



中国电子技术标准化研究院
China Electronics Standardization Institute

云计算标准化白皮书

(3.0)

中国电子技术标准化研究院

版权声明

本白皮书版权属于中国电子技术标准化研究院（工业和信息化部电子工业标准化研究院），凡转载或引用本文的观点、数据，请注明“来源：中国电子技术标准化研究院”。

前 言

云计算作为信息技术领域的一种创新应用模式，自其概念诞生以来一直备受国际国内的广泛关注，近年来被看作是新一代信息技术变革和商业模式变革的核心，具有广阔的市场前景。目前几乎所有的国际主流 IT 企业都已参与云计算领域，各公司根据自己的传统技术领域和市场策略从各个方向进军云计算。

我国正面临发展战略性新兴产业和推动信息化与工业化深度融合的重要时期，在国务院颁布实施的《关于加快培育和发展战略性新兴产业的决定》中明确提出包括新一代信息技术在内的七个重大发展领域。2012 年 5 月国务院常务会议讨论通过的《“十二五”国家战略性新兴产业发展规划》中对节能环保、新一代信息技术等七大战略性新兴产业“十二五”期间的发展作出总体部署。其中促进云计算产业研发和示范应用被看作是新一代信息技术发展的重要内容之一。

云计算标准化工作作为推动云计算技术产业及应用发展，以及行业信息化建设的重要基础性工作之一，近年来受到各国政府以及国内外标准化组织和协会的高度重视。

全国信息技术标准化技术委员会云计算标准工作组做为国内专门从事云计算标准化工作的技术组织，负责云计算领域的标准化工作，包括云计算领域的基础、技术、产品、

测评、服务、安全、系统和装备等国家标准的制修订。工作组按照“政府推动、企业为主、产学研用联合”的原则，一方面在研究梳理国际云计算标准的基础上，积极开展我国云计算标准体系框架的研究工作，从案例和场景的收集和标准化需求分析，到标准和规范的制定，再到标准的符合性测试、应用，内容覆盖云计算基础标准、互操作和可移植、数据中心和设备、安全和服务等各个方面；另一方面以 ISO/IEC JTC1 SC7、SC38 和 SC39 为依托，积极参与和推动云计算的国际标准化相关工作，以促进国内标准工作与国际工作的协同开展。

为了推动我国云计算标准体系的建设和相关标准的制定，支撑云计算产业和应用的发展，进一步促进我国与国际的云计算标准化工作融合发展，中国电子技术标准化研究院组织国内行业专家编写了《云计算标准化白皮书》。本白皮书分析了当前国内外云计算发展的现状及主要问题，梳理了国际标准组织及协会的云计算标准化工作，总结出云计算的主要支撑技术，并基于此，从促进我国云计算产业有序健康发展的角度，就我国的云计算标准体系以及未来云计算标准化工作提出了工作建议，为落实国家战略性新兴产业发展规划和推动云计算产业健康发展提供标准化支撑。

本白皮书的发布，旨在与业界分享中国电子技术标准化研究院近年来在云计算领域的标准研究成果。

目 录

一、绪论	1
(一) 背景	1
(二) 范围	2
(三) 缩略语和习语	2
1、组织协会缩略语	2
2、技术术语缩略语	3
二、云计算概述	4
(一) 云计算的定义	4
(二) 云计算的关键特征	4
(三) 云能力类型和云服务类别	6
1、云能力类型	6
2、云服务类别	6
(四) 典型的云计算部署模式	7
(五) 云计算参考架构	7
三、云计算支撑技术分析	14
1、系统虚拟化	15
2、虚拟化资源管理	16
3、分布式数据存储	17
4、并行计算模式	19
5、用户交互技术	21
6、安全管理	21
7、运营支撑管理	22
四、云计算应用情况分析	26
(一) 国际云计算应用情况分析	26
(二) 国内云计算应用情况分析	28
(三) 云计算面临的挑战	29
五、国际云计算标准化工作	31
(一) 国际云计算标准化工作概述	31
(二) 国际云计算标准化工作分析	32
六、国内云计算标准化工作	34
(一) 国内云计算标准化工作概述	34
(二) 云计算标准体系	35
1、基础标准	38
2、网络标准	39
3、整机装备标准	39
4、软件标准	40
5、服务标准	45
6、安全标准	47
7、其它标准	48
七、如何实施云计算	48

(一) 云计算实施总路线.....	48
(二) 云服务水平协议 (SLA) 实施步骤.....	52
(三) 云安全实施步骤.....	55
附录 A OpenStack 开源云计算平台介绍	61
A.1 OpenStack 云计算平台概述	61
A.2 OpenStack Compute.....	61
A.3 OpenStack Object Storage.....	63
A.4 OpenStack Image Service.....	64
附录 B 国际标准化组织和协会的主要工作.....	66
B.1 ISO/IEC JTC1/SC7 简介	66
B.2 ISO/IEC JTC1/SC27 简介	66
B.3 ISO/IEC JTC1/SC38 简介	67
B.4 ISO/IEC JTC1/SC39 简介	67
B.5 ITU-T SG13 简介	68
B.6 分布式管理任务组 (DMTF) 简介.....	68
B.7 云安全联盟 (CSA) 简介.....	69
B.8 欧洲电信标准研究所 (ETSI TC GRID) 简介.....	70
B.9 美国国家标准与技术研究院 (NIST) 简介.....	71
B.10 开放网络论坛开放云计算接口工作组 (OGF OCCI-WG) 简介...	72
B.11 全球网络存储工业协会 (SNIA) 简介.....	72
B.12 开放云计算联盟 (OCC) 简介.....	73
B.13 结构化信息标准促进组织 (OASIS) 简介.....	74
B.14 开放组群 (TOG) 简介.....	74
B.15 零售行业技术标准协会 (ARTS) 简介.....	75
B.16 电气与电子工程学会标准协会 (IEEE SA) 简介.....	75
B.17 云计算互操作论坛 (CCIF) 简介.....	76
B.18 开放云计算宣言 (OCM) 简介.....	76
B.19 云计算用户案例讨论组 (CCUCDG) 简介.....	76
B.20 云审计 (CloudAudit) 简介.....	77
B.21 OMG 云标准协调组 (OMG Cloud Standards Coordination) 简介	77
B.22 因特网工程任务组 (IETF) 简介.....	77
B.23 全球跨云技术论坛 (GICTF) 简介.....	78
B.24 TM Forum 云服务启动组简介	78
B.25 亚洲云计算协会 (ACCA) 简介.....	79
B.26 世界无线通讯解决方案联盟 (ATIS) 简介.....	79
B.27 开放数据中心联盟 (ODCA) 简介.....	80
B.28 云标准客户委员会 (CSCC) 简介.....	80
B.29 欧洲云行业联盟 (EuroCloud) 简介.....	81
B.30 欧洲网络和信息安全协会 (ENISA) 简介.....	81
B.31 韩国云计算论坛 (CCFK) 简介.....	82
B.32 韩国云服务联盟 (KCSA) 简介.....	82
B.33 云计算战略研究小组 (CSRT) 简介.....	83
参考文献	84

一、绪论

（一）背景

云计算作为一种 IT 基础设施交付和使用模式，一种信息服务交付和使用模式，一种基于互联网共享信息资源的新型计算模式，近年来备受业界和各国政府关注。全球云计算产业虽处于发展初期，但发展空间十分广阔，Gartner 报告显示，云计算服务市场规模总量目前仅占全球 ICT 市场总量的 1/40，但增长迅猛，未来几年年均增长率预计将超过 20%，到 2015 年，全球云计算服务市场规模预计将达到 1768 亿美元。众多国内外厂商围绕云计算开发出大量的产品，越来越多的互联网应用开始尝试构建在云平台之上，基于云计算的解决方案也在多个领域逐步开始实施，云计算市场方兴未艾。与此同时，云服务的多样性以及资源平台的异构性为不同云之间的互连互通带来了巨大挑战。针对云计算中的各个关键层面制定相应标准，成为屏蔽云服务多样性和资源异构性，搭建一个互联互通、安全可靠云计算环境的必要条件。

云计算标准化工作是推动云计算技术、产业及应用发展，以及行业信息化建设的重要基础性工作之一。云计算相关技术规范和标准也成为当前国际标准组织及协会的关注热点。近年来，ISO、IEC、ITU 等国际标准组织纷纷启动云计算标准化工作并取得了实质性进展。我国相关标准化组织也启动了云计算的标准化研究及规划工作。2012 年 9 月 20 日成立了“全国信息技术标准化技术委员会云计算标准工作组”（以下简称“云计算标准工作组”），开展我国云计算标准化工作。在我国云计算标准化工作中，一方面，梳理了国际标准组织及协会的云计算标准化工作，调研我国云计算标准化需求，参与我国云计算标准体系的研制，并开展急需的云计算标准制定；另一方面，积极参与和推动国际云计算标准化相关工作，以促进国内云计算标准工作与国际工作的协调开展。

为了推动我国云计算标准体系的建设和相关标准的制定，支撑云计算产业和应用的发展，进一步促进我国与国际的云计算标准化工作融合发展，中国电子技术标准化研究院组织编写了《云计算标准化白皮书》，本白皮书全面介绍了云计算的关键支撑技术，系统分析了云计算在国内外的应用情况，重点梳理了

国内外云计算标准化组织和协会的工作进展，最后提出了基于国家标准的我国云计算实施步骤建议。

（二）范围

《云计算标准化白皮书》将关注云计算的概念和发展趋势、介绍云计算技术的应用情况、全面分析国内外云计算标准化工作现状、同时结合我国云计算的产业和应用情况提出我国云计算实施步骤建议，为我国云计算产业落地应用提出参考意见。

（三）缩略语和习语

1、组织协会缩略语

A

ARTS: Association for Retail Technology Standards（零售行业技术标准协会）

C

CCIF: Cloud Computing Interoperability Forum（云计算互操作论坛）

CESI: China Electronics Standardization Institute（中国电子技术标准化研究院）

CSA: Cloud Security Alliance（云安全联盟）

CSRT: Cloud Strategy Research Team（云计算战略研究小组）

D

DMTF: Distributed Management Task Force（分布式管理任务组）

E

ETSI: The European Telecommunications Standards Institute（欧洲电信标准研究所）

EuroCloud: EuroCloud（欧洲云行业联盟）

G

GICTF: Global Inter-Cloud Technology Forum（全球跨云技术论坛）

I

IEEE: Institute of Electrical and Electronics Engineers（电气电子工程师学会）

ISO/IEC JTC1 SC7: International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee Sub-technical Committee 7（国际标准化组织/国际电工委员会第一联合技术委员会 7 分技术委员会）

ISO/IEC JTC1 SC38: International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee Sub-technical Committee 38（国际标准化组织/国际电工委员会第一联合技术委员会 38 分技术委员会）

ITU-T: International Telecommunication Union – Telecommunication Standardization

Sector （国际电信联盟电信标准化部）

K

KCSA: Korea Cloud Service Association （韩国云服务联盟）

N

NIST: National Institute of Standards and Technology （美国国家标准与技术研究院）

O

OASIS: Organization for the Advancement of Structured Information Standards （结构化信息标准促进组织）

OCC: The Open Cloud Consortium （开放云计算联盟）

OCM: Open Cloud Manifesto （开放云计算宣言）

OGF: Open Grid Forum （开放式网格论坛）

OMG: Object Management Group （对象管理组）

S

SNIA: Storage Networking Industry Association （全球网络存储工业协会）

T

TOG: The Open Group （开放群组）

2、技术术语缩略语

A

AJAX: Asynchronous JavaScript and XML （异步 JavaScript 和 XML）

C

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

CDMI: Cloud Data Management Interface （云数据管理接口）

CRM: Customer Relationship Management （客户关系管理）

E

EC2: Elastic Computing Cloud （弹性计算云）

G

GFS: Google File System （Google 文件系统）

H

HDFS: Hadoop Distributed File System （Hadoop 分布式文件系统）

I

IaaS: Infrastructure as a Service （基础架构即服务）

IAM: Identity and Access Management （身份及访问管理）

M

MPI: Message Passing Interface （消息传递接口）

O

OCCL: Open Cloud Computing Interface （开放云计算接口）

OVF: Open Virtualization Format （开放虚拟化格式）

P

PaaS: Platform as a Service （平台即服务）

PUE: Power Usage Effectiveness （电能利用率）

R

REST: Representational State Transfer (表述性状态转移)

S

SaaS: Software as a Service (软件即服务)

SLA: Service Level Agreement (服务水平协议)

SOA: Service Oriented Architecture (面向服务的体系架构)

SPoF: Single Point of Failure (单点登录故障)

SSO: Single Sign On (单点登录)

S3: Simple Storage Service (简单存储服务)

V

VMM: Virtual Machine Monitor (虚拟机监控器)

X

XAM: eXtensible Access Method (可扩展访问方法)

二、云计算概述

(一) 云计算的定义

随着云计算的不断发展，业界对云计算的定义认识已趋于统一，目前云计算的定义以ISO/IEC JTC1 和ITU-T组成的联合工作组制定的国际标准ISO/IEC 17788《云计算词汇与概述》(Information technology–Cloud Computing–Overview and vocabulary) DIS版的定义为主。其定义为：

云计算是一种将可伸缩、弹性、共享的物理和虚拟资源池以按需自服务的方式供应和管理，并提供网络访问的模式。云计算模式由关键特征、云计算角色和活动、云能力类型和云服务分类、云部署模型、云计算共同关注点组成。

(二) 云计算的关键特征

《云计算概述与词汇》中对云计算关键特征进行了具体规定。这些关键特征一方面可以帮助理解云计算的内涵和外延，另一方面可以作为区别云计算和其它各类计算模式的依据。云计算的关键特征为：

——广泛的网络接入。可通过网络，采用标准机制访问物理和虚拟资源的特性。这里的标准机制有助于通过异构用户平台使用资源。这个关键特性强调云计算使用户更方便地访问物理和虚拟资源：用户可以从任何网

络覆盖的地方，使用各种客户端设备，包括移动电话、平板、笔记本和 workstation 访问资源。

——可测量的服务。通过可计量的服务交付使得服务使用情况可监控、控制、汇报和计费的特性。通过该特性，可优化并验证已交付的云服务。这个关键特性强调客户只需对使用的资源付费。从客户的角度看，云计算为用户带来了价值，将用户从低效率和低资产利用率的业务模式转变到高效率模式。

——多租户。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的特性。在典型的多租户环境下，组成租户的一组云服务用户同时也属于一个云服务客户组织。在某些情况下，尤其在公有云和社区云部署模型下，一组云服务用户由来自不同客户的用户组成。一个云服务客户组织和一个云服务提供者之间也可能存在多个不同的租赁关系。这些不同的租赁关系代表云服务客户组织内的不同小组。

——按需自服务。云服务客户能根据需要自动，或通过与云服务提供者的最少交互，配置计算能力的特性。这个关键特性强调云计算为用户降低了时间成本和操作成本，因为该特性赋予了用户无需额外的人工交互，就能够在需要的时候做需要做的事情的能力。

——快速的弹性和可扩展性。物理或虚拟资源能够快速、弹性，有时是自动化地供应，以达到快速增减资源目的的特性。对云服务客户来说，可供应的物理或虚拟资源无限多，可在任何时间购买任何数量的资源，购买量仅仅受服务协议的限制。这个关键特性强调云计算意味着用户无需再为资源量和容量规划担心。对客户来说，如果需要新资源，新资源就能立刻自动地获得。资源本身是无限的，资源的供应只受服务协议的限制。

——资源池化。将云服务提供者的物理或虚拟资源进行集成，以便服务于一个或多个云服务客户的特性。这个关键特性强调云服务提供者既能支持多租户，又通过抽象对客户屏蔽了处理复杂性。对客户来说，他们仅

仅知道服务在正常工作，但是他们通常并不知道资源是如何提供或分布的。资源池化将原本属于客户的部分工作，例如维护工作，移交给了提供者。需要指出的是，即使存在一定的抽象级别，用户仍然能够在某个更高的抽象级别指定资源位置。

（三）云能力类型和云服务类别

1、云能力类型

云能力类型是根据资源的使用情况，对为云服务客户提供的云服务的功能进行的分类。有三类不同的云能力类型：应用能力类型、基础设施能力类型和平台能力类型。这三类能力类型有不同的关注点，即相互之间的功能交叉最少。这些云能力类型不应与云服务类别混淆。

- 应用能力类型。云服务客户能使用云服务提供者的应用的一类云能力类型。
- 基础设施能力类型。云服务客户能配置和使用计算、存储和网络资源的一类云能力类型。
- 平台能力类型。云服务客户能使用云服务提供者支持的编程语言和执行环境，部署、管理和运行客户创建或客户获取的应用的一类云能力类型。

2、云服务类别

云服务类别是拥有相同质量集的一组云服务。一种云服务类别可对应一种或多种云能力类型。

典型的云服务类别包括：

- 通讯即服务（CaaS）。为云服务客户提供实时交互与协作能力的一种云服务类别。
- 计算即服务（CompaaS）。为云服务客户提供部署和运行软件所需的配置和使用计算资源能力的一种云服务类别。
- 数据存储即服务（DSaaS）。为云服务客户提供配置和使用数据存储相

关能力的一种云服务类别。

——基础设施即服务（IaaS）。为云服务客户提供云能力类型中的基础设施能力类型的一种云服务类别。

——网络即服务（NaaS）。为云服务客户提供传输连接和相关网络能力的一种云服务类别。

——平台即服务（PaaS）。为云服务客户提供云能力类型中的平台能力类型的一种云服务类别。

——软件即服务（SaaS）。为云服务客户提供云能力类型中的应用能力类型的一种云服务类别。

（四）典型的云计算部署模式

云计算有四类典型的部署模式：“公有云”、“私有云”、“社区云”和“混合云”。具体描述如下：

——公有云。云基础设施对公众或某个很大的业界群组提供云服务。

——私有云。云基础设施特定为某个组织运行服务，可以是该组织或某个第三方负责管理，可以是场内服务（on-premises），也可以是场外服务（off-premises）。

——社区云。云基础设施由若干个组织分享，以支持某个特定的社区。社区是指有共同诉求和追求的团体（例如使命、安全要求、政策或合规性考虑等）。和私有云类似，社区云可以是该组织或某个第三方负责管理，可以是场内服务，也可以是场外服务。

——混合云。云基础设施由两个或多个云（私有云、社区云或公有云）组成，独立存在，但是通过标准的或私有的技术绑定在一起，这些技术可促成数据和应用的可移植性（例如用于云之间负载分担的 cloud bursting 技术）。

（五）云计算参考架构

在国家标准《信息技术 云计算参考架构》中，对展示了云计算模式和其他

计算模式之间的区别和联系，同时，展示了不同角色之间的分工、合作和交互，为云计算提供者和开发者搭建了一个基本的技术实现参考模型，该国家标准等同采用国际标准 ISO/IEC 17789《信息技术 云计算 参考架构》(Cloud Computing Reference Architecture)，简称 CCRA。

CCRA 从四个不同的视角描述了云计算，如图 1。

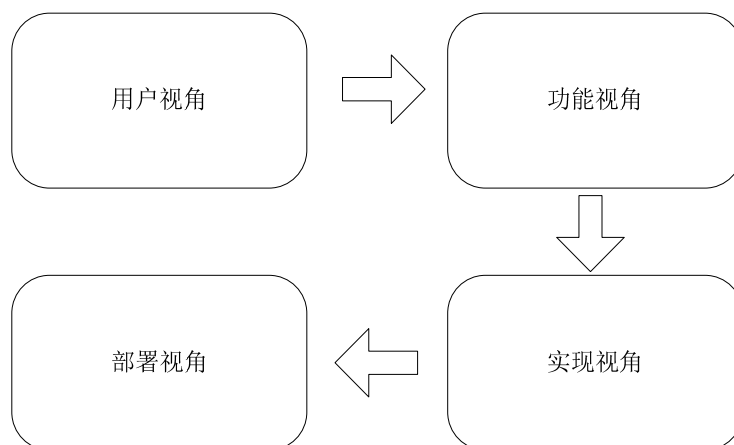


图 1 架构视角之间的转换

CCRA 包含了详细的用户视角和功能视角，并未包含实现视角和部署视角的具体介绍。图 2 给出了用户视角向功能视角的转换。

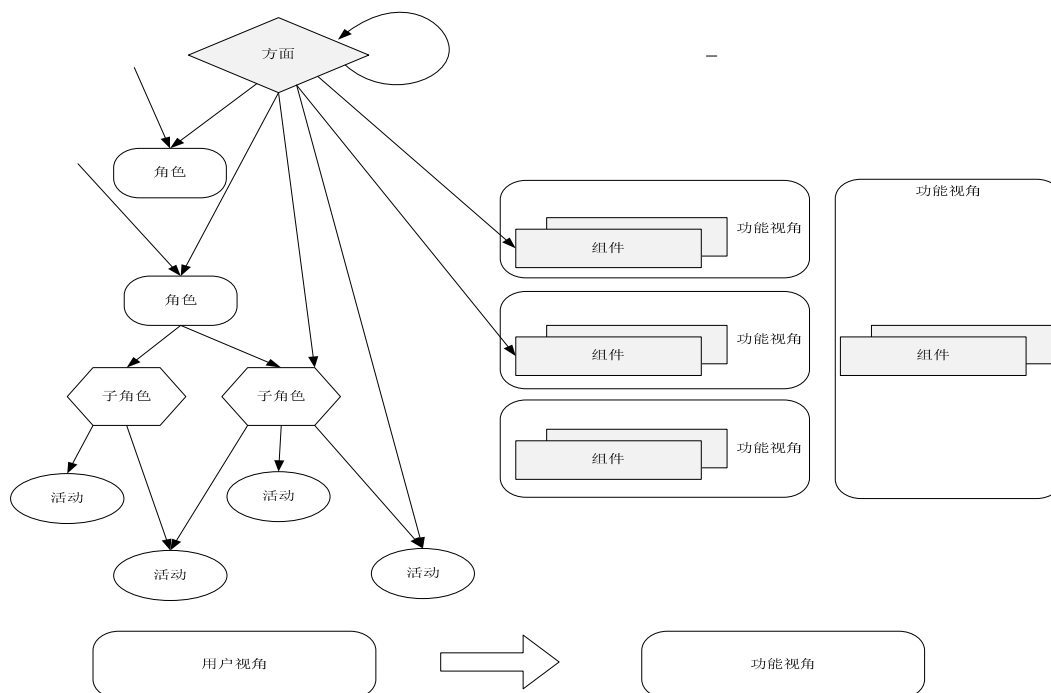


图 2 用户视角向功能视角的转换

用户视角涉及云计算活动，角色和子角色，参与方，云能力类型和云服务类别，云部署模型和共同关注点等云计算概念。见图 3。

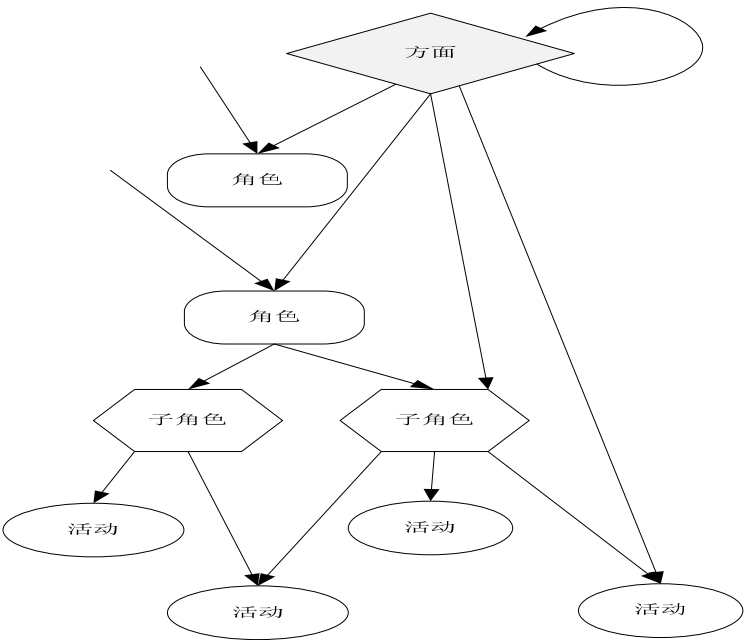


图 3 用户视角实体

其中，角色是一组具有相同目标的云计算活动的集合。其中云计算的角色包括：云服务客户，云服务提供者，云服务协作者。表 1 展示了云计算角色及其包含的子角色，及活动。

表 1 CCRA 角色、子角色和活动

角色	子角色	活动
云服务客户	云服务用户	使用云服务
	云服务管理者	<div><div></div>执行服务测试</div> <div><div></div>监控服务</div> <div><div></div>管理安全策略</div> <div><div></div>提供计费和使用量报告</div> <div><div></div>对问题报告的处理</div> <div><div></div>管理租户</div>

		<ul style="list-style-type: none"> ● 管理资产和库存 ● 提供审计数据
	云服务部署管理者	<ul style="list-style-type: none"> ● 定义环境和流程、 ● 定义度量指标的收集、 ● 定义部署步骤、
	云服务管理者	<ul style="list-style-type: none"> ● 提供服务、 ● 部署和配置服务、 ● 执行服务水平管理
	云服务业务管理者	<ul style="list-style-type: none"> ● 管理提供云服务的业务计划、 ● 管理客户关系、 ● 管理财务流程
	客户支持和服务代表	监控客户请求
	跨云提供者	<ul style="list-style-type: none"> ● 管理同级的云服务； ● 执行云服务的调节、聚集、仲裁、互连或者联合
	云服务安全和风险管理	<ul style="list-style-type: none"> ● 管理安全和风险 ● 设计和实现服务的连续性 ● 确保依从性
	网络提供者	<ul style="list-style-type: none"> ● 提供网络连接、 ● 交付网络服务、 ● 提供网络管理
云服务协作者	云服务开发者	<ul style="list-style-type: none"> ● 设计、创建和维护服务组件 ● 组合服务 ● 测试服务
	云审计者	<ul style="list-style-type: none"> ● 执行审计 ● 报告审计结果
	云服务代理者	<ul style="list-style-type: none"> ● 获取和评估客户 ● 选择和购买服务 ● 获取审计报告

CCRA 还有一个很重要的概念就是共同关注点，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。共同关注点包含可审计性，可用性，治理，互操作性，维护和版本控制，性能，可移植性，隐私，法规，弹性，可复原性，安全，服务水平和服务水平协议等。

CCRA 认为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。

功能视图涵盖了功能组件，功能层和跨层功能等云计算概念，如图 4。

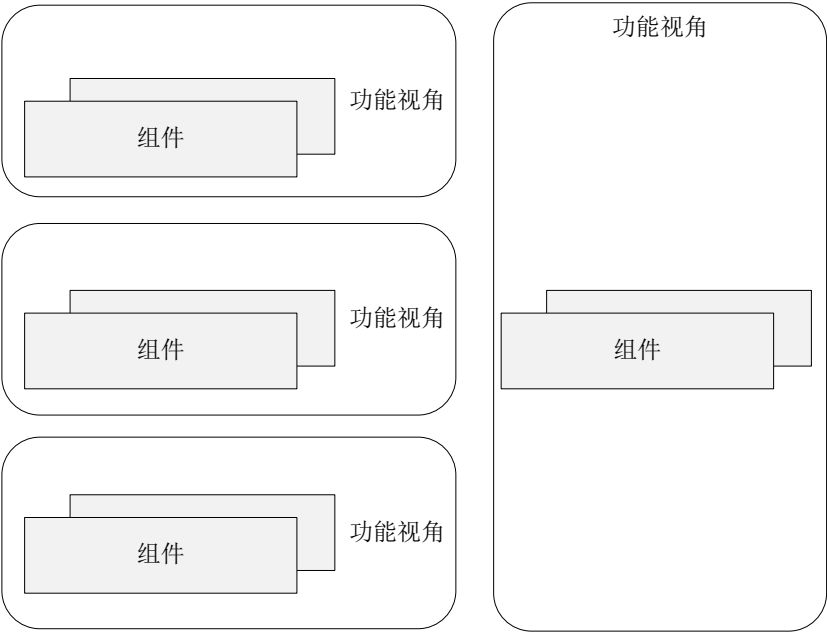


图 4 功能层

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。四层分别是：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 5 所示。

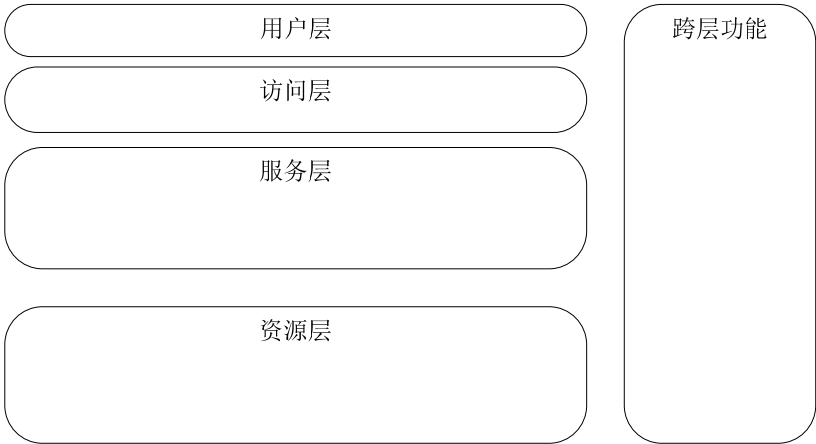


图 5 云计算层次框架

图 6 展示了使用分层框架方式组织的对 CCRA 组件的高层次概述。

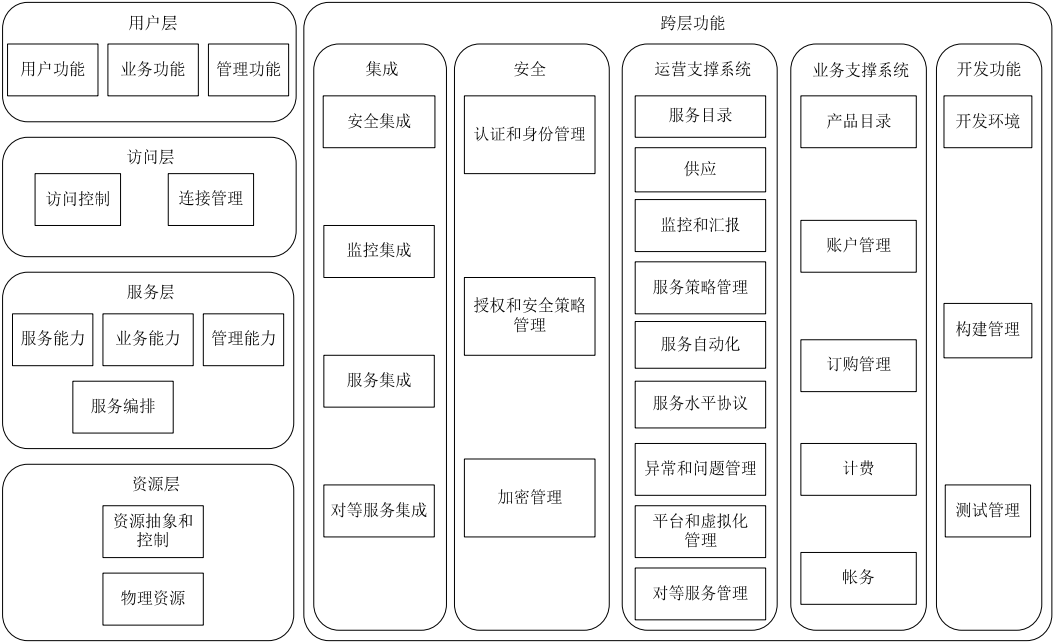


图 6 CCRA 功能组件

图 7 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（以及如何使用实现视图中的技术实现）。

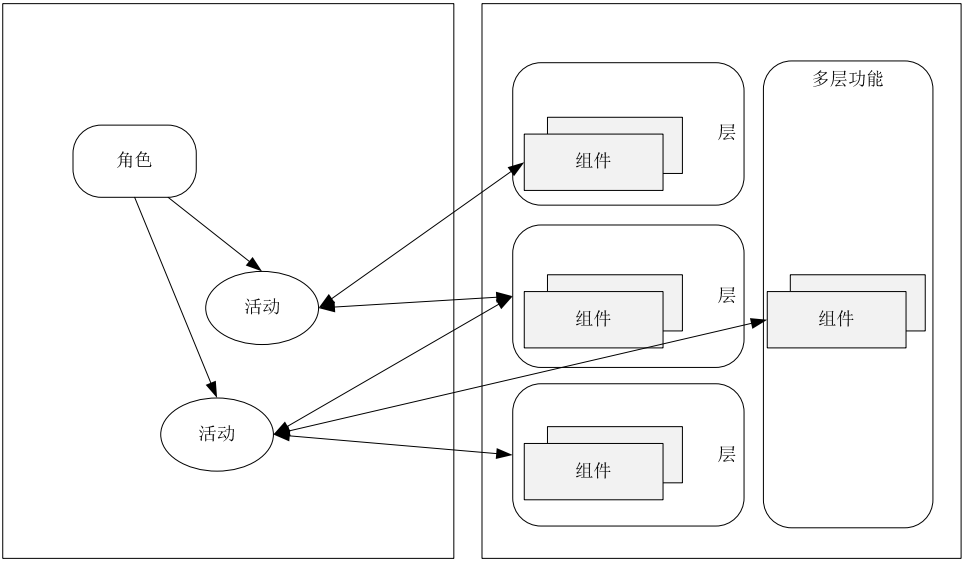


图 7 从用户视图到功能视图

图8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。

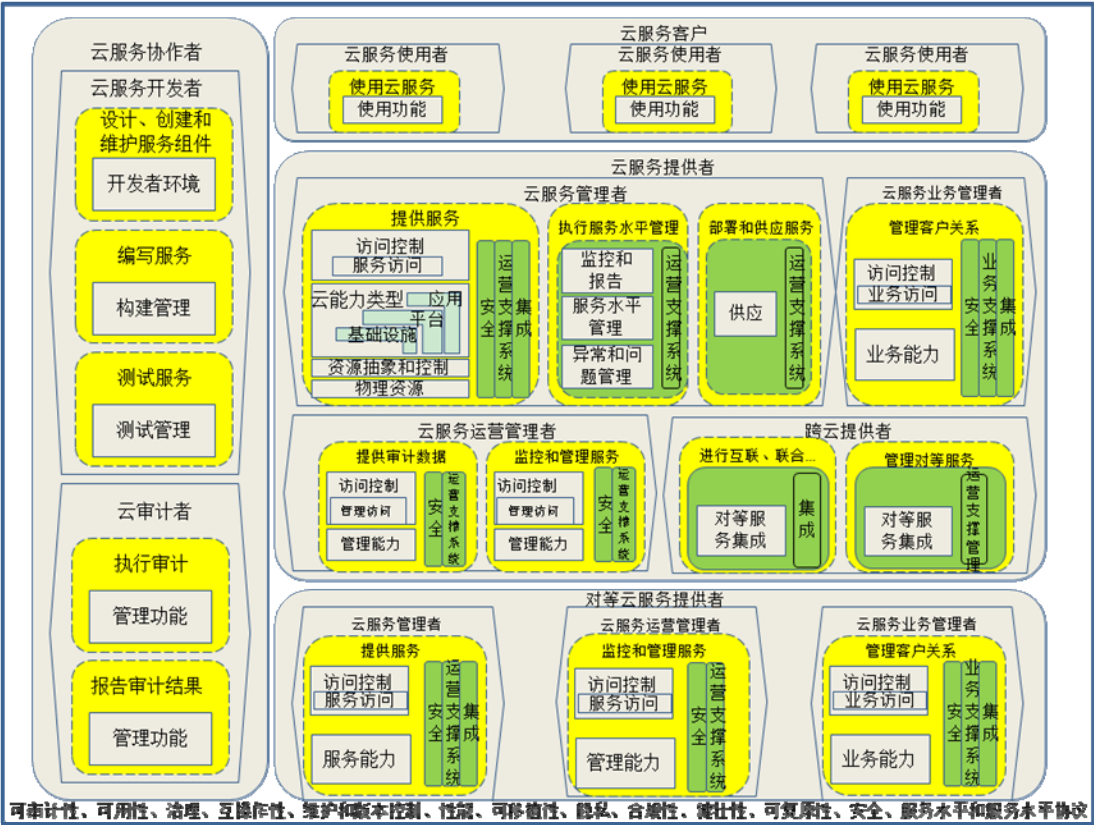


图 8 CCRA 主要元素的常用配置

图9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。

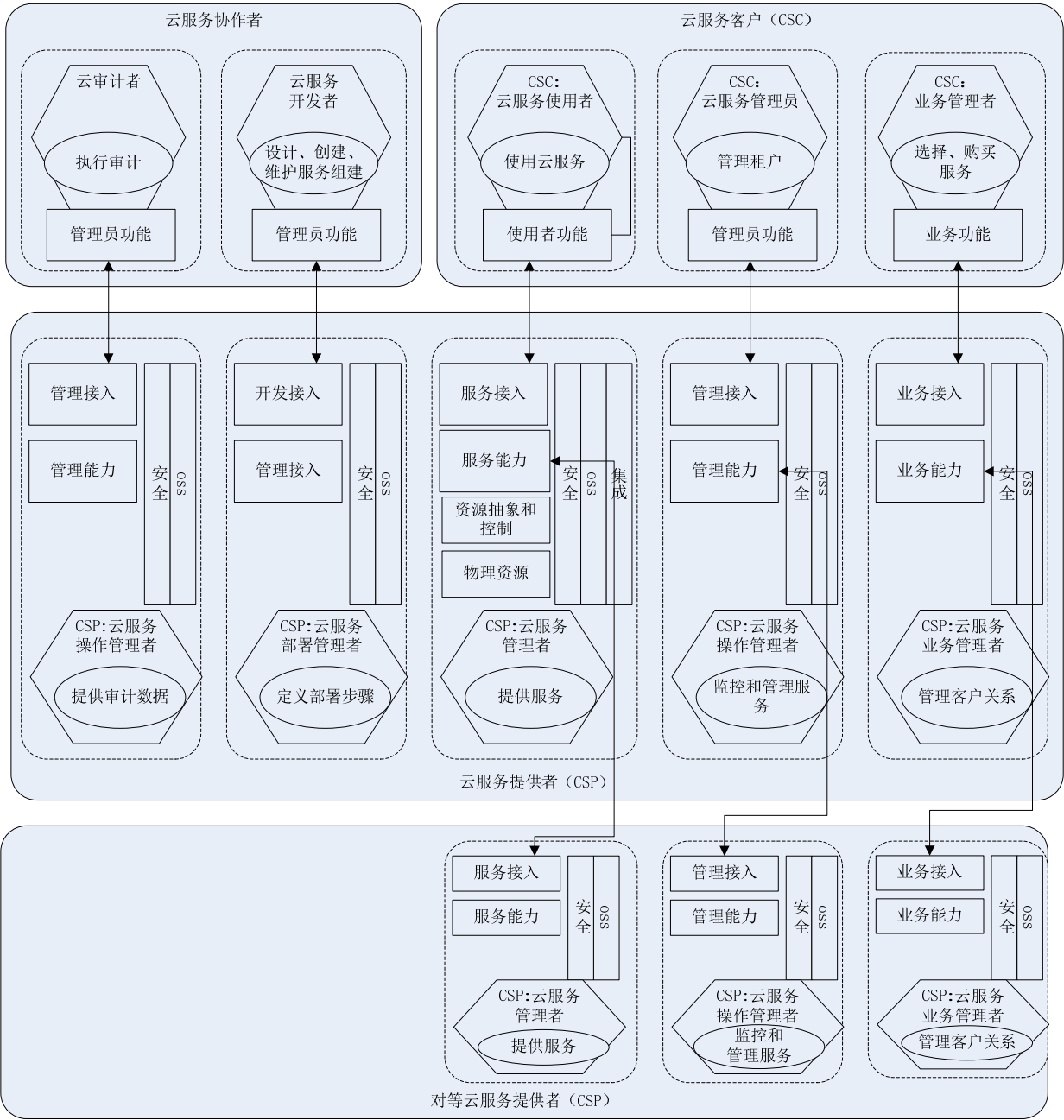


图9 活动和组件之间关系和交换示例

三、云计算支撑技术分析

通过对云计算参考架构中不同角色、不同功能的分析，我们总结出云计算的 7 类主要支撑技术，下面分别阐述这 7 类技术。

1、系统虚拟化

系统虚拟化是指将一台物理计算机系统虚拟化为一台或多台虚拟计算机系统。每个虚拟计算机系统（简称虚拟机）都拥有自己的虚拟硬件（如 CPU、内存和设备等），来提供一个独立的虚拟机执行环境。通过虚拟化层的模拟，虚拟机中的操作系统认为自己仍然是独占一个系统在运行。每个虚拟机中的操作系统可以完全不同，并且它们的执行环境是完全独立的。这个虚拟化层被称为虚拟机监控器（Virtual Machine Monitor，简称 VMM）。系统虚拟化的体系结构如图 10 所示。

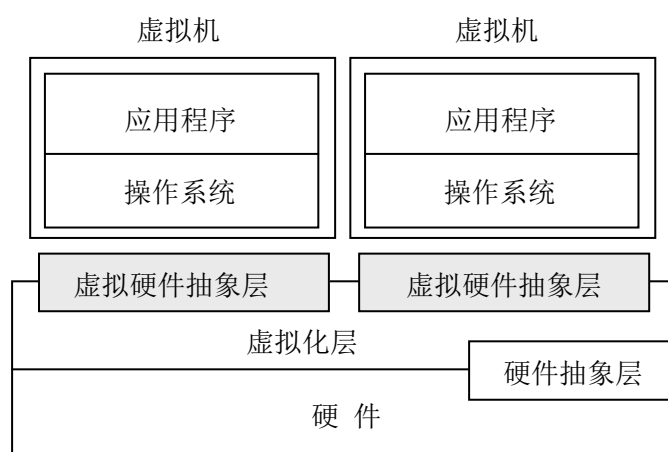


图 10 系统虚拟化体系结构图

虚拟机可以看作是物理机的一种高效隔离的复制。虚拟机具有三个典型特征：同质、高效和资源受控。同质指的是虚拟机运行环境和物理机环境在本质上需求是相同的，但是在表现上有一些差异。高效指的是虚拟机中运行的软件需要具有接近在物理机上直接运行的性能。资源受控指的是 VMM 需要对系统资源有完全控制能力和管理权限，包括资源的分配、监控和回收。

VMM 对物理资源的虚拟可以归结为三个主要任务：CPU 虚拟化、内存虚拟化和 I/O 虚拟化。CPU 虚拟化是 VMM 中最核心的部分，决定了内存虚拟化和 I/O 虚拟化的正确实现。CPU 虚拟化包括指令的模拟、中断和异常的模拟及注入和对称多处理器技术的模拟。内存虚拟化一方面解决了 VMM 和客户机操作系统对物理内存认识上的差异，另一方面在虚拟机之间、虚拟机和 VMM 之间进行隔离，防止某个虚拟机内部的活动影响到其他的虚拟机甚至是 VMM 本身，从而造成安全上的漏洞。I/O 虚拟化主要是为了满足多个客户机操作系统对外围设备的访问

需求，通过访问截获、设备模拟和设备共享等方式复用外设。

按照 VMM 提供的虚拟平台类型可以将 VMM 分为两类：完全虚拟化和半虚拟化。完全虚拟化下，VMM 虚拟的是现实存在的平台。在客户机操作系统看来，虚拟的平台和现实的平台是一样的，客户机操作系统觉察不到运行在一个虚拟平台上。这样的虚拟平台无需对现有的操作系统做任何修改。半虚拟化下，VMM 虚拟的平台在现实中是不存在的。这样的虚拟平台需要对客户机操作系统进行修改使之适应虚拟环境。操作系统知道自己运行在虚拟平台上，并且会主动去适应。

当前主流的虚拟化技术实现结构可以分为三类：Hypervisor 模型、宿主模型和混合模型。在 Hypervisor 模型中，VMM 可以看作是一个扩充了虚拟化功能的操作系统，对底层硬件提供物理资源的管理功能，对上层的客户机操作系统提供虚拟环境的创建和管理功能。与 Hypervisor 不同，宿主模型中，VMM 作为宿主操作系统独立的内核模块。物理资源由宿主机操作系统管理，VMM 提供虚拟化管理。宿主模型和 Hypervisor 模型的优缺点恰好相反。宿主模型的最大优点是可以充分利用现有操作系统的设备驱动程序以及其它功能，缺点是虚拟化效率较低，安全性取决于宿主操作系统。而 Hypervisor 模型虚拟化效率高、安全，但是需要自行开发设备驱动和其它一些功能。混合模型集成了上述两类模型的优点。混合模型中，VMM 让出大部分 I/O 设备的控制权，将它们交由一个运行在特权虚拟机中的特权操作系统来控制。因此，混合模型下 CPU 和内存的虚拟化由 VMM 负责，而 I/O 虚拟化由 VMM 和特权操作系统共同合作完成。

2、虚拟化资源管理

虚拟化资源是云计算中最重要的组成部分之一，对虚拟化资源的管理水平直接影响云计算的可用性、可靠性和安全性。虚拟化资源管理主要包括对虚拟化资源的监控、分配和调度。

云资源池中应用的需求不断改变，在线服务的请求经常不可预测，这种动态的环境要求云计算的数据中心或计算中心能够对各类资源进行灵活、快速、动态的按需调度。云计算中的虚拟化资源与以往的网络资源相比，有以下特征：

- (1) 数量更为巨大；

- (2) 分布更为离散;
- (3) 调度更为频繁;
- (4) 安全性要求更高。

通过对虚拟化资源的特征分析以及目前网络资源管理的现状，确定虚拟化资源的管理应该满足以下准则：

- (1) 所有虚拟化资源都是可监控和可管理的；
- (2) 请求的参数是可监控的，监控结果可以被证实；
- (3) 通过网络标签可以对虚拟化资源进行分配和调度；
- (4) 资源能高效地按需提供服务；
- (5) 资源具有更高的安全性。

在虚拟化资源管理调度接口方面，表述性状态转移（Representational State Transfer，简称 REST）有能力成为虚拟化资源管理强有力的支撑。REST 实际上就是各种规范的集合，包括 Http 协议、客户端/服务器模式等。在原有规范的基础上增加新的规范，就会形成新的体系结构。而 REST 正是这样一种体系结构，它结合了一系列的规范形成了一种新的基于 Web 的体系结构，使其更有能力来支撑云计算中虚拟化资源对管理的需求。

3、分布式数据存储

分布式数据存储技术包含非结构化数据存储和结构化数据存储。其中，非结构化数据存储主要采用文件存储和对象存储技术，而结构化数据存储主要采用分布式数据库技术，特别是 NoSQL 数据库。下面分别阐述这三方面的技术：

(1) 分布式文件系统

为了存储和管理云计算中的海量数据，Google 提出分布式文件系统 GFS（Google File System）。GFS 成为分布式文件系统的典型案例。Apache Hadoop 项目的 HDFS 实现了 GFS 的开源版本。

Google GFS 是一个大规模分布式文件存储系统，但是和传统分布式文件存储系统不同的是，GFS 在设计之初就考虑到云计算环境的典型特点：结点由廉价不可靠 PC 构建，因而硬件失败是一种常态而非特例；数据规模很大，因而相应的文件 I/O 单位要重新设计；大部分数据更新操作为数据追加，如何提高数据

追加的性能成为性能优化的关键。相应的 GFS 在设计上有以下特点：

- 利用多副本自动复制技术，用软件的可靠性来弥补硬件可靠性的不足。
- 将元数据和用户数据分开，用单点或少量的元数据服务器进行元数据管理，大量的用户数据结点存储分块的用户数据，规模可以达到 PB 级。
- 面向一次写多次读的数据处理应用，将存储与计算结合在一起，利用分布式文件系统中数据的位置相关性进行高效的并行计算。

GFS/HDFS 非常适于进行以大文件形式存储的海量数据的并行处理，但是，当文件系统的文件数量持续上升时，元数据服务器的可扩展性面临极限。以 HDFS 为例，只能支持千万级的文件数量，如果用于存储互联网应用的小文件则有困难。在这种应用场景面前，分布式对象存储系统更为有效。

（2）分布式对象存储系统

与分布式文件系统不同，分布式对象存储系统不包含树状名称空间（Namespace），因此在数量增长时可以更有效地将元数据平衡地分布到多个结点上，提供理论上无限的可扩展性。

对象存储系统是传统的块设备的延伸，具有更高的“智能”：上层通过对象 ID 来访问对象，而不需要了解对象的具体空间分布情况。相对于分布式文件系统，在支撑互联网服务时，对象存储系统具有如下优势：

- 相对于文件系统的复杂 API，分布式对象存储系统仅提供基于对象的创建、读取、更新、删除的简单接口，在使用时更方便而且语义没有歧义。
- 对象分布在一个平坦的空间中，而非文件系统那样的名称空间之中，这提供了很大的管理灵活性：既可以在所有对象之上构建树状逻辑结构；也可以直接用平坦的空间；还可以只在部分对象之上构建树状逻辑结构；甚至可以在同一组对象之上构建多个名称空间。

Amazon 的 S3 就属于对象存储服务。S3 通过基于 Http REST 的接口进行数据访问，按照用量和流量进行计费，其他的云服务商也都提供了类似的接口服务。很多互联网服务商，如 Facebook 等也都构建了对象存储系统，用于存储图片、照片等小型文件。

（3）分布式数据库管理系统

传统的单机数据库采用“向上扩展”的思路来解决计算能力和存储能力的

问题，即增加 CPU 处理能力、内存和磁盘数量。这种系统目前最大能够支持几个 TB 数据的存储和处理，远不能满足实际需求。采用集群设计的分布式数据库逐步成为主流。传统的集群数据库的解决方案大体分为以下两类：

- Share-Everything (Share-Something)。数据库结点之间共享资源，例如磁盘、缓存等。当结点数量增大时，结点之间的通信将成为瓶颈；而且处理各个结点对数据的访问控制也为事务处理带来麻烦。
- Share-Nothing。所有的数据库服务器之间并不共享任何信息。当任意一个结点接到查询任务时，都会将任务分解到其他所有的结点上面，每个结点单独处理并返回结果。但由于每个结点容纳的数据和规模并不相同，因此如何保证一个查询能够被均衡地分配到集群中成为一个关键问题。同时，结点在运算时可能从其他结点获取数据，这同样也延长了数据处理时间。在处理数据更新请求时，Share-Nothing 数据库需要保证多结点的数据一致性，需要快速准确定位到数据所在结点。

云计算环境下，大部分应用不需要支持完整的 SQL 语义，而只需要 Key-Value 形式或略复杂的查询语义。在这样的背景下，进一步简化的各种 NoSQL 数据库成为云计算中的结构化数据存储的重要技术。

Google 的 BigTable 是一个典型的分布式结构化数据存储系统。在表中，数据是以“列族”为单位组织的，列族用一个单一的键值作为索引，通过这个键值，数据和对数据的操作都可以被分布到多个结点上进行。

在开源社区中，Apache HBase 使用了和 BigTable 类似的结构，基于 Hadoop 平台提供 BigTable 的数据模型，而 Cassandra 则采用了亚马逊 Dynamo 的基于 DHT 的完全分布式结构，实现更好的可扩展性。

4、并行计算模式

并行计算模型是提高海量数据处理效率的常用方法。常用的并行计算模型主要包括两类：一类是面向高性能计算的，如 MPI (Message Passing Interface) 模型；另一类是面向互联网数据密集型应用的并行编程模型，如 Google 的 MapReduce 模型、微软的 Dryad 模型。第二类并行计算模型更适用于云计算环境。云计算下把海量数据分布到多个结点（通常是廉价不可靠的 PC 机）上，将计算

并行化，利用多机的计算资源，加快数据处理的速度。

云计算下的并行处理需要考虑以下关键问题：1) 任务划分，使得任务能更加优化的被分解和并行执行；2) 任务调度，操作尽量本地化，以保证在网络资源有限的情况下，最大程度地将计算任务在本地执行，减少通信开销；3) 自动容错处理机制，保证在结点失效的情况下处理任务仍然能够正确地执行。下面分别阐述这三方面内容。

(1) 任务划分

在 MapReduce 或 Dryad 中，数据以块的形式存储在集群的各个结点上，每个计算任务只需处理一部分数据，这样自然地实现了海量数据的并行处理。这种简单的根据存储位置进行任务划分的方式，只适用于不存在数据依赖关系的计算。而对于存在依赖关系的计算，MapReduce 将复杂的计算转化为一系列单一的 Map/Reduce 计算，串联起来完成多个 Map/Reduce 任务来实现复杂计算。转化有两者方式：手工转化和利用 Pig、Hive 等工具进行自动转化。Dryad 将存在依赖关系的复杂计算表示为一个有向无环图，利用图论对计算自动进行依赖性分析和优化，最后转化为高效的子任务执行。

(2) 任务调度

一个集群系统的存储和计算资源有两种组织方式：一是将存储和计算资源部署在相同结点上；另一种是存储和计算结点分开部署。MapReduce 和 Dryad 采用前者，MPI 采用后者。MapReduce 和 Dryad 在调度任务时认为“移动计算比移动数据更合算”，优先把计算任务调度到数据所在的结点或者就近的结点，这样在进行计算时，大部分的输入数据都能从本地读取，减少了网络带宽的消耗，提高了整个系统的吞吐量。另外，MapReduce 对于由于各种原因（例如硬盘出错）造成执行非常慢的子任务采用了备用任务的机制，当 MapReduce 操作接近完成时，调度备用任务进程来执行剩下的执行非常慢的子任务。

(3) 自动容错处理机制

常用恢复机制有两类：任务重做 (Task Re-execute) 和检查点 (Checkpoint) 回滚方式。这两种机制各有优缺点，前者实现非常简单，但是重做的代价比较大；后者实现较复杂，需要周期性地记录所有进程状态，但是恢复较快。MapReduce 和 Dryad 主要采用任务重做的方式来处理结点的失效，而 MPI 通常

采用检查点回滚的机制。

5、用户交互技术

随着云计算的逐步普及，浏览器已经不仅仅是一个客户端的软件，而逐步演变为承载着互联网的平台。浏览器与云计算的整合技术主要体现在两个方面：浏览器网络化与浏览器云服务。

国内各家浏览器都将网络化作为其功能的标配之一，主要功能体现在用户可以登录浏览器，并通过自己的帐号将个性化数据同步到服务端。用户在任何地方，只需要登录自己的帐号，就能够同步更新所有的个性内容，包括浏览器选项配置、收藏夹、网址记录、智能填表、密码保存等。

目前的浏览器云服务主要体现在 P2P 下载、视频加速等单独的客户端软件中，主要的应用研究方向包括：基于浏览器的 P2P 下载、视频加速、分布式计算、多任务协同工作等。在多任务协同工作方面，AJAX(Asynchronous JavaScript and XML，异步 JavaScript 和 XML)是一种创建交互式网页应用的网页开发技术，改变了传统网页的交互方式，改进了交互体验。

6、安全管理

安全问题是用户是否选择云计算的主要顾虑之一。传统集中式管理方式下也有安全问题，云计算的多租户、分布性、对网络和服务提供者的依赖性，为安全问题带来新的挑战。其中，主要的数据安全问题和风险包括：

（1）数据存储及访问控制

包括如何有效存储数据以避免数据丢失或损坏，如何避免数据被非法访问和篡改，如何对多租户应用进行数据隔离，如何避免数据服务被阻塞，如何确保云端退役(at rest)数据的妥善保管或销毁等等。

（2）数据传输保护

包括如何避免数据被窃取或攻击，如何保证数据在分布式应用中有效传递等。

（3）数据隐私及敏感信息保护

包括如何保护数据所有权、并可根据需要提供给受信方使用，如何将个人

身份信息及敏感数据挪到云端使用等。

（4）数据可用性

包括如何提供稳定可靠的数据服务以保证业务的持续性，如何进行有效的数据容灾及恢复等。

（5）依从性管理

包括如何保证数据服务及管理符合法律及政策的要求等。

相应的数据安全管理工作包括：

（1）数据保护及隐私（Data Protection and Privacy）

包括虚拟镜像安全、数据加密及解密、数据验证、密钥管理、数据恢复、云迁移的数据安全等。

（2）身份及访问管理（Identity and Access Management, 简称 IAM）

包括身份验证、目录服务、联邦身份鉴别/单点登陆(Single Sign on, 简称 SSO)、个人身份信息保护、安全断言置标语言、虚拟资源访问、多租用数据授权、基于角色的数据访问、云防火墙技术等。

（3）数据传输（Data Transportation）

包括传输加密及解密、密钥管理、信任管理等。

（4）可用性管理（Availability Management）

包括单点失败(Single Point of Failure, 简称 SPoF)、主机防攻击、容灾保护等。

（5）日志管理（Log Management）

包括日志系统、可用性监控、流量监控、数据完整性监控、网络入侵监控等。

（6）审计管理（Audit Management）

包括审计信任管理、审计数据加密等。

（7）依从性管理(Compliance Management)

包括确保数据存储和使用等符合相关的风险管理和安全管理的规定要求。

7、运营支撑管理

为了支持规模巨大的云计算环境，需要成千上万台服务器来支撑。如何对

数以万计的服务器进行稳定高效地运营管理，成为云服务被用户认可的关键因素之一。下面从云的部署、负载管理和监控、计量计费、服务水平协议（Service Level Agreement，简称 SLA）、能效评测这五个方面分别阐述云的运营管理。

（1）云的部署

云的部署包括两个方面：云本身的部署和应用的部署。如前所述，云一方面规模巨大，另一方面要求很好的服务健壮性、可扩展性和安全性。因此，云的部署是一个系统性的工程，涉及到机房建设、网络优化、硬件选型、软件系统开发和测试、运维等各个方面。为了保证服务的健壮性，需要将云以一定冗余部署在不同地域的若干机房。为了应对规模的不断增长，云要具备便利的、近乎无限的扩展能力，因而从数据存储层、应用业务层到接入层都需要采用相应的措施。为了保护云及其应用的安全，需要建立起各个层次的信息安全机制。除此之外，还需要部署一些辅助的子系统，如管理信息系统（MIS）、数据统计系统、安全系统、监控和计费系统等，他们帮助云的部署和运营管理达到高度自动化和智能化的程度。

云本身的部署对云的用户来说是透明的。一个设计良好的云，应使得应用的部署对用户也是透明和便利的。这依赖云提供部署工具（或 API）帮助用户自动完成应用的部署。一个完整的部署流程通常包括注册、上传、部署和发布四个过程。

（2）负载管理和监控

云的负载管理和监控是一种大规模集群的负载管理和监控技术。在单个结点粒度，它需要能够实时地监控集群中每个结点的负载状态，报告负载的异常和结点故障，对出现过载或故障的结点采取既定的预案。在集群整体粒度，通过对单个结点、单个子系统的信息进行汇总和计算，近乎实时地得到集群的整体负载和监控信息，为运维、调度和成本提供决策。与传统的集群负载管理和监控相比，云对负载管理和监控有新的要求：首先，新增了应用粒度，即以应用为粒度来汇总和计算该应用的负载和监控信息，并以应用为粒度进行负载管理。应用粒度是可以再细分的，在下面的“计量计费”一节中会提到，粒度甚至精细到 API 调用的粒度。其次，监控信息的展示和查询现在要作为一项服务提供给用户，而不仅仅是少量的专业集群运维人员，这需要高性能的数据流分

析处理平台的支持。

（3）计量计费

云的主要商业运营模式是采取按量计费的收费方式，即便对于私有云，其运营企业或组织也可能有按不同成本中心进行成本核算的需求。为了精确的度量“用了多少”，就需要准确的、及时的计算云上的每一个应用服务使用了多少资源，这称为服务计量。

服务计量是一个云的支撑子系统，它独立于具体的应用服务，像监控一样能够在后台自动地统计和计算每一个应用在一定时间点的资源使用情况。对于资源的衡量维度主要是：应用的上行(in)/下行(out)流量、外部请求响应次数、执行请求所花费的 CPU 时间、临时和永久数据存储所占据的存储空间、内部服务 API 调用次数等。也可认为，任何应用使用或消耗的云的资源，只要可以被准确的量化，就可以作为一种维度来计量。实践中，计量通常既可以用单位时间内资源使用的多少来衡量，如每天多少字节流量；也可以用累积的总使用量来衡量，如数据所占用的存储空间字节大小。

在计量的基础上，选取若干合适的维度组合，制定相应的计费策略，就能够进行计费。计费子系统将计量子系统的输出作为输入，并将计费结果写入帐号子系统的财务信息相关模块，完成计费。计费子系统还产生可供审计和查询的计费数据。

（4）SLA

SLA 是在一定开销下为保障服务的性能和可靠性，服务提供商与用户间定义的一种双方认可的协定。对于云服务而言，SLA 是必不可缺的，因为用户对云服务的性能和可靠性有不同的要求。从用户的角度而言，也需要从云服务提供商处得到具有法律效力的承诺，来保证支付费用之后得到应有的服务质量。从目前的实践看，国外的大型云服务提供商均提供了 SLA。

一个完整的 SLA 同时也是一个具有法律效力的合同文件，它包括所涉及的当事人、协定条款、违约的处罚、费用和仲裁机构等。当事人通常是云服务提供商与用户。协定条款包含对服务质量的定义和承诺。服务质量一般包括性能、稳定性等指标，如月均稳定性指标、响应时间、故障解决时间等。实际上，SLA 的保障是以一系列服务水平目标（Service Level Object，简称 SLO）的形式定

义的。SLO 是一个或多个有限定的服务组件的测量的组合。一个 SLO 被实现是指那些有限定的组件的测量值在限定范围里。通过前述的对云及应用的监控和计量，可以计算哪些 SLO 被实现或未被实现，如果一个 SLO 未被实现，即 SLA 的承诺未能履行，就可以按照“违约的处罚”对当事人（一般是云服务提供商）进行处罚。通常采取的方法是减免用户已缴纳或将缴纳的费用。

（5）能效评测

云计算提出的初衷是将资源和数据尽可能放在云中，通过资源共享、虚拟化技术和按需使用的方式提高资源利用率，降低能源消耗。但是在实际应用中，大型数据中心的散热问题造成了大量的能源消耗。如何有效降低能源消耗构建绿色数据中心成为云服务提供商迫切需要解决的问题之一。

云计算数据中心的能耗测试评价按照不同的维度有不同测试手段和方法。针对传统的数据中心它有显性评价体系和隐性评价体系两个方面。

显性的能耗测试评价可以参照传统数据中心的评价体系，具体包括：能源效率指标、IT 设备的能效比、IT 设备的工作温度和湿度范围、机房基础设施的利用率指标。能源效率指标用于评估一个数据中心使用的能源中有多少用于生产，还有多少被浪费。在这方面，绿色网格组织的电能利用率（Power Usage Effectiveness，简称 PUE）指标影响力较大。PUE 值越小，意味着机房的节能性越好。目前，国内绝大多数的数据中心 PUE 值为 3 左右，而欧美一些国家数据中心的 PUE 平均值为 2 左右。

隐性能耗测试评价包括云计算服务模式节省了多少社会资源，由于客户需求的不同，云吞吐量的变化节省了多少 IT 设备的投资和资源的重复建设。这些的测试评价很多时候是不能量化或者不能够进行精准地评价。

为了实现对数据中心能源的自动调节，满足相关的节能要求，一些 IT 厂商和标准化组织纷纷推出节能技术及能耗检测工具，如惠普公司的动态功率调整技术（Dynamic Power Saver，简称 DPS）、IBM 的 Provisioning 软件。

四、云计算应用情况分析

（一）国际云计算应用情况分析

当今世界，在经济全球化不断发展的同时，气候变化、能源安全、粮食安全等全球性问题更加突出，以知识技术密集、绿色低碳增长为主要特征的新兴产业蓬勃兴起，日益成为引领新一轮产业革命的主导力量。为应对新挑战、构建新优势，世界主要国家紧紧抓住新兴产业发展机遇，竞相出台发展战略，加大政府扶持力度，抢占经济科技发展制高点。

从 2009 年起，各国都在加快部署、纷纷出台战略规划和相关政策措施（如表 2 所示）、积极推动云计算产业发展和应用，以期在全球经济与竞争格局深刻变革之中占据最大优势。

表 2 国外主要国家/区域的云计算发展战略

政府的角色	典型	计划/项目	主要出发点
政府采购型	美国	联邦计算战略	1、云优先采用 2、节约政府财政预算 3、借助云计算提升政府公众服务能力
政府推动型	欧盟	RESERVOIR FR7	1、突破资源和服务虚拟化障碍 2、建立统一的云计算代码和架构规范 3、实现跨域工作均衡
	日本	智能云计算战略	1、提升 IT 技术更为广泛的应用 2、突破企业和行业边界，实现整个社会范围内的信息共享 3、建立知识信息社会，提升日本国际竞争力
	韩国		1、引导韩国的经济增长和增强韩国在国际技术标准等方面的影响力

上述国家或区域均制定了战略规划，明确了云计算发展方向和应用重点，明确了云计算政府管理机构；加大了资金投入、扶持和引导产业快速发展，支持技术创新、开展关键技术研发；同时，政府率先垂范、开展云计算应用示范

项目，并积极推动标准研制、规范应用和市场发展。

根据两家国际知名机构对未来市场的预测，云计算市场前景广阔，具体预测数据如下：

- 1、Gartner 预测 2017 年全球广义云服务市场高达 2442 亿美元，未来几年内会继续保持 15%以上的增长。
- 2、IDC 预测 2014 年，企业在云计算领域的支出将达到 1000 亿美元，增加 25%，其中包括云服务提供商为跟上用户需求而需要购买的相关硬件产品。

同时，以 I/P/S（IaaS, PaaS, SaaS）为代表的市场在 2013 年也达到了 333 亿美元，增长高达 29.7%。可以看出，云计算被大家一致看好，目前，IT 领域因受几大新型技术的影响，正逐渐转型过渡，云计算是 IT 转型过渡的主要推动力，其迅速发展对全球电子信息领域的软硬件产业产生重要影响，基于云的服务模式和解决方案已成为主流 IT 服务模式，众多的服务器、存储硬件厂商以及平台软件厂商都希望通过云计算平台将产品推广出去，以便未来能获得更多的市场机会。国际上许多研发公司已经将云计算作为战略核心并实施和部署。同时，云计算运营商也在这次大潮中实现跨越式发展。从而开创一种全新的 IT 应用前景。

目前几乎所有的国际主流 IT 企业都已参与云计算领域，各公司根据自己的传统技术领域和市场策略从各个方向进军云计算。不同企业凭借不同的技术背景，将以前的产品和技术中的云计算特征挖掘出来，如软件的虚拟化、分布式存储系统，提出自己的云计算产品线。国际主流公司有实力参与 IaaS 的竞争，获得垄断地位，而中小企业很难参与。PaaS 发展潜力巨大，年复合增长率高，是未来云计算产业链的关键环节。目前国际各大厂商都在积极构建和推广自己的 PaaS，以期在云计算产业链中占据有利地位。SaaS 市场规模最大，利润空间最大。基于 PaaS 进行各种服务、内容和应用的开发、运营和销售是 SaaS 的发展趋势。传统软件巨头也已开始进入 SaaS 领域。现在的云计算方案日趋成熟，在医疗、交通、电子商务、社交媒体等领域都有了成功应用。表 3 所示为每一层次上对应的一些典型国际云计算服务。

表 3 典型国际云计算服务

层次	典型云计算服务
SaaS	Google Apps、Salesforce CRM 等
PaaS	Google App Engine、force.com、Microsoft Azure 等
IaaS	Amazon EC2、Amazon S3、Rackspace cloudserver 等

表 3 列举的只是一些典型的国际云计算服务。实际上，越来越多的 IT 企业都将自己的传统业务逐渐转移到云计算平台上。目前国际上云计算产业在 IaaS，SaaS 领域已经有相对完善的服务，并得到了企业的认可，然而由于 PaaS 的特殊性其仍处于起步阶段，但也有很大的发展空间。

（二）国内云计算应用情况分析

“十二五”期间，我国将重点推进云计算技术研发的产业化，组织开展云计算应用试点示范，着力完善产业发展环境，我国已将云计算列为新一代信息技术产业的重点领域，并出台了一系列规划和政策措施给予支持。具体措施包括，加快云计算技术研发的产业化，组织开展云计算应用试点示范，着力完善产业发展环境等。

从产业支持上看，国家发改委、工信部、财政部等部委带头扶持云计算产业发展。2011 年，国家发改委和工信部已联合发文在北京、上海、深圳、杭州、无锡 5 个城市开展云计算服务创新应用试点示范。财政部表示，要积极探索云计算等新型业态的政府采购工作，不断拓展服务类采购领域，国内各地方政府与企业已经开始尝试合作，将云计算纳入地方政府采购目录。

在工信部的调查中显示，2013 年我国公有云服务市场约为 47.6 亿元人民币，增长率达 36%，有 8% 受访企业已经开始了云计算应用，其中公有云服务占 29.1%，私有云占 2.9%，混合云占 6%，更有 76.8% 的受访者表示会将更多的业务迁移至云环境，国内企业对云计算的认知和采用逐年提升。

国内云计算业务比较领先的企业也多从 IaaS 切入，这其中既有互联网原生企业，也有 IT/ICT 企业及电信运营商。虽然大家都在做云计算，却因为企业性

质不同导致切入口不同：虽然都是做云计算，但是ICT企业和原生互联网公司逐渐分化出了不同的发展策略和方向，形成了两股不同的力量。

PaaS领域，国内和国际情况类似，已取得了长足的发展，但是相对其它两个领域仍然处于弱势，虽然包括腾讯、百度、新浪、阿里云等各大云提供商都已发布PaaS服务，但所占的市场份额却并不大，提升缓慢。

SaaS可以说是当下国内最成熟的云服务，可以说是繁花似锦。八百客、金蝶、用友、云知声等企业已形成稳固的市场格局，部分公司的云服务营业额超过1亿元人民币。

表 4 所示为一些典型的国内云计算服务。

表 4 典型国内云计算服务

层次	典型云计算服务
SaaS	电子商务云、中小企业云、医疗云、教育云等
PaaS	APP 开发环境、APP 测试环境、应用引擎等
IaaS	虚拟机租用服务、存储服务、负载均衡服务、防火墙服务等

国内云计算主要集中在 SaaS 层，PaaS 和 IaaS 的服务还在不断发展中。

我国云计算的市场发展空间巨大，也将对我国的互联网产业、软件和服务产业以及通信产业的发展产生较大的影响。在当前情况下，云计算产业能否在我国得到健康快速的发展是从政策层面到市场层面都需要重视的一个问题。

（三）云计算面临的挑战

一方面，云计算的引入可以帮助用户，尤其是中小企业提高资源利用率、降低 IT 成本；另一方面，云计算还处于不断发展阶段，要实现云计算真正的产业化还面临以下挑战：

- 1、缺乏统一的技术标准。目前，资源层的接口标准已经成型，数据层和应用层的接口标准还将进一步加快研制；当前的云计算环境下，互操作和数据的可移植性成为广泛关注的问题，迫切需开展互操作和可移植、以及数据和跨设备与云服务的数据流动等方面的标准研究。

- 2、缺乏统一的运营服务标准。运营服务标准包括计量计费、评价服务质量、服务管理等等。可测量的服务是云计算的六大特征之一，然而随着云计算服务提供多种多样，产业链逐渐成熟，如何对不同服务提供商提供的云服务进行统一的计量计费，是政府采购，用户购买时的必要参考因素，没有可度量的标准，这对云计算产业的良性发展有很大的有阻碍。同时，如何定义和评价服务质量、如何对服务进行统一的部署，这些用户十分关注的问题目前还没有统一的标准。
- 3、服务的可用性问题。如何保证在出现网络故障、服务器故障、软件异常等情况下服务的可用性成为云服务提供商的头等大事。
- 4、运营管理问题。云计算下，用户的干预少、工作负载变化幅度大、共享设备多种多样、数据量大且增长迅速，如何保证动态环境下数据处理的效率和易管理性，对基于动态自调优的云管理提出很大挑战。
- 5、能效管理问题。云计算时代的大型数据中心其能耗是惊人的。构建大型的计算中心和数据中心不可避免地存在着能耗高问题。如何有效地降低能耗，构建绿色计算中心和数据中心成为服务提供商急待解决的问题之一。同时，如何选址，如何为数据中心提供足够的能源以维持数据中心正常的运转是必须要考虑的问题。
- 6、信用和安全问题。云计算时代，用户需要把自己的所有信息放到云计算提供商的服务器中，这就意味着用户无法掌控服务器数据的生命周期，那么能不能够保证用户的数据隐私和安全，是云计算提供商面临的一个巨大挑战。云安全包括数据的安全性、隐私问题、身份鉴别等方面。和传统应用不同，云计算下数据保存在云中，这对数据的访问控制、存储安全、传输安全和审计都带来极大的挑战。在身份鉴别方面还需要解决跨云的身份鉴别问题。
- 7、海量数据的产生。随着云计算的布局，计算量越来越大、数据越来越多、越来越动态，带来的海量数据中含有大量隐含信息，如何如何处理这些数据，挖掘出数据内的隐藏价值是云产业下一步应该考虑的问题。

此外，云计算的日益普及还给网络带宽带来了严峻考验。对此，一方面需要加强网络自身建设，另一方面，也对用户交互技术提出了挑战。

五、国际云计算标准化工作

（一）国际云计算标准化工作概述

2008 年来，云计算在国际上已成为标准化工作热点之一。国际上共有 33 个标准化组织和协会从各个角度在开展云计算标准化工作。这 33 个国外标准化组织和协会既有知名的标准化组织，如 ISO/IEC JTC1 SC27、DMTF，也有新兴的标准化组织，如 ISO/IEC JTC1 SC38、CSA；既有国际标准化组织，如 ISO/IEC JTC1 SC38、ITU-T SG13，也有区域性标准化组织，如 ENISA；既有基于现有工作开展云标准研制的，如 DMTF、SNIA；也有专门开展云计算标准研制的，如 CSA、CSCC。按照标准化组织的覆盖范围对 33 个标准化组织进行分类，结果如表 5 所示。

表 5 33 个国外标准化组织和协会分布表

序号	标准组织和协会	个数	覆盖范围
1.	ISO/IEC JTC1 SC7、SC27、SC38、SC39、ITU-T SG13	5	国际标准化组织
2.	DMTF、CSA、OGF、SNIA、OCC、OASIS、TOG、ARTS、IEEE、CCIF、OCM、Cloud use case、A6、OMG、IETF、TM Forum、ATIS、ODCA、CSCC	19	国际标准化协会
3.	ETSI、Eurocloud、ENISA	3	欧洲
4.	GICTF、ACCA、CCF、KCSA、CSRT	5	亚洲
5.	NIST	1	美洲

从表 5 的部分国际标准化组织云计算标准制定动态图中可以了解到，除了国际标准化组织和区域性标准化组织大力参与云计算标准化工作外，国际标准化协会日益成为云计算标准化工作的生力军。总的来说，目前参与云计算标准化工作的国外标准化组织和协会呈现以下特点：

（一）三大国际标准化组织从多角度开展云计算标准化工作

三大国际标准化组织 ISO、IEC 和 ITU 的云计算标准化工作开展方式大致分为两类：一类是已有的分技术委员会，如 ISO/IEC JTC1 SC7（软件和系统工程）、

ISO/IEC JTC1 SC27（信息技术安全），在原有标准化工作的基础上逐步渗透到云计算领域；另一类是新成立的分技术委员会如 ISO/IEC JTC1 SC38（分布式应用平台和服务）、ISO/IEC JTC1 SC39（信息技术可持续发展）和 ITU-T SG13（原 ITU-T FGCC 云计算焦点组），开展云计算领域新兴标准的研制。

（二）知名标准化组织和协会积极开展云计算标准研制

知名标准化组织和协会，包括 DMTF、SNIA、OASIS 等，在其已有标准化工作的基础上，纷纷开展云计算标准工作研制。其中，DMTF 主要关注虚拟资源管理，SNIA 主要关注云存储，OASIS 主要关注云安全和 PaaS 层标准化工作。截止 2014 年 1 月，DMTF 的 OVF（开放虚拟化格式规范）和 SNIA 的 CDMI（云数据管理接口规范）均已通过 PAS 通道提交给 ISO/IEC JTC1，正式成为 ISO 国际标准。

（三）新兴标准化组织和协会有序推动云计算标准研制

新兴标准化组织和协会，包括 CSA、CSCC、Cloud Use Case 等，正有序开展云计算标准化工作。这些新兴的标准化组织和协会，常常从某一方面入手，开展云计算标准研制，例如，CSA 主要关注云安全标准研制，CSCC 主要从客户使用云服务的角度开展标准研制。

（二）国际云计算标准化工作分析

国外标准化组织和协会纷纷开展云计算标准化工作，从早期的标准化需求收集和分析，到云计算词汇和参考架构等通用和基础类标准研制，从计算资源和数据资源的访问和管理等 IaaS 层标准的研制，到应用程序部署和管理等 PaaS 层标准的研制，从云安全管理标准的研制，到云客户如何采购和使用云服务，云计算标准化工作取得了实质性进展。

总的来说，33 个标准化组织和协会的云计算标准化工作分类情况如表 6 所示。

表 6 33 个标准化组织和协会关注点分析

关注点		相关标准组织
应用场景和案例分析		ISO/IEC JTC1、ITU-T、Cloud Use Case 等
通用和基础		ISO/IEC JTC1、ITU-T、ETSI、NIST、ITU-T、TOG 等
互操作&	虚拟资源管理	ISO/IEC JTC1、DMTF、SNIA、OGF 等

可移植	数据存储与管理	SNIA、DMTF 等
	应用移植与部署	OASIS、DMTF、CSCC 等
服务		ISO/IEC JTC1、DMTF、GICTF 等
安全		ISO/IEC JTC1、ITU-T、CSA、NIST、OASIS、ENISA 等

目前，云计算国际标准化工作从前期的标准化需求收集分析，到案例和场景的归类分析，逐步深入，在基础标准、互操作和可移植标准方面已经取得一些实质性进展。本报告详细梳理了 33 个标准化组织和协会的工作成果（参见附录二）。

通过对 33 个标准化组织和协会的输出物进行分析，我们发现这些输出物集中在以下 5 个方面：应用场景和案例分析、通用和基础标准、互操作和可移植标准、服务标准、安全标准。下面分别阐述这 5 个方面。

——应用场景和案例分析

ISO/IEC JTC1 SC38、ITU-T FGCC（云计算焦点组，后转换成 SG13）、Cloud Use Case 等多个组织纷纷开展云计算应用场景和案例分析。其中，SC38 将用户案例和场景分析文档作为其常设文件。该文件对目前已有的案例和场景从 IaaS、PaaS 等角度进行了分类和总结，并分析提出：目前案例主要集中在云运营以及提供商和消费者交互之间；尽管安全是一个非常重要的因素，目前没有一个安全用例；另外有关提供商和消费者之间的管理系统的集成、云服务中内部系统的集成等方面的案例目前缺少。目前，SC38 将基于用户案例和场景分析的方法作为评估新工作项目是否合理的方法之一。随着云服务的逐步应用推广，正在进行相应的用户案例和应用场景的补充和完善工作。

——通用和基础标准

云计算通用和基础标准旨在对云计算一些基础共性的标准进行制定，包括云计算术语、云计算基本参考模型、云计算标准化指南等。ISO/IEC JTC1 SC38 和 ITU-T SG13 通过成立联合工作组（CT）的方式开展云计算术语和云计算参考架构 2 项标准的研制。其中，云计算术语主要包括云计算涉及到的基本的术语，用于在云计算领域交流规范用语、明晰概念。云计算基本参考架构主要描述云计算的利益相关者群体，明确基本的云计算活动和组件，描述云计算活动和组件之间以及他们与环境之间的关系，为定义云计算标准提供一个技术中立的参

考点。

——互操作和可移植标准

互操作和可移植标准主要针对云计算中用户最为关心的资源按需供应、数据锁定和供应商锁定、分布式海量数据存储和管理等问题，以构建互连互通、高效稳定的云计算环境为目标，对基础架构层、平台层和应用层的核心技术和产品进行规范。目前，以 DMTF、SNIA 为代表的标准化组织和协会纷纷开展 IaaS 层标准化工作，OASIS 开展了 PaaS 层标准化工作。其中，OVF、CDMI 已经成为国际标准，VMAN、CIMI 正在进行国际标准的投票工作。

——服务标准

服务标准主要针对云服务生命周期管理的各个阶段，覆盖服务交付、服务水平协议、服务计量、服务质量、服务运维和运营、服务管理、服务采购，包括云服务通用要求、云服务级别协议规范、云服务质量评价指南、云运维服务规范、云服务采购规范等。目前，ISO/IEC JTC1 SC38、NIST、CSCC 等组织和协会正在开展云服务水平协议（SLA）相关的标准研制，已有 1 项标准处于国际标准草案阶段。

——安全标准

安全标准方面主要关注数据的存储安全和传输安全、跨云的身份鉴别、访问控制、安全审计等方面。目前 ISO/IEC JTC1 SC27、CSA、ENISA、CSCC 从多个方面开展云安全标准与指南编制工作，已有 3 项云安全国际标准处于委员会草案（CD）和国际标准草案（DIS）阶段。

六、国内云计算标准化工作

（一）国内云计算标准化工作概述

标准是云计算发挥其价值的必要基础，云计算标准化工作是推动我国云计算技术、产业及应用发展，以及行业信息化建设的重要基础性工作之一。云计算相关的标准化工作自 2008 年底开始被科研机构、行业协会及企业关注，云计算相关的联盟及标准组织在全国范围内迅速发展。总体而言，我国的云计算标准化工作从起步阶段进入了切实推进的快速发展阶段。

2013年8月，工业和信息化部组织国内产、学、研、用各界专家代表，开展了云计算综合标准化体系建设工作，对我国云计算标准化工作进行战略规划和整体布局，并梳理出我国云计算生态系统。全国信息技术标准化技术委员会云计算标准工作组，做为我国专门从事云计算领域标准化工作的技术组织，负责云计算领域的基础、技术、产品、测评、服务、系统和设备等国家标准的制修订工作，形成了领域全面覆盖、技术深入发展的标准研究格局，为规范我国云计算产业发展奠定了标准基础。

另一方面，我国也积极参与云计算国际标准化工作，在国际舞台发挥了重要的作用，当前我国的云计算标准化工作应注重国际国内协同开展；并且在前期云计算标准研究成果基础之上，注重标准落地应用，同时结合当今云计算产业发展需求，锁定产业急需，开展一系列重点领域的标准化预研工作。

（二）云计算标准体系

针对目前云计算发展现状，结合用户需求、国内外云计算应用情况和技术发展情况，同时按照工信部对我国云计算标准化工作的综合布局，建议我国云计算标准体系建设从“基础”、“网络”、“整机装备”、“软件”、“服务”、“安全”和“其它”7个部分展开，体系框架如图11所示。

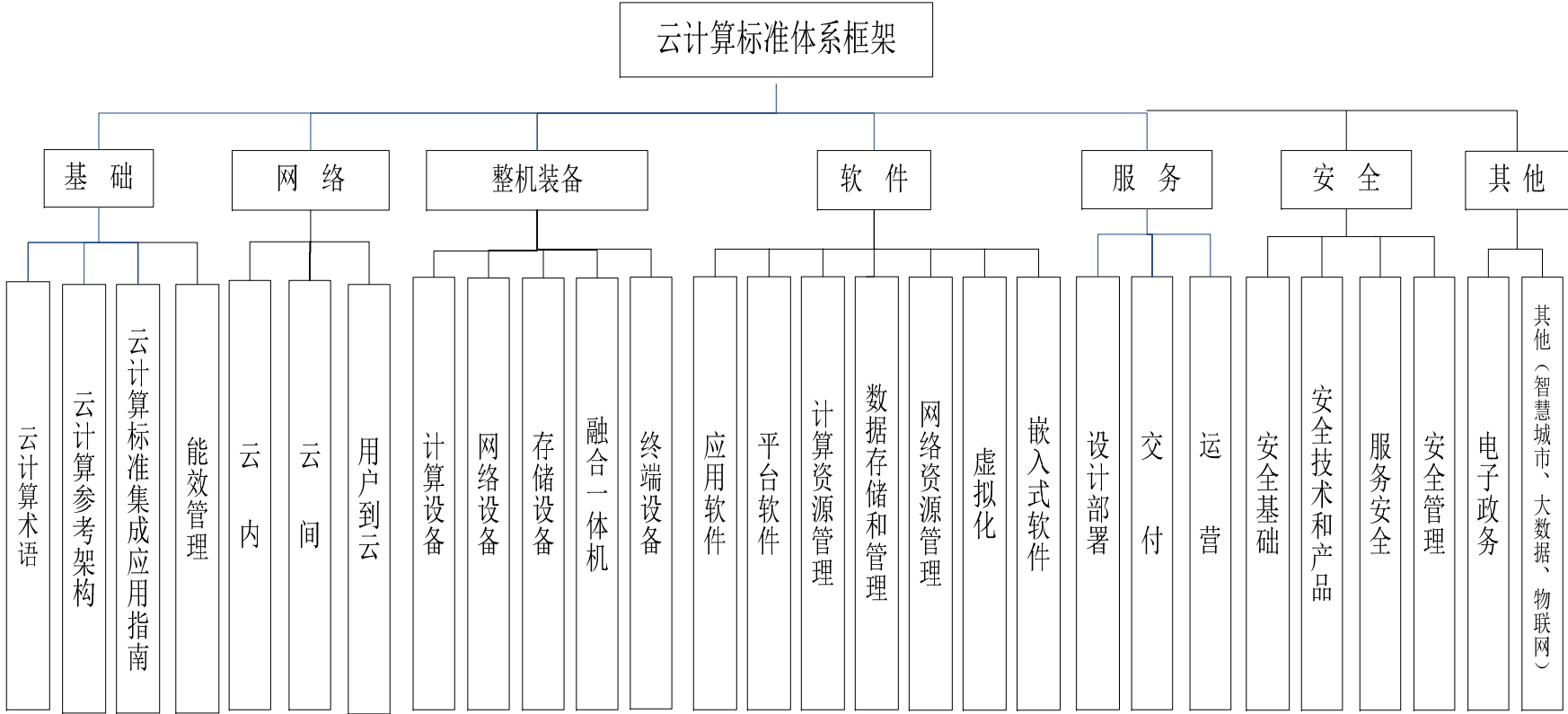


图 11 云计算标准体系框架

在研标准列表如表 7 所示：

表 7 云计算在研标准清单

序号	标准名称	状态
1.	弹性计算应用接口	国标报批
2.	信息技术 云数据存储和管理 第 1 部分 总则	国标报批
3.	信息技术 云数据存储和管理 第 2 部分 基于对象的云存储应用接口	国标报批
4.	信息技术 云数据存储和管理 第 5 部分 基于 Key-Value 的云数据管理应用接口	国标报批
5.	信息安全技术 云服务安全指南	国标报批
6.	信息安全技术 云服务安全能力要求	国标报批
7.	云计算术语	国标草案
8.	云计算参考架构	国标草案
9.	PaaS 平台参考架构	国标草案
10.	云计算数据中心参考架构	国标草案
11.	开放虚拟化格式规范	工作组草案
12.	云服务分类	工作组草案
13.	服务级别协议（SLA）规范	工作组草案
14.	虚拟机总体技术要求	工作组草案
15.	交付要求与原则	工作组草案
16.	云服务运营通用要求	工作组草案
17.	云服务监控技术要求	工作组草案
18.	云服务质量评价指标体系	工作组草案
19.	SAAS服务商能力要求与分级规范	工作组草案
20.	云服务应用和数据迁移指南	国标预研
21.	云服务计量指南	国标预研

其中，《信息技术 云数据存储和管理 第 1 部分 总则》、《信息技术 云数据存储和管理 第 2 部分 基于对象的云存储应用接口》、《信息技术 云数据存储

和管理 第 5 部分 基于 Key-value 的云数据管理应用接口》、《弹性计算应用接口》、《信息安全技术 云服务安全指南》、《信息安全技术 云服务安全能力要求》标准已进入报批阶段，一经正式发布，有望成为我国云计算领域内的首批国家标准。

下面介绍 7 个部分的概况以及所包含的在研标准情况：

1、基础标准

用于统一云计算及相关概念，为其他各部分标准的制定提供支撑。主要包括云计算术语、参考架构、指南、能效管理等方面的标准。

(1) 《云计算术语》和《云计算参考架构》

国际上 ISO/IEC JTC1 SC38 启动《云计算术语》和《云计算参考架构》国际标准的制定，开展云服务交付模式的研究。ITU-T SG 13 在原有云计算焦点组 (FGCC) 的基础上建立，开展《云计算术语》、《云计算参考架构》的研究。目前这两大国际云计算组织通过成立联合工作组的方式，共同推出这两个国际标准的制定，已经进入 DIS 阶段，参与基础标准的国际标准组织还有 ETSI、NIST、TOG 等。

国内上，我国在开展国际标准化工作的同时，同步开展《云计算术语》、《云计算参考架构》等基础标准的研制，中国和美国的贡献物成为《云计算参考架构》的基础文档，中国成功争取到《云计算参考架构》联合编辑职位。

云计算基本参考架构主要规定了云计算基本参考模型和基本的技术要求，以及基础设施即服务、平台即服务、软件即服务等服务模式的要求。云计算基本参考模型涵盖云服务客户、云服务提供者和云服务协作者三类角色。不同角色之间通过统一规范接口进行交互。云计算基本参考模型不仅为云计算提供者和开发者搭建了一个基本的技术参考实现模型，也为云计算服务的评价和审计人员提供相关指南。

(2) 云计算数据中心参考架构

定义了云计算数据中心基本参考架构，包括必备基本特征、推荐性建议，以及云计算数据中心参考架构中各组成部分及功能。并对云计算的基础设施，资源池，能效管理，安全，服务及运维管理提出了要求。

2、网络标准

用于规范网络连接、网络管理和网络服务。主要包括云内、云间、用户到云等方面的标准。

3、整机装备标准

用于规范适用于云计算的计算设备、存储设备、终端设备的生产和使用管理。主要包括整机装备的功能、性能、设备互联和管理等方面的标准。

包括《基于通用互联的存储区域网络（IP-SAN）应用规范》、《备份存储 备份技术应用规范》、《附网存储设备通用规范》、《分布式异构存储管理规范》、《模块化存储系统通用规范》、《集装箱式数据中心通用规范》等标准。

（1）基于通用互联的存储区域网络（IP-SAN）应用规范

本标准对 IP-SAN 存储设备和系统架构参考模型、IP-SAN 的统一描述方法及通信方式的规范、以及 IP SAN 数据安全规范和评估进行标准化。本标准可广泛适用于数据中心、存储局域网等环境下的 IP-SAN 存储设备和系统。

（2）备份存储 备份技术应用规范

本标准建立云存储数据备份应用的备份系统架构参考模型，对文件系统、数据库及虚拟机的具体应用进行备份流程、备份方式、备份策略方面进行标准化。

（3）附网存储设备通用规范

本标准规定了附网存储的术语、技术要求、测试方法、检验规则。本标准适用于服务网存储设备的生产厂商、以及使用附网存储设备的客户。

（4）分布式异构存储管理规范

本标准规范了存储管理信息的统一描述方法及通信方式，提出了符合国家需要的规范化存储管理安全保护机制，构建了分布式异构存储设备和系统的管理信息模型和实例，用于构建大规模、可扩展存储系统，满足当前日益增长的信息存储需求，有力地支撑国内存储产业的发展。

（5）模块化存储通用规范

本标准给出了模块化存储系统的界定说明与分类、模块化存储系统技术要求和设计规范，以及与技术要求相对应的检测方法，以此保障产品质量和使用安全。

（6）集装箱式数据中心通用规范

集装箱式数据中心是一个可作为数据中心构建的标准模块，为企业在短时间内完成数据中心容量的扩展；同时，也可作为单独使用的模块，在企业主数据中心之外建立独立的灾备站点，或用于军事项目、政府保密工程、能源勘察、大型活动的户外作业，是应对于企业级数据中心快速、灵活需求的最佳解决方案。本标准给出了集装箱式数据中心的设计规范和评价标准，为集装箱式数据中心的规格、架构、技术参数提供统一规范。

4、软件标准

用于规范云计算相关软件的研发和应用，指导实现不同云计算系统间的互联、互通和互操作。主要包括虚拟化、计算资源管理、数据存储和管理、平台软件等方面的标准。

软件标准中，“开放虚拟化格式”和“弹性计算应用接口”主要从虚拟资源管理的角度出发，实现虚拟资源的互操作。“云数据存储和管理接口总则”、“基于对象的云存储应用接口”、“分布式文件系统应用接口”、“基于 Key-Value 的云数据管理应用接口”主要从海量分布式数据存储和数据管理的角度出发，实现数据级的互操作。从国际标准组织和协会对云计算标准的关注程度来看，对虚拟资源管理、数据存储和管理的关注度比较高。其中，“开放虚拟化格式规范”和“云数据管理接口”已经成为 ISO/IEC 国际标准。

（1）弹性计算应用接口

弹性计算服务是基于虚拟化资源的云计算服务，是云服务的核心，是目前部署和应用较广泛的云服务。许多大型公司纷纷推出了弹性计算服务，包括 Amazon EC2, RackSpace Cloud Servers 等。但是这些弹性计算服务在接口功能、接口协议等方面存在诸多不一致、这些不一致带来了以下问题：

- 弹性计算服务间互联互通困难。由于不同的弹性计算服务提供不同接口功能及接口协议，因此用户在使用不同提供商提供的弹性计算服务时，无法实现上层应用的统一部署，这样容易导致用户被绑定至同一弹性计算服务提供商，为用户带来较大风险。
- 弹性计算服务接口的不统一阻碍弹性计算服务发展。用户若使用不同的弹性计算服务，必须进行相应的适配接口开发，阻碍用户选择弹性计算

服务。同时，围绕不同服务接口的特定语言编程包和第三方管理软件的开发需要做多种适配，造成行业发展力量分散，阻碍了弹性计算服务的发展。

“弹性计算应用接口”制定的目标是为用户和弹性计算服务的交互提供一套标准接口，支持用户在多个服务提供商中进行选择，支持用户上层应用的跨弹性计算服务部署。本规范的制定将有助于提高用户对弹性计算服务的体验，促进弹性计算产业的开放性和标准化，促进弹性计算产业的整体良性发展。该接口规范主要关注弹性计算服务接口问题，包括基于虚拟化资源的弹性计算体系框架，服务模型、接口功能、接口协议、标准操作集合、对安全的要求等。

（2）云数据存储和管理 第1部分 总则

云计算环境下数据量大且分布在网络上的不同结点、不同设备和系统上。从数据的结构化程度看，包含了结构化数据、半结构化数据和非结构化数据，且非结构化数据所占的比重日益增大。数据存储和管理应用接口旨在对存储在不同系统、结构化程度不同的数据提供统一的存储和管理接口。目前的云数据存储系统主要包括块文件存储系统和基于对象的云存储系统。数据存储管理接口必须兼顾这两类不同的存储系统。云数据管理系统包括基于 Key-Value 的数据管理、分布式关系数据管理和分布式数据仓库管理。从管理内容上看，数据存储和管理接口包括对各种类型存储设备、数据和元数据的增加、删除、修改和查询接口。这里的数据包括结构化数据、半结构化数据和非结构化数据。“云数据存储和管理应用接口总则”规定了云存储和数据管理体系框架、云数据存储类规范、云数据管理类规范、基本原则、质量和安全性要求等，供系列标准参考。其中，云数据存储和管理体系架构如图 12 所示。

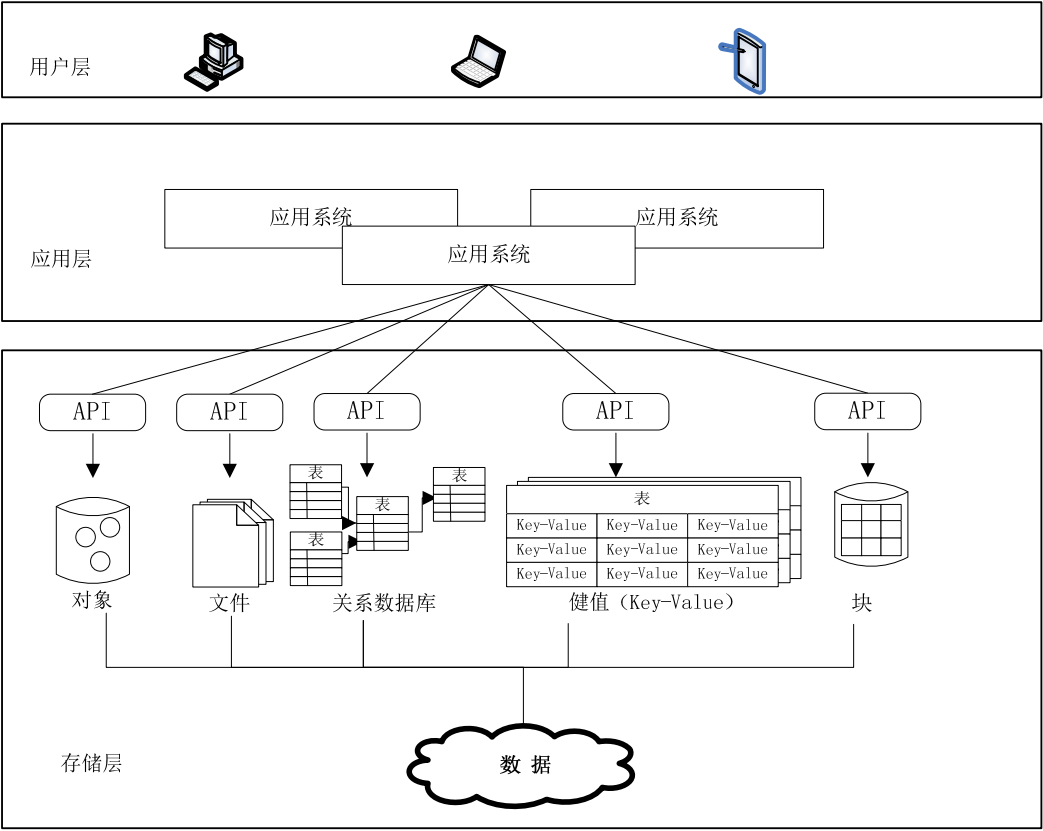


图 12 云数据存储和管理标准体系架构

（3）云数据存储和管理 第 2 部分 基于对象的云存储应用接口

目前国内外已有多家云存储服务提供商提供相关对象云存储服务，包括 Amazon 的 S3、谷歌的“Google Storage（GS）”云计算存储服务、AT&T 推出的基于 EMC Atmos 数据存储基础架构的 AT&T Synaptic Storage as a Service。一些国际标准协会也发布了云数据存储规范，如 SNIA 的 CDMI。

总体情况上，各家云存储服务接口不一，且为各互联网公司私有方案，给用户数据迁移和共享带来很大的障碍；而 CDMI 由于考虑到与传统存储体系的融合，体系架构较为复杂，与各互联网公司提供的对象云存储服务理念存在差异，且目前尚没有实际的商业服务实现。因此，对于中国的运营商和互联网公司来说，针对对象云存储提供服务的接口，目前尚无较好的标准可以参考。

本规范将面向中国公众云存储服务发展的业务需求，定义适合中国运营商和互联网公司提供公众对象云存储服务的统一接口规范。在定义中将充分参考现有

商业接口规范、CDMI 规范和 S3 等互联网公司私有方案的经验和优点。本标准规定了基于对象的云存储应用接口的体系框架，数据接口模型，接口协议，基本元数据，基本功能元素，标准操作集合，安全要求等。本标准适用于对象云存储应用接口的设计、开发和服务提供。本标准是制定具体对象云存储的技术标准、质量测评标准的依据。

(4) 云数据存储和管理 第 5 部分 基于 Key-Value 的云数据管理应用接口

Key-Value 数据库作为一种新兴的云数据库，是传统关系数据库的良好补充，在管理结构化数据和非结构化数据方面发挥着重要作用。

目前，各类 Key-Value 数据库和数据管理应用层出不穷，包括各种商业和开源系统。这些 Key-Value 云数据管理服务的定义和分类还未达成一致，各自有独立的服务接口，这为数据的动态迁移、高效集成、统一访问带来了很大困难，使得用户面临着数据锁定和服务商锁定问题。对基于 Key-Value 的云数据管理服务接口进行规范，不仅可以解决数据锁定和服务商锁定问题，实现不同 Key-Value 云数据管理平台之间的互操作，还可以促进上层应用的开发，营造健康有序的云计算产业发展环境。

本标准主要关注基于 Key-Value 的云数据管理服务接口问题，规定了基于 REST、SOAP 等协议的 NoSQL 云数据管理服务接口的一系列要求，主要包括：

- 服务的定义：为了将 Key-Value 数据库服务与传统的关系数据库服务区别开，并界定其服务内容范围，需要先给出基于 Key-Value 的云数据服务的准确定义。
- 服务的分类：Key-Value 数据库是一类新兴的数据库，仍在不断地发展和完善，目前尚未有统一的分类。虽然不同 Key-Value 数据库的存储结构有很多种，但是其中有些 Key-Value 数据库对外提供的服务十分类似，因此对基于 Key-Value 的云数据服务进行分类必要且可行。
- 服务接口通用性要求：为实现可高度支持的服务接口，对提供通用的服务接口类型和协议栈的要求。
- 服务接口要求：为界定每项服务的服务内容，对提供详细的服务接口描述的要求。
- 服务质量要求：对基于 Key-Value 的数据管理服务质量和等级加以规范。

- 服务安全接口要求：为保证服务的安全性，对提供安全的服务接口的要求。

本标准适用于 Key-Value 云数据库和数据管理服务的实现厂商、上层应用的开发厂商等。

（6）PaaS 平台参考架构

PaaS 是云计算的重要应用模式之一，PaaS 平台是实现 PaaS 模式的核心基础，它可以为 SaaS 应用提供统一的编程模型、快速开发和在线部署能力，以及计算能力的按需弹性扩展。PaaS 平台的组成和运作，国内目前仍然没有一个统一的概念性理解。本规范的目的在于提供一个 PaaS 平台的概念蓝图，使得在多个 PaaS 平台和应用的开发和交付项目之间能够确保一致性，从而更好的指导客户企业、SaaS 应用开发商和运营商、PaaS 技术和产品提供商搭建 PaaS 计算环境，高质量的交付云服务。

PaaS 平台参考架构是构建 PaaS 平台的基础，它是从架构的角度抽象概括组成一个完整的 PaaS 计算环境的基本组成元素及其之间的关联，以及治理其演变的架构性原则。PaaS 平台参考架构规范的工作任务如下：

- PaaS 平台的参与角色
- 组成 PaaS 平台的构件，及其相互之间的关系
- PaaS 平台的架构原则和相关指南

（7）开放虚拟化格式规范

虚拟化是云计算的重要支撑技术之一，而开放虚拟化格式又是服务器虚拟化的重要方面。云计算开放虚拟化格式规范主要描述运行在虚拟机上的软件的安全、开放、可移植、高效和可扩展的封装和分发格式。安全指的是该格式能够支持完整性验证和身份鉴别。开放和可移植指的是该格式独立于具体的供应商和平台。高效和可扩展指的是该格式能够支持自动分发、单虚拟机和多虚拟机分发、在不同平台间移植时能够兼顾特定平台的特性、易于本地化。从内容上看，该规范应该包含开放虚拟化格式的基本概念、结构，核心元素以及环境文档。

在开放虚拟化格式规范方面，国际协会组织 DMTF 于 2010 年 1 月 12 日发布了 Open Virtualization Format Specification 1.1.0，旨在定义组织结构和核心元素，但目前国内这方面尚属空白。

5、服务标准

用于规范云服务设计、部署、交付、运营和采购，以及云平台间的数据迁移。主要包括服务采购、服务质量、服务计量和计费、服务能力评价等方面的标准。

云服务标准以软件标准、整机装备等标准为基础，主要从各类服务的设计与部署、交付和运营整个生命周期过程来制定，主要包括云服务分类、云服务设计与部署、云服务交付、云服务运营、云服务质量管理等方面的标准。云计算中各种资源和应用最终都是以服务的形式体现出来。如何对形态各异的云服务进行系统分类是梳理云服务体系，帮助消费者理解和使用云服务的先决条件。服务设计与部署关注构建云服务平台所需要的关键组件和主要操作流程。服务运营和交付是云服务生命周期的重要组成部分，对服务运营和交付的标准化有助于对云服务提供商的服务质量和服务能力进行评估，同时注重服务的安全和服务质量的管理与测评。

（1）云服务分类

云服务分类标准将规定云服务的分类。包括云服务的分类、管理和编目，以及云服务的信息处理，并为云服务的开发、服务提供、服务消费及管理人员提供一个科学适用的分类原则和方法。

（2）服务级别协议（SLA）规范

规定了云计算环境下服务级别协议（SLA）的建立要求，云服务级别协议框架和术语给出云服务 SLA 的概述，理清主协议和 SLA 之间的关系，为云服务商和用户提供建立 SLA 所需的通用的概念、需求、术语以及度量指标的一致性认识。不是做云 SLA 的框架，而是从构建通用 SLA 所需的元素展开。

（3）虚拟机管理通用要求

本标准重点从虚拟机的基本功能和特性、虚拟机管理器中的虚拟机管理功能和特性以及虚拟资源管理平台中对虚拟机的生命周期和维护管理三个大的方面，从技术和商业服务模式两个角度提出了虚拟机管理的通用要求。本标准可适用于：

- a) 为虚拟化系统和云计算产品的生产商、集成商、运营商提供评价自身能力的指南；
- b) 为用户提供选择和评价提供虚拟化系统和相应服务的组织提供指导；

c) 第三方评测提供虚拟化系统和相应云服务的组织的能力。

(4) 交付要求与原则

提出云服务交付的框架，包含交付内容、交付过程、交付质量和服务交付管理并实现持续改进。本标准可作为云服务提供商用来评估和改进自身交付条件和能力的依据，也可以为第三方和用户评价和认定云服务提供商的服务交付能力提供指导。

(5) 云服务计量指南

可测量的服务是云计算的关键特征之一。目前，无论是公有云、私有云，还是混合云，国内外企业纷纷推出可计量的 IaaS、PaaS 和 SaaS 产品，云服务计量指南首先对国内外典型云服务产品以及开源产品的计量指标进行广泛调研，对国内外标准化组织和协会在云服务计量方面的工作进行系统研究。在以上工作的基础上，提出云服务计量的标准化需求，研究云服务计量指标体系。

云服务的计量指标主要作用包括：

a) 由于采用虚拟化技术，客户在选购云服务时需要统一的计量指标描述虚拟产品、服务水平等级以及性能，以便让用户容易理解购买的云服务产品与传统产品之间的关系，减少用户选择和使用云服务时的困扰；

b) 在云服务使用过程中使用统一的计量指标，方便让第三方机构对市场上的云服务进行监管；

c) 通过统一的计量指标，政府、企业在预算、招投标、项目计划等活动可以依据统一的计量指标和计费标准，开展预算工作。

(6) 云服务应用和数据迁移指南

本标准给出不同云平台间应用和数据迁移的指南。重点在对应用和数据迁移时，对信息采集评估、迁移方案设计（包括迁移的场景、方法、步骤等）等方面需要满足的技术要求、环境因素以及方法流程方面给出指导。

(7) 云服务运营通用要求

本标准规定了在提供云计算服务过程中的人员、过程、技术、资源和安全等方面的基本要求，从而最终确保可提供稳定、安全和可靠的云计算服务。

本标准通过对云计算服务的内部要素和外部特性的研究，给出了一个云计算服务的模型。该模型描述了云计算服务的用户可见的基本特性：按需服务、弹性、网络依存性和可计量，这些特性可作为判断某个信息技术服务是否是云计算服务

的基本依据。同时，该模型概括了云计算服务的四个基本内部要素：人员、资源、技术和过程，规定了云计算服务提供商在人员、资源、技术和过程方面所必需具备的基本能力，以确保其可以为用户提供稳定、安全和可靠的云计算服务。本标准适用于：规范云计算服务提供商的自身能力和服务交付过程，从而确保为用户提供可靠的云计算服务。

（8）云服务监控技术要求

本标准从云服务用户、云服务业务支撑和云服务运维支撑三个角度给出保障云服务运营的监控技术要求和关键指标。为云服务提供商在云计算环境下的基础设施资源、服务及运行等方面的监控提供了指导性建议，本标准适用于：

- a) 提供云服务的组织评估和改进自身的监控技术能力；
- b) 为云服务用户选择和评测提供云服务的组织的监控技术提供指南。

（9）云服务质量评价指标体系

本标准建立了云服务质量模型，规定了云服务质量的评价指标体系。为云服务相关方评价云服务质量提供一致的、公正的方法或依据。本标准从功能性、安全性、可靠性、响应性、有形性和友好型性等方面构建了云服务质量的模型框架以及相对应的指标评价体系。本标准适用于云服务的提供商、使用云服务的用户、第三方评测机构和云服务的审计人员。

（10）SAAS服务商能力要求与分级规范

为了规范和引导SAAS服务业发展，培育新兴业务模式，建立良好市场秩序。本标准SAAS服务组织提供了一个公共能力框架，规定了SAAS服务组织在资源、研发技术、运营、客户服务方面应具备的条件，并给出评价或选择SAAS服务组织的建议。

本标准适用于：

- a) 提供SAAS服务的各类组织评估和改进自身的条件和能力；
- b) 需要SAAS服务的组织选择和评价提供SAAS服务的组织；
- c) 第三方评价和认定提供SAAS服务组织的能力。

6、安全标准

用于指导实现云计算环境下的网络安全、系统安全、服务安全 and 信息安全，

主要包括云计算环境下的网络和信息安全标准。

（1）云服务安全指南

该标准描述了云计算服务可能面临的主要安全风险，提出了政府部门采用云计算服务的安全管理基本要求，及云计算服务的生命周期各阶段的安全管理和技术要求。该标准为政府部门采用云计算服务，特别是采用社会化的云计算服务提供全生命周期的安全指导，适用于政府部门采购和使用云计算服务，也可供重点行业或企事业单位参考。

（2）云服务安全能力要求

该标准对政府部门和重要行业使用的云计算服务提出了基本的安全能力要求，反映了云服务商在保障云计算平台上的信息和业务安全时应具有的基本能力。标准对云服务商提出了一般要求和增强要求。根据拟迁移到社会化云计算平台上的政府和行业信息、业务的敏感度及安全需求的不同，云服务商应具备的安全能力也各不相同。

7、其它标准

主要包括与电子政务、智慧城市、大数据、物联网、移动互联网等衔接的标准。

七、如何实施云计算

云计算已从最初的理念发展至今，不论是产品还是标准，都进入落地应用阶段，探索和建立适宜云计算发展的市场准入、服务采购和安全保障机制，推广应用安全可靠的云产品和云解决方案，以及如何实施云计算、构建云计算、如何从用户的视角选择适合的云相关产品，是目前产业界关注的重点。

云计算的本质是一种新型服务模式，而基于标准的云服务可通过开放的标准接口实现互操作性和可移植性，从应用角度出发，SLA、云安全也是云计算在实施过程中，云用户应关注的重点。下面分步介绍实施云计算的一系列步骤。

（一）云计算实施总路线

1、 组建团队

云用户可能是各类不同规模的企业，在决定采用云计算为自己服务时，需建立相应的工作团队，并明确在云实施不同阶段各角色的工作职责和工作目标。如图 13 所示。

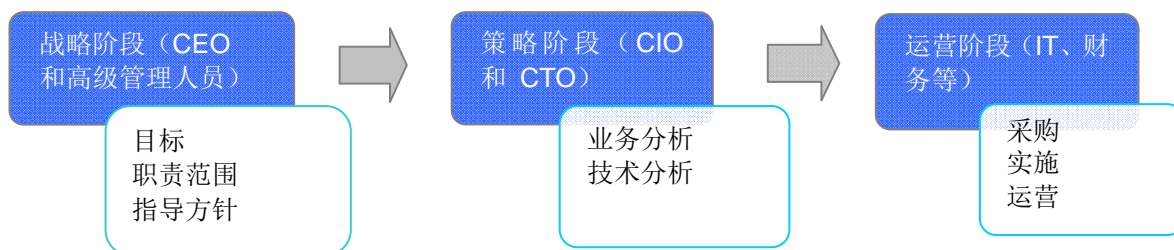


图 13 各角色的工作职责和目标

在云采用的战略阶段，CEO 和高级管理层领导公司确定目标、职责范围和指导方针。

在策略阶段，通常在 CIO 或 CTO 的领导下，公司执行业务分析和技术分析。

在运营阶段，不同运营组的主管针对云部署，共同完成持续运营业务的采购、实施和运营。

2、制定业务案例和云战略

云用户应明确自身需求，结合自身业务特点，制定适合自身发展的综合云战略。

在规划云战略时，应将以下因素考虑在内：培训团队、考虑现有IT环境、了解所需的服务和功能、确定所需的技能、制定长期和短期规划图、确定明确的目标和衡量进度的指标、了解法律法规要求、延长追踪结果的时间。

3、选择云部署模式

根据既定云战略，综合考量企业规模、云服务关键程度、业务迁移成本、弹性、安全和多租户等因素，选择合适的云部署模式。

4、选择云服务模式

根据云用户的IT成熟度和企业规模，结合各类云服务模式的特点，选择适合用户需求的云服务模式：

（1）基础设施即服务（IaaS）的优势：

——通过提高资源利用率和管理员对服务器的比例，减少 IT 运营支出和资本支出；

- 通过提高效率和标准化解决方案的自动化，提高产品推向市场的速度；
- 简化集成管理流程，包括实时监测和高扩展低干预的调配；
- 提高对业务流程和系统性能的可见性，以确定冗余和瓶颈；
- 对市场动态和业务战略需求实现可扩展的运营模式。

（2） 平台即服务（Paas）的优势：

- 快速经济的开发部署新应用程序；
- 面向预定义工作负载的高度标准化和自动化调配；
- 面向特定工作负载的集成式开发和运行平台；
- 面向大多数常见工作负载的基于模式的部署；
- 面向 SLA 执行、动态资源管理、高度可用性和业务优先级的集成式工作负载管理；
- 基于业务优先级和 SLA 的工作负载意识与最佳化；
- 简化的管理系统之下的工作负载整合。

（3） 软件即服务（Saas）的优势：

- 将计算变成用户可轻松采用的实用程序；
- 高度的可扩展性；
- 实施时间周期短；
- 升级更新、以及解决方案的可用性由提供商负责。

5、 明确由谁开发、测试和部署云服务

根据云用户的需要和能力，开发、测试和部署云环境，按部署方法可分成四种方式：

- 内部开发和部署；
- 云提供商开发和部署；
- 基于云服务的独立开发提供商；

——购买现成的云服务。

云用户应从技能、初始考虑项、服务更新以及测试和部署这几个方面，综合考虑选择哪类部署方式，也可以根据具体的云服务需求，同时利用多个方式。

6、 在生产之前制定概念验证 (POC)

一旦明确要实施云，可（推荐但不必须）建立概念验证 (POC) 团队，假设 POC 成功，符合或超出预期，则云服务可以交付进行生产实施。POC 既可以在公司内部实施，也可以直接在公有云中实施。POC 和目标云环境之间可能存在的差异，向生产环境迁移时，需要处理目标云环境。

一旦完成全部测试，并且运行正常，即可进一步完善商务合同、SLA等，将新的云服务投入生产。

7、 与现有企业服务集成

有多种方法可以在云服务和现有服务之间建立无缝连接。

——企业已确定采用开放基础设施标准，则云服务应建立在已实施的内容的基础上，可通过标准化的应用程序编程接口（API）来对此进行管理，这些 API 将成为云服务所支持的开放标准和企业现有服务之间的连接导管，实现云服务和企业服务之间的互操作性。

——企业没有确定要采用开放基础设施标准，则可使用新的云服务来设置基线。一个清晰的采用开放标准的计划能确保云服务的互操作性和可移植性，并简化新服务的基础流程，使之不受新的云服务的获取位置和方式的限制。

8、 制定和管理 SLA

SLA 是用于解决服务交付争议的书面协议。花费时间制定一份全面的 SLA 将有助于消除用户与提供商之间的预期异议，也有助于确保交付满意的服务水平。

在制定云用户（买方）和云提供商（卖方）之间的SLA时，不仅要考虑到不同类型的服务模式有不同的需求，还应关注的因素还有：组建内部SLA团队、为合约服务制定SLA、与提供商共同定义关键流程、定期与企业内的关键利益相关者举行评审会、定期与云提供商召开检查点会议等。

如何实施和评估SLA，将在（二）云服务水平协议（SLA）实施步骤中详细

讲述。

9、 管理云环境

企业管理和运营云环境需要CIO和用户支持经理共同负责，前者整体负责，后者负责管理日常运营，并建立通畅的沟通渠道，如问题不能解决，须参考SLA中相关规定。

技术支持和用户支持因服务模式、部署模式和托管选择而异：

——若选择私有云（现场），则对其管理应与企业现有服务的管理一致。

——若选择私有云（外包）和公有云，则应在 SLA 中规定对其管理责任。

SLA 要确定相关流程用以发现问题，确定负责人和问题影响范围，寻找可以用来解决问题的资源（来自用户和提供商）。

除此之外，还需对灾难恢复流程做定义和实施、对问题报告流程和问题报告回应达成书面协议 (SLA)，如果拥有多个云供应商，需对供应商管理流程进行明确定义。

（二）云服务水平协议（SLA）实施步骤

1、理解角色和责任

为使用户理解云 SLA 明示或暗示的具体角色和责任，必须了解云计算环境可能会涉及的不同角色。一般包含 5 种云角色：

——云用户：与云供应商维持业务关系或使用云供应商服务的个人或机构；

——云供应商：有责任向云用户提供服务的个人、机构或实体；

——云运营商：提供云供应商与云用户间云服务连接和传输的中介机构；

——云代理商：管理云服务使用、表现和交付，并协调云供应商和云用户关系的机构；

——云审计者：独立评估云服务、信息系统运营、云实施的性能和安全性的
一方。

用户需要了解每种云角色在云环境交付中的活动与责任，为每种角色准确设

定要求与服务水平。SLA 对不同的角色有不同要求，不限于定量方面，也包含遵照标准和数据保护等定性要求。通过 SLA 实施步骤，每个步骤都将详细介绍用户与供应商在业务水平目标和服务水平目标方面应负的责任。

2、评估业务水平策略

由于SLA所述策略与业务策略相关,用户在评审云SLA时必须考虑关键的策略问题。SLA内描述的云供应商的数据策略可能是最关键的业务水平策略，需要对其进行仔细评估。

SLA中涉及的数据策略包括：数据保存、数据冗余、数据位置、新数据位置的研究、数据获取、数据隐私。

除了数据策略外，云 SLA 内所述的其他业务水平策略也需要仔细评估，这些业务水平策略包括：承诺、可接受的使用策略、未涵盖服务列表、超额使用、激活、支付与惩罚模式、治理/版本控制、续约、转让、支持、计划内维护、分包服务、许可软件、行业特定标准等。

3、了解各种服务模型和部署模型的区别

云供应商提供的服务一般都可归纳为三种主要的服务模型：基础设施即服务 (IaaS)、平台即服务 (PaaS)、软件即服务 (SaaS)。对每一种类来说，云 SLA 内可能包含的云资源抽象水平、服务水平目标和关键性能指标各有不同。

除了服务模型外，云 SLA 还应包含服务部署条款，这些条款应确认部署模型、所采用的部署技术。

4、确定关键性能目标

云计算环境中的性能目标与服务交付的效率和准确性直接相关。性能一般通过可用性、响应时间、事务处理率和处理速度来衡量，但很多其他因素也可以衡量性能和系统的质量。因此，用户必须确定哪些因素对其云环境最为重要，并确保 SLA 中包含这些因素。

对云用户非常重要的性能声明需要具备可测量性，可以由用户对其审计，并且书面记录在 SLA 中，从而满足协议双方对服务水平的要求。性能的考虑因素因支持的服务模型 (IaaS、PaaS 和 SaaS) 和各模型提供的服务类型的不同而异，如 IaaS 模型提供网络、存储和计算服务。

为了确保性能目标有意义，当透明性和一致性对加强云服务的可信赖性非常重要时，度量是一个关键考虑事项。度量时，一定要清楚指标是怎样使用的，从

这些指标中能得到什么结论，不断对性能进行评估，使其达到具体的目标。

5、评估安全和隐私保护要求

确保云足够安全的首要措施是根据企业数据的重要性和敏感性创建分类方案，在整个企业内部施行。该方案应包括数据所有权、对安全水平的合适定义和保护控制等方面的详细信息，以及对数据保留和删除需求的简单描述。分类方案应作为控制实施的依据，如访问控制、归档或加密。为了确定具体资产所需要的安全水平，就要对资产的敏感性和重要性进行粗略的评估。

在隐私方面，很多国家的法律、法规和其他规定都要求公共和私立机构保护个人数据的隐私性以及信息系统和计算机系统的安全性。

数据传输到云中后，保护数据安全的义务通常都由数据的收集人或管理人承担，尽管有些情况下，收集人或管理人可能与其他人共同承担该义务。如需要第三方托管或处理数据，数据管理人仍应对数据的丢失、损坏或滥用负责。因此，数据管理人和云供应商签订书面（法律）协议是比较稳妥甚至是法律规定的做法，这样可以明确协议双方的职责和要求，并分割双方的相关责任。

6、明确服务管理需求

用户在与云计算供应商签订服务水平协议时需要考虑的有关服务管理的重要问题，主要包括：审计、监控和汇报、计量、快速调配、资源变更、对现有服务的升级等几个方面。

7、为服务故障管理做准备

云 SLA 应明确书面记录预期的服务能力和服务性能，否则用户和供应商发生误会的可能性会显著增加。例如，除非 SLA 中有明确规定，否则供应商不会认为 Web service 的响应时间过长属于服务故障。

服务故障管理的水平因供应商的不同而有很大差异，而能否争取到更高水平的管理服务则取决于用户公司的规模。因此，用户应在协议中包括其自身的服务故障管理能力，以确保能够及时获知出现的问题。

8、了解灾难恢复计划

灾难恢复属于业务连续性的范畴，主要指在发生灾难时，用于恢复应用程序、数据、硬盘、通信（如网络）和其他 IT 基础设施的流程和技术。这里的灾难既包括自然灾害，也包括影响 IT 基础设施或软件系统可用性的人为事件。

企业将基础设施即服务（IaaS）、应用程序即服务（SaaS）或平台即服务

(PaaS)外包至云环境并不意味着企业就不需要制定严格的灾难计划。每个企业外包的基础设施或应用程序的重要性不同,因此云灾难恢复计划也各不相同,而在制定灾难恢复计划时,业务目标是非常重要的参考。

9、开发有效的管理流程

不断发展的云计算需要有一套有效的管理流程,以解决可能遇到的各种问题。实行有效的管理流程是确保内部和外部用户对云服务的满意度的重要步骤。一个成功的管理流程的重要环节主要包括:确定每月例会、确保恰当的出勤、议题、追踪关键指标、生成报告。

10、了解退出流程

每个云 SLA 中都应包含退出条款,对退出流程进行详细规定,包括云供应商与用户的关系提前终止或到期终止时的责任分配。

SLA 都要明确规定退出流程,确保安全快速地转移用户的数据和应用程序。用户退出计划始终应在一开始签订 SLA 时就进行准备,并附在合同中。该计划应保证用户业务损失最小,并能顺利过渡。该退出流程应包括详细的程序,确保业务持续性,并明确提出可度量的指标,确保云供应商有效实施这些流程。

(三) 云安全实施步骤

当用户把其应用及数据转移到使用云计算时,在云环境中提供一个与传统 IT 环境一样或更好的安全水平至关重要。如果不能提供合适的安全保护,最终将造成更高的运营成本并有可能导致潜在的业务损失,从而影响云计算的收益。

本部分提供了云用户评估和管理其云环境安全应采取的系列规范性步骤,目标是帮助其降低风险并提供适当级别的支持。

1、 确保拥有有效的治理、风险及合规性流程

大多数机构已经为保护其知识产权和公司资产(尤其是在IT领域的资产)制定了安全及合规的策略和规程。对云计算环境的安全控制与传统IT环境下的安全控制是相似的,然而由于职责部门采用的云服务和运维模型、以及云服务所使用的技术等因素,云计算与传统IT解决方案相比会为机构带来不同风险。

依据安全和合规性政策,云服务用户保证其托管应用和数据安全的主要方式是参考相关的服务水平协议,核实用户和供应商之间的合同是否包含他

们的所有要求。用户了解与安全性相关的所有条款，并确保这些条款能满足其需要是至关重要的。如果没有合适的合同和SLA，不建议继续使用该机构的云服务。

2、 审计运维和业务流程报告

用户至少应保证看到独立审计师编写的关于云服务供应商的运维报告。能够自由获取重要的审计信息是用户与任何云服务供应商签订合同和SLA条款时的关键因素。作为条款的一部分，云服务供应商应将用户相关的特定数据或应用程序审计事项以及日志记录和报告信息及时提供，保证访问能力和自我管理能力。主要从以下三个领域对云安全进行考虑：

- 了解云服务供应商的内部控制环境，包括其调配的云服务时环境的风险、控制及其他治理问题。
- 对企业审计跟踪的访问，包括当审计跟踪涉及云服务时的工作流程和授权。
- 云服务供应商应向用户保证云服务管理和控制的设施是可用的，以及说明该设施是如何保障安全的。

对云服务提供商的安全审计是云用户在安全方面的重要考量，应由用户方或独立审计机构具备适当技能的人员进行操作。安全审计应以一个已发布的安全控制标准为基础，用户应检查安全控制是否符合其安全需求。

3、 管理人员、角色及身份

云用户必须确保其云服务供应商具备相关流程和功能来管理具有访问其数据和应用程序权限的人员，保证对其云环境的访问可控可管理。云服务供应商必须允许用户根据其安全策略为每一个用户分配、管理角色和相关等级的授权。这些角色和授权以单个资源、服务和应用程序为基础。

云服务供应商应包含一个安全系统来管理其用户和服务的唯一身份标识。这项身份管理功能必须支持简单的资源访问，以及可靠的用户应用程序和服务工作流。无论是何种角色或权限，供应商管理平台所有的用户访问或互操作行为都应该被监控并予以记录，以便为用户提供其数据和应用程序的所有访问情况的审计报告。

云服务供应商应设立正式流程，管理其员工对任何储存、传输或执行用户数据和应用程序的软硬件的访问情况，并应将管理结果提供给用户。

4、 确保对数据和信息的合理保护

云计算中的数据问题涉及到不同形式的风险，包括：数据遭窃取或未经授权的披露，数据遭篡改或未经授权的修改，数据损失或不可用。“数据资产”可能包括应用程序或机器镜像等，与数据库中的数据和数据文件一样，这些资产也有可能遇到相同的风险。

我国国家标准《云服务安全指南》（报批稿）和《云计算服务安全能力要求》（报批稿）对保障数据安全性、使用云服务时需要解决的数据安全注意事项等，从不同方面做了详细规定。

用户为确保云计算活动中的数据得到适当保护应注意以下几个方面：

- 创建数据资产目录
- 将所有数据包含其中
- 注重隐私
- 保密性、完整性和可用性
- 身份和访问管理

5、 实行隐私策略

在云计算服务合约和云服务水平协议中有必要充分解决隐私权保护问题。如果不明确列明隐私问题，用户应考虑通过其他方式实现其目标，包括寻找其他供应商或不将敏感数据导入云计算环境。例如，如果用户希望在云计算环境中导入HIPAA信息，用户必须寻找将与其签订HIPAA业务相关协议的供应商，否则用户不应将数据导入云计算环境中。

用户有责任制定策略以处理隐私权保护问题，并在其机构内部提高数据保护意识，同时还应确保其云服务供应商遵守上述隐私权保护策略。用户有义务持续核对其供应商是否遵守了上述策略，包括涵盖隐私权保护策略等所有方面的审计项目（涉及确保供应商是否采取改进措施的方法）。

6、 评估云应用程序的安全规定

制定明确的安全策略和流程，对确保应用程序能够帮助业务正常进行而避

免额外风险至关重要。应用程序的安全性为云服务供应商和用户至关重要，与保障物理和基础设施安全性一样，双方机构应尽力保障应用程序的安全性。不同云部署模型下的应用程序安全策略均不一样，主要区别如下：

（1）IaaS

- 用户有责任部署完整的软件栈（包括操作系统、中间件及应用程序等）以及与堆栈相关的所有安全因素；
- 应用程序安全策略应精确模拟用户内部采用的应用程序安全策略；
- 通常情况下，用户有责任给操作系统、中间件及应用程序打补丁；
- 应采用恰当的数据加密标准。

（2）PaaS

- 用户有责任进行应用程序部署，并有责任保证应用程序访问的安全性；
- 供应商有责任合理的保障基础设施、操作系统及中间件的安全性；
- 应采用恰当的数据加密标准；
- 在 PaaS 模式下，用户可能了解也可能不了解其数据的格式和位置。但有一点很重要，用户应被告知获得管理访问权限的个人将如何访问其数据。

（3）SaaS

- 应用程序领域安全策略的限制通常是供应商的责任并取决于合约及 SLA 中的条款。用户必须确保这些条款满足其在保密性、完整性及可用性方面的要求；
- 了解供应商的修补时间表、恶意软件的控制以及发布周期十分重要；
- 阈值策略有助于确定应用程序用户负载的意外增加和减少，阈值以资源、用户和数据请求为基础；
- 通常情况下，用户只能够修改供应商已公开的应用程序的参数，这些参数可能跟应用程序的安全配置无关，但用户应确保其配置更改不会妨碍供应商的安全模式；

- 用户应了解其数据如何受到供应商管理访问权限的保护。在 SaaS 模式下，用户可能并不了解其数据存储的位置和格式；
- 用户必须了解适用于其静态和动态数据的加密标准。

7、 确保云网络和连接的安全性

分外部网络和内部网络安全两部分。

建议从流量屏蔽、入侵检测防御、日志和通知等方面，来评估云服务提供商的外部网络管理。

内部网络安全与外部网络安全不同，在用户得以访问云服务供应商的部分网络后，维护内部网络安全由云服务提供商负责。用户应关注的主要内部网络攻击类别包括：保密性漏洞（敏感数据泄露）、完整性漏洞（未经授权的数据修改）以及可用性漏洞（有意或无意地阻断服务）。用户必须根据其需求和任何现存的安全策略评估云服务供应商的内部网络管理。建议从保护用户不受其他用户攻击、保护供应商网络和检测入侵企图等方面，对云服务供应商的内部网络管理进行评估和选择。

8、 评估物理基础设施和设备的安全管理

云服务供应商应采用的适用于物理基础设施和设备的安全管理包括：

- 物理基础设施和设备应托管在安全区域内。应设置物理安全界限以防止未授权访问，并配合物理准入控制设施以确保只有经授权的人员才能访问包含敏感基础设施的区域。所有安装与调配云服务相关的物理基础设施的办公室、房间或设备都应设置物理安保措施；
- 应针对外部环境威胁提供安保措施，火灾、洪灾、地震、国内动乱及其他潜在威胁都有可能破坏云服务，因此应对上述威胁提供安保措施；
- 应对在安全区域工作的员工进行管理。这类管理目的在于防止恶意行为；
- 应进行设备安全管理，以防止资产丢失、盗窃、损失或破坏；
- 应对配套公共设施进行管理，包括水、电、气的供应等。应防止因服务失败或设备故障（例如，漏水）导致的服务中断。应通过多路线和多个设备供应商保证公共设施正常运作；

- 保障线缆安全，尤其要保障动力电缆和通信线缆的安全，以防止意外或恶意破坏；
- 应进行适当设备维护，以确保服务不会因可预见的设备故障而中断；
- 管理资产搬迁，以防止重要或敏感资产遭盗窃；
- 保障废弃设备或者重用设备中的安全，这一点对可能包含存储媒体等数据的设备尤为重要；
- 保障人力资源安全，应对在云服务供应商的设施内的工作人员进行管理，包括任何临时或合约员工；
- 备份、冗余和持续服务计划。供应商应提供适当的数据备份，设备冗余和持续服务计划以应对可能发生的设备故障。

9、 管理云服务水平协议（SLA）的安全条款

云活动中的安全责任，必须由云服务提供商和用户双方，通过云服务水平协议（SLA）的条款来共同明确和承担，SLA保障安全的一大特征是，任何SLA中对云服务供应商提出的要求，该供应商为提供服务而可能会使用到的其他云服务提供商也必须遵守此SLA。

10、 了解退出过程的安全需要

用户退出或终止使用云服务的过程需要认真考虑安全事项。

从安全性角度出发，当用户完成退出过程，用户具有“可撤销权”，云服务供应商不可继续保留用户的数据。供应商必须保证数据副本已经从服务商环境下可能存储的位置（包括备份位置及在线数据库）彻底清除。同时，除法律层面需保留的用户数据可暂时保留一段时间外，其他与用户相关的数据信息（日志或审计跟踪等），供应商应全部清除。

附录 A OpenStack 开源云计算平台介绍

A.1 OpenStack 云计算平台概述

OpenStack 是 2010 年由美国国家航空航天局（NASA）和云计算提供商 Rackspace 合作开发的云计算平台，帮助服务商和企业内部实现类似于 Amazon EC2 和 S3 的云基础架构（IaaS）服务。OpenStack 是以 Apache 许可证授权的开源项目，除了有 Rackspace 和 NASA 的大力支持外，后面还有包括 Dell、Citrix、Cisco、Canonical 这些重量级公司的贡献和支持，发展速度非常快，并逐渐取代另一个业界领先开源云平台 Eucalyptus。OpenStack 云计算平台由 7 个核心组件构成，组件的描述如表 A.1 所示。

表 A.1 OpenStack 组件描述表

组件名称	描述
Compute (代号为“Nova”)	Nova 是一套控制器，用于为单个用户或使用群组启动虚拟机实例。Rackspace 公司和 HP 提供商业计算服务正是建立在 Nova 之上，NASA（Nova 项目的起源地）内部也是使用的 Nova。
Object Storage (代号为“Swift”)	是一套用于在大规模可扩展系统中通过内置冗余及容错机制实现对象存储的系统。
Image Service (代号为“Glance”)	是一个虚拟机镜像的存储、查询和检索系统，它提供了一个虚拟磁盘映像的目录和存储库，这些磁盘映像常常广泛应用于 OpenStack Compute 之中，而且这种服务在技术上是属于可选的，任何规模的云都适用于它。
Dashboard (代号为“Horizon”)	为所有 OpenStack 的服务提供了一个模块化的 web-based 用户界面。使用这个 Web GUI，可以在云上完成大多数的操作，如启动实例，分配 IP 地址，设置访问控制等。
Identity (代号为“Keystone”)	为所有的 OpenStack 服务提供身份验证和授权。它还提供了一个在特定 OpenStack 云服务上的服务目录。
Network (代号为“Quantum”)	在接口设备之间提供“网络连接作为一种服务”，而这些接口设备主要靠其他的 OpenStack 服务进行管理。该服务允许用户创建自己的网络，然后连接接口。Quantum 提供一个可插拔的体系架构，它能支持很多流行的网络供应商和技术。
Block Storage (代号为“Cinder”)	提供稳定的数据块存储服务。这个项目的很多代码最初是来自于 Nova 之中（即 the nova-volume service）。

A.2 OpenStack Compute

OpenStack Compute 提供给一个组织云的工具，其中的功能包括运行虚拟机

实例，管理网络以及通过用户和项目来控制对云的访问。OpenStack Compute 的开源项目名字称为 Nova，它提供的软件可以控制基础设施即服务 (IaaS) 云计算平台，和 AmazonEC2 和 Rackspace 云服务器有一定程度相似。OpenStack Compute 没有包含任何的虚拟化软件，相反它定义和运行在主机操作系统上的虚拟化机制交互的驱动程序，并通过基于 Web 的程序应用接口 (API) 来提供功能的使用。

OpenStack Compute 是由以下主要的组件所组成：

nova-api：组件实现了 RESTful API 功能，是外部访问 Nova 的唯一途径。nova-api 接收外部的请求并通过 Message Queue 将请求发送给其他的服务组件。

nova-compute：主要是一个人工守护进程，它可以通过虚拟机管理程序的 API (XenAPI for XenServer/XCP, libvirt for KVM or QEMU, VMwareAPI for VMware 等) 来创建和终止虚拟机实例。nova-compute 的基础原理为：接收队列中的动作，然后执行一系列的命令 (如启动 KVM 实例)，同时更新数据库中的状态。

nova-volume：给虚拟机分配额外持久化的存储，管理持久卷到计算实例的创建，连接和分离。

nova-network：该人工守护进程与 nova-compute 和 nova-volume 非常相似。它接受队列中的网络任务，然后执行任务操纵网络 (如设立桥接接口或更改 iptables 规则)。不过该项功能被移植到 Quantum 之中，已经成为一个独立的 OpenStack 服务。

nova-schedule：作为一个后台进程运行，根据一定的算法从计算资源池中选择的一个计算节点用于启动新的 VM 实例。

queue：提供了一个守护进程之间传递消息的中央枢纽。当前由 RabbitMQ 实现，理论上可以是 Python 的 amqp 支持的任何 AMPQ 消息队列。新的 Folsom 版本支持 Zero MQ。

SQL database：存储云基础设施的编译时和运行时的状态。这包括可用的实例类型，在使用中的实例，可用的网络和项目。从理论上讲，OpenStack Nova 可以支持任何 SQLAlchemy 支持的数据库，但是目前被广泛使用的数据库仅仅有 sqlite3 (只适用于测试和开发工作)，MySQL 和 PostgreSQL。

Nova 还提供控制台的服务，让最终用户通过代理服务器访问他们的虚拟实例的控制台。这涉及到多个守护进程 (nova-console, nova-vncproxy 和

nova-consoleauth)。

图 A.1 显示了 Nova 中的服务组件架构以及服务组件之间的通信系统。

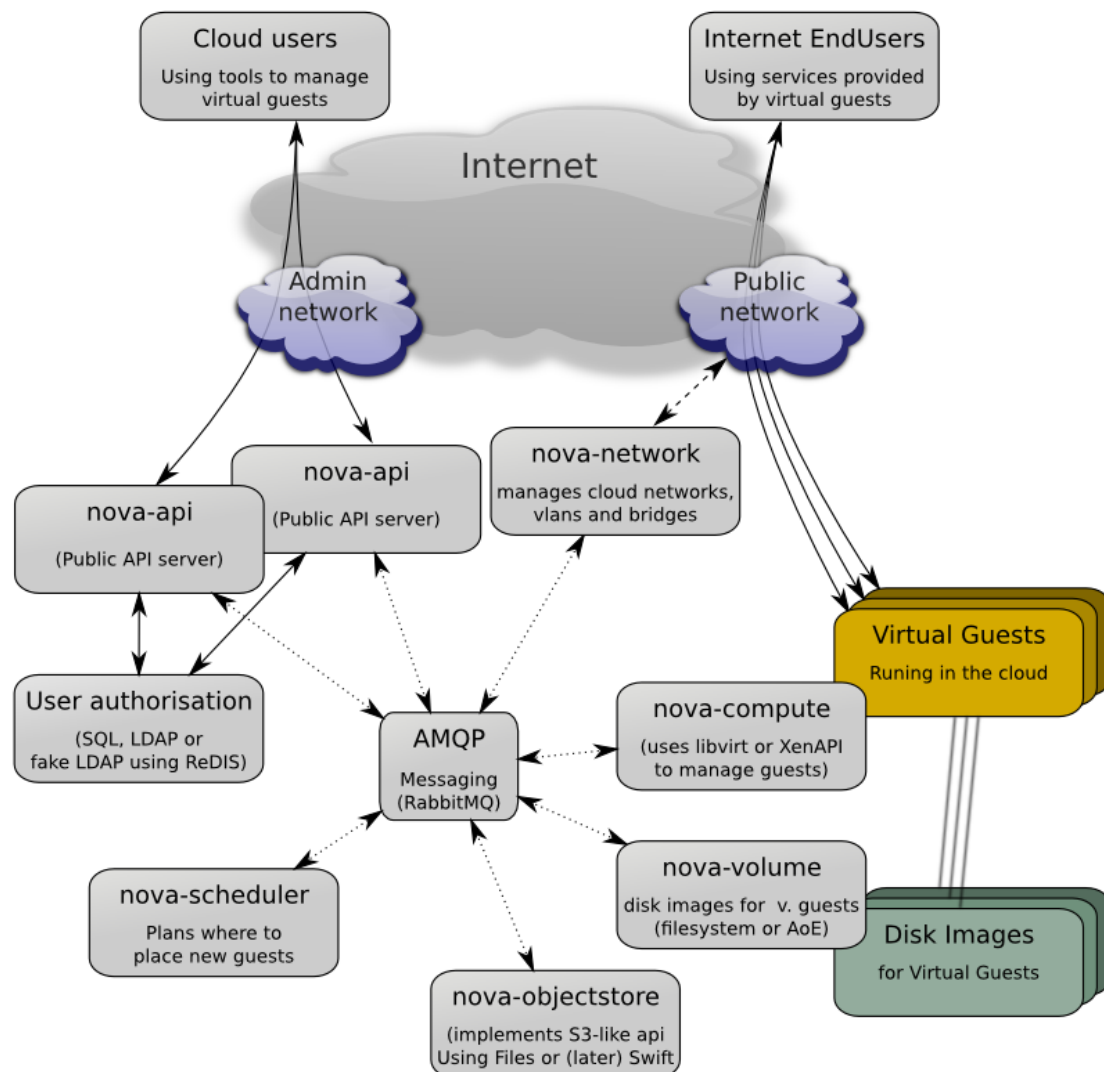


图 A.1 OpenStack Compute 服务架构图

A.3 OpenStack Object Storage

OpenStack Object Storage (Swift) 使用普通的服务器来构建冗余的、可扩展的分布式对象存储集群，存储容量可达 PB 级。Swift 的是用 Python 开发，前身是 Rackspace Cloud Files 项目，随着 Rackspace 加入到 OpenStack 社区，Racksapce 也将 Cloud Files 的代码贡献给了社区，并逐渐形成现在 Swift。

Swift 使用 RESTful API 对外提供服务，包含的功能如下：

- Account (存储账户) 的 GET、HEAD
- Container (存储容器，与 S3 的 bucket 相同) 的 GET、PUT、HEAD、DELETE

- Object（存储对象）的 GET、PUT、HEAD、DELETE、DELETE
- Account、Container、Object 的元数据支持
- 大文件（无上限，单个无文件最大 5G，大于 5G 的文件在客户端切分上传，并上传 manifest 文件）
- 访问控制、权限控制
- 临时对象存储（过期对象自动删除）
- 存储请求速率限制
- 临时链接（让任何用户访问对象，不需要使用 Token）
- 表单提交（直接从 HTML 表单上传文件到 Swift 存储，依赖与临时链接）
- 静态 WEB 站点（用 Swift 作为静态站点的 WEB 服务器）

Swift 的基础架构如图 A.2 所示。

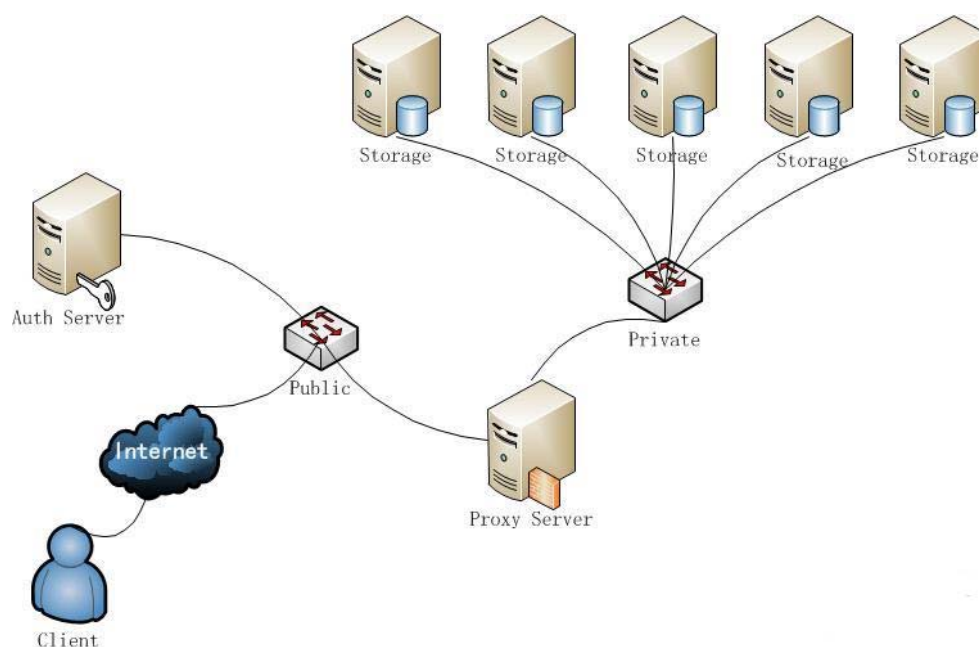


图 A.2 Swift 基础架构图

A.4 OpenStack Image Service

OpenStack Image Service 包括两个主要的部分，分别是 API server 和 Registry server(s)。

OpenStack Image Service 的设计，尽可能适合各种后端仓储和注册数据库方案。API Server（运行“glance api”程序）起通信 hub 的作用。比如各种各样的客户程序，镜像元数据的注册，实际包含虚拟机镜像数据的存储系统，都是

通过它来进行通信的。API server 转发客户端的请求到镜像元数据注册处和它的后端仓储。OpenStack Image Service 就是通过这些机制来实际保存进来的虚拟机镜像的。

OpenStack Image Service 支持的后端仓储有：

- a) OpenStack Object Storage。它是 OpenStack 中高可用的对象存储项目。
- b) FileSystem。OpenStack Image Service 存储虚拟机镜像的默认后端是后端文件系统。这个简单的后端会把镜像文件写到本地文件系统。
- c) S3。该后端允许 OpenStack Image Service 存储虚拟机镜像在 Amazon S3 服务中。
- d) HTTP。OpenStack Image Service 能通过 HTTP 在 Internet 上读取可用的虚拟机镜像。这种存储方式是只读的。

附录 B 国际标准化组织和协会的主要工作

B.1 ISO/IEC JTC1/SC7 简介

全称	软件和系统工程分技术委员会 Software and Systems Engineering
简称	SC7
官方网站	http://www.jtc1-sc7.org/
成立时间	1987 年
主要成员	新西兰（召集人）、中国（联合召集人）、印度（联合召集人）、西班牙、法国、爱尔兰、国际 IT 服务管理联盟。
主要活动	1. 2009 年 5 月成立了“云计算中 IT 治理研究组”，以研究分析市场对于 IT 治理中的云计算标准需求，并提出 JTC1/SC7 内的云计算标准目标及内容。 2. 2010 年 5 月的 SC7 全会上，此研究组重新更名为“云计算治理研究组”，并继续延续一年。
主要成果	《ISO/IEC 20000-1 在云计算中运用》

B.2 ISO/IEC JTC1/SC27 简介

全称	信息安全分技术委员会 ISO/IEC JTC1 SC27
简称	SC27
官方网站	http://www.iso.org/iso/iso_technical_committee?commid=45306
成立时间	成立于 1990 年
主要成员	美国，中国，加拿大、澳大利亚，德国，法国，丹麦等
主要成果	《基于 ISO/IEC 27002 的云计算服务的信息安全控制措施实用规则》 《公有云服务的数据保护控制实用规则》 《供应商关信息安全-第 4 部分 云服务安全指南》

B.3 ISO/IEC JTC1/SC38 简介

全称	分布应用平台服务分技术委员会 Distributed application platforms and services
简称	SC38
官方网站	http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=601355
成立时间	2009 年
主要成员	韩国（召集人）、瑞典（联合召集人）、及其他有兴趣的国家成员体；ISO 内的其他有兴趣的标准化组织及云计算协会。
主要活动	<ol style="list-style-type: none"> 2009 年在以色列特拉维夫召开的 JTC1 全会上宣布成立 SC38 工作组。该分会下设两个工作组和一个研究组：Web Service 工作组、SOA 工作组和云计算研究组。云计算研究组研究分析市场对于云计算标准的需求，与云计算相关的其他标准化组织或协会沟通，并确立 JTC1 内的云计算标准内容。 2012 年 SC38 成立了云计算工作组（WG3）。
主要成果	<ol style="list-style-type: none"> WG3 与 ITU-T 形成联合工作组共同推出《云计算概述和词汇》与《云计算参考架构》两项标准，目前这两项标准均处于 DIS 投票阶段。 WG3 新工作项目有《云计算 SLA 框架和术语》。

B.4 ISO/IEC JTC1/SC39 简介

全称	信息技术可持续发展分技术委员会 Sustainability for and by Information Technology
简称	SC39
官方网站	http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=654019
成立时间	2012 年
主要成员	美国，比利时，加拿大，中国等 16 家正式成员，4 家观察成员
主要活动	<ol style="list-style-type: none"> 2012 年 6 月 12~14 日，ISO/IEC JTC1/SC39 信息技术可持续发展委员会在美国旧金山召开成立以来的首次年会。参加会议的有来自加拿大、中国、芬兰、法国、德国、爱尔兰、日本、韩国、挪威、英国、美国等国家成员体，以及来自 Ecma international 等联络组织的 40 余名代表。

B.5 ITU-T SG13 简介

全称	多协议和 IP 的网络及其互通研究组 ITU-T SG13
简称	ITU-T SG13
官方网站	http://www.itu.int/ITU-T
成立时间	2011 年，由 ITU-T FGCC（云计算焦点组）转化而来
主要成员	相关成员及 3GPP，IETF 等组织
主要活动	“云计算专项工作组”旨在达成一个全球性生态系统，确保各个系统之间安全地交换信息，明确能促进电信/ICT 支持云计算的相关标准开发及优先工作，熟悉 ITU-T 及标准化团体中相关电信/ICT 支持云计算所带来的新特性和新挑战，分析云计算特性、功能所带来的变化，以评估电信/ICT 开展相关云计算标准化的合适时间。
主要成果	<ol style="list-style-type: none"> 《云计算安全框架》、《云计算身份管理要求》、《云计算框架&优先要求》、《云计算基础设施要求》、《E2e 云资源管理框架》、《云计算概述和词汇》、《互联云架构》、《云计算参考架构》、《DaaS 参考架构要求》等标准，其中《云计算概述和词汇》与《云计算参考架构》两项标准与 ISO/IEC JTC1 SC38 成立联合工作组共同制定。 《云生态系统介绍》、《功能要求和参考架构》、《云基础设施参考架构要求》、《云资源管理缺口分析》、《云安全》、《云计算相关 SD0s 综述》、《云在电信和 ICT 产业的收益》等报告或白皮书

B.6 分布式管理任务组（DMTF）简介

全称	分布式管理任务组 Distributed Management Task Force
简称	DMTF
官方网站	www.dmtf.org
成立时间	1992 年
主要成员	AMD、CISCO、CITRIX、EMC、HP、IBM、Intel、Microsoft、Novell、Redhat、Sun、VMWare、Savvis 等
主要活动	1. 2009 年 4 月 27 日，DMTF 在美国波特兰（俄勒冈州）宣布成立 DMTF 开放云标准孵化器，该研究组关注云计算管理方面的标准，通过制定

	<p>云资源管理的协议、封装格式和安全机制来制定互操作标准。</p> <ol style="list-style-type: none"> 成立云管理工作组，致力于改善云服务提供者和云服务使用者之间，以及云服务提供者和云服务开发者之间在云管理方面的互操作性。 成立云审计联合工作组 成立软件授权工作组 成立开发虚拟化工作组
主要成果	<ol style="list-style-type: none"> 《开放虚拟化格式规范（OVF）》 《开放虚拟化格式规范（OVF）2.0》 《云基础设施管理接口模型和 HTTP 规范下的 REST 接口》 《云基础设施管理接口-通用无条件模型》 《互操作云白皮书》 《云管理体系结构》 《云管理中的用户案例和交互流程》 《通用信息模型》

B.7 云安全联盟（CSA）简介

全称	云安全联盟 Cloud Security Alliance
简称	CSA
官方网站	http://www.cloudsecurityalliance.org/
成立时间	2009 年
主要成员	eBay, ING, Qualys, PGP, zScaler 等
主要活动	CSA 是提供云计算安全保障的非盈利性组织。成立了 10 个工作组：结构及框架工作组（Architecture and Framework），主要负责技术结构和相关框架定义的研究；GRC, Audit, Physical, BCM, DR 工作组，主要负责管理、风险控制、适应性、审计、传统及物理安全性、业务连续性管理和灾难恢复方面的研究；法律及电子发现工作组（Legal and eDiscovery），主要负责法律指导、合约问题、全球法律、电子发现及相关问题的研究；可移植性、互操作性及应用安全工作组（Portability, Interoperability and Application Security），主要负责应用层的安全问题研究并制定促进云服务提供商间互操作性及可移植性发展的指导意见；身份与接入管理、加密与密钥管理工作组（Identity and Access Mgt, Encryption & Key

	<p>Mgt), 主要负责身份及访问管理、密码及密钥管理问题的研究以及明确企业整合中出现的新问题及解决方案; 数据中心运行及事故响应工作组 (Data Center Operations and Incident Response), 主要负责事故响应及取证问题的研究, 并明确基于云的数据中心在运行中出现的相关新问题; 信息生命周期管理及存储工作组 (Information Lifecycle Management and Storage), 主要负责云数据相关问题的研究; 虚拟化及技术分类工作组 (Virtualization and Technology Compartmentalization), 主要负责如何对技术进行分类, 包括但也不局限于虚拟化技术; 安全即服务工作组 (Security as a Service), 主要负责研究如何通过云模式来提供安全解决方案; 一致性评估工作组 (Consensus Assessments Initiative), 主要负责研究用于对云服务提供商进行一致性检验的工具和流程。</p>
主要成果	<ol style="list-style-type: none"> 1. 《云计算关键领域安全指南 V2.1》 2. 《云控制矩阵》 3. 《云信任协议》 4. 《云审计》 5. 《隐私水平协议》 6. 《参考架构-可信云计划》 7. 《云计算的主要安全威胁报告》 8. 《开放认证构架》 9. 《云计算重点关键领域安全指南》 10. 《共识评估计划调查问卷》 11. 《安全即服务》 12. 《CSA 云控制模型》 13. 《身份识别和访问控制管理手册 v2.1》 14. 《CSA 报告》

B.8 欧洲电信标准研究所 (ETSI TC GRID) 简介

全称	<p>欧洲电信标准研究所网格技术委员会</p> <p>The European Telecommunications Standards Institute TC Grid</p>
简称	ETSI TC Grid
官方网站	http://www.etsi.org/
成立时间	1982

主要成员	涉及电信行政管理机构、国家标准化组织、网络运营商、设备制造商、专用网业务提供者、用户研究机构等
主要活动	ESTI STF 331 网格技术委员会主要是提供解决 IT 和电信产业的互操作方案。他们的关注点不仅仅是使用网格计算技术，而且还融入了云计算技术的电子商务平台，强调 IaaS 的交付模型。
主要成果	<ol style="list-style-type: none"> 1. 《网格计算和云计算技术：互操作和通信标准》 2. 《NFV 系列标准》 3. 《云计算在其他领域作为一种技术进行减少排放》 4. 《ICT 网络互操作性差异研究：ICT 利益相关者目录》 5. 《ICT 网络互操作性差异研究：互操作性差异和已有解决方案》 6. 《ICT 网络互操作性测试框架和现有 ICT 网络互操作性解决方案调查》 7. 《网格服务和电信网络：架构选项》 8. 《对云服务标准要求初始分析》 9. 《云服务的 SLA》 10. 云个人用户的建议 11. 合法监听系列标准 12. 电信服务质量系列标准

B.9 美国国家标准与技术研究院（NIST）简介



全称	美国国家标准与技术研究院 National Institute of Standards and Technology
简称	NIST
官方网站	http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
成立时间	1901 年
主要成员	美国 NIST 相关成员
主要活动	NIST 在云计算方面主要是通过技术引导和推进标准化工作来帮助政府和行业安全有效的使用云计算技术。NIST 成立了以下工作组：云计算参考架构和分类工作组，旨在促进云计算应用的标准推进工作组，云计算安全工作组，云计算标准路线图工作组和云计算业务用例工作组。
主要成果	<ol style="list-style-type: none"> 1. 《NIST 云计算术语定义 v15》 2. 《NIST 云计算参考架构》 3. 《美国政府技术路线图卷 1(1.0) 》

	4. 《美国政府技术路线图卷 2(1.0)》
	5. 《安全控制》

B.10 开放网格论坛开放云计算接口工作组（OGF OCCI-WG）简介

全称	开放式网格论坛开放云计算接口工作组 Open Grid Forum Open Cloud Computing Interface
简称	OGF OCCI-WG
官方网站	http://www.ogf.org/gf/group_info/charter.php?review&group=occi-wg
成立时间	开放式网格论坛是一个面向全球从事网格计算标准的国际协会，该协会在 2006 年由原来的全球网格论坛（the Global Grid Forum）和企业网格联盟（the Enterprise Grid Alliance）两个协会合并而成。
主要成员	Microsoft, Sun, Oracle, Fujitsu, Hitachi, IBM, Intel, HP, AT&T, eBay 等
主要活动	1、2009 年 4 月成立 OCCI 工作组（OCCI-WG），该工作组的目标是创建一个实用的 IaaS 接口解决方案—OCCI。这个接口方案将覆盖 IaaS 的使用、监督和定义；
主要成果	1、《OCCI(Open Cloud Computing Interface)》 2、《OCCI-云 API 的用例和需求分析》 3、《开放云计算接口系列标准》 4、《网络服务协议》 5、《网络服务协议协商》

B.11 全球网络存储工业协会（SNIA）简介



全称	全球网络存储工业协会 Storage Networking Industry Association
简称	SNIA
官方网站	http://www.snia.org/home/
成立时间	1997

主要成员	SNIA 是全球非盈利性组织，包括约 400 名会员，如 ActiFio, Bycast, Calsoft, Cisco, EMC, GoGrid, HCL Technologies, Hitachi Data Systems, HP, IBM, Intransa Joyent LSI Corporation, NetApp Nirvanix, Patni Computer Systems Ltd., Sun, Symantec, VMware, Xyratex 等。
主要活动	<p>2009 年 4 月 6 日 SNIA 在 SNW 网络存储世界春季大会上宣布成立云存储技术工作组，旨在为 SNIA 开发一套云存储的系统和接口标准。</p> <p>2010 年 4 月 SNIA 云存储技术工作组发布云数据管理接口（CDMI）草案 1.0 版本，其中包括了 SNIA 云存储的参考模型以及基于这个参考模型的 CDMI 参考模型。SNIA 希望为云存储和云管理提供相应的应用程序接口并向 ANSI 和 ISO 提交这些标准。</p>
主要成果	<ol style="list-style-type: none"> 1. 《SNIA 云数据管理接口规范 1.0》； 2. 《云存储白皮书》。

B.12 开放云计算联盟（OCC）简介



全称	开放云计算联盟 The Open Cloud Consortium
简称	OCC
官方网站	http://opencloudconsortium.org/
成立时间	2009 年
主要成员	Cisco, MIT 林肯实验室, Yahoo, 各个大学（包括芝加哥的伊利诺斯州大学）
主要活动	<p>OCC 是致力于云计算、跨云互操作框架的标准和云计算的基准测试、云计算的相关实施技术的支持。目前包括三个工作组来做以上工作：</p> <ol style="list-style-type: none"> 1. 大规模数据云的标准和互操作； 2. 开放云测试台工作组； 3. 开放科学数据云工作组； 4. 跨云测试平台工作组。
主要成果	《数据密集型计算的基准测试》

B.13 结构化信息标准促进组织（OASIS）简介

全称	结构化信息标准促进组织 Organization for the Advancement of Structured Information Standards
简称	OASIS
官方网站	http://www.oasis-open.org
成立时间	1993 年
主要活动	<ol style="list-style-type: none"> 1. 成立云技术委员会 IDCloud TC (OASIS Identity in the Cloud Technical Committee)。该技术委员会定位于云计算中的识别管理 (identity management) 安全，具体包括识别现有识别管理标准中的问题，调查跨云互操作需求，对收集用例进行风险分析。 2. 症状自动化框架 SAF (Symptoms Automation Framework)。云计算加重了基于消费者的业务需求和基于供应商的资讯反馈之间的隔离。SAF 方便不同领域的知识共享，让消费者和供应商共同协作，以最大限度地提高服务质量，降低成本。
主要成果	<ol style="list-style-type: none"> 1. 《云应用管理平台》 2. 《云应用程序拓扑和编排规范》 3. 《开放数据协议》 4. 《键值数据存储》 5. 《云用例定义》 6. 《云 PaaS 属性定义》 7. 《云外包属性定义》

B.14 开放组群（TOG）简介

全称	开放组群 The Open Group
简称	TOG
官方网站	http://www.opengroup.org
主要活动	成立云计算工作组，该工作组已经开展了以下项目： <ol style="list-style-type: none"> 1. 业务用例云； 2. 商业构件云；

	3. 云计算体系结构； 4. 面向服务的云计算基础设施； 5. 云中的安全。 另外，工作组计划提供一套工具和模板，帮助企业进行云计算方面的决策，具体工具和模板如下： 1. 云业务用例模板； 2. 买家云分类； 3. 卖家云分类； 4. 云财政和投资回报率模板； 5. 云商业应用策略； 6. 商业云定义。
主要成果	1. 《从云计算中构建投资回报率 V1.0》 2. 《云消费者决策树》 3. 《用于使用云的增强商业用例。》

B.15 零售行业技术标准协会（ARTS）简介

全称	零售行业技术标准协会 Association for Retail Technology Standards
简称	ARTS
官方网站	http://www.nrf-arts.org/
成立时间	1993 年
主要活动	ARTS 是一个零售商为主导的会员组织，致力于创建一个开放的环境，通过零售商和技术供应商的合作共创国际零售技术标准。
主要成果	《云计算白皮书》

B.16 电气与电子工程学会标准协会（IEEE SA）简介

全称	电气与电子工程师学会标准协会 The Institute of Electrical and Electronics Engineers Standards Association
简称	IEEE SA
官方网站	http://standards.ieee.org/

成立时间	2010
主要活动	IEEE SA 和 CSA 合作致力于云安全方面的标准研究
主要成果	《云内互操作和联邦标准》

B.17 云计算互操作论坛（CCIF）简介

全称	云计算互操作论坛 Cloud Computing Interoperability Forum
简称	CCIF
官方网站	http://www.cloudforum.org
主要成员	Cisco, Intel, Thomson Reuters, Orange, Sun, IBM, RSA 等
主要活动	2009 年 4 月 2 日举办华尔街云计算互操作论坛

B.18 开放云计算宣言（OCM）简介

全称	开放云计算宣言 Open Cloud Manifesto
简称	OCM
官方网站	http://www.opencloudmanifesto.org/
主要成员	目前已有 300 多家单位参与。
主要成果	《开放云计算宣言》

B.19 云计算用户案例讨论组（CCUCDG）简介

全称	云计算用户案例讨论组 Cloud Computing Use Case Discussion Group
简称	CCUCDG
官方网站	http://cloudusecases.org/
主要活动	定义云计算的通用用例
主要成果	《云计算用例白皮书 V4.0》

B.20 云审计（CloudAudit）简介

全称	云审计 CloudAudit and the Automated Audit, Assertion, Assessment, and Assurance API (A6)
简称	CloudAudit
官方网站	http://www.cloudaudit.org
成立时间	2010.1
主要成果	《云审计》

B.21 OMG 云标准协调组（OMG Cloud Standards Coordination）简介

全称	对象管理组云计算标准协调组 Object Management Group Cloud Standards Coordination
官方网站	http://www.omg.org/
主要活动	1. 2009 年 3 月举办 Strategies and Technologies for Cloud Computing Interoperability (SATCCI) workshop 2. 2009 年 7 月举办云标准峰会 3. 2009 年 12 月举办云互操作会议

B.22 因特网工程任务组（IETF）简介

全称	因特网工程任务组 Internet Engineering Task Force
简称	IETF
官方网站	http://www.ietf.org
主要活动	IETF-77 云计算讨论会 http://www.ietf.org/mail-archive/web/clouds
主要成果	1. 《访问云服务》 2. 《云参考架构》 3. 《云审计》

	4. 《应用层流量优化》 5. 《3 层虚拟室友网络》 6. 《网络虚拟化覆盖》 7. 《web 认证协议》 8. 《跨域身份识别管理系统》 9. 《Ip 性能度量》
--	--

B.23 全球跨云技术论坛（GICTF）简介

全称	全球跨云技术论坛 Global Inter-Cloud Technology Forum, Japan
简称	GICTF
官方网站	http://www.gictf.jp/index_e.html
成立时间	2009.07
主要成果	1. 《跨云用例和功能需求白皮书》 2. 《对于云内计算的用例和功能要求》 3. 《云内网络的技术要求》 4. 《云内接口技术要求 数据模型》 5. 《云内接口技术要求 协议》

B.24 TM Forum 云服务启动组简介

全称	TM Forum 云服务启动组 TM Forum Enabling Cloud Service Initiative
官方网站	http://www.tmforum.org
简称	TM Forum
成员	大型 IT 企业、电信运营商等
主要活动	目前该小组开展的主要工作包括： 1. 《云业务处理架构》 2. 《云服务定义和分类》 3. 《云计费兴趣组》 4. 《云 SLA 管理》 5. 《企业云领导委员会》

主要成果	<ol style="list-style-type: none"> 1. 《SLA 管理手册》 2. 《云快速启动包：解决故障》 3. 《云 SLA 操作说明书》 4. 《企业组 IaaS 需求》 5. 《云业务模型》 6. 《TMF 企业组对外计算 IaaS 需求》 7. 《参考实现》 8. 《支持端到端的云 SLA 管理》 9. 《混合云服务管理包-简介》 10. 《混合云服务管理包-业务指南》 11. 《合作伙伴和 B2B2X 最佳实践概述》 12. 《合作伙伴和 B2B2X 最佳实践合作-概念和案例》 13. 《合作指导手册-按步指导》 14. 《B2B2X 合作开发包》 15. 《RST API 区》 16. 《混合云服务管理包-业务指南》
------	--

B.25 亚洲云计算协会（ACCA）简介

全称	亚洲云计算协会 Asia cloud computing association
简称	ACCA
官方网站	http://www.asiacloud.org/index.php
成立时间	2010 年
主要活动	成立以下小组： <ol style="list-style-type: none"> 1. 《公共政策法规工作组》 2. 《安全工作组》 3. 《云分类工作组》 4. 《电信级应用级云工作组》

B.26 世界无线通讯解决方案联盟（ATIS）简介

全称	世界无线通讯解决方案联盟
----	--------------

	Alliance for Telecommunications Industry Solutions
简称	ATIS
官方网站	http://www.atis.org/
主要成果	<ol style="list-style-type: none"> 1. 《CDN 互联用例规范和高层次需求》 2. 《CDN 互联用例和基于多点传送内容分发要求》 3. 《电信服务云框架》 4. 《虚拟桌面要求》 5. 《可信信息交换》 6. 《云服务生命周期目录》 7. 《CDN 互联用例和多参与方联合环境要求》 8. 《ATIS 命名规则》 9. ATIS XML 模式开发指南

B.27 开放数据中心联盟（ODCA）简介

全称	开放数据中心联盟 Open Data Center Alliance
简称	ODCA
官方网站	http://www.opendatacenteralliance.org/
成立时间	2010 年
主要成果	<ol style="list-style-type: none"> 1. 《控制使用模型系列标准》 2. 《用法：数据安全框架》 3. 《混合云环境虚拟机互操作性》 4. 《用法：IaaS 标准衡量单位》

B.28 云标准客户委员会（CSCC）简介

全称	云标准客户委员会 Cloud Standard Customer Council
简称	CSCC
官方网站	http://www.cloud-council.org/
成立时间	2011 年
主要成果	<ol style="list-style-type: none"> 1. 《云计算实践指南》

	2. 《云计算级别协议指南》 3. 《云计算安全：确保成功的 10 步》 4. 《公共云服务协议：期望和谈判内容》 5. 《云安全标准：期望和谈判内容》
--	---

B.29 欧洲云行业联盟（EuroCloud）简介

全称	欧洲云行业联盟 EuroCloud
简称	EuroCloud
官方网站	http://www.eurocloud.org/
主要成果	《欧洲云审计》

B.30 欧洲网络和信息安全协会（ENISA）简介

全称	欧洲网络和信息安全协会 European Network and Information Security Agency
简称	ENISA
官方网站	http://www.enisa.europa.eu/
成立时间	2004
主要活动	<p>2011 年 10 月 ENISA 发布新指南，就成功打造有效的公私合作、构建弹性的 IT 安全提出了 36 条建议。该指南将 PPP (Public-Private-Partnerships, 公私合作, 以下简称 PPP) 按照安全和复原能力分成 3 类：预防为主的、反应为主的以及保护伞 PPP。指南整合了 PPP 分类并进行验证，以下是供参考的 5 个主要组成部分：为何建立 PPP、谁应当参与其中、应当如何管理 PPP、应该提供何种服务和激励措施、何时应当建立 PPP 以及其他时间选择问题。这些结果基于对 20 个国家的公私行业股东的 30 份调查问卷及 15 次深谈。指南还对来自美国、加拿大和澳大利亚的 PPP 进行了描述，确定信息共享的关键成功因素，指出了国际协作之路。</p> <p>2012 年 4 月 5 日，ENISA 公布了一项新的云计算服务操作指导办法：云计算合同监测指南。ENISA 于 2009 年启动相关研究工作，提出了云计算服务安全保障框架和工具包，使计算机团队对云计算服务提供商进行预评</p>

	估，确定是否采购其所提供的服务。在此基础上，ENISA 制定了新的“云计算合同监测指南”。新指南重点关注公共服务领域的合同，将评估工作贯穿整个合同期，详述了如何在云计算服务合同期内对服务的安全性进行检查。
主要成果	《过程安全-云合约安全服务水平监控指南》

B.31 韩国云计算论坛（CCFK）简介

全称	韩国云计算论坛 Cloud Computing Forum in Korea
简称	CCFK
主要活动	韩国云计算标准化工作由“云计算标准论坛”领导，与韩国通信委员会（Korea Communications Commission）和知识经济部（Ministry of Knowledge Economy）展开合作，同时由通信技术协会（Telecommunication Technology Association）和韩国技术与标准机构（Korean Agency for Technology and Standards）共同赞助下展开的。

B.32 韩国云服务联盟（KCSA）简介

全称	韩国云服务联盟 Korea Cloud Service Association
简称	KCSA
主要活动	韩国云服务协会是韩国云计算领域的重要组织之一。该协会分为政策部、云技术部、云服务部、云安全部和云试验平台预研。政策部进行云政策研究、政府计划、Billing & SLA 合同研究；云技术部讨论云技术：虚拟、平台栈、IaaS 栈、内容交付网络，全球 loadbalance，分布式系统监控和管理，网格中间件；云服务部进行云服务模式、web2.0、SLA、政策研究、政府计划、Billing & SLA 合同研究。

B.33 云计算战略研究小组（CSRT）简介

全称	云计算战略研究小组 Cloud Strategy Research Team
简称	CSRT
主要活动	日本 OSS 推进联盟专门成立了云计算战略研究小组（Cloud Strategy Research Team），研究云计算发展，领导开展相关云计算项目，其中长期战略组负责社会云评估，短期战略组负责私有云开源软件栈评估，并且其分小组已向 IPA 提交了技术问题，IPA 在本年度特别资助了 5 个云计算研究项目，包括： 1) 编制私有云 OSS 目录 2) KVM 性能/可靠性评估 3) OpenJDK 可靠性评估 4) OSS 云系统管理可靠性评估：Eucalyptus, OpenLDAP, OpenSSO, 系统管理软件 5) 研究 VM 控制界面规范

参考文献

- [1] ACM SIGCOMM Computer Communication Review, Volume 39, Number 1, January 2009. A Break in the Clouds: Towards a Cloud Definition.
- [2] <http://www.nist.gov/itl/csd/cloud-102511.cfm>
- [3] Report of JTC 1/SWG-P on possible future work on Cloud Computing in JTC 1
- [4] http://en.wikipedia.org/wiki/Cloud_computing
- [5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia: Above the Clouds: A Berkeley View of Cloud Computing (美国加州大学伯克利分校—在云端:伯克利认为的云计算) UC Berkeley Reliable Adaptive Distributed Systems Laboratory [http://radlab.cs.berkeley.edu/February 10, 2009](http://radlab.cs.berkeley.edu/February_10,_2009)
- [6] <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>
- [7] <http://cloud-standards.org>
- [8] OpenStack Object Storage Developer Guide.<http://docs.OpenStack.org/>
- [9] OpenStack Compute Administration Manual.
<http://docs.OpenStack.org/cactus/OpenStack-compute/admin/content>.
- [10] Practical Guide to Cloud Computing Version 1.0.
- [11] Practical Guide to Service Level Agreements Version 1.0
- [12] Security for Cloud Computing 10 Steps to Ensure Success