International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3520

(06/2013)

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

Cloud Computing

Cloud computing framework for end-to-end resource management

Recommendation ITU-T Y.3520

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.3520

Cloud computing framework for end-to-end resource management

Summary

Recommendation ITU-T Y.3520 presents general concepts of end-to-end resource management in cloud computing; a vision for adoption of cloud resource management in a telecommunication-rich environment; and multi-cloud, end-to-end resource management for cloud services, i.e., management of any hardware and software used in support of the delivery of cloud services.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.3520	2013-06-22	13

Keywords

Cloud computing, cloud service, framework, requirement, use case.

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.3520

Cloud computing framework for end-to-end resource management

1 Scope

This Recommendation provides a framework for end-to-end resource management in cloud computing. It includes:

– general concepts of resource management for end-to-end cloud computing resource management;
– a vision for adoption of resource management for cloud computing in a telecommunication-rich environment;
– multi-cloud, end-to-end management of cloud computing resources and services, i.e., management of any hardware and software used in support of the delivery of cloud services.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 emergency telecommunications (ET) [b-ITU-T Y.2205]: ET means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services.

3.1.2 emergency telecommunication service (ETS) [b-ITU-T E.107]: A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.

3.1.3 management system [b-ITU-T M.60]: A system with the capability and authority to exercise control over and/or collect management information from another system.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 resource management: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation
4G	Fourth Generation
CDN	Content Delivery Network
CRM	Customer Relationship Management
CSC	Cloud Service Customer
CSP	Cloud Service Provider
ET	Emergency Telecommunications
ETS	Emergency Telecommunication Service
FI	Functional Interface
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LTE	Long Term Evolution
MPLS	Multi-Protocol Label Switching
PHP	Hypertext Preprocessor
QoS	Quality of Service
SES	Software Enabled Services
SLA	Service Level Agreement
SMI	Service Management Interface
VoIP	Voice over IP
WAN	Wide Area Network
WiFi	Wireless Fidelity

5 Conventions

In this Recommendation:

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

In the body of this document and its appendixes, 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 Cloud resource management overview

The following clauses provide an overview of the general concepts of end-to-end cloud computing resource management in a telecommunication rich environment.

6.1 Introduction

One significant value of cloud service providers will most likely be the rapid design, development, deployment and management of cloud services. With the adoption of cloud computing service delivery capabilities, multiple service providers will provide more cloud services as composite or mash-up services. Service providers will increasingly have as objective the rapid delivery of more customized, composite cloud-based services tailored to various customer scenarios [b-FGCC Part 4].

In this Recommendation, the term multi-cloud refers to usage scenarios involving use of various cloud services implemented by more than one cloud service provider. This is not to be confused with the multi-platform cloud computing environment, which is a characteristic of cloud service providers that have chosen to offer a variety of programming and runtime execution facilities to assist in development and execution of cloud applications.

Cloud applications (also known as cloud workloads) are applications (i.e., software programs designed for a specific purpose) that require execution in the cloud service provider's data centres in order for cloud services to be instantiated and become available for use by the cloud service users. In other words, a cloud application needs to execute to make one or more cloud services available.

Cloud service providers need to increasingly offer multi-cloud platform solutions to support the above scenarios. Such solutions will need to be flexible and effective in managing resources across multi-cloud service providers [ITU-T Y.3501].

This can be realized using cloud services, delivered through cloud computing capabilities with reusable services. Cloud service providers need to develop deep insight into, and understanding of, the run-time aspects of service delivery as well as the management of these services and the resources required to deliver them.

Therefore, there is need for a common concept for end-to-end resource management across multiple cloud service providers.

Complex, media-rich, composite services use a variety of infrastructures, both telecommunication and information technology (IT), and are composed of individual service components that may be acquired from, or exposed to, third parties.

6.2 Service delivery management structure

The framework described in this Recommendation can be used to enable the delivery of cloud services, independent of the underlying software or network technologies. This framework, which is a service delivery management structure, needs to address the full cloud services lifecycle, covering such important use cases as service composition, aggregation, and service catalogues.

Management of cloud services needs to provide a framework for the essential building blocks required to manage the delivery of cloud services and foster the basis for detailed service delivery management.

One objective is to provide a means to allow consistent end-to-end management, including accounting, of services exposed by, and across, domains and platforms of different cloud service providers. A standard framework and best practices are needed to support business practices associated with multiple provider cooperation throughout the lifecycle of the service and to foster wide adoption of the standard artefacts in any architecture, technology environment and service domain.

Achieving consistent maintenance of cloud services sourced from different domains is a challenging task. To address this challenge, an approach is wanted that enables and supports consistent access to the cloud services. Such an approach is desired to complement the functional capabilities exposed by the software component's interfaces with additional lifecycle management operations. This approach should also enable reusability of services in different environments, especially in cloud computing.

Frameworks, architecture, design patterns and best practices are required to realize the above objectives for the cloud service providers. The interfaces of individual service components are not the primary focus as the actual interfaces may vary across different implementations, vendor technologies and operator requirements. Standard design principles and frameworks are required to allow for the rapid development, deployment and management of composite multi-cloud services provided by the telecommunication industry.

This Recommendation provides a framework to guide architects and developers of cloud service providers for the end-to-end management of cloud computing resources.

6.3 Difference between cloud computing and traditional form of computing

There are two principal differences between cloud computing and the traditional form of computing that make the problem of managing resources associated with cloud services more difficult. One difference is the virtualization of the computing and network resources in the cloud computing reference architecture [b-FGCC Part 2]. The other difference is that multiple cloud service provider domains are increasingly involved in the delivery of cloud services and this environment greatly complicates end-to-end resource management.

6.4 Resource management for a single cloud service provider

The overall resource management should be viewed from the point of view of the lifecycle management of a cloud application. The application, as it passes through its lifecycle, must be acted upon by traditional business processes associated with management system functions such as administration, provisioning/configuration, service assurance, and charging/billing/settlement.

As shown in Figure 1, in the simpler case of an application that resides on a single cloud computing infrastructure, it becomes dependent on two distinct categories of virtualized resources. The dotted arrows depict the active coordinated relationship that must be maintained between resources at each level.

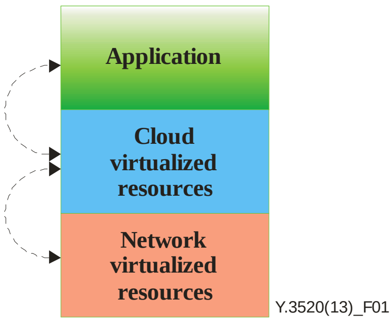


Figure 1 – Applications residing on a single cloud computing infrastructure

A resource management issue requiring further work is how to use existing cloud management systems to maintain awareness of which logical and physical resources are actually relevant to a specific instance of a specific application at any given point in time.

Due to the elasticity characteristic of cloud computing, the cloud computing infrastructure can configure additional resources to handle changing application demands; there are additional requirements, needing further analysis, for dynamically reconfiguring the underlying network configurations in response to the changing resources at various components of the cloud implementation. This issue arises both within the internal network fabric of large cloud computing data centres, between two and the interconnecting networks in hybrid scenarios, and across transport networks and content delivery networks.

Another issue that arises is the division of responsibility between an internal cloud computing virtualization management layer and an external management system. Although the cloud computing virtualization layer can typically manage its own physical and logical resource allocations for supported applications, an external management system may be desired to dynamically reallocate resources in a coordinated fashion across the three levels shown in Figure 1 or to track and have knowledge of those changing relationships.

As shown in Figure 2, the capability of a management system to both manage resource allocations and track their instantaneous state could enable that management system to provide the information necessary to display status of a given service, and all of the underlying relevant resources, at any given point in time.

From the point of view of the quality of service of resource management, the issue is how to ensure that the service assurance systems are receiving relevant telemetry from the cloud or network resources actually involved in delivering a particular instance of a service. The issue is less to do with what telemetry data need to be managed, as each dataset is often unique to a given telecommunication cloud implementation of a management system, but more to do with how to use the cloud infrastructure to do so effectively and economically.

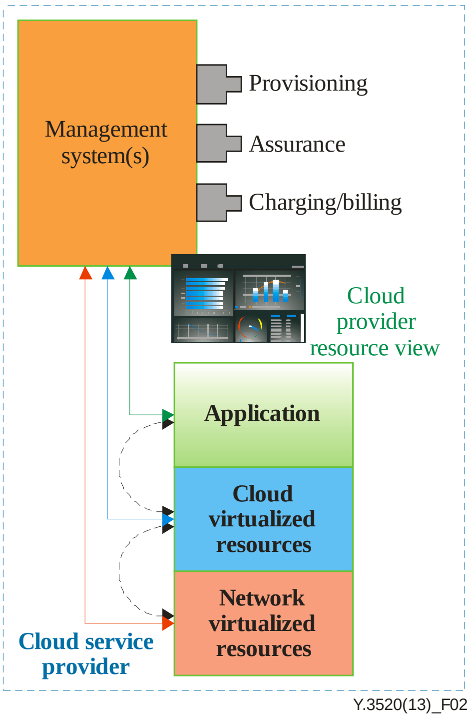


Figure 2 – Resource management system

6.4.1 Software enabled services

The objective of the software enabled services (SES) management concept [b-TMF SES] enables both traditional service providers and Internet content and media service providers to leverage the opportunities and service marketplace that are presented by the convergence of networking and IT. Specifically, the SES management solutions provide a means to allow consistent end-to-end management and metering of services exposed by and across different service providers' domains and technologies.

Operations, administration and management interfaces for cloud services today are structured in silos per technology, standardized by specific standards development organizations or implemented by vendors as proprietary implementations. This presents a challenge in the rendering of consistent management of services sourced from different domains.

The SES management solution proposes a mechanism to allow consistent access to the software components information as well as management operations. This consistent access is achieved by incorporating the management interface in addition to the functional interface (FI) definition that is part of software component creation. The SES design pattern per the SES reference architecture [b-TMF SES] enables reusability of services in different environments, including that of cloud computing by manipulating the SES lifecycle management metadata which is supporting the SES management interface (SMI) operations.

The SES pattern is defined to also handle those cases where the composed service is not able to manage all of the management dependencies by means of the logic which is triggered by the SMI operations. In this case, the lifecycle management metadata associated with the SMI is providing a recipe which describes how to manage the composition members.

Protocol neutral interface information models and class models of the SMI, along with corresponding statements of interface information requirements and interface information use cases, can be defined as described by the software enabled solution initiative [b-TMF SES].

In order for implementation of software enabled services (SES) to be as useful as possible, it is recommended that the following basic rules for a "well designed service" be considered.

- It is recommended that service design be as efficient as possible, requiring only the needed information for both input and output parameters, without being verbose. There should not be many arguments on the different management system operations.
- It is recommended that service design be simple, allowing for easy implementation in legacy as well as in new services. There should be no complex dependencies between the arguments of the different management information system operations.
- It is recommended that service implementation rely on industry standards in order to guarantee that it will be interoperable between different platforms.
- It is recommended that the service management interface (SMI) be extensible and generic to accommodate all SES scenarios. It is recommended that the SMI be easy to extend and that this interface be adapted to support additional management aspects of a specific domain or of a specific vendor.
- It is recommended that the SMI be agnostic to implementation architecture or business processes, to ensure adoption by many industry sectors.
- It is recommended that a non-"well designed service" be wrapped by a façade service in order to make it a "well designed service".

The SMI in the software enabled services reference architecture [b-TMF SES] can be used to describe the management capabilities of SES. Examples of these capabilities are in the areas of invocation, provisioning, status, history, usage and health monitoring and associated alerts, management lifecycle state configuration as well as decommissioning of a given software enabled service [b-TMF TR198].

The software enabled services (SES) management solution was designed to address the management of a single cloud service provider. In the next clause, it will be explained how the same concept can be applied to address a multiple cloud service provider scenario.

6.5 Resource management for multiple cloud service providers

Clause 6.4 describes the managing of resources for a single cloud service provider. However, cloud service delivery scenarios typically involve coordination across multiple cloud service providers residing in different domains.

Figure 3 illustrates the end-to-end management framework in a multi-cloud service provider domain scenario. Given the way in which customized management interfaces are exposed in a single cloud service provider implementation, the framework enables end-to-end management of composed services and their underlying dynamically changing resources.

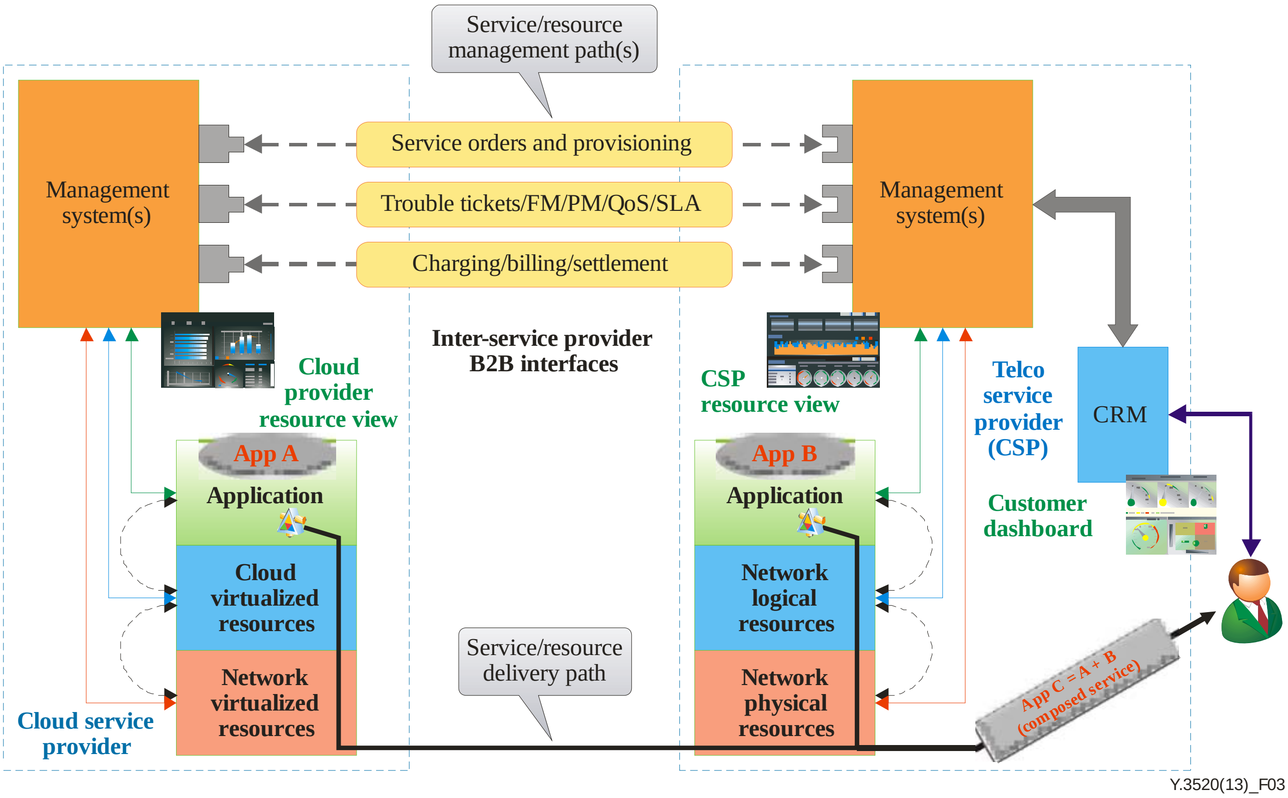


Figure 3 – End-to-end management expectations in a multi-cloud scenario

Similar to the case of a single cloud scenario, service and resource management interfaces need to be able to manage the relevant underlying resources in a coordinated manner that is effectively transparent to the external systems that are interacting with those management interfaces.

Figure 3 depicts a management system architecture providing the needed management interfaces (again, the interfaces themselves are not at issue, as each implementation may have fine-tuned its own). The best practices should provide the flexibility for the cloud application itself to expose its service/resource management interfaces. In addition, they need to enable a management system to expose one or more of the interfaces so that the management system is tracking the dynamic changes in the underlying resources allocated to support the cloud application being managed.

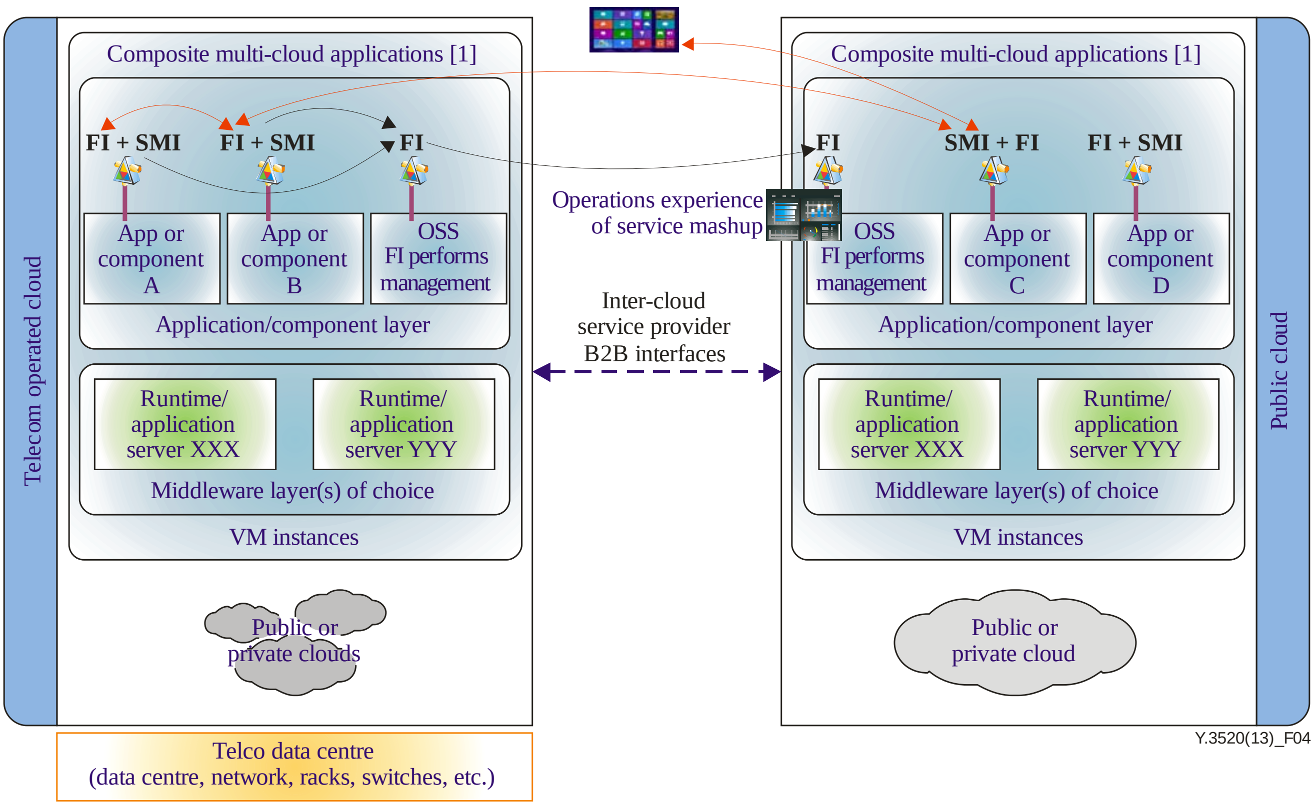
The framework permits each cloud service provider (CSP), as well as the cloud service user, to have an accurate knowledge regarding the actual status of services via metrics retrieved from the underlying relevant resources across a multi-cloud environment. In other words, all three dashboards depicted in Figure 3 need to accurately display the status of the services. In addition, the framework should consider a comprehensive service lifecycle management process from the point of view of cloud service providers and cloud service users, i.e., the stages needed from the time the cloud service user makes a request until the cloud service provider receives compensation.

7 Requirements for the resource management involving multi-cloud service providers

7.1 High-level architecture for end-to-end multi-cloud resource management

Figure 4 shows a high-level architecture for end-to-end multi-cloud resource management. This architecture depicts the virtual machines containing a software stack consisting of middleware layers containing application servers hosted by the runtime environment of choice, on top of which cloud applications execute.

Figure 4 also shows both functional interfaces (FIs) and service management interfaces (SMIs) being exposed by various cloud applications running on multiple cloud data centres. The information can be consumed from various SMIs that are exported by multiple applications executing in multiple cloud data centres, allowing for a comprehensive end-to-end multi-cloud resource management and monitoring system to be realized.



NOTE – Composite multi-cloud applications can be written in a runtime and programming environment of choice, independent of the choice of cloud provider or cloud-deployment model. For example, use of Java [b-java], Node.js [b-nodejs], PHP [b-PHP] or .NET [b-NET] in both private and public clouds.

Figure 4 – Architectural vision for multi-cloud, multi-platform cloud management

In Figure 4, the applications executing in the virtual machines (VMs) could be a composite, distributed application built from various software components. A VM instance could contain all software components that belong to such an application, or only some of them in the case where the application is distributed, and executing in more than one VM (hence the reference to application/components in Figure 4).

The architecture shown in Figure 4 enables interoperable applications to support cloud burst or hybrid cloud computing scenarios.

FI is the acronym for Functional Interface of a given cloud service; this is the service interface that actually delivers the functionality the service was designed for. SMI, however, is the acronym for SES Management Interface for that same given service (see clause 6.5 for details).

7.2 Functional requirements for end-to-end cloud resource management

To meet the high level architecture of end-to-end cloud resource management described in this Recommendation, a cloud computing platform should conform to the following requirements:

It is required that CSP supports the architectural and functional capabilities offered by the "Software Enabled Services" management solution as described in clause 6.4.1 in order to realize end-to-end cloud resource management.

It is recommended that the cloud computing platform offers the deployment choice and workload portability across multiple CSPs in order to share workloads.

It is recommended that the cloud computing platform provide the ability to support hybrid cloud applications, where the components of the cloud application run on various cloud data centres managed by different CSPs.

It is recommended that cloud service provider, irrespective of the deployment model they use, provide the support for multiple application frameworks, programming languages, tools, and technology platforms, thereby lowering the potential for lock-in into specific solution or middleware technology.

It is recommended that the cloud computing platform provides an architecture enabling telecommunications-grade capabilities including reliability, fail-over, and monitoring inclusive of choice of middleware, programming language and runtime.

It is recommended that the cloud computing platform supports workload portability and related management capabilities (e.g., control, operation and monitoring) amongst cloud service providers, supporting various cloud deployment models, in a cost effective way.

8 Cloud resource management for emergency telecommunications

Emergency Telecommunications (ET) [b-ITU-T Y.2205] are any emergency related service that requires special handling relative to other services (i.e., priority access for authorized users, and priority treatment to emergency traffic).

While not always required, if/when the resources of the CSP are used to support the Emergency Telecommunications Service (ETS) [b-ITU-T E.107], appropriate resource management functions will be needed to allow priority treatment in the use of the cloud computing resources by authorized users. The requirements in [b-ITU-T Y.1271] are relevant.

NOTE – Requirements in [b-ITU-T Y.1271] apply across multiple layers of the cloud computing reference architecture [b-FGCC Part 2].

9 Security considerations

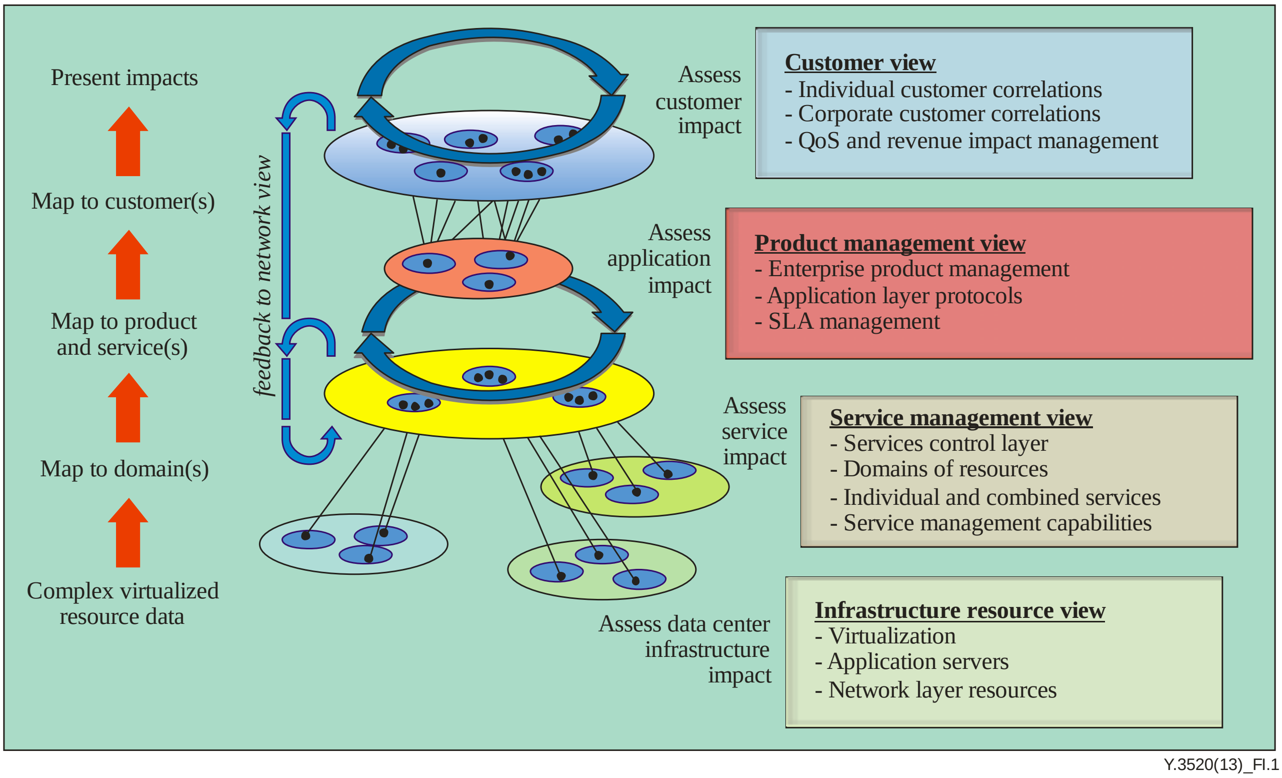
The single cloud and multi-cloud resource management framework described in this Recommendation is based on the interconnections within a single cloud provider or between two or more cloud computing systems operated by different service providers. Thus, secure interconnection within and across the systems should be considered. Protection of internal management system interfaces and information against unauthorized access, internally or by an external interconnected entity, should also be considered. Exposed internal and external management interfaces should also be security protected. It is recommended that the applicable X, Y and M series of ITU-T security Recommendations be taken into consideration, including access control, authentication, data confidentiality, communications security, data integrity, availability and privacy.

Appendix I

Comprehensive view of management layers

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

Figure I.1 is an attempt at describing the management layers and how the service management interface(s) SMI(s) for each layer correlate with each other to offer a complete picture. The cloud computing data centre implementation layers are depicted by large circles parallel to each other. The SMIs are depicted by small blue circles containing the information required by the management system in order to achieve a holistic view of the entire operation. The straight lines between each plane show the flow of information and relationship between what is happening at each layer, depicting how each layer is related to, and affected by, the neighbouring one. Looking at the diagram in its entirety helps the viewer to realize why it makes sense to expose consistent SMIs (management interfaces) from each layer, and to expose management information and telemetry in a consistent matter that can then be rolled up into a comprehensive diagnostics and management solution that can be used by a telecom operator offering and consuming cloud services and products.



NOTE – Domains are related to CSP.

Figure I.1 – Comprehensive view of management

Appendix II

Cloud service provider (CSP) end-to-end service management

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

The following use case describes the challenges associated with end-to-end service management.

Figure II.1 illustrates an example where a cloud VoIP service is provided by CSP1 to CSP2 that is bundling it with other services and reselling a package to a cloud service customer (CSC). Even if CSP1 runs network services such as a content delivery network (CDN), CSP2 provides network connectivity services to the end user through its own core networks (e.g., IP/MPLS) and access networks (e.g., the backhaul, Wi-Fi, 3G/4G/LTE and enterprise LAN/WAN infrastructures).

When a CSC, such as an IT department, has a problem with the cloud VoIP quality of service, it contacts CSP2 (using a customer relations management (CRM) system). The CSP2 support agent should have the capability to see the health and welfare of the VoIP service from a holistic (end-to-end) perspective. This requires visibility into the VoIP and network resource management systems of both CSP1 and CSP2.

As shown in Figure II.1, there are the two types of connection paths:

1. **Service delivery path** – used by the functional interfaces of the services to deliver the combined service value to the customer. In this use case, cloud VoIP and IP/MPLS are combined to create a premium ICT bundle.
2. **Service management path(s)** – all of the logical management paths that perform operations and maintenance functions such as provisioning, service assurance and charging/billing of the relevant services to this bundle.

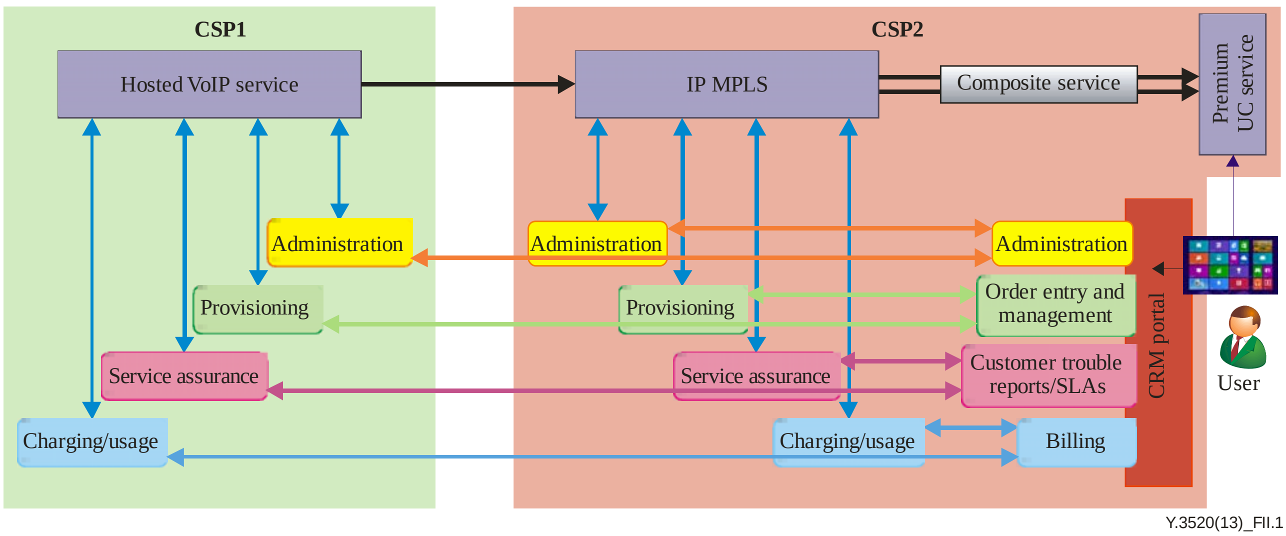


Figure II.1 – Managing multi-cloud services end-to-end

The delivery path for the service, via their functional interfaces, is not addressed by this use case.

What is addressed is efficient implementation of all of the resource management functions depicted by the lines between the CRM portal and the administrative, provisioning, service assurance, and charging functions for each component (VoIP, etc.) that makes up a complete service. This challenge, associated with effective cloud resource management, is a major technical issue and can be a limiting factor for the adoption of cloud computing based solutions. In order for the composite cloud computing services to work effectively, all the prerequisite services of both CSP1 and CSP2 must function properly.

When either of the two CSP's becomes aware of a VoIP problem, tools are needed so that they quickly resolve the problem in an effective manner. This includes being able to see via service dashboards/CRM portal what has occurred relative to the VoIP service and to investigate in order to obtain greater details concerning any significant item. Additionally, the customer service agent should also be able to initiate an order for new or changed service configurations. However, if the agent lacks access to useful end-to-end cloud resource management tools, and can only create a trouble ticket and then pass the problem off to another agent for action, the cloud service user will be unsatisfied and this could potentially result in excessive operational expenses.

Bibliography

[b-ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications*.

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks Emergency telecommunications – Technical considerations*.

[b-FGCC Part 2] ITU-T Focus Group on Cloud Computing -Technical Report (2012), *Part 2: Functional requirements and reference architecture.* http://www.itu.int/pub/T-FG-CLOUD-2012-P2

[b-FGCC Part 4] ITU-T Focus Group on Cloud Computing -Technical Report (2012), *Part 4: cloud resource management gap analysis.* http://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P4-PDF-E.pdf

[b-java] http://www.java.com.

[b-NET] http://www.microsoft.com/net/.

[b-nodejs] http://www.nodejs.org/.

[b-PHP] http://www.php.net/.

[b-TMF SES] TM Forum, Software Enabled Services Management http://www.tmforum.org/SoftwareEnabledServices/4664/home.html

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer and Code Pack, Release 1.5.* http://www.tmforum.org/TechnicalReports/TR198MultiCloudService/52095/article.html

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, 2013