文章编号：2095-2163(2020)06-0243-07 中图分类号：TP316.4 文献标志码：A

# 迈进云计算 4.0 时代-招商证券 IT 云化之路

何 宇，陈子升
（招商证券股份有限公司 信息技术中心，广东 深圳 518052）

**摘 要**：云计算技术在从提出至今已经过 13 a，期间，云计算的形态与应用范围发生了翻天覆地的变化：从最初以主机虚拟化为主的 1.0 阶段，到以软件定义与自服务为特征的 2.0 阶段，再到以混合云及多云管理为范围的 3.0 阶段，最后到现今以 IT 即服务的云服务中台为形态的 4.0 阶段。分别从云计算 1.0 至 4.0 这 4 个阶段，结合招商证券自身情况，介绍招商证券 IT 即服务的云化之路。

**关键词**：云计算；虚拟化；资源；服务；软件定义

# Stepping into cloud computing age 4.0—the IT cloudification road of China merchants securities

HE Yu, CHEN Zisheng
(Information Technology Center, China Merchants Securities, Shenzhen Guangdong 518052, China)

**【Abstract】** It has been 13 years since the introduction of cloud computing technology. During this period, the form and scope of cloud computing have undergone tremendous changes: from the stage 1.0, which is mainly about host virtualization, to the stage 2.0, which is characterized by software definition and self-service, to the stage 3.0, which includes hybrid cloud and multi-cloud management, and finally to the stage 4.0, which takes IT service as a service as a form. This article introduces the cloudification road of ITaaS of China Merchants Securities from the four stages of cloud computing stage 1.0 to 4.0, based on China Merchants Securities self-development.

**【Key words】** cloud computing; virtualization; resource; service; software-defined

## 0 引 言

从 2006 年谷歌首次提出云计算的概念至今 13 a期间，云计算的形态发生了翻天覆地的变化。从主机虚拟化到 ITaaS(IT 即服务)，本文把这段发展期划分为云计算 1.0 至 4.0 四个阶段。招商证券参考业内外成功案例，结合自身业务特点以及对云计算技术的思考，通过大量测试验证，摸索出符合自身情况的云计算技术应用的发展路径，搭建出 ITaaS 的云服务中台，为业务提质增效提供了有效的技术支持。本文分别从云计算 1.0 至 4.0 四个阶段，结合招商证券自身情况，介绍招商证券 IT 即服务的云化之路。

## 1 云计算 1.0：主机虚拟化

主机虚拟化技术把服务器虚拟化，整合成计算资源池。单台物理服务器上可运行多台虚拟机，结合 CPU 分片、内存共享、虚拟网卡、存储精简供应等技术，大大提升了资源利用率，节省了总体成本。同时，主机虚拟化管理平台使用热迁移、主机高可用、动态资源分配等技术，从平台层为虚拟机提高了灵活性与业务连续性。

主流的主机虚拟化产品有以下 3 种：(1) VMware vSphere。vSphere 是 VMware 公司推出的业界最通用的主机虚拟化产品，市场占用率高，成熟度高。支持在线热迁移、分布式虚拟交换机、HA、DRS 等高级功能。(2) Microsoft Hyper-v。Hyper-v 是微软公司推出的商业主机虚拟化产品，对 Windows 支持较好，功能与 VMware vSphere 类似。(3) KVM。KVM 是开源的主机虚拟化产品，使用 Linux 自身的调度器进行管理，仅能提供基本的虚拟化功能，不具备商业虚拟化产品能提供的高级功能。KVM 为开源产品，不需要软件许可，成本较低。

招商证券在云计算 1.0 阶段，基于异构，成本，功能、成熟度等因素的综合考虑，使用以上 3 种方式实现主机虚拟化。其中，VMware vSphere 与 Microsoft Hyper-v 承载相对关键业务，KVM 承载非关键业务。

作者简介：何 宇(1976-)，男，学士，主要研究方向：云计算、数据库、证券核心交易系统；陈子升(1990-)，男，学士，主要研究方向：云计算、大数据、DevOps。

收稿日期：2020-01-07


图 1 主机虚拟化

Fig. 1 Compute virtualization

## 2 云计算 2.0:软件定义与自服务

云计算 2.0 阶段在主机虚拟化的基础上,对存储与网络设备实现了虚拟化,通过 SDDC(软件定义数据中心)技术,将计算、存储、网络、安全等硬件资源整合为虚拟资源池。使用配备高容量磁盘、高速网卡的服务器组成集群,即可实现计算、网络、存储、安全的整体基础架构。SDDC 技术极大地改变了数据中心的形态,节省了空间、电力等基础设施资源,使硬件设备更标准化,易于扩展。

云计算 2.0 阶段,企业通过云管平台实现资源服务化与流程自动化,将过往通过人工申请,人工分配的低效的资源供应方式改变为自助申请、自动分配的高效资源供应方式。大大提升了资源申请与使用效率。

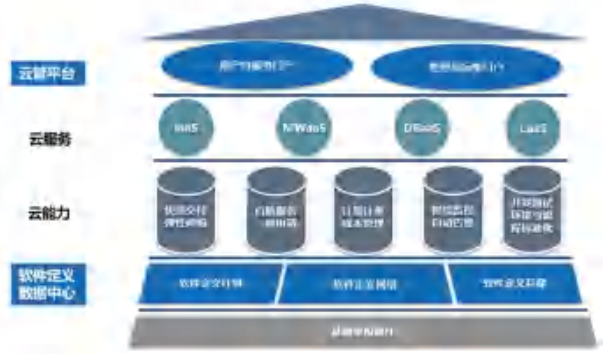


图 2 软件定义与自服务

Fig. 2 Software-defined and self-served

### 2.1 软件定义数据中心 SDDC

软件定义数据中心 SDDC 包含软件定义计算 SDC、软件定义存储 SDS、软件定义网络 SDN 三大方面。

#### 2.1.1 软件定义计算 SDC

SDC 即主机虚拟化技术,把服务器虚拟化,整合成计算资源池。

#### 2.1.2 软件定义存储 SDS

SDS 技术将服务器上的本地存储虚拟成分布式存储集群,整合成存储资源池。数据通过条带化分布在不同节点上,读写性能随着节点数量增长而递增;数据通过多副本冗余的方式保存在不同节点上,可靠性可通过增加副本数而提升。目前经过多年业界实践验证,分布式存储在性能与可靠性上可媲美甚至超越传统商业集中式存储。分布式存储按部署方式不同划分为超融合模式与计算存储分离两种模式:(1)超融合模式。集群内每台服务器均同时实现计算与存储功能。超融合方式更节省空间及成本,更灵活扩展。(2)计算存储分离模式。分别使用不同的服务器实现计算集群与存储集群。分离模式使计算集群专注于处理任务,存储集群专注于存储 IO 读写与数据复制,提供更优的性能。

考虑到以下因素,招商证券选择超融合方式实现软件定义存储:(1)CPU 芯片性能日益提升,CPU 一般不会成为虚拟化环境的性能瓶颈。(2)可使用不同的高速网卡组分别承载业务与存储网络,互不影响性能。(3)超融合模式能提供更低的成本与更灵活的扩展性。

#### 2.1.3 软件定义网络 SDN

SDN 技术将交换机、负载均衡、路由器、防火墙等网元虚拟化,整合成网络资源池,相对于传统网络有如下收益:

(1)SDN 技术通过 NFV(网络功能虚拟化)技术提供软件形态的交换机、路由器、防火墙、负载均衡、NAT 等设备,节省物理空间与电力资源,灵活部署。

(2)SDN 对全网络架构提供统一的图形化管理界面,配置与策略统一下发,可将重复性工作固化为模板,实现全链路的网络自动化,降低运维难度与配置出错概率。

(3)SDN 使用微分段技术,将安全隔离的粒度细化到业务或虚拟机,减少了网段数量,提高了管理精细度。

(4)SDN 提供网络多租户技术,配合云平台实现基础资源多租户,提供用户更大的配置灵活度与用户间更高的安全隔离。

SDN 又根据部署形态划分为软件 SDN 与硬件

SDN 方案，其中硬件 SDN 以 Cisco ACI，华为 Cloud Fabric，H3C VCF 等为主，软件 SDN 以 VMware NSX、Openstack Neutron、Juniper Contrail 等为主。软件 SDN，通过软件实现网络与安全设备，包括交换机、路由器、负载均衡等，节省总体成本，能实现全链路的自动化能力。软件 SDN 使用服务器 CPU 资源实现隧道技术网络包的封装与解封装，有一定性能损耗。硬件 SDN，通过硬件网络设备实现，网络包的封装与解封装在交换机上，性能更优，更稳定。硬件 SDN 一般需要借助硬件防火墙、负载均衡等实现安全与流量负载能力，自动化能力稍低。

侧重性能与稳定性，应优先选择硬件 SDN 方案；侧重成本与自动化能力，应优先选择软件 SDN 方案。招商证券基于以下 3 点考虑，在托管云选择软件 SDN 方案建设网络架构：(1)经测试，软件 SDN 跨宿主机访问有约 5%性能损耗，在可接受范围内；软件 SDN 采用分布式网关，能基于虚拟机所在节点进行智能选路，流量路径更优。(2)软件 SDN 能提供软件形态的网络设备，实现更高的网络的自动化能力，使网络与安全资源服务化，提供给用户更大的便利度。(3)通过网络多租户技术实现云平台多租户，供外部客户托管应用使用，租户间网络隔离，租户内网络灵活配置。

## 2.2　云管平台 CMP

CMP 在 SDDC 的基础上提供了服务编排、自助申请、计量计费，智能监控等能力，实现资源的统一管理与监控、资源申请和供应的自动化、以及资源使用过程的成本核算。

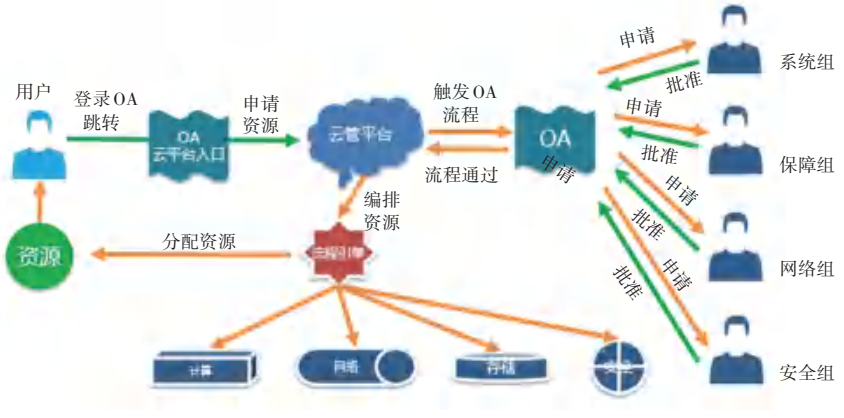


**图 3　云管平台自动化流程**

**Fig. 3　Automation process in cloud management platform**

CMP 使原来的“需求沟通->人工申请->人工审批->人工分配”流程简化为“自助申请->人工审批->自助分配”，将原来数天的资源申请与供应时间缩短为分钟。

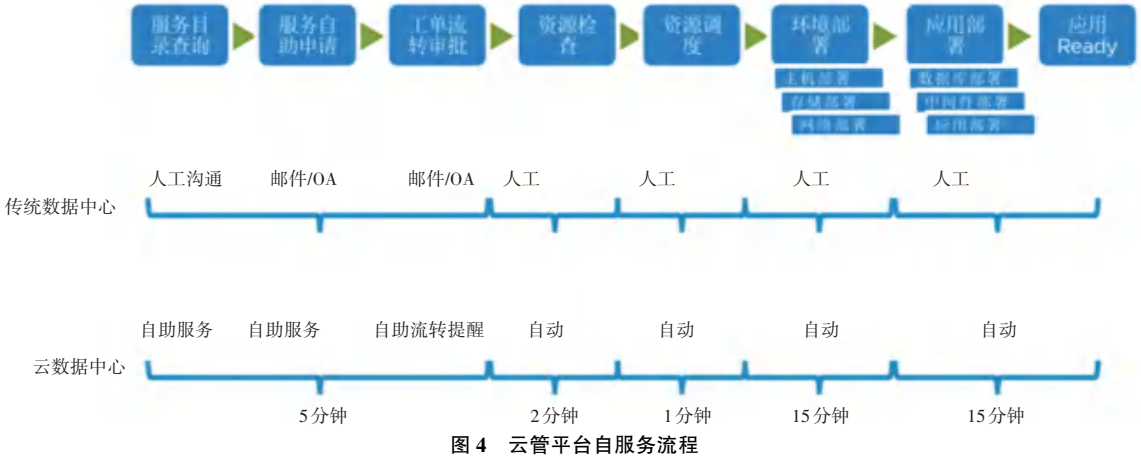


**图 4　云管平台自服务流程**

**Fig. 4　Self-served process in cloud management platform**

## 2.3　SDDC 与 CMP 选型

目前主流的 SDDC 与 CMP 产品主要包含 3 种类型。

### 2.3.1　商业私有云产品

主流的商业私有云产品有 VMware vCloud，Microsoft System Center 等。商业私有云产品具备全

套的 SDDC 与 CMP 组件,组件间关联紧密,兼容性好,使用便利。商业私有云产品包含资源管理、流程自动化、服务编排、运维监控、成本计费等多个组件,其中服务编排组件,可以对计算、存储、网络、安全、操作系统、软件等进行编排,整合为可一键申请的服务,对于想快速供应复杂运行环境的企业,提供了很大便利。

2.3.2 开源私有云产品

开源私有云产品主要以纯开源 Openstack 及基于 Openstack 二次开发的商业版本为主。开源私有云产品包含软件定义数据中心及基本的用户管理与计费组件,可满足基础的自助服务申请与分配需要。纯开源私有云产品成本较低,但运维难度较大。对于运维技术人员不充足的中小型企业,一般采用基于 Openstack 二次开发的商业版本。

2.3.3 公有云及其下沉的线下私有云版本

以 Amazon AWS、微软 Azure、阿里云、腾讯云为主的公有云服务一般提供完整的 SDDC 与 CMP 功能,按需租用即可。上述公有云服务提供商亦提供针对企业内部数据中心部署的私有云版本,如阿里云的飞天,腾讯云的 TCE,AWS 的 AWS Outposts,微软的 AzureStack。公有云下沉的私有云产品能提供类似于公有云的便捷的使用方式与丰富的服务类型,但整体架构相对繁重,对硬件资源要求高,维护难度大,成本昂贵。

招商证券在云计算 2.0 阶段,基于成熟度,便利性,复杂资源供应敏捷度等考虑,选择了商业私有云产品,包括软件定义计算,软件定义存储,软件定义网络,云管平台等组件,构建了以软件定义数据中心为基础,以自服务的使用方式为核心的云平台。

## 3 云计算 3.0:混合云及多云管理

随着公有云技术已趋成熟,产品日渐丰富,行业相关监管政策对公有云的承认度越来越高,且公有云原生具备的快速供应,弹性伸缩等特点,尤其适合券商行情及资讯等易产生突发性高峰的业务对资源供应敏捷性的需求。券商采用公有云承载部分非敏感性业务已成为行业趋势。

另外,考虑到分散单品牌风险与平衡成本,避免“把鸡蛋放在同一个篮子里”,企业在本地数据中心使用不同私有云产品承载不同关键级别的业务是更合理的做法。比如使用成本更低的开源或商业 Openstack 承载非关键的内部管理类业务,使用成熟度更高的商业私有云产品承载关键的交易类业务。

最后,伴随着互联网业务的高速发展,传统的开发模式已不足以支撑敏态应用快速迭代的需求,敏捷开发模型成为企业开发首选,但同时也对基础架构的资源类型提出了新的需求。随着容器、Kubernetes、微服务等技术及相应社区的成熟,采用容器云技术构建 DevOps 开发流程,支撑企业敏捷开发成为了必然趋势。

云计算 3.0 阶段,混合云及多云管理成为了云平台的新形态。企业云建设的重点由 IaaS 转化 为 PaaS。

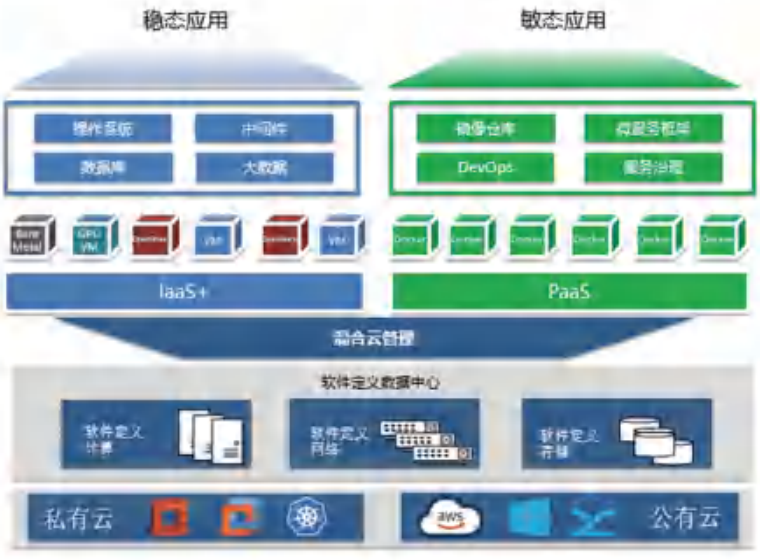


图 5 混合云与多云管理

Fig. 5 Hybrid cloud and multi cloud management

### 3.1 混合云管理

外资混合云管平台一般只对国外公有云如 AmazonAWS、Microsoft Azure、Google GCE 等提供支持。招商证券在云计算 3.0 阶段,使用了基于国产

云管平台二次开发的混合云管平台，纳管阿里云、腾讯云、微软 Azure 云等多种公有云，及本地生产、灾备私有云，在公有云多区域多可用区结合本地 IDC 混合部署的模式承载业务，最大程度上保证了上云业务的可靠性和连续性。

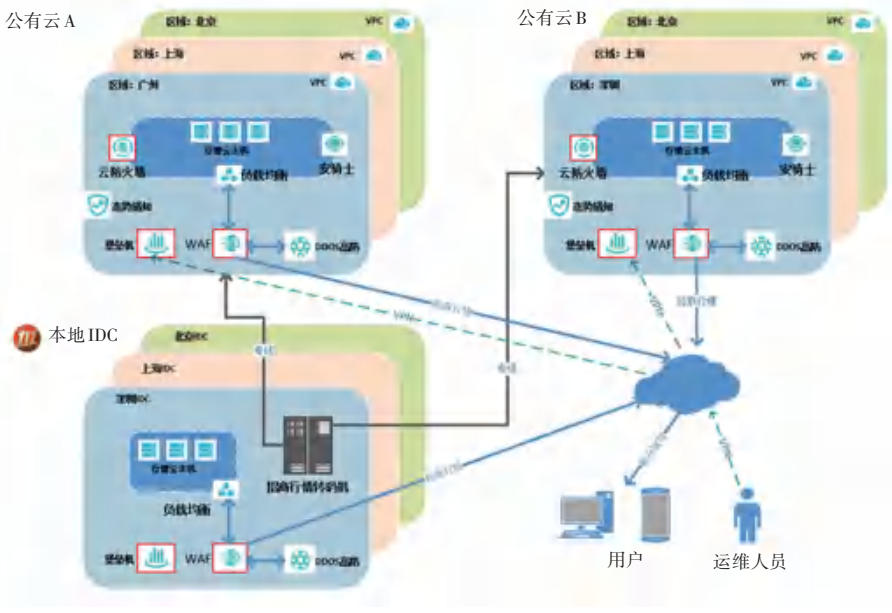


**图 6　混合云部署**

**Fig. 6　Hybrid cloud deployment**

### 3.2　多云管理

招商证券在开发测试环境使用基于 Kubernetes 和 Dockers 的容器云和整合 CI\CD 工具链的 PaaS 平台，构建 DevOps 开发测试一体化流程，节省基础架构资源，提高迭代开发效率。整个 PaaS 平台运行在 IaaS 平台之上，受云管平台统一管控。IaaS 平台的软件定义网络与软件定义存储技术为容器云平台提供容器网络插件（CNI）与持久化存储（PV），更高地保障 PaaS 平台的租户间的安全隔离与数据可靠性。

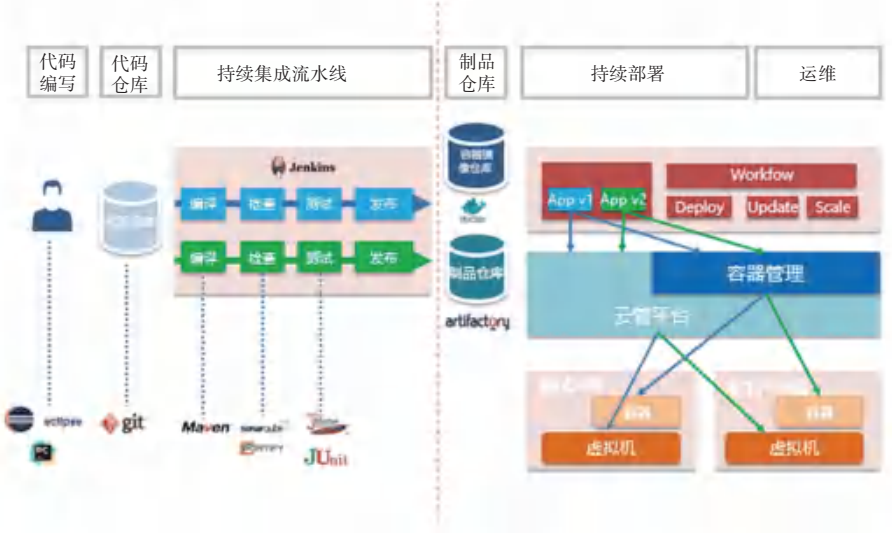


**图 7　PaaS 平台与 DevOps 流程**

**Fig. 7　PaaS Platform and DevOps process**

## 4　云计算 4.0：IT 即服务的云服务中台

X86 芯片性能的提升、X86 架构稳定性的增强、分布式应用技术的成熟，为 IT 资源全面云化提供了基础。近年，券商的绝大部分业务系统，包括核心交易系统的 x86 化、云化已有了成熟的解决方案及实践案例。

云计算 4.0 阶段，招商证券将打造云服务中台，将 IT 资源全面云化，为 IaaS\PaaS\SaaS 资源申请与

管控提供统一入口。主要包含以下两方面内容：

### 4.1 PaaS 向 SaaS 迈进

构建应用商店，使用资源编排、自动化运维等工具、将软件、运行环境、开发框架、自动化脚本等抽象为应用商店里的服务，无论是在裸金属、虚拟机或容器等形态的资源之上，均可一键部署服务。开发与运维人员不再需要进行重复的环境准备与配置变更工作，一切按需申请，自动部署。

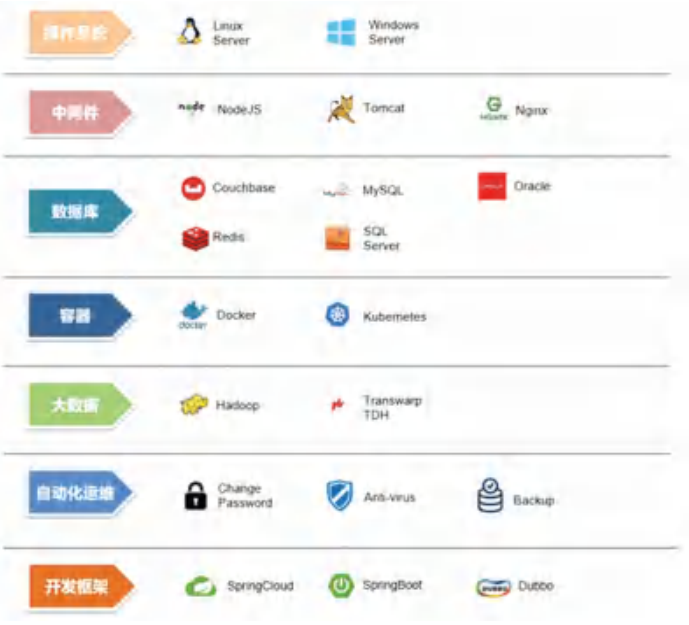


图 8 SaaS 应用商店

Fig. 8 SaaS application store

### 4.2 整合 ITIL 标准化流程

随着云计算、人工智能等技术的蓬勃发展，互联网金融的兴起，业务对运维管理提出了新的要求，以往孤立分散的监控运维体系须向监管控一体化、自动化、智能化的新型运维体系迈进，以适合云端应用对于运维的需求。

建立 ITIL 标准化流程有助于解决上述需求。但传统的 ITIL 标准化流程没有针对云环境作针对性改进，大量工作如资产录入，配置变更，监控与事件管理等还是依赖于人工操作。云服务中台的资源编排与自动化能力，可为建立 ITIL 流程、实现智能一体化运维包括 ITSM、CMDB、智能监控、自动化运维等提供自动化接入的基础。

招商证券在云计算 4.0 阶段，将在混合云管平台的基础上，补充从硬件到应用全栈式监控、多平台日志管理、应用商店、自动化运维等能力，打通运维的监管控，实现 ITIL 标准化流程。最终实现运维即云，IT 即服务。

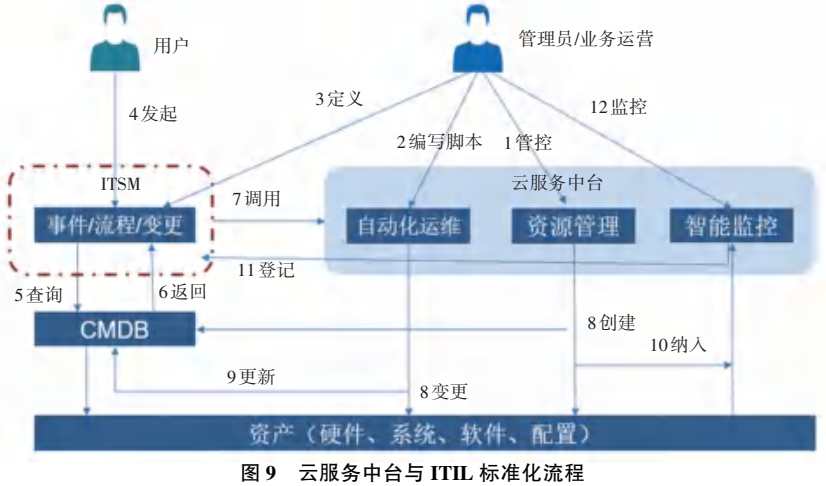


图 9 云服务中台与 ITIL 标准化流程

Fig. 9 Cloud service mid-platform and ITIL standardization process

（下转第 251）