructure resources which can be allocated within the scope of a namespace. Namespace quota are used to track the aggregate usage of infrastructure resources in the scope of a namespace and allow operators of clusters of CIS instances to specify resource usage limits that MCIOs created within the scope of a namespace may consume. Namespace quota can also be used to track and limit the number of MCIOs per type created within the scope of a namespace.

5.2.5   OS container Image

An OS container image is an abstract NFV object for OS container management and orchestration, representing a software image for an OS container. It is an object managed and exposed by the CIR, and contains all components required to deploy an OS container on a CIS instance.

OS container images are referenced in declarative descriptors of MCIOs. MCIOs which are built from OS container images, are created by deploying their OS containers from their respective images. The OS container images managed and exposed by a CIR are addressed and referenced by their names and the URLs of the respective CIR. OS container images may be included as software image artifacts in VNF Packages. As part of the VNF Package management, the NFVO distributes the OS container images to the CIR, as specified in clause 6.12 of ETSI GS NFV-IFA 010 [1].

NOTE: The NFVO role in distributing OS container images is the same behaviour as with done with VM software images.

5.3   Objects relationship

The relationships between the abstract NFV objects for OS container management and orchestration (in blue colour), as specified in the previous clauses, are illustrated in figure 5.3-1. Figure 5.3-1 also illustrates the relationships between the abstract NFV objects to existing objects of the NFV-MANO system (in yellow colour) where applicable.
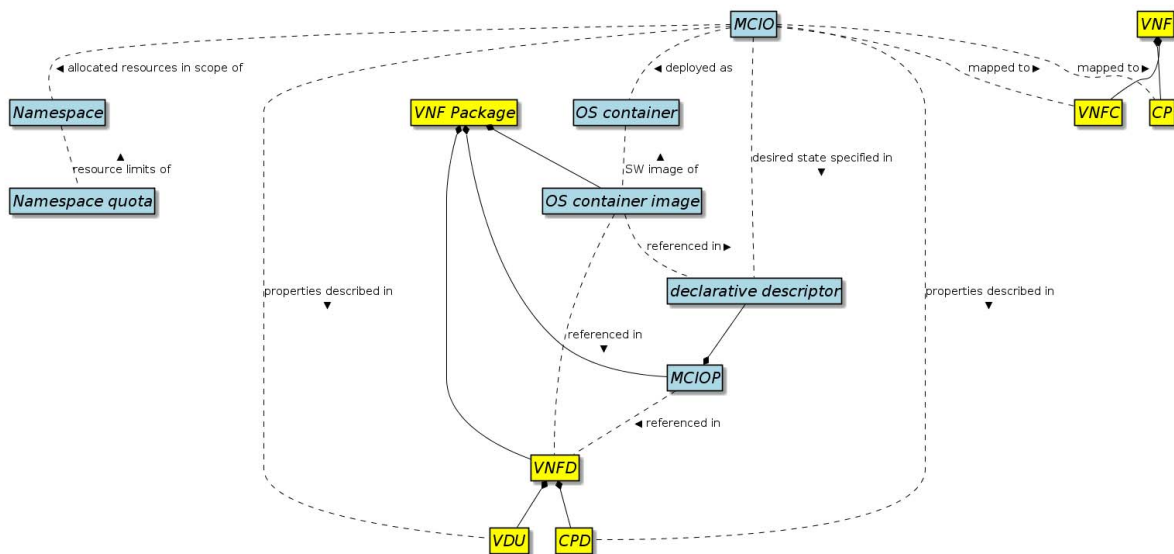
Figure 5.3-1: Abstract NFV objects relationship

NOTE 1: The explanation texts for the relationships in figure 5.3-1 all apply to corresponding dashed lines. The solid lines illustrate aggregations which do not have labels in the figure.

An MCIO is logically mapped to either a VNFC or a CP, depending on the MCIO's type. The properties of an MCIO relevant to being exposed to NFV-MANO are described in a VDU or applicable subclasses of a CPD respectively.

NOTE 2: The CPD in figure 5.3-1, although depicted as a distinct entity from the VDU, represents all classes of CPDs, including those embedded in a VDU.

The desired state of an MCIO, interpreted by the CISM, is specified in a declarative descriptor. Dependent on its type, an MCIO may be deployed as an OS container from its corresponding OS container image. The resources of an MCIO are allocated in the scope of a namespace under the limits of its namespace quota.

The OS container images are referenced in the declarative descriptors of an MCIO to be exposed to the CISM. The OS container images are referenced in the VNFD as software image artifacts, which may be included in the VNF Package.

The MCIO's declarative descriptors are aggregated as an MCIOP. MCIOPs are referenced in the VNFD as file artifacts included in the VNF Package.

6   CISM service requirements

6.1   Introduction

Clause 6 in the present document specifies the set of requirements applicable to interfaces exposing OS container management and orchestration services offered by the CISM function.

6.2   General CISM service requirements

Table 6.2-1 specifies requirements applicable to the services provided by the CISM.

Table 6.2-1: CISM service requirements

Identifier	Requirement
CismSvc.001	The CISM shall provide an OS container workload management service.
CismSvc.002	The CISM shall provide an OS container compute management service.
CismSvc.003	The CISM shall provide an OS container storage management service.
CismSvc.004	The CISM shall provide an OS container network management service.
CismSvc.005	The CISM shall provide an OS container configuration management service.
CismSvc.006	The CISM shall provide an OS container workload performance management service.

6.3 OS container workload management service interface requirements

Table 6.3-1 specifies the requirements applicable to the interface of the OS container workload management service produced by the CISM.

Table 6.3-1: OS container workload management service interface requirements

Identifier	Requirement
CismWkldMgt.001	The OS container workload management service interface produced by the CISM shall support instantiating containerized workloads based on a MCIOP.
CismWkldMgt.002	The OS container workload management service interface produced by the CISM shall support querying information about containerized workloads based on a MCIOP.
CismWkldMgt.003	The OS container workload management service interface produced by the CISM shall support modifying containerized workloads based on a modified MCIOP.
CismWkldMgt.004	The OS container workload management service interface produced by the CISM shall support terminating containerized workloads based on a MCIOP. See note.
CismWkldMgt.005	The OS container workload management service interface produced by the CISM shall support sending notifications in the event of changes to containerized workloads based on a MCIOP.
CismWkldMgt.006	The OS container workload management service interface produced by the CISM shall support access control (e.g. RBAC).
CismWkldMgt.007	The OS container workload management service interface produced by the CISM shall support subscribing to notifications on changes to containerized workloads based on a MCIOP.
NOTE: The assumption is that all objects as specified in the MCIOP are terminated gracefully by invoking this interface.	

6.4 OS container compute management service interface requirements

Table 6.4-1 specifies the requirements applicable to the interface of the OS container compute management service produced by the CISM.

Table 6.4-1: OS container compute management service interface requirements

Identifier	Requirement
CismCompMgt.001	The OS container compute management service interface produced by the CISM shall support creating Compute MCIOs.
CismCompMgt.002	The OS container compute management service interface produced by the CISM shall support modifying the desired state of Compute MCIOs.
CismCompMgt.003	The OS container compute management service interface produced by the CISM shall support modifying the actual state of Compute MCIOs.
CismCompMgt.004	The OS container compute management service interface produced by the CISM shall support replacing Compute MCIOs.
CismCompMgt.005	The OS container compute management service interface produced by the CISM shall support deleting Compute MCIOs in a graceful as well as in a forceful manner.
CismCompMgt.006	The OS container compute management service interface produced by the CISM shall support querying information about the desired and actual state of Compute MCIOs.
CismCompMgt.007	The OS container compute management service interface produced by the CISM shall support listing Compute MCIOs.
CismCompMgt.008	The OS container compute management service interface produced by the CISM shall support sending notifications in the event of changes to the desired or actual state of Compute MCIOs.
CismCompMgt.009	The OS container compute management service interface produced by the CISM shall support access control (e.g. RBAC).
CismCompMgt.010	The OS container compute management service interface produced by the CISM shall support subscribing to notifications on changes to the desired or actual state of Compute MCIOs.

6.5 OS container storage management service interface requirements

Table 6.5-1 specifies the requirements applicable to the interface of the OS container storage management service produced by the CISM.

Table 6.5-1: OS container storage management service interface requirements

Identifier	Requirement
CismStrgMgt.001	The OS container storage management service interface produced by the CISM shall support creating Storage MCIOs.
CismStrgMgt.002	The OS container storage management service interface produced by the CISM shall support modifying the desired state of Storage MCIOs.
CismStrgMgt.003	The OS container storage management service interface produced by the CISM shall support modifying the actual state of Storage MCIOs.
CismStrgMgt.004	The OS container storage management service interface produced by the CISM shall support replacing Storage MCIOs.
CismStrgMgt.005	The OS container storage management service interface produced by the CISM shall support deleting Storage MCIOs.
CismStrgMgt.006	The OS container storage management service interface produced by the CISM shall support querying information about the desired and actual state of Storage MCIOs.
CismStrgMgt.007	The OS container storage management service interface produced by the CISM shall support listing Storage MCIOs.
CismStrgMgt.008	The OS container storage management service interface produced by the CISM shall support sending notifications in the event of changes to the desired or actual state of Storage MCIOs.
CismStrgMgt.009	The OS container storage management service interface produced by the CISM shall support access control (e.g. RBAC).
CismStrgMgt.010	The OS container storage management service interface produced by the CISM shall support subscribing to notifications on changes to the desired or actual state of Storage MCIOs.

6.6   OS container network management service interface requirements

Table 6.6-1 specifies the requirements related to Network MCIOs and the requirements related to secondary container cluster internal/external networks identified in ETSI GR NFV-IFA 038 [i.5] applicable to the interface of the OS container network management service produced by the CISM.

Table 6.6-1: OS container network management service interface requirements

Identifier	Requirement
CismNetwMgt.001	The OS container network management service interface produced by the CISM shall support creating Network MCIOs.
CismNetwMgt.002	The OS container network management service interface produced by the CISM shall support modifying the desired state of Network MCIOs.
CismNetwMgt.003	The OS container network management service interface produced by the CISM shall support modifying the actual state of Network MCIOs.
CismNetwMgt.004	The OS container network management service interface produced by the CISM shall support replacing Network MCIOs.
CismNetwMgt.005	The OS container network management service interface produced by the CISM shall support deleting Network MCIOs.
CismNetwMgt.006	The OS container network management service interface produced by the CISM shall support querying information about the desired and actual state of Network MCIOs.
CismNetwMgt.007	The OS container network management service interface produced by the CISM shall support listing Network MCIOs.
CismNetwMgt.008	The OS container network management service interface produced by the CISM shall support sending notifications in the event of changes to the desired or actual state of Network MCIOs.
CismNetwMgt.009	The OS container network management service interface produced by the CISM shall support access control (e.g. RBAC).
CismNetwMgt.010	The OS container network management service interface produced by the CISM shall support creating a secondary container cluster internal/external network attachment.
CismNetwMgt.011	The OS container network management service interface produced by the CISM shall support modifying a secondary container cluster internal/external network attachment.
CismNetwMgt.012	The OS container network management service interface produced by the CISM shall support deleting a secondary container cluster internal/external network attachment.
CismNetwMgt.013	The OS container network management service interface produced by the CISM shall support querying the information about the current status of a secondary container cluster internal/external network attachment.
CismNetwMgt.014	The OS container network management service interface produced by the CISM shall support sending notifications in the event of changes for a secondary container cluster internal/external network attachment.
CismNetwMgt.015	The OS container network management service interface produced by the CISM shall support subscribing to notifications on changes to the desired or actual state of Network MCIOs.
CismNetwMgt.016	The OS container network management service interface produced by the CISM shall support subscribing to notifications on changes to a secondary container cluster internal/external network attachment.

6.7   OS container configuration management service interface requirements

Table 6.7-1 specifies the requirements applicable to the interface of the OS container configuration management service produced by the CISM.

Table 6.7-1: OS container configuration management service interface requirements

Identifier	Requirement
CismCfgMgt.001	The OS container configuration management service interface produced by the CISM shall support the creation of a namespace.
CismCfgMgt.002	The OS container configuration management service interface produced by the CISM shall support querying information about namespaces.
CismCfgMgt.003	The OS container configuration management service interface produced by the CISM shall support deleting namespaces.
CismCfgMgt.004	The OS container configuration management service interface produced by the CISM shall support the creation of a namespace quota.
CismCfgMgt.005	The OS container configuration management service interface produced by the CISM shall support querying information about namespace quota.
CismCfgMgt.006	The OS container configuration management service interface produced by the CISM shall support modifying namespace quota.
CismCfgMgt.007	The OS container configuration management service interface produced by the CISM shall support deleting namespace quota.
CismCfgMgt.008	The OS container configuration management service interface produced by the CISM shall support creating MCIO configurations. See note.
CismCfgMgt.009	The OS container configuration management service interface produced by the CISM shall support modifying MCIO configurations. See note.
CismCfgMgt.010	The OS container configuration management service interface produced by the CISM shall support replacing MCIO configurations. See note.
CismCfgMgt.011	The OS container configuration management service interface produced by the CISM shall support deleting MCIO configurations. See note.
CismCfgMgt.012	The OS container configuration management service interface produced by the CISM shall support querying information about MCIO configurations. See note.
CismCfgMgt.013	The OS container configuration management service interface produced by the CISM shall support listing MCIO configurations. See note.
CismCfgMgt.014	The OS container configuration management service interface produced by the CISM shall support sending notifications on events of MCIO configuration changes.
CismCfgMgt.015	The OS container configuration management service interface produced by the CISM shall support creating policies for MCIOs.
CismCfgMgt.016	The OS container configuration management service interface produced by the CISM shall support modifying policies for MCIOs.
CismCfgMgt.017	The OS container configuration management service interface produced by the CISM shall support replacing policies for MCIOs.
CismCfgMgt.018	The OS container configuration management service interface produced by the CISM shall support deleting policies for MCIOs.
CismCfgMgt.019	The OS container configuration management service interface produced by the CISM shall support querying information about policies for MCIOs.
CismCfgMgt.020	The OS container configuration management service interface produced by the CISM shall support listing policies for MCIOs.
CismCfgMgt.021	The OS container configuration management service interface produced by the CISM shall support sending notifications on events of MCIO policy changes.
CismCfgMgt.022	The OS container configuration management service interface produced by the CISM shall support sending notifications in the event of namespace quota changes.
CismCfgMgt.023	The OS container configuration management service interface produced by the CISM shall support access control (e.g. RBAC).
CismCfgMgt.024	The OS container configuration management service interface produced by the CISM shall support subscribing to notifications on changes to MCIO configurations.
CismCfgMgt.025	The OS container configuration management service interface produced by the CISM shall support subscribing to notifications on changes to MCIO policies.
CismCfgMgt.026	The OS container configuration management service interface produced by the CISM shall support subscribing to notifications on changes to namespace quotas.
NOTE:	An MCIO configuration can include certificate data for a containerized workload that is provisioned by means of MCIO configurations.

6.8   OS container workload performance management service interface requirements

Table 6.8-1 specifies the requirements applicable to the interface of the OS container workload performance management service produced by the CISM.

Table 6.8-1: OS container workload performance management service interface requirements

Identifier	Requirement
CismWkldPmMgt.001	The OS container workload performance management service interface produced by the CISM shall support querying performance information related to OS container workload (see note 1).
CismWkldPmMgt.002	The OS container workload performance management service interface produced by the CISM shall support sending notifications regarding events about performance information on OS container workload (see note 1).
CismWkldPmMgt.003	The OS container workload performance management service interface produced by the CISM shall support the capability of OS container workload performance management for controlling the collection and reporting of performance information in response to the request (see note 2).
CismWkldPmMgt.004	The OS container workload performance management service interface produced by the CISM shall support managing subscriptions to the notifications related to performance management of OS container workload.
NOTE 1:	OS container workload performance information can include the MCIO consumption level, such as OS container CPU utilization, OS container memory usage and OS container network bandwidth consumption.
NOTE 2:	The performance management includes creation, update, query and deletion of PM jobs and thresholds.

7　　OS container Image Registry service requirements

7.1　　Introduction

Clause 7 in the present document specifies the set of requirements applicable to interfaces exposing OS container image management services offered by the CIR function.

7.2　　General OS container image registry service requirements

Table 7.2-1 specifies requirements applicable to the services provided by the CIR.

Table 7.2-1: CIR service requirements

Identifier	Requirement
CirSvc.001	The CIR shall provide an OS container image management service.

7.3　　OS container image management service interface requirements

Table 7.3-1 specifies the requirements applicable to the interface of the OS container image management service produced by the CIR.

Table 7.3-1: OS container image management service interface requirements

Identifier	Requirement
CirImgMgt.001	The OS container image management service interface produced by the CIR shall support adding OS container images to the CIR.
CirImgMgt.002	The OS container image management service interface produced by the CIR shall support deleting OS container images from the CIR.
CirImgMgt.003	The OS container image management service interface produced by the CIR shall support querying information about OS container images in the CIR.
CirImgMgt.004	The OS container image management service interface produced by the CIR shall support sending notifications in the event of changes of OS container images in the CIR.
CirImgMgt.005	The OS container image management service interface produced by the CIR shall support access control (e.g. RBAC).

Annex A (informative):
Change history

Date	Version	Information about changes
October 2019	0.0.1	First draft, introducing the document skeleton
October 2019	0.1.0	Implementing contributions: NFVIFA(19)000804r1 - IFA040-Scope NFVIFA(19)000844r2 - IFA040-Clause 3.1-OS Container term definition NFVIFA(19)000847r2 - IFA040-Clause 4.1-Introduction NFVIFA(19)000849r2 - IFA040-Clause 4.2-Framework NFVIFA(19)000870 - IFA040-Clause 5.1-Introduction NFVIFA(19)000880 - IFA040-Remove Annex B-Authors and contributors Table of content updated to reflect new content
November 2019	0.2.0	Implementing contributions: NFVIFA(19)000873r5 - IFA040 5.2 Add MCIOP NFV object for OS container management NFVIFA(19)000909 - IFA040-Clause 5.2.1-Managed Container Infrastructure Object NFVIFA(19)000910r1 - IFA040-Clause 3.1-containerized workload term definition NFVIFA(19)000913r1 - IFA040-Clause 5.2.3-Namespace NFVIFA(19)000914r2 - IFA040-Clause 5.2.4-Namespace quota NFVIFA(19)000920r1 - IFA040-Clause 5.2.5-OS Container Image NFVIFA(19)000924r1 - IFA040-Clause 5.3-Objects relationship
February 2020	0.3.0	Implementing contributions: NFVIFA(19)000974 - IFA040-Clause 6.2-General CISM service requirements NFVIFA(19)0001015r1 - IFA040 6.3, 6.5 Adding CISM service interface requirements NFVIFA(19)0001016r2 - IFA040 7 Adding CIR service interface requirements NFVIFA(20)000003r3 - IFA040-Clause 6.4-Compute management service interface requirements NFVIFA(20)000005r3 - IFA040-Clause 6.5-Storage management service interface requirements NFVIFA(20)000006r3 - IFA040-Clause 6.7-Configuration management service interface requirements NFVIFA(20)000015 - IFA040-Clause 6-Additional CISM service requirements NFVIFA(20)000016 - IFA040-Clause 6.6-Network management service interface requirements NFVIFA(20)000019 - IFA040-Correct references to NFV 003
February 2020	0.4.0	Implementing contributions: NFVIFA(20)000062 - IFA040 Adding missing notification related requirements NFVIFA(20)000075 - IFA040 5.2.2.2 Editor's note resolution NFVIFA(20)000076r1 - IFA040 4.1 Editor's note resolution NFVIFA(20)000087 - IFA040-Editorial clean-up NFVIFA(20)000094r1 - IFA040 Adding tenant related requirements of CIR
March 2020	0.5.0	Implementing contributions: NFVIFA(20)000149 - IFA040 Editorial clean-up part 1 NFVIFA(20)000150 - IFA040 3.2 Void symbols clause NFVIFA(20)000151r2 - IFA040 Section 6 proposed changes NFVIFA(20)000175r2 - IFA040 - Review - Editorial improvements NFVIFA(20)000176 - IFA040 - Review - Minor Technical improvements NFVIFA(20)000178r2 - IFA040-Add requirements on access control for CISM service interfaces NFVIFA(20)000182r2 - IFA040 Editorial clean-up part 2 NFVIFA(20)000190r1 - IFA040 - Review - Clarifications on the model mapping
December 2020	4.1.2	First early draft for new edition IFA040ed421, based on published version 4.1.1
March 2021	4.1.3	Implementing contributions: NFVIFA(21)000074r1 - IFA040ed421 FEAT17 Adding MCIO definitions NFVIFA(21)000075 - IFA040ed421 FEAT17 Clarifications about MCIO and container granularity NFVIFA(21)000160r1 - IFA040ed421 FEAT17 MCIO configurable parameters Replaced all occurrences of "MCIO whose declarative descriptors [...] " with new terms "Compute MCIO" or "Storage MCIO" or "Network MCIO" Table of content updated
March 2021	4.1.4	Implementing contributions: NFVIFA(21)000236r1 - IFA040ed421 Mirror of 218 Avoid Reference to MAN001
July 2021	4.2.2	First early draft for new edition IFA040ed431, based on published version 4.2.1

Date	Version	Information about changes
March 2022	4.2.3	Implementing contributions: NFVIFA(22)000180 - IFA040ed431 MegaCR FEAT19a container networking Added reference to the ETSI Coordinated Vulnerability Disclosure (CVD) scheme according to the new GS skeleton Updated table of contents
June 2022	4.3.2	First early draft for new edition IFA040ed441, based on published version 4.3.1
October 2022	4.3.3	Implementing contributions: NFVIFA(22)000748- IFA040ed441-Clause 6 Add notification subscription requirements Table of content updated to reflect new content
November 2022	4.3.4	Implementing contributions: NFVIFA(22)000821 - IFA040ed441-Clause 3 Align with NFV003ed171
March 2023	V4.4.1	Version update for publication
April 2023	V4.4.2	First draft for ed451 created from published version v4.4.1
July 2023	V4.4.3	Updated with CRs: NFVIFA(23)000338r2 Adding requirement on OS container workload performance management NFVIFA(23)000457r1 Enh01.01 IFA040ed451 Mega CR

History

Document history		
V4.1.1	November 2020	Publication
V4.2.1	May 2021	Publication
V4.3.1	May 2022	Publication
V4.4.1	March 2023	Publication
V4.5.1	September 2023	Publication