



BSI Standards Publication

Cloud computing — Multi-cloud management

Part 1: Overview and use cases

National foreword

This Published Document is the UK implementation of ISO/IEC TR 10822-1:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/38, Cloud Computing and Distributed Platforms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 26124 0

ICS 35.210

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



Technical Report

ISO/IEC TR 10822-1

Cloud computing — Multi-cloud management —

Part 1: Overview and use cases

Informatique en nuage — Gestion multi-nuages —

Partie 1: Vue d'ensemble et cas d'utilisation

**First edition
2025-05**

Reference number
ISO/IEC TR 10822-1:2025(en)

 **Documents**
© ISO/IEC 2025 Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	1
5 Overview of multi cloud management	2
5.1 General	2
5.2 User view of multi-cloud management	4
5.3 Functional view of multi-cloud management	6
5.4 Functional architecture of multi-cloud management	8
6 Multi-cloud management activities, functions and roles	9
6.1 General	9
6.2 Multi-cloud management activities	9
6.2.1 General	9
6.2.2 Cloud service discovery and publishing	10
6.2.3 Resource management	10
6.2.4 Deployment management of resources and services	10
6.2.5 Cost optimization	11
6.2.6 Security and privacy	11
6.2.7 Policy-based governance	11
6.2.8 Integration, aggregation, intermediation, composition, chaining of service APIs	11
6.2.9 User identities and access control	12
6.2.10 Reporting and auditing of multi-cloud services	12
6.2.11 Interface for multi-cloud administration	12
6.3 Multi-cloud management functions	12
6.3.1 General	12
6.3.2 Uniform user interface	12
6.3.3 Access control through integrated identity management	13
6.3.4 Cloud service scheduler: service orchestration and management	15
6.3.5 Service discovery	18
6.3.6 Service library	18
6.3.7 Service catalogue	18
6.3.8 Provisioning and deprovisioning: resource and service	19
6.3.9 Resource operations management	20
6.3.10 Monitor multi-cloud services	20
6.3.11 SLA management	21
6.3.12 Report and audit	21
6.3.13 Uniform policy management	22
6.3.14 Security and privacy management	23
6.3.15 Centralized billing and metering	24
6.3.16 Interoperability functions-API abstraction and management framework	25
6.3.17 Connection management	28
7 Use cases	29
7.1 Multi-cloud management-API discovery in terms of service discovery and visualization	29
7.2 Multi-cloud management API discovery in terms of service provisioning	32
7.3 Multi-cloud management Resource Deployment	34
7.4 Multi-cloud environment - interoperable API abstraction and management	35
7.5 Multi-cloud management interoperable service provisioning	38
7.6 Multi-cloud management service billing and metering based on consumption-decision making iterations	40
7.7 Multi-cloud management SLA negotiation workflow in multi-cloud environment	44

7.8 Multi-cloud management API integration..... 46

7.9 Multi-cloud management API aggregation..... 48

7.10 Multi-cloud management policy enforcement framework..... 51

7.11 Multi-cloud management cloud service scheduler..... 52

7.12 Multi-cloud management storage API abstraction..... 54

8 Industry examples 55

9 Impact and benefits on industries 57

9.1 General..... 57

9.2 Additional impact of multi-cloud management..... 58

10 Conclusion 59

Annex A (informative) Further details on multi-cloud management user view and functional view 60

Bibliography 66

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

A list of all parts in the ISO/IEC 10822 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Many CSCs are using cloud services from multiple CSPs to achieve cost savings, vendor choice, business continuity, choice of services and security.

Operating in a multi-cloud environment poses a number of challenges for CSCs including varying interfaces, billing and metering schedules, security and privacy protections and performance.

CSCs can address multi-cloud challenges on their own, or by using cloud service partners, through standardized approaches.

Cloud computing — Multi-cloud management —

Part 1: Overview and use cases

1 Scope

This document is based on ISO/IEC 22123-1, ISO/IEC 22123-3 and ISO/IEC 5140 and provides an overview of the management challenges faced in multi-cloud deployments, as well as the management activities that can be undertaken to address these challenges.

Additionally this document provides use cases with user and functional views to further explain the multi-cloud management challenges and activities

2 Normative references

There are no normative references in this document.

3 Terms and definitions

No terms and definitions are listed in this document.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

4 Abbreviated terms

API	Application programming interface
CCPA	California consumer privacy act
CCRA	Cloud computing reference architecture
CSA	Cloud service agreement
CSC	Cloud service customer
CSN	Cloud service partner
CSP	Cloud service provider
CSU	Cloud service user
DR	Disaster recovery
GDPR	General data protection regulation
IaaS	Infrastructure-as-a-service

PaaS	Platform-as-a-service
PII	Personally identifiable information
QoS	Quality of service
SaaS	Software-as-a-service
SLA	Cloud service level agreement
SLO	Cloud service level objectives

5 Overview of multi cloud management

5.1 General

According to ISO/IEC 5140, multi-cloud management includes the use and operation of multiple cloud services from two or more CSPs. The CSPs and their associated cloud services can be unaware of each other, and the onus to manage the multi cloud ecosystem is on the CSC.

As different CSPs provide different capabilities, interfaces, datacentre locations, provisioning mechanisms, connectivity, security, and access protocols, manual management of a multi-cloud ecosystem for a CSC can prove cumbersome over time as the environment and number of application services grows.

Multi-cloud management solutions can assist CSCs manage their multi-cloud ecosystems, and they can work as aggregator, integrator, and customizer. They can also offer a consistent method for managing the provisioning and control mechanisms of cloud services, including access, security, connectivity, logging, and monitoring of resources and services across multiple cloud platforms and CSPs.

[Figure 1](#) shows a representative multi-cloud management ecosystem where a CSC uses more than one CSP, where APP-X and APP-Y represent applications in the CSC environment which are being managed by a Multi-cloud management solution.

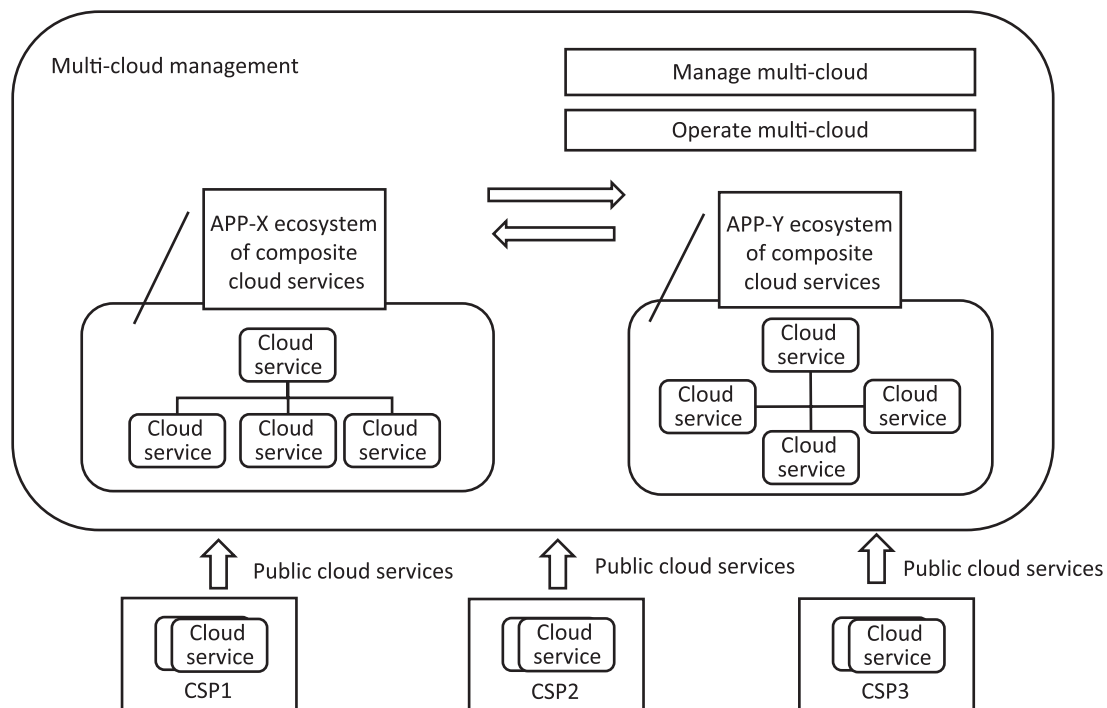


Figure 1 — A representative Multi-Cloud Management ecosystem

A Multi-cloud management solution can:

- Provide identification of cloud services offered by multiple CSPs;
- Provide the CSC with a single, uniform interface to the cloud services;
- Enable multiple cloud services from different CSPs to interact with each other;
- Enable composite cloud services;
- Facilitate control and provisioning of cloud services without compromising security or privacy.

Several challenges in multi-cloud management can include:

- Managing architectural complexity
- Managing security and compliance
- Managing distributed and heterogeneous policies
- Managing agile interoperability between different CSPs
- Managing visibility across CSP resources
- Managing increased complexity of operations across different CSPs
- Managing elimination of redundancies
- Managing the cost structure and bringing uniformity on cost visualization for CSCs across various CSPs.

Multi-cloud management platforms can be implemented or operated by CSNs, CSPs, or by CSCs.

5.2 User view of multi-cloud management

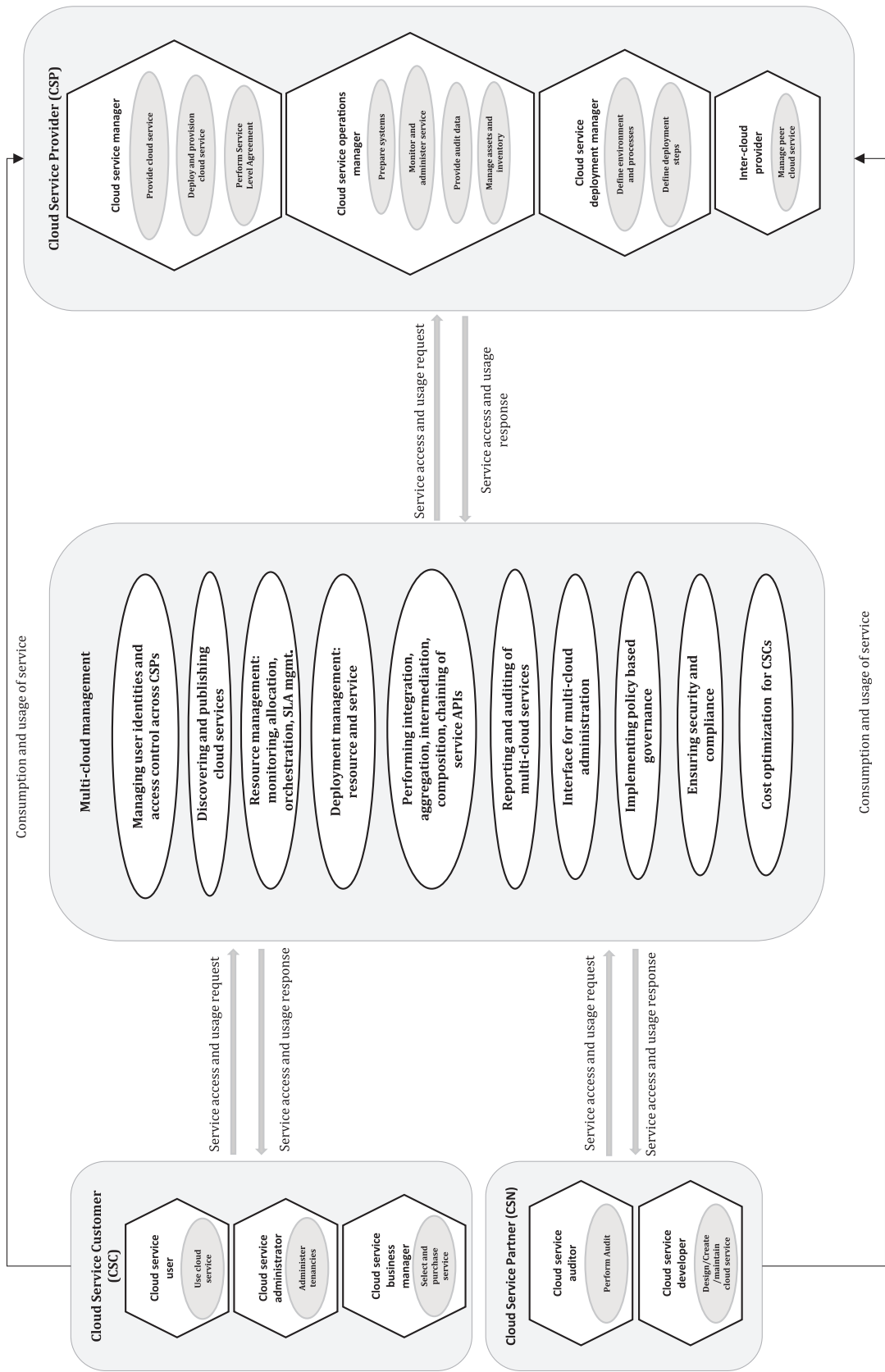


Figure 2 — User view of multi-cloud management

[Figure 2](#) illustrates the various activities and functions of multi-cloud management along with relevant CSC, CSN and CSP activities that can enable a Cloud Service Customer (CSC) to utilize cloud services from multiple Cloud Service Providers (CSPs).

[Figure 2](#) employs graphical conventions introduced in Figure 1 (Conventions for CCRA diagrams) of ISO/IEC 22123-3:2023. The boxes with continuous rounded edges represent roles, the hexagons represent sub-roles, and the rounded edged oval boxes represent cloud computing activities.

Multi-cloud management encompasses a variety of activities aimed at effectively managing multiple cloud environments.

Prospective users of multi-cloud management platform can be various cloud service customer (CSC) and cloud service partner (CSN) subroles like

- CSC: cloud service user;
- CSC: cloud service administrator;
- CSC: cloud service business manager;
- CSN: cloud service auditor;
- CSN: cloud service developer.

The multi-cloud management interface empowers CSC/CSN users or user subroles to seamlessly assimilate, deploy services, and execute tasks within the target cloud service provider (CSP) environment.

The process involves CSC or CSN users and user subroles submitting their requests to the multi-cloud management platform. The submitted requests are then forwarded to the CSPs through various multi-cloud management activities, triggering specific functions that facilitate the placement of the requests to the CSPs. The responses from the CSPs are interpreted by the multi-cloud management functions, enabling the provision of suitable services to the respective CSC or CSN users for their continued utilization.

[Clause 6.2](#) provides a detailed overview of the multi-cloud management activities where each activity is linked to specific functions supporting task execution, as further explained in [6.3](#). To enhance understanding of the functional components, review [5.3](#) before proceeding to [6.3](#).

For further details on multi-cloud management user view and functional view refer to [Annex A](#).

This document considers typical use cases for evaluating Multi-cloud management solutions. It is not meant to indicate that these exemplary views represent the only or the preferred implementation for such a use case.

5.3 Functional view of multi-cloud management

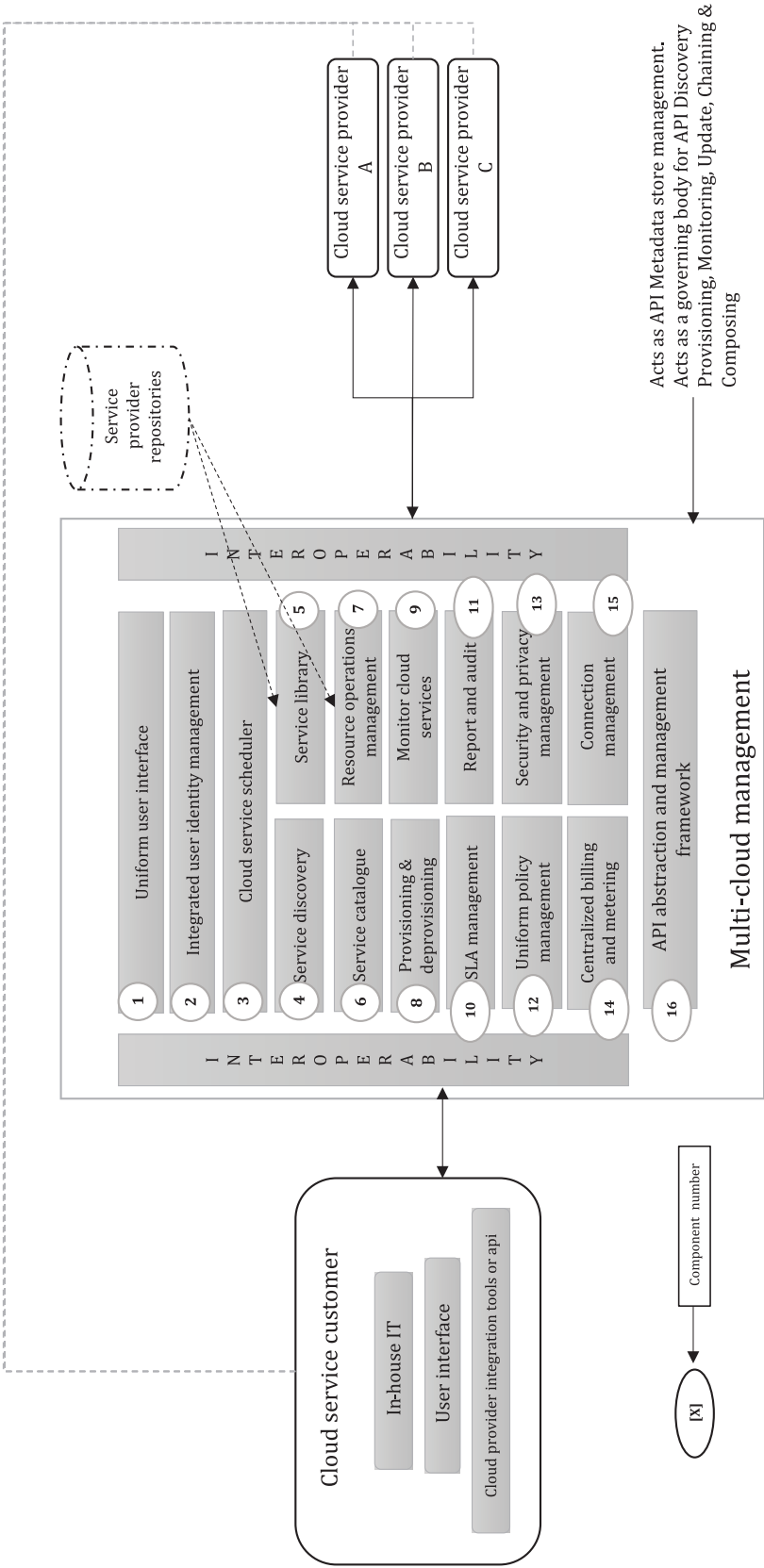


Figure 3 — Multi-cloud management functions

Figure 3 illustrates the various activities and functions of multi-cloud management that can enable a Cloud Service Customer (CSC) to utilize cloud services from multiple Cloud Service Providers (CSPs).

[Figure 3](#) uses graphical conventions introduced by Figure 1 in ISO/IEC 22123-3:2023. The boxes with continuous rounded edges represent roles, and the square ones with bricks are functional components.

Multi-cloud management encompasses the following functional components to address various aspects which are discussed in [6.3](#).

- Uniform user interface;
- Integrated user identity management;
- Cloud service scheduler;
- Service discovery;
- Service library;
- Service catalogue;
- Provisioning and deprovisioning;
- Resource operations management;
- Monitor cloud services;
- SLA management;
- Report and audit;
- Uniform policy management;
- Security and privacy management;
- Centralized billing and metering;
- API abstraction and management framework;
- Connection management through inter-cloud gateway.

5.4 Functional architecture of multi-cloud management

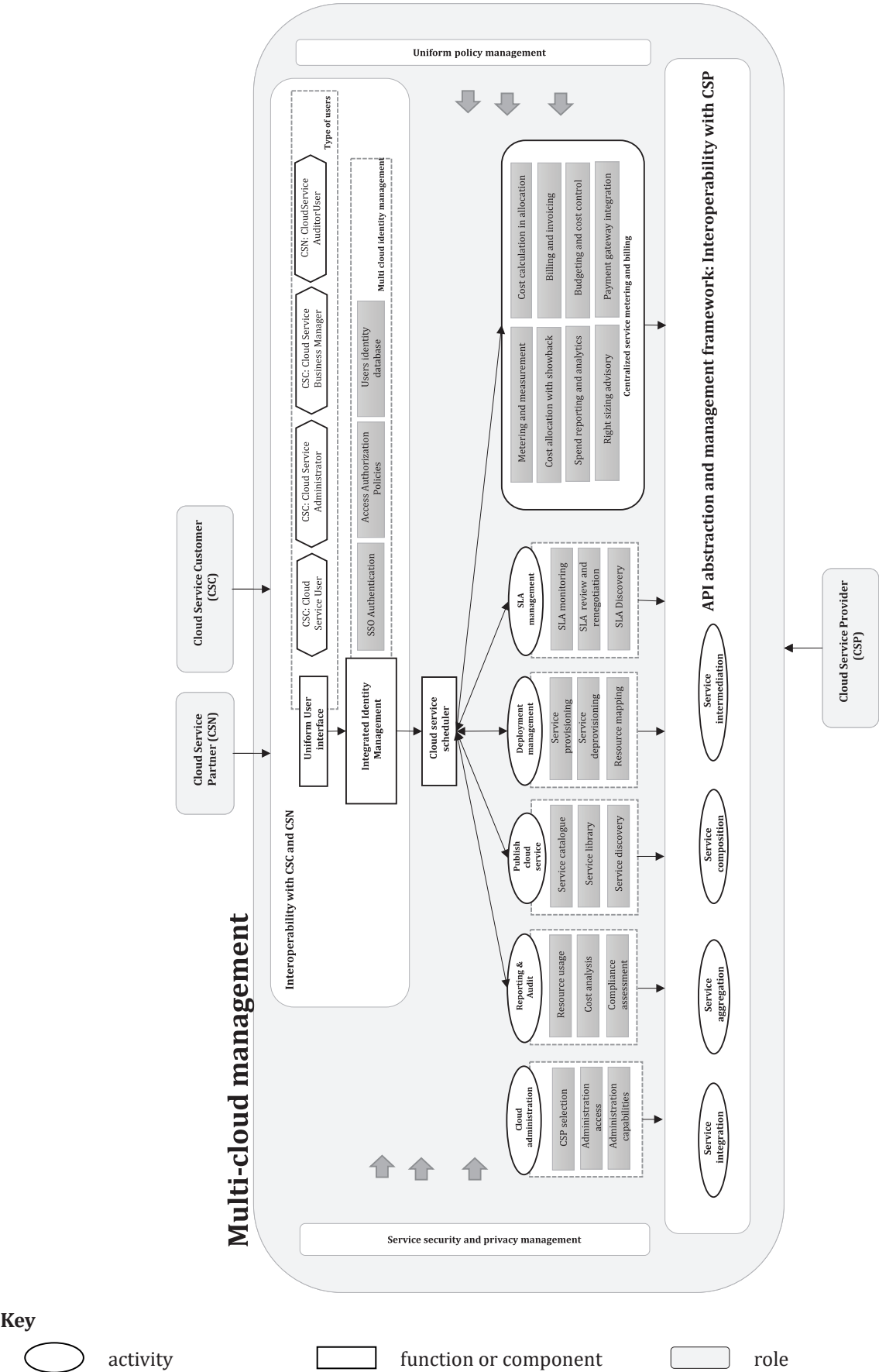


Figure 4 — Functional architecture of multi-cloud management on component association

This document draws inspiration from ISO/IEC 5140 and ISO/IEC 22123-3:2023. The goal is to avoid positioning it as a standalone multi-cloud management entity. Instead, the aim is to present it within the broader context of multi-cloud management, emphasizing its role as a platform or ecosystem.

[Figure 4](#) uses graphical conventions introduced by Figure 1 of ISO/IEC 22123-3:2023. The roles are represented by boxes with continuous rounded edges, cloud computing activities are represented by rounded edge boxes, and the functional components are represented by square boxes with bricks.

It is evident that Roles are set of activities in cloud computing, and these activities are performed using functional components.

The proximity of the graphical elements representing roles is meaningful and signifies close interaction between roles, assuming neighbouring roles. For instance, the multi-cloud management role is positioned at the centre of the diagram to emphasize its interaction with all other roles. Similarly, the positioning of the multi-cloud computing activities inside a given role, as well as the relative placement of functional components within a specific activity, follows the same principle. For example, the service capabilities functional component is positioned above the resource abstraction and control functional component, to indicate the dependency of the former on the latter.

The functional architecture for multi-cloud computing describes cloud computing in terms of a high-level set of functional components. The functional components represent sets of functions that can be utilized to perform the multi-cloud computing activities for the various roles and sub-roles involved in cloud computing.

The functional architecture describes functional components using conventions introduced in Figure 1 of ISO/IEC 22123-3:2023. The layering framework as outlined in Figure 11 of ISO/IEC 22123-3:2023 is adhered to as a part of the functional architecture depicted in [Figure 4](#), although it is not diagrammatically represented to maintain a less complex and cumbersome appearance.

For the understanding of the layering framework and its accordance with Figure 1 of ISO/IEC 22123-3:2023, please refer to [Figure A.2](#).

6 Multi-cloud management activities, functions and roles

6.1 General

Multi-cloud management can enable a consistent and uniform cloud management ecosystem for a given CSC whose workloads hosted across different CSPs, that interact and collaborate effectively across different cloud platforms. Multi-cloud management solutions can allow CSCs to manage multi-cloud management operations from a single interface with efficient monitoring and trustworthy security.

6.2 Multi-cloud management activities

6.2.1 General

Multi-cloud management activities can include:

- hand-shake between selected CSPs as needed by exchanging information using pre-defined and agreed methods;
- point of entry for the CSC to manage multiple cloud services;
- single and consistent interface to multiple CSPs to host and access their workloads;
- managing CSU identities uniformly for a CSC, across multiple CSPs;
- validating requests from authorized sources;

- visibility into selected CSPs;
- performing role of Cloud Aggregation, Cloud Integration and Cloud Customization;
- discovering and publishing cloud services;
- resource management;
- deployment management: resource and service;
- monitoring cloud services;
- cost optimization for the CSCs;
- ensuring security and compliance;
- performing integration, aggregation, intermediation, composition, chaining of service APIs;
- implementing policy-based governance;
- reporting and auditing of multi-cloud services;
- acting as interface for multi-cloud administration.

Subclauses [6.2.2](#) to [6.2.11](#) delve into a comprehensive description of the key activities involved in multi-cloud management, aiming to efficiently oversee multiple cloud environments.

6.2.2 Cloud service discovery and publishing

In multi-cloud management, the process of discovering and publishing cloud services involves identifying available services within various cloud environments and making them accessible to CSUs. This ensures efficient utilization of services and enhances the CSU experience. This activity can be associated with:

- service discovery;
- service library and catalogue management;
- service publication.

6.2.3 Resource management

Multi-cloud resource management involves functions related to the monitoring, management, and optimization of computing resources within multi-cloud environment (e.g. CPU, storage, memory, and network bandwidth) to meet the demands of applications and services running in the cloud. The goal of resource management is to ensure efficient utilization of available resources while maintaining performance, scalability, load balancing, and cost efficiency. It achieves this objective through functions like:

- resource allocation;
- load balancing;
- monitoring multi-cloud services;
- SLA management;
- service orchestration and management.

6.2.4 Deployment management of resources and services

Multi-cloud deployment management involves provisioning, or deprovisioning, and allocating, or deallocating, cloud resources and services across different CSPs. It ensures that the necessary resources, such as virtual machines, storage, and networking components, are provisioned based on demand and workload requirements.

Multi-cloud management facilitates the deployment, usage, and orchestration of services across multiple clouds. It enables the seamless integration and coordination of services to support complex applications and workflows that span across different cloud environments. Deployment management ensures that the necessary resources and dependencies are made available and properly configured for the application or service to function effectively in the multi-cloud environment as requested by the CSU. This activity can be associated with:

- resource provisioning and deprovisioning;
- service provisioning and deprovisioning.

6.2.5 Cost optimization

Multi-cloud management aims to optimize costs by efficiently allocating resources, leveraging pricing models, identifying cost-effective CSPs or services and providing a centralized billing. It helps organizations achieve a balance between performance, functionality, and cost efficiency. This activity can include:

- cloud service price schedules;
- cloud service agreements;
- cloud SLAs.

6.2.6 Security and privacy

Multi-cloud management involves implementing and enforcing security and privacy measures and policies across multiple clouds. It ensures consistent security practices, controls access to resources, and mitigates risks associated with data privacy requirements.

6.2.7 Policy-based governance

Multi-cloud management includes establishing governance frameworks, managing policies and best practices for cloud usage across multiple CSPs.

6.2.8 Integration, aggregation, intermediation, composition, chaining of service APIs.

Multi-cloud management can be utilized to perform servicing, security, monitoring, policy integration, aggregation, intermediation, composition, and chaining of service APIs.

- Service integration is the process of connecting different cloud-based services. It allows CSCs to share data and processes across their cloud environments, regardless of where the data or applications are located.
- Aggregation is the process of collecting data from multiple sources and presenting it in a single view. It can help in obtaining an overview of data and make better decisions.
- Intermediation is the process of providing a layer of abstraction between two or more services. It simplifies the way that services interact and makes it easier to manage them.
- Composition is the process of combining multiple services to create a new service. It can be used to create more complex and powerful solutions that are not feasible with a single service.
- Chaining is the process of connecting multiple services in a sequence, helping to create workflows that automate tasks and improve efficiency.

A multi-cloud management platform can perform roles such as a "cloud aggregator," "cloud integrator," and "cloud customizer" to fulfil the aforementioned tasks. A brief description of these roles is provided in 6.4, while [6.3.16](#) explains the functions associated with these activities

6.2.9 User identities and access control

Multi-cloud management can be used to manage CSU identities and access control across multiple CSPs. This involves implementing a consistent approach to CSU authentication, authorization, access control. This activity can involve:

- CSU accounts;
- CSU identities;
- CSU permissions.

6.2.10 Reporting and auditing of multi-cloud services

Multi-cloud management platforms can provide robust reporting and auditing capabilities for cloud services, enabling organizations to monitor and analyse various aspects of their multi-cloud environment. They can generate reports, which can be essential for audits, like:

- resource utilization report;
- cost analysis report;
- compliance and security report;
- service performance;
- governance and policy compliance;
- customize reports based on specific requirements.

6.2.11 Interface for multi-cloud administration

Multi-cloud management can provide a centralized control panel where administrators can perform cloud administrative tasks like “resource management” and “service management”.

By performing these activities, multi-cloud management enables organizations to effectively manage and leverage the benefits of multiple cloud environments, optimizing resource utilization, performance, cost efficiency, security, and compliance.

6.3 Multi-cloud management functions

6.3.1 General

This description outlines functions that can be part of a multi-cloud management platform as described in [6.2](#).

6.3.2 Uniform user interface

In multi-cloud management, a uniform user interface can ensure a consistent CSU experience across multiple cloud platforms through a single management interface. The user interface of a multi-cloud management platform can incorporate the following elements:

- **Centralized dashboard:** The interface includes a centralized dashboard that provides an overview of the CSU’s connected cloud environments, including resources, services, and their status across multiple clouds. It allows CSUs to monitor and manage their cloud assets from a single location.
- **Cloud service integration:** The user interface integrates with various cloud service provider APIs to enable management and orchestration of resources across different clouds. It provides a consistent way to interact with services such as virtual machines, storage, networking, databases, and other cloud-specific offerings.

- **Unified navigation and controls:** A uniform user interface provide consistent navigation and control mechanisms, allowing CSUs to easily switch between different clouds and perform management tasks seamlessly. It includes standardized menus, sidebars, and controls to ensure familiarity and ease of use across various cloud environments.
- **Resource management:** The interface provides capabilities for managing cloud resources across multiple CSPs. CSUs can perform tasks such as provisioning and deprovisioning resources, scaling resources, starting/stopping resources and monitoring resource usage and performance across different clouds, through integrated service APIs.
- **Security and access control:** A uniform user interface provides consistent security and access control mechanisms. It allows CSUs to manage authentication, permissions, and security policies consistently across multiple clouds. This ensures that CSUs can enforce a unified security policy across their cloud environments.
- **Monitoring and analytics:** The interface can include unified monitoring and analytics features that aggregate data from different cloud providers. This allows CSUs to gain insights into the performance, health, and utilization of their multi-cloud infrastructure.

By providing a uniform user interface, the multi-cloud management platform simplifies the complexity of managing multiple clouds and enhances user productivity by offering a consistent and streamlined experience for monitoring, provisioning, managing, and securing resources across diverse cloud environments.

6.3.3 Access control through integrated identity management

Access control, facilitated by the integrated identity management of a multi-cloud management platform, allows CSUs to access specific services from designated CSPs. The core aspect of access control involves authenticating a user through the presentation and validation of credentials, followed by authorizing the authenticated user to access particular services. The multi-cloud management platform to provide access control for cloud services, their dependent resources, and the corresponding control functions.

Users affected by multi-cloud access control can include:

- CSC: cloud service user(CSU);
- CSC: cloud service administrator;
- CSC: cloud service business manager;
- CSN: cloud service auditor user.

The integrated identity management activity can include three functions:

— SSO Authentication:

Multi-cloud management facilitates Single Sign-On (SSO) authentication, streamlining the authentication process for users across multiple cloud environments. With SSO, users can access multiple cloud services and platforms using a single set of credentials. It eliminates the need to remember and enter separate login information for each cloud provider.

By integrating SSO authentication into the multi-cloud management platform, users can securely authenticate once and gain access to their authorized resources and services across different clouds. It simplifies the login experience and also enhances security by reducing the risk associated with managing multiple sets of credentials.

Furthermore, SSO authentication in multi-cloud management provides centralized control and visibility over user access rights and permissions. Administrators can efficiently manage user authentication, access policies, and authorization levels from a single management interface. This helps enforce consistent security practices and simplifies the management of user access across different cloud environments.

— Access Authorization Policies:

Multi-cloud management involves the implementation of access authorization policies across different cloud environments. These policies define the rules and permissions for user access to resources and services within the multi-cloud infrastructure.

By implementing access authorization policies in multi-cloud management, administrators can enforce consistent security practices, limit access to sensitive resources, and mitigate risks associated with unauthorized access. These policies provide a systematic and controlled approach to managing user access across multiple cloud platforms within the multi-cloud environment.

Access authorization policies in multi-cloud management can include:

- **Role-based access control(RBAC):** RBAC assigns users roles based on responsibilities, granting appropriate permissions to access resources and perform actions relevant to their role in the multi-cloud environment;
- **Fine-Grained Access Control:** Fine-grained access control provides detailed user permission control, allowing administrators to define specific rules based on attributes like user, group, IP address, or resource type;
- **Attribute-based access control (ABAC):** ABAC considers user attributes, resource attributes, and environmental factors to determine access, allowing flexible policies based on dynamic conditions and contextual information;
- **Policy-Based Access Control:** Policy-based access control uses predefined policies to determine access, considering factors like time, location, user role, or resource attributes. It simplifies access control management by centrally defining and managing policies.
- **Multi-Factor Authentication (MFA):** MFA enhances security by requiring multiple forms of authentication, such as a password and a unique mobile code, ensuring authorized access to the multi-cloud management platform;
- **Users' identity database:**

The users' identity database in multi-cloud management serves as a central repository for storing and managing user identities and related information.

The user identity database plays a crucial role in enforcing access control policies. It stores information about user roles, privileges, and permissions, enabling administrators to define and manage access rights for different users. This helps ensure that users have appropriate access to resources and functionalities within the multi-cloud environment. It can also store additional information about users, such as contact details, organizational affiliations, and preferences, thus providing a comprehensive view of user profile.

The user identity database enables administrators to create, modify, and delete user accounts within the multi-cloud management platform. It allows for the management of user attributes, such as usernames, email addresses, roles, and permissions.

User Authentication uses the identity database to verify the authenticity of users by validating their credentials during the authentication process. This ensures that only authorized users can access the multi-cloud management platform.

The user identity database implements security measures to protect user identities and sensitive information. It includes mechanisms such as encryption, strong access controls, and monitoring to prevent unauthorized access or data breaches.

The users' identity database in multi-cloud management enables secure user authentication, efficient user management, fine-grained access control, and the overall security and integrity of user identities and associated information.

6.3.4 Cloud service scheduler: service orchestration and management

6.3.4.1 General

The cloud service scheduler in multi-cloud management is a component that orchestrates the scheduling, usage, and allocation of cloud resources across multiple cloud environments.

The cloud service scheduler serves as a centralized controller in multi-cloud management, orchestrating and coordinating various functions within the system. It acts as the command center, directing and invoking other functions as needed. It ensures that the different elements used for a service or application to function together seamlessly, are orchestrated and synchronized. By effectively managing and scheduling tasks, the cloud service scheduler ensures the smooth execution of operations across the multi-cloud environment.

The cloud service scheduler invokes specific functions as an integral part of the multi-cloud management platform, thereby facilitating execution of the associated tasks.

By leveraging the cloud service scheduler in multi-cloud management, organizations can achieve efficient resource utilization, improved performance, cost optimization, and scalability across their multi-cloud environments.

The cloud service scheduler serves as a central component that handles user requests after authentication. It identifies the appropriate function to execute the task and coordinates the necessary activities. [Figure 4](#) provides an illustration of the associated activities, which can involve additional functions to complete the task successfully.

For instance, when a CSU logs into the multi-cloud management platform via the "uniform user interface" and successfully undergoes authentication and authorization by the "integrated identity management," the user seeks out specific cloud service provider (CSP) services. At this point, the multi-cloud management "cloud service scheduler" initiates the "publish cloud service" activity. This activity, in turn, triggers a series of functions like "service discovery," "service library," and "service catalog" to present a comprehensive list of services to the CSU.

If the CSU wishes to deploy or provision particular services, the "cloud service scheduler" activates the "deployment management" activity. This activity orchestrates a sequence of functions like "provision service" and "service registration" to provision and register the service specifically for the CSU within the chosen CSP, facilitated through the multi-cloud management platform.

Furthermore, other essential functions such as "SLA management" and "Service metering and billing" come into play once a service has been successfully registered under the CSU ensuring seamless service management and accurate billing.

6.3.4.2 Task type: Identifying which cloud service to use

Activities, functions and tasks associated with selecting a cloud service can include:

- Activities:
 - discover cloud service;
 - publish cloud service.
- Functions:
 - service discovery;
 - service library;
 - service publication;