International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3513

(08/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Cloud Computing

Cloud computing – Functional requirements of Infrastructure as a Service

Recommendation ITU-T Y.3513

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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**

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

Recommendation ITU-T Y.3513

Cloud computing – Functional requirements of Infrastructure as a Service

Summary

Recommendation ITU-T Y.3513 introduces the concept of Infrastructure as a Service (IaaS) and describes its functional requirements. As one of the cloud computing service categories, Infrastructure as a Service provides cloud service customers with computing, storage and network services by cloud service providers. To derive those requirements, relevant use cases are also presented.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3513	2014-08-29	13	11.1002/1000/12286

Keywords

Cloud computing, Infrastructure as a Service, IaaS, virtual machine.

---

* 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.3513

Cloud computing – Functional requirements of Infrastructure as a Service

1 Scope

This Recommendation provides functional requirements and use cases of Infrastructure as a Service (IaaS), one of the representative cloud service categories. This Recommendation covers the following:

– General description of IaaS;

– Functional requirements of IaaS;

– Typical IaaS use cases.

NOTE – The general requirements of IaaS can be found in [ITU-T Y.3501].

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 (2014), *Security framework for cloud computing*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), Information technology – *Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), Information technology – *Cloud computing – Reference architecture*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud capabilities type [ITU-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resource used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.2 cloud computing [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.

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

3.1.4 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

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

3.1.6 cloud service customer data [ITU-T Y.3500]: Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service.

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.

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

3.1.8 cloud service provider data [ITU-T Y.3500]: Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider.

NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.1.9 Infrastructure as a Service [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.10 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.

3.1.11 open virtualization format [b-ISO/IEC OVF]: An open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

3.1.12 party [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.13 tenant [ITU-T Y.3500]: Group of cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU Central Processing Unit

CSC Cloud Service Customer

CSP	Cloud Service Provider
LUN	Logical Unit Number
IaaS	Infrastructure as a Service
IP	Internet Protocol
I/O	Input/Output
NaaS	Network as a Service
NAT	Network Address Translation
NIC	Network Interface Card
OVF	Open Virtualization Format
QoS	Quality of Service
SLA	Service Level Agreement
UML	Unified Modelling Language
VLAN	Virtual Local Area Network
VM	Virtual Machine

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.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

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 are to be interpreted as having no normative intent.

6 General description

Infrastructure as a Service (IaaS) is one of the representative categories of cloud services, in which the cloud capabilities type provided to the cloud service customer (CSC) is an infrastructure capabilities type. IaaS allows the CSC to use cloud infrastructure resources (processing, storage or networking). Use of cloud infrastructure resources is supported by service functions, which can include the relevant operations.

IaaS provides to the CSC the following service functions:

– **computing service functions** allow the CSC to provision and use processing resources. CSC can perform operations relevant to processing resources including machine (physical or virtual machine) lifecycle operations and functions such as virtual machine (VM) migration, backup, snapshot, clone and reservation;

– **storage service functions** allow the CSC to use storage resources. The CSC can perform operations relevant to storage resources including lifecycle operations and functions such as snapshot, backup, input/output (I/O) performance, load balance and reservation;

– **network service functions** allow the CSC to use networking resources. The CSC can integrate infrastructure resources using network relevant functions such as IP address, network isolation (e.g., virtual local area network (VLAN)), virtual networking (e.g., virtual switch), load balance and firewall.

The high level concept of IaaS using the layering framework defined in [ITU-T Y.3502] is illustrated in Figure 6-1.

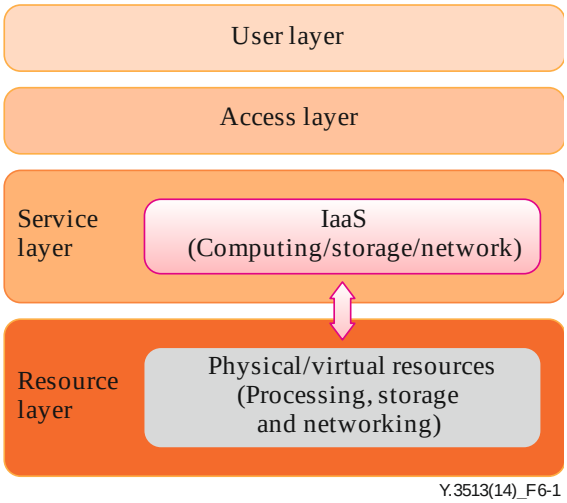


Figure 6-1 – High level concept of IaaS

An IaaS instance can be configured by the CSC using a template to define the set of parameters stating, how infrastructure resources are organized. Such IaaS instance consists of configured processing, storage or networking resources, as well as information located in the resources, which may include cloud service provider data, cloud service customer data or both.

IaaS cloud service provider (CSP) also provides business and administration capabilities to CSC, which are common capabilities for cloud services. The functional requirements of business and administration capabilities are for further study.

NOTE – Regarding the network connectivity, one important difference between IaaS and Network as a Service (NaaS) is that IaaS is a cloud service category that is offered in only one flavour of cloud capability type, and that is infrastructure capabilities type [ITU-T Y.3500]. However, NaaS is a cloud service category that can be offered in all three cloud capabilities types.

7 Functional requirements

– It is recommended that IaaS CSP provides to the CSC IaaS functions, such as a composition of processing, storage, and networking resources with service logic, specific service level agreements (SLAs) and charging model.

– It is required that IaaS CSP provides the CSC with operations handling mechanisms related to provisioned infrastructure resources, such as assign, modify, query and release.

– It is recommended that IaaS CSP provides status information about the infrastructure in response to queries from the CSC.

NOTE – The status information includes, but not limited to, available, reserved and in-use.

– It is recommended that IaaS CSP provides template to the CSC, related to instantiation of infrastructure, which allows to provision processing, storage and networking resources that could be implemented based on the configuration.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to infrastructure templates to allow modification of infrastructure, such as upload, update, disable, enable, query or release.

7.1 Computing service functional requirements

– It is required that IaaS CSP provides computing functions with specific SLAs and charging model to the CSC.

7.1.1 Physical machine

– It is recommended that IaaS CSP provides specific hardware specifications of physical machine to the CSC according to SLA.

NOTE – SLA includes, but not limited to, central processing unit (CPU) type, CPU speed, number of CPU cores, memory size, disk size and network interface card (NIC) number.

– It is recommended that IaaS CSP provides the CSC with operation handling mechanisms related to physical machine such as start, shutdown, hibernate and wakeup.

– It is recommended that IaaS CSP provides physical machine related information in response to queries from the CSC.

NOTE – The information includes, but not limited to, physical machine specifications, status and network interfaces.

7.1.2 Virtual machine

– It is recommended that IaaS CSP provides virtual machine based on the VM template.

NOTE – By using the VM template, CSC can select the required number of CPU cores, memory size, disk size, NIC within the resources available according to SLA.

– IaaS CSP can optionally provide virtual machine based on the configurations specified by the CSC.

– It is required that IaaS CSP provides the CSC with operations handling mechanisms related to VM, including, but not limited to, create, delete, start, shutdown, suspend, restore, hibernate and wakeup.

– It is recommended that IaaS CSP provides VM related information in response to queries from the CSC.

NOTE – The VM related information includes, but not limited to, VM specifications, volume information, VM status, IP address and network interfaces.

7.1.3 VM migration

– It is recommended that IaaS CSP provides virtual machine with migration functions. Based on migration policies, the virtual machine can be migrated from one host to another.

7.1.4 VM scaling

– It is recommended that IaaS CSP provides virtual machine with scaling functions based on the scaling policies and monitored events of the virtual machine.

NOTE – The types of VM scaling includes, but not limited to, configuration changes (e.g., CPU, memory, bandwidth increased or bandwidth decreased) or components changes (new virtual machine added or removed).

7.1.5 VM snapshot

– It is recommended that IaaS CSP provides virtual machine with snapshot functions. Schedule of snapshots taken from the virtual machine can be performed automatically or manually.

7.1.6 VM clone

– It is recommended that IaaS CSP provides virtual machine with clone functions. The cloned VM has identical configuration and CSP/CSC data as the original one.

7.1.7 VM backup

– It is recommended that IaaS CSP provides virtual machine with backup functions. When VM becomes faulty or its data is lost, the VM can be restored using its backup stored according to the CSC policy.

7.1.8 VM time synchronization

– It is recommended that IaaS CSP provides time synchronization functions, which allow the CSC to control the VM time.

7.1.9 VM reservation

– It is recommended that IaaS CSP provides processing resources reservation (such as CPU, memory) functions. Resources reservation is used to reserve available resources from IaaS infrastructure before VM is initiated.

7.1.10 VM image

– It is recommended that IaaS CSP offers the ability for the CSC to provide and use virtual machine images. VM image consists of infrastructure configuration and CSP data, CSC data or both.

NOTE – VM image allows to start a new instance of VM.

– It is recommended that IaaS CSP supports different machine image format.

– It is required that IaaS CSP provides operation handling mechanisms related to image，including, but not limited to, add, import, store, register, deregister, query, update, delete and export.

7.1.11 VM template

– It is recommended that IaaS CSP supports open virtualization format (OVF) template, which is a packaging standard designed to address the portability and deployment of virtual appliances.

– It is recommended that IaaS CSP provides operations handling mechanisms related to machine templates, such as upload, update, disable, enable, query and delete to the CSC.

7.2 Storage service functional requirements

– It is recommended that IaaS CSP provides storage functions, such as block level storage, file level storage and object-based storage, with specific SLAs and charging model to the CSC. The storage functions can be provided to the CSC directly or used by the virtual machine as attached storage.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to storage, such as create, attach, detach, query and delete a volume of storage at either block level or file-system level, write, read and delete data for a given storage.

– It is recommended that IaaS CSP provides storage utilisation information in response to queries from the CSC.

7.2.1 Storage migration

– It is recommended that IaaS CSP provides storage migration functions. Based on migration policies, data can be migrated between different logical unit numbers (LUNs), different storage devices, local storage to shared storage and vice versa.

7.2.2 Storage snapshot

– It is recommended that IaaS CSP provides storage with snapshot functions. Snapshot can be realized at either block or file-system levels. The data can be restored using the snapshot.

7.2.3 Storage backup

– It is recommended that IaaS CSP provides storage with backup functions. Backup can be realized at block level, file level or object-based storage.

7.2.4 I/O performance

– It is recommended that IaaS CSP provides input/output (I/O) limitation for each VM.

7.2.5 Storage resource reservation

– It is recommended that IaaS CSP provides storage resource (e.g., storage space and LUN) reservation functions.

7.3 Network service functional requirements

– It is recommended that IaaS CSP provides network functions, such as IP address, VLAN, virtual switch, load balance, firewall, with specific SLAs or charging model. Network functions are applied to access and interconnect of processing and storage resources.

– It is recommended that IaaS CSP provides network information in response to queries from the CSC.

NOTE – The information includes, but not limited to, network device(s) specification, network traffic performance (in terms of throughput, jitter, loss, delay) and network topology.

7.3.1 Network policy migration

– It is recommended that IaaS CSP provides network policy migration along with virtual machine migration. In that case, the network policy of the migrated virtual machine is the same as before the migration.

7.3.2 Network QoS

– It is recommended that IaaS CSP provides operation handling mechanisms related to the network quality of service (QoS), such as bandwidth limit, bandwidth reservation, traffic shaping, traffic classification, congestion avoidance, at port level, device level and network level.

7.3.3 IP address

– It is recommended that IaaS CSP provides IP address reservation.

NOTE – CSP reserves a pool of public IP addresses or a segment of private IP addresses for the CSC.

– It is required that IaaS CSP allows the CSC to apply, bind, unbind, query, release an IP address to processing resources or storage resources.

– It is recommended that IaaS CSP allows the CSC to allocate IP addresses to provisioned processing resources or storage resources with dynamic or static method.

– IaaS CSP can optionally provide network address translation (NAT).

7.3.4 Network isolation

– It is required that IaaS CSP provides the CSC with isolated tenants' networks.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to isolated tenants' networks, such as create, query and release.

7.3.5 Virtual networking

– It is recommended that IaaS CSP manages virtual networking to provide network connectivity amongst various processing and storage resources.

7.3.6 Load balance

– It is recommended that IaaS CSP optimizes infrastructure resources utilization by providing load balance related functions, such as throughput, response time, to avoid overload of any one of the infrastructure resources.

– IaaS CSP can optionally provide multipath routing to achieve an optimized traffic management (e.g., to improve network utilization, to guarantee QoS at network congestion or fault).

7.3.7 Firewall

– It is recommended that IaaS CSP delivers physical or virtual firewall to the CSC.

7.3.8 Gateway

– It is recommended that IaaS CSP provides necessary network interworking functions so that the CSC uses provisioned infrastructure resources as if they are at the CSC's premises.

7.3.9 Network configuration

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to the network configurations according to the objectives of the SLA.

8 Security considerations

Security aspects for consideration within the cloud computing environment, including IaaS, are addressed by security challenges for the CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of Infrastructure as a Service

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

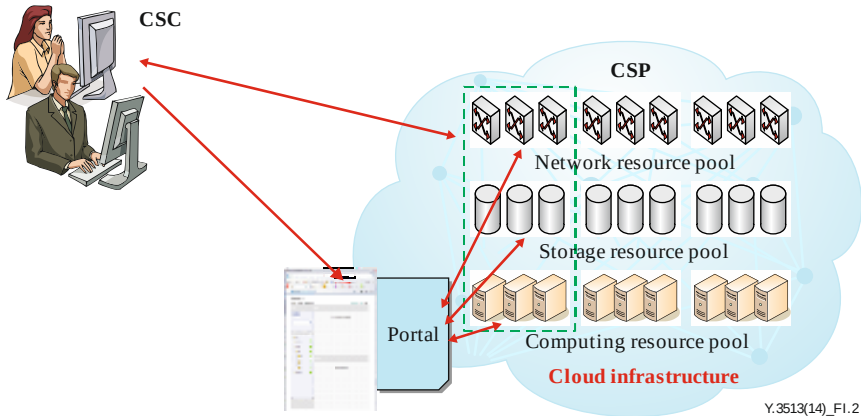
This appendix includes IaaS related use cases including an infrastructure level use case, and computing , storage and network service use cases.

I.1 Use case template

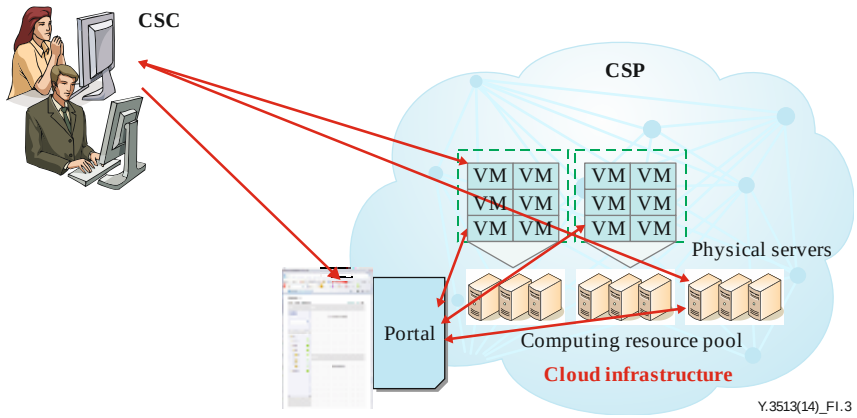
The use cases developed in this appendix should adopt the following unified format for better readability and convenient material organization.

Use case	
Name	Title of the use case
Abstract	Description for overview and feature of the use case
Roles	Roles relating to or appearing in the use case
Figure	Figure to present the use case (UML-like diagram is suggested for clarifying relations between roles but it is not mandatory)
Pre-conditions (optional)	The pre-conditions represent the necessary conditions or use cases that should be achieved before starting to describe the use case. As dependency may exist among different use cases, such a description can help others to understand relation among the use cases.
Post-conditions (optional)	Similar to that for pre-conditions, the post-conditions describe conditions or use cases that will be carried out after the termination of currently describing use case. Such an inter-use case dependency clarification improves the collaboration of use cases.
Description	Description introduces the detail information of the use case, such as the processes or major steps. It is helpful for the reader to better understand it.
Requirements	Requirements (titles) derived from the use case. For example; – **Large-scale migration**: A CSP in the inter-cloud federation is required to be able to guarantee continuity of all the services in this CSP by large-scale service migration with minimum impact during a desired period. It is recommended to consider priority of services when migrating.

I.2 IaaS use case on infrastructure level

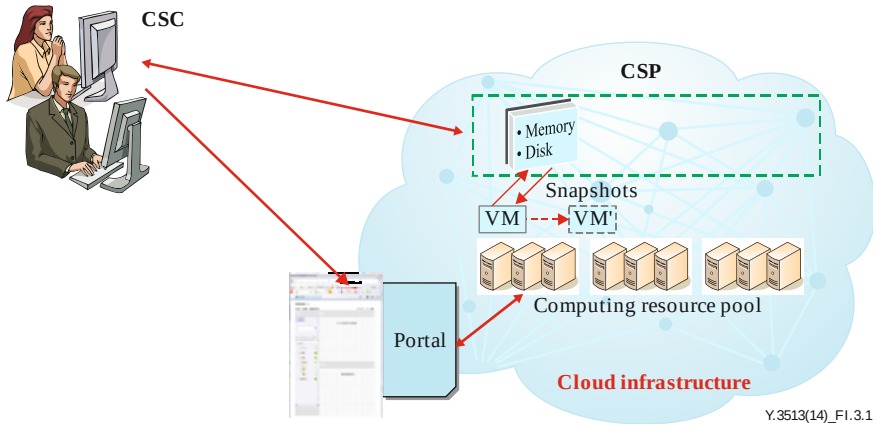
Use case	
Name	IaaS use case on infrastructure level
Abstract	CSC uses a composition of processing, storage and networking resources with service logic, specific SLAs and charging model, provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves computing, storage and network functions.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions (e.g., infrastructure templates) related to the infrastructure. – CSC selects the appropriate infrastructure template from the query results and requests the CSP to create an infrastructure based on the selection. – CSC manages and monitors the created infrastructure during its lifecycle. It includes, but not limited to: • **assign**: start IaaS by allocating to the service the **available resources** as identified by **configuration** (e.g., create, initiate, start, enable, power-on) • **modify**: change the amount of **resource** being **in-use** according to the demand (e.g., update, add, enable, disable) • **release**: close the IaaS service by making **available** the **resource** being **in-use** by the service (e.g., delete, shutdown, disable, power-off) • **query**
Requirements	– IaaS operations (refer to clause 7) – Infrastructure resources status (refer to clause 7) – Infrastructure template (refer to clause 7)

I.3 IaaS computing service use case

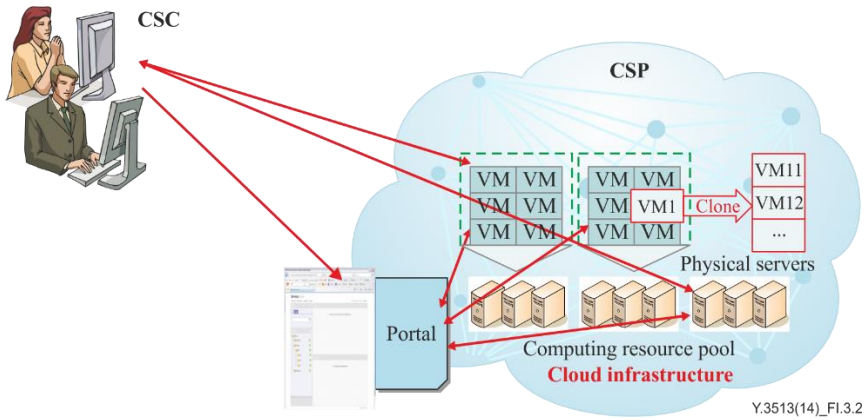
Use case	
Name	IaaS use case on computing
Abstract	CSC uses physical machine or virtual machine provided by the CSP.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves the functions exposed that are related to computing.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions necessary for computing functions. – CSC selects the appropriate template and image from the query results and requests CSP to create a virtual machine or physical machine based on the selection. – CSP creates a virtual machine or physical machine from the computing resource pool based on the information provided by the CSC. – CSC requests CSP to start up the virtual machine or physical machine. – CSC manages and monitors the created virtual machine or physical machine during its lifecycle. It includes, but not limited to: • start, shutdown, suspend, restore, hibernate, wakeup and delete the virtual machine; • start, shutdown, hibernate and wakeup physical machine; • query the virtual machine or physical machine information and its status; • set migration or scaling policies for the virtual machine; • scaling the virtual machine; • execute performance metrics; • snapshot, backup, clone the virtual machine; • configure VM time synchronization; • reservation computing resource; • make image based on the virtual machine; • generate template based on the virtual machine.
Requirements	– Physical machine (refer to clause 7.1.1) – Virtual machine (refer to clause 7.1.2) – VM migration (refer to clause 7.1.3)

Use case	
	– VM scaling (refer to clause 7.1.4) – VM snapshot (refer to clause 7.1.5) – VM clone (refer to clause 7.1.6) – VM backup (refer to clause 7.1.7) – VM time synchronization (refer to clause 7.1.8) – VM reservation (refer to clause 7.1.9) – VM image (refer to clause 7.1.10) – VM template (refer to clause 7.1.11)

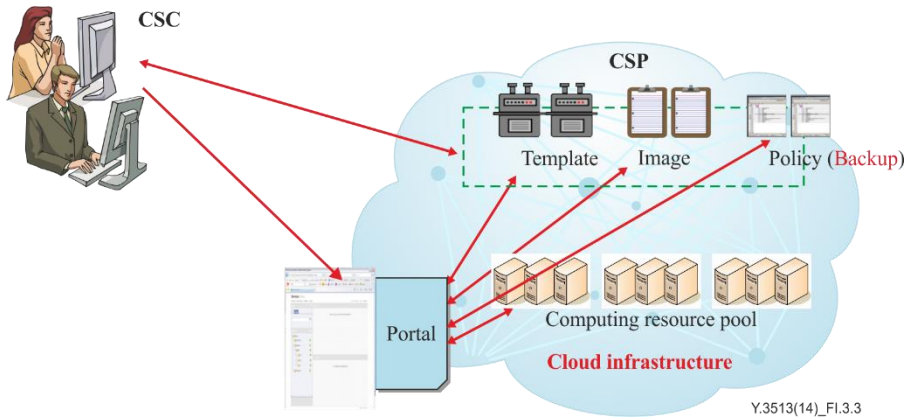
I.3.1 VM snapshot use case

Use case	
Name	IaaS use case on VM snapshot
Abstract	CSC uses the snapshot functions during the lifecycle of a VM.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM which is in normal running state, stopped state or suspending state.
Post-conditions (optional)	
Description	– CSC has found that the VM is working properly; and an operation that may cause faults, for example, conducting a software upgrade, is to be performed. – CSC snapshots the VM, a name for the snapshot is required while the description is optional. It also contains the runtime information, including the VM CPU and memory states, if the VM is not powered-off. – CSC performs the software upgrade operation, VM is in VM' (as the figure shows) state and there is something wrong, for example, the user data of the software has been lost and VM cannot work properly. – CSC recovers the VM using the snapshot it created above and all the software running on the VM is recovered to state "VM" too.
Requirements	– VM snapshot (refer to clause 7.1.5)

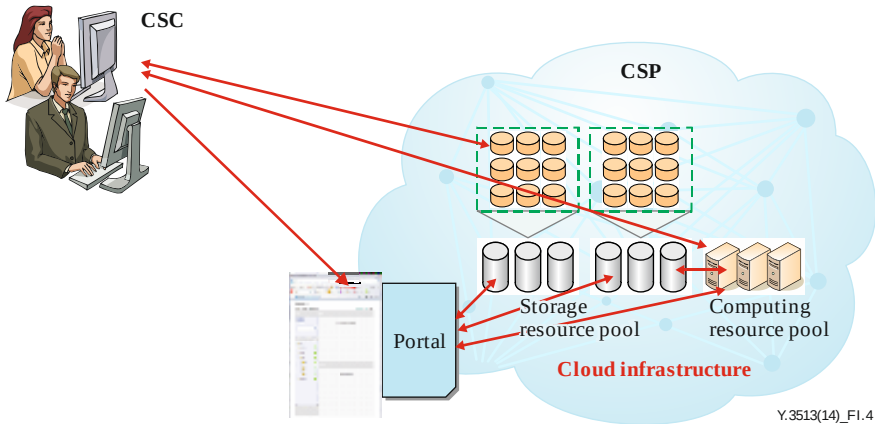
I.3.2 VM clone use case

Use case	
Name	IaaS use case on VM clone
Abstract	CSC uses the clone functions to create a new VM.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM (e.g., VM1). – CSC needs more VMs identical or similar to VM1.
Post-conditions (optional)	
Description	– CSC selects VM1 which it wants to clone. – CSC selects clone operation, and changes some regular parameters, for example, VM name, the number of CPUs and memory. In this case, CSC clones two VMs, i.e., VM11 and VM12. – CSC starts the cloned VMs, and the cloned VMs are similar to the original one, with slight difference in the changed parameters.
Requirements	– VM clone (refer to clause 7.1.6)

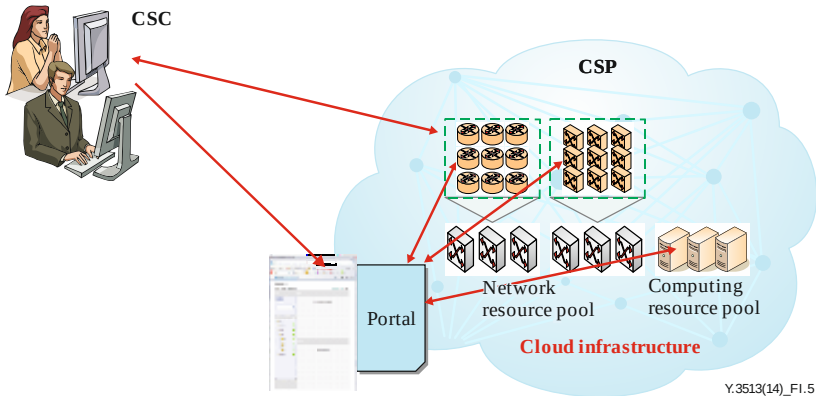
I.3.3 VM backup use case

Use case	
Name	IaaS use case on VM backup
Abstract	CSP recovers the VM according to the backup policies CSC configured.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM which is in a normal running state and deployed CSC's application on the VM. – CSC needs backup functions to support its application.
Post-conditions (optional)	
Description	– CSC configures the backup policy for the VM, and the policy could be weekly backup. – CSP performs the backup operation according to the policy the CSC configured. – CSP detects that the VM becomes faulty or its data is lost, CSP recovers the VM using backup automatically without CSC's awareness.
Requirements	– VM backup (refer to clause 7.1.7)

I.4 IaaS storage service use case

Use case	
Name	IaaS use case on storage
Abstract	CSC uses block, file or object storage directly or attach to the virtual machine provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through the portal with appropriate security mechanism and retrieves the functions exposed that are related to storage and attached computing, if needed.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions related to storage functions. – CSC selects the appropriate storage from the query results and requests the CSP to create block, file or object storage based on the selection. – CSP creates block, file or object storage from the storage resource pool based on the information provided by the CSC. – CSC attaches the created storage to specified virtual machine if needed. – CSC manages and monitors the created storage during its lifecycle. It includes, but not limited to: • create, attach, detach, query and delete a volume of storage at either block level or file-system level; • write, read and delete data; • query the storage information and its status; • set migration or I/O limitation policies; • execute performance metrics; • snapshot or backup the storage; • reservation storage resource.
Requirements	– Storage migration (refer to clause 7.2.1) – Storage snapshot (refer to clause 7.2.2) – Storage backup (refer to clause 7.2.3) – I/O performance (refer to clause 7.2.4) – Storage resource reservation (refer to clause 7.2.5)

I.5 IaaS network service use case

Use case	
Name	IaaS use case on network
Abstract	CSC uses network functions, such as IP address, VLAN, virtual switch, load balance and firewall provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves the functions exposed that are related to network and computing, if needed.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported network functions (e.g., IP address, VLAN, virtual switch, load balance, firewall). – CSC selects the appropriate network service from the query results and requests CSP to create a network based on the selection. – CSC requests the CSP to attach the created network with the related virtual machine. – CSC manages and monitors the created network during its lifecycle. It includes, but not limited to: • bind the network connectivity service to the related virtual machine; • query the network and its status; • update, upgrade or scaling the network; • execute performance metrics; • manage the IP address pool; • manage network services, such as VLAN, virtual switch, load balance, firewall, gateway; • manage tenants' network according to the SLA objectives.
Requirements	– Network policy migration (refer to clause 7.3.1) – Network QoS (refer to clause 7.3.2) – IP address (refer to clause 7.3.3) – Network isolation (refer to clause 7.3.4) – Virtual networking (refer to clause 7.3.5) – Load balance (refer to clause 7.3.6) – Firewall (refer to clause 7.3.7) – Gateway (refer to clause 7.3.8) – Network configuration (refer to clause 7.3.9)

Appendix II

Methodology of mapping use cases and requirements

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

In order to improve the effectiveness of this Recommendation and the harmonization with the related ITU-T Recommendations, the same use case driven approach is applied in this Recommendation as described in [ITU-T Y.3501]. A set of use cases had been selected and elaborated, based on these use cases, different categories of requirements may be introduced.

Bibliography

[b-ISO/IEC OVF] ISO/IEC Standard 17203:2011, Information technology -- *Open Virtualization Format (OVF) specification*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014