International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3537

(09/2022)

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

Cloud Computing

Cloud computing – Functional requirements of a cloud service partner for multi-cloud

Recommendation ITU-T Y.3537

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
Computing power networks	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.3599**
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–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.3537

Cloud computing – Functional requirements of a cloud service partner for multi-cloud

Summary

Recommendation ITU-T Y.3537 provides the overview of multi-cloud and the functional requirements of a cloud service partner for supporting multi-cloud by identifying various use cases related to multi-cloud in terms of cloud service customer, cloud service provider and cloud service partner. It also provides cloud computing activities to support multi-cloud as a sub-role of cloud service partner by identifying interactions between cloud service customer, cloud service provider and cloud service partner.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3537	2022-09-29	13	11.1002/1000/15060

Keywords

Cloud computing, cloud service partner, functional requirement, multi-cloud manager, multi-cloud.

---

* 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 received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Y.3537

Cloud computing – Functional requirements of a cloud service partner for multi-cloud

1 Scope

This Recommendation provides the overview of multi-cloud and functional requirements of a cloud service partner for supporting multi-cloud. It addresses the following subjects:

– Overview of multi-cloud and multi-cloud management;

– Cloud computing activities of a multi-cloud manager as a sub-role of cloud service partner;

– Interactions between cloud computing roles;

– Functional requirements of multi-cloud manager;

– Use cases to derive functional requirements of multi-cloud manager.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 cloud deployment model [ITU-T Y.3500]: The way in which cloud computing can be organized based on the control and sharing of physical or virtual resources.

NOTE – The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.

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

3.1.5 cloud service partner [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

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

3.1.7 community cloud [ITU-T Y.3500]: Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.8 hybrid cloud [ITU-T Y.3500]: Cloud deployment model using at least two different cloud deployment models.

3.1.9 private cloud [ITU-T Y.3500]: Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer.

3.1.10 public cloud [ITU-T Y.3500]: Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 composed cloud service: Cloud services in a group.

NOTE – In multi-cloud, composed cloud service is managed as a group by multi-cloud management.

3.2.2 data connectivity: Ability to access and share the data for interoperability.

3.2.3 multi-cloud: Use of cloud services in the public cloud from two or more independent cloud service providers at the same time for business.

NOTE – Multi-cloud, known as multi-cloud computing, is distinguished from multiple cloud which is an environment involving two or more cloud service providers (CSPs).

3.2.4 multi-cloud management: Management of cloud services in form of a composed cloud service from multiple cloud service providers at a single point.

NOTE – Capabilities of multi-cloud management include configuring, controlling and monitoring composed cloud service from multiple cloud service providers.

3.2.5 network connectivity: Ability to connect various networks for interoperability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

I/O Input/Output

vCPU virtual Central Processing Unit

VPN Virtual Private Network

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 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 Overview of multi-cloud

6.1 Introduction to multi-cloud

Multi-cloud refers to the use of cloud services in the public cloud from two or more independent cloud service providers (CSPs) at the same time for the customer's business as shown in Figure 6-1, which is also known as multi-cloud computing. It differs from hybrid cloud, inter-cloud, and federated cloud which also uses an environment involving two or more CSPs.

– **Hybrid cloud**: Cloud deployment model using at least two different cloud deployment models such as public cloud, private cloud, and community cloud described in [ITU-T Y.3500]. In a hybrid cloud, synchronization and communication between different cloud deployment models for interoperability and portability are provided.

– **Inter-cloud**: Paradigm for enabling the interworking between two or more cloud service providers, described in [b-ITU-T Y.3511]. Inter-cloud interacts between CSPs, while multi-cloud interacts between CSPs and a cloud service customer (CSC).

– **Federated cloud**: Practice of interconnecting two or more CSPs for the use of the federated cloud resources, depending on the specific federation agreement between CSPs.

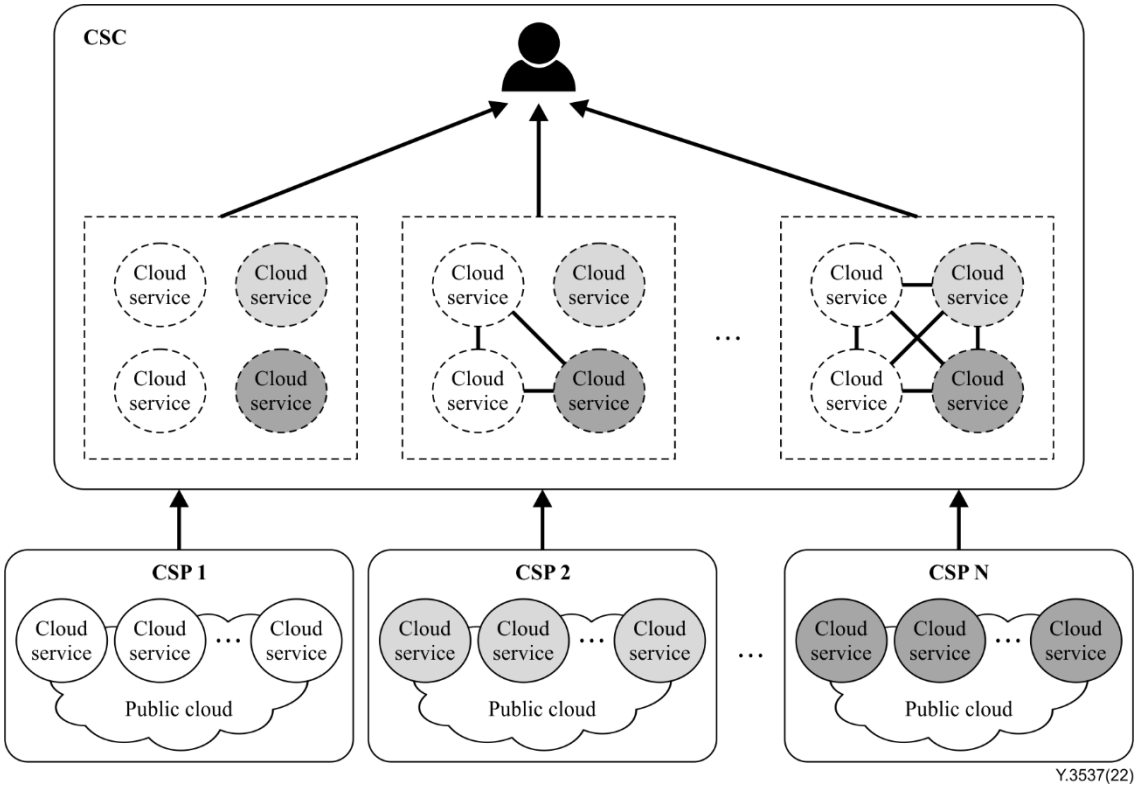


Figure 6-1 – Concept of multi-cloud

There are several reasons to deploy multi-cloud, such as avoiding the reliance on a specific vendor, selecting and using cost-effective or low latency cloud services, mitigating the risk from disasters, and so on.

The representative benefits of adopting multi-cloud are considered as follows:

– **Risk mitigation**: By multi-cloud, a business avoids service outages due to the failure of cloud services. If one CSP goes down, the business service will be still available to users from the other CSPs by leveraging the redundancy capability of multi-cloud.

– **Avoiding vendor lock-in**: Vendor lock-in is usually the result of proprietary technologies of a CSP that are incompatible with those of other CSPs. The migration of the cloud services from one CSP to the other CSP by multi-cloud reduces the dependence on any single vendor.

– **Best-of-breed selection**: By using information about cloud services from multiple CSPs, CSCs select the best cloud services among multiple CSPs that meet CSC's requirements in the multi-cloud.

– **Cost reduction**: Multi-cloud makes users pick and choose the most affordable cloud services from different CSPs at the lowest cost.

– **Reducing latency**: Multi-cloud makes users select and use cloud services that provide low latency to users. One of the ways to provide low latency in a multi-cloud is to use locational information of globally distributed clouds to a CSC to select the closest cloud services to the data and the users.

Although multi-cloud provides benefits to CSC compared with the use of a single CSP, there are several challenges to deploying multi-cloud as follows:

– **Complexity**: Multi-cloud deployment means interfacing with several different CSPs. It makes CSCs harder to manage cloud services running in multiple CSPs. Thus, simple and consistent management of cloud services is required.

– **Latency**: While multi-cloud can provide the benefit of reducing latency, the latency can be increased if cloud services need to frequently interact with one another and the cloud services are not properly selected. Multi-cloud needs to provide a way to minimize this kind of latency.

– **Performance**: It is difficult to balance loads across cloud services of geographically distributed clouds to guarantee the performance reliability required by users.

– **Cost overhead**: Although the multi-cloud approach is considered to be cost-saving for CSCs, it adds complexity to the cost estimation of cloud services, and users can suffer from large expenses of using cloud services due to poor multi-cloud management.

– **Complex monitoring**: Monitoring is also difficult in a multi-cloud environment so integrated and unified monitoring for cloud services from different CSPs needs to be provided. Moreover, additional monitoring metrics specific to multi-cloud are required especially in case of tight interworking of cloud services.

6.2 Introduction to multi-cloud management

In a multi-cloud, it is necessary to select and use the appropriate cloud services from multiple CSPs. To help a CSC for multi-cloud, multi-cloud management provides capabilities to compose, configure, control and monitor different cloud services on multiple CSPs for management efficiency. Examples of management efficiency are single point management, common usage of different cloud services, unified control of cloud services and so on. Multi-cloud management also provides the capability for coordination to interact among cloud services in a group.

A CSC easily uses cloud services in the public cloud provided by different CSPs with the help of multi-cloud management, where cloud services are managed in a form of a composed cloud service by a cloud service partner (CSN).

Multi-cloud management manages composed cloud services in a unified way, which means all cloud services belonging to the group are managed as a group rather than individually. Figure 6-2 shows an overview of the multi-cloud management.

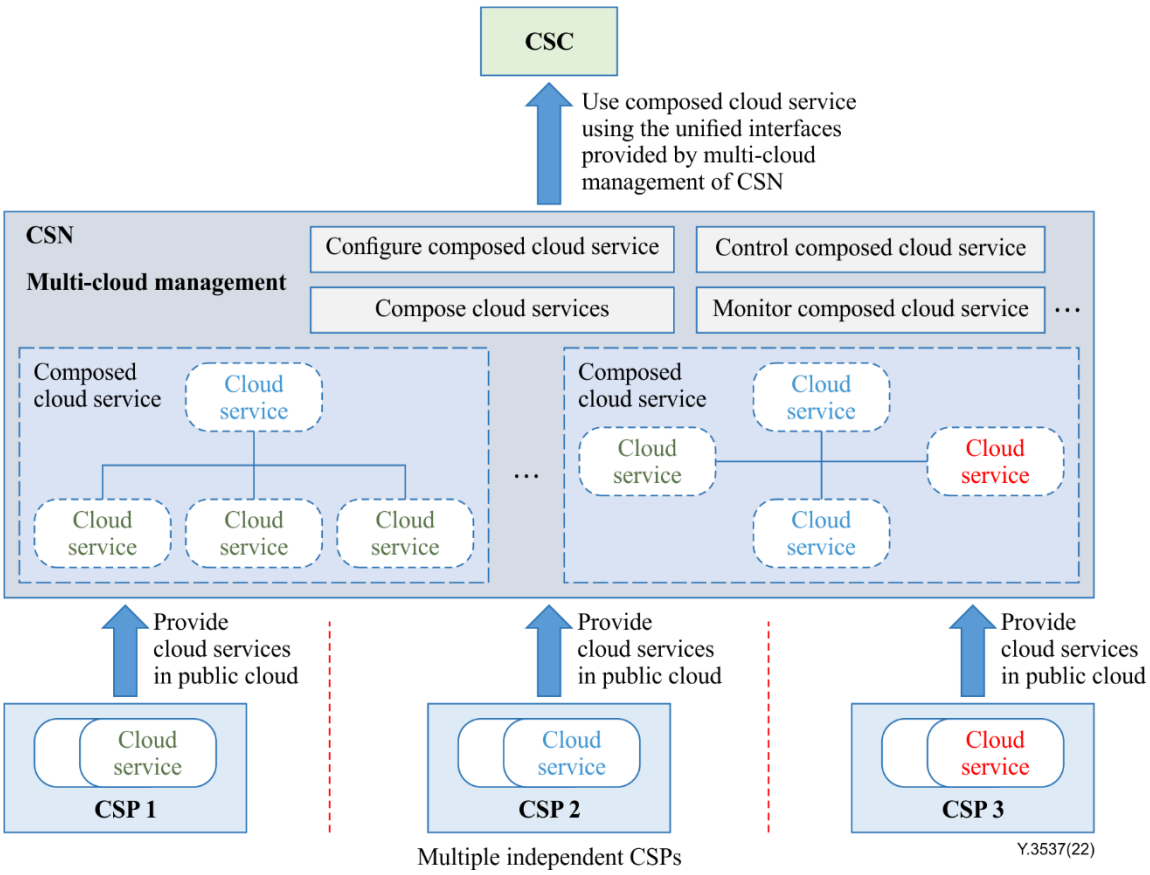


Figure 6-2 – Overview of multi-cloud management

A CSC requests cloud services in a public cloud using unified interfaces provided by the multi-cloud management. Multi-cloud management finds available cloud services in different and independent CSPs that meet the CSC's requirements and configures them into a composed cloud service. Now, the CSC can use the composed cloud service. During usage of the composed cloud service, the CSC controls and monitors them through the unified interfaces provided by the multi-cloud management.

NOTE 1 – Examples of cloud services come under the cloud service categories such as IaaS, PaaS and SaaS.

NOTE 2 – Composed cloud service is a group of cloud services which is a unit for configuring, controlling and monitoring cloud services as a whole in a multi-cloud. Additional configurations that can be applied to composed cloud services are load balancing, overlay networking, high availability, storage sharing and so on.

7 Sub-role and activities of cloud service partners for multi-cloud management

7.1 CSN:multi-cloud manager and cloud computing activities

A multi-cloud manager is a sub-role of a cloud service partner (CSN) that is responsible for providing the capabilities of multi-cloud management between a CSC and multiple CSPs. The CSN:multi-cloud manager is engaged in support of the CSC that wants to use cloud services from multiple independent CSPs as a group.

The CSN:multi-cloud manager's cloud computing activities include:

– Discover cloud services (clause 7.1.1);
– Perform intermediation and aggregation (clause 7.1.2);
– Manage connectivity across cloud services (clause 7.1.3);
– Coordinate identity and security credentials (clause 7.1.4);
– Coordinate customer requests (clause 7.1.5);

– Monitor and report cloud services (clause 7.1.6);
– Manage governance policies (clause 7.1.7).

The cloud computing activities which relate to CSN:multi-cloud manager are shown in Figure 7-1.

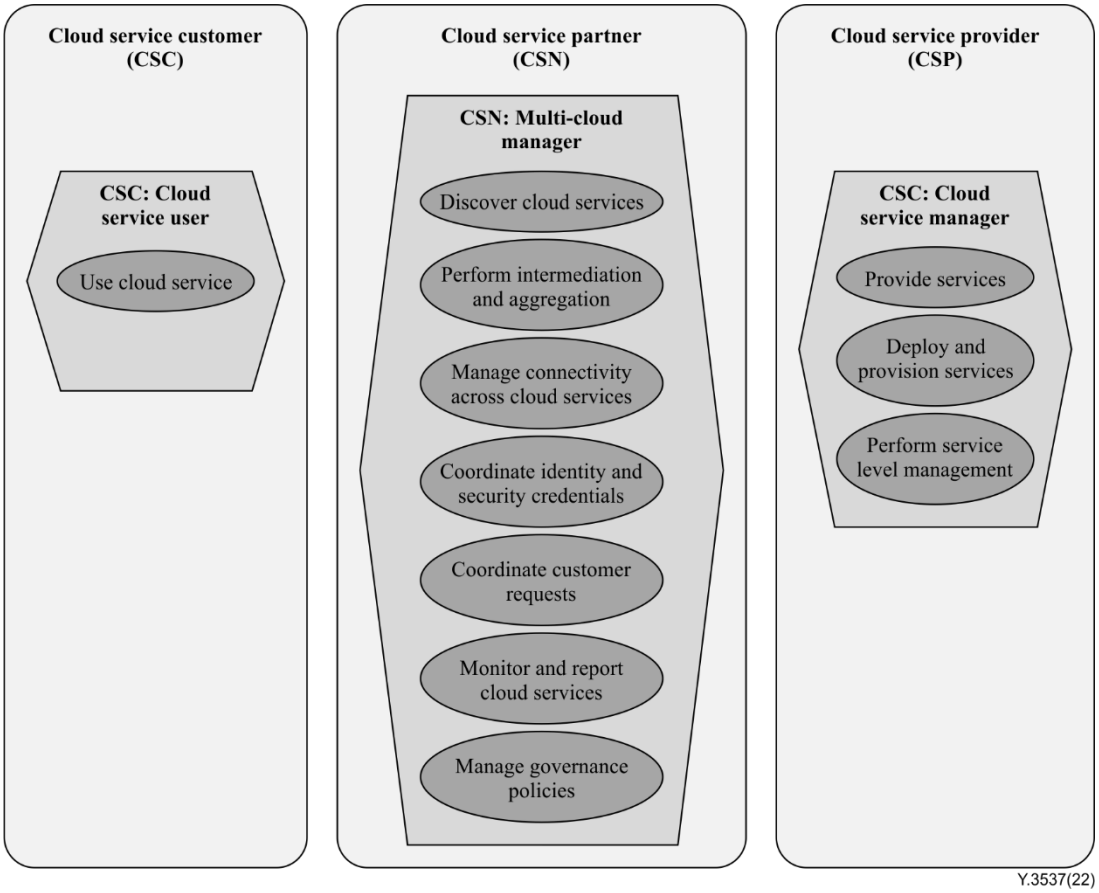


Figure 7-1 – Cloud computing activities of CSN:multi-cloud manager

7.1.1 Discover cloud services

The discover cloud services activity involves searching and discovering the available cloud services in the public cloud of CSPs.

This activity typically involves:

– finding available cloud services in the public cloud from the service catalogues provided by CSPs;
– selecting, provisioning and configuring the best-matched cloud services to the CSC requests from available cloud services.

7.1.2 Perform intermediation and aggregation

The perform intermediation and aggregation activity involves composing cloud services provided by multiple CSPs in particular ways.

This activity involves:

– intermediating cloud services by providing unified interfaces so that a CSC uses cloud services provided by different CSPs;
– aggregating cloud services provided by multiple CSPs by composition.

7.1.3 Manage connectivity across cloud services

The manage connectivity across cloud services activity involves the interoperability management in composed cloud service by providing network connectivity and data connectivity. It sets up the virtual network connections and related capabilities for the composed cloud service, which can include the establishment of various network facilities, such as an overlay network or a virtual private network (VPN). It also creates and provides virtual storage for data connectivity, which are shared in the composed cloud service.

This activity involves:

– provisioning virtual network capabilities among cloud services, such as VPN, tunnelling or load balancing;

– operating, maintaining and provisioning the cloud adaptive network among cloud services;

– provisioning virtual storage capabilities among cloud services;

– operating, maintaining and provisioning cloud adaptive storage among cloud services.

7.1.4 Coordinate identity and security credentials

The coordinate identity and security credentials activity involves the coordination of identity and security credentials between a CSC and all CSPs.

This activity involves:

– managing identity for the invocation and access of the cloud services in the public cloud through the associated authentication and authorization;

– provisioning and managing user credentials to enable the multiple CSPs to authenticate the user and grant access to the cloud services.

7.1.5 Coordinate customer requests

The coordinate customer requests activity involves handling requests from a CSC and ensuring the agreed SLA for a group of cloud services.

This activity involves:

– handling requests from a CSC while using a composed cloud service. The CSN:multi-cloud manager provides a variety of means to communicate with the CSC, such as web portals or user interfaces (RESTful application programming interface (API), gRPC API, etc.);

– monitoring and managing composed cloud service to ensure that all cloud services in the composed cloud service meet the agreed SLAs.

7.1.6 Monitor and report cloud services

The monitor and report cloud services activity involves monitoring composed cloud services and reporting their behaviours in the aggregated forms.

This activity involves:

– monitoring the status of the composed cloud service by getting the data of metrics for each cloud service from the multiple CSPs, or by collecting them in alternative ways, such as the installation of agents;

– providing various reports to a CSC. The reports include usage reports, audit reports, problem reports, performance reports, and so on provided by each CSP.

7.1.7 Manage governance policies

The manage governance policies activity involves managing the various policies to control the provisioning and use of cloud services and the related data.

This activity involves:

– providing and managing the governance policies during provisioning and using composed cloud service, with consideration of cost management, security and compliance, inventory, utilization, and automation / self-healing;
– managing the procedures for governing data in multi-cloud for data collection, ingestion, storage, cataloguing, deployment, backup and periodic removal.

7.2 Logical components of CSN:multi-cloud manager

The logical components of CSN:multi-cloud manager consist of service discovery, access management, service management, connectivity management, monitoring and reporting and policy management as shown in Figure 7-2.

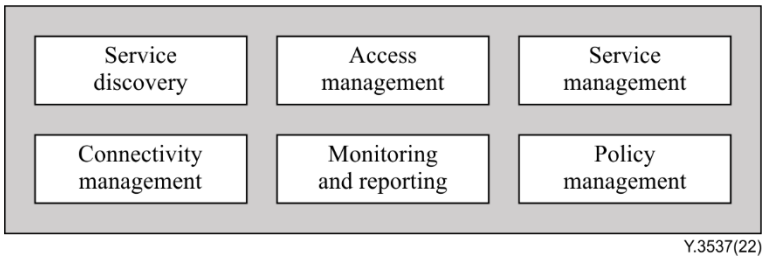


Figure 7-2 – Logical components of CSN:multi-cloud manager

NOTE – Relationship between the logical components and the cloud computing activities of CSN:multi-cloud manager is described in Appendix II.

7.2.1 Service discovery

A service discovery logical component searches the available cloud services in the public cloud from service catalogues provided by the available CSPs. After discovering the best-matched cloud services to the CSC's requirements among available cloud services, this logical component provisions them to the corresponded CSPs. This logical component can evaluate the available cloud services before provisioning them to provide optimal cloud services for the CSC's requirements.

7.2.2 Access management

An access management logical component coordinates the identities and security credentials between a CSC and CSPs to help the CSC access each CSP so that the CSC uses each cloud service in the composed cloud service. This logical component interacts with each CSP separately for the identities and credentials needed to access CSPs and use the composed cloud service, on behalf of the CSC. Also, this logical component manages the credentials for the CSPs to guarantee the CSC as the authorized user, while using the composed cloud service.

7.2.3 Service management

A service management logical component composes, configures and controls the provisioned cloud services according to the CSC's request through interfaces such as RESTful API, gRPC API and so on, ensuring that each cloud service in the composed cloud service meets the agreed SLA. This logical component delivers the control requests for each cloud service in the composed cloud service to the corresponded CSP, to start, stop, suspend, resume, reboot and/or terminate the composed cloud service. Moreover, this logical component provides unified interfaces so that the CSC can use the composed cloud service.

7.2.4 Connectivity management

A connectivity management logical component sets up the network connection and the related capabilities across the cloud services to provide the network connectivity to the composed cloud service. This logical component provides and manages the network capabilities such as the VPN, tunnelling, load balancing and so on to the composed cloud service. Moreover, this logical component

provides the data connectivity for the data sharing in the composed cloud service by federating the cloud storage provided by each CSP.

7.2.5 Monitoring and reporting

Monitoring and reporting logical component monitors the composed cloud service in the aggregated forms by collecting the metric data from CSPs or agents running in each cloud service. This logical component also collects the reports such as usage reports, audit reports, problem reports and so on from CSPs, and provides them to the CSC in the aggregated form.

7.2.6 Policy management

A policy management logical component provides and manages the various policies for cost management, optimized utilization, and autonomous management of cloud services in composed cloud services during provisioning and using a composed cloud service. This logical component especially checks the utilization of the composed cloud service by interacting with the monitoring and reporting logical components to adjust various policies such as auto-scaling in/out, load-balancing, high availability and so on to the composed cloud service. This logical component also manages the procedure to collect, store, backup and remove various data such as the monitoring metric data, log data and so on.

7.3 Interactions of CSN:multi-cloud manager

The CSN:multi-cloud manager involves managing the cloud services on multiple CSPs in order to support a CSC that uses a composed cloud service with an interoperability aspect.

The CSN:multi-cloud manager gets the credentials for the CSPs from the CSC and verifies them for each CSP, as shown in Figure 7-3. The CSN:multi-cloud manager delivers a set of the service catalogues provided by each CSP to the CSC. After checking the delivered service catalogues, the CSC requests to provision multiple available cloud services to be used as a group. The CSN:multi-cloud manager requests the cloud services to each CSP according to the CSC's request. After all the requested cloud services are successfully created in each CSP, the CSN:multi-cloud manager composes the created cloud services and provides it to the CSC with the access information. If necessary, the CSC can add the interconnectivity capability for the composed cloud service through the CSN:multi-cloud manager such as setting up the network connectivity and/or the data connectivity for the composed cloud service on behalf of the CSC. Now, the CSC can access the composed cloud service and the CSN:multi-cloud manager manages and monitors the composed cloud service for the CSC.

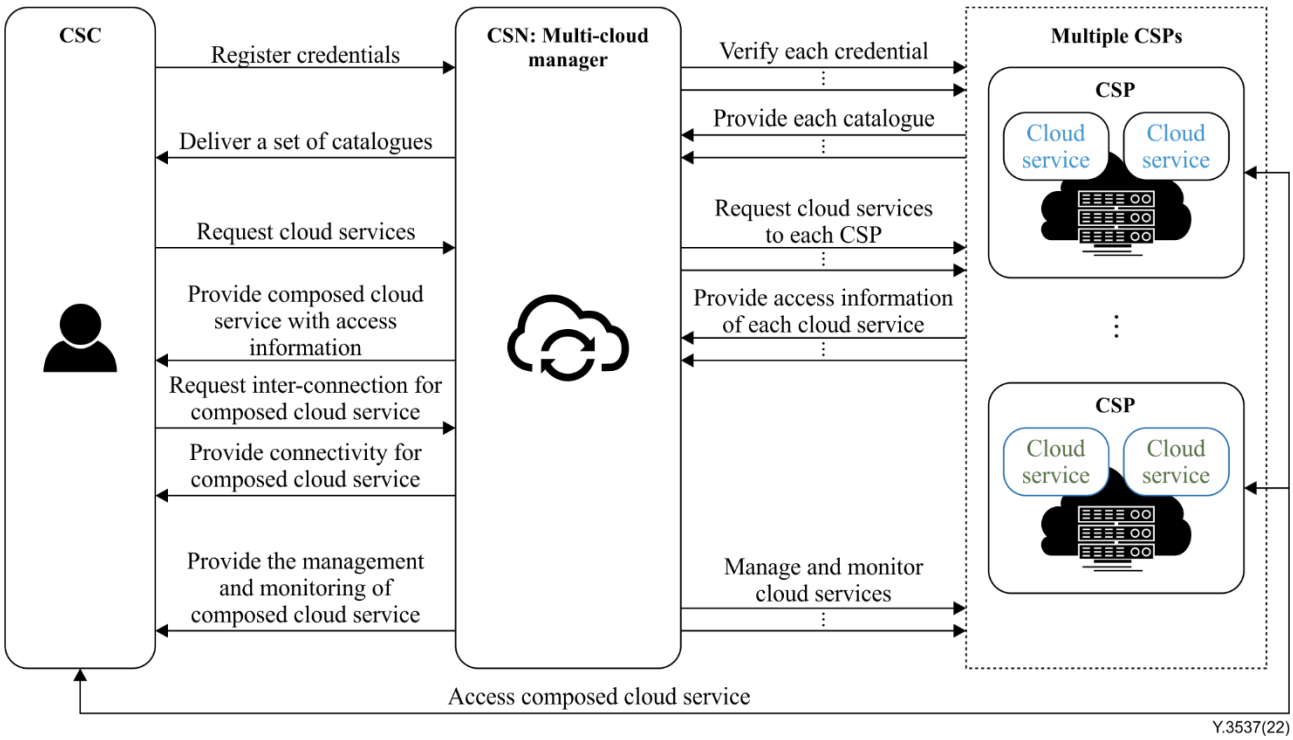


Figure 7-3 – Interactions of CSN:multi-cloud manager with CSC

8 Functional requirements of CSN:multi-cloud manager

8.1 Functional requirements for service discovery

– **Providing information on the available cloud services**: It is required that CSN:multi-cloud manager provides available cloud services and their specifications.

NOTE 1 – The specification of cloud service is the information for describing the features or properties of cloud service, such as the number of virtual central processing units (vCPUs), memory size, and disk type and size.

NOTE 2 – The specifications of available cloud services are collected from the CSP's cloud service catalogues. Available cloud services and their specifications are periodically or irregularly checked to update the outdated information to avoid providing unavailable cloud services and inaccurate information to the CSCs. The metrics included in the collected specification are converted to the metrics used by the CSN:multi-cloud manager, if the collected specification uses different metrics. An example of the converted metrics is gigabytes which are converted to gibibytes (GiB).

– **Evaluating performance for cloud services**: It is required that CSN:multi-cloud manager provides performance evaluation of cloud services from multiple CSPs to benchmark the cloud services.

NOTE 3 – Performance evaluation is performed periodically or irregularly on each type of cloud service for performance metrics. The performance of cloud service is evaluated by running the cloud service with various patterns of workload.

NOTE 4 – Examples of performance metrics for cloud services are computing speed, memory read and write speed, file input/output (I/O) speed, database transaction speed, and network latency among cloud services.

– **Discovering best matched cloud services**: It is required that CSN:multi-cloud manager provides discovery of best matched cloud services in order to compose cloud services according to the CSC's requirements.

NOTE 5 – Examples of CSC's requirements for a composed cloud service are the type and the number of cloud services, specifications, computing performance, response time, price, location, and network latency among cloud services.

NOTE 6 – Matching cloud services to the CSC's requirements is performed by filtering and prioritizing the list of cloud services along with static information such as specifications and dynamic information based on performance evaluations. Multiple requirements are combined by using a weighted sum for filtering and prioritizing the list of cloud services. Matched cloud services are used to provide composed cloud service to CSC.

– **Estimating cost for composed cloud service**: It is recommended that CSN:multi-cloud manager provides an estimated cost to the CSC before provisioning composed cloud service.

– **Delivering provisioning requests for cloud services**: It is required that CSN:multi-cloud manager provides delivery of provisioning requests for cloud services from the CSC to multiple CSPs.

8.2 Functional requirements for access management

– **Managing access information for CSP**: It is required that CSN:multi-cloud manager provides management of access information for CSP.

NOTE 1 – Access information for CSP is used to interact with CSP. An example of access information for CSP is a credential which consists of an ID, password, and access key or token needed to use the CSP's open interfaces.

NOTE 2 – The sensitive data of access information for CSP is stored in a secure repository or memory maintained by the CSN:multi-cloud manager.

– **Authorizing access information for CSP**: It is required that a CSN:multi-cloud manager provides the authorization for registered access information for CSPs only to the authorized CSCs.

– **Providing access information for composed cloud service**: It is required that CSN:multi-cloud manager provides access information for composed cloud service only to an authorized CSC.

NOTE 3 – Examples of access information are IP addresses of composed cloud service, credentials to authenticate and authorize CSC, such as private keys for each secure shell and account name.

NOTE 4 – Access information of composed cloud service is a set of access information of cloud services in a composed cloud service. Also, access information provides an entry point to access any cloud service in a composed cloud service.

– **Updating access information for composed cloud service**: It is required that CSN:multi-cloud manager provides an update of access information in case of changes in a composed cloud service.

NOTE 5 – A set of access information is updated if any cloud service in the composed cloud services is changed, Also, if a cloud service in the composed cloud service that acts as an entry point is terminated, the existing access information is updated to make the composed cloud service accessible.

8.3 Functional requirements for service management

– **Providing unified interfaces to CSC**: It is required that CSN:multi-cloud manager provides unified interfaces for a CSC to use a composed cloud service commonly.

NOTE 1 – Each CSP provides different interfaces to CSC for using its own cloud services. Unified interfaces help the CSC to use cloud services from different CSPs in the same way.

NOTE 2 – An example to unify the different interfaces of CSPs is to register interface drivers of each CSP to a CSN:multi-cloud manager. The interface driver converts the unified interfaces to the open interfaces of each CSP for CSC to use the composed cloud service in the same way.

– **Composing cloud services**: It is required that CSN:multi-cloud manager provides a composition of cloud services from multiple CSPs to manage cloud services simultaneously as a group.

– **Configuring composed cloud service**: It is required that CSN:multi-cloud manager provides the configuration of a composed cloud service.

NOTE 3 – Configurations are applied to composed cloud services, such as overlay network, subnetwork, VPN, load-balancer and shared storage.

NOTE 4 – Configurations of composed cloud services are stored, removed, or changed when needed.

– **Adding new cloud services to the composed cloud service**: It is required that CSN:multi-cloud manager provides adding a new cloud service to a composed cloud service.

– **Removing existing cloud services from a composed cloud service**: It is required that CSN:multi-cloud manager provides removing an existing cloud service from a composed cloud service.

– **Applying existing configuration to new cloud services**: It is required that CSN:multi-cloud manager provides applying the configurations used in existing composed cloud service to new cloud services.

– **Controlling composed cloud service**: It is required that CSN:multi-cloud manager provides the control of a composed cloud service as requested by CSC.

NOTE 5 – The control request of a composed cloud service is delivered to a CSP to the control cloud service. The example of cloud service control includes an operation for the whole lifecycle of a cloud service such as create, suspend, resume, reboot and terminate.

– **Checking the status of the composed cloud service**: It is required that CSN:multi-cloud manager provides status checking for a composed cloud service.

NOTE 6 – The examples of status for a composed cloud service are running, suspending, suspended, rebooting, terminating and terminated.

8.4 Functional requirements for connectivity management

– **Providing virtual network connections**: It is required that CSN:multi-cloud manager provides virtual network connections for cloud services in a composed cloud service.

NOTE 1 – Examples of virtual network connections are overlay networks, VPN, tunnelling-based networks, etc.

– **Collecting network information**: It is required that CSN:multi-cloud manager provides a collection of network information for each cloud service in a composed cloud service to set up a virtual network connection.

NOTE 2 – The examples of network information include the endpoint of each cloud service such as IP/port, network configuration, etc.

– **Updating virtual network connections dynamically**: It is required that CSN:multi-cloud manager provides dynamic updates of virtual network connections to maintain the connectivity for cloud services in a composed cloud service, even when network information of cloud service is changed.

– **Providing virtual network connection information**: It is recommended that CSN:multi-cloud manager provides information for virtual network connections to the CSC to check the status of virtual network connections as well as to create new virtual network connections.

NOTE 3 – The information for the virtual network connections includes the private network configuration for a composed cloud service.

– **Collecting cloud storage information**: It is required that CSN:multi-cloud manager provides collected cloud storage information from CSPs for a composed cloud service.

– **Creating shared virtual volume for cloud service**: It is required that CSN:multi-cloud manager provides creation of virtual volume shared for composed cloud service by federating cloud storage provided by each CSP.

– **Providing mounting of shared virtual volume**: It is required that CSN:multi-cloud manager provides mounting of shared virtual volume to each cloud service in a composed cloud service.

NOTE 4 – A method to mount the shared storage volume is to install a device driver in each cloud service in the composed cloud service.

– **Providing stability for shared virtual volume**: It is recommended that CSN:multi-cloud manager provides stable shared virtual volume to CSC.

NOTE 5- The ways to provide stable shared virtual volume include auto-scaling, high availability and disaster recovery.

NOTE 6 – Auto-scaling, high availability and disaster recovery for shared virtual volume are provided by the support of CSPs.

8.5 Functional requirements for monitoring and reporting

– **Monitoring composed cloud service**: It is required that CSN:multi-cloud manager provides monitoring composed cloud service to the CSC.

NOTE 1 – Monitoring of composed cloud service utilizes the status of each cloud service and the measured network performance among cloud services.

– **Monitoring cloud service**: It is required that CSN:multi-cloud manager provides monitoring cloud services from different CSPs, which are used in a composed cloud service to the CSC.

NOTE 2 – Monitoring data is collected from CSPs or from agents that are installed in each cloud service.

– **Storing monitoring data**: It is recommended that CSN:multi-cloud manager provides storing monitoring data in terms of composed cloud service, which are delivered to the CSC.

NOTE 3 – Monitoring data is stored in a storage maintained by CSN:multi-cloud manager.

– **Providing reports**: It is recommended that CSN:multi-cloud manager provides reports to the CSC based on the monitoring data.

NOTE 4 – Examples of reports are usage reports, audit reports, problem reports, performance reports, etc.

8.6 Functional requirements for policy management

– **Providing management policies to CSC**: It is required that CSN:multi-cloud manager provides management policies to the CSC to manage composed cloud service autonomously.

NOTE 1 – A management policy is to autonomously control cloud services in a composed cloud service according to conditions such as a threshold of resource utilization rate or workload, and actions such as scaling-out of composed cloud service for stability and efficiency.

NOTE 2 – A management policy is registered or deregistered by the CSC's request.

– **Detecting matched conditions of management policy**: It is required that CSN:multi-cloud manager provides the detection of matched conditions for a composed cloud service according to the management policies.

– **Applying management policy proactively**: It is required that CSN:multi-cloud manager provides proactive management of composed cloud service according to the management policies

NOTE 3 – To prevent quality degradation of cloud services or waste of resources due to rapid changes in workload, CSN:multi-cloud manager proactively determines to add new cloud services or remove the existing cloud services in the composed cloud service, to modify the specifications of the cloud services, or to change the status of the cloud services such as suspending or resuming them according to the expected workloads and cost.

NOTE 4 – Proactive change of the status of the cloud services in the composed cloud service reduces the cost and increases resilience. For instance, several cloud services such as virtual machines in suspended status can be changed to the running status, if the workload increases fast enough to reach the resource limits. Resuming the suspended virtual machines is faster than creating and running new virtual machines. On the other hand, once the workload has been stabilized, the multi-cloud manager suspends the appropriate virtual machines to minimize the cost of the composed cloud service.

– **Logging events and actions by management policy**: It is required that CSN:multi-cloud manager provides logging of events and actions by management policies.

9 Security considerations

It is recommended that the security framework for cloud computing described in [b-ITU-T X.1601] be considered for the multi-cloud. [b-ITU-T X.1601] analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and meet security challenges.

It is recommended that the guidelines for the operational security of cloud computing described in [b-ITU-T X.1642] be considered for the multi-cloud. [b-ITU-T X.1642] clarifies the security responsibilities between the CSPs and CSCs and analyses the requirements and categories of security metrics of operational security for cloud computing.

Relevant security requirements in [b-ITU-T X.1631] need to be taken into consideration for the multi-cloud. [b-ITU-T X.1631] provides guidelines supporting the implementation of information security controls for CSCs and CSPs. Many guidelines aid the CSPs to assist the CSCs in implementing the controls and guide them to implement such controls. The selection of appropriate information security controls and the application of the implementation guidance provided depends on a risk assessment, as well as any legal, contractual, regulatory, or other cloud-sector-specific information security requirements.

Appendix I

Use cases of multi-cloud

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

Table I.1 – A general use case for a multi-cloud management

Title	A general use case for a multi-cloud management
Description	This general use case includes general procedures for managing composed cloud services for multi-cloud. This general use case consists of four phases (preparation, request, provisioning and management phases). (Preparation phase) A CSC prepares credentials for each CSP, where the CSC wants to use the cloud services, and registers them to the CSN:multi-cloud manager which manages the cloud services of the involved CSPs. The CSC checks the available cloud services from the catalogues of CSPs provided by the CSN:multi-cloud manager and registers information to the CSN:multi-cloud manager for requesting the cloud services. Now, for the CSC, the CSN:multi-cloud manager has all the information for delivering the requests to the CSPs to control the cloud services. (Request phase) When the CSC needs to deploy or execute applications in the cloud computing platform for business, the CSC analyses the requirements of the applications and determines the expected form of cloud services. For example, the CSC wants to use seven cloud services to provide virtual machines distributed world-wide. The CSC requests the CSN:multi-cloud manager to provide the composed cloud service. (Provisioning phase) The CSN:multi-cloud manager discovers the most appropriate cloud services and delivers the requests for creating the cloud services to each CSP with the registered credentials of the CSC. With replies from all CSPs, the CSN:multi-cloud manager composes the selected cloud services and stores the status of the composed cloud service. Also, the CSN:multi-cloud manager applies configurations to set up the overlay network and/or the shared storage for the composed cloud service, if necessary. Once all provisioning processes across CSPs are completed, the CSN:multi-cloud manager notifies the CSC. Finally, the CSC can deploy and run its applications for business on the composed cloud service. (Management phase) If the resources that the running applications on the composed cloud service use may not be enough, the CSC can extend the composed cloud service easily through the support of the CSN:multi-cloud manager. For example, the CSN:multi-cloud manager can auto-scale the composed cloud service by provisioning additional cloud services to the composed cloud service. Also, the CSN:multi-cloud manager continues monitoring the status of the composed cloud service and provides the collected monitoring data to the CSC.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager

Table I.1 – A general use case for a multi-cloud management

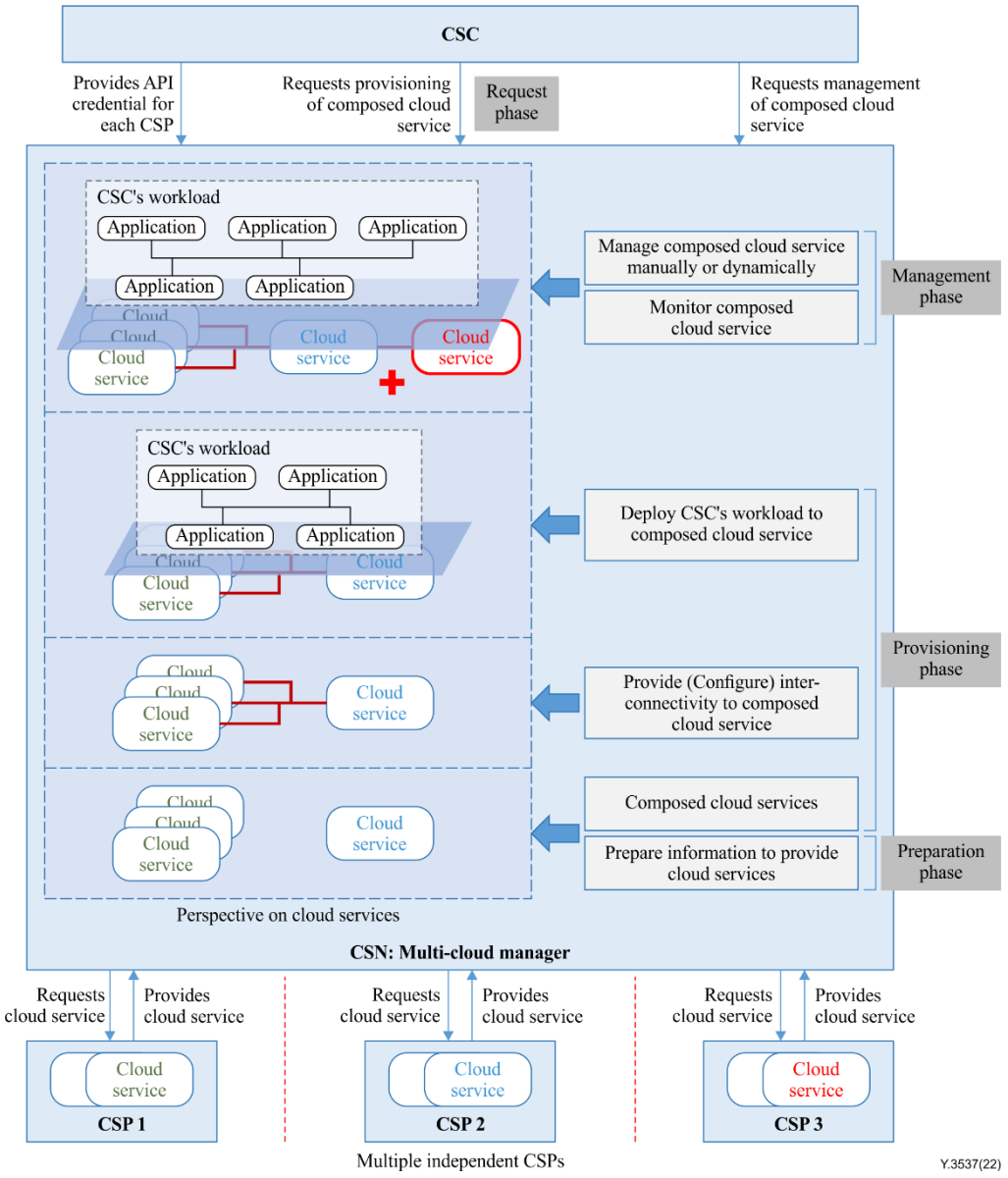
Figure	
Pre-conditions (optional)	CSC has credentials to get permission to use the cloud services of the CSPs. CSPs are independent of one another and communications among CSPs are not required.
Post-conditions (optional)	
Derived requirements	– Managing access information for CSP (see clause 8.2) – Authorizing access information for CSP (see clause 8.2) – Discovering best matched cloud services (see clause 8.1) – Delivering provisioning requests for cloud services (see clause 8.1) – Providing unified interfaces to CSC (see clause 8.3) – Composing cloud services (see clause 8.3) – Providing access information for composed cloud service (see clause 8.2) – Configuring composed cloud service (see clause 8.3) – Controlling composed cloud service (see clause 8.3)

Table I.1 – A general use case for a multi-cloud management

	– Adding new cloud services to the composed cloud service (see clause 8.3) – Removing existing cloud services from a composed cloud service (see clause 8.3) – Applying existing configuration to new cloud services (see clause 8.3) – Checking the status of the composed cloud service (see clause 8.3) – Monitoring composed cloud service (see clause 8.5)

Table I.2 – A use case for deploying global-scale computing infrastructure

Title	Deploying global-scale computing infrastructure.
Description	This use case depicts a scenario in which CSC cooperates with the CSN:multi-cloud manager to use the cloud services that cover the global areas in a simple way. In case the CSC tries to make a global business in a cloud computing environment, the CSC needs a global-scale computing infrastructure using cloud services in terms of virtual machines distributed all over the world. However, since any single CSP cannot provide all the required cloud services in terms of location, capacity, and type of cloud services, adoption of multi-cloud is a reasonable approach for a CSC. Nevertheless, it is hard for the CSC itself to communicate with each different CSP respectively because a CSC needs to understand and use different interfaces and procedures of each CSP for using its cloud services. Therefore, it is more efficient that a CSC cooperates with a CSN:multi-cloud manager that supports the single-point operation and management for cloud services from different CSPs. Detailed procedures for deploying the global-scale computing infrastructure are as follows. 1) A CSC sends requirements to a CSN:multi-cloud manager, such as the number of cloud services, specification, performance, OS image, location and so on, to set up cloud services covering the global areas required. For instance, the CSC may request 200 high performance virtual machines that are geographically close to the desired areas. To satisfy these requirements, the CSN:multi-cloud manager discovers and configures the most appropriate cloud services based on the information and evaluations of cloud services from multiple CSPs. 2) The CSN:multi-cloud manager provides the result of the selected cloud services to the CSC. If the CSC decides to use them, the CSC requests provisioning of the selected cloud services with the information of the related resources (e.g., virtual network resource, SSH key resource, and security group for virtual machines) to the CSN:multi-cloud manager. The CSN:multi-cloud manager maintains the information for the requested cloud services and the related resources so that the CSC and the CSN:multi-cloud manager can cooperate together while using the cloud services. 3) The CSN:multi-cloud manager delivers the requests for creating the cloud services with the related resources to each CSP, using credentials that the CSC already provided. After each CSP creates the requested cloud services with the related resources, the CSN:multi-cloud manager receives the result and the access information for the created cloud services from each CSP. 4) Once the CSN:multi-cloud manager verifies that all the requested cloud services are available from the involved CSPs, the CSN:multi-cloud manager composes the created cloud services as a group and proceeds with the configurations to set up the overlay network and/or the shared storage for the composed cloud service. The overlay network makes the cloud services hosted by different CSPs seamless, and the shared storage is used for sharing data together among the cloud services.

Table I.2 – A use case for deploying global-scale computing infrastructure

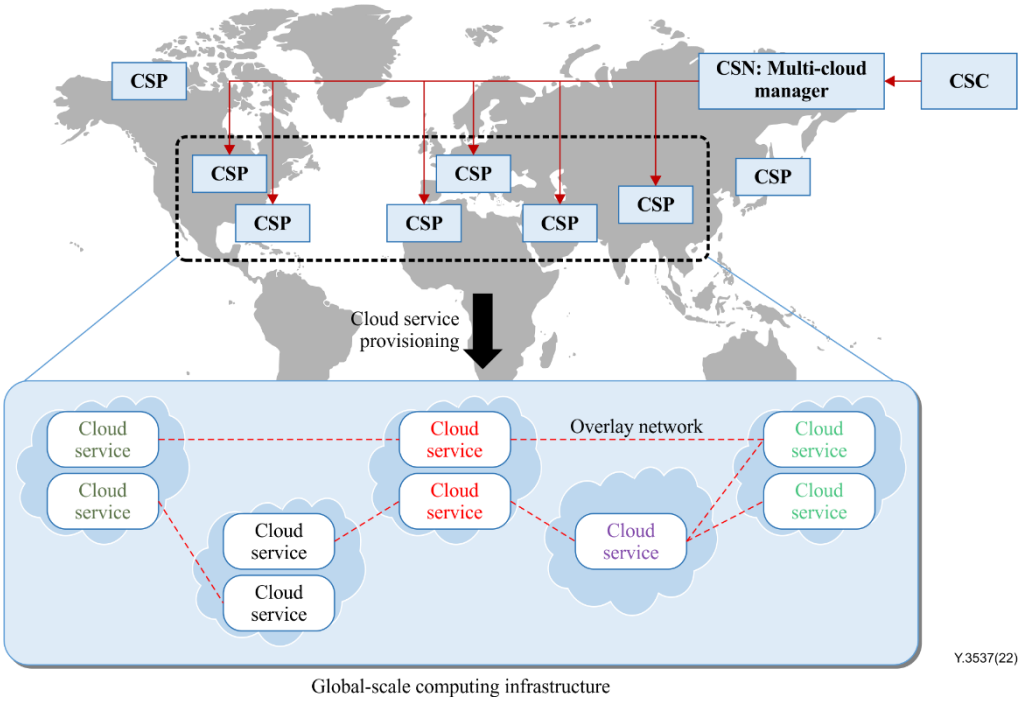
	5) After the provisioning for all CSPs is completed, the CSN:multi-cloud manager informs the CSC that the composed cloud service is ready along with the status and the access information. Finally, the CSC can deploy and run its own applications for the business in the composed cloud service distributed all over the world.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager
Figure	 Global-scale computing infrastructure
Pre-conditions (optional)	CSC has credentials to get permission to use the cloud services of CSPs. CSPs are independent and communications among CSPs are not required.
Post-conditions (optional)	
Derived requirements	– Providing information on the available cloud services (see clause 8.1) – Evaluating performance for cloud services (see clause 8.1) – Discovering best matched cloud services (see clause 8.1) – Authorizing access information for CSP (see clause 8.2) – Delivering provisioning requests for cloud services (see clause 8.1) – Providing unified interfaces to CSC (see clause 8.3) – Composing cloud services (see clause 8.3) – Configuring composed cloud service (see clause 8.3) – Providing access information for composed cloud service (see clause 8.2)

Table I.3 – A use case for control of composed cloud service

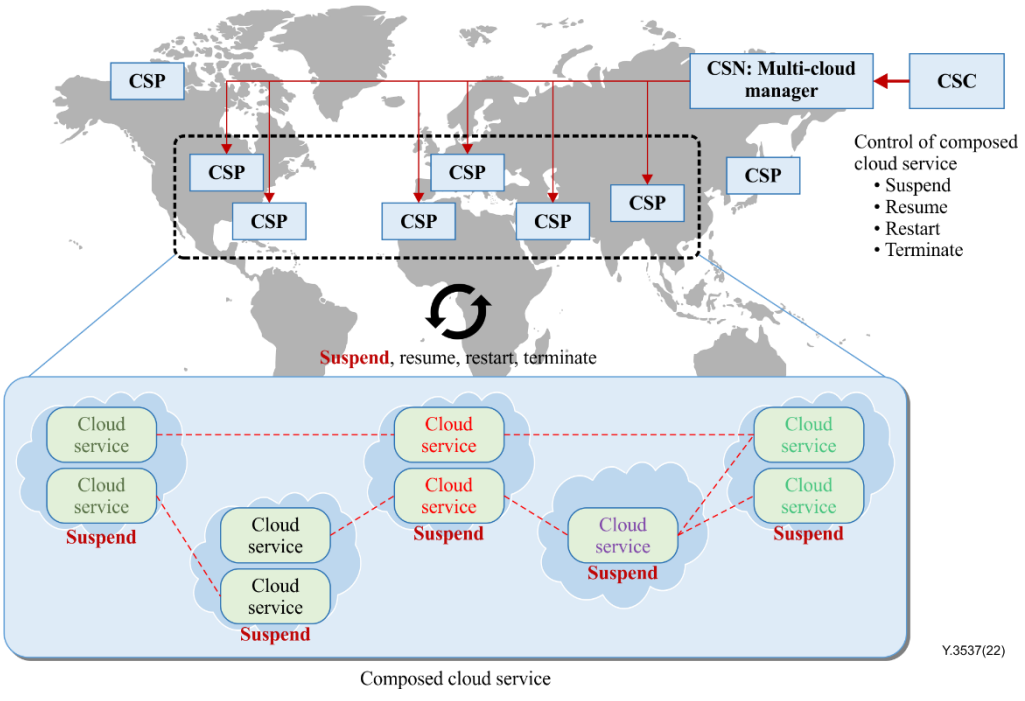
Title	Controlling composed cloud service
Description	It is difficult and inefficient for a CSC to interface with each CSP respectively for controlling composed cloud service provided by multiple CSPs, because each CSP provides different APIs, controlling procedures and status of a cloud service. For instance, some CSPs provide the functionality to restart cloud services even with a different name of APIs, while others do not. Therefore, CSN:multi-cloud manager needs to provide the capabilities to easily control composed cloud service and manage the status of a composed cloud service, on behalf of a CSC. The detailed procedure for controlling and managing composed cloud service is as follows. 1) A CSC sends a control request for the composed cloud service to a CSN:multi-cloud manager using the unified interfaces, such as restarting or initializing all the cloud services. 2) The CSN:multi-cloud manager converts this control request into multiple operation forms and procedures that are acceptable to each CSP which provides some cloud services in the composed cloud service. Then, the CSN:multi-cloud manager delivers each converted control request to the corresponded CSP. 3) The CSN:multi-cloud manager continues checking the status of the cloud services from all the involved CSPs for the status of the composed cloud service. 4) When the CSN:multi-cloud manager verifies that all the cloud services in the composed cloud service are in the targeted status, the CSN:multi-cloud manager notifies the result of the control request to the CSC. Also, if the CSN:multi-cloud manager finds any changes in the composed cloud service such as changes in the entry point, the CSN:multi-cloud manager updates the related information and notifies the CSC.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager
Figure	

Table I.3 – A use case for control of composed cloud service

Pre-conditions (optional)	CSC submits the credentials for CSPs to the CSN:multi-cloud manager in order to get permission to access the cloud services provided by each CSP. CSN:multi-cloud manager composes the created cloud services and delivers them to the CSC.
Post-conditions (optional)	
Derived requirements	– Providing access information for composed cloud service (see clause 8.2) – Providing unified interfaces to CSC (see clause 8.3) – Controlling composed cloud service (see clause 8.3) – Checking the status of the composed cloud service (see clause 8.3) – Updating access information for composed cloud service (see clause 8.2)

Table I.4 – A use case for multi-cloud monitoring

Title	Multi-cloud monitoring
Description	This use case describes a scenario that CSC monitors the composed cloud service through a CSN:multi-cloud manager, where cloud services are provided by two or more CSPs. A CSC can create and deploy a new composed cloud service through a CSN:multi-cloud manager. At this time, the CSC may request the installation of agents to all the created cloud services to the CSN:multi-cloud manager for monitoring the required metrics related to the interoperation among the cloud services such as network connectivity and performance, because each CSP which provides its cloud services has no information for the cloud services provided by other CSPs. On the other hand, this installation of agents can be executed automatically during the creation of each cloud service. After the creation of the composed cloud service, the CSN:multi-cloud manager gathers and stores the monitoring data from the installed agents as well as the CSPs, and provides them to the CSC. While the CSN:multi-cloud manager monitors the metrics for each cloud service itself to ensure that each CSP meets the agreed SLAs, it can monitor metrics related to the interoperation across the cloud services from the installed agents in order to ensure that the SLA of the composed cloud service can be met. By using the collected and stored monitoring data, the CSN:multi-cloud manager provides various reports, such as usage, audit, problem, performance, etc, to the CSC.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager

Table I.4 – A use case for multi-cloud monitoring

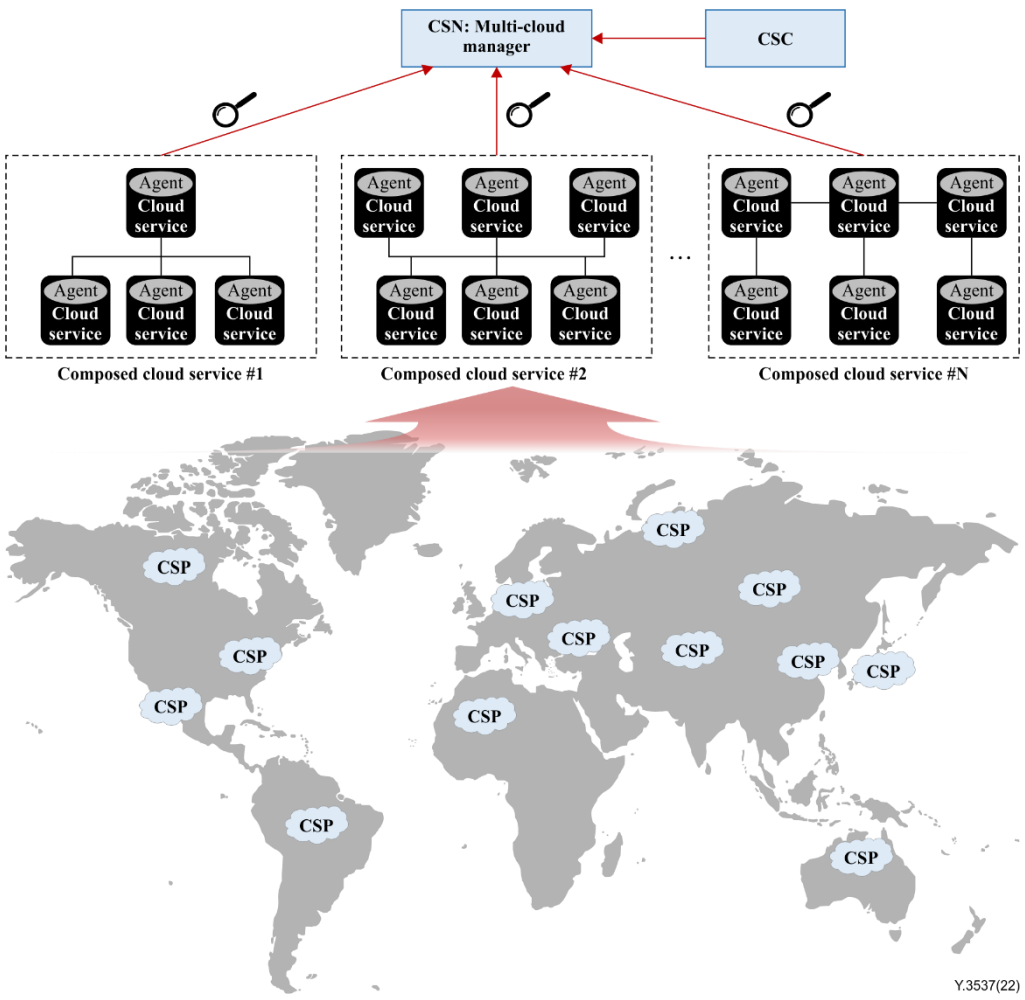
Figure	
Pre-conditions (optional)	CSC submits the credentials for CSPs to the CSN:multi-cloud manager in order to get permission to access the cloud services provided by each CSP. CSN:multi-cloud manager installs the monitoring agent in each cloud service during the creation of the cloud service by the request of the CSC or automatically.
Post-conditions (optional)	
Derived requirements	– Composing cloud services (see clause 8.3) – Configuring composed cloud service (see clause 8.3) – Monitoring composed cloud service (see clause 8.5) – Monitoring cloud services (see clause 8.5) – Storing monitoring data (see clause 8.5) – Providing reports (see clause 8.5)

Table I.5 – A use case for network connectivity for composed cloud service

Title	Providing network connectivity for composed cloud service
Description	This use case describes a scenario in which CSN:multi-cloud manager provides the capability of the network connectivity by setting up the network connection among composed cloud services by the CSC's request, after the CSN:multi-cloud manager composes the cloud services for multi-cloud. A CSC is provided with a composed cloud service created by the CSC's request through a CSN:multi-cloud manager. At this time, each cloud service in the composed cloud service uses different networks, because each cloud service is provided by different CSPs. The CSC requests the network connection among cloud services to the CSN:multi-cloud manager to use all cloud services in the composed cloud service as if they are provided by a single CSP. The CSN:multi-cloud manager gets the network information of each cloud service in the composed cloud service from each CSP, and sets up the virtual network connection among the cloud services for interoperability. The virtual network connection may be configured by various methods, such as an overlay network, VPN, tunnelling-based network, etc, which are provided by the CSN:multi-cloud manager. The configured virtual network connections among cloud services are maintained and managed only by the CSN:multi-cloud manager because these virtual network connections cannot be recognized by each CSP. If necessary, the CSN:multi-cloud manager can provide additional capabilities over the configured virtual network connections for the CSC, such as load balancing, high availability, replication and so on. Also, the CSN:multi-cloud manager provides the information for the supported virtual network connections to the CSC in order to check the current status of the virtual network connection or to create a new virtual network connection. Now, the CSC can use the composed cloud service with a network connectivity among the cloud services, which means that all the cloud services in the composed cloud service can be used as if they are provided by a single CSP.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager

Table I.5 – A use case for network connectivity for composed cloud service

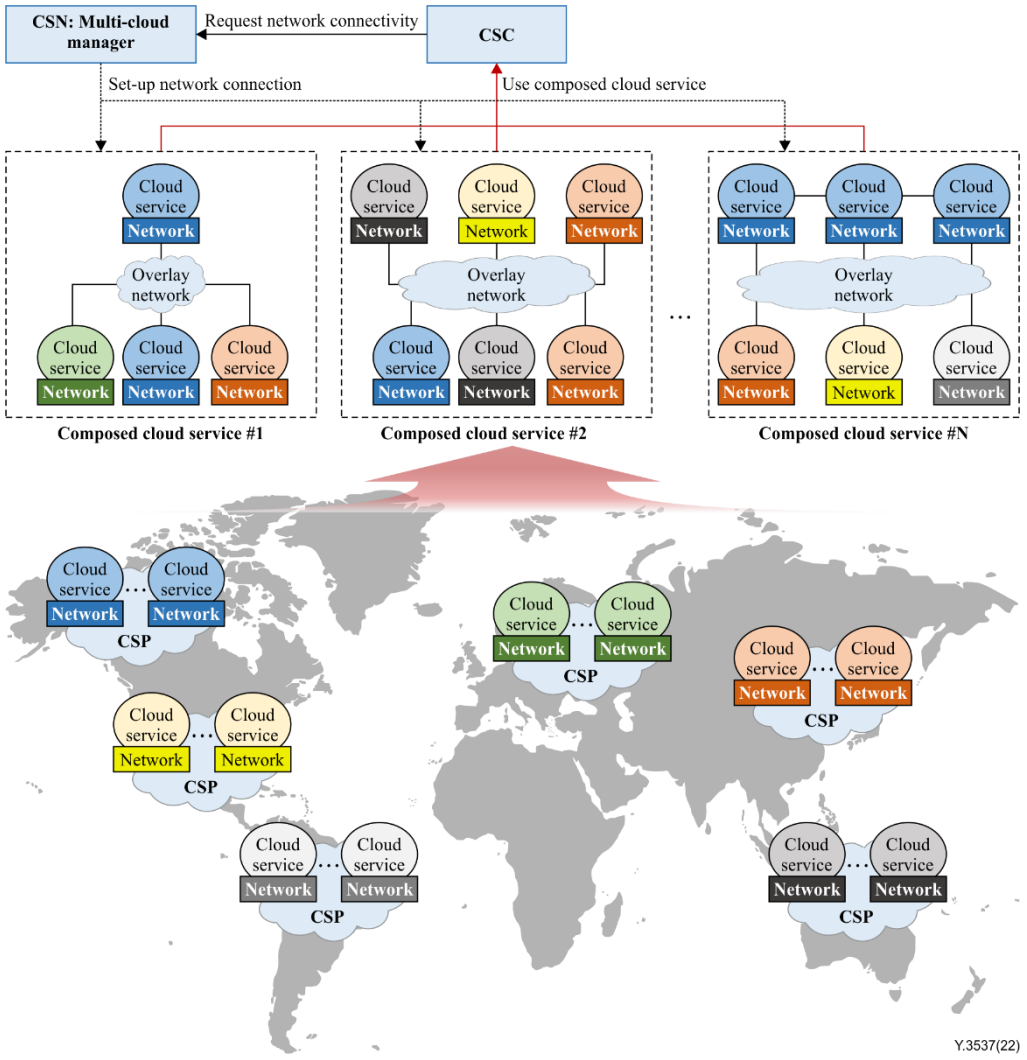
Figure	
Pre-conditions (optional)	CSC provides the credentials for CSPs to CSN:multi-cloud manager in order to get permission to access the cloud services provided by each CSP. CSN:multi-cloud manager composes the cloud services best matched to the CSC's requirements and delivers them to the CSC.
Post-conditions (optional)	
Derived requirements	– Composing cloud services (see clause 8.3) – Configuring composed cloud service (see clause 8.3) – Providing virtual network connections (see clause 8.4) – Collecting network information (see clause 8.4) – Updating virtual network connections dynamically (see clause 8.4) – Providing virtual network connection information (see clause 8.4)

Table I.6 – A use case for data connectivity for composed cloud service

Title	Providing data connectivity for composed cloud service
Description	This use case describes a scenario in which a CSN:multi-cloud manager provides the capability of the data connectivity by creating a single virtual volume shared among the composed cloud service, after the CSN:multi-cloud manager composes the cloud services provided by multiple CSPs. A CSC is provided with a composed cloud service created by the CSC's request through a CSN:multi-cloud manager. At this time, the cloud services in the composed cloud service cannot share the data with one another because each cloud service uses its own storage provided by the corresponding CSP. The CSC requests the data connectivity among the composed cloud service to the CSN:multi-cloud manager in order to share and access the data among all the cloud services in the composed cloud service. The CSN:multi-cloud manager gets the cloud storage information used by each cloud service from the corresponding CSP and creates the single virtual volume shared among the composed cloud service by connecting the cloud storage. This single virtual volume may have the capacity just enough for a composed cloud service to use, based on the connected cloud storage resources. Also, this single virtual volume may be provided in the form of a block device, an object device or a disk. The CSN:multi-cloud manager may install the device driver for the single virtual volume to each cloud service in the composed cloud service so that each cloud service can mount the shared virtual volume. If necessary, the CSN:multi-cloud manager may provide additional capabilities over the shared virtual volume for the CSC, such as auto-scaling, high availability, disaster recovery and so on, with the help of the capabilities of each CSP. Now, the CSC can use the composed cloud service with data connectivity among the cloud services, which means that all the cloud services in the composed cloud service can share and access the data as if they are provided by a single CSP.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager

Table I.6 – A use case for data connectivity for composed cloud service

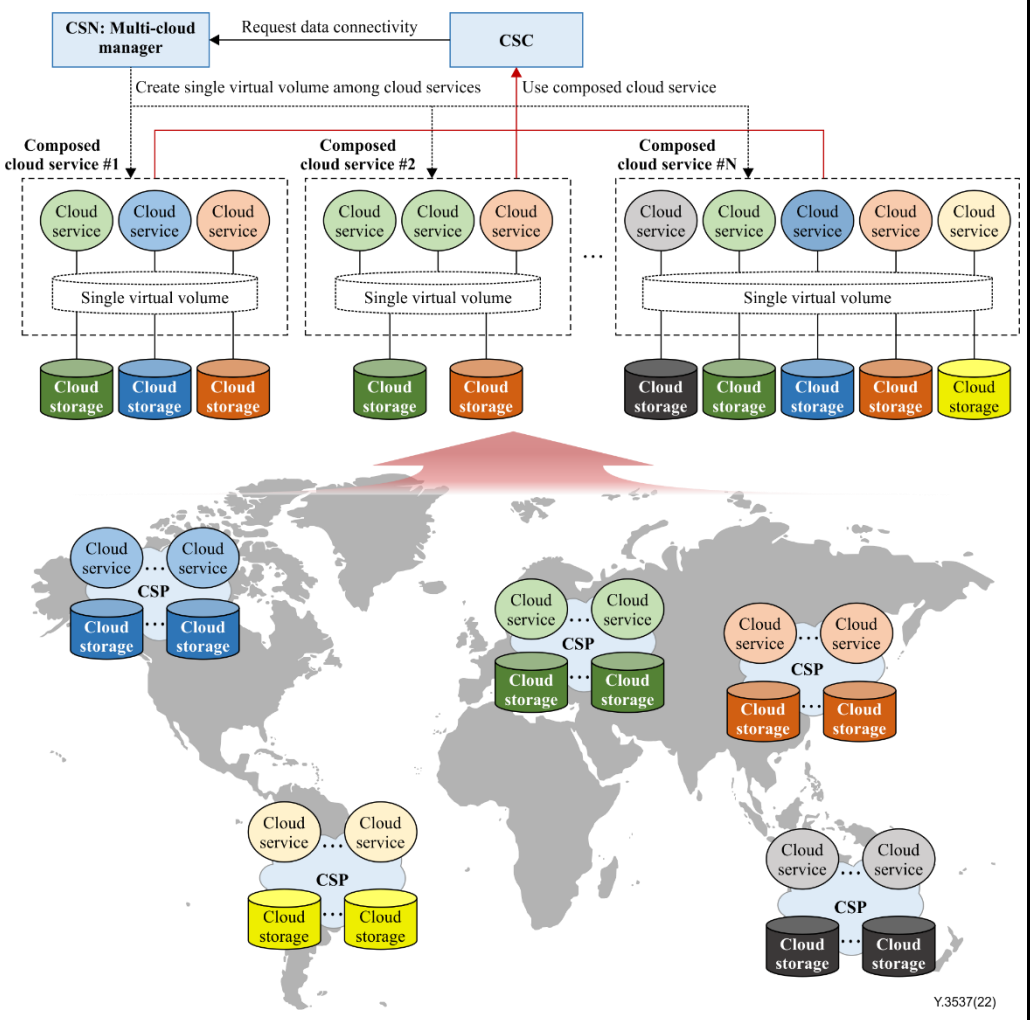
Figure	
Pre-conditions (optional)	CSC is supported by a CSN:multi-cloud manager. CSC provides the credentials for CSPs to the CSN:multi-cloud manager to get permission to access the cloud services provided by each CSP. CSN:multi-cloud manager provisions and composes the cloud services according to CSC's requirements and provides the composed cloud service to the CSC.
Post-conditions (optional)	
Derived requirements	– Composing cloud services (see clause 8.3) – Configuring composed cloud service (see clause 8.3) – Collecting cloud storage information (see clause 8.4) – Creating shared virtual volume for cloud service (see clause 8.4) – Providing mounting of shared virtual volume (see clause 8.4) – Providing stability for shared virtual volume (see clause 8.4).

Table I.7 – A use case for access management in multi-cloud

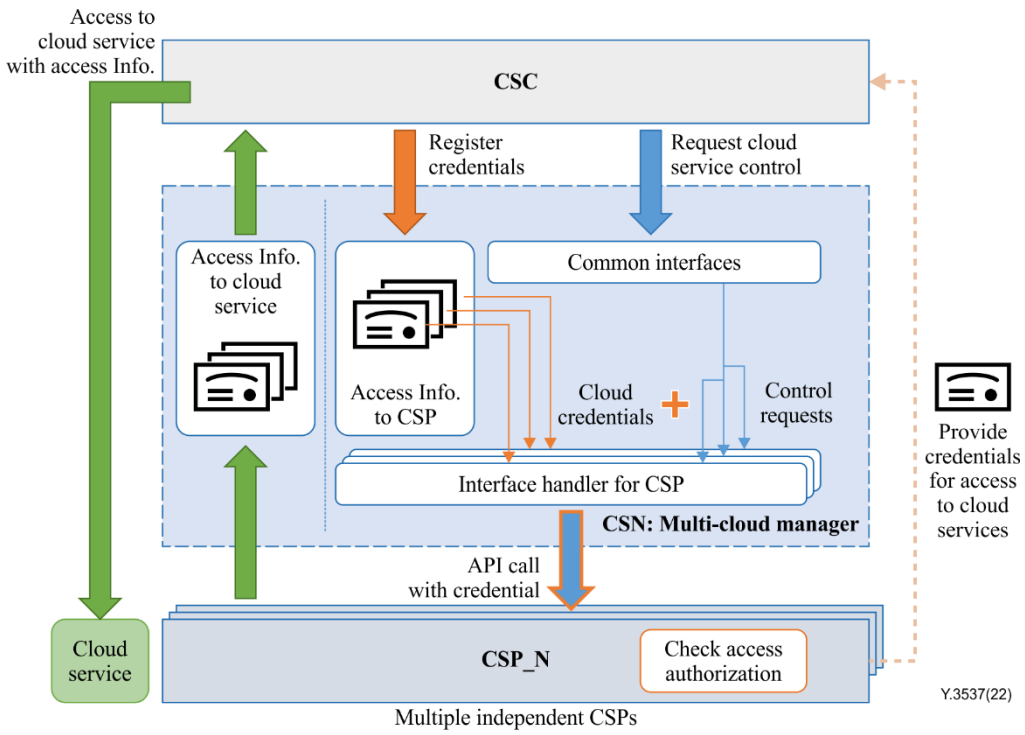
Title	Access management in a multi-cloud
Description	This use case shows a scenario where the CSC cooperates with a CSN:multi-cloud manager which manages the access information for a CSP to access the interface of each CSP and the cloud service. The detailed procedures for managing access to a CSP are as follows. 1) A CSC signs up for each CSP and requests a credential to get permission to use its interfaces. 2) Each CSP creates a credential and provides it to the CSC with access information for the CSP. 3) The CSC registers the credentials and the access information for the CSPs to the CSN:multi-cloud manager. 4) The CSN:multi-cloud manager stores them and utilizes them whenever the CSC requests any control for CSPs. Since the CSN:multi-cloud manager manages the credentials and access information for the CSP, the CSC does not need to provide access information for the CSP whenever it uses the CSP's interfaces. The detailed procedures for managing the access to a composed cloud service are as follows. 1) After a CSN:multi-cloud manager requests the cloud services to multiple CSPs on behalf of a CSC, each CSP provides the access information for its cloud services to the CSN:multi-cloud manager. 2) The CSN:multi-cloud manager stores and manages the collected access information for the composed cloud service to provide them to the CSC whenever requested. 3) The CSC can access the composed cloud service by using the delivered access information of each cloud service from the CSN:multi-cloud manager.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager
Figure	
Pre-conditions (optional)	

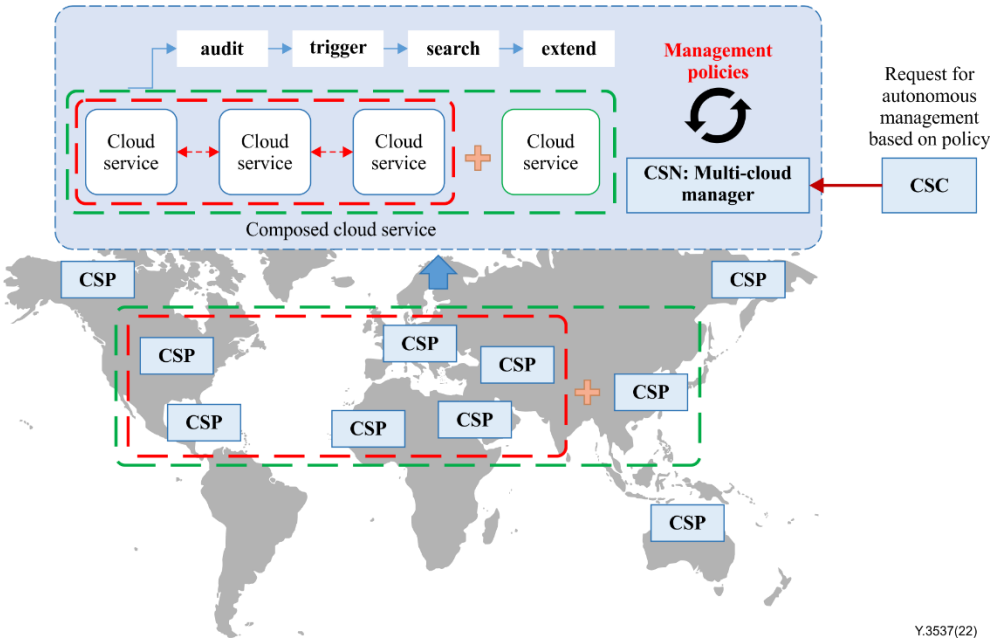
Table I.7 – A use case for access management in multi-cloud

Post-conditions (optional)	
Derived requirements	– Managing access information for CSP (see clause 8.2) – Authorizing access information for CSP (see clause 8.2) – Providing access information for composed cloud service (see clause 8.2) – Updating access information for composed cloud service (see clause 8.2)

Table I.8 – A use case for management policy for composed cloud service

Title	Management policy for composed cloud service
Description	For the CSC, it is hard to manage large-scale cloud services manually. It is much harder if the cloud services are from different CSPs and regions. Therefore, in this use case, a CSC cooperates with a CSN:multi-cloud manager to manage a composed cloud service automatically based on the management policy requests by the CSC. The management policy of composed cloud service is an automated management of composed cloud service according to the given policies and rules that consist of conditions and following actions. The detailed procedure for rule-based management of composed cloud service is as follows. 1) A CSC requests an autonomous management based on the policy for composed cloud service to a CSN:multi-cloud manager to automatically extend the composed cloud service (e.g. adding an additional cloud service) if the utilization rate of the composed cloud service is too high. 2) To comply with the management policy, the CSN:multi-cloud manager monitors the composed cloud service to check the workload on the composed cloud service which exceeds the limitation defined in the management policy. 3) If the CSN:multi-cloud manager detects a workload pattern that exceeds the limitation defined in the policy, the CSN:multi-cloud manager extends the composed cloud service by adding a new cloud service into the existing composed cloud service according to the actions defined in the management policy. The new cloud service can be selected by discovering the most appropriate cloud service in the available CSPs, in terms of cost, performance, response time and so on. 4) The CSN:multi-cloud manager applies the same configuration with the composed services to the new cloud service and adds the new cloud service to the composed cloud service so that the CSC can control and manage easily. 5) Without any manual control of the composed cloud service, the CSC is prepared for peak workload over the composed cloud service.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager

Table I.9 – A use case for service discovery in a multi-cloud

Title	Service discovery in a multi-cloud
Description	This use case shows a scenario that the CSC cooperates with a CSN:multi-cloud manager to discover cloud services from multiple CSPs to compose cloud services. The detailed procedures for service discovery in multi-cloud are as follows. 1) A CSN:multi-cloud manager regularly gathers information on cloud services from multiple CSPs and evaluates them to be prepared for service discovery requests from a CSC. 2) The CSC requests to compose cloud services to the CSN:multi-cloud manager with requirements, such as type and the number of cloud services, specification, performance, location and so on. For instance, the CSC requests 20 high performance virtual machines. 3) To satisfy the requirements, the CSN:multi-cloud manager tries to discover the most appropriate cloud services based on the information and evaluations of cloud services from multiple CSPs. 4) After discovering the best-matched cloud services, the CSN:multi-cloud manager notifies the results to the CSC. 5) The CSC confirms it and requests the provisioning of a composed cloud service that consists of the best-matched cloud services.
Roles/sub-roles	CSP, CSC, CSN:multi-cloud manager
Figure	
Pre-conditions (optional)	CSC provides the credentials for CSPs to the CSN:multi-cloud manager to get permission to access the cloud services provided by each CSP.
Post-conditions (optional)	
Derived requirements	– Providing information on the available cloud services (see clause 8.1) – Evaluating performance for cloud services (see clause 8.1) – Managing evaluation data of cloud services (see clause 8.1) – Discovering best matched cloud services (see clause 8.1) – Estimating cost for composed cloud service (see clause 8.1) – Delivering provisioning requests for cloud services (see clause 8.1)

Appendix II

Relationship between logical components and cloud computing activities of a CSN:multi-cloud manager

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

Cloud computing activities of a CSN:multi-cloud manager consist of (1) discover cloud services, (2) coordinate identity and security credentials, (3) coordinate customer requests, (4) perform intermediation and aggregation, (5) manage network connectivity, (6) manage governance policies and (7) monitor and report cloud services.

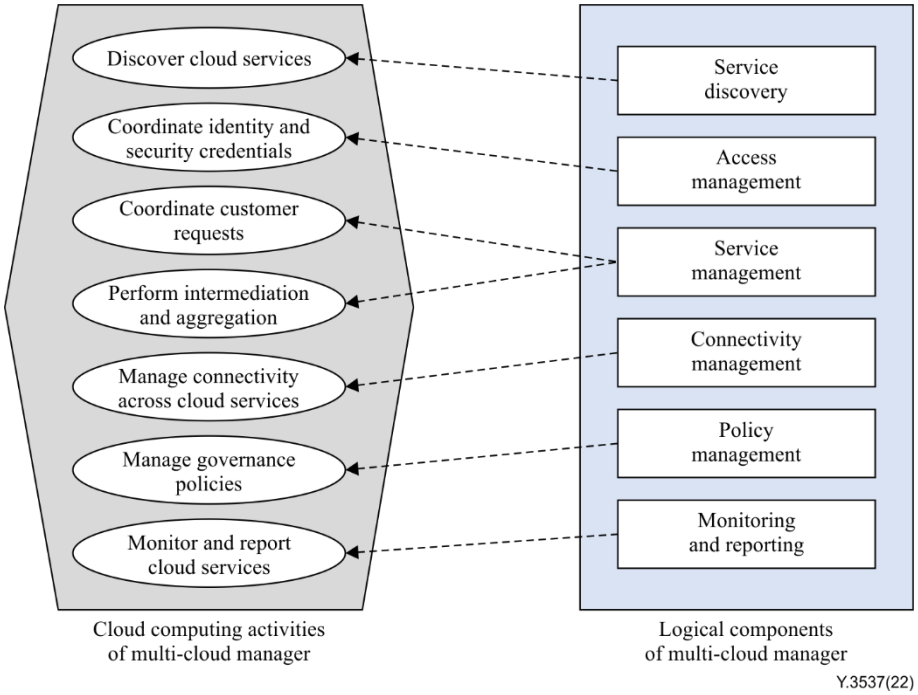


Figure II.1 – Relationship between logical components and cloud computing activities of a CSN:multi-cloud manager

1) **Logical components that can cover discover cloud services activity**: The discover cloud services activity (clause 7.1.1) involves searching and discovering the available public cloud services which can be provided by CSPs. The service discovery logical component searches the available cloud services in the public cloud from service catalogues provided by available CSPs. Also, the service discovery logical component (clause 7.2.1) provisions the optimal cloud services to the corresponded CSPs. So, the service discovery logical component fully supports the discover cloud services activity.

2) **Logical components that can cover coordinate identity and security credentials activity**: The coordinate identity and security credentials activity (clause 7.1.4) involves the coordination of identity and security credentials between a CSC and all CSPs. The access management logical component (clause 7.2.2) coordinates the identities and security credentials between a CSC and CSPs. Also, the access management logical component manages the credentials for the CSPs to guarantee the CSC as the authorized user while using the composed cloud service. So, the access management logical component fully supports the coordinate identity and security credentials activity.

3) **Logical components that can cover coordinate customer requests activity**: The coordinate customer requests activity (clause 7.1.5) involves handling requests from a CSC

and ensures the agreed SLA for a group of cloud services. The service management logical component (clause 7.2.3) composes, controls and manages the provisioned cloud services according to the CSC's request, ensuring that all cloud services in the composed cloud service meet the agreed SLA. The service management logical component delivers the control requests for each cloud service in the composed cloud service to the CSPs on behalf of the CSC. So, the service management logical component fully supports the coordinate customer requests activity.

4) **Logical components that can cover perform intermediation and aggregation activity**: The perform intermediation and aggregation activity (clause 7.1.2) involves composing cloud services provided by multiple CSPs in particular ways. The service management logical component (clause 7.2.3) composes, controls and manages the provisioned cloud services according to the CSC's request through various interfaces such as RESTful API, gRPC API and so on. Also, the service management logical component provides unified interfaces so that the CSC can use the composed cloud service in the same way, as when the CSC uses cloud services directly provided by CSPs. So, the service management logical component fully supports the perform intermediation and aggregation activity.

5) **Logical components that can cover manage connectivity across cloud services activity**: The manage connectivity across cloud services activity (clause 7.1.3) involves the interoperability management among composed cloud services by providing network connectivity and data connectivity. It sets up the virtual network connections and related capabilities among the composed cloud service, which can include the establishment of various network facilities, such as an overlay network or VPN. It also creates and provides virtual storage for data connectivity which are shared among composed cloud services. The connectivity management logical component (clause 7.2.4) sets up the network connection and the related capabilities among cloud services in the composed cloud service to provide the network connectivity to the composed cloud service. This logical component provides and manages the various network capabilities such as the VPN, tunnelling, load balancing and so on to the composed cloud service. Moreover, this logical component provides the data connectivity for the data sharing for the composed cloud service by federating the storage services provided by each CSP. So, the connectivity management logical component fully supports the manage connectivity across cloud services activity.

6) **Logical components that can cover manage governance policies activity**: The manage governance policies activity (clause 7.1.7) involves managing the various policies to control the provisioning and use of cloud services and the related data composed cloud service. The policy management logical component (clause 7.2.6) provides and manages the various policies for cost management, optimized utilization and autonomous management of cloud services in composed cloud service during provisioning and using composed cloud service. The policy management logical component also manages the procedure to collect, store, backup and remove various data such as monitoring metric data, log data and so on. So, both logical components support the management of the various policies to control the provisioning and use of cloud services and the related data.

7) **Logical components that can cover monitor and report cloud services activity**: The monitor and report cloud services activity (clause 7.1.6) involves monitoring all cloud services of the CSPs and reporting the behaviours in the aggregated forms. The monitoring and reporting logical component (clause 7.2.5) monitors all the cloud services in the composed cloud service in the aggregated forms. Also, the monitoring and reporting logical component collects the various reports such as usage reports, audit reports, problem reports and so on from CSPs, and provides them to CSC in the aggregated form. So, the monitoring and reporting logical component fully supports the monitor and report cloud services activity.

Appendix III

Relationship between cloud service customer, cloud service provider and cloud service partner

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

The interoperability aspect of the cross-cutting aspects described in [b-ITU-T Y.3502] includes the ability for one cloud service to work with other cloud services, either through a CSP:inter-cloud provider, or where a cloud service customer uses multiple different cloud services in some form of composition to achieve their business goals.

Figure III.1 shows the relationship between CSC, CSP and CSN for the interoperability among the cloud services from the multiple CSPs. Unlike CSP:inter-cloud provider, CSN:multi-cloud manager itself doesn't provide any cloud service and its role is independent of the role of the inter-cloud provider.

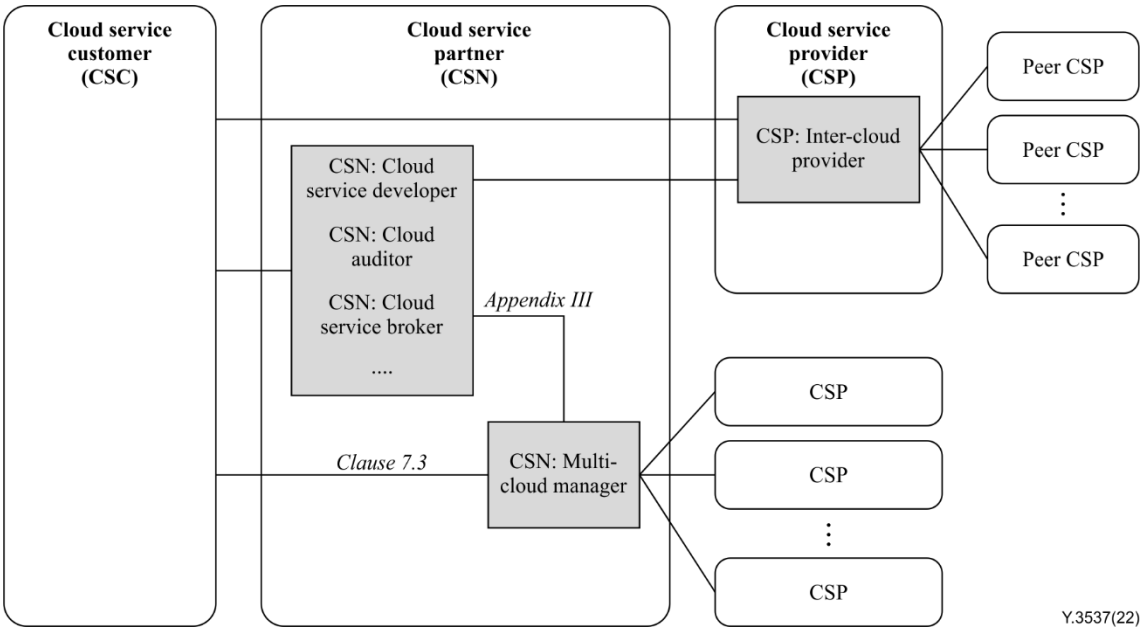


Figure III.1 – Relationship between CSC, CSP and CSN for the interoperability

A CSC uses multiple cloud services from the different CSPs through a CSP:inter-cloud provider of the primary CSP. Without any support of an inter-cloud relationship by a CSP, the CSC itself is able to interact with two or more CSPs. The CSN:multi-cloud manager supports this CSC to use cloud services from the multiple CSPs with interoperability aspect among the cloud services because the CSN is a party which is engaged in support of, or auxiliary to, the activities of the CSP or the CSC, or both, which is described in [b-ITU-T Y.3502].

On the other hand, the existing sub-roles of the CSN such as CSN:cloud service developer, CSN:cloud auditor, and CSN:cloud service broker also need an environment involving two or more CSPs, and their several activities assume multiple cloud services. Moreover, cloud service brokerage which is a service that arbitrates, delivers, and manages cloud services provided by CSPs for CSCs and is realized by a CSN:cloud service broker categorizes the three service models in [b-ITU-T Y.3506], such as the cloud service aggregation, cloud service integration and cloud service customization. While the existing sub-roles of CSN can perform their activities to the multiple cloud service through the CSP:inter-cloud provider, the CSN:multi-cloud manager helps them to perform their activities for

the cloud services from the multiple independent CSPs, without any support of an inter-cloud provider by CSP.

While the CSN:multi-cloud manager mainly interacts with a CSC for multi-cloud, it also involves managing the cloud services on multiple CSPs for other sub-roles of CSN which perform their activities to the multiple independent CSPs as well as the single CSP. Compared to a CSC who just wants to use the cloud services with the help of the CSN:multi-cloud manager, the existing sub-roles of the CSN have the information about the targeted CSP or the cloud services to perform their activities. So, the existing sub-roles register the credentials for the targeted CSPs to the CSN:multi-cloud manager and perform their own activities to each CSP through the CSN:multi-cloud manager, as shown in Figure III.2.

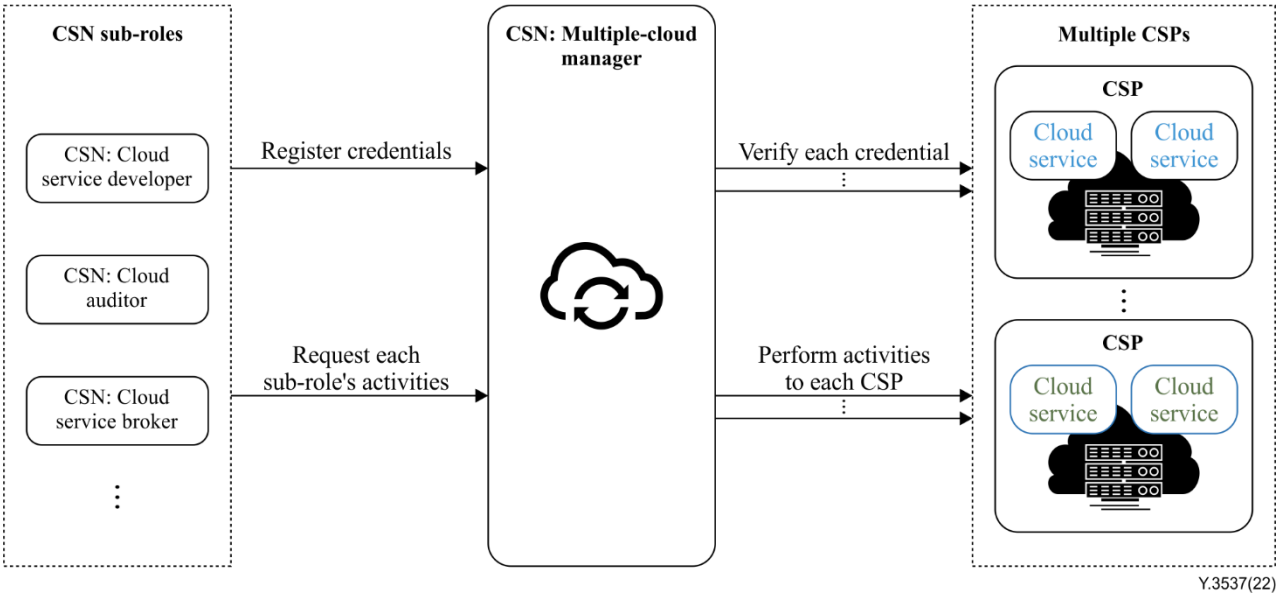


Figure III.2 – Interactions of CSN:multi-cloud manager with other sub-roles of CSN

Bibliography

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

[b-ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[b-ITU-T X.1642] Recommendation ITU-T X.1642 (2016), *Guidelines for the operational security of cloud computing*.

[b-ITU-T Y.3506] Recommendation ITU-T Y.3506 (2018), *Cloud computing – Functional requirements for cloud service brokerage*.

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

[b-ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

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, 2022