国　际　电　信　联　盟

ITU-T Y.3502

(08/2014)

国际电信联盟
电信标准化部门

Y系列：全球信息基础设施、互联网协议问题、
下一代网络、物联网和智慧城市

云计算

信息技术 – 云计算 – 参考架构

ITU-T Y.3502建议书

ITU-T Y系列建议书

全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市

全球信息基础设施	
概要	Y.100 – Y.199
业务、应用和中间件	Y.200 – Y.299
网络问题	Y.300 – Y.399
接口和协议	Y.400 – Y.499
编号、寻址和命名	Y.500 – Y.599
运营、管理和维护	Y.600 – Y.699
安全	Y.700 – Y.799
性能	Y.800 – Y.899
互联网的协议问题	
概要	Y.1000 – Y.1099
业务和应用	Y.1100 – Y.1199
体系、接入、网络能力和资源管理	Y.1200-Y.1299
传输	Y.1300 – Y.1399
互通	Y.1400 – Y.1499
服务质量和网络性能	Y.1500 – Y.1599
信令	Y.1600 – Y.1699
运营、管理和维护	Y.1700 – Y.1799
计费	Y.1800 – Y.1899
经由NGN的IPTV	Y.1900 – Y.1999
下一代网络	
框架和功能体系模型	Y.2000 – Y.2099
服务质量和性能	Y.2100 – Y.2199
业务方面：业务能力和业务体系	Y.2200 – Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250 – Y.2299
NGN的增强功能	Y.2300 – Y.2399
网络管理	Y.2400 – Y.2499
网络控制体系和协议	Y.2500 – Y.2599
基于分组的网络	Y.2600 – Y.2699
安全	Y.2700 – Y.2799
通用移动性	Y.2800 – Y.2899
运营商水平的开放环境	Y.2900 – Y.2999
未来网络	Y.3000 – Y.3499
云计算	**Y.3500 – Y.3999**
大数据	Y.3600 – Y.3799
量子密钥分发网络	Y.3800 – Y.3999
物联网和智慧城市及社区	
概要	Y.4000-Y.4049
定义和术语	Y.4050-Y.4099
要求和应用案例	Y.4100-Y.4249
基础设施、连接和网络	Y.4250-Y.4399
框架、构架和协议	Y.4400-Y.4549
业务、应用、计算和数据处理	Y.4550-Y.4699
管理、控制和性能	Y.4700-Y.4799
识别与安全	Y.4800-Y.4899
评估与评定	Y.4900-Y.4999

欲进一步了解详细信息，请查阅ITU-T建议书清单。

国际标准ISO/IEC 17789
ITU-T Y.3502建议书

信息技术 – 云计算 – 参考架构

摘要

ITU-T Y.3502建议书 | ISO/IEC 17789为云计算提供了参考架构，其中包括云计算角色、云计算活动以及云计算功能组件及其之间的关系。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T Y.3502	2014-08-13	13	11.1002/1000/12209

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息通信技术（ICT）领域工作的联合国专门机构。国际电联电信标准化部门（ITU-T）是国际电联的一个常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化发布有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，而后由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准ITU-T建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，也指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性的条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才认为达到了本建议书的合规性要求。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已声明的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的、有关已声明之知识产权的证据、有效性或适用性不表明任何意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的、有关受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新的信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

国际标准
ITU-T建议书

信息技术 – 云计算 – 参考架构

1 范围

本建议书 | 国际标准为云计算规定了参考架构（CCRA）。参考架构包括**云计算角色**、**云计算活动**以及**云计算功能组件**及其之间的关系。

2 规范性参考文献

下列建议书和国际标准所包含的条款，通过在本建议书中的引用而构成本建议书 | 国际标准的条款。所注明版本在出版时有效。所有建议书和标准均可能进行修订；因此鼓励根据本建议书 | 国际标准达成协议的各方了解使用最新版本的下列建议书和标准的可能性。IEC和ISO的各成员保存着当前有效的国际标准的目录。国际电联电信标准化局保存着当前有效的ITU-T建议书的清单。

2.1 相同建议书 | 国际标准

– ITU-T Y.3500建议书（2014年）| ISO/IEC 17788:2014，信息技术 – 云计算 – 概述和词汇表。

2.2 其他参考文献

– ISO/IEC 29100:2011，信息技术 – 安全技术 – 隐私框架。

3 定义

出于本建议书 | 国际标准的目的，ITU-T Y.3500建议书 | ISO/IEC 17788中的术语和定义以及以下定义适用。

3.1 他处定义的术语

在ISO/IEC/IEEE 42010中定义了以下术语：

3.1.1 架构：系统在其环境中的基本概念或属性，体现在其元素、关系以及设计和演进的原则中。

在ISO/IEC 29100中定义了以下术语：

3.1.2 个人可识别信息（PII）：（a）可用于识别与此类信息相关的PII主体，或（b）与PII主体直接或间接或者可能直接或间接相关的任何信息。

注 – 为确定PII主体是否可以识别，应考虑持有该数据的隐私利益攸关方或任何其他**方**可合理使用的所有手段，以识别该自然人。

3.2 本建议书 | 国际标准中定义的术语

本建议书 | 国际标准定义了以下术语：

3.2.1 活动：指定的工作或任务集。

3.2.2 云服务产品：云服务，与据其提供云服务的业务条款集相关联。

注 - 业务术语可以包括定价、评级和服务水平。

3.2.3 功能组件：参与**活动**（第3.2.1节）所需的功能构建块，由实施方案支持。

注 - 业务术语可以包括定价，评级和服务水平。

3.2.4 对等云服务：一个**云服务提供商**的**云服务**，作为一个或多个其他**云服务提供商**的**云服务**的一部分。

3.2.5 对等云服务提供商：一个**云服务提供商**，它提供一个或多个**云服务**，供一个或多个其他**云服务提供商**使用，作为其**云服务**的一部分。

3.2.6 **产品目录**：**云服务提供商**可提供给**云服务客户**的所有**云服务产品**（第3.2.2节）的清单。

3.2.7 **角色**：服务于共同目的的一组**活动**（第3.2.1节）。

3.2.8 **服务目录**：特定**云服务提供商**的所有云服务的清单。

3.2.9 **子角色**：给定**角色**（第3.2.7节）的**活动**（第3.2.1节）的一个子集。

4 缩写词

出于本建议书 | 国际标准，以下缩写适用：

API 应用程序接口
CaaS 通信即服务
CCRA 云计算参考架构
CPU 中央处理单元
CS 云服务
CSC 云服务客户
CSN 云服务合作伙伴
CSP 云服务提供商
IaaS 基础设施即服务
ICT 信息通信技术
KPI 关键性能指标
MSA 主服务协议
NaaS 网络即服务
PaaS 平台即服务
PII **个人可识别信息**
QoS 服务质量
RAM 随机访问存储器
SaaS 软件即服务
SLA 服务水平协议
ToS 服务条款
T&C 条款和条件
VLAN 虚拟局域网
VPN 虚拟专用网
VM 虚拟机

5 惯例

以下惯例适用：

1) 在整个本建议书|国际标准中，使用图表来帮助说明CCRA。关于图中的内容，使用了如图5-1所示的惯例。

注 – 在图5.1中，“问题（aspect）”应理解为指的是“跨领域问题”。

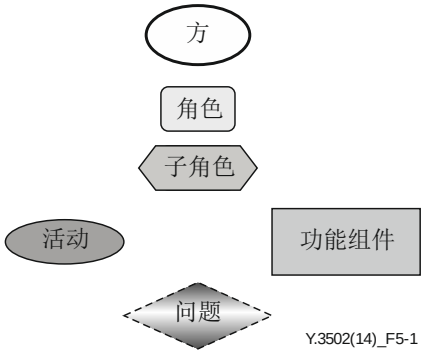


图5-1 – 在整个本建议书 | 国际标准中使用的图表图例

2) 该CCRA使用术语“ICT”和“ICT系统”，其中缩写词ICT代表“信息通信技术”，如ISO/IEC/IEEE 24765第3.1332节中所定义。该术语旨在表明CCRA不仅涵盖与计算机系统相关的计算和存储技术，而且涵盖将系统链接在一起的通信网络。

3) 参考第3节和ITU-T Y.3500建议书 | ISO/IEC 17788中定义的条款，以粗体显示。

6 参考架构的目标和目的

云计算是一种有助于网络以按需、自助提供和管理方式获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。参见ITU-T Y.3500建议书 | ISO/IEC 17788。

本建议书|国际标准中所述的CCRA提供了一个架构框架，它可以有效地描述**云计算角色**、**子角色**、**云计算活动**、跨领域问题以及**云计算**的功能架构和**功能组件**。

CCRA服务以下目标：

- 描述**云计算**的利益攸关方社区；
- 描述**云计算**系统的基本特性；
- 指定基本的**云计算活动**和**功能组件**，并描述其相互之间的关系以及它们与环境的关系；
- 确定指导**CCRA**设计和演变的原则。

CCRA支持以下重要的标准化目标：

- 支持制定一套连贯一致的**云计算**国际标准；
- 为定义**云计算**标准提供技术中立的参考点；
- 鼓励在识别**云计算**收益和风险方面的开放性和透明性。

CCRA侧重于**云服务**提供“什么”的要求，而不是“如何”设计基于云的解决方案和实施方案。CCRA并不代表特定**云计算**系统的系统架构，尽管它可以对特定系统施加约束。CCRA与任何特定供货商的产品、服务或参考实施方案无关；它也没有定义抑制创新的规范性解决方案。

CCRA还旨在：

- 促进对**云计算**操作复杂性的理解；
- 说明并提供对各种**云服务**及其供应和使用的理解；
- 提供技术参考，使国际社会能够理解、讨论、分类和比较**云服务**；
- 成为使用通用参考框架来描述、讨论和开发系统特定架构的工具；
- 促进对安全性、**互操作性**、可移植性、**可逆性**、可靠性和服务管理等领域候选标准的分析，并支持对参考实施方案的分析。

7 参考架构概念

本建议书 | 国际标准定义了一个CCRA，它可以作为**云计算**标准化的基本参考点，为**云计算**系统的基本概念和原则提供了一个总体框架。

本节概述了本建议书|国际标准中使用的架构方法。

7.1 CCRA架构视图

可以使用视点方法来描述**云计算**系统。

CCRA中采用了四种不同的视点（见图7-1）：

- 用户视图；
- 功能视图；
- 实施视图；以及
- 部署视图。

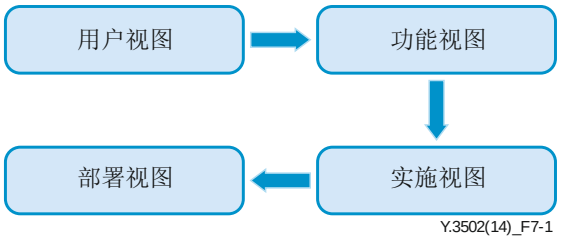


图7-1 – 架构视图之间的转换

表7-1对这些视图中的每一个做了描述。

表7-1 – CCRA视图

CCRA视图	CCRA视图描述	范围
用户视图	系统情形、**各方**、**角色**、**子角色**和**云计算活动**	在范围内
功能视图	支持**云计算活动**所需的功能	在范围内
实施视图	在服务部分和/或基础设施部分内实施**云服务**所需的功能	在范围外
部署视图	如何在现有的基础设施元素内或在此基础设施中引入的新元素内在技术上实现**云服务**的功能	在范围外
注 – 虽然在本建议书	国际标准内阐述了有关用户视图和功能视图的详细内容，但实施视图和部署视图与技术和供货商特定的**云计算**实施方案和实际部署有关，因此不在本建议书	国际标准的讨论范围内。

图7-2显示了从用户视图到功能视图的转换。详情若第7.4节所述。

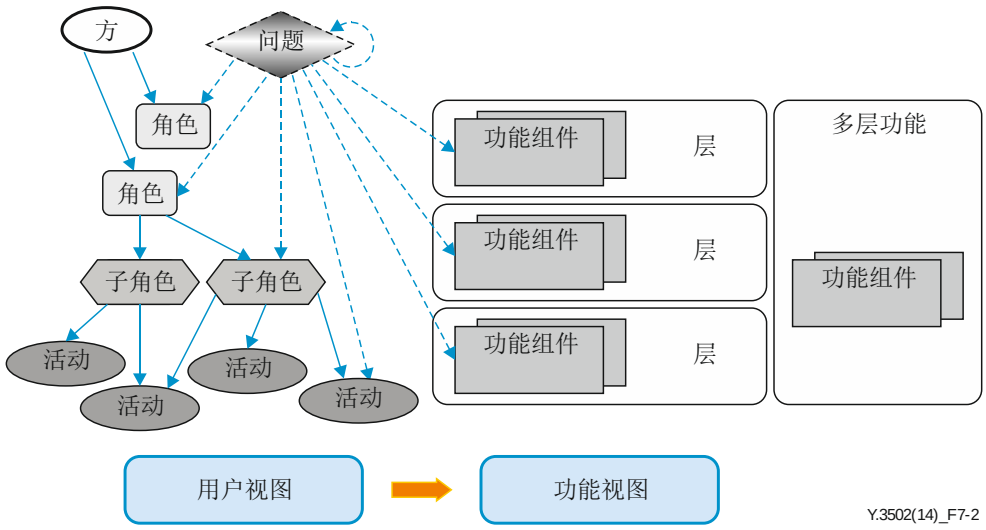


图7-2 – 从用户视图转换为功能视图

7.2 云计算用户视图

用户视图阐述了以下**云计算**概念:

- **云计算活动；**
- **角色**和**子角色；**
- **各方；**
- **云服务；**
- **云部署模型；**
- 跨领域问题。

图7-3说明了为用户视图定义的各实体。

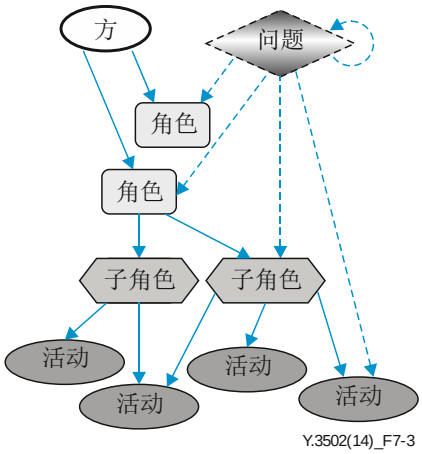


图7-3 – 用户视图实体

7.2.1 云计算活动

云计算活动被定义为指定的工作或任务集。

云计算活动需要有一个目的并交付一个或多个结果。

云计算系统中的**活动**是使用**功能组件**进行的（见第7.3.1节）。

云计算活动在第8节中做了更详细的确定和描述。

7.2.2 角色和子角色

角色是服务于共同目的的一组**云计算活动**。

在CCRA中，定义了三个**角色**：

- **云服务客户（CSC）**：出于使用**云服务**的目的，存在业务关系的一个**参与方**。
- **云服务提供商（CSP）**：提供**云服务**的一个**参与方**。
- **云服务合作伙伴（CSN）**：为**云服务提供商**或**云服务客户**或二者提供支持或辅助的一个**参与方**。

子角色是给定**角色**的**云计算活动**的一个子集。

不同的**子角色**可以共享与给定**角色**相关联的**云计算活动**。

第8节提供了对**云计算角色**和**子角色**的描述。

7.2.3 各方

一个**参与方**指的是一个自然人或法人，无论是否合并或是二者的一个团体。**云计算**系统中的**各方**是其利益攸关方。

一个**参与方**可以在任何给定时间点承担多个**角色**，并可以参与该**角色**的特定**活动**子集。各方的例子包括但不限于大公司、中小规模企业、政府部门、学术机构和公民个人。

7.2.4 云服务

云服务是**云计算**的基本要素。ITU-T Y.3500建议书 | ISO/IEC 17788涵盖了**云服务**。本节提供了一个概述。

基于**云服务**提供的资源，可以根据它们提供的**云功能类型**来描述**云服务**。有三种**云功能类型**：

- **应用能力类型；**
- **平台能力类型；**
- **基础设施能力类型。**

ITU-T Y.3500建议书 | ISO/IEC 17788涵盖了**云功能类型**和**云服务类别**。

云服务也分为多个类别，当中的每个类别是一组拥有共同质量的**云服务**。这些类别中的服务可包括来自上述一种或多种**云功能类型**的功能。

代表性的**云服务类别**包括：

- **基础设施即服务（IaaS）；**
- **平台即服务（PaaS）；**
- **软件即服务（SaaS）；**
- **网络即服务（NaaS）。**

在ITU-T Y.3500建议书 | ISO/IEC 17788中对其他**云服务类别**做了描述。

7.2.5 云部署模式

ITU-T Y.3500建议书 | ISO/IEC 17788涵盖了**云部署模型**。本节提供了一个概述。

云部署模式是指在控制和共享物理或虚拟资源的基础上用于组织**云计算**的方式。

云部署模式包括：

- **公有云；**
- **私有云；**
- **社区云；**
- **混合云。**

7.2.6 跨领域问题

跨领域问题指的是行为或功能，需要在**角色**间对之进行协调，并在一个**云计算**系统中一致地予以实施。

跨领域问题可以共享，并可影响多个**角色**、**云计算活动**和**功能组件**。

跨领域问题适用于多个单独的**角色**或**功能组件**。

跨领域问题的一个例子是安全性。

第8.5节提供了对跨领域问题的描述。

7.3 云计算的功能视图

功能视图是形成**云计算**系统所需之功能的技术中立视图。功能视图描述了支持**云计算活动**所需的功能分布。

功能架构还定义了功能与功能之间的依赖关系。

功能视图阐述了以下**云计算**概念：

- **功能组件**；
- 功能层；以及
- 多层功能。

图7-4说明了功能、层和**功能组件**的概念。

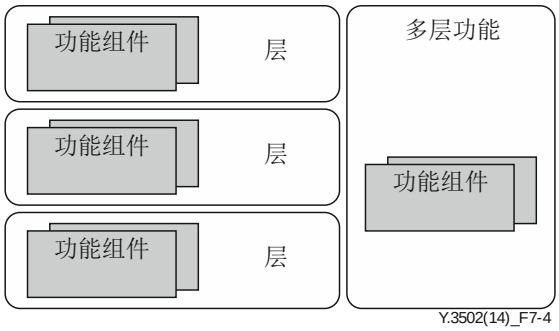


图7-4 – 功能分层

云计算功能架构在第9.1节中描述。

7.3.1 功能组件

功能组件是参与**活动**所需的功能构建块，由实施方案支持。

云计算系统的功能完全由已实现的**功能组件**集来定义。

第9.2节进一步描述了**功能组件**。

7.3.2 功能层

一层指的是一组提供类似功能或服务共同目的的**功能组件**。

功能架构是部分分层的（即有若干层和一组多层功能）。

在CCRA中定义了四个不同的层：

- 用户层，包括支持**云服务客户**和**云服务合作伙伴**之**云计算活动**的**功能组件**；
- 接入层，包括促进功能分布和互连的**功能组件**；
- 服务层，包括提供**云服务**本身的**功能组件**以及相关的管理和业务能力，以及实现它们所需的编排能力；

- 资源层，包括表示实现**云计算**系统所需资源的**功能组件**。

注意：并非所有层或**功能组件**都必须在某个特定的**云计算**系统中实例化。

7.3.3 多层功能

多层功能包括提供跨多个功能层使用之能力的**功能组件**。

多层功能被分组为子集。

定义了以下多层功能的子集：

- 开发支持；
- 集成；
- 安全系统;
- 运营支持系统；
- 业务支持系统。

多层功能的**功能组件**在第9.2.5节中进行描述。

7.4 用户视图与功能视图之间的关系

图7-5说明了用户视图如何提供在功能视图中表示的**云计算活动**集（并使用实施视图的技术来实现）。

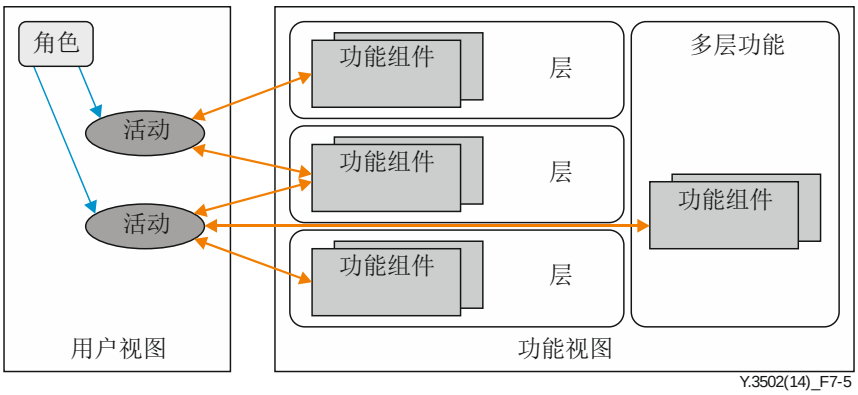


图7-5 – 从用户视图到功能视图

有关用户视图与功能视图之间关系的更多详细信息，请参见第10节。

7.5 用户视图和功能视图与跨领域问题的关系

跨领域问题，顾名思义，适用于**云计算**的用户视图和功能视图。

跨领域问题适用于用户视图中的**角色**和**子角色**，它们直接或间接影响这些**角色**执行的**活动**。

跨领域问题也适用于功能视图内的**功能组件**，在执行用户视图中描述的**活动**时使用这些组件。

第8.5条中描述的**云计算**的跨领域问题包括：

- 可审性；
- **可用性**；
- 治理；
- **互操作性**；
- 维护和版本控制；

- 性能；
- 便携性；
- **个人可识别信息**的保护；
- 监管；
- 适应性；
- **可逆性**；
- 安全性；
- 服务水平和**服务水平协议**。

7.6 云计算的实施视图

虽然在本建议书 | 国际标准中阐述了用户视图和功能视图的详细信息，但实施视图超出了本建议书 | 国际标准的讨论范围。

7.7 云计算的部署视图

虽然在本建议书 | 国际标准中阐述了用户视图和功能视图的详细信息，但部署视图超出了本建议书 | 国际标准的讨论范围。

8 用户视图

8.1 角色、子角色和云计算活动介绍

鉴于分布式服务及其交付是**云计算**的核心，所有与**云计算**有关的**活动**都可分为三大类：使用服务的**活动**、提供服务的**活动**和支持服务的**活动**。

本节包含与**云计算**关联的一些常见**角色**和**子角色**的描述。

重要的是要注意，**一方**可以在任何给定时间点扮演多个**角色**。在扮演**角色**时，**一方**可以限制自己扮演一个或多个**子角色**。**子角色**是给定**角色**的**云计算活动**的一个子集。

如图8-1所示，**云计算**的**角色**是：

- 云服务客户（第8.2节）
- 云服务提供商（第8.3节）；
- 云服务合作伙伴（第8.4节）。

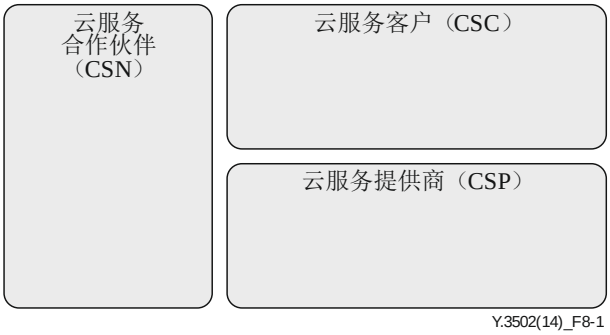


图8-1 – 云计算角色

图8-2显示了**云计算**的**角色**及其相关的**子角色**。对图中所示的每个**子角色**，都将在以下各节中予以更详细的描述。

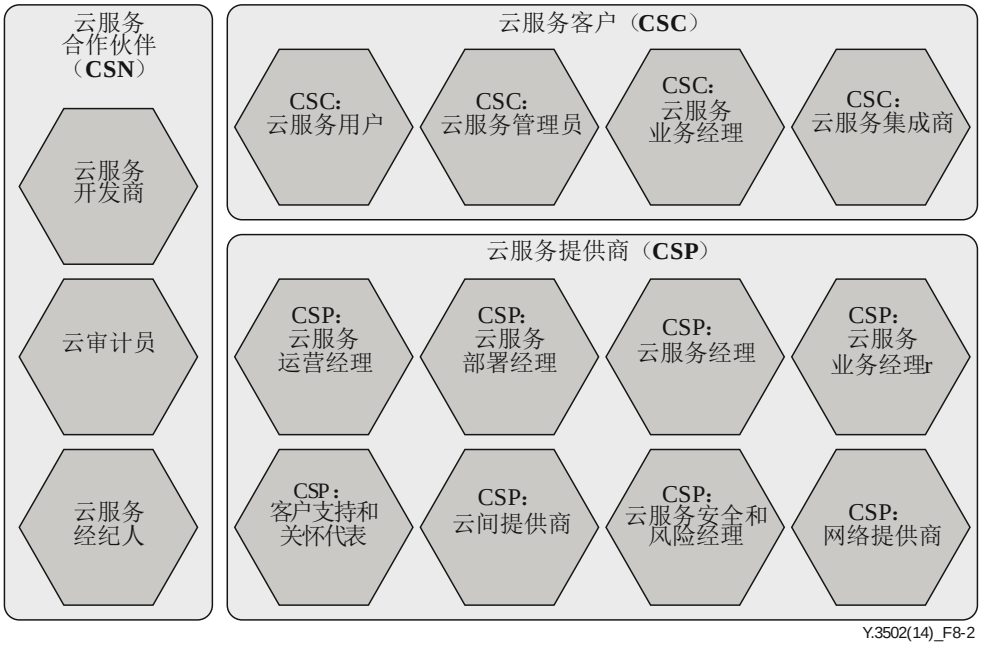


图8-2 – 角色和子角色

8.2 云服务客户

8.2.1 角色

出于使用**云服务**的目的，**云服务客户**（CSC）与**云服务提供商**存在业务关系。出于各种各样的目的，**云服务客户**还可以与**云服务合作伙伴**建立业务关系。

云服务客户的活动包含在第8.2.1.1节至第8.2.1.4节所述的**子角色**之下。

8.2.1.1 CSC：云服务用户

CSC：云服务用户是与使用**云服务**的**云服务客户**相关联的自然人或代表其行事的实体所对应的**云服务客户**的**子角色**。

CSC：云服务用户的**云计算活动**包括：

- 使用**云服务**（第8.2.2.1节）。

8.2.1.2 CSC：云服务管理员

CSC：云服务管理员是**云服务客户**的一个**子角色**，其主要目标是确保客户顺利使用**云服务**，并确保这些**云服务**与客户现有的ICT系统和应用能一起良好运转。CSC：云服务管理员监督与使用**云服务**相关的所有操作流程，并充当**云服务客户**与**云服务提供商**之间技术沟通的联络人。

CSC：云服务管理员的**云计算活动**包括：

- 进行服务试用（第8.2.2.2节）；
- 监测服务（第8.2.2.3节）；
- 管理服务安全性（第8.2.2.4节）；
- 提供计费和使用报告（第8.2.2.5节）；
- 处置问题报告（第8.2.2.6节）；
- 管理租户（第8.2.2.7节）。

8.2.1.3 CSC：云服务业务经理

CSC：云服务业务经理是**云服务客户**的一个**子角色**，它旨在通过以成本高效的方式获取和使用**云服务**来满足**云服务客户**的业务目标。CSC：云服务业务经理的主要职责涉及**云服务**使用的财务和法律方面问题，包括批准、持续所有权和问责制。

CSC：云服务业务经理的**云计算活动**包括：

- 执行业务管理（第8.2.2.8节）；
- 选择和购买服务（第8.2.2.9节）；
- 请求审计报告（第8.2.2.10节）。

8.2.1.4 CSC：云服务集成商

CSC：云服务集成商是**云服务客户**的一个**子角色**，它负责将**云服务**与**云服务客户**现有的ICT系统相集成，包括应用功能和数据。

CSC：云服务集成商的**云计算活动**包括：

- 将ICT系统连接到**云服务**（第8.2.2.11节）。

8.2.2 云计算活动

与**云服务客户**的**子角色**有关的**云计算活动**如图8-3所示。

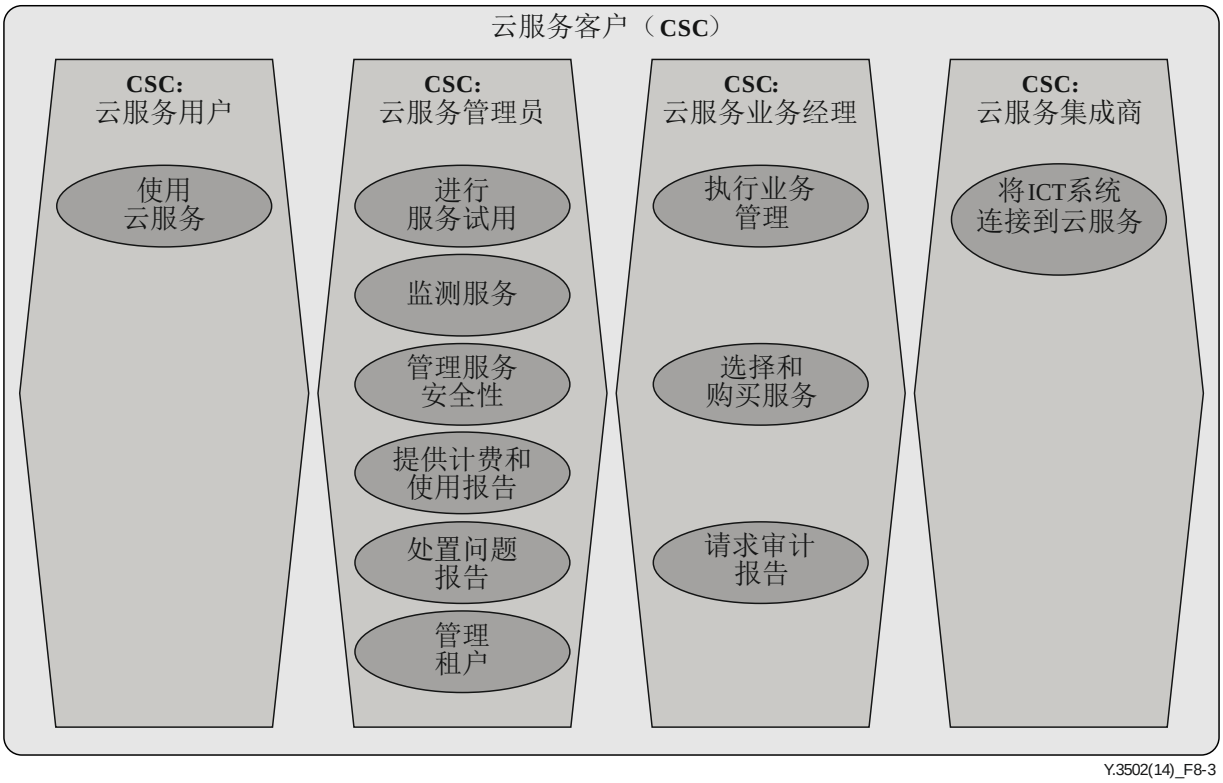


图8-3 – 与云服务客户子角色有关的云计算活动

8.2.2.1 使用云服务

使用**云服务活动**涉及使用**云服务提供商**的服务，以完成某些任务。

使用**云服务活动**通常涉及：

1) 提供用户凭证，使**云服务提供商**能够对用户进行身份验证并授予对**云服务**的访问权限；
2) 调用**云服务**，而后运行并交付其指定的结果。

8.2.2.2 进行服务试用

进行服务试用**活动**涉及使用**云服务提供商**的服务，以确保**云服务**适合**云服务客户**的业务需求。**云服务**在**云服务提供商**与**云服务客户**之间相互同意和理解的基础上进行试用。

进行服务试用**活动**包括：

1) 提供用户凭证，使**云服务提供商**能够对用户进行身份验证并授予对“试用”的云服务的访问权限；
2) 调用“试用”的云服务，出于业务目的，它可以由**云服务客户**来进行测试。

8.2.2.3 监测服务

监测服务**活动**依据**云服务客户**与**云服务提供商**之间**服务水平协议（SLA）**中定义的服务水平来监测交付的服务质量。

本**活动**利用云系统的内在监测功能。本**活动**涉及：

- 跟踪每项**云服务**的使用量以及用户的使用情况。这包括确保使用恰当；
- 监测**云服务**与客户现有ICT系统的集成，以确保实现业务目标；
- 定义与相关服务有关的测量点和性能指标（例如，服务**可用性**、服务中断频率、平均修复时间、提供商咨询台的响应能力等）；
- 监测、分析和归档这些指标数据；
- 将提供的实际服务质量与约定的服务质量进行比较。

8.2.2.4 管理服务安全性

管理服务安全性**活动**涉及：

- 确保放置在**云计算**环境中的**云服务客户数据**的适当安全性；
- 制定数据备份和恢复计划，以及潜在的数据复制和故障恢复计划；
- 管理安全政策；
- 定义加密和**完整性**技术，以应用于静态和动态的**云服务客户数据**；
- 定义如何处置**云服务客户数据**中的任何**个人可识别信息（PII）**。

8.2.2.5 提供计费和使用报告

提供计费和使用报告**活动**涉及准备关于客户组织使用**云服务**的报告以及与该使用有关的计费/发票数据相关报告。这些报告提供给CSC：业务经理。

8.2.2.6 处置问题报告

处理问题报告**活动**涉及客户方处置与使用**云服务**相关的任何报告的问题。这包括：

- 评估每个问题的影响；
- 排除故障以确定问题的原因；
- 向**云服务提供商**开具问题报告并跟踪解决；
- 制定解决问题的变通办法；
- 未在商定的时间范围内得到解决或对业务产生严重影响的问题不断升级。

8.2.2.7 管理租户

管理租户**活动**涉及管理**云服务客户**与**云服务提供商**的租户。本**活动**涉及：

- 配置和控制安全方面问题，包括用户帐户、安全**角色**、身份和权限；
- 识别和控制**租户**内用户之间共享的数据；
- 创建和删除**租户**；
- 管理用户和分配给**租户**的资源；
- 为每个**租户**定义执行策略。

8.2.2.8 执行业务管理

执行业务管理**活动**涉及对使用**云服务**的业务问题管理，包括会计和财务管理。本**活动**包括：

- 调整业务计划以适应**云服务**的使用；
- 跟踪服务的使用并处理会计和财务管理；
- 处置从**云服务提供商**处收到的、有关**云服务**使用的账单/发票；
- 确保计费与**云服务客户**对**云服务**的实际使用相匹配；
- 向**云服务提供商**付款；
- 保留与**云服务**使用有关的帐户。

8.2.2.9 选择和购买服务

选择和购买服务**活动**涉及：

- 检查（一个或多个）**云服务提供商**的**云服务**产品，以确定所提供的服务是否满足**云服务客户**的业务和技术要求。这通常涉及阅读**产品目录**和每项服务的文档，当中可包括有关服务及其**SLA**的技术信息，以及包括定价在内的业务信息；
- 协商**云服务**的条款（如果**云服务提供商**允许服务的可变条款）；
- 接受**云服务**合同并在**云服务提供商**处进行注册。

8.2.2.10 请求审计报告

请求审计报告**活动**涉及**云服务客户**请求**云服务**审计报告，通常符合特定审计标准或方案。**云服务客户**可以请求**云审计员**或可能请求**云服务提供商**提供报告，尽管审计报告预计由独立于**云服务提供商**的实体来准备，两种情况都在购买完成之前进行，并且一旦该服务投入使用，将需定期准备。

8.2.2.11 将ICT系统连接到云服务

将ICT系统连接到**云服务活动**包括现有ICT系统与**云服务**之间的集成，并涉及现有ICT组件和应用与目标**云服务**的连接，以及客户监测和管理系统与**云服务提供商**对**云服务**监测和控制的连接。

现有ICT组件和应用与目标**云服务**的连接涉及：

- 评估**云服务**对现有流程、系统和服务的影响；
- 在**云服务客户**现有的ICT 系统与**云服务**之间映射业务数据；
- 从现有的 ICT 组件和应用处调用**云服务**操作，并提供输入数据和处置输出数据；
- 为CSC：云服务用户提供访问权限；
- 定义和实施安全相关要求，包括数据流的**机密性**和**完整性**；
- 将用于管理用户帐户、安全**角色**、身份和权限的客户设施与用于**云服务**的等效设施相集成；
- 创建和监测特定用户帐户和身份以使用有关**云服务**的管理接口；
- 在**云服务**与**云服务客户**监测和管理基础设施之间集成日志记录和安全事件管理。

8.3 云服务提供商

8.3.1 角色

云服务提供商（CSP）向**云服务客户**提供**云服务**。该**角色**（及其所有**子角色**）侧重于提供**云服务**所需的**云计算活动**，以及确保将其交付给**云服务客户**以及**云服务**维护所需的**云计算活动**。

云服务提供商负责处理与**云服务客户**的业务关系。

云服务提供商的**活动**包含在第 8.3.1.1节至第8.3.1.8节中所描述的各**子角色**之下。

8.3.1.1 CSP：云服务运营经理

CSP：云服务运营经理是**云服务提供商**的一个**子角色**，负责执行**云服务提供商**的所有运营流程和程序，确保所有服务和相关基础设施满足运营目标。

CSP：云服务运营经理的**云计算活动**包括：

- 准备系统（第8.3.2.1节）；
- 监测和管理服务（第8.3.2.2节）；
- 管理资产和库存（第8.3.2.3节）；
- 提供审计数据（第8.3.2.4节）。

8.3.1.2 CSP：云服务部署经理

CSP：云服务部署经理是**云服务提供商**的一个**子角色**，负责计划将服务部署到生产中。这包括定义服务的操作环境、部署服务及其依赖项的初始步骤，以及启用在服务运行期间使用的操作流程。

CSP：云服务部署经理的**云计算活动**包括：

- 定义环境和流程（第8.3.2.5节）；
- 定义和收集指标（第8.3.2.6节）；
- 定义部署步骤（第8.3.2.7节）。

8.3.1.3 CSP：云服务经理

CSP：云服务经理是**云服务提供商**的一个**子角色**，负责确保**云服务提供商**的服务可供**云服务客户**使用，并确保其正常运行和符合**服务水平协议**中指定的目标。CSP：云服务经理还负责确保**云服务提供商**业务支持系统和运营支持系统的顺利运行，以及提供给**云服务客户**和**云服务合作伙伴**、用于管理和其他**云计算活动**的其他功能的良好运行。

CSP：云服务经理的**云计算活动**包括：

- 提供服务（第8.3.2.8节）；
- 部署和提供服务（第8.3.2.9节）；
- 执行服务水平管理（第8.3.2.10节）。

8.3.1.4 CSP：云服务业务经理

CSP：云服务业务经理是**云服务提供商**的一个**子角色**，全面负责向**云服务客户**提供**云服务**的业务方面问题。CSP：云服务业务经理创建和跟踪业务计划，定义服务提供策略并管理与**云服务客户**之间的业务关系。

CSP：云服务业务经理的**云计算活动**包括：

- 管理业务计划，以提供**云服务**（第8.3.2.11节）；
- 管理客户关系（第8.3.2.12节）；
- 管理财务处理（第8.3.2.13节）。

8.3.1.5 CSP：客户支持和关怀代表

CSP：客户支持和关怀代表是**云服务提供商**的一个**子角色**，是**云服务客户**与**云服务提供商**的主要接口，负责以及时和成本高效的方式对客户问题和询问做出响应，目标是保持客户对**云服务提供商**及所提供**云服务**的满意度。

CSP：客户支持和关怀代表的**云计算活动**包括：

- 处置客户请求（第8.3.2.14节）。

8.3.1.6 CSP：云间提供商

CSP：云间提供商是**云服务提供商**的一个**子角色**，依赖一个或多个**对等云服务提供商**来提供该CSP：云间提供商向**云服务客户**提供的部分或全部**云服务**。CSP：云间提供商的主要活动是从**云服务客户**的角度对**对等云服务提供商**的**云服务**及其业务和管理能力进行中介、聚合、套利、对等或联邦，以便**云服务客户**只使用云间服务提供商的服务 、业务和管理接口。

CSP：云间提供商的**云计算活动**包括：

- 管理**对等云服务**（第8.3.2.15节）；
- 执行对等、联邦、中介、聚合和套利（第8.3.2.16节）。

8.3.1.7 CSP：云服务安全和风险经理

CSP：云服务安全和风险经理是**云服务提供商**的一个**子角色**，负责确保**云服务提供商**适当地管理与**云服务**的开发、交付、使用和支持相关的风险。这包括确保**云服务客户**和**云服务提供商**的**信息安全**策略保持一致并满足**SLA**中规定的安全要求。

CSP：云服务安全和风险经理的**云计算活动**包括：

- 管理安全和风险（第8.3.2.17节）；
- 设计和实施服务连续性（第8.3.2.18节）；
- 确保合规（第8.3.2.19节）。

8.3.1.8 CSP：网络提供商

CSP：网络提供商是**云服务提供商**的一个**子角色**，为**云服务客户**、**云服务合作伙伴**和**云服务提供商**提供网络连接和网络服务。CSP：网络提供商可在**云服务提供商**数据中心内的系统与系统之间提供网络连接，或者在**云服务提供商**的系统与提供商数据中心外的系统之间提供网络连接，例如，**云服务客户**系统或属于其他**云服务提供商**的系统。

CSP：网络提供商的**云计算活动**包括：

- 提供网络连接（第8.3.2.20节）；
- 交付网络服务（第8.3.2.21节）；
- 提供网络管理服务（第8.3.2.22节）。

CSP：网络提供商还可以选择将网络连接的动态控制作为**NaaS**来提供。

8.3.2 云计算活动

与**云服务提供商**的**子角色**有关的**云计算活动**如图8-4所示。

图8-4 – 与云服务提供商子角色有关的云计算活动

8.3.2.1 准备系统

准备系统**活动**侧重于为新的**云服务**部署准备有关提供商环境的系统。本**活动**涉及：

- 评估新服务部署或现有服务使用增加的影响；
- 修改或扩展数据中心的资源以满足新部署的需要。

8.3.2.2 监测和管理服务

监测和管理服务**活动**侧重于监测和管理服务及其相关基础设施，包括用户和系统权限。本**活动**涉及：

- 监测**云服务提供商**的服务和基础设施；
- 捕获对提供商的业务而言很重要的事件和数据，并以对CSP：云服务业务经理很重要的形式来呈现这些数据。此类信息包括诸如**云服务客户**对**云服务**的使用情况以及提供这些服务的成本等科目；
- 管理网络基础设施，包括路由器、域名服务器、IP地址、虚拟专用网络（VPN）、防火墙和内容过滤；
- 分配和管理存储；
- 管理用户和系统权限；
- 配置和维护操作系统与管理程序；
- 管理虚拟化环境；

- 监测**云服务提供商**的ICT环境的行为，以确保其正确运行以及所提供**云服务**符合**SLA**的条款要求；
- 记录问题，适当地报告问题（这可涉及向一个或多个客户发送的消息），并遵循问题解决流程，直到问题得到解决。

8.3.2.3 管理资产和库存

管理资产和库存**活动**涉及：

- 跟踪所有计算、存储、网络和软件资产以及它们之间的关系。这包括跟踪诸如版本和补丁级别等方面，以及相关的配置信息；
- 新资产的“加入”和旧资产的处置。这可包括确保新资产适合目的，并从安全性和可管理性的角度做了适当的检查，还可包括处置不再需要的资产。这可包括对可能持有数据的任何资产进行适当的安全处置。

8.3.2.4 提供审计数据

提供审计数据**活动**是收集和提供与审计请求相关的数据，例如，与安全控制或服务性能有关的数据。所请求的数据将取决于正在使用的审计方案或标准。本**活动**涉及：

- 从日志等创建和发送适当的审计信息；
- 从可能包含敏感信息或**PII**的任何日志记录或其他数据中编辑信息。

8.3.2.5 定义环境和流程

定义环境和流程**活动**侧重于定义服务运行时使用的所需技术环境和操作流程。本**活动**涉及：

- 在计算、存储和网络资源、包括配置在内的软件依赖性方面定义所需的技术环境；
- 为响应不断变化的使用需求定义扩大和缩小资源使用的策略和流程；
- 确保**云服务**遵守与安全性和业务合规性有关的适当标准；
- 定义服务运行时要遵循的流程，包括修复、升级和迁移计划。

8.3.2.6 定义和收集指标

定义和收集指标**活动**侧重于定义服务水平指标和管理。本**活动**涉及：

- 定义与**云服务**运营有关的指标，这些指标通常体现在与这些服务有关的**SLA**中；
- 设计如何为每个**云服务**捕获指标；
- 定义如何报告和管理指标，特别是确保满足**SLA**目标。

8.3.2.7 定义部署步骤

定义部署步骤**活动**侧重于定义服务部署的步骤。本**活动**涉及描述运营和支持团队需要采取的每个步骤，以便服务实施方案得到部署并准备好供**云服务客户**使用。

8.3.2.8 提供服务

提供服务**活动**涉及向其**云服务客户**提供**云服务**所需的所有步骤。提供服务**活动**包括接受和处理来自用户的服务调用以及用户身份的相关认证和授权。服务调用的处理是通过服务实施方案的实例来完成的，这又可以涉及其他服务的组合和调用，这取决于服务实施方案的设计和配置。

提供服务**活动**还涉及以下内容：

- 管理服务故障处置过程；
- 管理业务支持系统和运营支持系统；
- 维护服务和底层基础设施；
- 自动化系统流程；

- 管理长期容量和性能趋势；
- 为**云服务提供商**数据中心的计算、存储和网络功能所需的硬件安装、配置和执行维护更新；
- 安装和配置运行云提供商的数据中心和支持**云服务**实施方案所需的软件。这包括根据需要对该软件采取修复、更新和升级措施。

8.3.2.9 部署和提供服务

部署和供应服务**活动**涉及让服务实施方案运行并使之在CSC：云服务用户可访问的网络端点上可用，并使之能够处置来自用户的服务请求。本**活动**包括：

- 遵循为服务定义的部署流程。

注 – 本活动还涵盖取消部署和取消提供云服务所需的流程。

8.3.2.10 执行服务水平管理

执行服务水平管理**活动**侧重于管理与**SLA**目标的合规性。本**活动**涉及：

- 监测每项服务的指标，并将它们与服务**SLA**要求的服务目标进行比较；
- 在指标不符合**SLA**要求的值时采取行动，使服务重新符合**SLA**，例如，通过遵循CSP：云服务部署经理制定的程序；
- 如果无法保持合规性，则报告问题。

8.3.2.11 管理业务计划

管理商业计划**活动**涉及：

- 定义服务产品，描述产品的技术方面问题（功能接口、**SLA**等）和产品的业务方面问题；

  注 – 在建立服务产品时，**云服务提供商**可以考虑与**对等云服务提供商**交互有关的问题。
- 制定业务计划，涵盖向客户提供一项或多项**云服务**、处置服务的财务和技术问题、目标客户群、合同和**SLA**、市场渠道、销售目标等；
- 根据计划跟踪销售和服务使用情况，以确保实现**云服务提供商**的财务目标；
- 准备业务计划并调整业务计划以提供**云服务**。

8.3.2.12 管理客户关系

管理客户关系**活动**涉及管理**云服务提供商**与**云服务客户**的业务关系，包括：

- 创建和维护**产品目录**的内容；
- 获取客户；
- 为客户提供有关所有业务事宜的联络点；
- 讨论和解决客户提出的疑虑或问题；
- 处理变更请求（例如，权利变更）。

8.3.2.13 管理财务处理

管理财务处理**活动**涉及：

- 处理计费更新或挑战；
- 生成与使用**云服务**有关之费用的计费信息和/或发票，并将计费信息或发票传输给**云服务客户**；
- 处置收到来自**云服务客户**的付款及其会计处理。

8.3.2.14 处置客户请求

处置客户请求**活动**涉及：

- 处置来自**云服务客户**的支持请求、报告和事件，无论收到什么。可以为客户提供多种沟通方式，从论坛、电子邮件、客户支持台系统或门户网站，到与提供商支持人员的实时沟通；

注 – 一些请求或报告仅需要提供信息或澄清细节。其他请求和报告可能需要问题分析，或者它们可能涉及创建变更请求。

8.3.2.15 管理对等云服务

管理对等**云服务活动**侧重于管理**对等云服务提供商**之**云服务**的使用。本**活动**涉及：

- 选择和使用**对等云服务提供商**的一项或多项服务；
- 监测和管理**对等云服务提供商**的**云服务**，以确保它们满足商定的**SLA**目标，包括报告和解决这些服务存在的问题；
- 管理**对等云服务提供商**的**云服务**的业务问题，包括业务计划和财务处理；
- 跟踪**对等云服务提供商**的各**云服务**的使用量和用户，包括确保使用是适当的并在业务计划内；
- 监测**对等云服务提供商**的**云服务**与服务实施方案的集成，以确保实现业务目标；
- 协调**云服务客户**与所有**对等云服务提供商**之间的身份和安全证书。

8.3.2.16 执行对等、联邦、中介、聚合和套利

执行对等、联邦、中介、聚合和套利**活动**涉及以特定方式使用**对等云服务提供商**的**云服务**：

- 对等指的是使用**对等云服务提供商**的**云服务**；
- 联邦涉及使用一组**对等云服务提供商**（它们相互组合其服务能力）的**云服务**，以便提供客户要求的**云服务**集。
- 中介涉及**云服务提供商**提供基于调节或增强**对等云服务提供商**之**云服务**的**云服务**。增强功能的例子包括管理对**云服务**的访问、提供**云服务**应用程序编程接口（API）“外立面”、身份管理、性能报告、增强的安全性等；
- 聚合涉及**云服务提供商**提供基于**对等云服务提供商**提供之服务集组合的**云服务**。
- 套利涉及提供**云服务**的**云服务提供商**，它基于从**对等云服务提供商**提供的一组服务中选择一项服务。

8.3.2.17 管理安全和风险

管理安全和风险**活动**侧重于管理与**云服务**的开发、交付、使用和支持相关的安全和风险。本**活动**涉及：

- 定义**信息安全**政策 – 考虑服务要求、法律和监管要求以及合同和**SLA**义务；
- 定义与**云服务**有关的**信息安全**风险以及满足**云服务提供商**业务目标的风险处理方法。此处的一个重点是管理**信息安全**风险存在一定的相关成本，提供商可采取不处置某些风险的业务立场，而是通过服务协议将这些风险的责任转移给**云服务客户**，以解决市场某些部分的成本要求问题。
- 选择解决与所选服务和设计点相关的风险问题所需的设计点和相关**信息安全**控制。这些控制通常涵盖一组类别，例如：
  - 身份和访问管理；
  - 发现、分类、保护数据和信息资产；
  - 信息系统的获取、开发和维护；
  - 保护基础设施免受威胁和漏洞影响；
  - 问题和**信息安全事件**管理；
  - 安全治理和合规性；
  - 人身和人员安全；
  - 网络和通信安全；
  - 隔离（多租户情况下的**租户**之间）。
- 确保为已部署的服务和底层基础设施实施确定的控制措施；
- 设计、实施和评估系统和应用的安全性；
- 管理、设计、实施和评估**对等云服务提供商**之**云服务**的安全性；
- 评估所实施控制措施的有效性，并根据经验进行改变；
- 确保运营和业务支持系统根据向其提供服务的特定**云服务客户租户**向**云服务提供商**员工提供数据访问。

8.3.2.18 设计和实施服务连续性

设计和实施服务连续性**活动**涉及：

- 考虑**云服务**和支持基础设施的潜在故障模式，并通过故障转移和冗余等技术实施恢复流程，使**云服务**能够在**SLA**条款内可用。

8.3.2.19 确保合规

确保合规**活动**侧重于实现法规和标准合规。本**活动**涉及：

- 确保**云服务**及其支持基础设施的实施方案符合任何需要支持之标准的要求，例如，目标客户集可以要求这些标准，或者提供商选择的认证方案可以要求这些标准，以确保达成服务；
- 确保**云服务**及其支持基础设施（包括数据处置）的实施方案符合对服务或对服务存储或处理之数据可能存在的任何监管要求。

8.3.2.20 提供网络连接

提供网络连接**活动**涉及建立所请求的网络连接和相关能力，包括（除其他外）**云服务客户**与**云服务提供商**系统之间以及一个**云服务提供商**系统与另一个**云服务提供商**系统之间的连接。这可包括建立诸如VPN或专用带宽连接等设施。

网络能力包括为所有**云服务类别**以及在**NaaS**情况下为云和非云目的提供适当的有界延迟、抖动、带宽、服务质量和可靠性的能力。

8.3.2.21 交付网络服务

交付网络服务**活动**涉及提供网络相关服务，例如，防火墙或负载平衡。

8.3.2.22 提供网络管理服务

提供网络管理服务**活动**侧重于管理用于承载**云服务**的网络基础设施。本**活动**提供允许操作、管理、维护和供应云网络基础设施的方法、工具和程序。它包括以下任务：

- 保持网络正常运行；
- 跟踪网络中的资源及其分配方式；
- 进行维修和升级，例如，当设备必须更换或升级为新功能时；
- 配置网络中的资源以支持**云服务**。

8.4 云服务合作伙伴

8.4.1 角色

一个**云服务合作伙伴（CSN）**即一个**参与方**，它为**云服务提供商**和/或**云服务客户**的**活动**提供支持或辅助。

一个**云服务合作伙伴**的**云计算活动**会因合作伙伴的类型及其与**云服务提供商**和**云服务客户**之间的关系而有所不同。

8.4.1.1 云服务开发商

云服务开发商是**云服务合作伙伴**的一个**子角色**，负责设计、开发、测试和维护**云服务**的实施方案。这可涉及从现有服务实施方案组合服务实施方案。

云服务开发商的**云计算活动**包括：

- 设计、创建和维护服务组件（第8.4.2.1节）；
- 组合服务（第8.4.2.2节）；
- 测试服务（第8.4.2.3节）。

注1 – 云服务集成商和云服务组件开发商描述了云服务开发商的**子角色**，当中云服务集成商负责处置来自其他服务的某项服务的组合，而云服务组件开发商负责处置单个服务组件的设计、创建、测试和维护。

注2 – 这包括涉及与**对等云服务提供商**交互的服务实现和服务组件。

8.4.1.2 云审计员

云审计员是**云服务合作伙伴**的一个**子角色**，负责对云服务的供应和使用进行审计。云审计通常涵盖操作、性能和安全性，并检查是否满足一组指定的审计标准。审计标准有多种规范，例如，ISO/IEC 27002论述了安全性方面的考虑。

云审计员的**云计算活动**包括：

- 执行审计（第8.4.2.4节）；
- 报告审计结果（第8.4.2.5节）。

8.4.1.3 云服务经纪人

云服务经纪人是**云服务合作伙伴**的一个**子角色**，负责协商**云服务客户**与**云服务提供商**之间的关系。**云服务经纪人**本身不是**云服务提供商**，不应与**云间提供商**的**角色**混淆（见第8.3.1.6节）。**云服务经纪人**角色可以与云间提供商的角色结合或独立运作。

云服务经纪人的**云计算活动**包括：

- 获取和评估客户（第8.4.2.6节）；
- 评估市场（第8.4.2.7节）；
- 建立法律协议（第8.4.2.8节）。

市场评估可以在客户获取之前进行，与**云服务提供商**建立预先协议，这可以使**云服务客户**能够从**服务目录**中选择**云服务提供商**，可能在选择时协商服务细节（例如，服务水平目标）。

在任一情况下，**云服务经纪人**仅在服务的签约阶段在**云服务客户**与**云服务提供商**之间起作用。在消费服务的过程中不涉及**云服务经纪人**。在此类情况下，**活动**涉及**云服务提供商**的**活动**。

8.4.2 云计算活动

与**云服务合作伙伴**的**子角色**有关的**云计算活动**如图8-5所示。

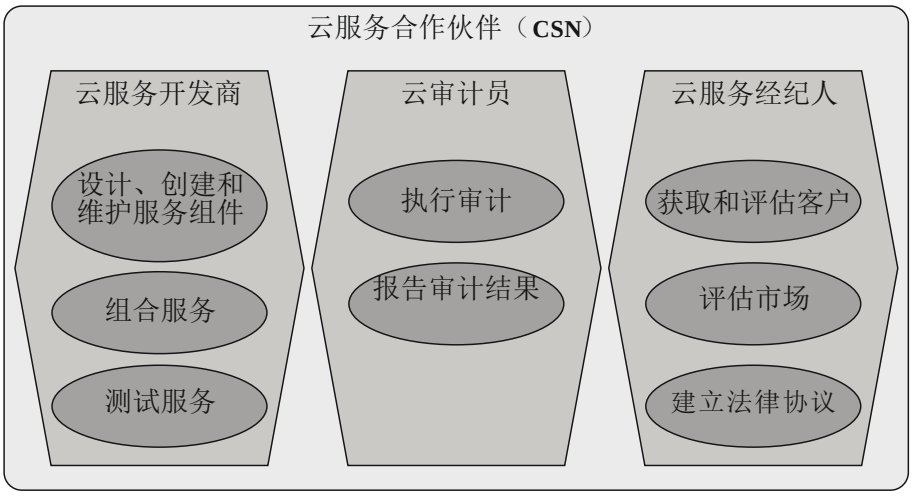


图8-5 – 与云服务合作伙伴子角色有关的云计算活动

8.4.2.1 设计、创建和维护服务组件

设计、创建和维护服务组件**活动**涉及：

- 设计和创建作为服务实施方案一部分的软件组件；
- 创建提供给服务用户的功能，这还涉及将服务组件连接到提供商的运营支持系统，以便可以监测和控制服务实施方案；
- 处理与服务实施操作有关的问题报告；
- 提供对服务实施方案的修复；
- 提供对服务实施方案的增强。

8.4.2.2 组合服务

组合服务**活动**侧重于使用现有的服务来组合服务。本**活动**涉及：

- 通过将别处提供的一项或多项现有服务组合在一起来创建服务功能；
- 描述服务的技术方面问题（功能接口、**SLA**等）；
- 为**云服务客户**设计一个接口，代表来自多个**云服务提供商**产品的组合服务；
- 进行可能涉及现有服务之中介、聚合或套利的组合。

8.4.2.3 测试服务

测试服务**活动**侧重于测试云服务开发商创建的组件和服务。本**活动**涉及：

- 对构成服务实施方案的组件进行测试，以确保它们完整且正确地执行服务的功能。
- 确保与**对等云服务提供商**提供之**云服务**的**互操作性**；
- 测试应包括检查与**云服务提供商**运营支持系统的连接是否正常运行 – 因此，通常有必要在**云服务提供商**数据中心的测试区域内执行某些测试。

8.4.2.4 执行审计

执行审计**活动**涉及：

- 请求或获取审计证据；
- 对被审计系统进行任何必要的测试；
- 通过被审计系统提供的一组接口，以编程方式获取证据；
- 必要时编辑证据，以保护敏感信息或受监管控制的信息（例如，**PII**）；
- 将获得的审计证据与正在使用之审计方案或标准所描述的审计标准进行比较。

所需审计证据的类型和用于评估它的标准由所使用的审计方案或标准来决定。示例包括与特定服务的安全控制和性能数据有关的数据。除了获取数据之外，还可以要求执行审计**活动**，以评估**云服务提供商**提供的服务，它包括安全控制、隐私影响、性能以及审计请求者确定的、与**云服务**有关的其他**云计算活动**。该请求可以来自**云服务提供商**本身，当中**云服务提供商**想要证明其**云服务**的质量，然后可以将之提供给潜在的**云服务客户**。

8.4.2.5 报告审计结果

报告审计结果**活动**涉及提供执行审计结果的书面报告，例如，关于某项**云服务**或关于某个**云服务提供商**或关于某个**云服务客户**对某项**云服务**的使用。书面报告的形式可以由正在使用的设计方案来规定。审计结果可能会提供给**云服务提供商**，也可能应**云服务客户**的要求来提供，具体取决于业务情况或法律背景。

8.4.2.6 获取和评估客户

获取和评估客户**活动**包括营销和销售**云服务**所需的任务，直至**云服务客户**同意使用一项或多项服务的合同。本**云计算活动**包括：

- 向潜在客户提供有关可用服务和相关**SLA**以及合同条款的信息；
- 与客户磋商条款和价格；
- 评估客户对**云服务**的需求和要求。

注 – **云服务客户**需求评估活动包括为确定和解决**云服务客户**的需求而采取的行动，这些需求是通过查看客户的当前能力及其期望的未来能力而进行的差距分析所确定的。

8.4.2.7 评估市场

评估市场**活动**侧重于评估当前的**云服务**市场，以找到满足客户需求的**云服务**。本**云计算活动**包括：

- 调查**云服务提供商**的产品，获取技术和业务信息；
- 订购和接收有关**云服务提供商**之**产品目录**内容更改的通知。
- 将产品供应与客户的需求和要求相匹配，包括技术、业务和监管方面的问题。

8.4.2.8 建立法律协议

建立法律协议**活动**涉及**云服务客户**与所选**云服务提供商**之间的服务协议。这涉及在**云服务客户**与所选**云服务提供商**之间协商服务协议，旨在满足客户的需求。

8.5 跨领域问题

8.5.1 概述

跨领域问题包括架构和操作方面的考虑。跨领域问题适用于CCRA描述内的多个要素，或者与其作为实例化系统的操作有关。这些跨领域问题是跨**角色**、**活动**和**功能组件**的共享问题。例如，安全性是一个跨领域的问题，因为它适用于基础设施、服务、**云服务提供商**、**云服务客户**和**云服务合作伙伴**（**云审计员**、云服务开发商等）。对所有这些都需要保证其安全，但如何保证其安全因保护的内容而异。因此，保护基础设施和基础设施服务的安全与保护软件服务的安全是很不同的。

某些跨领域问题可适用于其他跨领域问题，例如，治理适用于功能要素以及有关性能和安全性的跨领域问题。

跨领域问题通常会影响**角色**执行的**云计算活动**。**角色**可以协调支持其自身及其**云计算活动**之间的跨领域问题。支持跨领域问题还需要**功能组件**为**云计算活动**、技术能力和实施方案提供支持。

为每个跨领域问题，定义了一组**云计算活动**和**功能组件**来支持它们。不同的**角色**和解决方案可以使用这些的不同子集。

跨领域问题包括：

- 可审性（第8.5.2节）；
- **可用性**（第8.5.3节）；
- 治理（第8.5.4节）；
- **互操作性**（第8.5.5节）；
- 维护和版本控制（第8.5.6节）；
- 性能（第8.5.7节）；
- 便携性（第8.5.8节）；
- **个人可识别信息**的保护（第8.5.9节）；
- 监管；
- 适应性（第8.5.10节）；
- **可逆性**（第8.5.11节）；
- 安全性（第8.5.12节）；
- 服务水平和**服务水平协议**（第8.5.13节）。

8.5.2 可审性

可审性是一种能力，出于进行审计的目的，它收集和提供与**云服务**运营和使用有关的必要证据信息。与**云服务**治理有关的是确保这些服务的提供和使用与**云服务客户**、**云服务提供商**和**云服务合作伙伴**之间的相关服务协议一致。这种保证最通常的作法是通过对服务进行独立的审计来实现。审计通常包括提供给相关服务协议各方的审计报告或审计证明：**云服务客户**、**云服务提供商**和**云服务合作伙伴**。

审计本身取决于可用的数据和证据，这些数据和证据与服务和相关资源的使用、环境、**可用性**和性能有关。此类数据和证据包括管理协议各方操作环境的活动和条件记录与日志。这些记录与日志需要以安全的方式来收集和维护。

8.5.3 可用性

可用性是一种属性，对授权实体的需求来说易于理解和使用。“授权实体”通常是一个**云服务客户**：

8.5.4 治理

治理是一种系统，通过它来对**云服务**的提供和使用进行指导和控制。

内部云治理条款用于设计时和运行时政策的应用，以确保基于**云计算**的解决方案得以设计和实施，并确保依据指定的期望交付基于**云计算**的服务。这些期望可涵盖任何或所有跨领域问题。

云服务客户与**云服务提供商**使用的单个治理实践存在于从简单到复杂的连续统一体中，并封装在其**角色**中。每个**角色**都有责任根据其需求来实施治理。云治理被列为跨领域问题，原因是需要保证透明度，以及需要通过**SLA**和其他协议要素（关于**云服务客户**与**云服务提供商**之间的关系）来使治理行动合理化。

外部云治理条款用于**云服务客户**与**云服务提供商**之间某种形式的协议，它涉及**云服务客户**对**云服务**的使用。协议可以参考**服务水平协议**，它提供有关服务功能和非功能方面问题的详细信息。

8.5.5 互操作性

在**云计算**情形下，**互操作性**包括**云服务客户**与**云服务**交互并依照既定的方法交换信息并获得可预测结果的能力。典型的情况是，**互操作性**意味着**云服务**很可能是根据标准化的、商定的规范来运行。**云服务客户**在与**云服务**交互时应该能够使用内部广泛可用的ICT设施，避免使用专有的或高度专业化的软件。

互操作性还包括一种**云服务**与其他**云服务**共同工作的能力，要么通过CSP：云间提供商关系，要么**云服务客户**以某种组合形式来使用多种不同的**云服务**以实现其业务目标。

互操作性超越了**云服务**本身，还包括**云服务客户**与**云服务提供商**的**云服务**管理设施的交互。理想情况下，**云服务客户**应该拥有一致且可互操作的**云服务**管理功能接口，并能够与两个或多个**云服务提供商**进行交互，而无需以专门的方式来与每个提供商打交道。

实施标准是为了支持组件之间的**互操作性**或者支持数据或程序组件的可移植性。实施方案应该支持所用标准的演进，无论是从标准的一个早期版本演进到一个后期版本，还是从一个标准演进到另一个标准，同时最大限度地减少破坏性变动。

8.5.6 维护和版本控制

与治理有关的一个重要项是服务和基础资源的维护。维护可能出于多种原因，包括需要修复故障以及出于业务原因需要升级或扩展设施。维护行动可能会改变**云服务**的行为 – 尤其是更改会影响客户使用服务时的运行方式。

区分**云服务提供商**执行的维护与**云服务客户**执行的维护很重要。在**SaaS**服务情况下，几乎所有的维护行动都可能由提供商来执行。在**IaaS**和**PaaS**服务情况下，应用组件属于**云服务客户**，**云服务客户**负责这些组件的维护。提供商负责应用组件运行的环境，这取决于服务的细节，但可能包括诸如硬件资源、操作系统或中间件等要素。

一方面，升级或修复服务或服务平台可能符合客户的利益。另一方面，服务行为的任何变化都可能对客户产生负面影响，可能需要更改应用组件和客户ICT系统或者要求对客户服务用户进行再培训。因此，重要的是服务的维护受制于治理实践，这对客户是透明的。

维护实践应记录在**云服务**的**SLA**中，并应包括客户报告问题和请求修复的能力，以及**云服务提供商**通知客户未决之维护更改及其进度的机制。

版本控制是服务（或服务组件，例如，**IaaS**服务中使用的操作系统等级）的适当标签，以便客户清楚正在使用某个特定版本。在进行**云服务**维护时，为服务赋予一个新的版本标签很重要。

如果在两个版本之间对服务进行了重大更改，则旧版本的服务应与新版本并行提供一段商定的时间。

8.5.7 性能

性能包括一组与云服务操作有关的非功能方面问题，例如：

- 服务的**可用性**；
- 完成服务请求的响应时间；
- 执行服务请求的事务处理率；
- 服务请求的延迟；
- 数据吞吐率（输入和输出）；

- 并发服务请求的数量（可扩展性）；
- 数据存储容量；
- （对**IaaS**和**PaaS**）应用可用之并发执行线程的数量；
- （对**IaaS**和**PaaS**）运行程序可用的内存（RAM）量；
- 数据中心网络IP地址池和/或VLAN范围容量。

在服务涉及运行某个应用程序（**IaaS**、**PaaS**）的情况下，相同的性能方面适用于在**云服务提供商**环境中运行的应用程序的行为。

根据收费模型，**云服务**根据**SLA**条款扩展其资源使用的能力也可以是性能的一个重要方面。性能应该在**SLA**中为确定的每个性能条件定义指标，并应在**云服务**运行期间监测这些指标，以确保服务满足**SLA**的性能条款要求。

8.5.8 可移植性

可移植性在**云计算**中很重要，因为预期的**云服务客户**在选择使用**云服务**时有兴趣避免锁定。**云服务客户**需要知道其可以在多个**云服务提供商**之间以较低的成本和最小的中断来移动**云服务客户数据**或其应用。可接受的成本和中断数量可因正在使用的**云服务**类型而异。

例如，如果**云服务客户**组织正在考虑从一个**IaaS云服务提供商**迁移到另一个**IaaS云服务提供商**，则**云服务客户**应该能够获取其数据和虚拟机（VM）映像，并以一种相对直接的方式在等效的**IaaS**服务上启动和运行。在**SaaS**环境中，当**云服务客户**组织想要将**SaaS**应用迁移到不同的**云服务提供商**（即切换**SaaS**服务提供商）时，**云服务客户**需要能够随身携带其数据，但其余的切换成本将包括把数据导出、映射和导入到新**云服务提供商**的**SaaS**应用中，而该成本取决于两个**SaaS云服务提供商**的数据模型和格式的排列情况。理想情况下，**SaaS云服务提供商**应采用与其应用领域相关的标准数据交换格式。**SaaS**应用之间的更改还可能涉及**云服务客户**适应新的服务接口（这与服务的**互操作性**有关）。

不过，由于不同的**云能力类型**可能对可移植性有不同的要求，因此专注于特定类型的可移植性更有用，例如，**云数据可移植性**和**云应用可移植性**。

云服务客户数据是**云服务客户**控制下的一类数据对象。**云数据可移植性**使**云服务客户**能够通过网络访问或存储设备的物理传输将**云服务客户数据**复制到**云服务**中或从**云服务**中复制出来。

云应用可移植性允许将诸如完全停止的虚拟机实例或机器映像（**IaaS**服务）等项从一个**云服务提供商**迁移到另一个**云服务提供商**，或者将应用组件（**PaaS**服务）从一个**云服务提供商**迁移到另一个**云服务提供商**。在这两种情况下，都存在支持与应用组件相关之元数据的可移植性的相关问题，并提供有关程序组件关系和程序组件所需基础设施（例如，负载平衡配置、防火墙设置）的信息。

8.5.9 保护个人可识别信息（PII）

云服务提供商应保护与**云服务**有关的**个人可识别信息（PII）**确定、合适和持续的收集、处理、通信、使用和处置。

根据既定的准则，组织的关键业务要务之一是确保做好对**个人可识别信息（PII）**的保护。尽管**云计算**为共享资源、软件和信息提供了灵活的解决方案，但它也给使用**云服务**的**云服务客户**以及**云服务提供商**带来了额外的**机密性**挑战。

在许多司法管辖区，有严格的规则和条例适用于**PII**处置 – 任何使用**云服务**来存储和处理**PII**的行为通常都必须遵守这些规则和条例。

法律法规方面的要求因市场部门和司法管辖区而异，它们可以改变**云服务客户**和**云服务提供商**的责任。遵守此类要求通常与治理和风险管理**活动**有关。

8.5.10 适应性

适应性是系统在面对影响正常运行的故障时（无意的、有意的或自然引起的）提供并维持可接受之服务水平的能力。

适应性描述了一组监测、预防和响应流程，这些流程使**云服务**能够通过故障和恢复行动来提供持续操作或者可预测和可验证的中断。这可包括硬件、通信和/或软件故障，并可作为孤立的事件或组合的事件，包括串行故障。这些流程可包括自动化的和手动的行动，通常跨越多个系统，因此其描述和实现是整个云基础设施的一部分，而不是一个独立的功能。

适应性的内在是风险管理的实现 – 因为适应性是由系统中适应性最小的组件来决定的，而成本/性能或其他因素会限制适应性可能的或实际的程度。在提供适应性的实施方案选择中实现风险与价值的关联。

8.5.11 可逆性

可逆性是一个术语，它适用于**云服务客户**检索其**云服务客户数据**和应用工件以及**云服务提供商**在约定期限后删除所有**云服务客户数据**以及合同指定之**云服务派生数据**的过程。原则是“被遗忘权”，即**云服务客户**有权期望一旦其向**云服务提供商**表明将停止使用服务，那么对**云服务客户**将有一个有序的过程来检索**云服务客户数据**及其应用工件，并且**云服务提供商**将在约定期限后删除所有副本且不保留属于**云服务客户**的任何资料。

与**可逆性**有关的活动在大多数情况下会涉及一系列步骤，通常需要**云服务客户**检索其数据并通知**云服务提供商**可删除其**云服务客户数据**的副本 – 在退出过程发生故障的情况下，保护备份副本至该时刻。这些步骤也需适用于**云服务提供商**用来支持**云服务提供商**服务的任何对等服务。

8.5.12 安全性

8.5.12.1 概述

至关重要的一点是要认识到安全性是架构的一个跨领域问题，它跨越参考模型的所有视图，从物理安全性到应用安全性。因此，**云计算**架构中的安全性不仅是**云服务提供商**控制下的一个跨领域问题，它还影响到**云服务客户**、**云服务合作伙伴**及其**子角色**。

云计算系统可满足安全性要求，例如，认证、授权、**可用性**、**机密性**、不可否认性、身份管理、**完整性**、审计、安全监测、事件响应和安全策略管理。本节描述**云计算**的特定视角，以帮助分析和实施**云计算**系统中的安全性。

云服务的安全功能包括：访问控制、**机密性**、**完整性**和**可用性**。在其他规范中详细描述了**云计算**的安全性。

安全能力还包括用于控制**云服务**、底层资源和**云服务**使用的管理功能，需要特别关注对这些功能用户的访问控制。除此之外：

- 能够及早发现、诊断和修复**云服务**和资源相关问题的设施；
- 安全记录网络上的访问记录、活动报告、会话监测和分组检查结果；
- 为**云服务提供商**的系统提供防火墙、恶意攻击检测和预防。一个用户不应能干扰其他用户的**云服务**使用。

应在将**云服务客户**连接到**云服务提供商**的网络上提供内联网水平的安全性（例如，通过使用VPN能力）。

云计算中的安全措施旨在解决与**云服务客户**使用**云服务**有关的一系列威胁，这些威胁既会影响**云服务客**，也会影响**云服务提供商**。对这些威胁在其他规范中有更全面的描述，例如，ISO/IEC 27018。

8.5.12.2 安全责任分配

云服务提供商和**云服务客户**对**云计算**系统中的计算资源的控制程度不同。相比传统信息技术系统（当中，由一个组织来控制整个计算资源栈和系统整个生命周期），**云服务提供商**和**云服务客户**协同设计、构建、部署和操作**云计算**系统。

控制的分离意味着两个**角色**现在分担为**云计算**系统提供足够保护的责任。安全是一项共同的责任。需要分析安全控制，即用于提供保护的措施，以确定哪个**角色**更适合实施此类控制。这种分析需要从服务类别的角度来考虑，不同的**云服务类别**意味着**云服务提供商**与**云服务客户**之间不同的控制程度。为客户和提供商的责任提供一个明确的定义并确保涵盖安全性的所有方面问题以避免责任模糊，这一点很重要。

例如，**IaaS**服务之初始系统特权用户的帐户管理控制通常由**IaaS云服务提供商**来执行；同时，部署到该**IaaS**服务之应用的应用用户帐户管理通常由使用**IaaS**服务部署应用的**云服务客户**来负责。相比之下，对于**SaaS**应用服务，所有类型用户的账户管理控制权都掌握在**云服务提供商**手中（虽然**云服务客户**可提供如第三方认证等能力）。

8.5.12.3 云服务类别视角

ITU-T Y.3500建议书 | ISO/IEC 17788中定义的**云服务类别**是一组拥有共同质量集的**云服务**。**云服务类别**为**云服务客户**提供不同类型的服务管理操作，并显露不同的入口点给**云计算**系统，这反过来也为对手创造了不同的攻击面。因此，重要的是要考虑**云服务类别**的影响及其在安全设计和实施中的不同问题。

例如，**SaaS**为用户提供使用网络连接的**云计算**产品的可访问性，可能通过互联网和万维网浏览器。**SaaS云计算**系统安全考虑中一直强调万维网浏览器的安全性。**IaaS**服务的CSC：云服务用户通常会获得在主机中的管理程序上执行的虚拟机（VM）；因此，已经为使用虚拟化技术的**IaaS云服务提供商**广泛研究了用于实现VM隔离的管理程序安全性。

8.5.12.4 云部署模型的含义

不同的**云部署模型**具有重要的安全含义。从部署模型的角度来看安全含义的一种方法是部署模型中**租户**的不同等级的排他性。**私有云**专用于一个**云服务客户**组织，而**公有云**可以让来自许多不同组织的**租户**共存。

分析**云部署模型**安全含义的另一种方法是使用访问边界概念。例如，当**私有云**系统在**云服务客户**组织的网络边界内现场托管时，在**云服务**边界处，现场**私有云**系统需要或不需要额外的边界控制器，而外包的**私有云**往往需要在**云服务**边界处建立这种外围保护。

8.5.12.5 数据保护策略和责任

数据保护假定**云计算**的一个新维度。一个组织可以选择将其数据存储在**云服务**中，但而后需要明确同意数据保护责任和问责制。**云服务客户**采取的第一步是对数据进行正确分类，并确定其敏感性及其泄漏、丢失或损坏对业务可能带来的风险。（请参阅ISO/IEC 27002，作为如何确定数据敏感性的参考）。

理想情况下，在将数据迁移到**云计算**系统之前，对数据做好保护应该是**云服务客户**的责任。不过，提供商将对任何数据篡改或盗窃负责。加密是一种潜在的使用技术，但在**云服务客户**或任何第三方管理密钥的情况下，必须考虑密钥管理。如果密钥由**云服务提供商**来管理，则其负责密钥以及数据的逻辑和物理控制。

8.5.13 服务水平和服务水平协议

服务水平协议是**云计算**治理的重要组成部分，代表确保达成**云服务客户**与**云服务提供商**之间商定之服务质量所需的可测量要素。

云计算服务水平协议（云**SLA**）是**云服务提供商**与**云服务客户**之间的**服务水平协议**，基于的是一种**云计算**特定术语的分类法，以设定所交付**云服务**的质量。它从以下几个方面来表征所交付**云服务**的质量：

- 一组特定于**云计算**（业务和技术）的可测量属性；
- 一组给定的**云计算角色**（**云服务客户**和**云服务提供商**以及相关的**子角色**）。

例如，**云服务客户**需要一个云**SLA**来指定一个或多个**云服务**的技术性能要求。云**SLA**可涵盖有关服务质量、安全性、性能和针对未能满足**SLA**条款之补救措施的条款。**云服务提供商**还可以在云**SLA**内列出一组明确未向**云服务客户**做出的承诺，即**云服务客户**需要接受的限制和义务。云**SLA**应定义数据对象（即**云服务客户数据**、**云服务提供商数据**和**云服务派生数据**）的分类、谁有权访问和控制这些数据分类中的数据对象以及如何使用它们。

服务水平协议应规定与服务**可用性**、服务**机密性**和**完整性**以及适用于服务访问控制有关的信息。**服务水平协议**应指定如何处置与**云服务**有关的任何**个人可识别信息**。

服务协议 – 也称为主服务协议（MSA）、服务条款（ToS）、条款和条件（T&C），或者简称为“合同” – 是各方间协议中的更高级文件，**服务水平协议（SLA）**从属于它。这是一个重要的区别，因为**SLA**首字母缩略语常常且不正确地被用来指代整个合同关系 – 单个**SLA**无法履行的一个**角色**。服务协议涉及整个合同关系，因此包含与**云计算**没有直接关系的合同要素。

9 功能视图

9.1 功能架构

云计算的功能架构依据一组高级**功能组件**来描述**云计算**。**功能组件**代表执行**云计算活动**（如第8节中为**云计算**涉及之各种**角色**和**子角色**所做的描述）所需的功能集。

功能架构依据分层框架描述**功能组件**，当中特定类型的功能被分组到每一层中，并在连续层中的**功能组件**之间存在接口。

9.1.1 分层框架

CCRA中使用的分层框架有四层，以及一组跨层的功能。这四层分别是：

- 用户层；
- 接入层；
- 服务层；
- 资源层。

跨层的功能称为多层功能。

分层框架如图9-1所示。

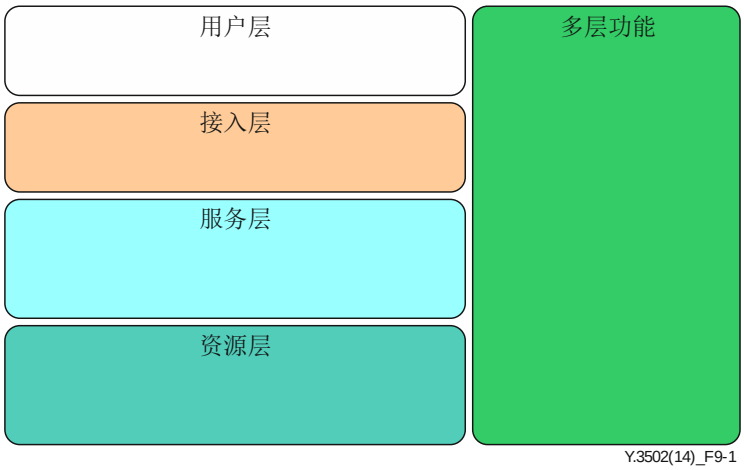


图9-1 – 云计算分层框架

在以下子节中对框架中的每一层做了描述。

9.1.1.1 用户层

用户层是用户接口，**云服务客户**通过它来与**云服务提供商**和**云服务**交互、执行与客户有关的管理**活动**以及监测**云服务**。它还可以将**云服务**的输出提供给另一个资源层实例。

9.1.1.2 接入层

接入层为手动和自动接入服务层中可用的功能提供了一个通用接口。这些能力包括服务能力以及管理和业务能力。

接入层负责通过一种或多种访问机制来表现**云服务**能力 – 例如，作为一组通过浏览器访问的网页，或作为一组可以通过安全通信以编程方式访问的万维网服务。接入层的另一个职责是将适当的安全功能应用于对**云服务**能力的访问。接入层负责通过使用用户证书来对请求进行认证，并负责验证用户对使用特定能力的授权。接入层还负责在需要时处置加密和检查请求**完整性**问题。

接入层还可以负责对来自用户层的流量（例如，对**云服务提供商**的服务请求）和流向用户层的流量（例如，**云服务**的输出）实施QoS策略。

接入层将经过验证的请求传给服务层中的组件。接入层接受**云服务客户**或**云服务提供商**的**云服务**消费请求，以访问**CSP**的服务和资源。

9.1.1.3 服务层

服务层包含**云服务提供商**提供之服务的实施方案。服务层包含并控制实现服务的软件组件（但不是底层管理程序、主机操作系统、设备驱动程序等。），并安排通过**接入层**向用户提供**云服务**。

服务层中的服务实施方案软件反过来依赖资源层中可用的能力来提供所提供的服务，并确保满足与服务有关的任何**SLA**的要求，例如，通过使用足够的资源。

9.1.1.4 资源层

资源层是资源所在处。这包括通常用于数据中心的设备，例如，服务器、网络交换机和路由器、存储设备，以及运行在服务器和其他设备上的相应的非云特定软件，例如，主机操作系统、管理程序、设备驱动程序和通用系统管理软件。

资源层还代表和容纳云传输网络功能，该功能需要在**云服务提供商**与用户之间以及在**云服务提供商**内和**对等云服务提供商**之间提供底层网络连接。

注意：为使**云服务提供商**提供符合**SLA**要求的服务，它可能需要用户与**云服务提供商**之间专用的和/或安全的连接。

9.1.1.5 多层功能

多层功能包括一系列**功能组件**，这些**功能组件**与上述其他四层的**功能组件**交互，以提供支持能力，包括但不限于：

- 运营支持系统能力（运行时管理、监测、供应和维护）；
- 业务支持系统能力（**产品目录**、计费和财务管理）；
- 安全系统能力（认证、授权、审计、验证、加密）；
- 集成能力（不同组件的链接，以实现所需的功能）；
- 开发支持能力（涉及服务和服务组件的创建、测试和生命周期管理）。

9.2 功能组件

本节根据**云计算功能组件**通用集来描述云架构。**功能组件**是CCRA的一个功能要素，用于执行**活动**或**活动**的某些部分，并在架构的具体实现中拥有实施方案工件，例如，软件组件、子系统或应用程序。

图9-2提供了通过分层框架进行组织的、有关CCRA**功能组件**的高层概览。

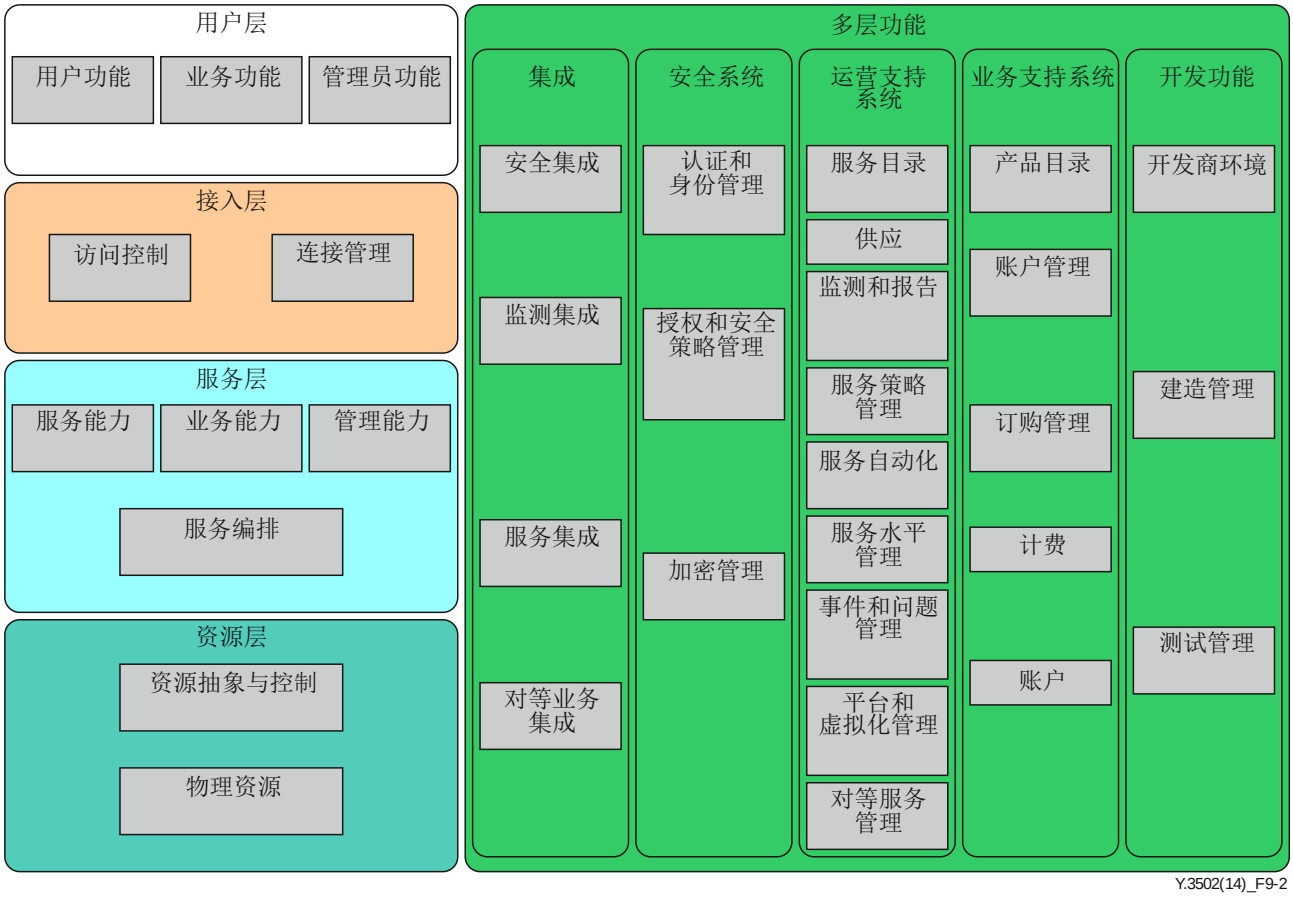


图9-2 – CCRA的功能组件

9.2.1 用户层功能组件

用户层**功能组件**包括：

- 用户功能；
- 业务功能；
- 管理员功能。

提供给CSC：云服务用户的**云服务**可分为两大类：功能服务和自助管理服务。后者可进一步分为：业务服务和管理服务。

提供给**云服务**用户的接口包含**云服务**的主要功能。这与用于管理**云服务**使用的接口有所不同。但所有情况都是为不同类型的能力而量身定制的**云服务**。

9.2.1.1 用户功能

用户功能**功能组件**支持CSC：云服务用户访问和使用**云服务**（**使用服务活动**）。在某些情况下，用户功能**功能组件**可以像在用户设备上运行的浏览器一样简单。不过，在其他情况下，它可能涉及运行业务流程、应用程序、中间件和相关基础设施的复杂的企业系统。

9.2.1.2 业务功能

业务功能**功能组件**支持CSC：业务经理的**云计算活动**，包括**云服务**的选择和购买、与使用**云服务**有关的会计和财务管理。应该注意的是，业务能力本身是通过**云服务**来提供的。

9.2.1.3 管理员功能

管理员功能**功能组件**支持CSC：云服务管理员的**云计算活动**。这包括用于管理用户身份和配置文件、监测服务活动和使用、事件处置和问题报告的功能。云管理能力只能使用**云服务**来访问。

9.2.2 接入层功能组件

接入层**功能组件**如图9-3所示，它包括：

- 访问控制：
  - 服务访问；
  - 业务访问；
  - 管理访问；
  - 开发访问。
- 连接管理。

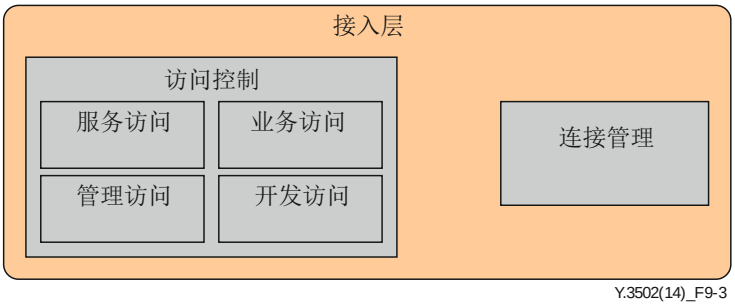


图9-3 – 接入层功能组件

9.2.2.1 访问控制

访问控制限制用户使用特定服务。原则上，访问控制涉及通过提供和验证证书来对用户进行认证，然后授权该经认证的用户使用特定的服务。与此相关的是身份管理。

应提供对**云服务**及其依赖之资源的访问控制以及相关的控制功能。

9.2.2.2 服务访问

服务访问**功能组件**提供对**云服务提供商**提供之**云服务**的访问。

9.2.2.3 业务访问

业务访问**功能组件**提供对由业务支持系统实现的、**云服务提供商**提供之业务能力的访问。

9.2.2.4 管理访问

管理访问**功能组件**提供对由运营支持系统实现的、**云服务提供商**提供之管理能力的访问。

9.2.2.5 开发服务

开发访问**功能组件**提供对提供商系统内一组功能的访问，该系统支持**云服务**实施方案的开发、测试和维护。

9.2.2.6 连接管理

连接管理**功能组件**对自和/或至用户层**功能组件**的流量实施QoS策略。连接管理**功能组件**与多层功能交互，以检索存储在彼处的策略，并在访问层本地执行它们。

9.2.3 服务层功能组件

服务层**功能组件**包括：

- 服务能力；
- 业务能力；
- 管理能力；
- 服务编排。

9.2.3.1 服务能力

服务能力**功能组件**由实施提供给**云服务客户**之服务所需的必要软件组成。它实现了通过服务接口定义的功能，即独立于服务实施方案、提供给**云服务客户**的接口。

9.2.3.2 业务能力

业务能力**功能组件**提供一组用于访问与提供**云服务**有关的业务功能的能力。业务功能本身包含在业务支持系统**功能组件**中。

9.2.3.3 管理能力

管理能力**功能组件**提供一组用于访问与提供**云服务**有关的管理功能的能力。

管理功能本身包含在运营支持系统和业务支持系统**功能组件**中。

9.2.3.4 服务编排

服务编排**功能组件**提供多个服务组件的协调、聚合和组合，以便交付**云服务**。

9.2.4 资源层功能组件

资源层**功能组件**包括：

- 资源抽象与控制；
- 物理资源。

9.2.4.1 资源抽象与控制

云服务提供商使用资源抽象与控制**功能组件**，通过软件抽象，来提供对物理计算资源的访问。资源抽象需要确保底层基础设施的高效、安全和可靠使用。**功能组件**的控制特征实现了对资源抽象特征的管理。

资源抽象与控制**功能组件**使**云服务提供商**能够提供诸如快速适应、**资源池化**和**按需自助服务**等品质。资源抽象与控制**功能组件**可包括软件要素，例如，管理程序、虚拟机、虚拟数据存储和分时。

资源抽象与控制**功能组件**启用控制功能，启用在运营支持系统**功能组件**中实现的监测和管理能力（见第9.2.5.3节）。例如，可以有一个集中的算法来控制、关联和连接物理资源中的各种处理、存储和网络单元，以便它们一起提供一个可以提供**NaaS**、**IaaS**、**PaaS**或**SaaS云服务类别**的环境。控制器可决定哪些CPU和/或机架包含哪些虚拟机来执行给定**云服务**工作负载的哪些部分，以及此类处理单元如何相互连接，以及随着条件的变化何时动态地和透明地将部分工作负载重新分配给新的单元。

关于是否虚拟化物理资源的决定取决于要运行的工作负载特性。对许多**云服务**的工作负载（例如，与**计算即服务**和**数据存储即服务**相关的）而言，将底层物理资源虚拟化是很方便的，特别是因为虚拟化可以实现一些物理基础设施基本上无法实现的场景（例如，与图像管理或根据需要动态扩展CPU容量相关的场景）。对其他工作负载（例如，分析和/或搜索）而言，需要拥有最大计算能力并使用成百上千个节点来运行单个专门的工作负载。在这种情况下，非虚拟化物理资源可能更合适。

9.2.4.2 物理资源

物理资源**功能组件**代表**云服务提供商**运行和管理其提供之**云服务**所需的要素。

物理资源包括硬件资源，例如，计算机（CPU和内存）、网络（路由器、防火墙、交换机、网络链路和网络连接器、存储组件（硬盘）和其他物理计算基础设施元素。这些资源可以包括那些驻留于云数据中心（例如，计算服务器、存储服务器和数据中心内联网）之内的那些资源，以及驻留于数据之外的那些资源，通常是联网资源，例如，数据中心间网络和核心传输网络。

物理资源的所有要素都由运营支持系统**功能组件**管理，能够根据需要将每个**云服务**的实例放置到资源上，以满足客户需求。注意：通常，运营支持系统**功能组件**本身运行于物理资源的某个部分上。

9.2.5 多层功能

9.2.5.1 集成功能组件

集成**功能组件**负责连接架构中的**功能组件**，以创建一个统一的架构。集成**功能组件**在云架构及其**功能组件**内以及与外部**功能组件**之间提供消息路由和消息交换机制。消息路由可以基于各种各样的标准，例如，情形、策略。

集成**功能组件**包括：

- 安全集成；
- 监测集成；
- 服务整合；
- 对等服务集成。

9.2.5.1.1 安全集成

安全集成**功能组件**提供对包括认证、授权、加密和**完整性**验证在内的安全能力的集成以及与安全能力有关的策略机制的集成。

9.2.5.1.2 监测集成

监测集成**功能组件**提供从接入层、服务层和资源层的**功能组件**到运营支持系统的监测和报告能力的连接。

9.2.5.1.3 服务集成

服务集成**功能组件**提供到在提供商环境内运行之服务的连接。服务集成**功能组件**是虚拟化服务的一个重要问题，例如，这样，其位置和实施方案细节对依赖这些服务的组件而言就是隐藏的。

9.2.5.1.4 对等服务集成

对等服务集成**功能组件**用于以受控方式连接**对等云服务提供商**的服务，具有适当的安全性并对使用情况进行适当的记帐，链接回**云服务客户**的身份。对等服务集成**功能组件**还将与目标服务的链路虚拟化，以便这些服务的细节可动态变化，而不影响引用这些服务的**功能组件**。

9.2.5.2 安全系统功能组件

安全系统**功能组件**负责应用与安全有关的控制，以缓解**云计算**环境中的安全威胁。安全系统**功能组件**包括所有支持**云服务**所需的安全设施。

安全管理**功能组件**包括：

- 认证和身份管理；
- 授权和安全策略管理；
- 加密管理。

9.2.5.2.1 认证和身份管理

认证和身份管理**功能组件**提供与用户身份有关的能力，以及在用户访问**云服务**及其相关管理和业务能力时对用户进行认证所需的证书。

身份管理可涉及联邦身份管理，以允许用户使用相同的身份和证书来访问多个**云服务**，提供诸如“单点登录”等能力。

9.2.5.2.2 授权和安全策略管理

授权和安全策略管理**功能组件**为用户访问特定的能力或数据提供控制和应用授权的能力。服务策略管理提供与**云服务**有关的安全策略的定义和应用。

9.2.5.2.3 加密管理

加密管理**功能组件**提供与数据加密有关的能力，无论是对静态数据还是对动态数据。加密密钥管理和加密方案选择是所提供的部分功能。

9.2.5.3 运营支持系统功能组件

运营支持系统**功能组件**包含一组与运营有关的管理能力，为管理和控制提供给客户的**云服务**，需要这些能力。

运营支持系统**功能组件**包括：

- **服务目录；**
- 供应；
- 监测和报告；
- 服务策略管理；
- 服务自动化；
- 服务水平管理；
- 事件和问题管理；
- 平台和虚拟化管理；
- 对等服务管理。

9.2.5.3.1 服务目录

服务目录功能组件提供特定**云服务提供商**之所有**云服务**的清单。**服务目录**可以包含/引用部署、供应和运行**云服务**所需的所有相关技术信息。

9.2.5.3.2 供应

供应**功能组件**提供用于供应服务的能力，包括服务实施和接入端点的供应以及确保以正确顺序供应各要素所需的工作流。

9.2.5.3.3 监测和报告

监测和报告**功能组件**提供以下能力：

- 监测整个**云服务提供商**系统中其他**功能组件**的**云计算活动**。这包括CSC：云服务用户直接使用**云服务**所涉及的**功能组件**，例如，服务访问和服务实施方案（例如，特定用户调用**云服务**操作）。这也包括支持**云服务**所涉及的**功能组件**，例如，OSS本身的**功能组件**，如服务自动化**功能组件**（例如，为特定客户提供服务实例）；
- 提供有关**云服务提供商**系统行为的报告，对于带有时敏性问题的行为（例如，故障的发生、任务的完成）可以采取告警的形式，也可以采取历史数据聚合的形式（例如，服务使用情况数据）；
- 存储和检索监测与事件数据作为日志记录。

需要保证监测和报告**功能组件**所持有之日志记录的**可用性**、**机密性**和**完整性**。对多租户**云服务**而言，还需要设计对记录的访问，以便特定**租户**只能访问关于其自身租户的信息，而不能访问其他租户的信息。

9.2.5.3.4 服务策略管理

服务策略管理**功能组件**提供定义、存储和检索适用于**云服务**之策略的能力。策略可以包括适用于**云服务**及其**云服务客户**使用的业务、技术、安全、隐私和认证策略。

一些策略可以是通用的，并适用于**云服务**，而与所涉及的客户无关。其他策略可特定于某个特定客户。

9.2.5.3.5 服务自动化

服务自动化**功能组件**提供用于服务交付的能力，包括服务模板的管理和执行以及服务的编排。服务自动化**功能组件**持有服务模板，它们定义在**服务目录**中提供和交付特定条目所需的**云计算活动**和工作流。

云服务供应可被自动化，以便支持可扩展的资源操作，包括配置和收费。

云服务客户的**云服务**管理**活动**可被自动化且无需**云服务提供商**的任何干预。

服务自动化**功能组件**与供应**功能组件**和服务集成**功能组件**协同工作，以实现其目标。

9.2.5.3.6 服务水平管理

服务水平管理**功能组件**提供用于管理特定**云服务**之服务水平的能力，旨在确保**云服务**满足适用于该服务的**SLA** 的要求。

服务水平管理**功能组件**管理与**云服务**有关的容量和性能。这可能涉及服务策略的应用（例如，旨在避免单点故障的配置规则）。

服务水平管理**功能组件**从监测和报告**功能组件**获取监测信息，以测量和记录有关**云服务**的关键性能指标（KPI）。根据这些KPI来分配或取消分配容量。

服务水平管理**功能组件**还跟踪已分配资源和可用资源的整体状态。将分配的容量与**云服务**性能KPI进行比较，可帮助确定当前的或潜在的瓶颈，以支持容量规划。

9.2.5.3.7 事件和问题管理

事件和问题管理**功能组件**提供用于捕获事件或问题报告并管理这些报告直至解决的能力。

事件和问题可以由**云服务提供商**的系统来检测和报告，也可以由**云服务客户**来检测和报告。

9.2.5.3.8 平台和虚拟化管理

平台和虚拟化管理**功能组件**提供用于管理**云服务提供商**底层资源（计算、存储、网络）和虚拟化使用这些资源（例如，通过管理程序）的能力。

资源通常被组织成具有关键特性的资源池：

- 标准化的硬件组件和配置；
- 可通过增加新硬件容量轻松扩展；
- 随着工作负载需求的变化而自动转移资源；
- 相邻工作负载和数据的保护与隔离；
- 通过在资源之间移动工作负载和数据来缩短和/或消除停机时间；
- 根据目标（例如，性能、**可用性**、许可、能源使用）管理资源消耗。

9.2.5.3.9 对等服务管理

对于提供商使用的**对等云服务**，对等服务管理**功能组件**提供用于将提供商运营支持系统和业务支持系统连接到**对等云服务提供商**管理能力和业务能力的能力。

对等服务管理**功能组件**负责建立所需的通信路径，并通过向**对等云服务提供商**提出请求来传递适当的身份和证书。

9.2.5.4 业务支持系统组件

业务支持系统**功能组件**包含一组与客户和支持流程打交道的业务相关管理功能。

业务支持系统**功能组件**包括：

- **产品目录**；
- 帐户管理；
- 订阅管理；
- 计费；
- 账户。

9.2.5.4.1 产品目录

产品目录**功能组件**为**云服务客户**提供浏览其可购买之可用服务产品清单的能力，以及一组用于管理**云服务提供商**员工可用之目录内容的能力。

产品目录条目包含有关每个服务产品的技术信息（服务提供的能力、服务的接口定义，包括可用的服务操作、安全信息），以及相关的业务信息，例如，定价或评级。

9.2.5.4.2 帐户管理

账户管理**功能组件**提供用于管理**云服务客户**关系的能力，包括：

- 合同管理；
- **云服务**订购；
- 权利；
- 服务定价，这可涉及客户特定的条款，例如，折扣；
- 适用于处理**云服务客户数据**的策略。

由于与客户账户有关的数据的重要性和敏感性，账户管理**功能组件**及其相关数据库受制于有关**可用性**和安全性的严格要求。

9.2.5.4.3 订购管理

订购管理**功能组件**处置**云服务客户**对特定**云服务**的订购，旨在记录客户新的或更改的订购信息，并确保将订购的服务交付给客户。

9.2.5.4.4 计费

计费**功能组件**具有以下能力：

- 对**云服务客户**使用**云服务**情况进行计量和评级 – 当中，计量是对每个**云服务客户**对**云服务**的消费情况进行度量，评级是对计量数据应用定价方案。计量数据的形式取决于**云服务**的性质，定价方案可能涉及客户特定的条款（例如，折扣）并需要针对计量数据进行算法应用；
- 根据计量和评级功能创建之**云服务**的使用费用生成发票，并将发票传给**云服务客户**。发票数据也提交给帐户**功能组件**和帐户管理**功能组件**。

9.2.5.4.5 账户

账户**功能组件**拥有与总账和一般会计功能有关的能力，包括应收账款和应付账款。注意：帐户**功能组件**用于**云服务提供商**组织本身的会计事务，不涉及个人客户帐户的维护（这些由帐户管理**功能组件**来处置）。

9.2.5.5 开发支持功能组件

开发支持**功能组件**支持云服务开发商的**云计算活动**。这包括支持服务实施方案的开发和/或组合、建造管理和测试管理。

开发支持**功能组件**包括：

- 开发商环境；
- 建造管理；
- 测试管理。

9.2.5.5.1 开发商环境

开发商环境**功能组件**提供支持服务实施方案软件开发的能力。支持为服务开发软件组件，以及有助于从一组其他服务中组合服务的工具。

开发商环境**功能组件**支持使用**云服务提供商**环境提供之能力，包括与资源和网络的连接、与其他服务（包括**对等云服务提供商**的服务）的集成、与监测和管理能力的集成、与安全能力的集成。

开发商环境**功能组件**还支持创建与正在开发之服务有关的配置元数据，并支持创建提供商运营支持系统用来提供和配置服务的脚本和相关工件。

9.2.5.5.2 建造管理

构建管理**功能组件**支持构建准备部署的软件包，该软件包可传给**云服务提供商**，以部署到**云服务**环境中。该软件包由服务实施方案软件以及配置元数据和脚本组成。

9.2.5.5.3 测试管理

测试管理**功能组件**支持针对服务实施方案的任何构建执行测试用例。测试管理**功能组件**生成已执行测试的报告，这些报告可以与服务实施方案的构建一起传达给**云服务提供商**。

通常在专门的测试环境中执行测试，该环境非常接近生产环境，而不会干扰生产环境。对**云计算**，测试环境可由**云服务提供商**来提供。

10 用户视图与功能视图之间的关系

10.1 概述

除了在第8节中指定**角色**和**云计算活动**视图以及在第9节中指定包括架构**功能组件**在内的功能视图外，本建议书 | 国际标准在本节中描述**角色**和**云计算活动**与**功能组件**的逻辑关系。

标准可能与其中一些关系相关。与关系相关的标准可用于（i）指定信息流的等级或其他类型的**互操作性**；和/或（ii）确保指定的质量等级（例如，安全性或服务水平）。

在本架构中定义的逻辑关系是指定CCRA及其行为的一个重要组成部分。本关系描述诸如CCRA中**功能组件**之间所需的信息流等事项。

10.2 综述

图10-1概述了CCRA在一个通用配置中的主要元素 – **角色**、**云计算活动**和**功能组件**。

图10-1使用第5节中介绍的图形约定。带有连续圆边的框代表**角色**，六边形代表**子角色**，圆边的虚线框代表**云计算活动**，带砖块的正方形是**功能组件**。服务能力**功能组件**内的“L”形框代表基于基本**云能力类型**的**云服务**接口。在图10-1中，显然**角色**是**云计算活动**的集合，**云计算活动**本身是通过**功能组件**来实施或实现的。

代表角色的图形元素彼此接近是有意义的，并代表承担相邻**角色**的角色之间的密切交互。例如，**云服务提供商角色**位于图的中心，以强调它与所有其他**角色**都有交互。给定**角色**内的**云计算活动**的定位以及给定**活动**内**功能组件**的相对定位也是如此。例如，服务能力**功能组件**位于资源抽象与控制**功能组件**之上，以表示前者对后者的依赖。

可审性、**可用性**、治理、**互操作性**、维护和版本控制、性能、可移植性、**个人可识别信息**保护、监管、适应性、**可逆性**、安全性、服务水平和**服务水平协议**的跨领域问题由图10-1中的最外层方框来表示，旨在表明跨领域问题适用于图10-1中的所有其他要素 – **角色**、**活动**和**功能组件**。例如，CSC：云服务用户必须拥有一个身份以及一组证书，在执行使用**云服务活动**时，必须将其提供给用户功能**功能组件**。将身份和证书提供给访问控制**功能组件**以及作为提供服务**活动**一部分来执行的认证和授权，在将**云服务**提供给CSC：云服务用户之前调用适当的安全**功能组件**能力。

图10-1的服务能力**功能组件**代表了**云服务**本身的实施方案。

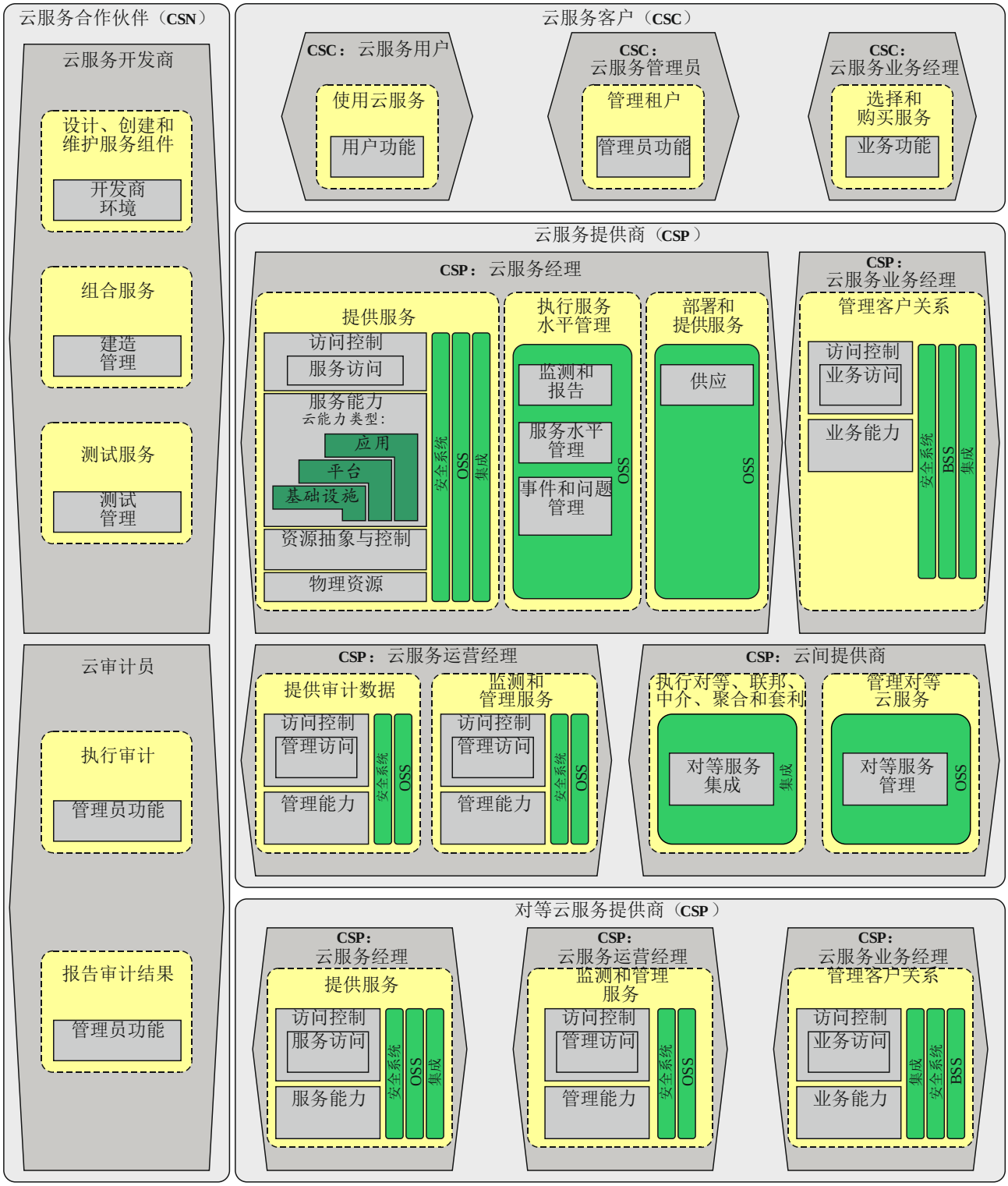
10.2.1 服务能力功能组件

云服务通过服务接口来提供，可以提供一种或多种**云能力类型**，由服务能力**功能组件**内的“倒L”形来表示。最上面的L形代表**应用能力类型**，而下一个较低的L形代表平台能力类型，底部的L形代表基础设施能力类型。

L形的含义是**应用能力类型**可以使用或不使用平台能力类型（由**云服务提供商**来选择）来实施，且平台能力类型可以使用或不使用基础设施能力类型来实施。

对**SaaS**或**CaaS云服务类别**，服务能力**功能组件**包含特定于应用的软件或通信应用程序，它们以实现SLA中确定之服务水平的方式部署到资源层上。

对其他**云服务类别**，请参阅ITU-T Y.3500建议书 | ISO/IEC 17788中的云计算概述和词汇表。



可审性、可用性、治理、互操作性、维护和版本控制、性能、便携性、个人可识别信息的保护、监管、适应性、可逆性、安全性、服务水平和服务水平协议

图10-1 – 角色、云计算活动和功能组件的通用视图

10.2.2 常见角色、活动和功能组件

在图10-1中，**云服务提供商**有一个**子角色**，即CSP：云服务经理，它执行提供服务**活动**，为**云服务客户**的CSC：云服务用户提供实际使用的服务。但在使用服务之前，需要开发和部署**云服务**才能运行。

这种情况涉及**云服务合作伙伴**的两个**子角色**，即云服务开发商和**云审计员**。云服务开发商使用开发工具**功能组件**来开发**云服务**的实施方案，并使用测试管理**功能组件**来测试服务。然后利用部署信息对云服务进行封装并提供给CSP：云服务经理，以执行部署和提供服务**活动**，从而在提供服务**活动**中提供服务能力**功能组件**。同时，**云审计员**根据各自的政策和治理制度，对云服务开发商、**云服务提供商**或**云服务客户**进行执行审计和报告审计结果**活动**。

CSP：云服务经理执行部署和提供服务**活动**后，提供服务**活动**使用服务能力**功能组件**，这是服务的实施方案，进而对运行服务所需的计算、存储和网络资源使用资源层**功能组件**。提供服务**活动**还涉及将服务能力**功能组件**与安全系统**功能组件**相集成，以提供安全和保护**个人可识别信息**能力，例如，数据加密。运营支持系统**功能组件**支持对服务和资源的管理、监测、自动化和配置。此外，CSP：云服务经理进行执行服务水平管理**活动**。执行服务水平管理**活动**管理**云服务**的**可用性**和性能，使之满足适用于**云服务**的、在**SLA**中定义的目标。使用服务水平管理**功能组件**、监测和报告**功能组件**以及事件和问题管理**功能组件**来完成此任务。

有时，CSP：云服务经理与另一个CSP：云服务经理开展协作以提供服务，调用该**对等云服务提供商**中的**云服务**。而后CSP：云服务经理执行管理**对等云服务活动**，以设置使用**对等云服务**的合同和**SLA**。**对等云服务提供商**还提供管理和使用**云计算活动**：提供服务和执行服务水平管理**云计算活动**，就像任何其他**云服务提供商**一样。

这些是有关CSP：云服务经理的一组常见**云计算活动**，但还有其他可以执行并在本规范中记录的**云计算活动**。

一旦**云服务**可供使用，两个**云服务客户子角色**将执行各种**活动**。首先，CSC：云服务管理员使用管理员功能**功能组件**执行管理租户**活动**，以设置租户并授予CSC：云服务用户访问权限。一旦完成，CSC：云服务用户通过利用用户功能**功能组件**执行使用**云服务活动**来与**云服务**交互。同时，CSC：云服务管理员通常会再次使用管理员功能**功能组件**来监测服务，以确保它正确运行并满足**SLA**的条款要求。

图10-2提供了**角色**、**云计算活动**和**功能组件**的视图，在多个**角色**的**云计算活动**之间绘制了链接。附件A对这些关系中的每一个做了描述。

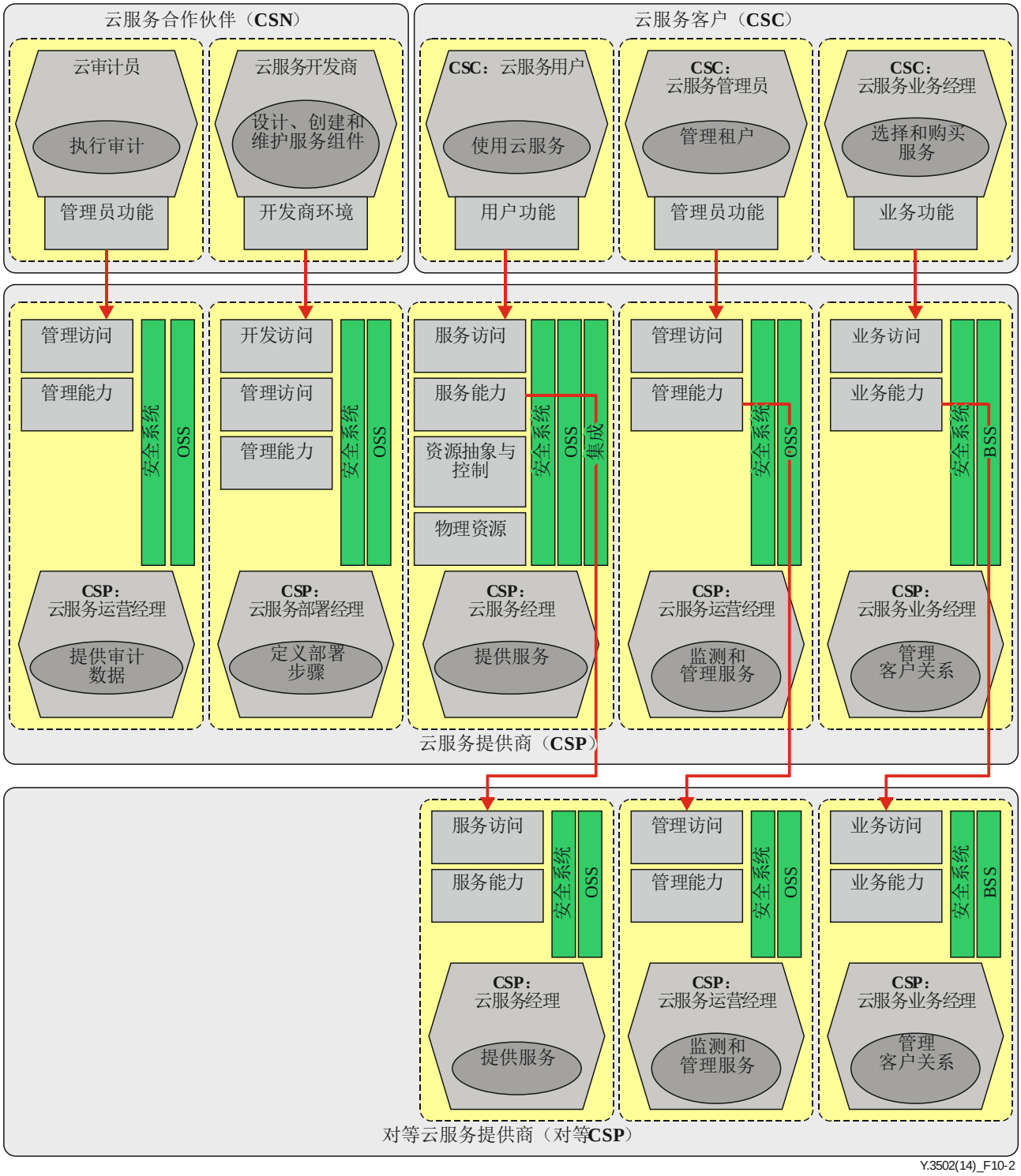


图10-2 – 活动与功能组件之间关系和交互示例

10.2.3 多租户和隔离

云计算涉及某些资源的共享，这通常意味着与所涉及的**云服务**的其他客户共享这些资源。术语**租户**和**多租户**用于描述共享资源的情况。

云服务的**租户**与**云服务客户**并不完全相同 – **租户**是一组CSC：云服务用户，它们共享对一组物理和虚拟资源的访问权限。通常，CSC：云服务用户组将与某个特定的**云服务客户**相关联，但一个**云服务客户**很可能有多个**租户** – 例如，来自客户组织内不同部门的用户组。

多租户是物理或虚拟资源的一种分配方式，通过它，多个**租户**及其计算和数据相互隔离且无法相互访问。换句话说，属于一个租户的用户应该完全不知道来自另一个租户的用户的存在。

多租户不仅影响**云服务**本身；它还影响**云服务提供商**向**云服务客户**提供的业务和管理能力。有关用户帐户、订购、使用和计费的信息都必须保持隔离，且仅对拥有相关租户的客户可见。必须特别注意日志文件等资源，这些资源可能包含与多个**租户**有关的记录。如果特定客户需要访问日志记录，例如，发生事件时，那么必须对日志记录加以过滤，以便客户只能看到与其租户有关的记录。

附件A

有关用户视图和功能视图的更多详细信息

（此附件为本建议书 | 国际标准的资料性组成部分。）

本附件提供了有关用户视图和功能视图关系的更多详细信息。

A.1 云服务客户 – 云服务提供商关系

在**云服务客户** – **云服务提供商**关系中有三个关键要素：

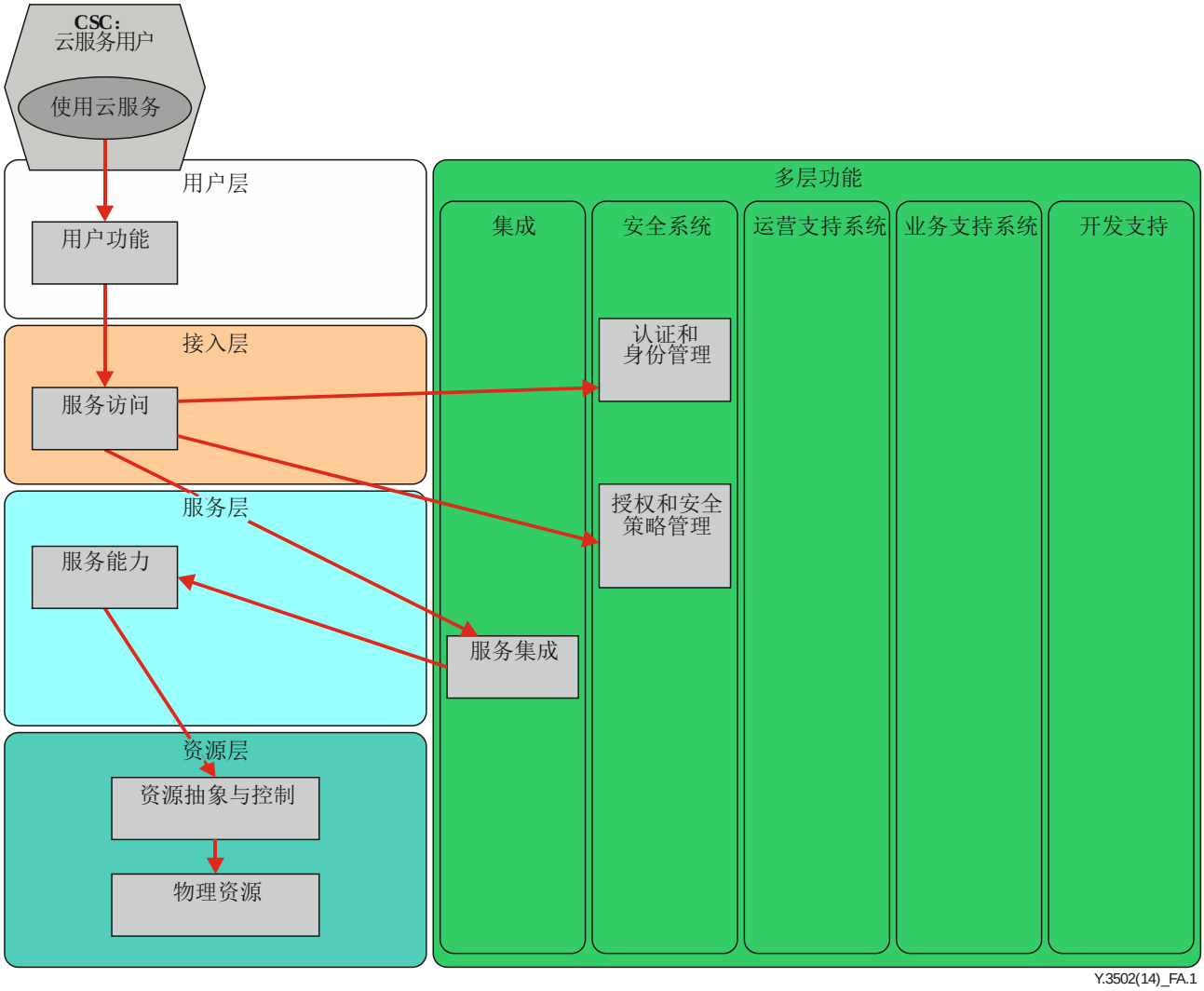
1) CSC：云服务用户使用提供商的**云服务**来实现其业务目标；
2) CSC：业务经理使用**云服务提供商**业务能力来订购云服务并从业务角度来对其使用进行管理；
3) CSC：云服务管理员使用**云服务提供商**管理能力从**云服务客户**角度来对云服务的使用进行管理。

A.1.1 功能关系

通过服务访问**功能组件**启用的端点和接口将**云服务**提供给CSC：云服务用户。该接口的功能和相关的信息流是特定于**云服务**的领域，因此不在参考架构的范围内。不过，有一些广泛的问题应该反映在服务接口中，特别是需要确定和认证CSC：云服务用户。

CSC：云服务用户通过用户功能**功能组件**来执行使用**云服务活动**，然后通过服务访问**功能组件**来调用**云服务**。服务访问**功能组件**执行对CSC：云服务用户的任何认证，并建立使用**云服务**特定能力的授权。如果得到授权，那么服务访问**功能组件**调用执行请求的**云服务**实施方案。

图A.1说明了CSC：云服务用户使用**云服务活动**中涉及的**功能组件**关系。



图A.1 – CSC：有关“使用云服务”活动的云服务用户关系

A.1.2 业务关系

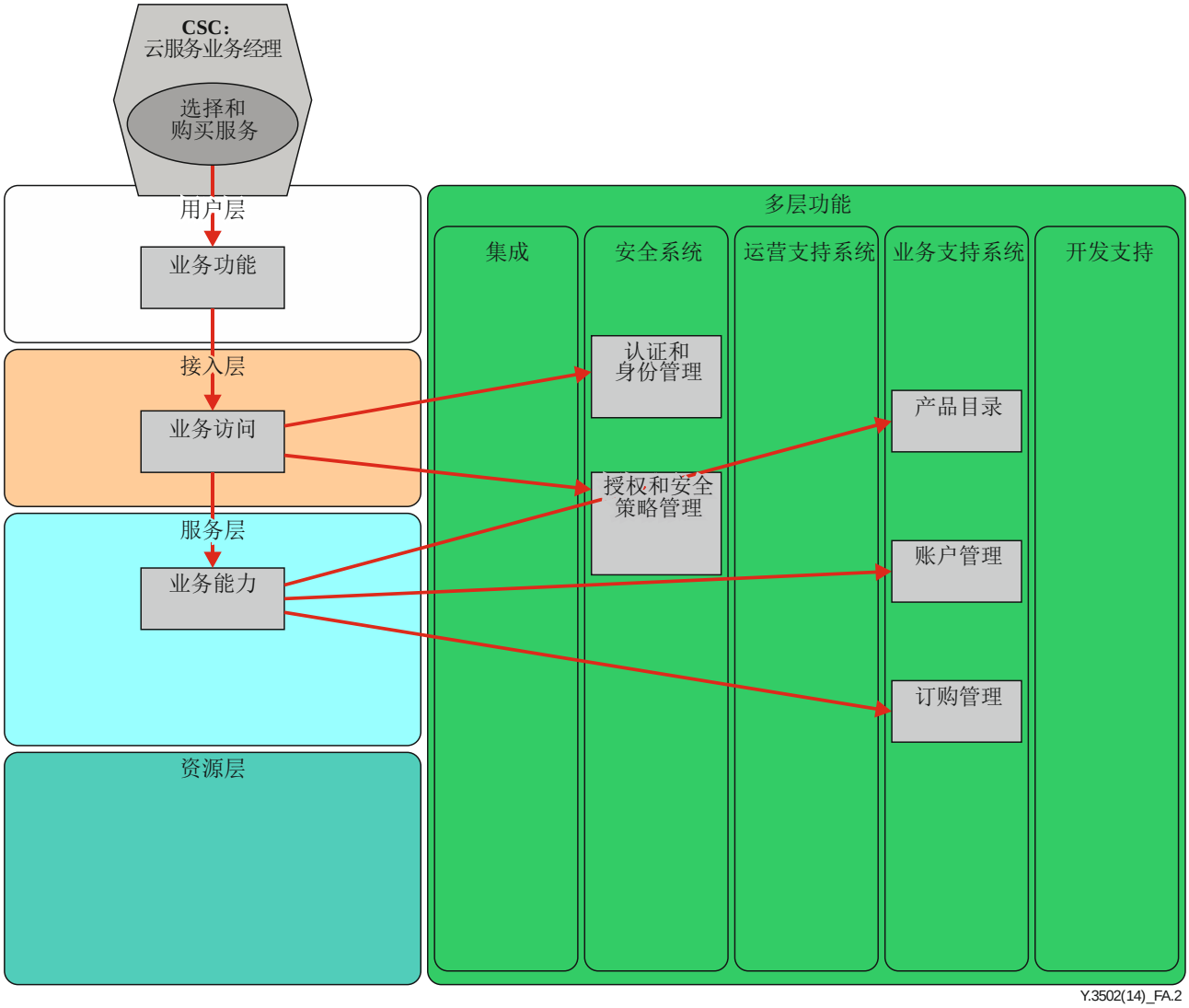
CSC：云服务业务经理通过用户层的业务功能**功能组件**来执行**云计算活动**选择和购买服务、执行业务管理和请求审计报告。业务功能**功能组件**通过业务访问**功能组件**启用的端点和接口来调用**云服务提供商**的业务能力。

业务访问**功能组件**执行对云CSP：云服务业务经理的任何认证，并建立使用业务能力特定功能的授权。业务能力**功能组件**与业务支撑系统**功能组件**交互，以完成CSC：云服务业务经理提出的请求 – 包括**产品目录**、账户管理和订购管理**功能组件**。

与业务能力有关的信息通常是：

- 可用**云服务**的**产品目录**条目，以及相关的技术信息、定价、条款和条件；
- 关于客户订购哪些服务的订购信息，以及相关的定量信息（例如，用户数量、数据量、处理量等）；
- 计费信息，它可包括关于使用费用、付款和帐户状态的信息。

图A.2说明了CSC：云服务业务经理在选择和购买服务**活动**中涉及的**功能组件**关系。



图A.2 – CSC：有关“选择和购买服务”活动的云服务业务经理关系

A.1.3 管理关系

CSC：云服务管理员通过管理员功能**功能组件**来执行以下云计算活动：

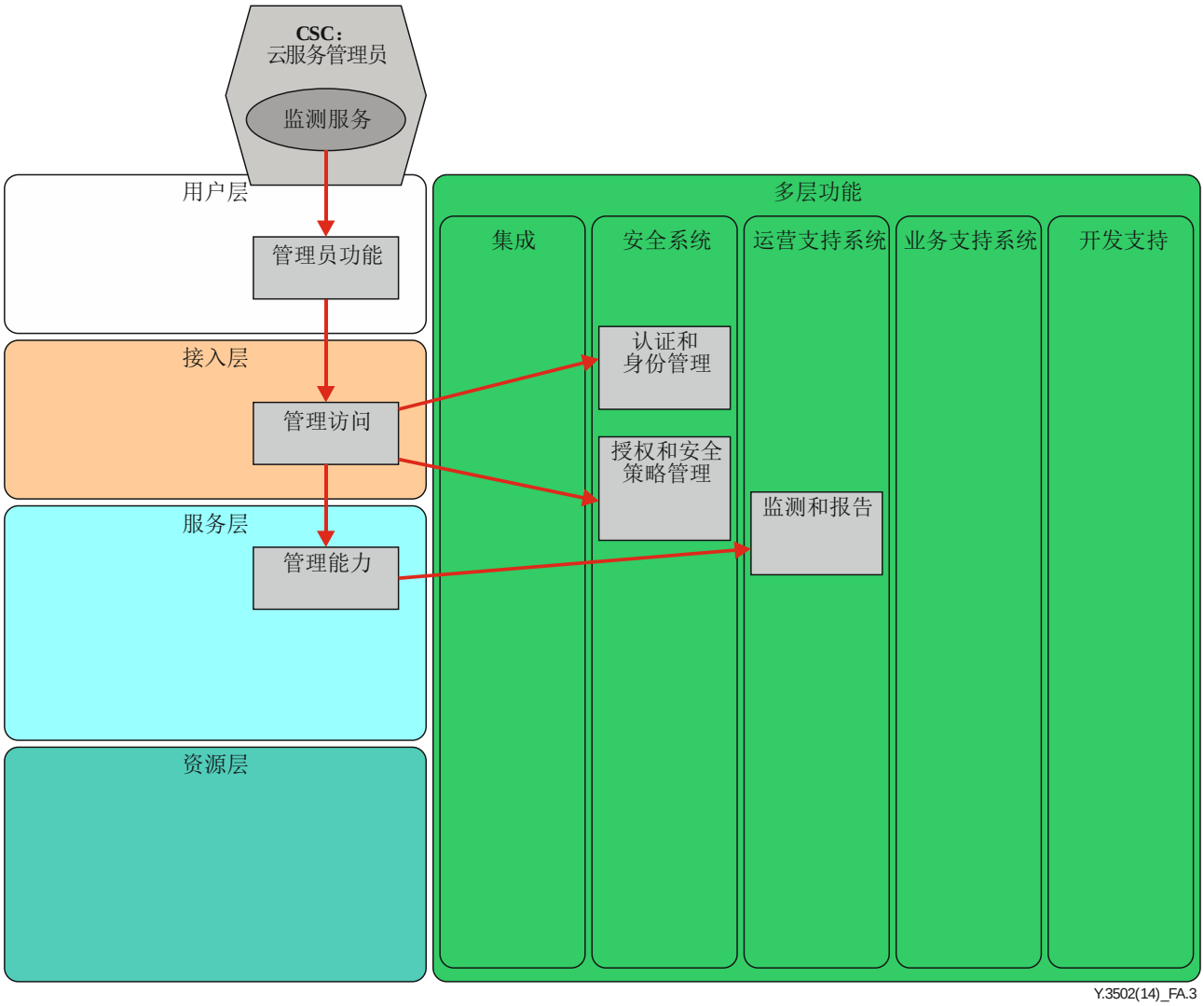
- 监测服务；
- 提供计费和使用报告；
- 管理租户；
- 管理服务安全性；
- 处置问题报告。管理员功能**功能组件**通过管理访问功能组件启用的端点和接口来调用**云服务提供商**的管理能力**功能组件**。

管理访问**功能组件**执行对CSC：云服务管理员的任何认证，并建立授权以使用管理能力**功能组件**的特定功能。管理能力**功能组件**与运营支持系统**功能组件**交互，以完成CSC：云服务管理员提出的请求，例如，监测和报告**功能组件**。

与管理能力有关的信息包括：

- 安全性信息，例如，用户帐户和授权数据的设置、数据的加密；
- 有关服务使用情况的通知，包括使用情况统计、日志记录（例如，出于安全目的）；
- 异常报告/事件（例如，违反某些服务**SLA**目标或发生安全事件）。

图A.3说明了CSC：云服务管理员监测服务**活动**中涉及的**功能组件**关系。



图A.3 – CSC：有关“监测服务”活动的云服务管理员关系

与**云服务客户** – **云服务提供商**关系相关的其他要素可包括客户与提供商之间的协议，它可包括**SLA**、知识产权问题和监管事项，例如，适当保护个人数据。

A.2 提供商 – 对等提供商（或“云间”）关系

云服务提供商可使用其他**云服务提供商**提供的一项或多项**云服务**。这被描述为提供商与**对等云服务提供商**的关系，或者称为“云间”关系 – 使用这些服务的提供商被称为主**云服务提供商**，而正在使用其服务的提供商被称为次**云服务提供商**。

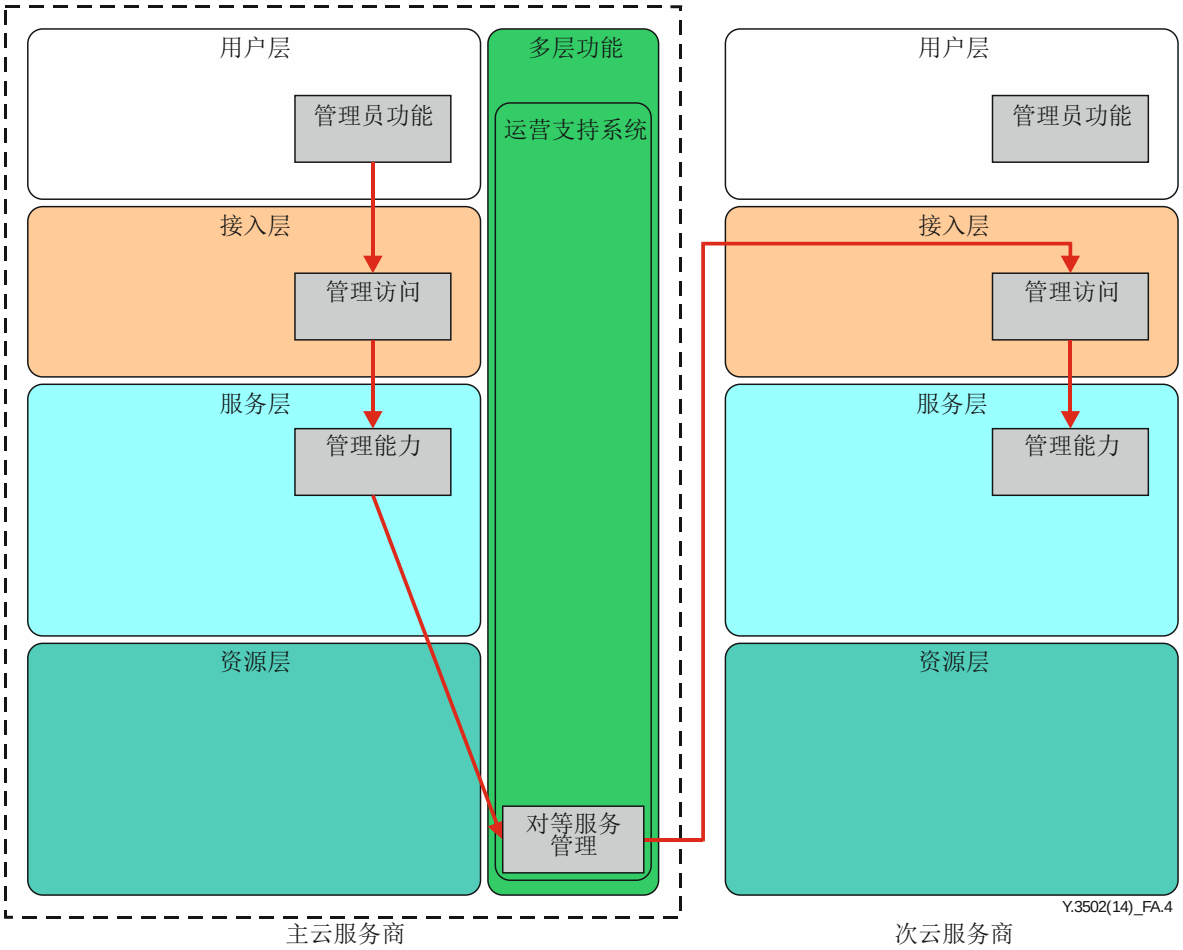
与**云服务客户** – **云服务提供商**关系的情况一样，对两个**云服务提供商**之间的关系存在两个**功能组件**：

- 主提供商使用次提供商**云服务**；
- 主提供商的CSP：云服务运营经理和CSP：云服务经理使用次提供商的业务和管理能力来建立和控制次提供商**云服务**的使用。

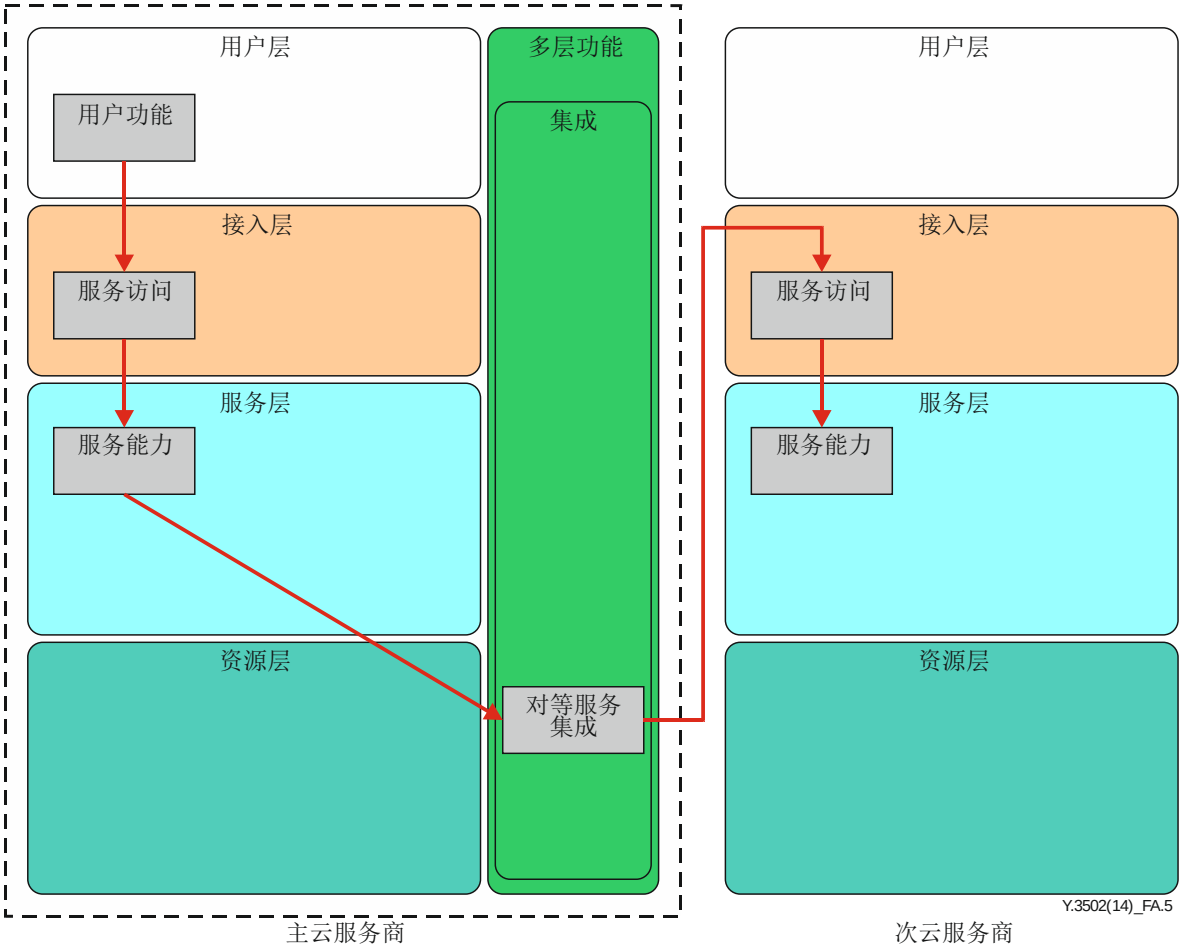
对次提供商，主提供商承担**云服务客户**的角色。次**云服务提供商**的服务由主**云服务提供商**的客户来提供和使用。次**云服务提供商**与主提供商的**云服务客户**之间由此产生的联系需要具体考虑安全性、PII保护和数据所有权等问题。

主提供商必须确保次提供商服务所提供的**SLA**适合主提供商服务的要求 – 并且任何违反**SLA**的行为都能得到适当管理。

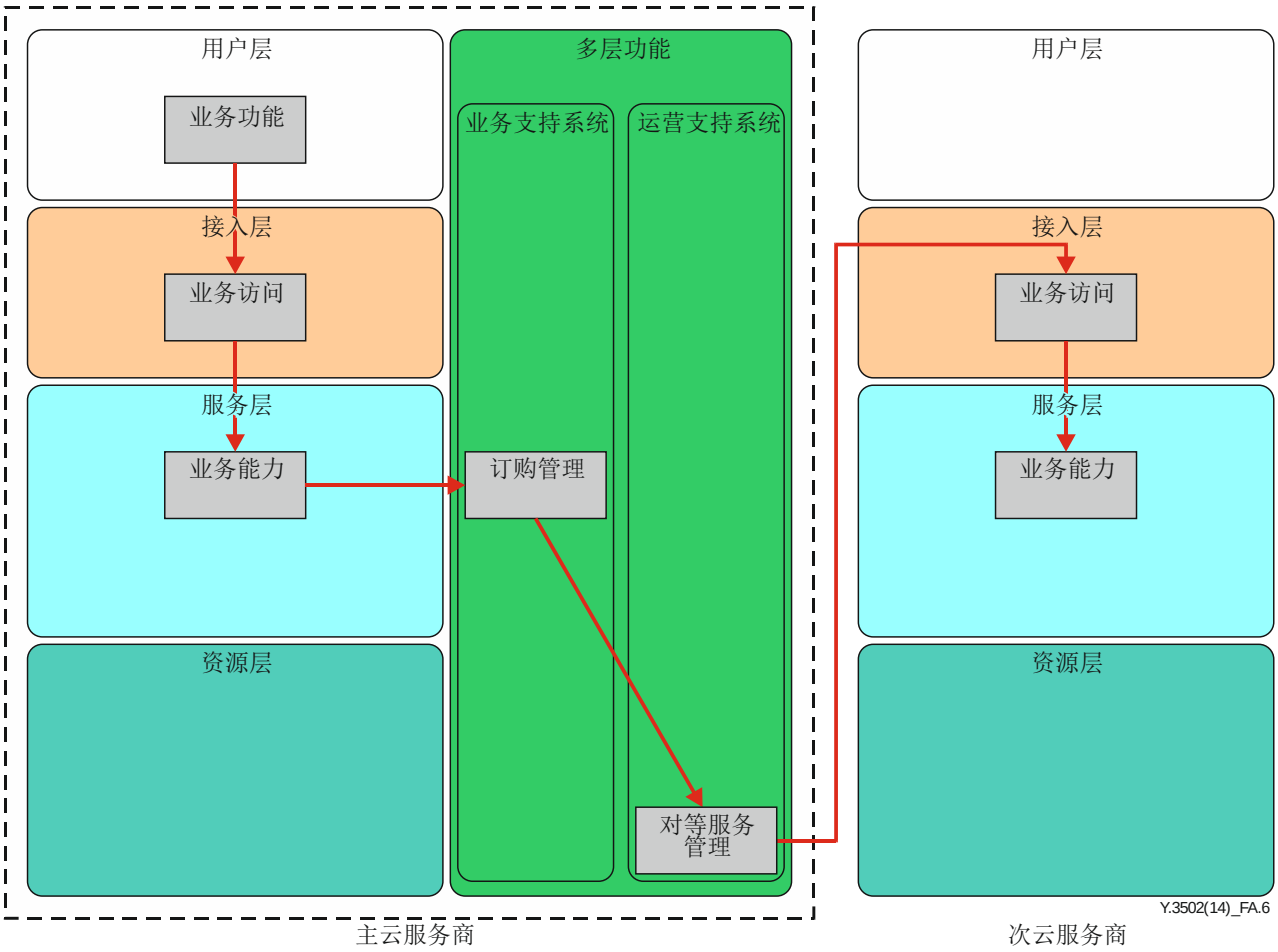
提供商 – 对等提供商关系中涉及三个接口 – 管理接口、业务接口和服务接口，它们广泛提供与**云服务客户 – 云服务提供商**关系中等效接口相同的功能。管理接口的使用方式如图A.4所示，服务接口的使用方式如图A.5所示，业务接口的使用方式如图A.6所示。



图A.4 – 有关管理员活动的提供商 - 对等提供商关系



图A.5 – 有关使用服务活动的提供商 - 对等提供商关系



图A.6 – 有关业务接口的提供商 - 对等提供商关系

A.3 云服务开发商 – 云服务提供商关系

云服务开发商创建并封装服务实施方案，并将之交给**云服务提供商**进行部署和运营。因此，云服务开发商与**云服务提供商**交互，以：

1) 检查**云服务提供商**的服务执行环境；
2) 测试服务实施方案；
3) 移交服务实施方案包。

开发支持**功能组件**支持云服务开发商的**云计算活动**，包括开发服务、测试服务和维护服务**云计算活动**。这些**云计算活动**依赖于开发环境、构建管理和测试管理**功能组件**。

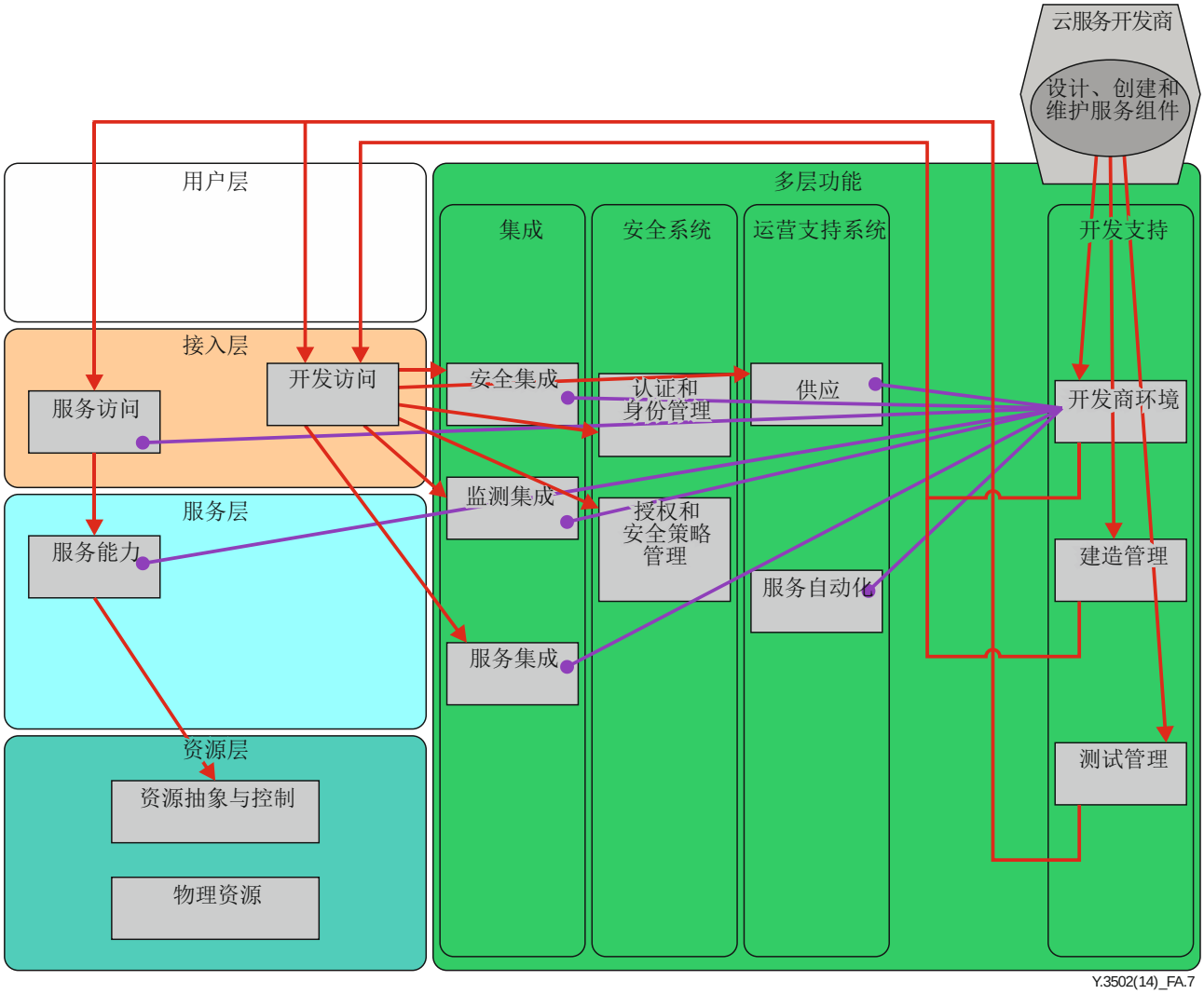
图A.7中从开发商环境组件辐射的线条表明，云服务开发商开发**云服务**的实施方案，并使用开发环境**功能组件**来组合服务，然后使用构建管理系统来在一个可部署的包中构建服务及其相关的工件。指向/来自测试管理**功能组件**的箭头表示测试管理系统对所构建的包执行适当的测试，从构建管理系统获取包并通过开发访问**功能组件**来与提供商的环境进行交互，以部署测试版本的服务并执行测试。

在图A.7中，来自开发环境的线条显示开发环境和构建管理系统用于创建软件和服务实施方案的相关工件（用于提供服务接口）。云服务开发商还可以创建服务访问实施方案。

为了在目标执行环境中运行服务实施方案和服务访问，需要开发正确的安全、监测、管理和自动化功能，以及集成到服务执行环境的功能。云服务开发商通过使用开发访问能力来发现合适的监测集成、安全集成和服务集成功能。此外，通过开发访问**功能组件**来检索启用认证和身份管理以及授权和安全策略管理的信息和要求。

还可以使用开发环境和构建管理系统（例如，通过脚本和配置元数据文件）来启用用于部署和供应的**云服务**功能。云服务开发商使用开发访问**功能组件**来发现供应和部署需求是什么。

服务实施方案与部署和供应信息封装在一起，并传给CSP：云服务经理，以执行部署服务**活动**，从而使服务可供客户在提供服务**活动**中使用。



图A.7 – 云服务开发商 – 云服务提供商关系

A.4 云服务提供商 – 审计员关系

云审计员应根据商定的规范、策略和协议开展审计。

审计规范可以是由**云服务提供商**设置的标准、由审计员设置的标准，或者是独立设置的标准（可能是法律要求的）。使用哪种标准取决于审计员审计结果的目标是什么。如果审计结果的目标是需要一些独立保证的**云服务客户**，那么审计应该使用独立设置的标准。

策略由提供商设置，用于审计提供商的基础设施和服务。这些策略由业务在治理过程中进行设置。

云服务协议可以包括与**云服务提供商**和可能的**云服务客户**之审计有关的条款。主**云服务提供商**与次**云服务提供商**之间可以签订类似的协议。审计员的职责在每种情况下都是相同的。

云审计员的**云计算活动**有安全审计、隐私影响审计和性能审计。对所有这些**云计算活动**，**云审计员**都可从**云服务提供商**处获取审计证据。审计证据的形式将因审计类型和适用于审计的标准而有所不同。证据可采取程序文件的形式，也可采取日志记录的形式。在任何情况下，**云服务提供商**都可以通过某种方式来让**云审计员**获得所需的证据。

在图10-2中，**云审计员**的执行审计**活动**通过**云服务提供商**的管理访问**功能组件**向**云服务提供商**提出有关审计证据的请求，并调用必要的管理能力。

A.4.1 安全审计

系统安全审计存在各种标准。ISO/IEC 27001就是这样一种标准，它涵盖**信息安全**管理。还有许多其他组织为云安全提供可审计的标准。

A.4.2 隐私影响审计

各种各样的数据保护机构（例如，加拿大的隐私专员和英国的信息专员）发布了有关评估和/或审计方案、策略或系统之隐私影响的指导方针。**PII的保护**通常受制于法规和/或立法，但与**云服务**相关的问题之一是**云服务客户**可能位于与适用于**云服务提供商**的司法管辖区不同的司法管辖区中。如果**云服务提供商**在不同的司法管辖区运营多个数据中心并在这些数据中心之间移动数据或执行服务（例如，出于服务连续性或高效使用资源的目的），那么情况可能会变得更加复杂。

ISO/IEC 27018是一项标准，它定义了**云服务提供商**在充当数据处理器时适用的**信息安全**控制。ISO/IEC还处理更广泛的隐私问题（例如，参见ISO/IEC 29100系列标准）。

云审计员应根据数据保护机构发布的指导方针和相关标准，评估**云服务**的**个人可识别信息**保护和**云服务提供商**的运营是否符合相应司法管辖区的数据保护法规。

A.4.3 性能审计

性能审计旨在评估**云服务提供商**达成为其**云服务**指定的性能目标的能力，通常记录在**SLA**中。

参考书目

- ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.（信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇表）
- ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.（信息技术 – 安全技术 – 信息安全管理系统 – 要求）
- ISO/IEC 27002:2013, *Information technology – Security techniques – Information security management systems – Code of practice for information security management*.（信息技术 – 安全技术 – 信息安全管理系统 – 信息安全管理行为准则）
- ISO/IEC 27018:2014, *Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.（信息技术 – 安全技术 – 信息安全管理系统 – 在充当PII处理器的公有云中保护个人可识别信息 (PII) 的行为准则）
- ISO/IEC/IEEE 24765:2010, *Systems and software engineering – Vocabulary*.（系统和软件工程 – 词汇表）
- ISO/IEC/IEEE 42010:2011, *Systems and software engineering – Architecture description*.（系统和软件工程 – 架构描述）

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费和结算原则以及国际电信/ICT经济和政策问题
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	环境和ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M系列	电信管理，包括电信网管管理和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令以及相关的测量与测试
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网络、开放系统通信和安全
Y系列	**全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦