ICS 35.100.05
L 79

中华人民共和国国家标准

GB/T 32399—2015

信息技术　云计算　参考架构

Information technology—Cloud computing—Reference architecure

(ISO/IEC 17789:2014,MOD)

2015-12-31 发布　　2017-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中华人民共和国
国家标准
信息技术 云计算 参考架构
GB/T 32399—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.5 字数 102 千字
2016年2月第一版 2016年2月第一次印刷
*
书号:155066·1-52850 定价 48.00 元

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准使用重新起草法修改采用国际标准 ISO/IEC 17789:2014《信息技术　云计算　参考架构》。

本标准与 ISO/IEC 17789:2014 相比，除编辑性修改外主要技术变化如下：

——合并了第 2 章规范性引用文件中的 2.1 和 2.2，删除 2.1 和 2.2 条款号及标题；

——修改了正文中的图号，由按章编号修改为按在本标准中出现的顺序编号；

——修改了正文中的表号，由按章编号修改为按在本标准中出现的顺序编号；

——第 4 章增加了缩略语 OSS；

——修改了附录 B 为参考文献(见参考文献)。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位：中国电子技术标准化研究院、深圳市金蝶中间件有限公司、中国移动通信有限公司研究院、华为技术有限公司、浪潮(北京)电子信息产业有限公司、东软集团股份有限公司、上海计算机软件技术开发中心、中兴通讯股份有限公司、北京东方通科技股份有限公司、大唐电信科技股份有限公司、工业和信息化部电子第五研究所、中国软件与技术服务股份有限公司、太极计算机股份有限公司。

本标准主要起草人：王洁萍、林琳、文兰玲、田忠、李海波、周平、王宝艾，吴涛、邵伟翔、丁蔚、何光宇、蔡立志、徐宝新、魏乐霞、陈娜、刘俊鹏、寇欣、董晶、严磊、李东、陈志峰、杨丽蕴。

信息技术　云计算　参考架构

1　范围

本标准规定了云计算参考架构(CCRA),包括**云计算角色**、**云计算活动**、**云计算功能组件**以及他们之间的关系。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 32400—2015　信息技术　云计算　概览与词汇(ISO/IEC 17788:2014,IDT)

ISO/IEC 29100:2011　信息技术　安全技术　隐私框架(Information technology—Cloud computing—Overview and vocabulary)

3　术语和定义

GB/T 32400—2015 界定的以及下列术语和定义适用于本文件。

3.1　其他标准中定义的术语

3.1.1

架构　architecture

通过系统元素、元素间的关系,以及系统设计和进化原则体现出来的一个系统在其环境中的基本概念或属性。

[ISO/IEC/IEEE 42010:2011]

3.1.2

个人识别信息　personally identifiable information

PII

能用于识别相关的 PII 主体,或可能与某 PII 主体直接或间接相关的信息。

[ISO/IEC 29100:2011]

注:为了判定某个 PII 主体是否可识别,必须考虑持有数据的隐私相关方或其他**参与方**为识别某自然人能合理采取的所有措施。

3.2　本标准中定义的术语

3.2.1

活动　activity

一组特定任务的集合。

3.2.2

云服务产品　cloud service product

与一组商业条款一同被提供的一个云服务。

注:商业条款能包括定价、定级和服务水平。

3.2.3

功能组件　functional component

参与**活动**(3.2.1)所需的,可实现的一个功能构件块。

3.2.4

对等云服务　peer cloud service

某个云服务提供者提供的,用于组成其他一个或多个云服务提供者云服务的云服务。

3.2.5

对等云服务提供者　peer cloud service provider

为其他一个或多个云服务提供者提供部分云服务的云服务提供者。

3.2.6

产品目录　product catalogue

云服务提供者提供给云服务客户的所有**云服务产品**(3.2.2)列表。

3.2.7

角色　role

一组服务于共同目的的**活动**(3.2.1)的集合。

3.2.8

服务目录　service catalogue

某个云服务提供者的所有云服务的列表。

3.2.9

子角色　sub-role

给定**角色**(3.2.7)的**活动**(3.2.1)的子集。

4　缩略语

下列缩略语适用于本文件。

API　应用编程接口(Application Programming Interface)

CaaS　通信即服务(Communications as a Service)

CCRA　云计算参考架构(Cloud Computing Reference Architecture)

CPU　中央处理单元(Central Processing Unit)

CS　云服务(Cloud Service)

CSC　云服务客户(Cloud Service Customer)

CSN　云服务合作者(Cloud Service Partner)

CSP　云服务提供者(Cloud Service Provider)

IaaS　基础设施即服务(Infrastructure as a Service)

ICT　信息和通信技术(Information and Communication Technology)

KPI　关键性能指标(Key Performance Indicator)

MSA　主服务协议(Master Service Agreement)

NaaS　网络即服务(Network as a Service)

OSS　运营支撑系统(Operational Support System)

PaaS　平台即服务(Platform as a Service)

PII　个人识别信息(Personally Identifiable Information)

QoS 服务质量(Quality of Service)
RAM 随机访问内存(Random Access Memory)
SaaS 软件即服务(Software as a Service)
SLA 服务水平协议(Service Level Agreement)
ToS 服务条款(Terms of Service)
T&C 条款(Terms and Conditions)
VLAN 虚拟局域网(Virtual Local Area Network)
VPN 虚拟专用网(Virtual Private Network)
VM 虚拟机(Virtual Machine)

5 约定

本标准采用以下约定：

a) 本标准采用图来帮助理解 CCRA。图 1 给出了图中使用的图例；

注：图 1 中，“关注点”指的是共同关注点。

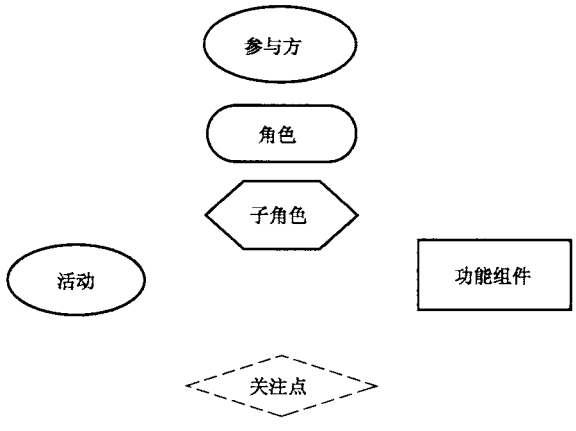

图 1 本标准的图中使用的图例

b) CCRA 使用术语“ICT”和“ICT 系统”。缩略语 ICT 指的是 ISO/IEC/IEEE 24765:2010 3.1332[5]中定义的“信息和通信技术”。使用 ICT 是为了表明 CCRA 不仅包含了计算机系统相关的计算和存储技术，还包含了连接不同系统的通信技术；

c) 对第三章中术语的引用采用粗体字标识。

6 CCRA 的目的和目标

云计算是一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式[ITU-T Y.3500|ISO/IEC 17788]。

本标准中的云计算参考架构提供了一个体系框架，用于有效描述**云计算角色**、**子角色**、**云计算活动**、共同关注点、功能架构和**云计算功能组件**。

CCRA 的目的包括：

- 描述云计算的利益相关者群体；
- 描述云计算系统的基本特征；

- 规范基本的**云计算活动**和**功能组件**，描述它们之间的关系以及它们与环境之间的关系；
- 识别 CCRA 设计和改进的指导原则。

CCRA 的核心标准化目标包括：

- 有助于制定一系列协调配套的**云计算**国际标准；
- 为定义**云计算**标准提供一个技术中立的参考点；
- 在识别**云计算**利益和风险时提倡开放性和透明性。

CCRA 重点关注**云服务**提供什么，而不是如何设计基于云的解决方案和实现方式。尽管 CCRA 可能会限制某个实际系统的系统架构，但是 CCRA 并不代表任何具体**云计算**系统的系统架构。CCRA 并不依赖于任何具体提供商的产品、服务或参考实现，也不定义有碍创新的常规方案。

CCRA 还用于：

- 帮助理解**云计算**的运营复杂性；
- 展示和理解各类**云服务**以及服务的供应和使用；
- 为国际社区理解、讨论、分类和比较**云服务**提供技术参考；
- 为使用通用的参考架构描述、讨论和编制系统特定的架构提供工具；
- 促进在下述领域进行潜在标准分析，包括：安全、**互操作性**、可移植性、**可复原性**、可靠性和服务管理，同时支持后续的参考实现分析。

7 参考架构概念

本标准定义的 CCRA 能作为**云计算**标准化的基本参考点，同时也为**云计算**系统的基本概念和原则提供一个总体框架。

本章给出了本标准所使用的体系化方法。

7.1 CCRA 的架构视图

云计算系统能采用视图方法进行描述。

CCRA 采用 4 个不同的视图进行描述(如图 2)：

- 用户视图；
- 功能视图；
- 实现视图；
- 部署视图。

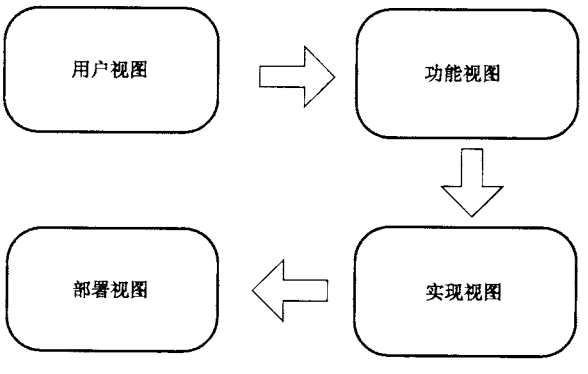

图 2 不同架构视图之间的转换

表 1 给出对每个视图的描述。

表 1 CCRA 视图

CCRA 视图	视图描述	范围
用户视图	系统环境、**参与方**、**角色**、**子角色**和**云计算活动**	范围内
功能视图	支撑**云计算活动**的所需功能	范围内
实现视图	实现服务、基础设施部件内的**云服务**所需的功能	范围外
部署视图	基于已有或新增的基础设施，对**云服务**功能的技术实现	范围外
注：虽然本标准包含了对用户视图和功能视图的详细描述，但并不包含对实现视图和部署视图的描述，因为实现视图和部署视图与技术，以及供应者特定的**云计算**实现和部署方式相关。		

图 3 给出了用户视图向功能视图的转换。详细信息见 7.4。

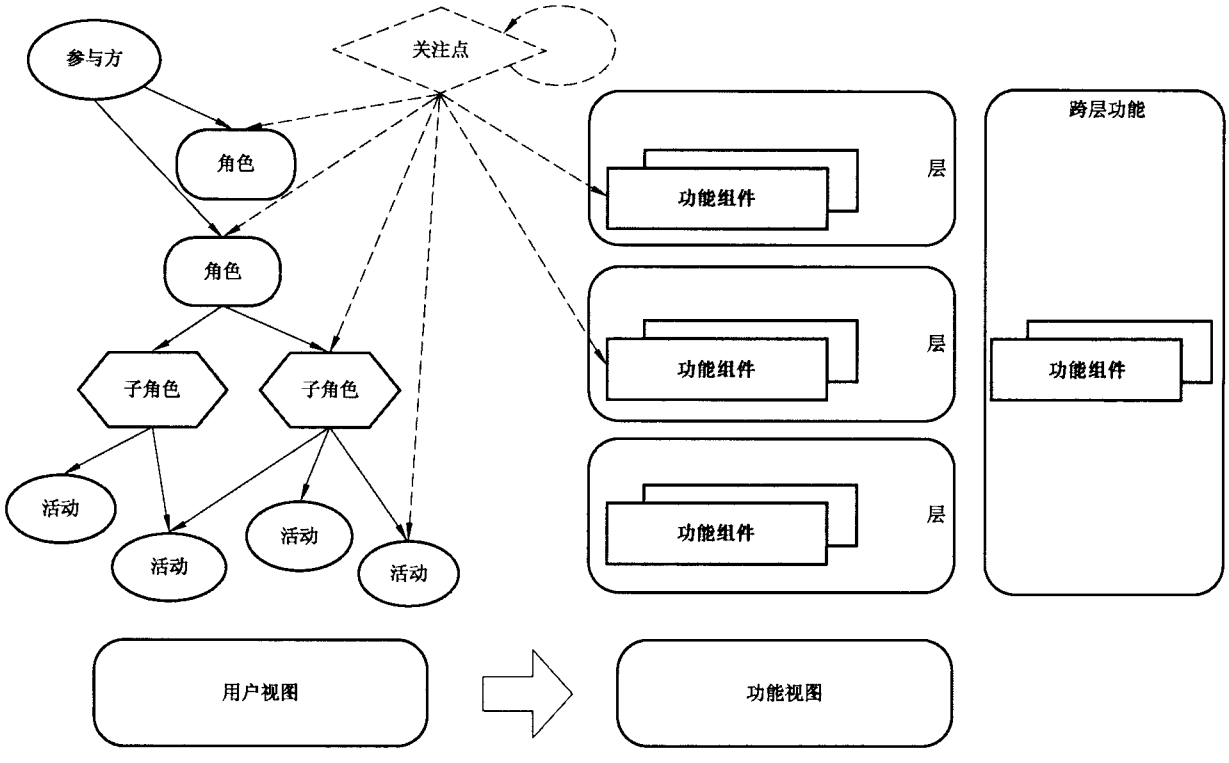

图 3 用户视图向功能视图的转换

7.2 云计算用户视图

用户视图涉及以下云计算概念：

- **云计算活动**；
- **角色**和**子角色**；
- **参与方**；
- **云服务**；
- **云部署模型**；
- 共同关注点。

图 4 展示了用户视图所定义的实体。

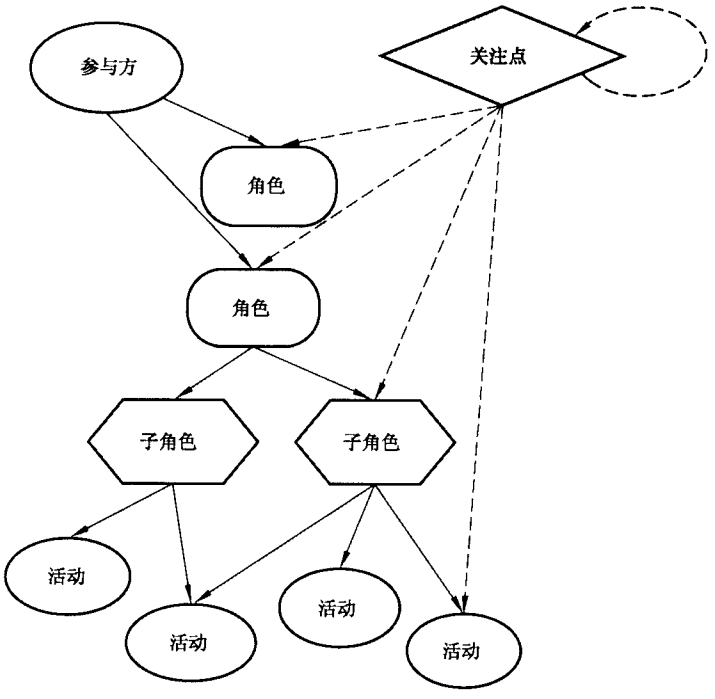

图 4　用户视图实体

7.2.1　云计算活动

云计算活动定义为一组特定任务的集合。

云计算活动需要有一个目标，并能交付一个或多个结果。

云计算系统的活动通过**功能组件**来实现(见 7.3)。

第 8 章给出**云计算**活动并进行详细描述。

7.2.2　角色和子角色

角色是一组具有共同目标的**云计算活动**的集合。

CCRA 定义了 3 个主要角色：

- **云服务客户(CSC)**：使用**云服务**的业务**参与方**；
- **云服务提供者(CSP)**：提供**云服务**的**参与方**；
- **云服务合作者(CSN)**：为**云服务提供者**、**云服务客户**的活动提供支撑或辅助功能的**参与方**。

子角色是某个指定**角色**的**云计算活动**的子集。

某个**角色**的**云计算活动**能被该角色下的不同的**子角色**所共享。

第 8 章给出**云计算**的**角色**和**子角色**描述。

7.2.3　参与方

参与方是一个或一组自然人或者法人，不论该法人是否注册。**云计算**系统中的**参与方**是**云计算**系统的利益相关者。

在某个给定时间点，参与者可承担多个**角色**，也可承担某个**角色**活动的指定子集。在**云计算**系统中，任何**参与方**至少需要承担一个**角色**才能成为利益相关方。

7.2.4 云服务

云服务是**云计算**的核心要素。云计算概览与词汇(ITU-T Y.3500|ISO/IEC 17788)给出了对**云服务**的定义。本节给出内容概述。

云服务可根据提供资源的不同,通过其提供的**云能力类型**进行描述。**云能力类型**包括3类:

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

云计算概览与词汇(ITU-T Y.3500|ISO/IEC 17788)给出了对**云能力类型**和**云服务类别**的定义。

云服务组成不同的服务类别。每一类云服务代表一组具有相同质量特征的云服务。服务类别中的**云服务**能包含一个或多个**云能力类型**。

典型的**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)**。

其他的**云服务类别**在云计算概览与词汇(ITU-T Y.3500 | ISO/IEC 17788)中描述。

7.2.5 云部署模型

云计算概览与词汇(ITU-T Y.3500 | ISO/IEC 17788)给出了对**云部署模型**的定义。本节给出内容概述。

云部署模型是根据对物理或虚拟资源的控制和共享方式对**云计算**进行的分类。

云部署模型包括:

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

7.2.6 共同关注点

共同关注点指的是需要在不同**角色**之间协调,且在**云计算**系统中一致实现的行为或能力。

共同关注点能被多个**角色**、**云计算活动**和**功能组件**所共享,且对他们产生影响。

共同关注点适用于多个不同的**角色**或**功能组件**。

8.5给出对共同关注点的描述。

7.3 云计算功能视图

功能视图是构建**云计算**系统所必需功能的技术中立的视图。功能视图描述了支持**云计算活动**所必需功能的分布。

功能架构还定义了功能之间的依赖关系。

功能视图涵盖了以下**云计算**概念:

- **功能组件**;
- 功能层;

- 跨层功能。

图 5 展示了功能、层和**功能组件**的概念。

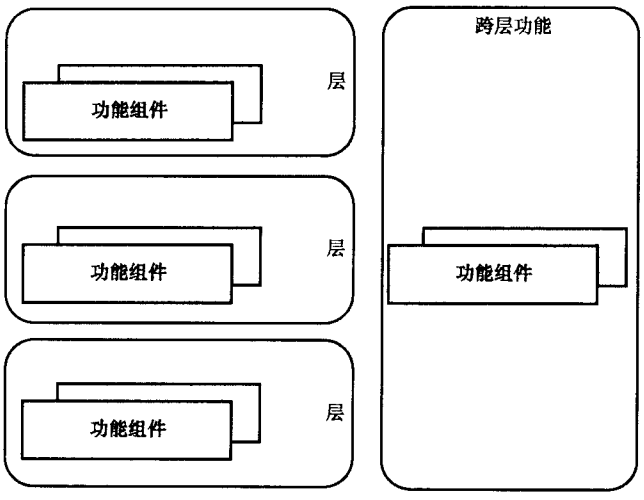

图 5　功能层

9.1 描述**云计算**功能架构。

7.3.1　功能组件

一个**功能组件**是参与某一活动所需的，能实现的功能构件。

云计算系统的能力完全由一组已实现的**功能组件**所定义。

9.2 进一步描述**功能组件**。

7.3.2　功能层

层是一组提供类似功能或服务于共同目标的**功能组件**的集合。

功能架构可部分层次化(即包含多个层和一组跨层功能)。

CCRA 定义了 4 个不同的层：

- 用户层：支撑**云服务客户**和**云服务合作者**的**云计算活动**的**功能组件**；
- 访问层：有助于功能分配和功能互连的**功能组件**；
- 服务层：提供**云服务**，以及实现相关的管理能力、业务能力和服务编排能力的**功能组件**；
- 资源层：为实现**云计算**系统所需资源的**功能组件**。

需要注意的是，对于某个具体的**云计算**系统，并不需要提供上述的全部**功能组件**层次。

7.3.3　跨层功能

跨层功能提供跨越多个功能层次能力的**功能组件**。跨层功能可进行分组。

已定义的跨层功能子集包括：

- 开发功能；
- 集成；
- 安全系统；
- 运营支撑系统；
- 业务支撑系统。

9.2.5 描述跨层功能组件。

7.4 用户视图和功能视图之间关系

图 6 展示了用户视图如何提供云计算活动的集合，以及这些云计算活动在功能视图中如何表示（并通过实现视图中的技术来实现）。

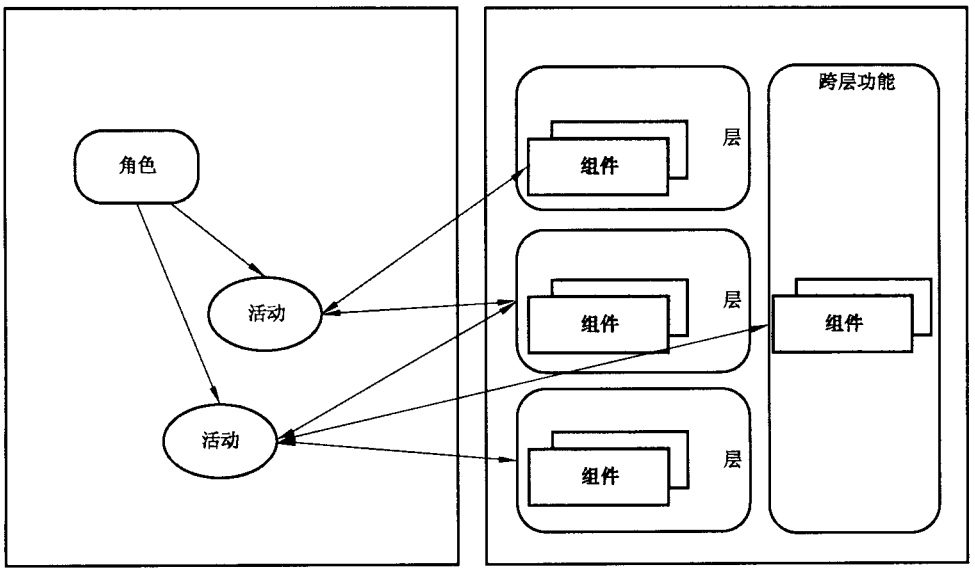

图 6 从用户视图到功能视图

第 10 章进一步描述用户视图和功能视图之间的关系。

7.5 用户视图与共同关注点以及功能视图与共同关注点之间关系

如名称所示，共同关注点既适用于云计算的用户视图，又适用于云计算的功能视图。

共同关注点适用于用户视图中的角色和子角色，并且直接或间接地影响这些角色所执行的活动。

共同关注点也适用于功能视图中的功能组件。这些组件在执行用户视图所描述的活动时被使用。

8.5 描述云计算的共同关注点。共同关注点包括：

- 可审计性；
- 可用性；
- 治理；
- 互操作性；
- 维护和版本控制；
- 性能；
- 可移植性；
- 隐私；
- 健壮性；
- 可复原性；
- 安全；
- 服务水平和服务水平协议。

7.6 云计算实现视图

虽然本标准详细描述了用户视图和功能视图，但是实现视图不在本标准的范围之内。

7.7 云计算部署视图

虽然本标准详细描述了用户视图和功能视图，但是部署视图不在本标准的范围之内。

8 用户视图

8.1 角色、子角色和云计算活动概述

云计算的核心是分布式服务及服务交付。据此将所有云计算相关的活动分为3组：使用服务的活动、提供服务的活动和支撑服务的活动。

本章描述一些常用的与云计算相关的角色和子角色。

值得注意的是：在任意给定的时间点，一个参与方可承担多个角色。当承担一个角色时，参与方可限制其只承担该角色的一个或多个子角色。对于给定角色，子角色是其云计算活动的子集。

如图7所示，云计算的角色包括：

- 云服务客户(见8.2)；
- 云服务提供者(见8.3)；
- 云服务合作者(见8.4)。

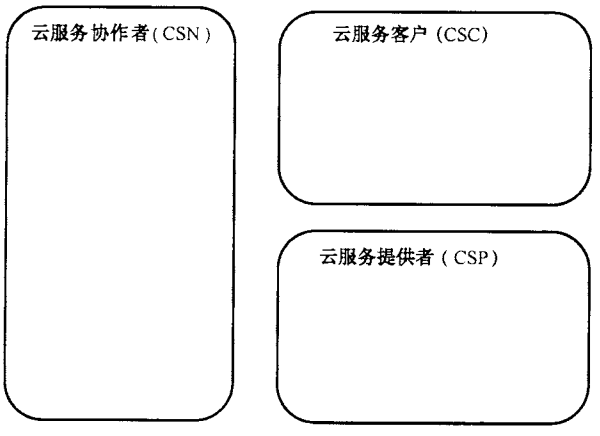

图7 云计算角色

图8展示了云计算的角色及其包含的子角色。后续章节中详细描述图中的每一个子角色。

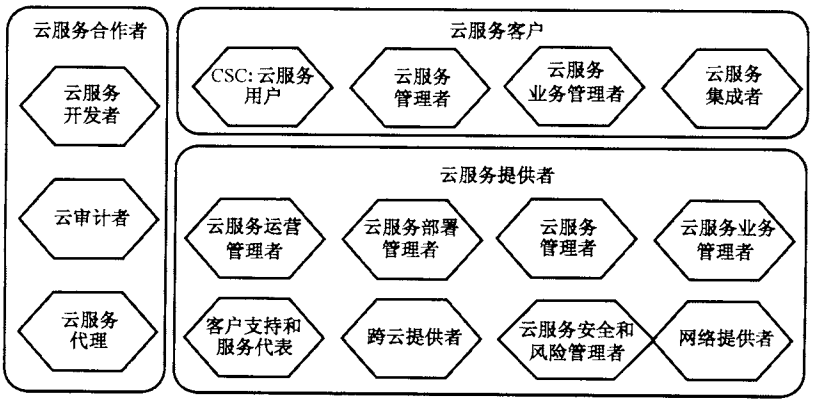

图8 角色和子角色

8.2 云服务客户

8.2.1 角色

为使用云服务，云服务客户与云服务提供者建立业务关系。云服务客户也可出于各种原因与云服务合作者建立业务关系。

云服务客户的活动包含在 8.2.1.1～8.2.1.4 所描述的子角色中。

8.2.1.1 CSC：云服务用户

云服务用户是云服务客户的一个子角色。云服务用户是自然人，或代表该自然人的实体。云服务用户与某个云服务客户相关。该云服务客户使用云服务。

云服务用户的云计算活动包括：

- 使用云服务（见 8.2.2.1）。

8.2.1.2 CSC：云服务管理者

云服务管理者是云服务客户的一个子角色。云服务管理者的主要目的是保证用户使用云服务时运行稳定，同时保证云服务与客户已有的 ICT 系统和应用之间运行良好。云服务管理者监控所有与使用云服务相关的操作流程，并承担云服务客户与云服务提供者之间技术交互的切入点。

云服务管理者的云计算活动包括：

- 试用服务（见 8.2.2.2）；
- 监控服务（见 8.2.2.3）；
- 安全策略管理（见 8.2.2.4）；
- 提供计费和使用量报告（见 8.2.2.5）；
- 问题处理（见 8.2.2.6）；
- 管理租户（见 8.2.2.7）。

8.2.1.3 CSC：云服务业务管理者

云服务业务管理者是云服务客户的一个子角色，其目的是通过经济有效的方式获取和使用云服务，满足云服务客户的业务目标。业务管理者的主要职责是关注使用云服务时的财务和法律方面，包括批准，持续的所有权和责任。

云服务业务管理者的云计算活动包括：

- 执行业务管理（见 8.2.2.8）；
- 选择和购买服务（见 8.2.2.9）；
- 获取审计报告（见 8.2.2.10）。

8.2.1.4 CSC：云服务集成者

云服务集成者是云服务客户的一个子角色，负责云服务与云服务客户现有 ICT 系统的集成，包括应用功能和数据的集成。

云服务集成者的云计算活动包括：

- 连接 ICT 系统和云服务（见 8.2.2.11）。

8.2.2 云计算活动

与云服务客户的子角色相关的云计算活动如图 9 所示：

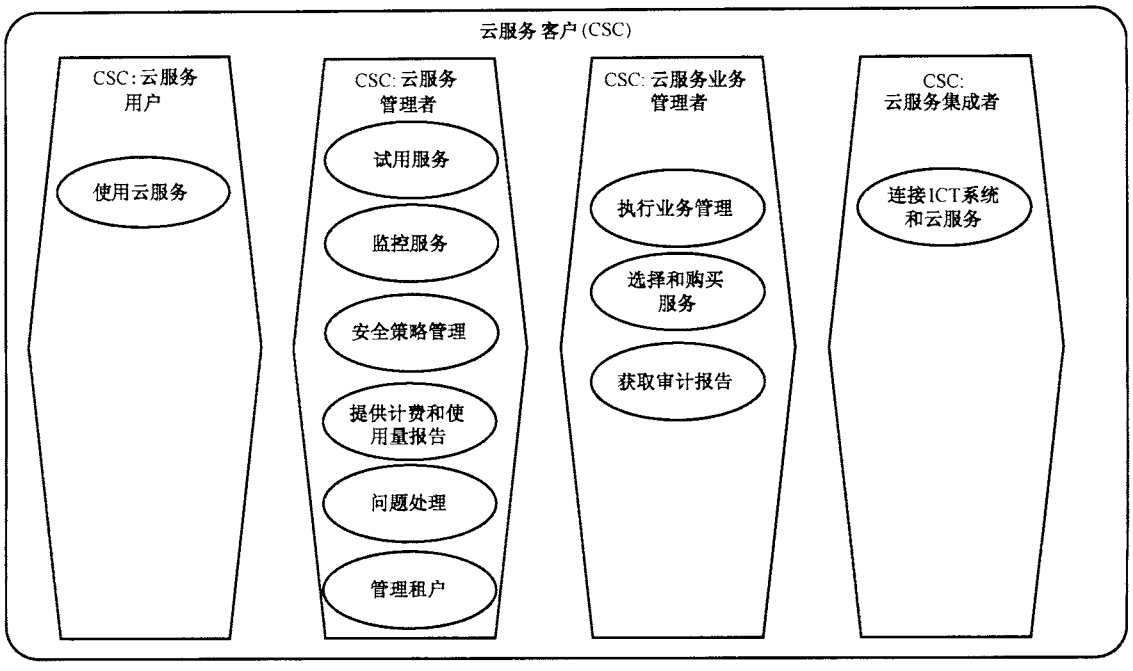

图 9　与云服务客户的子角色相关的云计算活动

8.2.2.1　使用云服务

使用云服务活动指的是为了完成某些任务使用云服务提供者的服务。

典型的使用云服务活动包含：

- 提供用户证书，使得云服务提供者能够认证用户并赋予对云服务的访问权限；
- 调用云服务去执行操作并交付特定结果。

8.2.2.2　试用服务

试用服务活动指的是使用云服务提供者的服务以确保云服务能够满足云服务客户的业务需求。在云服务提供者和云服务客户相互同意和理解，进行服务试用的基础上使用云服务。

试用服务活动包括：

- 提供用户证书，使得云服务提供者能够认证用户并赋予对“测试”云服务的访问权限；
- 调用“试用”云服务。云服务客户能对“试用”云服务进行业务需求的测试。

8.2.2.3　监控服务

监控服务活动根据云服务客户与云服务提供者之间的服务水平协议(SLA)所定义的服务水平监控已交付服务的质量。该活动利用云系统固有的监控功能。该活动包括：

- 跟踪每个云服务的使用量，以及被哪个用户使用。通过跟踪保证适宜的云服务使用量；
- 监控云服务与客户现有 ICT 系统的集成，以确保业务目标的满足；
- 定义服务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、提供者帮助平台的响应性)；
- 监控、分析和归档指标数据；
- 比较实际交付服务的服务质量和达成协定的服务质量。

8.2.2.4 安全策略管理

安全策略管理活动包括：

- 确保存放在云计算环境中的云服务客户数据的安全性；
- 制定确保数据备份和恢复，以及可能的数据复制和故障转移的计划；
- 定义适用于静态和动态云服务客户数据的加密和完整性技术；
- 定义对云服务客户数据中的所有个人识别信息(PII)的处理。

8.2.2.5 提供计费和使用量报告

提供计费和使用量报告活动包括准备客户组织的云服务使用量报告，以及与使用量相关的账单/发票数据的报告。这些报告提供给业务经理。

8.2.2.6 问题处理

问题处理活动包括客户端对于云服务使用量相关问题的处理，具体包括：

- 评估每个问题的影响；
- 通过故障排除，找到问题的原因；
- 向云服务提供者公开问题，并跟踪至问题解决；
- 寻找问题解决办法；
- 将在约定时间内无法修复或对业务具有严重影响的问题进行升级。

8.2.2.7 管理租户

管理租户活动管理和云服务提供者之间的租赁关系。该活动包括：

- 对安全性的配置和控制，包括用户账、安全角色、身份识别和权限；
- 对同一租户内不同用户间共享数据的识别和控制。

8.2.2.8 执行业务管理

执行业务管理活动包括对使用云服务的业务方面进行管理，包括会计和财务管理，具体包括：

- 调整业务计划以适应云服务的使用；
- 跟踪服务的使用，处理会计和财务管理；
- 处理因使用云服务而收到的来自云服务提供者的账单/发票；
- 确保账单和云服务客户的实际云服务使用量相匹配；
- 向云服务提供者进行支付；
- 记录与使用云服务相关的账务。

8.2.2.9 选择和购买服务

选择和购买服务活动包括：

- 检查(一个或多个)云服务提供者的云服务供应，以决定供应的服务是否满足云计算客户的业务和技术需求。这个活动通常包括读取每项服务的产品目录和文档。这些文档中可能包含服务的技术信息、SLA、以及包含定价内容的业务信息；
- 协商云服务条款(如果云服务提供者允许可变更的服务条款)；
- 客户接受云服务合同，并在云服务提供者处注册。

8.2.2.10 获取审计报告

获取审计报告活动指的是云服务客户通常遵循特定的审计标准或方案，获取云服务的审计报告。

云服务客户既可向云审计者获取报告，也可向云服务提供者获取报告，但是一般情况下，审计报告由独立于云服务提供者的实体提供。审计报告既在服务购买完成前提供，又在服务使用中定期提供。

8.2.2.11 连接 ICT 系统和云服务

连接 ICT 系统和云服务活动包括集成现有的 ICT 系统和云服务，既包括集成现有的 ICT 组件和应用到目标云服务，又包括集成客户和云服务提供者的监控和管理系统。

集成现有的 ICT 组件和应用到目标云服务包括：

- 评估云服务对现有的流程、系统和服务的影响；
- 云服务客户的现有 ICT 系统与云服务之间的业务数据映射；
- 在现有 ICT 组件和应用中调用云服务，包括提供云服务输入数据，处理云服务输出数据；
- 为云服务用户提供访问权限；
- 定义和实现安全相关的需求，包括数据流的保密性和完整性；
- 集成管理用户账号、安全角色，身份和许可权的客户设施和管理云服务的对等设施；
- 创造和监控使用云服务管理接口的特定用户账号和身份；
- 集成云服务与云服务客户的监控和管理基础设施之间的登录和安全事件管理。

8.3 云服务提供者

8.3.1 角色

云服务提供者为云服务客户提供云服务。该角色(及其所有子角色)包括提供云服务、确保云服务交付，以及维护云服务所必需的云计算活动。

云服务提供者负责处理和云服务客户之间的业务关系。

8.3.1.1～8.3.1.8 描述了云服务提供者包含的子角色活动。

8.3.1.1 CSP：云服务运营管理者

CSP：云服务运营管理者是云服务提供者的子角色，负责执行云服务提供者的所有运营过程和流程，确保所有的服务和相关的基础设施满足运营目标。

CSP：云服务运营管理者的云计算活动包括：

- 准备系统(见 8.3.2.1)；
- 监控和管理服务(见 8.3.2.2)；
- 管理资产和库存(见 8.3.2.3)；
- 提供审计数据(见 8.3.2.4)。

8.3.1.2 CSP：云服务部署管理者

CSP：云服务部署管理者是云服务提供者的子角色，负责规划服务部署。该活动包括定义服务运营环境、定义服务部署的初始步骤、定义服务运行过程的依赖资源和可用的运营流程。

CSP：云服务部署管理者的云计算活动包括：

- 定义环境和流程(见 8.3.2.5)；
- 定义度量指标的收集(见 8.3.2.6)；
- 定义部署步骤(见 8.3.2.7)。

8.3.1.3 CSP：云服务管理者

CSP：云服务管理者是云服务提供者的子角色，负责确保云服务客户使用云服务提供者的云服务

时，服务功能正确并且和服务水平协议描述的目标一致。云服务管理者还负责确保云服务提供者的业务支撑系统和运营支撑系统运营稳定，以及向云服务客户和云服务合作者提供的管理和其他云计算活动运营稳定。

CSP：云服务管理者的云计算活动包括：

- 提供服务（见 8.3.2.8）；
- 部署和配置服务（见 8.3.2.9）；
- 执行服务水平管理（见 8.3.2.10）。

8.3.1.4 CSP：云服务业务管理者

CSP：云服务业务管理者是云服务提供者的子角色，整体负责向云服务客户提供云服务的业务方面。CSP：云服务业务管理者创建和跟踪业务计划，定义服务供应策略，管理和服务客户之间的业务关系。

CSP：云服务业务管理者的云计算活动包括：

- 管理提供云服务的业务计划（见 8.3.2.11）；
- 管理客户关系（见 8.3.2.12）；
- 管理财务流程（见 8.3.2.13）。

8.3.1.5 CSP：客户支持和服务代表

CSP：客户支持和服务代表是云服务提供者的子角色，是云服务客户和云服务提供者之间的主要接口，负责及时、高成本效益地对客户的问题和咨询做出响应，以维护云服务提供者及其提供云服务的客户满意度。

CSP：客户支持和服务代表的云计算活动包括：

- 监控客户请求（见 8.3.2.14）。

8.3.1.6 CSP：跨云提供者

CSP：跨云提供者是云服务提供者的子角色。该子角色依靠一个或者多个云服务提供者向云服务客户提供部分或者全部云服务。跨云提供者的主要活动是互连、联合、强化、聚合和仲裁其他云服务提供者的云服务。从云服务客户的角度看，跨云提供者以一种不透明的方式提供管理能力，这使得云服务客户只使用跨云服务提供者的服务和管理接口。

CSP：跨云提供者的云计算活动包括：

- 管理同级的云服务（见 8.3.2.15）；
- 执行云服务的调解、聚集、仲裁、互连或者联合（见 8.3.2.16）。

8.3.1.7 CSP：云服务安全和风险管理者

CSP：云服务安全和风险管理者是云服务提供者的子角色，负责确保云服务提供者能恰当地管理与云服务的开发、交付、使用和支撑相关的风险，确保云服务客户的信息安全策略和云服务提供者的信息安全策略相一致，并能满足 SLA 中的安全需求。

CSP：云服务安全和风险管理者的云计算活动包括：

- 管理安全和风险（见 8.3.2.17）；
- 设计和实现服务的连续性（见 8.3.2.18）；
- 确保依从性（见 8.3.2.19）。

8.3.1.8 CSP：网络提供者

CSP：网络提供者是云服务提供者的子角色，主要为云服务客户、云服务合作者和云服务提供者提

供网络连接和网络服务。CSP:网络提供者可以在数据中心内部和/或数据中心外部运营。

CSP:网络提供者的云计算活动包括:

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

CSP:网络提供者可将对网络连接的动态控制作为 NaaS 提供。

8.3.2 云服务活动

与云计算服务提供者包含的子角色相关的云计算活动如图 10 所示。

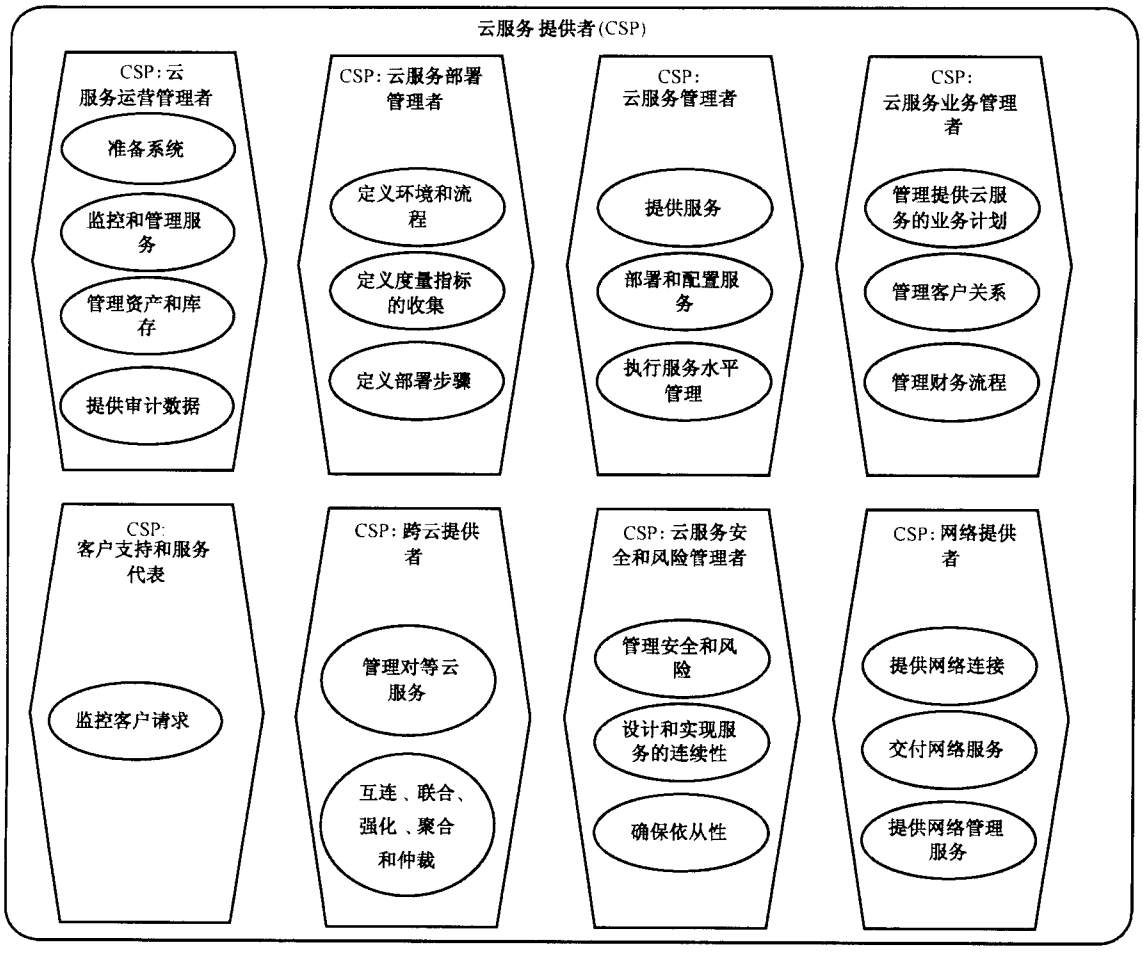

图 10 与云服务提供者的子角色相关的云计算活动

8.3.2.1 准备系统

准备系统活动主要是为部署新的服务,在云服务提供者环境中所做的系统准备工作。该活动包括:

- 评估新服务的部署或已有服务的增长所带来的影响;
- 修改数据中心的资源配置,或扩展数据中心的资源规模,以满足新的部署需求。

8.3.2.2 监控和管理服务

监控和管理服务活动关注于监控和管理服务及相关的基础设施,包含用户权限和系统权限。该活动包括:

- 监控云服务提供者的服务和基础设施；
- 获取对提供者业务重要的事件和数据，并将数据以有价值的形式提供给云服务业务管理者。此类信息包括云服务客户的云服务使用量和云服务的供应成本等；
- 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）、防火墙以及内容过滤器等；
- 分配和管理存储资源；
- 管理用户和系统权限；
- 配置和维护操作系统和资源管理程序；
- 管理虚拟化环境；
- 监控云服务提供者的 ICT 环境，以确保该环境正常运行，且所提供的服务符合 SLA 中的条款；
- 记录和适时地报告问题（可能涉及向一个或多个客户发送问题消息），并跟踪问题处理流程，直到问题解决。

8.3.2.3 管理资产和库存

管理资产和库存活动包括：

- 跟踪计算、存储、网络和软件资产的多个方面，例如版本和补丁信息，相关的配置信息等；
- 新资产的上线和旧资产的回收。这一过程可包括确保新上线的资产符合使用目的，且对安全性和可管理性已进行适当的检查，也包括对不再需要资产的处理。这一过程可包含对保存数据的所有资产进行适当的安全处理。

8.3.2.4 提供审计数据

提供审计数据活动指的是对于审计请求相关的数据的收集和提供，例如系统的安全控制日志，服务的性能监控数据等。审计数据的内容取决于所使用的审计方案或标准。该活动包括：

- 根据日志等数据生成和发送合适的审计信息；
- 基于日志记录，或可能包含敏感信息或个人识别信息（PII）的数据编写信息。

8.3.2.5 定义环境和流程

定义环境和流程活动关注于定义服务运行所需的技术环境和操作流程。该活动包括：

- 定义服务运行所需的技术环境，包括计算、存储和网络资源，以及服务所依赖的软件和相应的配置；
- 定义资源可伸缩性使用的策略和流程，以实现资源的按需供应；
- 确保云服务符合与安全性和业务合规性相关的标准；
- 定义服务运行所遵循的流程，包括问题修复、升级和迁移流程等。

8.3.2.6 定义度量指标的收集

定义度量指标的收集活动关注于定义服务水平指标和管理。该活动包括：

- 定义与云服务运营相关的指标，这些指标通常体现在与服务相关的 SLA 条款中；
- 设计每个云服务的指标如何收集；
- 定义如何报告和管理服务指标，以确保满足 SLA 的目标。

8.3.2.7 定义部署步骤

定义部署步骤关注于定义服务部署的步骤。该活动描述运营和支撑团队为实现服务部署并保证服务对云服务客户可用所需采取的所有步骤。

8.3.2.8 提供服务

提供服务活动包括将云服务交付给云服务客户所需的所有步骤。该活动包括接受和处理经过授权和认证用户的服务调用请求。对服务调用的处理应由某个服务实例完成。该服务实例的设计和配置决定其是否会涉及到其他服务的组合以及对其他服务的调用。该活动还包括以下内容：

- 管理服务的异常处理过程；
- 管理业务支撑系统和运营支撑系统；
- 维护服务和底层的基础设施；
- 自动化系统流程；
- 管理长期的容量趋势和性能走势；
- 安装、配置和维护云服务提供者的数据中心所需的硬件，包括计算、存储和网络通信能力；
- 对运营云提供者数据中心和支持云服务实现所需的软件进行安装和配置。根据需要对软件进打补丁、更新和升级。

8.3.2.9 部署和配置服务

部署和配置服务活动包括将已实现的服务投入运行使得服务使用者可通过网络终端访问服务，以及能够处理来自用户的服务请求。该活动包括：

- 遵循为服务定义的部署流程。

注：该活动还包含实现服务的去部署和去配置的云计算活动。

8.3.2.10 执行服务水平管理

执行服务水平管理活动主要管理服务与 SLA 条款之间的依从性。该活动包括：

- 监控每个服务的指标，并与该服务 SLA 中定义的服务水平进行对比；
- 当服务指标不符合 SLA 中定义的水平时，采取相应的措施使其与 SLA 保持一致，例如，执行由云服务部署管理者定义的处理流程；
- 当服务无法达到与 SLA 一致的水平时，报告问题。

8.3.2.11 管理提供云服务的业务计划

管理提供云服务的业务计划活动包括：

- 定义服务交付，描述服务交付的技术方面（如功能接口、SLA 等）和业务方面；

注：当建立服务交付时，云服务提供者可能需要考虑与对等的服务提供者之间的交互。

- 创建业务规划，包括以下方面：为客户交付一个或多个云服务、处理服务的财务和技术方面内容、目标客户群、合约和 SLA、市场渠道和销售目标等；
- 根据业务规划，跟踪销售和服务使用情况，以确保云服务提供者财务目标的实现；
- 为提供云服务准备和调整业务规划。

8.3.2.12 管理客户关系

管理客户关系活动包括对云服务提供者和云服务客户之间业务关系的管理，具体包括：

- 创建和维护产品目录的内容；
- 获取客户；
- 为客户提供各项业务事宜的联系方式；
- 讨论并解决客户的顾虑或问题；
- 处理客户的需求变更请求（例如，客户权利的变更）。

8.3.2.13 管理财务流程

管理财务流程活动包括：

- 处理账单更新或客户对账单的疑问；
- 云服务提供者生成与云服务使用相关的账单信息和/或发票，并将其发送给云服务客户；
- 收取云服务客户支付的费用，与云服务客户进行费用核算。

8.3.2.14 监控客户请求

监控客户请求活动包括：

- 处理云服务客户发来的服务请求和报告。云服务提供者可向客户提供多种与服务支持人员交流的方式，如论坛、电子邮件、客户支持桌面系统、Web 门户、即时通信等；
- 一些请求或报告可能只要求提供信息，或详细说明，其他的请求和报告可能要求对问题的分析，或者是需求变更申请。

8.3.2.15 管理对等云服务

管理对等云服务活动关注于对一个对等云服务提供者的云服务使用的管理。该活动包括：

- 选取和使用一个对等云服务提供者的一个或多个服务；
- 监控和管理对等云服务提供者的云服务，确保这些服务符合 SLA 中定义的服务水平，包括服务相关问题的报告和解决；
- 管理对等云服务提供者的云服务的业务方面，包括业务规划和财务处理等；
- 跟踪对等云服务提供者的每一个云服务的使用情况，包括服务的使用量、使用服务的用户，并确保服务使用合理，并在业务规划范围内；
- 监控对等云服务提供者的云服务和已有的服务实现的集成，以确保业务目标的实现；
- 在云服务客户和所有对等的云服务提供者之间协调身份和安全证书。

8.3.2.16 互连、联合、强化、聚合和仲裁

互连、联合、强化、聚合和仲裁活动是指按如下特定的方式使用对等云服务提供者的云服务。

- 互连是指使用一个对等云服务提供者的云服务；
- 联合是指使用一组对等云服务提供者的云服务，组合这组云服务提供者的服务能力，来提供客户需要的一组云服务；
- 强化是指云服务提供者通过调整或增强对等云服务提供者的云服务来提供自己的云服务。增强云服务的例子包括管理对云服务的访问，提供云服务应用编程接口(API)、身份管理、性能报告、增强的安全性等；
- 聚合是指云服务提供者通过组合对等云服务提供者提供的一组云服务提供一个云服务；
- 仲裁是指云服务提供者从对等云服务提供者提供的一组云服务中进行选择从而提供云服务。

8.3.2.17 管理安全和风险

管理安全和风险活动主要关注与云服务的开发、交付、使用和支持相关的安全和风险管理。该活动包含：

a) 定义信息安全策略，需要考虑服务需求、法令法规需求、合同和 SLA 要求；

b) 定义与云服务相关的信息安全风险，以及为满足云服务提供者的业务目标而对这些风险所采取的解决办法。这里的一个重点是管理信息安全风险有相应的成本，提供者可从业务的角度考虑自己不处理一些风险，相反通过服务协议的方式，交给云服务客户处理，以满足部分市场

的成本需求；

c) 为解决与所选的服务和设计点相关的风险，选取设计点和相关的信息安全控制。信息安全控制通常包括以下类别，如：
   1) 身份和访问管理；
   2) 发现、分类、保护数据和信息资产；
   3) 信息系统的获取、开发和维护；
   4) 对威胁和漏洞安全的基础设施；
   5) 问题和信息安全事件管理；
   6) 安全治理和合规性；
   7) 物理安全和人员安全；
   8) 网络安全和通信安全；
   9) 隔离性(多租户情况下多个租户之间)。
d) 确保为部署的服务和底层的基础设施落实可识别的信息安全控制；
e) 设计、实现和评价系统和应用的安全性；
f) 管理、设计、实现和评价对等云服务提供者的云服务安全性；
g) 评价已实现的信息安全控制的有效性，并基于经验做相应的调整；
h) 确保运营支撑系统和业务支撑系统基于特定的云服务客户租户提供对云服务提供者内容的数据访问。

8.3.2.18 设计和实现服务的连续性

设计和实现服务的连续性活动包括：

- 考虑到云服务和支撑基础设施的潜在故障模式，通过诸如故障转移和冗余等技术，落实恢复流程使得云服务在 SLA 条款内的可用。

8.3.2.19 确保依从性

确保依从性活动主要实现对法规合规性和标准合规性的支持。该活动包括：

- 确保云服务和支撑基础设施的实现满足所有需要支持的标准的需求。例如，目标客户群要求的标准，或者提供者用来保证服务所选择的认证体系所要求的标准；
- 确保云服务和支撑基础设施的实现(包括数据处理)满足对服务或服务所存储或处理数据的所有法规需求。

8.3.2.20 提供网络连接

提供网络连接活动包括在云服务客户系统和云服务提供者系统之间，或两个云服务提供者系统之间建立所需要的网络连接和网络能力。该活动包括建立 VPN、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 NaaS 下的云和非云场景提供适宜有限的延迟、抖动、带宽、服务质量以及可靠性的能力。

8.3.2.21 交付网络服务

交付网络服务活动提供网络相关的服务，例如防火墙或者负载均衡等。

8.3.2.22 提供网络管理服务

提供网络管理服务活动主要管理承载云服务所需的网络基础设施。该活动提供对云网络基础设施进行运营、管理、维护和供应所需的方法、工具和流程。该活动包含的任务用于以下目的：

- 保持网络正常并运行流畅；
- 跟踪网络资源及其分配状况；
- 进行维修和升级，例如当需要置换设备或升级设备增加新功能的时候；
- 配置网络中的资源以支持云服务。

8.4 云服务合作者

8.4.1 角色

云服务合作者是为云服务提供者和/或云服务客户的活动提供支撑或辅助功能的参与方。

云服务合作者的云计算活动随着合作者的类型及其与云服务提供者和云服务客户之间关系的不同而变化。

8.4.1.1 云服务开发者

云服务开发者是云服务合作者的子角色，负责云服务实现的设计、开发、测试和维护。这可能涉及根据现有服务的实现来组合(新的)服务实现。

云服务开发者的云计算活动包括：

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

注 1：云服务集成者和云服务组件开发者是云服务开发者的子角色。其中，云服务集成者处理服务的组合，云服务组件开发者处理单个服务组件的设计、创建、测试和维护。

注 2：该活动包括服务实现和服务组件。服务组件涉及与对等云服务提供者的交互。

8.4.1.2 云审计者

云审计者是云服务合作者的子角色，负责审计云服务的供应和使用。云审计通常覆盖运营、性能和安全。云审计检查一组特定的审计准则是否得到满足。

注：针对审计准则的规范有很多，例如，ISO/IEC 27002 涉及安全规范。

云审计者的云计算活动包括：

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

8.4.1.3 云服务代理者

云服务代理者是云服务合作者的子角色，负责在云服务客户和其他云服务提供者之间进行协商。云服务代理者不提供与云服务提供者环境中的云服务客户数据进行交互的跨云能力。云服务代理者可与跨云服务相结合，也可独立运营。

云服务代理者的云计算活动包括：

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

市场评估也可发生在以下活动之前：客户获取，客户与云服务提供者签订预协议，客户根据服务目录选择云服务提供者，(可能的)在选择阶段进行的服务细节(例如服务水平目标)协商。

无论市场评估在之前或之后发生，云服务代理者只在云服务客户和云服务提供者之间的合约签订阶段发挥作用。云服务代理者不参与服务消费过程。服务消费过程的活动涉及云服务提供者的活动。

8.4.2 云计算活动

与云服务合作者的子角色相关的云计算活动见图 11。

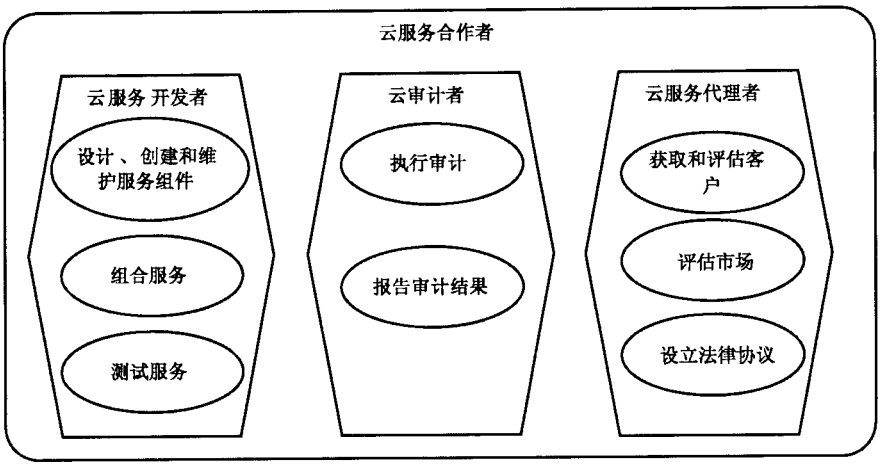

图 11 与云服务合作者的子角色相关的云计算活动

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如下内容：

- 设计和创建用于服务实现的软件组件；
- 创建新的功能并提供给服务用户使用。该功能也包括将服务组件连接至云服务提供者的运营支撑系统，以便监控和控制服务实现；
- 处理与服务实现的运营相关的问题报告；
- 提供对服务实现的修正能力；
- 提供对服务实现的扩展能力。

8.4.2.2 组合服务

组合服务活动主要关注通过已有服务组合新的服务。该活动包括：

- 通过组合已有的一个或多个服务来创建新的服务功能；
- 描述服务的技术方面(例如功能接口，SLA)；
- 为云服务客户设计一个简单统一的接口来访问多个云服务提供者提供的服务；
- 组合可包括对已有服务的强化、聚合或仲裁。

8.4.2.3 测试服务

测试活动主要关注于测试云服务开发者创建的组件和服务。该活动包括：

- 对构成服务实现的组件进行测试，以确保这些组件完整并正确地实现了服务功能；
- 确保与对等云服务提供者提供的服务/功能接口的互操作性；
- 应检查与云服务提供者的运营支撑系统的连接是否运行正常。因此，通常有必要在云服务提供者数据中心的测试区执行部分测试。

8.4.2.4 执行审计

执行审计活动包括：

- 请求或获取审计证据；
- 可在待审计系统上进行任何需要的测试；
- 通过待审计系统提供的一组接口，通过程序调用的方式获取审计证据；
- 在必要时可修改审计证据，以保护敏感信息或受法规控制的信息（例如：PII）；
- 对比所用的审计方案或审计标准中描述的审计准则和获得的审计证据。

所需的审计证据类型和评估准则取决于正在使用的审计方案或审计标准。审计证据包括指定服务的安全控制相关的数据和性能数据。除了获取数据，该活动还可用来评估云服务提供者提供的各类服务，包括安全控制、隐私影响、性能，以及其他由审计请求者标识的与云服务相关的云计算活动。审计请求可来自云服务提供者自身。此时，云服务提供者需要得到其提供的云服务质量的证明，以便递交给潜在的云服务客户。

8.4.2.5 报告审计结果

报告审计结果活动提供对指定服务或指定云服务提供者审计结果的文档报告。文档报告的形成取决于正在使用的审计方案。审计结果可根据业务场景或法律法规，提交给云服务提供者或云服务客户。

8.4.2.6 获取和评估客户

获取和评估客户活动包括为销售云服务所需的各种任务，此时云服务客户签订协议同意使用一个或多个服务。该云计算活动包括：

- 为潜在客户提供关于可用的服务、相关的 SLA 以及合同条款的相关信息；
- 与客户协商服务条款和价格；
- 评估客户对云服务的需求。

注：云服务客户的需求评估活动包括为确定和解决云服务客户的需求所采取的措施。其中，云服务客户的需求在对客户现有能力和预期能力进行差距分析的基础上标识。

8.4.2.7 评估市场

评估市场活动主要关注于评估当前的云服务市场和生态系统，从而为客户寻找符合其需求的云服务。该活动包括：

- 对云服务提供者所供应的产品进行调研，获取技术信息和商业信息。
- 订阅和接受云服务提供者产品目录内容变更的通知。
- 对产品供应和云服务客户需求进行匹配，匹配内容包括技术、商业和法规等方面。

8.4.2.8 设立法律协议

设立法律协议活动主要关注于云服务客户与所选定的云服务提供者之间的服务协议。该活动包括云服务客户和所选的云服务提供者之间为满足客户需求，对服务协议进行的协商。

8.5 共同关注点

8.5.1 概述

共同关注点包含架构层面和运营层面的考虑。共同关注点适用于 CCRA 描述范围内或与 CCRA 实例系统运营相关的多个元素。这些共同关注点在多个角色、活动和组件中共享。

例如，安全性是一个共同关注点，因为它适用于基础设施、服务、云服务提供者、云服务客户和云服务合作者（包括云审计者、云服务开发者等）。虽然所有这些元素都需要安全防护，但如何进行安全防护会因安全防护对象的不同而不同。因此，确保基础设施以及基础设施服务的安全和确保软件服务的安全区别很大。

某些共同关注点能应用于其他共同关注点。例如，治理既应用于功能元素，也应用于其他共同关注点，包括性能与安全性。

共同关注点常常影响到角色所执行的云计算活动。为了支持一个共同关注点，需要在不同角色和同一角色的不同活动之间进行协调。支持共同关注点还需要支持云计算活动、技术能力和实现的组件。针对每个共同关注点，需要定义一组云计算活动和组件。不同的角色和解决方案可能使用这些共同关注点的不同子集。

共同关注点包括：

- 可审计性(见 8.5.2)；
- 可用性(见 8.5.3)；
- 治理(见 8.5.4)；
- 互操作性(见 8.5.5)；
- 维护和版本控制(见 8.5.6)；
- 性能(见 8.5.7)；
- 可移植性(见 8.5.8)；
- PII 保护(见 8.5.9)；
- 健壮性(见 8.5.10)；
- 可复原性(见 8.5.11)；
- 安全(见 8.5.12)；
- 服务水平和服务水平协议(见 8.5.13)。

8.5.2 可审计性

云服务治理要求确保云服务的供应和使用符合云服务客户、云服务提供者和云服务合作者之间的服务协议。这通常通过独立的服务审计实现。审计通常包括审计报告或审计证明。这些审计报告或审计证明提供给服务协议的相关参与方，包括：云服务客户、云服务提供者和云服务合作者。

审计本身依赖于与服务及相关资源的用法、环境、可用性和性能相关的数据和证据的可用性。这些数据和证据包括协议所有参与方的活动和运营环境条件的记录和日志。这些记录和日志需要以安全的方式收集和维护。

8.5.3 可用性

可用性是一个云服务在一段约定的时间内执行其功能的能力。从客户角度看，可用性通常是服务的一个关键属性。

可用性也是授权实体按需进行访问和使用的属性(ITU-T X.800|ISO/IEC 27000:2012)。

8.5.4 治理

内部云治理指的是：通过设计时和运行时策略的运用，确保按照特定的预期，设计和实现基于云计算的解决方案，交付基于云计算的服务。这些预期可能涵盖部分或全部的共同关注点。

由云服务客户和云服务提供者所使用的独立的治理实践存在一个从简单到复杂的连续桶。这些治理实践封装在角色中。每个角色的责任是根据各自的需求来实施治理。为了满足透明性需求，以及理顺以下关系的需求：云治理的云计算活动和 SLA，云治理的云计算活动和云服务客户与云服务提供者之间的其他合同要素，把云治理作为共同关注点之一。

外部云治理关注云服务客户对云服务的使用，适用于云服务客户和云服务提供者之间的某些形式的协议。该协议可参照一个服务水平协议。该服务水平协议提供关于服务的功能性和非功能性方面的详细信息。

服务水平协议应规定与服务的可用性、服务的保密性和完整性、服务的访问控制相关的信息。服务水平协议应规定如何处理与云服务相关的任何个人身份信息。

8.5.5 互操作性

云计算语境下的互操作性包括云服务客户与云服务之间按照规定的方法交互和交换信息并获得可预测结果的能力。通常情况下，互操作性意味着云服务按照一个商定的规范运营，此规范尽可能是标准化的。当与云服务交互时，云服务客户在内部应能采用广泛可用的信息和通信技术(ICT)设施，避免使用专有的或高度专业化软件的需要。

互操作性还包括一个云服务与其他云服务一起工作的能力，既可以通过一个云服务提供者(CSP)的云间提供商关系，也可以由云服务客户自己以某种形式组合多个不同的云服务来实现其业务目标。

延伸到云服务本身之外，互操作性还包括云服务客户与云服务提供者的云服务管理设施的交互。理想情况下，云服务客户应有一个一致的、可与云服务管理功能进行互操作的接口，且不需按每个云服务提供者专有方式就能与两个或两个以上云服务提供者进行交互。

标准的实现应以支持组件之间的互操作性，或支持数据或程序组件的移植性为目标。标准的实现应支持已用标准从一个标准早期版本到后续版本，或从一个标准到另一个不同标准的两种方式的演变，同时最大限度地减少颠覆性变化。

8.5.6 维护和版本控制

服务及相关资源的维护是与治理相关的一个重要条目。维护的发生有多种可能原因，包括需要排除故障，也包括因业务原因需要升级或扩展设施。维护云计算活动可能会改变云服务行为的效果——特别是当一个客户使用服务时进行变更可能会影响一个服务的运作。

区分由云服务提供者和云服务客户执行的维护非常重要。在一个 SaaS 服务的用例中，很可能由提供者执行几乎所有的维护云计算活动。在 IaaS 和 PaaS 服务的用例中，应用程序组件属于客户-提供者负责应用程序组件运行的环境，环境会根据服务细节而不同，但其中可能包括如硬件资源、操作系统或中间件的内容。

一方面，可以根据客户的利益来升级或修复服务或服务平台。另一方面，一个服务行为的任何变化可能对客户产生不利的影响，可能需要改变应用程序组件，改变客户信息和通信技术系统，或需要重新培训(负责)客户服务的用户。其结果是，服务的维护须遵守对客户透明的治理实践非常重要。

维护实践应记录在云服务的 SLA 中，并宜包括为客户提供报告问题和请求修复的能力，也应包括一种云服务提供者将等待维护变更的内容和其进度通知客户的机制。

版本控制是给一个服务(或一个服务的组件，如用于 IaaS 服务的操作系统级别)标上适当的标签，以便使客户清楚地了解正在使用(服务)的特定版本。当发生云服务维护时给该服务赋予新的版本标签非常重要。

一个服务在两个版本之间的发生重大变化时，旧版本和新版本服务应是在一段约定期限内并行可用。

8.5.7 性能

性能包括与云服务操作相关的非功能层面的一个集合：

- 服务的可用性；
- 完成服务请求的响应时间；
- 执行服务请求的交易速率；

- 延迟服务请求；
- 数据吞吐量速率(输入和输出)；
- 并发服务请求数量(可扩展性)；
- 数据存储容量；
- (对于 IaaS 与 PaaS)一个应用可用的并发执行线程数量；
- (对于 IaaS 与 PaaS)正在运行程序可用的内存(RAM)数量；
- 数据中心网络的 IP 地址池和/或 VLAN 范围容量。

当服务涉及应用(IaaS 或 PaaS)的运行时，上述同样的性能项也适用于云服务提供者环境下服务的行为。

基于不同收费模式，云服务按照服务水平协议(SLA)条款来伸缩使用资源的能力也可成为性能的一个重要层面。性能应使每一个被标识的性能条件在 SLA 中有度量指标定义，并且应在云服务的操作过程中监测这些指标，以确保服务满足 SLA 性能条款。

8.5.8 可移植性

由于潜在云服务客户选择使用云服务时，会关注避免(厂商)锁定，因此移植性在云计算中非常重要。云服务客户须了解，他们能在多个云服务提供者之间，以低成本和最小中断时间来移动云服务客户数据或他们的应用。

可接受的成本和中断时间的数量可能会根据正在使用的云服务类型不同而不同。

例如，如果一个云服务客户组织正在考虑从一个 IaaS 云服务提供者移至另一个，云服务客户宜能用相对直接的方式，获取它的数据和虚拟机(VM)镜像并在另一个同样的 IaaS 服务上安装和运行。在 SaaS 环境中，当一个云服务客户组织希望将一个 SaaS 应用移至不同的云服务提供者(例如，替换 SaaS 服务提供商)，云服务客户需要能获取他们自己的数据，但其余的替换成本仍将包括导出、映射和将数据导入新的云服务提供者的 SaaS 应用，这些成本是两个 SaaS 云服务提供者的数据模型和格式对应排列程度的一个函数。在理想的情况下，SaaS 云服务提供者宜采用应用程序相关领域标准的数据交换格式。SaaS 应用之间切换，也允许涉及云服务客户自己去适应新的(与服务互操作性相关的)服务接口。

然而，由于不同的云能力类型可以有不同的可移植性相关的需求，因此，专注于特定类型的可移植性，如云数据可移植性和应用可移植性，将更加有用。

云服务客户数据是一类云服务客户控制下的数据对象。云数据可移植性允许云服务客户通过网络访问或存储设备的物理传输方式从/向云服务中复制云服务客户数据的能力。

应用可移植性允许将某些项目，如完全停止的虚拟机实例或机器镜像(IaaS 服务)，从一个云服务提供者到另一个云服务提供者的迁移，或者将应用组件(PaaS 服务)从一个云服务提供者迁移到另一个。在这两种情况下，有一个和应用部件相关的元数据可移植性支持的相关方面，来提供关于程序组件间关系和有关程序组件所需的基础设施(如负载均衡配置，防火墙设置)的信息。

8.5.9 PII 保护

云服务提供者宜保护与云服务相关的个人可标识信息(PII)的收集、处理、传播、使用和处置的确信、合适和一致。

根据既定指南，一个组织的关键业务必要需求之一是确保个人可识别信息(PII)的隐私。虽然云计算提供了一个灵活地共享资源、软件与信息的解决方案，但它也给云服务客户使用云服务和云服务提供者带来了额外的隐私挑战。

在许多司法管辖领域，有适用于处理 PII 的严格规则和法规——任何使用云服务来存储和处理的

PII 可遵守这些规则和法规。

法令、监管和法律需求会因市场区域和司法管辖范围不同而变化，他们能改变云服务客户和云服务提供服者的责任。符合这类需求往往和治理、风险管理活动相关。

8.5.10 健壮性

健壮性是一个系统在面对影响正常运转的故障(无意的、故意的或自然造成的)时提供和维持一种可接受的服务水平的能力。

健壮性描述了监测、预防和响应等过程的集合，这些过程能使云服务通过故障和恢复行动，提供连续运转或可预见并可验证的中断。这些故障可包括硬件、通信和/或软件的故障，可以孤立或组合事件的形式发生，包括序列故障。这些过程可包括自动和手动行动，通常跨越多个系统，因此他们的描述和实现是整体云基础设施的一部分而不是一个独立的功能。

实现风险管理是弹性的固有内容——因为弹性是由系统中最小弹性的组件，以及成本/性能或对弹性成为可能或实际的限制范围等其他因素决定的。风险和价值的结合在选择提供弹性的实施中实现。

8.5.11 可复原性

可复原性是指云服务客户有权取回云服务客户数据和应用内容，云服务提供者有义务删除所有云服务客户数据，并且在约定的时间之后，删除由合同确认的云服务衍生数据。本原则的实质是“被忘记的权力”，保证云服务客户一旦向云服务提供者声明所使用的服务即将到期之后，将启动一个顺序执行的流程，云服务客户取回云服务客户数据和应用内容，云服务提供者将删除所有拷贝，并在约定的时间之后不再保存任何属于云服务客户的资料。

与可复原性相关的活动大多数情况下包含一系列的步骤，典型的是要求云服务客户取回数据并通知云服务提供商删除云服务客户数据的拷贝——同时需要保持备份拷贝一段时间，以防止在退出流程中出错。这些步骤也必须应用于所有云服务提供者使用的其他同类服务中，用以支持云服务提供者的服务。

8.5.12 安全

8.5.12.1 一般要求

理解安全是跨越参考模型中所有视图的跨领域要素是重要的，从物理安全到应用安全。因此，云计算架构中的安全不仅是一个在云服务提供商控制之下的跨领域要素，同时也会影响云服务客户、云服务合作伙伴以及他们的子角色。

云计算系统的安全需求可能包括认证、授权、可获得、保密、不可抵赖、身份管理、完整性、审计、安全监控、事故反馈和安全策略管理。本条款描述了云计算通过特定角度分析和实施云计算系统中的安全策略。

云服务的安全功能包括：存取控制、保密、完整性和可获得性。其他规范会详细描述云计算安全。

安全能力也包括控制云服务、底层资源和云服务应用的管理和监督功能，并特别关注控制这些功能用户的存取权限。还包括：

- 支持尽早探测、诊断和修复云服务和资源的相关问题；
- 对于网络上的存取记录、活动报告、进程监控和包检测实施安全日志管理；
- 为云服务提供者系统提供防火墙、恶意攻击检测和防护服务。一个用户不能干扰其他用户使用云服务。

在连接云服务客户和云服务提供者之间的网络连接上提供内部网级别的安全性(例如通过使用

VPN)。

云计算的安全度量描述了云服务客户使用云服务的一系列威胁，这些威胁也会同时影响云服务客户和云服务提供者。其他规范会更加完整地描述这些威胁。

8.5.12.2 分布式安全责任

在一个云计算系统中，云服务提供商和云服务客户对于计算资源有不同的控制能力。与传统信息技术系统中一个组织可以控制计算资源的完整堆栈和信息系统全生命周期不同，云服务提供商和云服务客户共同合作设计、开发、部署和运营云计算系统。

控制的分离意味着两个角色在保护云计算系统方面分担责任。安全是一个分享的责任。需要分析安全控制，即实施保护的方法，来决定哪个角色在实施控制方面具有相对有利的地位。分析需要从服务目录的角度来考虑，不同的云服务目录意味着云服务提供商和云服务客户分担不同的安全控制级别。清晰定义客户和提供商的责任是很重要的，可以保证能够覆盖安全的全部要素，同时避免责任的模糊性。

例如，IaaS 云服务提供商通常执行 IaaS 服务初始化系统特权用户的账户管理控制，同时采用 IaaS 服务来部署应用的云服务客户承担部署到 IaaS 服务的应用账户管理工作。相反，对于 SaaS 应用服务，所有类型用户的账户管理控制都是由云服务提供商完成的(虽然云服务客户可能提供某些能力，例如第三方认证)。

8.5.12.3 云服务类别视角

云服务目录在 ITU-T Y.CCDEF | ISO/IEC 17788 定义为一组具有通用质量集合的云服务。云服务目录向云服务客户展现不同类型的服务管理操作，并向云计算系统开放不同的接入点，这些接入点同时又为攻击方提供了多个攻击入口。因此，需要重点考虑云服务目录所产生的影响以及在安全设计和实施方面出现的不同问题。

例如，SaaS 为用户提供了通过网络连接获取云计算的能力，可能通过互联网和 Web 浏览器。SaaS 云计算系统重视 Web 浏览器的安全性。IaaS 服务的 CSC：云服务用户可以在主机系统监控管理程序上执行虚拟机(VMs)，因此，采用虚拟技术的 IaaS 云服务提供者对于能够提供虚拟机隔离的监控管理程序的安全性进行了广泛的研究。

8.5.12.4 云部署模型的影响

不同的云部署模型对安全性有很大的影响。分析云部署模型安全影响的一个角度是不同部署模型的租户拥有不同层次的独占性。私有云只为一个云服务客户的组织服务，而公有云可能为来自同时存在的不同组织的租户提供服务。

分析云部署模型安全影响的另一个角度是采用访问边界的概念。例如，当私有云系统存在于云服务客户组织网络边界之内，本地的私有云系统不一定需要在云服务边界之上增加边界控制器，然而一个外包的私有云倾向于需要在云服务的边界上建立保护机制。

8.5.12.5 数据保护策略和责任

数据保护是云计算的一个新维度。一个组织可能倾向于在云服务中存储数据，但是数据保护的责任和义务需要清晰地定义。**云服务客户**执行的第一步是恰当地分类数据、确定敏感度、数据泄露、丢失和损坏带来的业务风险。

注：如何识别敏感数据见 ISO/IEC 27002。

理想情况下，**云服务客户**应当有责任保证在迁移到**云计算**系统之前的数据安全。然而，提供商需要审计任何数据的篡改和丢失。可以选择加密技术，但是密钥管理必须考虑云服务客户的位置，也可以由第三方来管理密钥。如果由云服务提供商管理密钥，则他们有责任对于密钥和数据提供逻辑上和物理上的保护。

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，有助于形成可测量的元素，用以保证云服务客户和云服务提供者之间已达成协议的服务质量。

云计算服务水平协议(云 SLA)基于对云计算特有术语的分类，在云服务提供者和云服务客户之间所达成的对所交付的云服务质量进行设置的服务水平协议。云 SLA 描述了所交付的云服务质量的以下方面：

- 一组云计算特有的可测量的属性(业务方面和技术方面)；
- 一组指定的云计算角色(云服务客户和云服务提供者，及其相关子角色)。

例如，云服务客户需要通过云 SLA 去规定云服务提供者履行的技术性能要求。云 SLA 能覆盖以下条款：服务质量、安全性、性能、为满足云 SLA 条款所采取的失败补救措施。云服务提供者还可在云 SLA 内列出一组不针对云服务客户的明确承诺，例如，云服务客户需要接受的限制和义务。云 SLA 应定义数据对象分类(例如，云服务客户数据、云服务提供者数据、云服务衍生数据)，谁可以访问和控制这些数据分类中的数据对象，以及如何使用这些数据对象。

服务协议，有时称之为主服务协议(MSA)、服务条款、条款(T&C)、或简言之合约，是参与方之间协议的上层文档。服务水平协议是服务协议的下层文档。这是服务协议和服务水平协议之间的重要区别，但是 SLA 常常被错误地用来指代整个合约关系。实际上，这个合约关系是 SLA 自身不能承担的。服务协议覆盖了整个合约，因此也包含了与云计算不直接相关的合约因素。

9 功能视图

9.1 功能架构

云计算功能架构用一组高层的功能组件来描述云计算。功能组件代表了为执行第 8 章描述的与云计算相关的各种角色和子角色的云计算活动的功能集合。

功能架构通过分层框架来描述组件。在分层框架中，特定类型的功能被分组到各层中，相邻层次的组件之间通过接口交互。

9.1.1 分层框架

CCRA 的分层框架包括 4 层，以及一个跨越各层的跨层功能集合。这 4 层分别是：

- 用户层；
- 访问层；
- 服务层；
- 资源层。

跨越各层的功能称为跨层功能。

分层框架如图 12 所示。

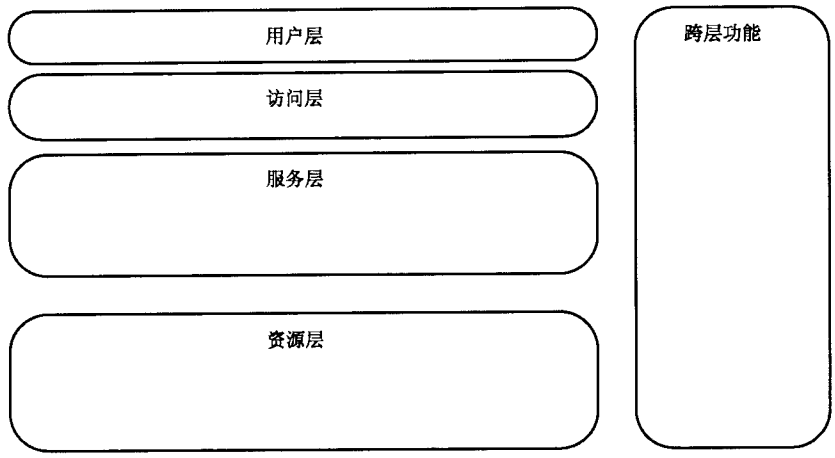

图 12　云计算层次框架

框架中的每一层在后续章节中描述。

9.1.1.1　用户层

用户层是用户接口。通过该接口，云服务客户和云服务提供者及其云服务进行交互，执行与客户相关的管理活动，监控云服务。用户层也可提供云服务的输出到另一个资源层的实例。

9.1.1.2　访问层

访问层提供对服务层能力进行手动和自动访问的通用接口。这些能力既包含服务能力，也包含管理能力和业务能力。

访问层负责将云服务能力通过一种或多种访问机制展现出来，例如，通过浏览器访问一组 web 页面，或在安全通信的基础上，通过编程的方式访问一组 web 服务。访问层的另一个职责是为云服务能力的访问提供合适的安全功能。访问层负责通过用户证书来验证用户请求，验证用户是否被授权使用特定的能力。访问层还负责在需要时进行加密处理，检查请求的完整性。

访问层还负责对来自用户层（例如，提交给向云服务提供者的服务请求）和流向用户层的（例如，云服务的输出）流量实施 QoS 策略。

访问层将经过验证的请求传递给服务层组件。访问层接收云服务客户或云服务提供者的云服务消费请求，并访问云服务提供者的服务和资源。

9.1.1.3　服务层

服务层包含对云服务提供者所提供服务的实现。服务层包含和控制实现服务所需的软件组件（但不包括底层的虚拟机监控器、主机操作系统、设备驱动程序等），并安排通过访问层为用户提供云服务。

服务层的服务实现软件依次依赖于资源层的可用能力来提供服务，并确保满足服务的任何 SLA 需求（例如，通过使用充足的资源）。

9.1.1.4　资源层

资源层驻留各类资源，包括数据中心通常使用的设备，例如服务器、网络交换机和路由器、存储设备等，和服务器上运行的非云特有的软件，以及其他设备，例如主机操作系统、虚拟机监控器、设备驱动程序、通用系统管理软件。

资源层也表示和提供云传输网络功能。通过此功能，在云服务提供者和用户之间，云服务提供者内部，云服务提供者和对等云服务提供者之间提供底层的网络连接。

注：云服务提供者为了提供符合 SLA 的服务，需要在用户和云服务提供者之间建立专用和/或安全的连接。

9.1.1.5 跨层功能

跨层功能包括一系列功能组件。这些功能组件与上述4层的组件进行交互以提供支撑能力。这些支撑能力包括但不限于：

- 运营支撑系统能力(运行时管理、监控、供应和维护)；
- 业务支持系统能力(产品分类、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(连接不同组件以实现所需的功能)；
- 开发支撑能力(包括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

本节从云功能组件通用集的角度描述了云架构。一个功能组件是CCRA的一个功能元素，用来执行一个活动或活动的一部分。该功能组件在具体的参考架构实现中有相应的实现构件，例如，软件组件、子系统或应用。

图13展示了使用分层框架方式组织的对CCRA组件的高层次概述。

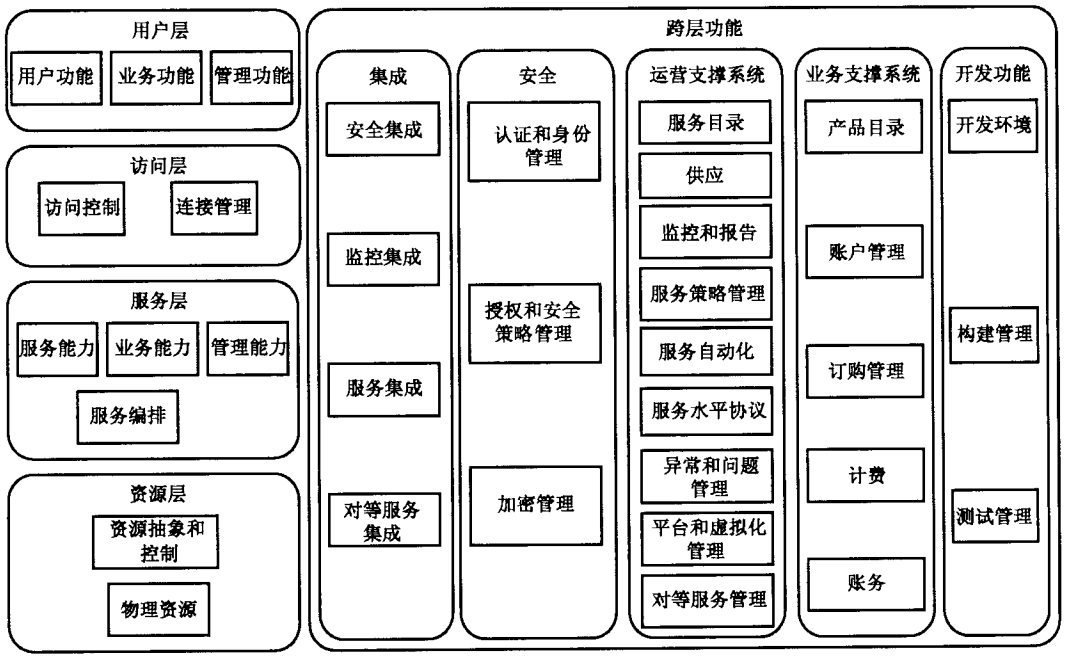

图13 CCRA功能组件

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；
- 管理功能。

提供给CSC：云服务用户的云服务主要可以分为两大类：功能服务和自服务管理服务。后者可进一步分解为业务服务和管理服务。

提供给云服务用户的接口包括了云服务的主要功能。该接口不同于管理云服务使用的接口，但是无论哪类接口都是将不同类型的能力定制的云服务。

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(使用云服务活动)。某些情况下,用户功能组件可以和运行在个人计算机上的浏览器一样简单。然而,在某些情况下,用户功能组件可能包含一个运行着业务处理、应用、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:业务管理者的云计算活动,包括云服务的选择和订购,使用云服务涉及的账务和财务管理。需要注意的是业务功能自身也是通过云服务来提供。云业务能力只能通过使用云服务来获取。

9.2.1.3 管理功能

管理功能**功能组件**支持 CSC:云服务管理者的云计算活动,包括用户身份和配置文件管理、对服务活动和服务使用的监控、事件处理和问题报告。云管理能力只能通过使用云服务来获取。

9.2.2 访问层组件

图 14 展示了访问层组件,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

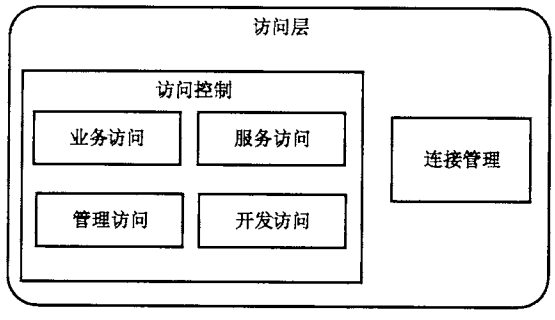

图 14 访问层组件

9.2.2.1 访问控制

访问控制限制用户对特定服务的使用。访问控制主要包括:通过提供和检查证明文件来实现对用户的鉴别,以及对鉴别通过的用户使用特定的服务进行鉴权。身份管理与访问控制相关。

应提供对云服务、云服务所依赖的资源,以及相关控制功能的访问控制。

9.2.2.1.1 服务访问

服务访问组件提供对云服务提供者提供的云服务的访问。

9.2.2.1.2 业务访问

业务访问组件提供对云服务提供者提供的业务能力的访问。该组件由业务支撑系统实现。

9.2.2.1.3 管理访问

管理访问组件提供对云服务提供者提供的管理能力的访问。该组件由运营支撑系统实现。

9.2.2.1.4 开发访问

开发访问组件提供对提供者系统内一组能力的访问。该组能力支撑云服务实现的开发、测试和维护。

9.2.2.2 连接管理

连接管理组件依据来自用户层组件的流量和/或流向用户层组件的流量，提供对 QoS 策略的执行。连接管理组件与跨层功能交互以获取存储在那里的策略，并在访问层执行这些策略。

9.2.3 服务层组件

服务层组件包括：

- 服务能力；
- 业务能力；
- 管理能力；
- 服务编排。

9.2.3.1 服务能力

服务能力组件包括为实现提供给云服务客户的服务所必需的软件。服务能力组件实现了服务接口（例如，提供给云服务客户的服务接口）所定义的功能。服务能力组件不依赖于服务实现。

9.2.3.2 业务能力

业务能力组件实现了一组服务。该组服务访问与云服务提供相关的业务功能。业务功能自身包含在业务支撑系统组件中。

9.2.3.3 管理能力

管理能力组件实现了一组服务。该组服务访问与云服务提供相关的管理功能。管理功能自身包含在业务支撑系统和业务支撑系统组件中。

9.2.3.4 服务编排

服务编排组件提供对多个服务组件的协调、聚合和组合，以实现云服务的交付。

9.2.4 资源层组件

资源层组件包括：

- 资源抽象和控制；
- 物理资源。

9.2.4.1 资源抽象和控制

云服务提供者使用资源抽象和控制**功能组件**通过软件抽象提供对物理计算资源的访问。资源抽象需要确保对底层基础设施进行高效、安全和可靠地使用。该组件的控制特性能实现对资源抽象特性的管理。

资源抽象和控制**功能组件**使云服务提供者能够实现例如快速弹性扩展、资源池化、按需自服务等云计算特征。资源抽象与控制组件可以包含管理程序、虚拟机、虚拟数据存储和分时等软件元素。

资源抽象与控制组件帮助运营支撑系统组件(见 9.2.5.3)实现控制功能、监视和管理能力。例如,可以存在一个集中的算法来控制、关联和连接物理资源中不同的处理、存储和网络单元,使它们能共同交付一个 NaaS、IaaS、PaaS、SaaS 等类型的云服务的运行环境。控制器可以决定哪个 CPU 或机架来承载哪个虚拟机,执行给定云负载的哪个部分,以及这些处理单元如何相互连接,以及在条件变化时如何动态透明地将这些负载重新分配给新的单元。

资源是否是虚拟化的取决于负载的特征。对许多负载(例如计算、存储即服务类型的负载)而言,将底层物理资源虚拟化是很方便的,特别是对一些物理基础设施无法实现的场景(例如与镜像管理相关或根据需要动态扩展 CPU 容量的场景)。对其他负载而言(例如分析或搜索),需要尽可能大的运算能力,使用成百上千的节点来执行一个特定的任务。在这样的情况下采用非虚拟化的物理资源可能更为合适。

9.2.4.2 物理资源

物理资源**功能组件**代表云服务提供者运行和管理其提供的云服务所需的各种元素。

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。这些资源既能包括那些位于云数据中心内部的资源(例如计算服务器、存储服务器和数据中心的内部网络),也能包括那些位于数据中心外部的资源,通常是网络资源,例如数据中心间的网络和核心传输网络。

所有物理资源都由运营支撑系统**功能组件**管理。这些**功能组件**具备将各个云服务的实例分配到资源上以满足客户需求的能力。需要注意的是,通常运营支撑系统**功能组件**自身也运行在一些物理资源上。

9.2.5 跨层功能

9.2.5.1 集成组件

集成组件负责连接体系架构中的其他组件,以构成一个统一的架构体系。

集成组件提供云计算体系架构内部、体系架构的组件间,以及体系架构与外部组件间的消息路由和消息交换机制。消息路由可以基于不同的标准,例如,上下文,策略等。

集成组件包括:

- 安全集成;
- 监控集成;
- 服务集成;
- 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包括鉴别、授权、加密和完整性验证等在内的安全能力集成,以及与安全能力相关的策略机制集成。

9.2.5.1.2 监控集成

监控集成功能组件提供从访问层、服务层和资源层的组件到运营支撑系统中监控能力和报告能力的连接。

9.2.5.1.3 服务集成

服务集成功能组件提供与服务提供者环境中运行的服务的连接。服务集成功能组件是实现服务虚拟化的重要方面，可以使服务的位置和实现细节对服务组件不可见。

9.2.5.1.4 对等服务集成

对等服务集成组件用于以可控方式连接对等云服务提供者的服务，这种连接采用适当的安全措施，并按适当的计量方式计算使用量，同时连接云服务用户的身份系统。对等服务集成组件也把与目标服务的连接虚拟化，以便这些目标服务可以动态改变，而不对影响依赖它们的那些服务产生影响。

9.2.5.2 安全组件

安全组件应用与控制有关的安全策略来降低云计算环境中的安全威胁。安全组件包括所有支持云计算所需的安全工具。

安全组件包括：

- 鉴别和身份管理；
- 授权和安全策略管理；
- 加密管理。

9.2.5.2.1 鉴别和身份管理

鉴别和身份管理组件提供访问云服务及其相关管理和业务能力时的用户身份识别能力。

身份管理可以包括联合身份管理，以允许用户用同一个身份和证书访问多个云服务，提供诸如“单点登录和鉴别”类能力。

9.2.5.2.2 授权和安全策略管理

授权和安全策略管理组件为用户访问特定的功能或数据提供授权控制和应用能力。安全策略管理用于与服务有关的安全策略的定义和应用。

9.2.5.2.3 加密管理

加密管理提供与数据(静态或动态数据)加密有关的能力，例如加密密钥管理和加密模式选择等。

9.2.5.3 运营支撑系统组件

运营支撑系统组件包括一组与操作有关的管理功能，这些功能用于管理和控制提供给用户使用的云服务。

运营支撑系统组件包括：

- 服务目录；
- 交付；
- 监测与报告；
- 服务策略管理；
- 服务自动化；
- 服务水平管理；
- 异常和问题管理；
- 平台与虚拟化管理；
- 对等服务管理。

9.2.5.3.1 服务目录

服务目录**功能组件**提供某一特定云服务提供者的所有云服务列表。服务列表包括/参考所有部署、提供和运行云服务有关的技术信息。

9.2.5.3.2 供应

供应**功能组件**提供服务交付功能，以服务实现和访问端点两种形式提供。同时，该组件提供必需的工作流，以确保这些服务元素以正确的顺序提供。

9.2.5.3.3 监控和报告

监测和报告**功能组件**提供如下功能：

- 通过云服务提供者的系统监测其他组件的云计算活动。这包括由 CSC：云服务用户（诸如服务访问和服务实现）直接使用云服务时（例如，某一用户调用一个云服务操作）涉及的组件。这包括对云服务进行支撑的组件，例如 OSS 的服务自动化组件（例如，为某一用户提供服务实例）；
- 提供云服务提供者系统的行为报告，具有时间敏感特性的行为可采取警告的形式（例如，某个错误的发生，任务的完成），或者采用历史数据聚合的形式（例如，服务使用数据）；
- 以日志记录存储和访问监控和事件数据。

需要保证监控和报告组件中记录的日志记录的可用性、可信性和完整性。对多租户云服务，需要对记录的访问进行设计，以使特定的租户只能访问自己的信息，而不能访问其他的租户。

9.2.5.3.4 服务策略组件

服务策略**功能组件**提供云服务的定义、存储和访问策略。这些策略包括用于云服务本身及其使用的业务、技术、安全、隐私和认证等策略。

一些策略是通用的，适用于所有用户。另一些策略则专门是针对特定用户的。

9.2.5.3.5 服务自动化

服务自动化**功能组件**提供服务交付能力，包括服务的执行和管理，以及服务的协同。服务自动化组件保存服务的模板，该模板定义了用于提供和交付服务特定访问入口的云计算行为和工作流。

云服务的交付可以自动化，以支持可伸缩的资源操作，包括配置和负载。

云服务用户的云服务管理功能也能够自动化，而不需要云服务提供者的任何干预。

服务自动化组件与交付组件及服务集成组件一起配合实现这一目标。

9.2.5.3.6 服务水平管理

服务水平管理**功能组件**提供特定云服务的服务级别管理功能，以使服务符合它的 SLA 要求。

服务级别管理组件管理云服务的功能和性能，这包括各项服务策略应用（例如，用于避免单点失效的分布规则）。

服务级别管理组件从监控和报告组件获得监控信息，以为云计算服务衡量和记录关键的性能指标。基于这些 KPI 来分配或去除相应的能力。

服务级别管理组件也记录已分配或可用资源的整体状态。已分配的能力与云服务性能 KPI 的比较有助于识别当前或潜在的瓶颈，以支持能力规划。

9.2.5.3.7 异常和问题管理

事件和问题管理**功能组件**提供事故和问题报告的捕获功能，并通过分析来管理这些报告。

事故和问题可由云服务提供方系统或云服务用户检测和报告。

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**提供管理云服务提供方(如计算机、存储、网络)基础资源的功能,以及这些资源的虚拟化使用能力(例如,通过管理程序)。

典型情况下这些资源组成资源池。资源池具有如下重要特征:

- 标准化硬件部件和配置;
- 通过新硬件的增加随时扩展;
- 当负载有变化时,可动态迁移资源;
- 保护和隔离邻近的负载和数据;
- 通过资源间的负载和数据转移,减少/消除宕机时间;
- 基于目标(例如,性能、可用性、许可权和能源使用)管理资源消费。

9.2.5.3.9 对等服务管理

对等服务管理**功能组件**提供连接服务提供方的运营支撑系统、业务支撑系统和对等云服务提供方的管理及业务功能。

对等服务管理**功能组件**根据对等云服务提供者的请求,负责建立所需的通信路径,传送合适的身份和证件。

9.2.5.4 业务支撑系统组件

业务支撑系统**功能组件**涵盖了与业务相关的处理客户和支撑流程的管理能力,包括:

- 产品目录;
- 账户管理;
- 订单管理;
- 计费;
- 账务。

9.2.5.4.1 产品目录

产品目录组件为云服务的客户提供可购买的服务列表的查看功能,并为云服务提供商的员工提供产品目录的内容管理功能。

产品目录中的每个条目包含了相应云服务的技术信息(如服务所提供的功能,可用服务操作的接口定义,安全信息等)和商务信息(如价格和计费方式)。

9.2.5.4.2 账户管理

账户管理组件提供管理云服务客户关系的功能,包括:

- 合同管理;
- 云服务订单;
- 权限;
- 服务定价,可包含对特定用户的特殊条款(如折扣);
- 云服务用户数据的处理策略。

源于用户账户数据的重要性和敏感性,账户管理组件及其相关的数据库有严格的可用性和安全要求。

9.2.5.4.3 订单管理

订单管理组件负责处理云服务客户的云服务订单，记录用户新建或修改的订单信息，并确保订单中服务的交付。

9.2.5.4.4 计费

计费组件提供以下功能：

- 云服务客户使用云服务的计量和计费——其中计量是指对云服务客户消费使用云服务的度量，计费是指根据计费方法和计量数据计算出费用。对数据的具体计量形式根据云服务的特性而定。计费方法可包含针对特定用户特殊条款（如折扣），并需要确定的折算计量数据的算法；
- 基于以上功能产生的费用生成账单，并把账单提交给云服务客户。另外，账单数据还用于账户管理**功能模块**和账务**功能模块**。

9.2.5.4.5 账务

账务**功能组件**负责总账和会计相关的功能。包含应收账款和应付账款。注意账户组件只负责云服务提供商的账户，不涉及客户账户（后者由账户管理组件负责）。

9.2.5.5 开发功能组件

开发功能组件支撑云服务开发者的云计算活动，包括服务实现的开发和/或集成、构建管理和测试管理。

开发功能组件由以下组件构成：

- 开发环境；
- 构建管理；
- 测试管理。

9.2.5.5.1 开发环境

开发环境**功能组件**提供用于服务实现的软件的开发，支持服务中软件模块的开发，提供服务组合的工具。

开发环境组件支持使用云服务提供者所提供的服务能力，包括资源连接和网络连接，与其他服务（包括对等云服务提供者的服务）的集成，监控和管理能力的集成，安全能力的集成。

开发环境组件支持开发的服务相关的配置元数据的生成；支持供服务提供商运维支撑系统使用的服务配置脚本和组件的生成。

9.2.5.5.2 构建管理

构建管理**功能组件**构建可发布的软件包。该软件包可提交给云服务提供者，并部署在云服务环境中。软件包既包含用于服务实现的软件，又包含配置元数据和配置脚本。

9.2.5.5.3 测试管理

测试管理**功能组件**支持对所有的服务实现软件的测试。测试管理组件生成测试报告，并将测试报告和服务实现软件一同提供给云服务提供者。

一般情况下，测试会在一个特殊的测试环境中执行。测试环境与生产环境非常类似。同时，测试环

境不会影响到生产环境。云计算下的测试环境可由云服务提供者提供。

10 用户视图与功能视图之间关系

10.1 概述

在第8章介绍云计算角色与活动的用户视图，第9章介绍包含功能组件的功能视图的基础上，本章描述角色和活动与功能组件之间的逻辑映射关系。

映射关系是标准的一部分。标准中的映射关系可应用于：

a) 明确信息流或其他类型互操作的程度；

b) 确保指定的质量(例如安全或服务水平)。

本架构中定义的逻辑关系是确定CCRA及其行为的重要组成部分。该逻辑关系描述内容包括CCRA组件间交互所需的信息流。

10.2 概览

图15展示了CCRA主要元素的常用配置，包括角色、云计算活动和组件。

在图15中，圆角实线矩形代表角色，六边形代表子角色，圆角虚线矩形代表云计算活动，砖形填充的矩形代表组件。云能力组件内的L型框代表基于基本云能力类型的云服务接口。从图15中可以明显看出：角色是云服务活动的集合，云服务活动本身又通过组件实现。

角色框之间的距离是有意义的，表示相邻角色之间的交互程度。例如，将云服务提供者角色放在图的中央，强调它与其他所有角色都进行交互。这同样适用于给定角色中云计算活动之间的位置关系，以及给定活动中组件之间的位置关系。例如，服务能力组件位于资源抽象和控制组件之上，表明前者依赖于后者。

共同关注点包括可审计性、可用性、治理、互操作性、维护和版本控制、性能、可移植性、隐私、弹性、可逆性、安全性、服务水平和服务水平协议等。共同关注点在图15中最外层的边框内标识，表明共同关注点的内容适用于图15中所有其他元素，包括角色、活动和组件。因此，举个例子，CSC：云服务用户必须有一个身份标识和一组凭证信息。当用户执行使用云服务活动时，身份标识和凭证信息必须提交给用户功能组件。用户功能组件将身份标识和凭证信息提交给访问控制组件。作为提供服务活动的一部分，访问控制组件执行认证与授权，并在云服务提供给CSC：云服务用户之前，调用适当的安全组件。

图15中的云服务能力组件代表云服务自身的实现。

10.2.1 服务能力组件

云服务通过服务接口提供一种或多种云能力类型。云能力类型通过服务能力组件中的倒置L形框来表示。顶层的L形框代表应用能力类型，中间层的L形框代表平台能力类型，底层的L形框代表基础设施能力类型。

L形框的含义是应用能力类型的实现可以使用或者不使用平台能力(取决于云服务提供者的选择)，平台能力类型的实现可以使用或者不使用基础设施能力类型。

对于SaaS或CaaS云服务类别，服务能力组件包含应用相关的软件或通信应用软件。这些软件部署在资源层上以便实现SLA中指定的服务水平。

其他云服务类别见ITU-T Y.CCDEF|ISO/IEC 17788。

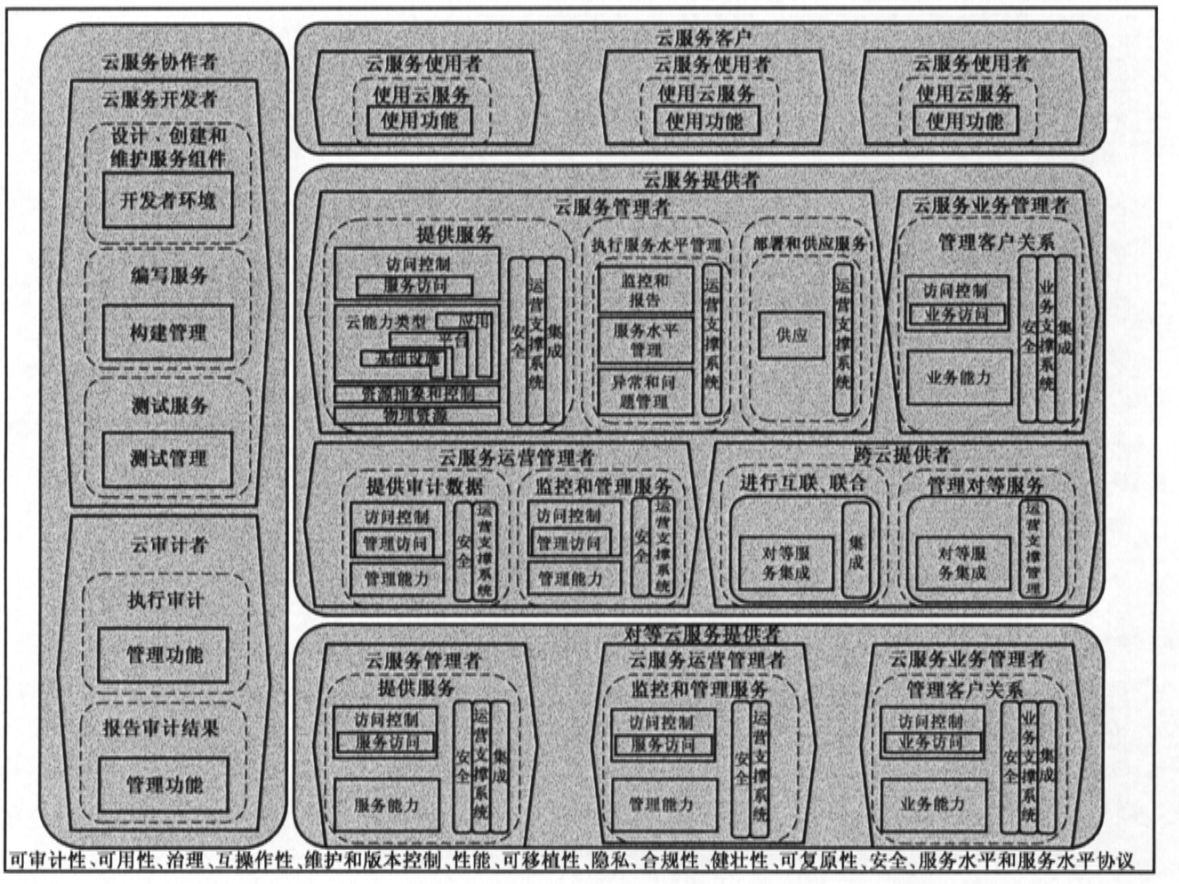

图 15　角色，云计算活动和组件的通用视图

10.2.2　常用角色、活动和组件

图 15 中云服务提供者有一个叫 CSP：云服务管理者的子角色。云服务管理者执行提供服务活动。该活动为 CSC：云服务用户提供实际使用的服务。但是，在服务能被使用之前，需要进行云服务的开发、部署和运维。

图 15 中云服务合作者有两个子角色：云服务开发者和云审计者。云服务开发者使用开发工具组件开发云服务，使用测试管理组件测试服务。然后将云服务和部署信息一起打包发送给 CSP：云服务管理者。CSP：云服务管理者执行部署和供应服务活动，以便在提供服务活动中提供服务能力组件。同时，根据各自的策略和治理方案，云审计者对云服务开发者、云服务提供者或云服务客户从事执行审计和报告审计结果活动。

在 CSP：云服务管理者执行完部署和供应服务活动之后，提供服务活动使用服务能力组件。该组件是对服务的实现，并依次使用资源层组件中的计算、存储和网络资源运行服务。提供服务活动还包括集成服务能力组件，与安全组件集成提供安全和隐私能力，例如数据加密。运营支持系统组件支持对服务和资源的管理、监控、自动化和配置。此外，CSP：云服务管理员从事执行服务水平管理活动。该活动管理服务的可用性和性能，以便服务遵循与云服务客户签订合同中所包含的 SLA。服务水平管理、监控和报告、异常和问题管理这 3 个组件都是用来实现此目标。

有时，CSP：云服务管理者通过与另一 CSP：云服务管理者合作，调用该云服务管理者服务的方式提供服务。CSP：云服务管理者执行管理对等云服务活动，为使用对等服务签订协议和 SLA。对等云服务

提供者还提供和其他云服务提供者类似的管理云计算和使用云计算活动，包括：提供服务、执行服务水平管理。

图 15 中描述了 CSP：云服务管理员提供的常用云计算活动集合，但是，本标准也描述了其他的云计算活动。

现在服务是可用的。云服务客户有两个子角色：CSC：云服务管理员和 CSC：云服务用户。CSC：云服务管理员测试云服务，监控和执行 SLA、为使用云服务提供订阅和报告。作为 CSC：云服务管理者活动的一部分，执行管理租户活动使用管理员功能组件保证租户需求被合适地实现。完成上述操作之后，子角色 CSC：云服务用户执行使用云服务活动。该活动使用用户功能组件与云服务进行交互。

图 16 展示了角色、云计算活动和组件。箭头表明多个云计算活动和多个角色之间的关系。附录 A 给出了这些关系的描述。

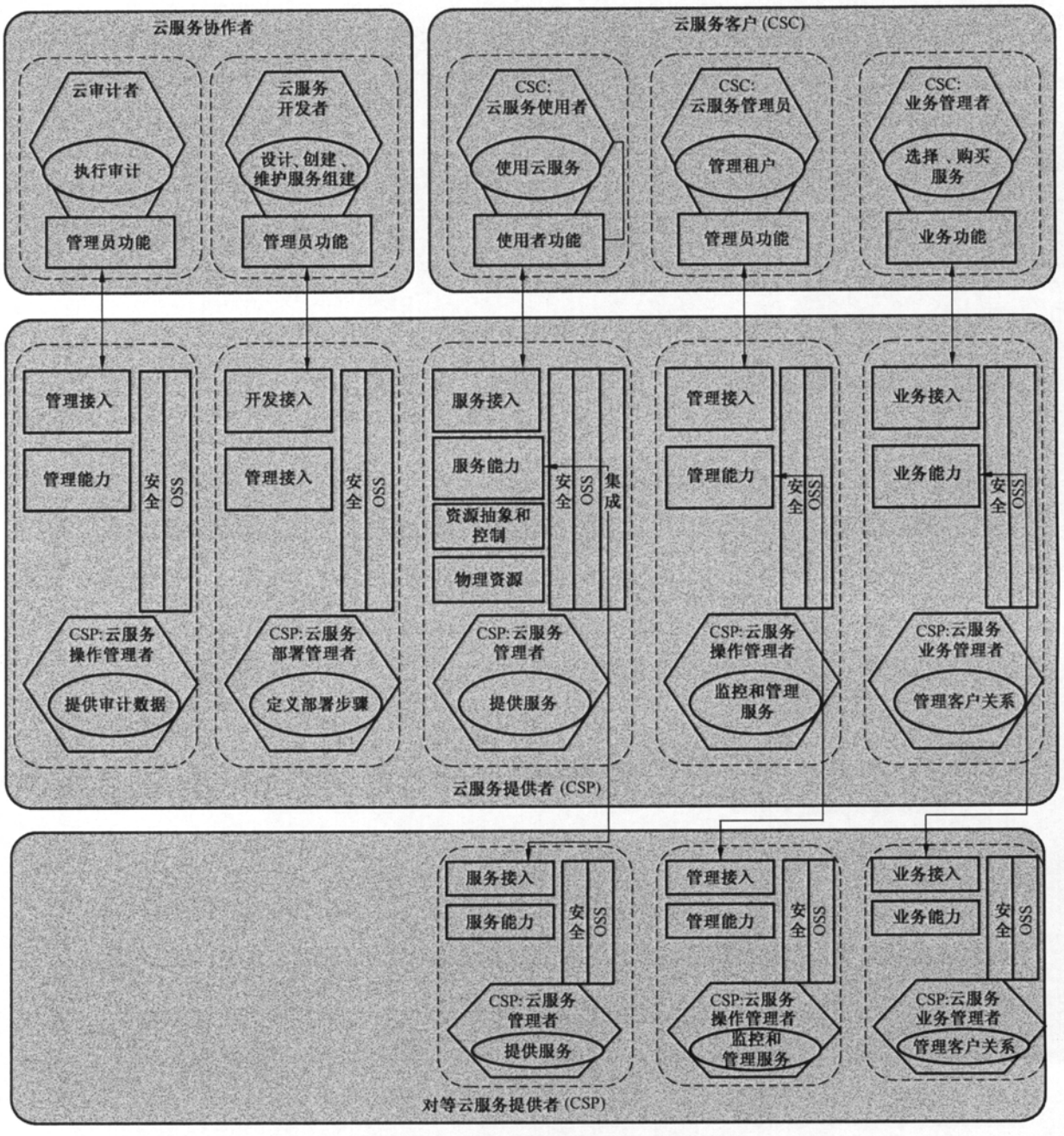

图 16　活动和组件之间关系和交换示例

10.2.3 多租户和隔离

云计算涉及对一些资源的共享。这通常意味着要在云服务的多个客户内共享这些资源。术语租户和多租户用来描述资源共享的场景。

云服务的租户与云服务客户并不完全相同。一个租户是一组 CSC：云服务用户，这些用户共享对一组物理资源和虚拟资源的访问。通常情况下，一组 CSC：云服务用户与一个特定的云服务客户有关，但是，一个云服务客户可以包含多个租户，例如，来自客户组织内不同部门的用户组。

通过对物理或虚拟资源的分配保证多个租户以及他们的计算和数据彼此隔离和不可访问。也就是说，一个租户的用户应该完全感知不到另一个租户的用户的存在。

多租户不仅影响云服务自身，还影响云服务提供者提供给云服务客户的业务能力和管理能力。关于用户账号、订阅、使用量和计费的信息必须被全部隔离，并且只对相关租户所属的客户可见。与资源相关的内容，比如包含多个租户记录的日志文件，必须被额外关注。如果一个客户需要在事故发生时访问日志记录，那么必须对日志记录进行过滤以保证客户只能看到该客户下属租户的日志记录。

附 录 A
（资料性附录）
关于用户视图和功能视图的进一步描述

A.1 云服务客户和云服务提供者关系

在云服务客户和云服务提供者关系中有 3 个关键要素：

a) CSC：云服务用户使用提供者的云服务来实现自身的业务目标；

b) CSC：业务管理者基于云服务提供商的业务能力订购云服务并从业务的视角管理服务；

c) CSC：云服务管理者基于云服务提供者提供的管理能力，从云服务客户的视角来管理云服务的使用。

A.1.1 功能关系

云服务用户通过终端和服务访问功能组件提供的接口来使用云服务。接口的功能和相应的信息流与特定的云服务相关，因此不属于参考架构的范畴，但是服务接口中应反映某些通用需求，特别是需要识别和验证云服务用户的需求。

CSC：云服务用户通过用户功能组件来执行使用云服务的活动。该功能组件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：云服务用户的身份验证，并进行使用特定云服务能力的授权。如果被授权，服务访问功能组件调用云服务实现来完成用户请求。

图 A.1 展示了 CSC：云服务用户使用云服务活动过程中所涉及功能组件之间的关系。

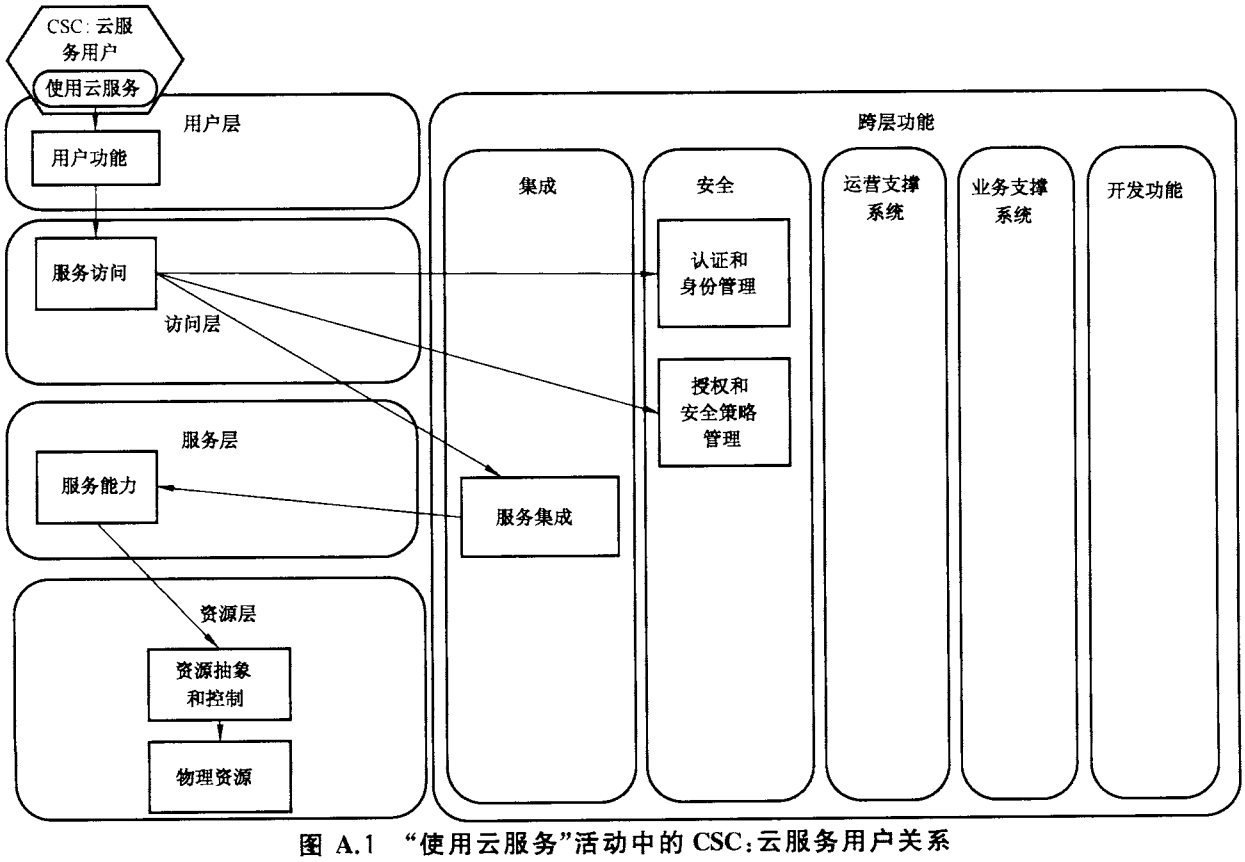

图 A.1 “使用云服务”活动中的 CSC：云服务用户关系

A.1.2 业务关系

CSC:云服务业务管理者通过用户层的业务功能**功能组件**来完成各类**云计算活动**:选择和购买服务、执行业务管理和获取审计报告。业务功能**功能组件**通过业务访问**功能组件**的终端和接口来调用云服务提供者的业务能力。

业务访问**功能组件**验证 CSP:云服务业务管理者的身份,并授权其访问业务能力的特定功能。业务能力**功能组件**与业务支撑系统**功能组件**交互来完成 CSC:云服务业务管理者的各类请求。业务支撑系统**功能组件**包括**产品目录**,账户管理和订购管理。

业务能力相关的信息通常包括:

a) 可用云服务的**产品目录**,包含相关的技术信息、定价、条款和条件等;

b) 订购信息,包括客户订购了哪些服务,以及可能包含的相关数量信息(如用户数、数据量、处理量等);

c) 计费信息,包括使用量计费、付款和账户状态。

图 A.2 展示了 CSC:云服务业务管理者选择和购买服务活动过程中所涉及功能组件之间的关系。

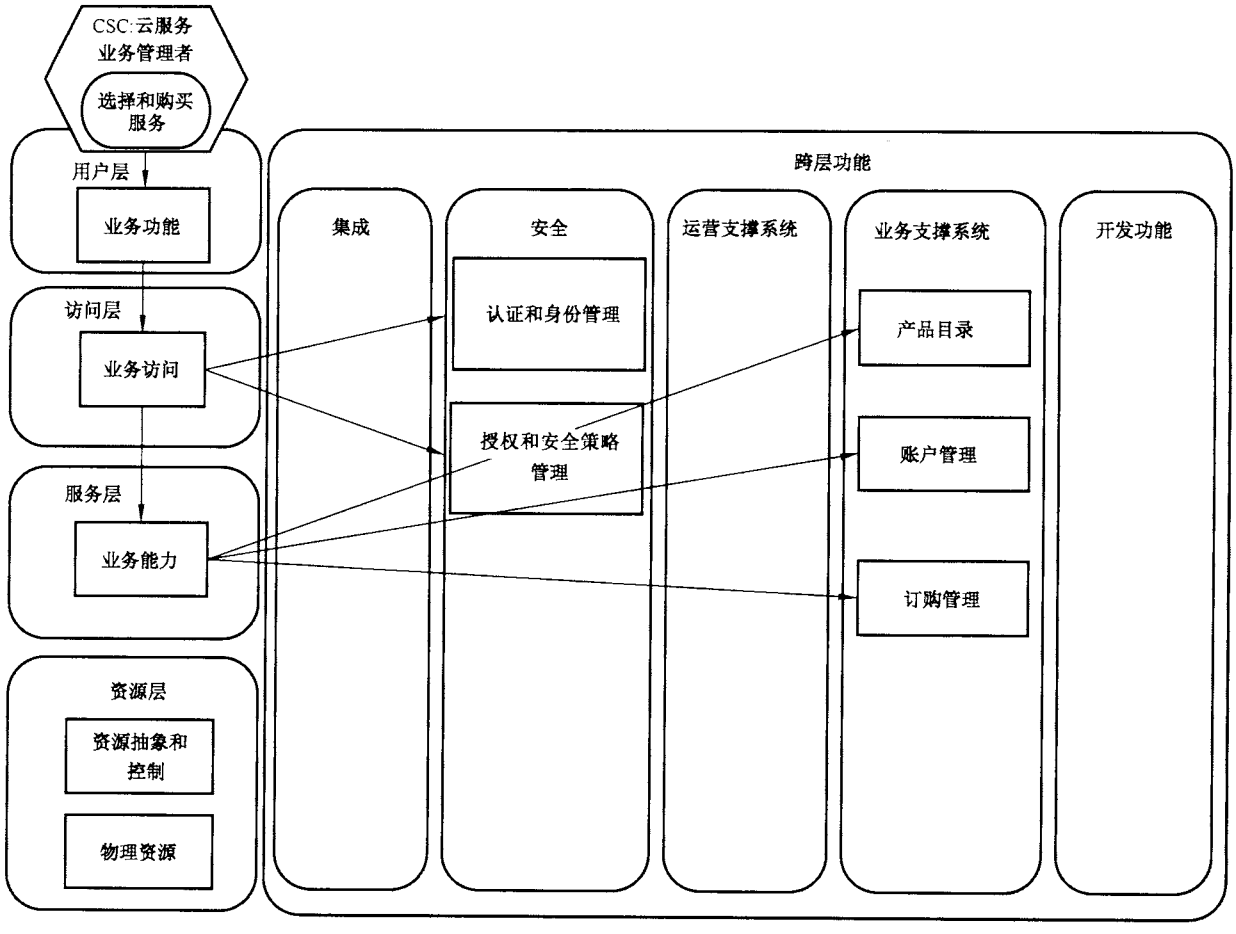

图 A.2 “选择和购买服务”活动中的 CSC:云服务业务管理者关系

A.1.3 管理关系

CSC:云服务管理者通过管理功能**功能组件**执行以下云计算活动:

- 监控服务;

- 提供计费和使用量报告；
- 管理租户；
- 管理服务安全性；
- 处理问题报告。

管理功能**功能组件**通过管理访问**功能组件**的终端和接口来调用云服务提供者的管理功能**能力组件**。管理访问**功能组件**完成对 CSC：云服务支配者的身份验证并授权其使用特定支配能力组件的功能。支配能力组件与运行支撑系统组件一起响应 CSC：云服务支配者的请求，如监控和报告。

管理访问**功能组件**验证 CSP：云服务管理者的身份，并授权其访问管理能力**功能组件**的特定功能。管理能力**功能组件**与运营支撑系统**功能组件**交互来完成 CSC：云服务管理者的各类请求。运营支撑系统**功能组件**包括监控和报告**功能组件**。

管理能力相关的信息通常包括：

- 安全信息，例如用户账户和授权数据的设置，数据加密；
- 服务使用情况报告单，包括使用情况统计，日志记录（如出于安全目的）；
- 异常报告和事件（如违反某个 SLA 目标，或发生安全事故）。

图 A.3 展示了 CSC：云服务管理者的监控服务活动所涉及**功能组件**间的关系。

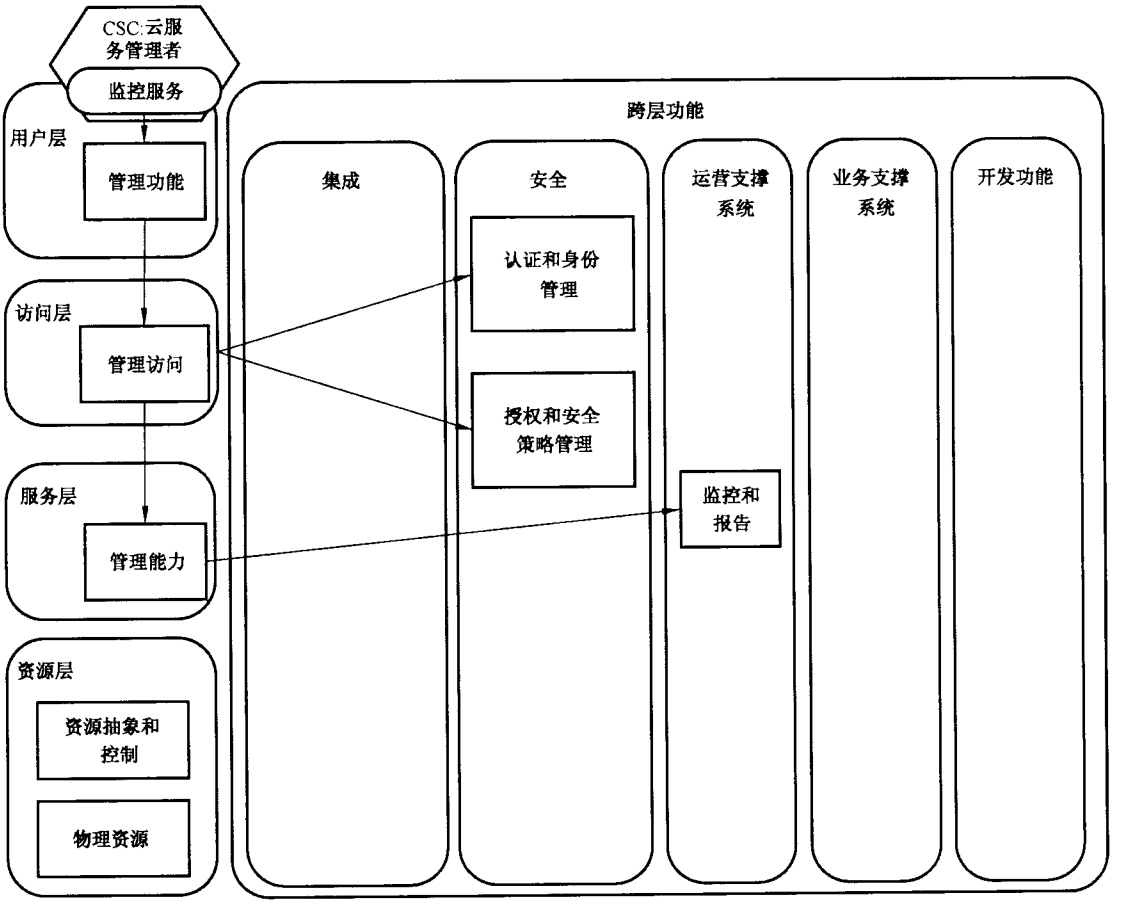

图 A.3 “监控服务”活动所涉及的 CSC：云服务管理者关系

其他与**云服务客户**和**云服务提供者**之间关系相关的因素能包括客户和提供者之间的协议。该协议能包含 SLA、知识产权和管理，例如对个人数据的适当保护。

A.2 提供者和对等提供者("云间")关系

一个**云服务提供者**能使用其他**云服务提供者**提供的一个或多个**云服务**。这种关系称为提供者与对等提供者关系,也称为"云间"关系。其中,使用服务的提供者称为主**云服务提供者**,提供服务的提供者称为从**云服务提供者**。

相较于云服务客户和云服务提供者间的关系,云服务提供者间的关系包含两个**功能组件**:

- 主云服务提供者使用从服务提供者的云服务;
- 主云服务提供者的 CSP:云服务运营管理者和 CSP:云服务管理者使用从云服务提供者的业务能力和管理能力来使用和控制从提供者的云服务。

对于从服务提供者来说,主服务提供者承担云服务客户的角色。从**云服务提供者**的服务提供给主云服务提供者的客户使用。通过主提供者将从**云服务提供者**和**云服务客户**联系起来时,需要特别考虑安全、PII 保护和数据所有权等方面。

至关重要的是,主提供者需要确保从提供者的服务(SLA)满足主提供者的服务要求,并且任何违背 SLA 的情况都得到适当处理。

提供者和对等提供者关系中包含 3 类接口:管理接口、业务接口和服务接口,这些接口提供了与云服务客户和云服务提供者间接口大体相同的能力。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。

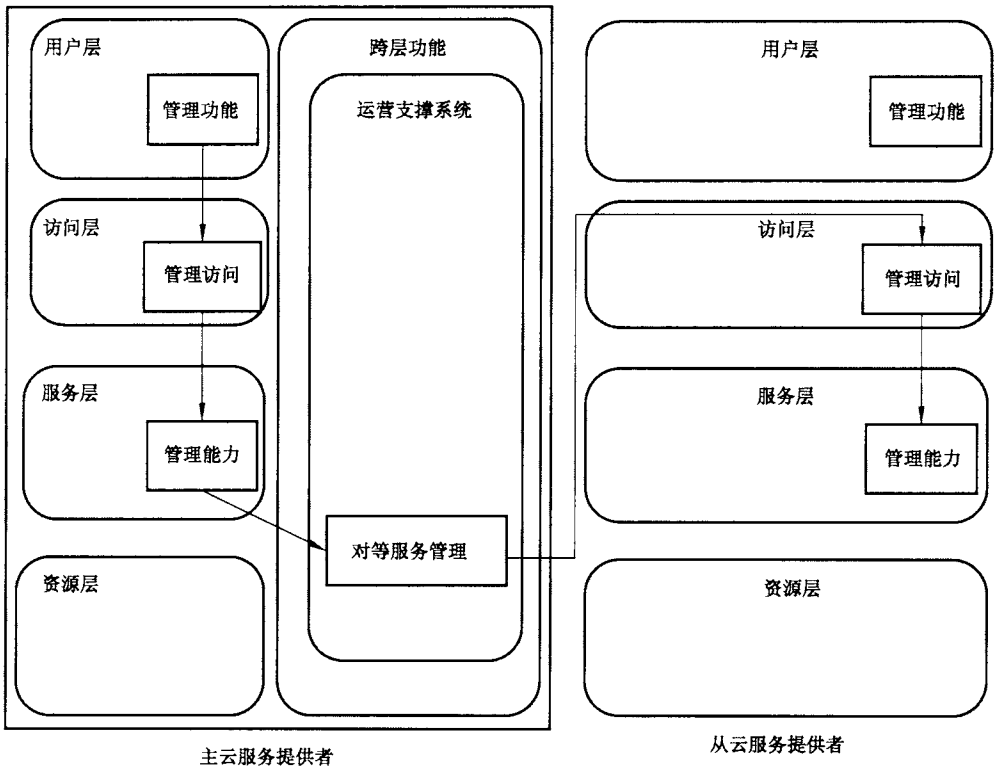

图 A.4 提供者和对等提供者之间的管理活动关系

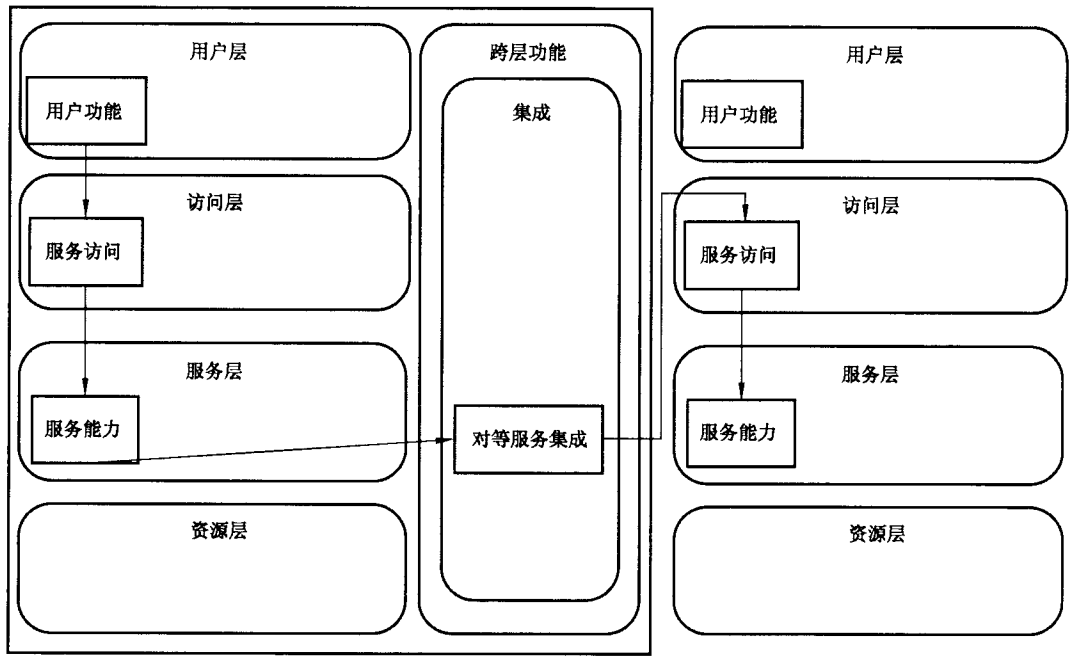

图 A.5　提供者和对等提供者之间的使用服务活动关系

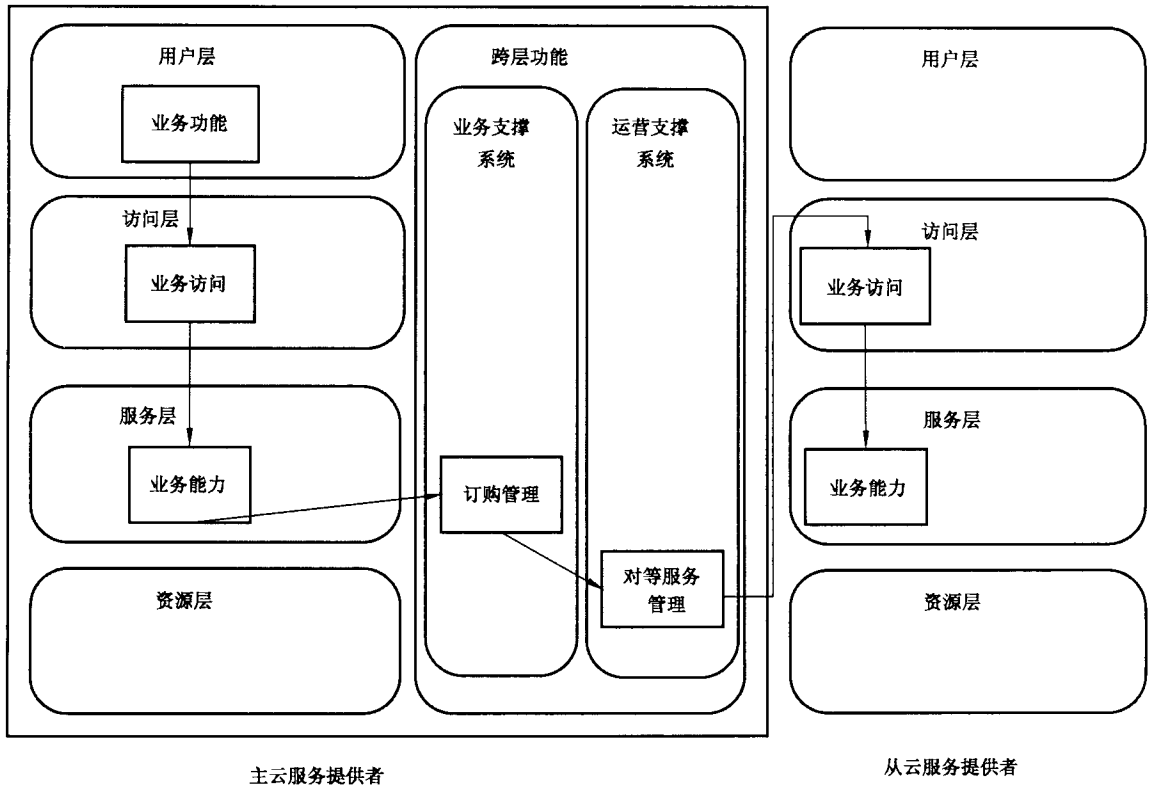

图 A.6　提供者和对等提供者之间的业务接口关系

A.3 云服务开发者和云服务提供者关系

云服务开发者完成服务实现和服务打包，然后提交给**云服务提供者**部署和运营。因此服务开发者与**云服务提供者**交互实现以下目标：

- 检查云服务提供者的服务执行环境；
- 测试服务实现；
- 提交服务实现包。

开发功能**功能组件**支持的云服务开发者**云计算活动**包括：开发服务、测试服务和维持服务。这些**云计算活动**依赖开发环境、构建管理和测试管理**功能组件**。

图 A.7 中开发环境组件相关的线条表示云服务开发者实现服务，并使用开发环境**功能组件**组合服务，然后使用构建管理系统构建服务和相关的构件，并打成一个部署包。测试管理**功能组件**进出的线段表明测试管理系统针对构建好的包执行相应的测试，从构建管理系统获取包，通过开发访问**功能组件**与开发环境交互来部署服务的测试版本，并执行测试。

为了在目标执行环境运行服务实现和服务访问，安全、监控、管理、自动化等需要正常启动，同样需要成功的集成到服务集成环境。云服务开发者(红线)通过使用开发接口活动发现监控集成、安全集成和服务集成的合理实现。此外认证和身份管理及授权和服务政策管理的信息和需求通过开发接入组件恢复。

部署和配置云服务实现的启动同样通过开发环境和构建管理系统完成(例如，通过脚本生配置元数据文件)。云服务开发者使用开发接口组件发现配置和部署的需求。

服务实现同配置和部署一起被打包，并传给源程序：云服务管理者执行部署服务活动，结果是在提供服务活动中服务对消费者是可用的。

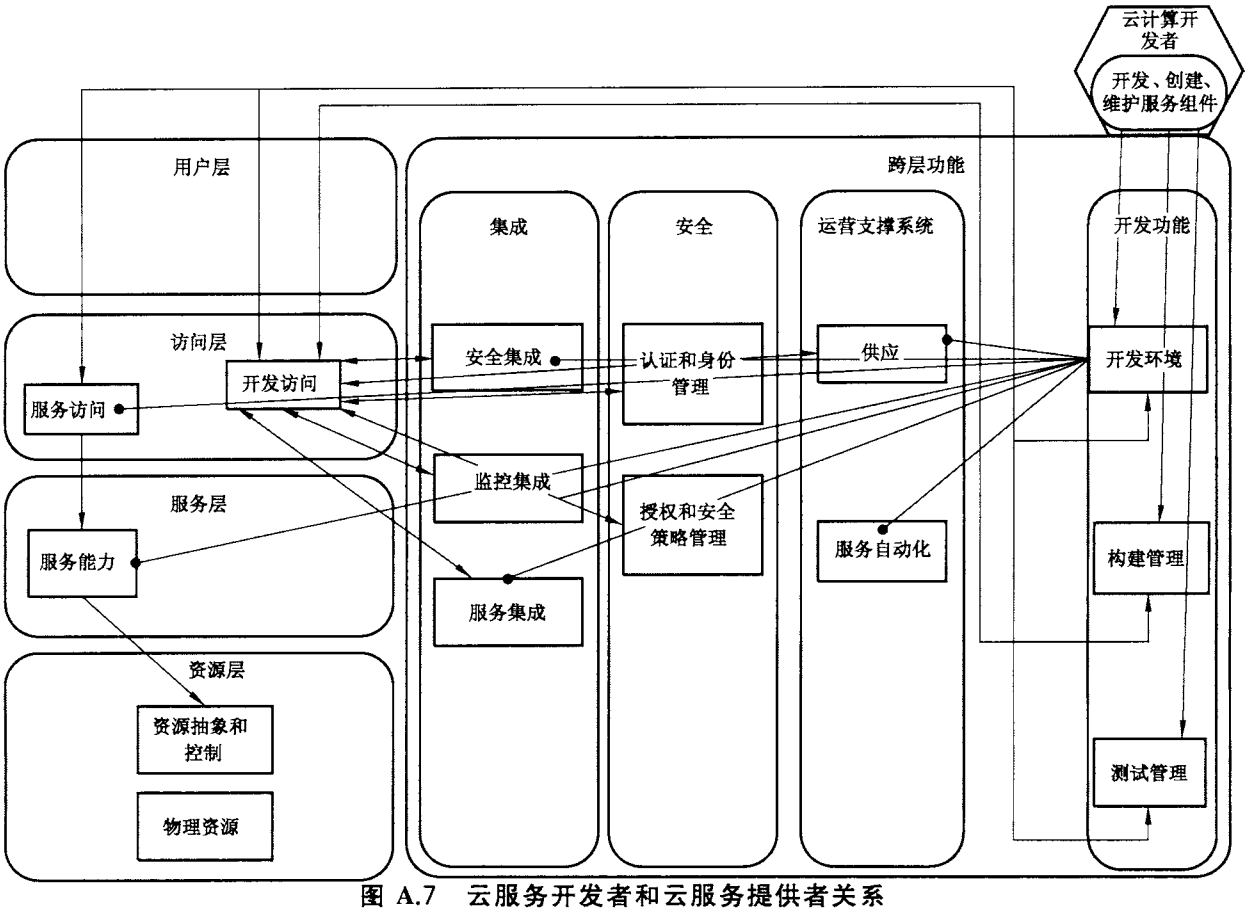

图 A.7 云服务开发者和云服务提供者关系

A.4 云服务提供者和审计者关系

云审计者应审计议定的技术参数、政策及协议。

审计技术参数以是云服务提供者设定标准，审计员设定的标准，独立设定的标准或根据法律需要设定。选取哪个取决于审计者审计结果的目标。如果审计结果的目标是需要一些独立保证的云服务消费者，那么审计使用独立设定的标准。

政策由提供者为审计提供者的基础设施各服务设定。这些政策在治理过程中由生意设定。

云服务协议可能包括与云服务提供者审计，或可能为云服务消费者审计相关的条款。相似的协议应该在主要的云服务提供者与次要云服务提供者之间合适的位置。审计者的责任在不同情况下是相同的。

云审计者的云计算活动有安全审计，隐私影响审计和业绩审计。对所有这些云计算活动，审计者可从云服务提供者那里得到审计凭证。审计凭证的格式将取决于适应于审计的审计和标准的类型而多种多样。凭证可以是程序文件的形式，也可以是日志记录。无论如何，云服务提供者都有云审计者获取所需凭证的手段。

在图 16 中，云审计者的执行审计活动通过提供者的管理接入组件，调用必要的管理活动向云提供者得出审计凭证的要求。

A.4.1 安全审计

系统安全审计有各种各样的标准。涵盖信息安全管理的 ISO/IEC 27001 是其中之一。同时还有很多其他组织为云安全提供审计标准。

A.4.2 隐私审计

各种数据保护部门(例如，加拿大隐私权专员和英国信息专员)均发布了程序、政策或系统的隐私安全的评定和/或审计的指导方针。个人验证信息的保护是管理和/或立法的典型对象，但与云服务相关的问题之一是，云服务消费者与云服务提供在不同的管辖区内。如果云服务提供者在不同的辖区内操作多个数据中心并在这些数据中心间转移数据或服务执行(例如，出于服务连续的目的或资源利用的有效性的目的)，情况会变得更加复杂。

ISO/IEC SC 27 负责制定定义适用于担当数据处理器的云服务提供者的信息安全控制的标准。ISO/IEC SC 27 同时处理更广的安全标准(例如 ISO/IEC 29100 系列标准)。

数据审计者按照数据保护部门的执导方针和相关标准，对云服务的隐私方面和云服务提供者针对适合的隐私规则的操作进行评估。

A.4.3 性能审计

性能审计评估云服务提供者的能力是否与待定云服务性能目标是否一致，性能目标通常记录在 SLA 中。

参 考 文 献

[1] ISO/IEC 27000:2014, Information technology—Security techniques—Information security management systems—Overview and vocabulary

[2] ISO/IEC 27001 Information technology—Security techniques—Information security management systems—Requirements

[3] ISO/IEC 27002 Information technology—Security techniques—Information security managementsystems—Code of practice for information security management

[4] ISO/IEC 27018 Information technology—Security techniques—Information security management systems—Code of practice for PII protection in public clouds acting as PII processors

[5] ISO/IEC/IEEE 24765:2010, Systems and software engineering—Vocabulary

[6] ISO/IEC/IEEE 42010:2011, Systems and software engineering—Architecture description

GB/T 32399-2015

*

书号:155066 · 1-52850

定价: 48.00 元

打印日期: 2016年3月17日 F009B