International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3523

(08/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

Metadata framework for NaaS service lifecycle management

Recommendation ITU-T Y.3523

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3523

Metadata framework for NaaS service lifecycle management

Summary

Recommendation ITU-T Y.3523 specifies the metadata framework for Network as a Service (NaaS) service lifecycle management in a closed-loop automation environment. This Recommendation is an extension to Recommendations ITU-T Y.3512 and ITU-T Y.3515 as the NaaS series Recommendations. It provides the metadata framework for NaaS service lifecycle management with a highlight on a NaaS operational policy framework.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3523	2019-08-13	13	11.1002/1000/13989

Keywords

Closed-loop automation, lifecycle management, metadata framework, NaaS service, NaaS service operational policy framework.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3523

Metadata framework for NaaS service lifecycle management

1 Scope

This Recommendation provides the metadata framework for the closed-loop automation lifecycle management of Network as a Service (NaaS) service, specifically in the environments of development and operations (DevOps) and continuous integration/continuous delivery (CI/CD). This Recommendation covers the following aspects:

– general description of metadata for NaaS service lifecycle management;

– metadata in NaaS service;

– metadata framework for NaaS service lifecycle management;

– NaaS service operational policy framework.

This Recommendation also provides Appendix I describing:

– metadata applicability in NaaS service lifecycle management.

NOTE 1 – The objective in defining a metadata framework of NaaS service lifecycle management is not to invent new metadata, but rather to make the existing metadata interoperable and integrated in the closed-loop automation management of NaaS service, especially in the environments of DevOps and CI/CD.

NOTE 2 – "Metadata" in this Recommendation refers to NaaS service data model, NaaS service operational policy data model and NaaS resource data model.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

[ITU-T Y.3515] Recommendation ITU-T Y.3515 (2017), *Cloud computing – Functional architecture of Network as a Service*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.6 network function [ITU-T Y.3515]: A function of a network infrastructure whose external interfaces and functional behaviour are well specified.

NOTE – Examples of network functions include network switches and network routers.

3.1.7 network service [ITU-T Y.3515]: A collection of network functions with a well specified behaviour.

NOTE – Examples of network services include content delivery networks (CDNs) and IP multimedia subsystem (IMS).

3.1.8 software-defined networking [b-ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 NaaS service operational policy administration point (NPAP): An entity in the Network as a Service (NaaS) service operational policy framework that administrates the policies.

3.2.2 NaaS service operational policy decision point (NPDP): An entity in the Network as a Service (NaaS) service operational policy framework that makes authorization decisions and distributions of the policies.

3.2.3 NaaS service operational policy enforcement point (NPEP): An entity in the Network as a Service (NaaS) service operational policy framework that implements the decisions of NPDP (3.2.2).

3.2.4 NaaS service operational policy information point (NPIP): An entity in the Network as a Service (NaaS) service operational policy framework that stores the policies.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CI	Continuous Integration
CD	Continuous Delivery
CDN	Content Delivery Network
CE	Customer Edge
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DevOps	Development and Operations

ECA	Event, Condition and Action
IMS	IP Multimedia Subsystem
NaaS	Network as a Service
NF	Network Function
NPAP	NaaS Service Operational Policy Administration Point
NPDP	NaaS Service Operational Policy Decision Point
NPEP	NaaS Service Operational Policy Enforcement Point
NPIP	NaaS Service Operational Policy Information Point
NS	Network Service
OSS	Operation Support System
PE	Provider Edge
SDN	Software-Defined Networking
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 General description

The increasing demands on the closed-loop automation management of cloud service causes methods and technology widely used in information technology (IT) like DevOps and CI/CD to be considered and adopted by the telecommunications industry.

The existing initiative aims to enable operational processes and tasks (e.g., delivery, deployment, configuration, assurance and optimization) to be executed automatically, such as ETSI ZSM ISG [b-ZSM], or to provide a comprehensive platform for real-time, policy-driven orchestration and automation of physical and virtual network functions (NFs), like open source open network automation platform (ONAP) [b-ONAP].

According to [ITU-T Y.3522], the complexity of re-design, re-configuration and re-deployment problems can be addressed through cloud service lifecycle management metadata. A new service can be created with changes only in metadata, which can be regarded as the linkage between design time and execution time. Taking NaaS service as an example, whose functional requirements and architecture are well defined in [ITU-T Y.3512] and [ITU-T Y.3515], the related metadata has been defined in several different standards developing organizations (SDOs) and used in many network areas.

However, there is no specification to address the detailed position and function of metadata in the context of the entire closed-loop automation lifecycle management of the NaaS service, whose dependencies and constraints vary unavoidably.

This Recommendation specifies the interoperability and integration of the existing NaaS-related data models as a typical kind of Anything as a Service (XaaS). Although, there are other activities on data models' development on NaaS service aspect (e.g., OASIS TOSCA [b-TOCSA], IETF YANG [b-YANG], OASIS BPEL [b-BPEL]), this Recommendation is focused on specifying the framework with attention on policy aspects, and applicability of data models in closed-loop automation management of NaaS service.

7 Metadata in NaaS service

This clause aims to specify the positions and functions of NaaS service metadata for the entire lifecycle management. The positions of NaaS-related data models are illustrated as shown in Figure 7-1.

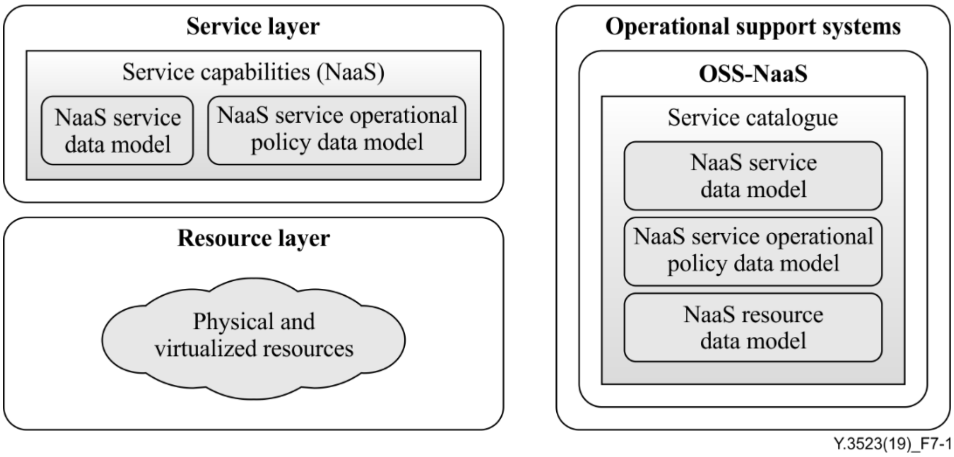
Service layer
Service capabilities (NaaS)
NaaS service data model
NaaS service operational policy data model
Resource layer
Physical and virtualized resources
Operational support systems
OSS-NaaS
Service catalogue
NaaS service data model
NaaS service operational policy data model
NaaS resource data model
Y.3523(19)_F7-1

Figure 7-1 – Illustration of NaaS-related metadata positions

Operation support system (OSS)-NaaS service catalogue functional components (see clause 8.3.1 of [ITU-T Y.3515]) includes a listing of all cloud services of NaaS cloud service providers (CSPs) including the relevant NaaS services. NaaS service data model, NaaS service operational policy data model and NaaS resource data model are needed in this functional component for NaaS service instantiation.

The service capabilities (NaaS) functional component (see clause 8.2.3 of [ITU-T Y.3515]) in the service layer provides capabilities exposed to the NaaS cloud service customer (CSC) according to the NaaS service data model and NaaS service operational policy data model selected by the NaaS CSC through business level interactions with the NaaS CSP.

7.1 NaaS service data model

The NaaS service data model (see clause 8.3.1 of [ITU-T Y.3515]) describes the specific network service based on the characteristic of the service that can be used for service delivery, e.g., L3VPN and L2VPN data models under development of the working groups L3SM [b-L3SM] and L2SM [b-L2SM] of IETF.

7.2 NaaS service operational policy data model

The NaaS service operational policy data model (see clause 8.3.1 of [ITU-T Y.3515]) describe high-level network-wide polices for a given NaaS service, which can be input into the network management function (within a software-defined networking (SDN) controller, an orchestrator, or a network element), and combined with the NaaS service data model and mapped into a target configuration of network elements, e.g., generic policy data model described in [b-SUPA] of IETF. The network management function can control the configuration and monitor the network elements and services according to such policies.

7.3 NaaS resource data model

The NaaS resource data model (see clause 8.3.1 of [ITU-T Y.3515]) describes topology of NaaS CSP's resources across different layers and reflects the attributes and operational parameters of given NaaS resources (e.g., network services (NSs), NFs, virtualised resources, physical resources).

7.4 Relationship among metadata in NaaS service

The NaaS service operational policy data model can manage and adjust service behaviours as necessary. The NaaS service operational policy data model and the NaaS service data model have a one-to-many relationship.

The NaaS service operational policy data model can manage and adjust resources behaviour as necessary. The NaaS service operational policy data model and the NaaS resource data model have a one-to-many relationship.

8 Metadata framework for NaaS service lifecycle management

This clause aims to specify the metadata framework in NaaS service lifecycle management by reflecting the interoperability and integration of the NaaS service metadata, especially in the environments of DevOps and CI/CD.

As described in [ITU-T Y.3522], metadata is used in the entire cloud service lifecycle management, from design, deployment, operation, to retirement stages. For NaaS service, closed-loop automation management is achieved by using data models of NaaS service, NaaS service operational policy, and NaaS resource, as a linkage, in the four iterative stages of NaaS service lifecycle management. These four iterative stages can be categorized into design time, including design stage, and runtime execution time, including deployment stage, operation stage and retirement stage.

Figure 8-1 depicts the metadata framework for NaaS service lifecycle management. The metadata of NaaS service is created in design time, and then distributed to runtime execution time to be used in implementing a metadata-driven service deployment, operation and retirement. The feedback from runtime execution time to design time is to help identify the changes needed for the metadata.

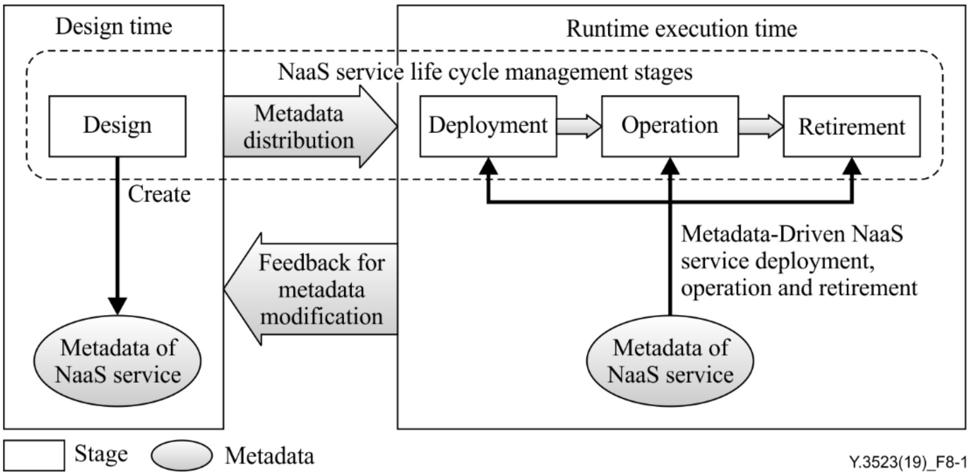

Figure 8-1 – Metadata framework for NaaS service lifecycle management

8.1 Metadata of NaaS service in design time

Models of NaaS service, NaaS service operational policy, and NaaS resource are created and developed in design time for making services and resources available, using modelling tools provided by NaaS CSP. The modelling process will not trigger any NaaS service instantiation in the runtime execution environment until the OSS-NaaS receives a request to do so.

The basic extendable model templates are defined and stored in service catalogue of OSS-NaaS (NaaS service data model and NaaS service operational policy data model) and network controller (NaaS resource data model) during design time and can be configured and extended with additional parameters, parameter value ranges and validation rules according to NaaS CSC's request.

8.2 Metadata of NaaS service in runtime execution time

The modelled NaaS service is instantiated in runtime execution time and the specific NaaS service model and its NaaS service operational policy data model drive the corresponding codes. The active NaaS service is continuously monitored by event listening. The event, requiring healing and/or scaling based on real-time NaaS CSC requests, is responded to based on the associated condition pre-defined in NaaS service operational policy data model.

Based on the monitoring data collected during runtime execution time, the patterns governing usage, thresholds, events, policy effectiveness, etc., are discerned and the necessary feedback to effect modelling changes in design time is enabled.

9 NaaS service operational policy framework

This clause aims to present the NaaS service operational policy framework which consists of elements and functions provided by the CSP and the corresponding procedure.

9.1 Elements of NaaS service operational policy

NaaS service operational policy data models are operated from creation to execution in the NaaS service operational policy framework. The main elements of the NaaS service operational policy framework are described as follows.

9.1.1 NaaS service operational policy administration point

The NaaS service operational policy administration point (NPAP) is responsible for the creation, translation, and validation of new NaaS service operational policy data models, and the modification of existing ones, both during design time and runtime execution time. NaaS service operational policy data models are created with the integration of NaaS service data models.

9.1.2 NaaS service operational policy decision point

The NaaS service operational policy decision point (NPDP) is responsible for the distribution and decisions of NaaS service operational policy data models. Once the NaaS service operational policy data model is initially created or an existing one is modified, the NPDP sends it from the repository to the NaaS service operational policy enforcement point (NPEP) before it is actually needed. In this distributed manner, NaaS service operational policy data models will be available when needed in order to minimize the latency for real-time requests or triggers to the NPDP. In some required cases, NaaS service operational policy data models can be subscribed and automatically updated on the NPEP.

9.1.3 NaaS service operational policy information point

The NaaS service operational policy information point (NPIP) is responsible for storing new NaaS service operational policy data models in the repository which are verified by the NPAP. The existing ones can be retrieved in the repository.

In the repository, NaaS service operational policy data models are grouped by different dimensions, which include, but are not limited to, the corresponding NaaS service data model, the type or category, the lifecycle, the ownership or administrative domain, the geographic area or location, the technology type, the describing language and version, and the security level.

9.1.4 NaaS service operational policy enforcement point

The NPEP is responsible for the enforcement of NaaS service operational policy data models during the runtime execution time.

9.2 Functions of NaaS service operational policy

Table 9-1 provides descriptions of the main functions related to the NaaS service operational policy data model.

Table 9-1 – Functions related with NaaS service operational policy data model

No.	Function	Description
1	Create policy	The CSP creates a NaaS service operational policy data model on the NPAP based on the required policy parameters and the NPIP stores it with the allocated labels which indicates its dimensions.
2	Delete policy	The CSP deletes the specified NaaS service operational policy data model on the NPAP and the NPIP removes it from the repository.
3	Update policy	The CSP updates a NaaS service operational policy data model on the NPAP based on the new policy parameters and the NPIP re-stores it and the original one is overwritten accordingly.
4	Get policy	The NPDP requests the specified NaaS service operational policy data model from the NPIP and gets it from the repository.
5	Distribute policy	The NPDP distributes the specified NaaS service operational policy data model to the NPEP and the NPEP makes the subscription on the NPDP for its update.
6	List policy	The NPIP lists all the NaaS service operational policy data models on demand.
7	Retrieve policy	The NPIP provides the retrieved NaaS service operational policy data models on demand based on the specified retrieval conditions.
8	Enforce policy	The NPEP enforces the NaaS service operational policy data models based on the trigger condition or request.

9.3 Procedure of NaaS service operational policy from creation to enforcement

The interactions among the main elements of NaaS service operational policy framework from creation to enforcement of the policy data model are described as follows in Figure 9-1.

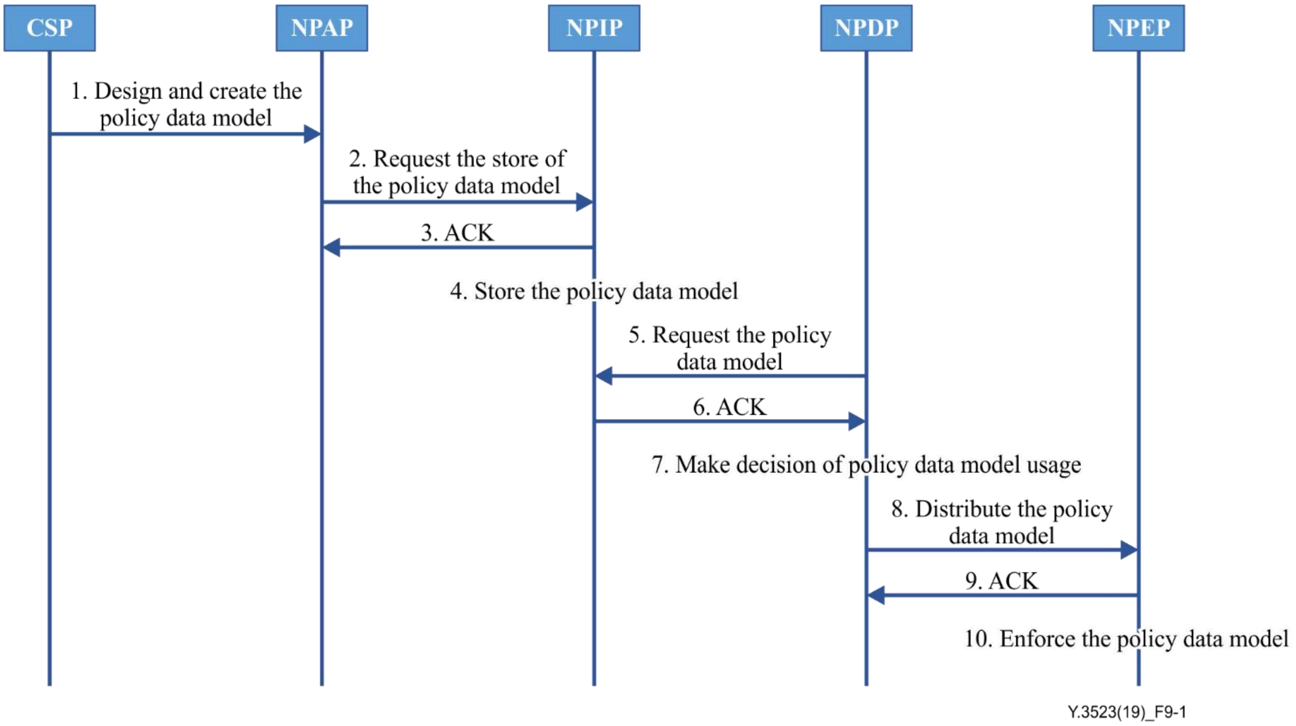
CSP
NPAP
NPIP
NPDP
NPEP
1. Design and create the policy data model
2. Request the store of the policy data model
3. ACK
4. Store the policy data model
5. Request the policy data model
6. ACK
7. Make decision of policy data model usage
8. Distribute the policy data model
9. ACK
10. Enforce the policy data model
Y.3523(19)_F9-1

Figure 9-1 – Procedure from creation to enforcement of the NaaS service operational policy data model

1) The CSP designs and creates the NaaS service operational policy data model on NPAP.

2) The NPAP requests the NPIP to store the newly created NaaS service operational policy data model.

3) The NPIP sends an acknowledgement to the NPAP.

4) The NPIP stores the newly created NaaS service operational policy data model in the repository.

5) The NPDP requests the NaaS service operational policy data model from the NPIP for decision.

6) The NPIP sends an acknowledgement to the NPDP.

7) The NPDP decides how to deal with the NaaS service operational policy data model.

8) The NPDP distributes the NaaS service operational policy data model to the NPEP which subscribed it.

9) The NPEP sends an acknowledgement to the NPDP.

10) The NPEP enforces the NaaS service operational policy data model once it is triggered.

10 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are addressed by security challenges for CSPs as described in [ITU-T X.1601]. [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges. This Recommendation does not introduce any new security issues.

Appendix I

Metadata applicability in NaaS service lifecycle management

(This appendix does not form an integral part of this Recommendation.)

This appendix aims to provide applicability examples of NaaS service lifecycle management metadata.

I.1 Virtual private cloud

The manipulation of the virtual private cloud (VPC) network may also affect the configuration of physical networks. For example, when two new virtual machines (VMs) associated to a given VPC are deployed in two different data centres (DCs), the VPC control mechanism needs to generate a virtual private network (VPN) between these two data centres for the internal VPC communications. Therefore, the control mechanism for a VPC should be able to adjust the underlying network at run time when a CSC requests changes to the VPC network or service deployment.

When a CSC moves from one location to another, which is near to another CSP's data centre, and in the case where the network load between these two data centres is low, the CSC's VM(s) should be migrated to the new data centre to allow for a better user experience.

As illustrated by Figure I.1, a VPC corresponds to a combination of cloud computing resources with a VPN infrastructure to give NaaS service CSCs the abstraction of a private set of cloud resources that are transparently and securely connected to their own infrastructure. VPCs are created by taking dynamically configurable pools of cloud resources and connecting them to enterprise sites with VPNs.

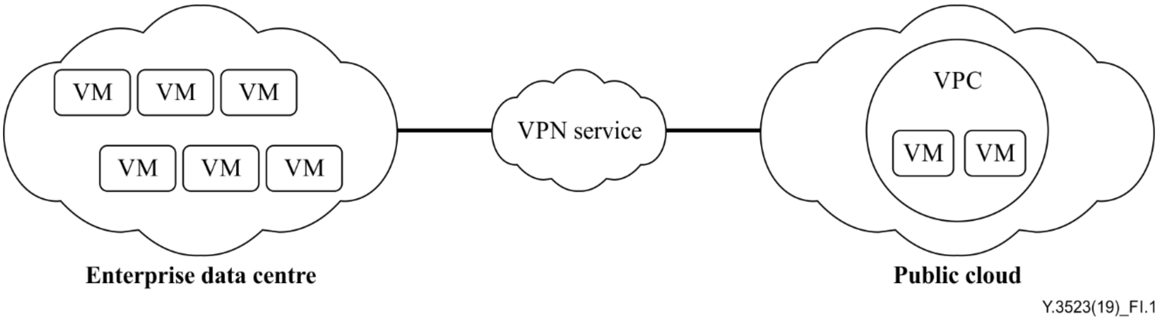

Figure I.1 – Illustration of virtual private cloud

The NaaS resource data model needs to be used in this scenario for modelling the physical nodes and links.

The NaaS service data model, specifically for L3VPN, is needed to model the L3VPN attributes, including, but not limited to: tenant ID, VPN site IDs, VPN type, access bandwidth.

Here, the NaaS policy data model can be described as follows, using event, condition and action (ECA) policy.

– Event: a VPC user's location is changed (near to another DC)

– Condition: network_load(DC_old, DC_new) < threshold

– Action:

  1) migrate the VM to the new data center (DC_new);

  2) update the VPNs connecting the CSC's services.

I.2 Instant VPN

Traditionally, when a NaaS CSP needs to deploy VPN services for an enterprise NaaS CSC, the NaaS CSP will send service staff to the NaaS CSC site to make the wired connection between the customer edge (CE) and provider edge (PE) devices. The service staff also collects configuration information such as port/frame/slot of PE and the PE ID, and then sends the collected information back to the management system. The management system then configures the network according to this information, as well as the NaaS CSC's information (e.g., bandwidth, SLA). The problem with this approach is that the service staff needs to collect the connection information and feed it back to the management system, and they must make sure that the collected information matches the actual connection. This process is error prone.

New approaches should not count on the physical/geographical information feedback by the service staff and should minimize the operational procedures. The CE should send an authentication request (with credentials) to the PE, and the PE should forward the request to the management system, together with the port/frame/slot on which the request is received, the PE ID, etc. The goal is that NaaS CSP configures a VPN for an enterprise NaaS CSC to connect its enterprise network. The NaaS resource data model needs to be used in this scenario for modelling the physical nodes and links.

The NaaS service data model, specifically for L3VPN, is needed to model the L3VPN attributes, including, but not limited to: tenant ID, VPN site IDs, VPN type and access bandwidth.

Here, the NaaS policy data model can be described as follows, using ECA policy.

– Event: service management system receives a CE request for VPN creation (forwarded by PE);
– Condition: authentication and authorization results are acknowledged;
– Action: configure a VPN based on received requests, including the NaaS CSC's grade and physical information (port/slot/frame/route id, etc.) from which the request is received.

Bibliography

[b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-BPEL] OASIS BPEL 2.0 (2007), *Web Services Business Process Execution Language Version 2.0.* <http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html> (last accessed 28 June 2019)

[b-L2SM] IETF RFC 8466 (2018), *A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery*.

[b-L3SM] IETF RFC 8299 (2018), *YANG Data Model for L3VPN Service Delivery*.

[b-ONAP] ONAP, *Open Network Automation Platform*. https://www.onap.org/ (Referenced 28 06 2019).

[b-SUPA] IETF RFC 8328 (2018), *Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA).*

[b-TOCSA] OASIS TOSCA 1.0 (2013), *Topology and Orchestration Specification for Cloud Applications Version 1.0.* <http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html> (last accessed 28 June 2019)

[b-YANG] IETF RFC 6020 (2010), *YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF).*

[b-ZSM] ETSI ISG ZSM, *Industry Specification Group Zero touch network and Service Management*. <https://portal.etsi.org/tb.aspx?tbid=862&SubTB=862,863> (last accessed 28 June 2019)

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019