ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0166—2020
代替 JR/T 0166—2018

云计算技术金融应用规范　技术架构

Financial application specification of cloud computing technology——
Technical architectures

2020－10－16 发布　　2020－10－16 实施

中国人民银行　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替JR/T 0166—2018《云计算技术金融应用规范 技术架构》，与JR/T 0166—2018相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了金融云的定义（见3.11）；

——增加了在云计算部署中金融机构与云服务提供者相关责任(见 5.2)；

——增加了金融云机房建设标准符合性要求（见 7.2.2）；

——更改了虚拟机全生命周期管理功能（见 7.4.2.1，2018 年版的 7.4.2.1）。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行科技司、中国人民银行成都分行、中国人民银行广州分行、中国人民银行西安分行、中国金融电子化公司、网联清算有限公司、中国银联股份有限公司、中国工商银行、中国农业银行、中国银行、中国建设银行、招商银行、中国光大银行、中国民生银行、兴业银行、平安银行、国泰君安证券股份有限公司、华泰证券股份有限公司、中国人寿保险（集团）公司、中国人民保险集团股份有限公司、中国互联网金融协会、中国人民银行德阳市中心支行、财付通支付科技有限公司、蚂蚁科技集团股份有限公司、华为技术有限公司、阿里云计算有限公司、京东数字科技控股股份有限公司、北京百度网讯科技有限公司、新华三技术有限公司、兴业数字金融服务（上海）股份有限公司、亚马逊通技术服务（北京）有限公司、北京中金国盛认证有限公司、北京金融科技产业联盟、中金金融认证中心有限公司、北京银联金卡科技有限公司、北京软件产品质量检测检验中心。

本文件主要起草人：李伟、李兴锋、强群力、涂晓军、张宏基、孙维挺、侯晓晨、邬向阳、班廷伦、杨倩、聂丽琴、王力、王岚、郭林、韩韬、雷平、张海燕、唐辉、胡达川、朱勇、周国林、辛路、杨彬、陈则栋、刘运、杨硕飞、田昆、吴永强、吴金海、符海芳、赵华、赵春华、张翰林、李佐鸿、陈章龙、庄勇、孔令斌、白阳、蒋增增、钟琪、孔昊、于柳绮、刘力慷、薛松源、宋铮、邓峰、李进、张文涛、杜辉、侯大鹏、郑子洲、周伟然、居未伟、王超、李义高、胥少龙、来宾、陈永杰、王宇翔、陈晨、陈雪秀、曹伟、戴蕾、穆冬生、宋杰、瞿红来、张宪铎、王晓燕、李明凯、莫云飞、陈当阳、金千里、张亮、刘刚、陈当阳、高坤、樊华、张峻华、杨俊、郝轶、罗子强、雷佳杰、张国泽、许涛、赵波、渠韶光、贾铮、李博文、王绍斌、李国俊、王展、张荣典、王仕、杨德娜、种毓鑫、孔令俊、张寿元、张峻华、胡仲海、董亮、苏晗、高天游、金怡、王研娟、林春、闫莅、焦振新、蔡志玮。

本文件及其所替代文件的历次版本发布情况为：

——2018年首次发布为JR/T 0166—2018，本次为第1次修订。

引　言

本文件是云计算技术金融应用系列标准之一，云计算技术金融应用系列标准包括：

——《云计算技术金融应用规范 技术架构》；

——《云计算技术金融应用规范 安全技术要求》；

——《云计算技术金融应用规范 容灾》。

云计算技术金融应用规范　技术架构

1　范围

本文件规定了金融领域云计算平台的技术架构要求，涵盖云计算的服务类别、部署模式、参与方、架构特性和架构体系等内容。

本文件适用于金融领域的云服务提供者、云服务使用者、云服务合作者等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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　信息技术　云计算　概览与词汇

GB 50174　数据中心设计规范

JR/T 0071　金融行业信息系统信息安全等级保护实施指引

JR/T 0131　金融业信息系统机房动力系统规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

参与方　party

1个或1组自然人或法人，无论该法人是否注册。

[来源：GB/T 32400，3.1.6]

3.2

云计算　cloud computing

1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。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源：GB/T 32400，3.2.5]

3.3

云服务　cloud service

通过云计算已定义的接口提供的1种或多种能力。

[来源：GB/T 32400，3.2.8]

3.4

云服务提供者　cloud service provider

提供云服务的参与方。
[来源：GB/T 32400，3.2.15]

3.5

云服务使用者 cloud service consumer

使用云服务的参与方。

3.6

云服务合作者 cloud service partner

支撑或协助云服务提供者活动、云服务使用者活动或者两者共同活动的参与方。

3.7

云服务审计者 cloud service auditor

负责审计云服务的供应和使用的云服务参与方。

3.8

云计算平台 cloud computing platform

云服务提供者和云服务合作者提供的云计算基础设施及其上服务软件的集合。

3.9

私有云 private cloud

仅被1个云服务使用者使用，且资源被该云服务使用者控制的1种云部署模式。

3.10

团体云 community cloud

由1组特定的云服务使用者使用和共享，且资源被云服务提供者或使用者控制的1种云部署模式，云服务提供者和使用者在监管政策、安全要求等方面相同或高度相似。

3.11

金融团体云 financial community cloud

又称金融云
仅供金融机构共享使用，承载金融业务系统的团体云。

3.12

公有云 public cloud

可被任意云服务使用者使用，且资源被云服务提供者控制的1种云部署模式。

3.13

混合云 hybrid cloud

包含2种及以上部署模式的云部署模式。

3.14

基础设施即服务 infrastructure as a service

云服务使用者提供云能力类型中的基础设施能力类型的1种云服务类别。

3.15

平台即服务 platform as a service

云服务使用者提供云能力类型中的平台能力类型的1种云服务类别。

3.16

软件即服务 software as a service

云服务使用者提供云能力类型中的应用能力类型的1种云服务类别。

3.17

租户 tenant

对1组物理和虚拟资源进行共享访问的1个或多个云服务使用者。

3.18

多租户 multi-tenancy

通过对物理或虚拟资源的分配实现多个租户以及他们的计算和数据彼此隔离和不可访问。

[来源：GB/T 32400，3.2.27]

3.19

数据中心 data center

为集中放置的电子信息设备提供运行环境的建筑场所，可以是1栋或几栋建筑物，也可以是1栋建筑物的一部分，包括主机房、辅助区、支持区和行政管理区等。

[来源：GB 50174，2.0.1]

3.20

物理机 physical machine

相对于虚拟机的物理服务器，可为虚拟机提供硬件环境。

3.21

物理机服务 physical machine service

直接向云服务使用者提供物理机的服务。

3.22

虚拟机 virtual machine

通过各种虚拟化技术，为用户提供的与原有物理服务器相同的操作系统和应用程序运行环境的统称。

注：虚拟机通常使用物理服务器的资源，在用户看来它与物理服务器的使用方式完全相同。

3.23

容器 container

通过操作系统虚拟化技术实现的、轻量且隔离的1组进程或资源的运行环境。

3.24

资源池 resource pool

1组物理资源或虚拟资源的集合。

注：按照一定规则可从池中获取资源，也可释放资源并由资源池回收。资源包括物理机、虚拟机、物理存储资源、虚拟存储资源、物理网络资源和虚拟网络资源等。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

CPU：中央处理单元（Central Processing Unit）

DSaaS：数据存储即服务（Data Storage as a Service）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

I/O：输入/输出（Input/Output）

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

NaaS：网络即服务（Network as a Service）

PaaS：平台即服务（Platform as a Service）

QoS：服务质量（Quality of Service）

SaaS：软件即服务（Software as a Service）

SQL：结构化查询语言（Structured Query Language）

TCP：传输控制协议（Transmission Control Protocol）

VPC：虚拟私有云（Virtual Private Cloud）

VPN：虚拟专用网络（Virtual Private Network）

CNAME：别名记录（Canonical Name）

MX：邮件交换记录（Mail Exchanger）

MPI：信息传递接口（Message Passing Interface）

5 概述

5.1 服务类别

云服务主要包括IaaS、PaaS和SaaS，此外根据服务内容还可分为NaaS和DSaaS等具体服务类别。

IaaS提供计算、存储、网络等基础资源服务。云服务使用者可通过管理平台、应用编程接口等使用、监控、管理云计算平台中的资源。

PaaS提供运行在云计算基础设施上的软件开发和运行环境服务。云服务使用者可基于PaaS提供的工具及环境进行系统开发、测试、集成、部署、运行、维护等工作。

SaaS提供运行在云计算基础设施上的应用软件服务，如电子邮箱服务等。

NaaS是为云服务使用者提供传输连接和相关网络能力的1种云服务类别。

DSaaS是为云服务使用者提供配置和使用数据存储及相关能力的1种云服务类别。

5.2 部署模式

金融领域云计算部署模式主要包括私有云、团体云以及由其组成的混合云等。金融机构应秉持安全优先、对用户负责的原则，根据信息系统所承载业务的重要性和数据的敏感性、发生安全事件的危害程度等，充分评估可能存在的风险隐患，谨慎选用与业务系统相适应的部署模式。金融机构是金融业务系统风险管理的责任主体，其应承担的安全责任不因使用云服务而免除或减轻。云服务提供者是云服务的供应者，应对云服务的安全性、可靠性和可用性负责。

5.3 云服务参与方

云服务的参与方包括：

a) 云服务使用者。

b) 云服务提供者。

c) 云服务合作者。

云服务提供者为云服务使用者提供IaaS、PaaS、SaaS等类别的云服务（见图1），并负责云计算平台的建设、运营和管理；云服务使用者基于云服务提供者提供的云服务构建、运行、维护自身的应用系统，或直接使用可作为应用系统的云服务；云服务合作者为云服务提供者、云服务使用者提供支撑或协助。云服务审计者是1种特殊的云服务合作者，应对云服务提供者、云服务使用者、其他云服务合作者进行独立审计。

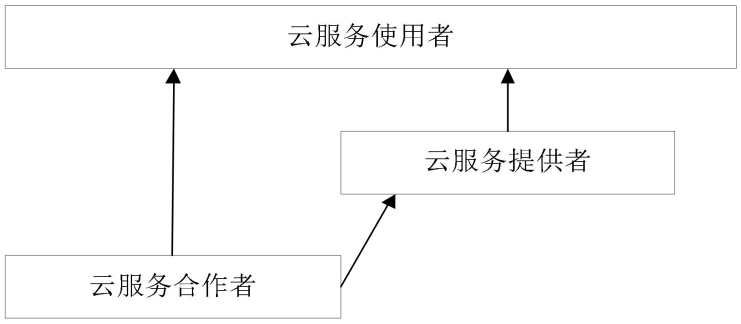

图1 云服务参与方视图

6 架构特性

6.1 高弹性

云计算平台应具备资源弹性伸缩能力。在业务高峰期，云计算平台资源能够快速扩容支持大流量、高并发的金融交易场景；在业务低谷期，云计算平台资源能够合理收缩，避免资源过度配置。

6.2 开放性

云计算平台应采用开放的架构体系，使得云服务使用者不与某个特定的云服务提供者绑定。在云服务使用者中止或变更服务时，云计算平台应支持应用和数据在不同用户信息系统、云计算平台间进行快速便捷迁移。

6.3 互通性

云计算平台应支持通用、规范的通信接口，同一云计算平台内或不同云计算平台间的云服务应能够按需进行安全便捷的信息交互。

6.4 高可用性

云计算平台应具备软件、主机、存储、网络节点、数据中心等层面的高可用保障能力，能够从严重故障或错误中快速恢复，保障应用系统的连续正常运行，满足金融领域业务连续性要求。

6.5 数据安全性

云计算平台应在架构层面保障端到端的数据安全，对用户数据进行全生命周期的严格保护，保证数据在产生、使用、传输和存储等过程中的完整性、可用性和保密性，避免数据的损坏、丢失和泄露。

7 架构体系

7.1 概述

云计算平台架构体系可以分为基础硬件设施与设备、资源抽象与控制、云服务、运维运营管理等部分（见图2），包含：

a) 基础硬件设施与设备主要包括机房及其附属设施、计算设备、存储设备、网络设备和其他设备。
b) 资源抽象与控制主要包括计算资源池、存储资源池、网络资源池、资源管理和调度平台等。
c) 云服务主要包含 IaaS、PaaS、SaaS 等类型的服务。
d) 运维运营管理主要包括日常管理、资源监控、运维管理、自助服务和服务管理等。

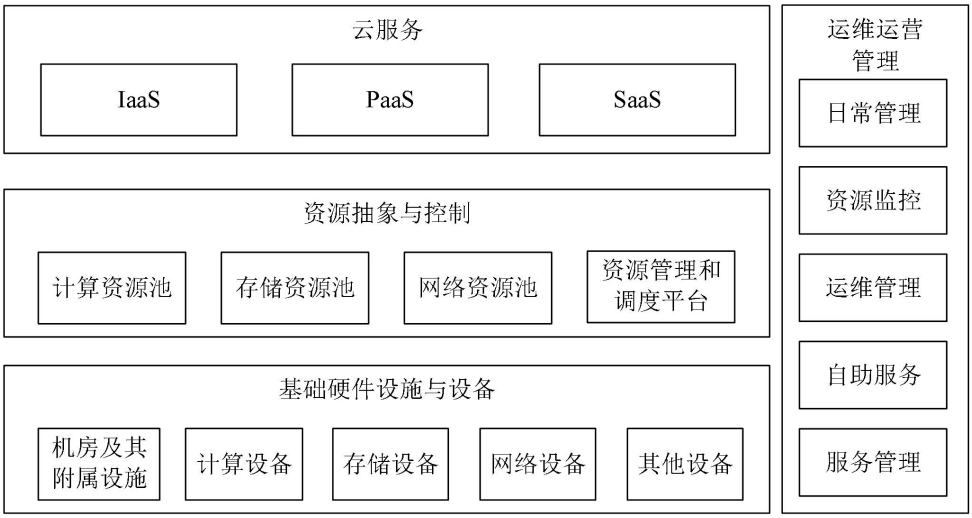

图 2 云计算平台架构体系

7.2 基础硬件设施与设备

7.2.1 概述

基础硬件设施与设备是指机房等基础设施以及计算、存储、网络等设备，是云计算平台的物理基础。云计算平台应使用安全可控、体系架构开放的硬件进行构建，保障可用性、安全性和可靠性。

7.2.2 机房建设

机房在选址、建筑结构、供电、制冷、消防、布线、物理访问控制、防盗防破坏、监控巡查、防雷消防、通讯等方面应符合GB 50174、JR/T 0131、JR/T 0071有关要求。金融云机房建设除符合上述要求外，应符合GB 50174中关于A级数据中心建设标准的要求。

7.2.3 网络设备

云计算平台网络主要包括数据中心内部网络和跨数据中心网络，具体要求如下：

a) 数据中心内部网络应采用高可靠、低时延、可扩展的网络架构，跨数据中心网络应采用高可靠、可扩展的网络架构。
b) 应支持按照计算、存储设备的通信需求，提供高并发接入。
c) 应支持按照管理粒度提供网络区域间的物理或逻辑隔离的功能。

7.2.4 计算和存储设备

计算设备指提供计算能力的物理服务器，应支持纳入计算资源池进行管理。

存储设备类型分为集中式存储和分布式存储，具体要求如下：

a) 集中式存储设备的具体要求如下：
   ——应采用高密度物理磁盘和高可用控制器；
   ——集中式存储架构应具备较高的 I/O 处理能力，支持存储扩展。
b) 分布式存储设备应支持将数据分散存储在不同的存储服务器中，支持存储服务器分布式扩展。

7.3 资源抽象与控制

7.3.1 概述

资源抽象与控制是实现基础硬件设施与设备服务化的基础，包括计算资源池、存储资源池、网络资源池，以及资源管理和调度平台，并为云服务和运维运营管理提供支撑。

7.3.2 计算资源池

计算资源的管理主要包括物理机管理和虚拟机管理两大类。所有计算资源应按照资源池进行管理，计算虚拟化技术和计算资源管理是构建计算资源池的重要基础。

a) 计算虚拟化技术能够利用虚拟化软件从计算资源池中虚拟出1台或多台虚拟机，虚拟化软件的功能要求如下：
   ——应支持多虚拟机管理与配置；
   ——应支持不同虚拟机之间资源逻辑隔离；
   ——应支持虚拟机对 CPU 和内存等资源的使用进行 QoS 配置；
   ——应支持设置 CPU 和内存使用的上限和下限；
   ——应支持动态增加虚拟机 CPU、内存的配置或采用热迁移等方式增加 CPU、内存的配置，满足业务运行需求。
b) 计算资源管理将各类计算资源统一管理并提供服务，计算资源管理的功能要求如下：
   ——应支持计算资源池化，提供可动态调整的 CPU、内存、I/O 设备等资源；
   ——应支持物理机和虚拟机的生命周期管理；
   ——应支持镜像的生命周期管理；
   ——应支持虚拟机的克隆、快照和备份管理；
   ——应支持按网络结构、资源池规划、管理粒度、资源种类等灵活划分资源池；
   ——应支持计算资源灵活调配的功能；

——应支持根据资源使用情况自动伸缩资源；
——应支持运行状态下的虚拟机动态迁移，并维持业务正常运行；
——应支持屏蔽相同架构类型下不同硬件的实现差异；
——应支持虚拟机的故障恢复功能。

7.3.3 存储资源池

7.3.3.1 概述

存储资源池由存储资源管理和存储系统组成，见图3。

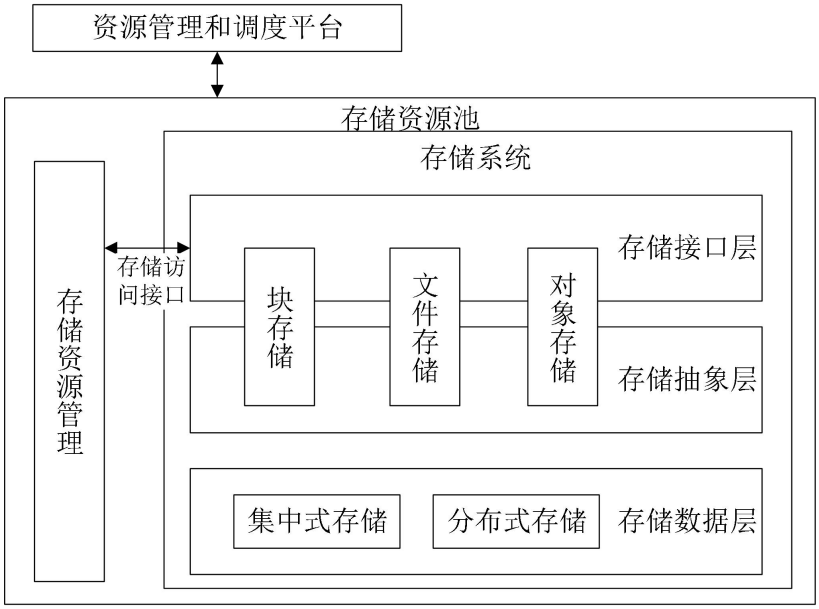

图 3 存储资源池

7.3.3.2 存储资源管理

存储资源管理负责存储系统资源的管理，其功能要求如下：

a） 应支持按存储资源类型实现资源池的分类管理和调度。
b） 应支持提供多种 I/O 性能的存储资源。
c） 应支持存储资源灵活调配的功能。
d） 应支持通过精简配置等功能提升存储资源利用率。
e） 宜支持多种存储系统的统一管理，如块存储、对象存储、文件存储。

7.3.3.3 存储系统

存储系统的通用功能要求如下：

a） 应支持高可扩展性，支持数据的存储和读写。
b） 应支持故障自动侦测、故障隔离和数据迁移，避免单点故障风险。
c） 应具备可靠的数据存储保护能力。
d） 应支持存储系统在线扩容和自动数据平衡。

存储系统包含存储数据层、存储抽象层和存储接口层：

a） 存储数据层是云计算存储系统的最底层，是数据存储的载体，可基于集中式存储或分布式存储构建，其功能要求如下：

——应支持 1 种或多种硬盘、存储服务器、磁盘阵列等存储资源；

——应支持存储容量按需扩容；

——应支持屏蔽相同架构类型下不同硬件的实现差异。

b） 存储抽象层为上层应用提供存储资源的抽象，包括但不限于块存储、文件存储和对象存储等。

c） 存储接口层提供块存储接口、文件存储接口和对象存储接口等存储系统与外部的接口，应支持高速可靠的数据传输。

7.3.4 网络资源池

7.3.4.1 概述

网络资源池是将网络设备进行逻辑抽象和集中管理形成的资源池，由基础物理网络、虚拟网络和网络资源管理等部分组成，其中基础物理网络到虚拟网络的抽象通过网络虚拟化技术实现。网络资源池的层次划分见图4。

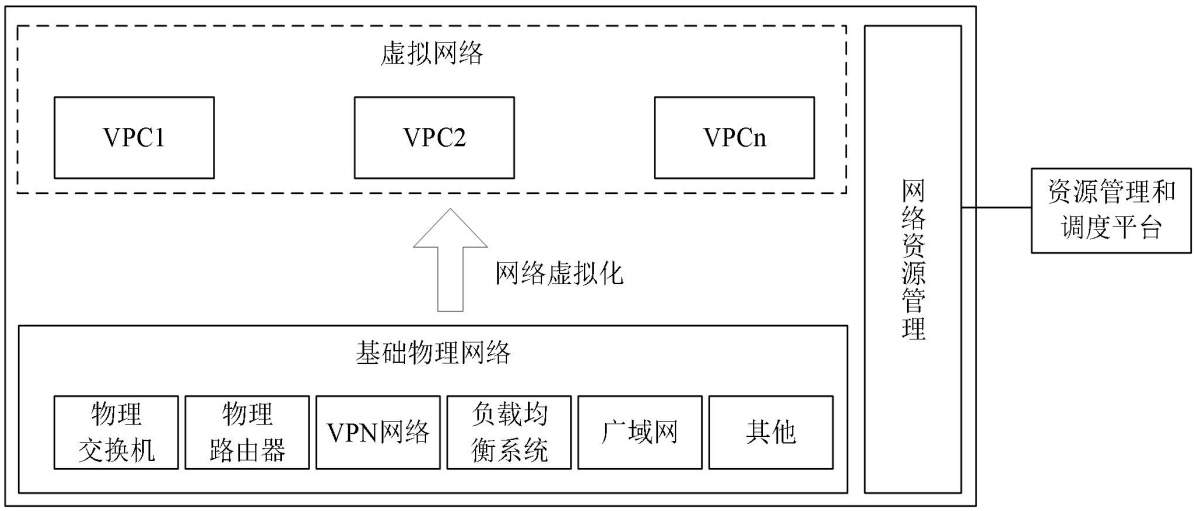

图 4 网络资源池

7.3.4.2 基础物理网络

基础物理网络是云计算平台网络资源池的底层基础，包括物理交换机、物理路由器、VPN网络、负载均衡系统等，基础物理网络的架构要求如下：

a） 应保证主要网络设备和通信线路冗余。

b） 网络设备业务处理能力应满足业务高峰期需要。

c） 应支持多条物理链路之间互为备份。

d） 应支持多条物理链路之间对流量进行负载分担。

e） 宜支持跨设备配置链路备份，可将不同设备上的物理以太网端口配置成 1 个聚合端口。

f） 采用控制与转发分离架构时应同时支持网络转发平面和控制平面的高可用性。

VPN网络在广域网中建立安全可靠、稳定的隧道连接，以保障信息传输安全，用于实现云计算平台内部网络的拓展，保障租户接入云计算平台内部网络的连接安全，VPN网络的功能要求如下：

a） 应支持可靠的身份认证，支持传输数据加密技术，能够有效隐藏云计算平台内部网络拓扑结构。

b） 宜支持通过数据压缩等技术实现网络加速。

负载均衡（可通过硬件或软件实现）包括服务器负载均衡。对于拥有多数据中心的云计算平台，也包括全局负载均衡，负载均衡要求如下：

a） 服务器负载均衡由负载均衡服务器将业务流量按一定策略分配到多台部署相同业务的服务器上，服务器负载均衡的功能要求如下：

——应采用冗余架构，避免单点故障；

——应支持传输层(如 TCP/UDP 协议)和应用层（如 HTTP/HTTPS 协议）的负载均衡；

——HTTPS 协议应提供集中化的证书管理系统能力；

——应支持弹性扩展，可与虚拟机配合提供系统的弹性扩展。

b） 全局负载均衡通过在多数据中心部署相同业务应用的方式提供服务，全局负载均衡的功能要求如下：

——应支持负载均衡设备间配置同步；

——应支持根据策略将业务流量分配到多数据中心；

——宜支持多种全局负载均衡调度算法，包括随机访问和优先级访问；

——宜支持多种应用健康检测方式，通过健康检测检查业务服务器和服务端口的可用性，优先选用服务器和服务端口满足健康检测要求的站点。

云计算平台与运营商网络的连接要求如下：

a） 应采用多线路设计，避免单点故障。

b） 应具备故障快速恢复能力。

c） 应支持数据中心出口流量优化，自动均衡各个出口流量利用率。

d） 宜支持基于时延、带宽等链路特点选择特定路径。

e） 宜支持流量管控，接入广域网时可区分其中的非正常业务流量。

7.3.4.3 虚拟网络

云计算平台使用网络虚拟化的技术将物理网络抽象成若干可以分配给云服务使用者使用的VPC。虚拟网络是指这些VPC的合集。云服务使用者可根据业务需求定义自己的VPC，包括定义网络拓扑、创建路由、创建虚拟交换机、创建子网、定义ACL等，虚拟网络的功能要求如下：

a） 应支持为同一租户或不同租户创建单个或多个独立的虚拟网络，不同虚拟网络之间逻辑隔离。

b） 应支持根据业务需求实现同一租户或不同租户 VPC 之间的互通。

c） 应支持虚拟网络和物理网络之间的 3 层交换。

7.3.4.4 网络虚拟化

利用网络虚拟化可在1个物理网络上模拟出多个虚拟网络。网络虚拟化包括网卡的虚拟化，物理网络设备的虚拟化，租户网络的虚拟化，以及网络功能虚拟化，网络虚拟化的功能要求如下：

a） 应支持将物理网络设备虚拟化为逻辑网络设备使用。

b） 应支持挂载和卸载虚拟机网卡。

c） 应支持远程运维和故障分析的能力。

d） 应支持分布式虚拟交换机功能。

e） 应支持虚拟机和物理网卡直通功能，提升虚拟机网络性能。

f） 应支持通过隧道封装技术为租户构建独立隔离的虚拟网络。

g） 宜支持网络功能虚拟化，在物理机上提供网络功能。

7.3.4.5 网络资源管理

网络资源管理将物理和虚拟网络资源形成资源池进行统一管理调度，网络资源管理的功能要求如下：

a） 应采取冗余架构等措施，避免网络资源管理节点的单点故障。

b） 宜支持对不同厂商网络设备的管理和配置自动下发，包括子网、网关、路由等参数的配置。

7.3.5 资源管理和调度平台

资源管理和调度平台能够接收服务资源请求，实现对资源的调度分配，资源管理和调度平台的功能要求如下：

a） 应支持对计算、存储、网络资源的统一管理。

b） 应对不同租户的计算、存储、网络资源在性能和访问上进行隔离。

c） 应支持资源协同管理，能够按需整合计算、存储、网络资源。

d） 应支持资源负载自动感知，可根据负载情况灵活调配资源。

e） 应支持自动检测故障和系统热点，保证业务稳定可靠运行。

f） 应支持多数据中心资源的统一管理。

g） 应支持资源管理和调度平台的高可用。

h） 宜支持多种虚拟化技术的统一管理。

i） 宜支持虚拟化资源和物理资源的转换。

7.4 云服务

7.4.1 概述

云服务层按照应用场景需要将IT资源、平台、应用等1种或多种功能封装成不同的云服务提供给云服务使用者，可分为IaaS、PaaS和SaaS等服务类别。IaaS包括但不限于虚拟机服务、物理机服务、存储服务、负载均衡服务、内容分发网络服务、VPC服务、网络连接服务、域名服务等。PaaS包括但不限于数据库服务、容器服务、中间件服务、分布式数据处理服务等。SaaS包括行业类SaaS和通用类SaaS等。云服务的层次划分见图5。云计算平台在提供相应服务时应满足本规范的要求，但并不要求云计算平台提供以上全部服务。

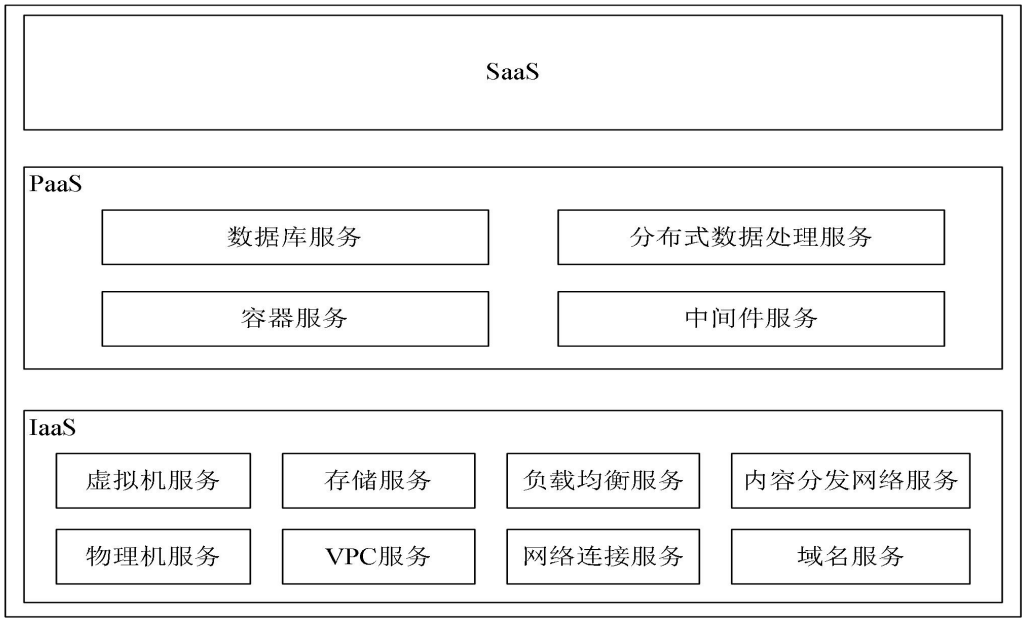

图 5 云服务的层次划分

7.4.2 IaaS

7.4.2.1 虚拟机服务

虚拟机服务是指云服务提供者向云服务使用者提供面向操作系统的计算服务，虚拟机服务的功能要求如下：

a） 应具备虚拟机全生命周期管理功能，支持对虚拟机进行创建、删除、回收、关闭、重启等操作。
b） 应支持不同类型的操作系统和存储设备。
c） 应支持创建自定义 CPU、内存、网络、磁盘等属性的虚拟机。
d） 应支持对运行或停止状态的虚拟机生成快照，并提供快照恢复功能。
e） 应支持计算能力的垂直伸缩，如按需调整 CPU 或内存配置、增加或减少磁盘容量和网卡数量。
f） 应支持计算能力的水平伸缩，如按需调整虚拟机实例数量。
g） 应支持从虚拟机或快照中创建虚拟机实例镜像。
h） 应支持自定义网络配置。
i） 应支持故障场景下的虚拟机恢复。
j） 宜支持将虚拟机在运行情况下迁移至其他宿主机。

7.4.2.2 物理机服务

物理机服务为用户提供专用的物理机，满足其业务安全性、稳定性及部分业务无法在虚拟机部署的需求，物理机服务的功能要求如下：

a） 应支持不同物理机规格和配置。
b） 应支持多种操作系统。
c） 应支持物理机的自动发放。
d） 应支持物理机自动完成网络配置和操作系统安装。
e） 应支持同一个租户的虚拟机和物理机相互连通。

7.4.2.3 存储服务

存储服务是指为云服务使用者提供数据存储的服务，存储服务可分为块存储服务、文件存储服务、对象存储服务和归档存储服务等，存储服务的功能要求如下：

a） 块存储服务是指将虚拟化的物理磁盘空间直接映射给服务器使用的存储服务；块存储服务可用于构建独立可扩展硬盘、文件系统、数据库存储等，块存储服务的功能要求如下：
——应支持基于多租户的身份认证和数据隔离等存储管理功能；
——应支持良好的 I/O 性能、数据传输和数据读写访问功能；
——应支持冗余副本、冗余访问路径等方式实现故障容错；
——应支持实现数据的快速备份和恢复；
——应支持存储容量扩展。
b） 文件存储服务是指以文件传输协议为主要接入方式的文件级数据存储服务，文件存储服务的功能要求如下：
——应支持基于多租户的身份认证和数据隔离等存储管理功能；
——应通过冗余副本、集群等方式保障高可靠性；
——应支持多个设备同时挂载同一文件系统以实现文件共享功能；
——应支持低延时、高并发的数据访问；
——应支持存储容量的在线扩展。

c） 对象存储服务以数据标记为主要文件组织方式，提供完全扁平化的存储服务，对象存储服务的功能要求如下：

——应支持基于多租户的身份认证和数据隔离等存储管理功能；

——应通过冗余副本、集群等方式保障高可靠性；

——应支持低延时、高并发的数据访问；

——应支持存储容量的在线扩展；

——应支持对象存储用户配额的设置和检查，保证使用容量达到配额后不能继续占用更多存储空间。

d） 归档存储服务主要用于存储访问频率极低的数据，并提供数据归档和备份管理，归档存储服务的功能要求如下：

——应支持基于多租户的身份认证和数据隔离等存储管理功能；

——应通过冗余副本、集群等方式保障高可靠性；

——宜支持为云服务使用者的历史数据提供区别于实时交易性能的存储介质，并支持高压缩比的文件存储功能。

7.4.2.4 VPC 服务

VPC服务为云服务使用者在云计算平台上构建出1个逻辑隔离、私有的虚拟网络环境，使云服务使用者可以自行管理、控制该环境内的IP地址、网段、路由和虚拟网络设备等，VPC服务的功能要求如下：

a） 应支持同一租户或不同租户之间的不同 VPC 网络的逻辑隔离。

b） 应支持自定义私网网段，分配私网地址。

c） 应支持互联网接入，支持 IP 地址转换和带宽配置。

d） 应支持私网内的子网划分、路由连通等功能。

e） 应支持根据业务需求实现同一租户或不同租户 VPC 之间的互通。

f） 应支持访问控制规则配置。

7.4.2.5 负载均衡服务

负载均衡服务的功能应符合7.3.4.2的有关要求。

7.4.2.6 网络连接服务

网络连接服务提供跨网络的互联互通服务，按使用方式可包括专线服务和基于VPN的连接服务等，网络连接服务的功能要求如下：

a） 应提供安全可靠的网络连通。

b） 应支持按云服务使用者要求定义网络路由规则。

7.4.2.7 内容分发网络服务

内容分发网络服务是指在现有网络基础上增加能够快速响应服务的加速节点，以有效降低用户访问延迟，对于运行金融业务系统的云计算平台内容分发网络服务的功能要求如下：

a） 应支持稳定、可靠的网络服务和终端接入。

b） 应支持通过分布多地的内容分发网络节点提供网络优化和网络加速。

c） 应提供用户自服务功能，包括创建、删除、修改加速内容等。

d） 应提供基本的数据分析和监控功能，包括消耗统计、访问统计、源站数据统计等。

7.4.2.8 域名服务

域名服务为云服务使用者提供域名的生命周期管理，包括域名注册、域名解析、域名转入、域名备案等服务，域名服务的功能要求如下：

a） 应支持自服务的域名注册、批量注册、域名转入等功能。

b） 应支持多种域名记录类型，如 A 记录、CNAME 记录、MX 记录等。

c） 应支持域名解析到云资源，如解析到云计算平台服务器的互联网 IP 和端口等。

d） 应支持域名解析快速生效和同步的功能。

7.4.3 PaaS

7.4.3.1 数据库服务

数据库服务主要包括关系型数据库服务和非关系型数据库服务，其中关系型数据库服务包含集中式关系型数据库服务和分布式关系型数据库服务，数据库服务的功能要求如下：

a） 集中式关系型数据库服务的功能要求如下：

——应基于集群及负载均衡等技术提供高可用性；

——应具备纵向和横向的扩展功能；

——应支持读写分离功能；

——应支持数据库集群的节点在线扩容和升级；

——应支持数据同步功能，能够采用实时、离线方式进行数据迁移；

——宜支持基于多租户的数据存储和数据隔离。

b） 分布式关系型数据库服务提供多节点的关系型数据库处理，其功能要求如下：

——应提供跨数据库节点的数据操作，并保证数据的一致性；

——应支持数据库的横向扩容和分库分表；

——应支持数据库算法跨数据库节点进行数据处理，保证数据处理的准确性；

——应支持多节点数据库的统一监控运维。

c） 非关系型数据库服务功能要求如下：

——应支持数据的全生命周期管理，可实现数据的多副本存储；

——应支持横向扩容功能。

7.4.3.2 分布式数据处理服务

分布式数据处理服务通过大规模、可扩展的分布式架构，对海量数据提供高效的存储、计算和分析，分布式数据处理服务的功能要求如下：

a） 应支持海量数据存储与计算。

b） 应提供多维度任意组合查询的数据访问接口。

c） 应支持并行计算框架，如 Map/Reduce、MPI 等。

d） 应提供按需使用、弹性伸缩的服务模式，可进行在线升级和扩容。

e） 应支持跨集群的作业调度和数据流动。

f） 应提供数据同步工具，实现和其他数据持久化层软件的双向数据同步。

g） 宜支持多租户管理体系，实现应用、数据等方面的多租户隔离。

7.4.3.3 容器服务

容器服务为云服务使用者提供轻量级的应用封装、管理和运行解决方案，容器服务的功能要求如下：

a） 应支持不同应用的逻辑隔离。

b） 应支持容器镜像管理。

c） 应支持自定义网络配置。
d） 应支持完善的容器调度伸缩和应用集群管理功能。
e） 宜支持界面化容器编排。
f） 宜支持基于多租户的数据和权限管理机制。
g） 应支持自定义存储配置。

7.4.3.4 中间件服务

中间件服务应具备较高性能，支持完善的日志记录，提供良好的管理界面和操作审计功能。中间件服务应包括消息中间件、数据访问中间件、事务中间件等，中间件服务的功能要求如下：

a） 消息中间件服务应支持节点故障处理、消息防丢失、消息持久化、消息副本及备份等功能。
b） 数据访问中间件服务的功能要求如下：
——应支持对数据库、数据缓存的透明访问；
——应支持标准的 SQL 语法，支持把标准 SQL 翻译为特定数据源语义；
——应支持对 SQL 的优化，如基于规则的优化等。
c） 事务中间件服务的功能要求如下：
——应支持事务管理机制，确保跨节点的事务一致性；
——应支持异常事务的处理机制；
——应支持高并发的事务处理。

7.4.4 SaaS

SaaS是云服务提供者为云服务使用者提供的1种可直接使用的软件应用服务，可分为行业类SaaS和通用类SaaS。行业类SaaS指根据不同行业的业务场景向用户提供业务系统服务。通用类SaaS指向用户提供消息通讯、数据分析、人工智能和辅助工具等通用服务。

云计算平台提供SaaS时，应满足金融领域相应类型的信息系统在服务外包、信息安全、业务流程等方面的监管要求。

7.5 运维运营管理

7.5.1 日常管理

日常管理的功能要求如下：

a） 应支持平台配置、应用发布部署、资源动态伸缩的统一管理。
b） 应支持统一展现、统一告警、统一流程处理功能。
c） 宜具备对用户、租户的全生命周期管理功能。

7.5.2 资源监控

资源监控的功能要求如下：

a） 应支持信息采集功能，能够实时采集云计算平台各类资源及服务的状态信息。
b） 应支持数据分析功能，能够对采集信息进行综合分析、准确诊断和动态展示。
c） 应支持资源池监控功能，能够对各类资源运行状态进行实时监控。
d） 应提供其他监控平台的接入接口。

7.5.3 运维管理

运维管理提供运维工作界面和工具支撑，其功能要求如下：

a） 应支持变更管理和配置一致性检测，且能够在失败或者发生错误时回滚配置。
b） 支持维护事件自动提醒，能够实时将运维事件通知相关人员。
c） 应支持定期对云计算平台的资源和应用系统进行健康巡检，自动生成巡检日志。
d） 应支持自动生成维护报告，定期提供平台运行情况和资源利用情况的分析报告。
e） 宜支持多租户运维管理功能，租户可通过管理界面自主查看、配置和分析云计算平台资源。

7.5.4 自助服务

自助服务主要向云服务使用者提供可自由调配资源和使用云服务的功能，自助服务的功能要求如下：

a） 应支持自助完成资源的申请、使用、配置、修改、删除。
b） 应支持自助查看申请资源的使用情况、性能状况、申请状态、操作日志等。
c） 应支持对计算、存储、网络等资源的自助调度。

7.5.5 服务管理

服务管理的功能要求如下：

a） 应支持服务计量功能，能够度量云服务所使用的各类资源数量和时间。
b） 应支持分级分角色的用户管理功能。
c） 应支持服务审计功能，能够按照云服务使用者、云服务和资源等维度进行审计。
d） 宜支持服务计费功能。