



顾炯炯 编著

云计算架构 技术与实践

..... (第2版)

CLOUD COMPUTING
ARCHITECTURE TECHNOLOGIES & PRACTICE,
SECOND EDITION



清华大学出版社

顾炯炯 编著

云计算架构 技术与实践

..... (第2版)

清华大学出版社
北京

内 容 简 介

云计算概念诞生至今约10年的时间,这10年来,相比云计算诞生初期,技术条件、行业和市场环境均发生了巨大变化,广大读者对云计算的认知需求,也从当初的粗浅概念阶段,发展到希望深度探索的阶段。

本书以云计算架构技术为核心,从讨论云计算发展为起点,围绕云计算架构涉及的核心技术与商业实践展开。论及的核心技术包括计算、存储、网络、数据、管理、接入、安全等方面,涵盖了云计算的最新趋势、原理、特性与实践。

本书针对希望了解云计算技术最新进展的读者和希望深入探索云计算架构技术的读者编写,适用于企业IT部门首席信息官(CIO)、IT主管、技术类人员、IT技术公司、互联网公司、教育机构的师生、IT技术工程师等。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

云计算架构技术与实践/顾炯炯 编著. —2版. —北京:清华大学出版社,2016(2016.10重印)
ISBN 978-7-302-44877-8

I. ①云… II. ①顾… III. ①云计算—架构 IV. ①TP393.027

中国版本图书馆 CIP 数据核字(2016)第 194400 号

责任编辑:陈莉 高岫

封面设计:周晓亮

版式设计:方加青

责任校对:曹阳

责任印制:宋林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:北京亿浓世纪彩色印刷有限公司

经 销:全国新华书店

开 本:185mm×240mm 印 张:21.75 字 数:597千字

版 次:2016年9月第2版 印 次:2016年10月第2次印刷

印 数:3501~5500

定 价:68.00元

产品编号:070544-01

编委会

第一作者：顾炯炯

第2版作者团队(排名不分先后)

李明 章宇 李金成 王道辉 申思 李力 罗浩 刘阳 申骞 李嘉 熊文辉
夏泉源 宋宇 金波 陈普 鲍亮 吕鹂啸 邹睿 闫启明 陈水星 王政 闵小勇
孙万琪 张大震等

第1版作者团队(排名不分先后)

黄朝意 金波 李力 吴天议 王道辉 闵小勇 熊文辉 李浩 严天科 钟颀 吴鸿钟
琚列丹 胡斐然 皮楚贤 陈普 李嘉 朱照生 周建军 刘红霞 肖江波 谢宁 孙万琪
潘少钦 胡善勇 王静 宁志强 张大震等

第2版序言

2014年我们出版了本书第1版，试图帮助大家揭开云计算技术与架构的神秘面纱。然而两年以来，如何让云计算真正走下技术的神坛，脚踏实地地服务好全球各行各业，使其ICT生产效率提升，促使ICT产业尽快完成面向极致开放化、敏捷化与智能化的升级转型，仍旧是摆在广大云计算从业者面前共同的课题与挑战。带着这些问题，针对第1版中已覆盖的云计算技术趋势、OpenStack、软件定义网络、云安全、大数据、分布式软件定义存储、软件定义Overlay网络、云计算实践等内容，我们在第2版中均做了与时俱进的更新，分享了华为在云计算核心竞争力构建与价值转换方面的经验与建议，并补充了业界在公有云、私有云、行业云以及电信网络云化商用落地与技术应用方面的成功优秀实践。与此同时，针对两年来云计算在前沿创新领域最新进入人们视野的新热点，诸如Docker容器与微服务敏捷迭代、大数据与数据库云化、行业建模与机器学习算法、混合云与管理自动化编排、云生态建设等，我们在第2版中也重点新增了对其技术与架构发展动态以及应用前景的探讨，希望能给大家带来更多的启发与帮助。

在此，我谨代表全体参与本书编纂写作的专家团队，再次衷心感谢广大读者的持续关心与支持！愿大家在云计算产业化发展之路上共勉，收获更多、走得更远！

顾炯炯

序言一

早在3000多年前,《易经》出现时,人类使用朴实的哲学思想揭示了一个变化的世界。变化无所不在,体现在政治、经济、社会、科学等方方面面。其中科学技术的发展变化,是这几个领域中被人们最能感同身受的。在科学技术领域,IT技术又成了科技变化发展的急先锋。IT领域的“云计算”在2007年还是个未知概念,到2014年“云计算”不仅已经家喻户晓,而且在基于云计算平台上,创造了一个又一个发展速度的新纪录:一款在云平台上的游戏,可以在几个月发展数千万用户;云平台支撑的电子商务,1秒钟可以完成数万笔交易。目前这种IT云计算领域的发展变化模式已经不再局限于令人瞠目的数字,而是已经开始向传统行业乃至国家整体经济与社会领域进行快速渗透。我们相信,在不久的将来,全球的经济、社会与科学的面貌,在云计算技术、服务与理念的推动下会焕然一新。这就是我们过去十几年常说的“信息技术革命”,在我们眼前正在发生、发展和不断演变着。

“云计算”这个名词虽然目前已经家喻户晓,而且业内基本认可美国国家标准与技术研究院(NIST)对云计算的概念定义,但人们对云计算的理解至今依旧不同。究其根因,一方面是云计算的技术、服务模式和理念在不断演进和发展变化,另一方面,云计算的宣传推广主体,出于商业或理念的差异而对云计算的内涵进行了不同方向的强化和引申。人们对云计算的不同理解,势必引发概念定义上的争议,但一个不争的共识是:云计算已经落地生根,并快速地发展壮大,“像用电一样使用信息服务”的云计算理想虽然还未完全实现,但距离这个目标已经越来越近。我们每个人对云计算的发展阶段同样可能有不同的理解和划分,这很正常,也很有益,因为多样化的观点碰撞是创新灵感的源泉。本书也将“云计算”的技术内涵进行了更大范围的发展和延伸。这让我联想到互联网行业正在发生的变化,早期的互联网公司仅仅开发与其直接相关的web网站,但现如今,大型互联网公司,所做的产品与业务早已远远地超出当初的范畴,不仅在看似简单的web网站下面搭建了一个庞大的数据处理与分析平台,而且支撑其网站的服务器、存储、网络乃至数据中心这些硬件产品均由互联网公司自己研发与设计,领先的互联网公司做的产品还远不止这些,Google推出了手机操作系统、眼镜,并致力于开发、完善无人驾驶汽车;亚马逊开发无人飞机用于物流投递;Facebook在虚拟现实领域进行了高额投入;国内的阿里、腾讯等公司在开发各种金融类创新产品。针对这些巨大的变化,在没有更好的名称之前,我们依然要称呼它们是互联网公司,我们只能说当今互联网的含义比10年前的互联网更加宽泛。“云计算”也是如此。在IT领域,基本上每3~5年便会进行一次产品技术的更新换代,云计算经过多年发展,无论在技术深度还是在技术广度上均会有显著延展。通过阅读此书,可以明显感受

到云计算技术这些年来的发展和进步，以及云计算技术在企业IT和电信网络重构中的作用。

云计算不仅对企业和电信的发展有重大的推动作用，对教育科研领域也将有深远的影响。“云计算”是由企业提出的概念，并一直由企业主导“云计算”技术的研发、推广与应用。特别是云计算所支撑的大数据概念与技术的出现，企业主导，特别是互联网企业主导技术发展的趋势更加明显。之所以企业能够主导云计算与大数据技术的发展，原因可能来自三个方面：一是企业拥有的雄厚资金；二是云计算技术与企业应用及市场需求呈现出了紧耦合的发展；三是企业(特别是互联网企业)拥有足量的数据资源和计算资源。企业主导，也同时意味着传统先有理论后有应用，大学科研机构负责理论(学术)创新，企业负责应用创新(工程实践)的分工模式，在云计算与大数据领域基本不再适用。大学教育科研机构，特别是信息技术学科，需要调整自身角色来顺应这一趋势的发展。云计算领域提供了非常丰富的开源环境，例如OpenStack、Hadoop、Xen、KVM等，互联网同时提供了数量庞大的信息技术文章，云计算厂商会提供免费或低价的试用软件或云计算环境，再加上不断出版更新的信息技术类书籍，这些资源构成了一个开放且实时更新的教学乃至实验环境，可以供广大学生学习 and 实践使用。未来大学对学生的培养工作可能将集中在四个方面：方向性的指导；综合技能的认证；给学生提供专心学习交流的环境；为学生搭建创新的平台。大学的信息技术类学科的科研机构，需要与企业 and 市场更加紧密的结合，双方共享数据，共享研发测试环境，专利交叉共享，项目收益共享。大学科研机构可侧重承担企业偏远期的云计算与大数据技术的开发，企业侧重承担近期应用技术开发，双方的界限会很模糊。在云计算时代，年龄、资历和职称都不再是科研创新的门槛，大学生可以广泛参与和承担云平台类产品应用开发，学生的自主创新成果(同时参照产品受市场欢迎的程度)将是个人能力认证的一个重要依据。

希望本书的所有读者，在了解到云计算技术的同时，都能够积极地投身到云计算产业实践中来。只有更多的人认识到云计算的价值，才能挖掘出更多云计算的价值，云计算产业才会有源源不断的动力来蓬勃发展，相信读者中的很多人都将成为云计算产业的中坚力量。

李德毅

中国工程院院士，国际欧亚科学院院士

合作创新，云以致用

云计算从概念到大规模实践，短短数年间迅猛发展。它与诸多行业深度融合，带来了颠覆性的创新，凸显出巨大应用价值和发展前景。读到华为公司云计算首席架构师顾炯炯新著《云计算架构技术与实践(第2版)》，我倍感兴奋。著作概括了华为的云计算构想，表明华为云计算布局已走在行业的前列，也预示着英特尔和华为在云计算方面的合作将更加密切。

随着计算的延伸与扩展、移动互联网的发展，中国消费者拥有了越来越多的智能设备。为了让消费者在不同时间、不同场合获得实时信息服务，需要将各种内容和应用通过云端进行整合、匹配，推向不同的终端用户，实现从云到端高效顺畅的体验。从电信运营商到服务提供商，通过云架构部署各种移动设备和个性化服务，无疑是非常经济、便捷的途径。

同时，在经济发展和行业变革中，人们所遇到的挑战也日益复杂，需要综合的解决方案来应对。例如，在城镇化进程中，利用云计算结合物联网与大数据解决方案，可推动智能交通、平安城市、智慧医疗、环境监测等项目建设，带来更好的城市运行管理和公共服务。将云计算与传统行业融合，将带来跨界创新，催生前所未有的商业模式、产业生态。云计算越来越从一种降低成本与提高效率的方式，演变成向企业和消费者提供新服务的途径。

面对在线应用、服务和数据的高速增长，数据中心规模急剧膨胀，需要对数据中心 IT 基础设施的主要组成部分——服务器、存储和网络设备进行以软件定义为导向的创新，实现自动供给的 IT 资源池。英特尔于2013年开始践行“软件定义基础设施”战略，在开放平台上由用户自行定义他们的基础设施，这将使用户在云资源池内“调兵遣将”时更加轻松，进而也让他们的新应用和新服务更快得到底层支持，实现迅速交付。

英特尔长期专注于计算的创新，我们提供从服务器到存储、网络全面的计算能力及软件优化支持，与产业伙伴共同应对各种云计算发展难题，真正实现“云以致用”。为此英特尔与产业界协同合作，基于开放架构推出了英特尔云构建计划，帮助开放数据中心联盟发掘和定义企业用户的云计算需求，并提供丰富的云计算解决方案。

携手推动云计算创新，英特尔与华为的合作是一个很好的例证。华为不仅在通信行业处于领先地位，过去几年间其云计算业务也成倍增长。英特尔与华为的合作由来已久，双方都较早受到信息通信

产业中最大的潮流——信息技术和通信技术融合的影响，合作领域不断拓展，从最初在通信领域，扩展到服务器、存储、网络领域，现在又把共同的目标放在了云计算和大数据的创新机会上。我们对双方的合作前景充满信心。

中国互联网用户众多，信息终端普及率很高，企业及消费者对于IT技术的了解和接受速度也非常快，再加上政府大力支持云计算产业，并实施宽带中国战略，这就使得中国在云计算部署规模、技术以及商业模式创新方面迅猛发展。我们期待着与国内合作伙伴深化和扩展合作领域，让更多源自中国的云计算创新成果去影响并推动全球信息技术和通信产业的发展进程！

杨叙
英特尔公司
全球副总裁兼中国区总裁

前 言

什么是云计算？美国国家标准与技术协会(NIST)对此有这样一个权威和经典的定义：“所谓云计算，就是这样一种模式，该模式允许用户通过无所不在的、便捷的、按需获得的网络接入到一个可动态配置的共享计算资源池(其中包括了网络设备、服务器、存储、应用以及业务)，并且以最小的管理代价或者业务提供者交互复杂度即可实现这些可配置计算资源的快速发放与发布。”

云计算的核心可以用五大基本特征、三种服务模式以及四类部署模式来概括。五大基本特征是：按需获得的自助服务，广泛的网络接入、资源池化、快捷的弹性伸缩以及可计量的服务。三种服务模式为：云基础设施即服务(IaaS)，云平台即服务(PaaS)，以及云软件即服务(SaaS)。四类部署模式可以划分为：专有云(私有云)、行业云、公有云，以及混合云。

从各类云服务的创建、部署以及消费角度来描述云计算的实质，意味着云计算天然要求支持面向服务的能力。现代企业通常会将其IT基础设施、业务平台以及软件即服务的对外开放作为其整体端到端企业信息架构SOA解决方案中的重要一环来执行。当然软件即服务(SaaS)作为一个流行多年的话题，其最早出现是在云计算概念出现之前，其实已经不是什么新鲜概念了。

以亚马逊2006年3月13日发布的S3服务为起点，到“云计算”概念2008年最早被Google提出，至今已有10年多的历史了，其核心理念已广为人们所传播和接受，也经历了方兴未艾的发展。当云计算还处于概念炒作的初始阶段时，云计算一度成为IT业界、媒体传播渠道，乃至所有涉及IT信息化、政府宏观规划、关系国计民生的各大垂直行业关注的焦点，云计算也因此成为街头巷尾热议的“时髦”话题，与此同时，各种关于云计算的商业和解决方案应运而生，各类理念和包装良莠不齐、不一而足，反而让大家对云计算到底能做些什么，对其潜在的客户到底能够解决什么实际问题，能够带来什么样的实际价值感到迷惘，使得大家对云计算的未来前景产生了怀疑。

关于云计算的社会价值与意义，我们常常用一句话表达云计算的目标诉求：“未来让人们像用水和用电那样使用云计算”。在这里，人们将云计算视为一种“水和电”那样无处不在、人类社会日常生产和生活过程中必不可少的基础资源。这里我们用“电力”来形容云计算可能更为恰当，因为电力是上一个工业文明时代最关键的生产资料。电灯、收音机、电视机、电冰箱、电风扇，乃至于自动化生产线等无不需要依赖于电力驱动。相比电力，云计算则对应于当前的知识与信息时代进行任何信息分析与处理的生产资料，用于支撑ERP/CRM/Email/BI大数据乃至金融实时交易数据处理等所有维持企业业务正常运作所需的按需获取、按需分配的关键资源。

从技术架构演进的视角来看，有人将云计算视为自IT领域冯·诺依曼计算机架构诞生之后的第三

次里程碑式的变革，是对传统计算架构与计算模式的颠覆与创新。也有人认为云计算无非是一种商业理念上的包装，所谓“新瓶装旧酒”，只是各个IT厂商用来“促销”自己产品的一种“营销活动”，并没有带来根本性的技术变革，也并没有给IT架构带来根本性的变化，那么真相究竟是怎样的呢？

回顾企业IT架构演进的整个历史，我们不难看到，冯·诺依曼架构的第一台计算机诞生以来的前30年，计算高度集中化、支持多用户多任务的大型机和小型机是企业IT的主流形态，构成IT系统的软硬件堆栈各层之间缺少统一的工业标准，呈现出内聚与耦合的特征，仅少数厂家拥有提供端到端高度复杂化的IT系统软硬件的能力。那个时代的IT系统造价高昂，往往是少数高端企业才能拥有的“奢侈品”。

于是，20世纪80年代，以x86服务器和PC系统的诞生为标志，企业IT系统迎来了第二次里程碑式的变革：从All in One、全封闭的软硬件栈走向了水平分层的网络、存储、服务器、操作系统、中间件、应用层等多层次水平分工的架构，各层之间接口标准化、规范化，极大简化了每一层的技术复杂度，各层IT产业链获得了大繁荣与大发展，涌现出一批优秀的专业化厂家，聚焦于提供该领域内质量最佳的产品和解决方案，IT系统终于开始走入“寻常百姓家”。

然而，所谓“物极必反”，当这个架构分层发展到一定阶段，弊端逐步显现。由于企业IT的层次太多，各层之间集成交付的难度越来越大，尤其是当今企业软件应用已从单一实例应用，迅速走向大规模分布式应用，一个关键业务的部署往往需要涉及服务器、网络、存储等各方面基础设施资源的协同配合，业务驱动的基础设施层服务器、存储、网络资源的集成管理配置和按需供给成为影响企业IT快速响应企业业务需求的关键制约因素。同时软硬件各层的开发虽然实现了解耦，部署和运行态仍然是软硬件耦合绑定的关系，因此跨服务器的资源出现忙闲不均时，依旧无法有效利用IT资源。

随着企业信息化进程的不断推进，企业IT系统的使用者和维护者们逐渐发现，分层架构体系也存在着诸多弊端：

- ❖ 软硬件开发态解耦，但部署和运行态并未解耦。
- ❖ 生态链大繁荣的同时，多厂家硬件异构集成与管理的复杂度越来越高。
- ❖ 企业信息化的重心向软件转移，但计算、存储、网络硬件弹性供给能力及其相互协同的不足，越来越成为软件价值提升的制约性因素。

那么，是否存在一条IT架构演进路径，可以在代价最小化，即在不对现有软硬件堆栈做颠覆式改动的前提下，有效应对上述关键痛点与挑战呢？

答案是肯定的，这就是IT领域的第三次里程碑式演进变革：从PC+服务器时代迈入云计算时代，通过虚拟化与云调度管理技术，将来自不同厂家的、多台烟囱式的、彼此孤立和割裂的计算、存储、网络设备在逻辑上整合成为一台“超大规模云计算机”，为上层的软件提供弹性的按需资源供给的能力，从而实现软硬件部署过程与运行态的解耦，屏蔽软硬件异构多厂家差异性与复杂度，并填补计算与存储之间的性能鸿沟。

大家也许已经注意到，我们谈到云计算驱动的第三次IT架构变革浪潮，其实早在云计算理念问世前的几年时间里，在众多互联网厂家中已被多次实践过，并且取得了巨大成功。那么普遍意义上的企业IT的云化重构又与互联网成功的实践之间存在着什么样的关联呢？

Google、Facebook的“云计算”服务于其特定商业模式和业务应用，例如搜索类、社交类应用，而企业IT云化架构所期望的“云计算”，则面临着大量的、形形色色的面向传统IT基础设施架构开发的企业应用和电信应用，他们的应用场景需求既有相同点，也存在着巨大的差异化。

相同点在于：

- ❖ 计算、存储实现了大规模资源池化，实现了规模经济效益；

- ✧ 对于分布式架构与负载均衡能力，资源可按业务需求灵活扩展伸缩；
- ✧ 依赖分布式软件在系统整体层面而非单点硬件层面实现高可靠性及高性能保障。

不同点在于：

- ✧ 普适性——互联网平台一般仅为其特定业务模型定制，企业云平台则要求具备对异构多厂家应用的普遍适用性；
- ✧ 异构兼容性——企业云平台需要考虑异构厂家硬件的兼容性，需要对企业IT基础设施现有投资提供最大化的保护；
- ✧ 高性能——互联网业务虽然并发量和注册用户量庞大，但企业高端应用在时延和性能方面却有更高的要求；
- ✧ 自动化、虚拟化——互联网业务模式一般为自主开发、自主运营(DevOps, Development和Operations的组合)，因此对管理自动化要求不迫切，企业应用则由于应用颗粒度不一，基础设施采购自第三方，因此管理自动化和虚拟化基本为必选能力。

“天下大势，合久必分，分久必合！”，云计算时代IT基础设施演进的下个十年，是从分离重新走向融合的十年：

- ✧ 通过云操作系统，将数据中心多厂家异构的计算、存储、网络资源进行水平融合，对外提供开放与标准化的IT服务接口，实现面向利用IT基础设施的“融合”；
- ✧ 通过超融合架构，单厂家计算、存储与网络资源进行垂直融合，提供模块化、一站式、高性能、性价比最优、面向新建IT基础设施的交付模式。

无论IT架构如何螺旋式演进，客户价值和驱动力都体现在：

- ✧ 更低的TCO；
- ✧ 更高的业务部署与生命周期管理效率；
- ✧ 更优的业务性能与用户体验。

IT基础设施架构从分离重新走向融合，并非简单的历史重复，而是在继承现有成果基础上的创新突破。无论水平融合，还是垂直融合，在核心技术支撑方面并未将现有已形成产业规模的x86 CPU及其服务器计算架构推倒重来，而是在最大限度地重用这些成熟产业组件的前提下，借助虚拟化及分布式云计算调度管理软件的作用，将多厂家异构，或者单厂家同构的计算、存储、网络整合为规模可大可小的“云计算机”，从而有效地解决传统IT架构所面临的业务上线周期长、TCO居高不下、企业关键应用性能低下的问题和挑战。

目 录

第 1 章	云计算的商业动力与技术趋势	1
1.1	云计算基础概念与架构	2
1.2	云计算的商业动力：企业ICT转型	3
1.3	企业云计算的发展趋势	12
第 2 章	云计算的架构内涵与关键技术	19
2.1	云计算的总体架构	20
2.2	云计算架构关键技术	34
2.3	云计算核心架构竞争力衡量维度	47
2.4	云计算解决方案的典型服务与落地架构	51
第 3 章	云计算及大数据开源软件概览	65
3.1	OpenStack概述	66
3.2	容器开源软件：Kubernetes / Mesos / Docker	72
3.3	大数据开源软件：Hadoop/Spark	73
3.4	开源还是闭源	81
第 4 章	面向计算资源共享最大化和自动化管理的软件定义计算	83
4.1	XEN/KVM虚拟化引擎	84
4.2	基于OpenStack Nova的计算资源池调度算法	86
4.3	计算高可靠性保障	91
4.4	针对企业关键应用云化的虚拟化调优	92
4.5	基于OpenStack Ironic的裸金属服务	101
4.6	异构适配多种Hypervisor类型	106
第 5 章	面向应用敏捷化部署的Docker容器及其调度	108
5.1	容器典型应用场景	109
5.2	Docker容器关键技术	110
5.3	容器操作系统	112

5.4	Docker容器资源管理调度和应用编排	115
5.5	Docker容器与软件定义计算的集成	123
第6章	分布式软件定义存储概述	128
6.1	分布式软件定义存储	129
6.2	支持企业关键应用的软件定义块存储	135
6.3	传统存储SAN/NAS的管理整合及性能加速	142
6.4	分布式对象存储	143
6.5	面向云存储服务的QoS/SLA管理	148
6.6	分布式软件定义存储的Erasure Code, 分布式重删压缩	149
第7章	面向自动化、多租户的软件定义网络	153
7.1	网络虚拟化的驱动力与关键需求	154
7.2	软件Overlay SDN网络, L2/L3网络	164
7.3	硬件Underlay SDN网络	170
7.4	软件化L4~L7网络功能	172
7.5	网络虚拟化端到端解决方案	176
第8章	无边界计算的混合云	186
8.1	混和云的驱动力与背景	187
8.2	典型的混合云架构模式	189
8.3	基于OpenStack级联的开放异构混合云	190
第9章	PaaS应用开发平台	193
9.1	PaaS简介	194
9.2	基于Docker的新型PaaS	195
9.3	消息中间件服务	198
9.4	数据库和缓存服务	200
9.5	大数据服务	201
第10章	大数据平台核心技术与架构	205
10.1	大数据特点与支撑技术	206
10.2	企业级Hadoop	208
10.3	流处理技术	220
10.4	大数据在金融领域的探索与实践	225
10.5	未来大数据应用畅想	230
第11章	企业桌面云接入的关键技术架构与应用	235
11.1	桌面云接入概述	236
11.2	桌面云接入的架构	239
11.3	桌面云接入的典型应用	239

11.4	桌面云接入的关键技术	244
11.5	面向多租户的企业桌面公有云服务	252
11.6	终端无关的移动办公接入	254
第 12 章	第三方云应用生态Marketplace及应用编排自动化	259
12.1	基于开放云平台的云生态系统构建	260
12.2	Marketplace系统架构	262
12.3	面向电信网络和业务云化的CT编排自动化-MANO	262
12.4	面向IT应用的IT编排自动化——Heat & TOSCA	270
12.5	TOSCA(云应用的拓扑编排标准)	272
第 13 章	云微服务敏捷治理架构与组织流程	275
13.1	从瀑布式到敏捷式，从服务到微服务	276
13.2	微服务的治理架构	278
13.3	支撑敏捷开发与上线的微服务CI/CD工具链	286
13.4	面向微服务的DevOps研发运维组织变革	288
第 14 章	云安全架构与应用实践	290
14.1	端到端云安全架构	291
14.2	可信计算TPM/vTPM	294
14.3	虚拟机的安全隔离	298
14.4	虚拟化环境中的网络安全	300
14.5	云数据安全	301
14.6	公有云、私有云的安全组	303
14.7	云安全管理	304
14.8	安全即服务	306
14.9	云安全应用实施案例	306
14.10	云计算安全的其他考虑	307
14.11	云计算服务法律风险及其应对	308
缩略语		319
后 记		329

第 1 章

云计算的商业动力与 技术趋势

1.1 云计算基础概念与架构

云户端、服务器端并重的传统模式，向以“广泛的网络接入”、“计算、存储的集中资源池化”、“快捷的弹性伸缩”、“按需自助及可计量的服务”为典型特征的云计算模式的演进铺平了道路，并掀起了正在席卷全球的第三次IT变革浪潮。

在传统IT体系架构下，当前企业基础设施建设与运维所面临的核心痛点问题可以总结概括为如下几点。

1. 平均资源利用率及能耗效率低下

针对基础设施平台建设、扩容与更新换代，当前企业普遍采用的模式是服务器、网络交换与安全，以及存储设备的水平分层采购。各个IT基础设施单部件的选型、数量以及不同部件的组网连接方案均取决于企业IT收集的各业务部门对于IT核心业务处理量需求的预测和规划。同时所有企业IT应用软件、数据库以及中间件软件均采用独占计算、存储和网络资源的烟囱式部署。软件应用与硬件唯一捆绑，不同应用之间无法动态、高效共享相同的计算与存储资源。加之按照摩尔定律不断翻番增长的CPU计算能力已大大超出应用软件对计算资源利用率的同步能力，导致企业IT的平均资源利用率始终处于低于20%的水平。

2. 新业务上线测试周期长，效率低下

企业任何一项新业务上线，从最基础的硬件平台开始，向上逐层延伸至操作系统、中间件、数据库、CRM/ERP/HRM/PDM/Email/UC等各类业务关键软件堆栈，均需要投入IT专业化团队，进行软件安装、调试、功能与性能验证测试、网络配置及修改调整，然后经过若干轮测试、故障及性能稳定性测试定位及重配置和调整之后，才能最终达到期望正式上线运行的成熟度水准。这个过程一般需要长达2至3个月的时间。

资源储备及弹性伸缩能力不足，不具备应对企业IT突发业务高峰处理的能力

针对特定垂直行业短时间内突发性的高流

量、高密度业务需求(比如节假日期间对视频网站的突发业务流程冲击)，企业内部物理基础设施资源往往无法满足短时间内迅速获取所需资源的需求，以及处置业务高峰过后的资源闲置问题。

3. 企业核心信息资产通过个人办公PC/便携外泄的安全风险，无法在个人智能终端(平板电脑、智能手机)方便地访问企业防火墙后的 workflow 及文档

部分企业核心信息资产通过员工个人PC电脑或便携设备外泄给竞争对手，对企业竞争力和商业利益带来负面影响。过分严格的信息安全管控措施又导致了工作效率的下降，企业管理层及员工无法便捷地通过无所不在的网络访问企业防火墙内部的信息资产。

4. 中小型企业希望通过宽带网络管道，从电信运营商或其他主机托管运营商的托管应用数据中心“按需获取”其所需的企业IT应用能力，从而实现日常运作中IT成本开销最小化

数量众多的中小企业，缺少IT领域专业经验，甚至没有财力和精力建设和维持自己专属的IT部门以及IT基础设施平台，普遍希望可以直接从托管运营商那里获取支撑其日常业务运作所需的SaaS服务。

针对解决上述企业IT系统建设和维护过程中遇到的普遍痛点问题，迫切呼唤业界IT软硬件解决方案提供商借助云计算技术，打造TCO、性价比与效率最优的“IT基础设施私有云及公有云”，具体包括：

✎ 面向大型企业和行业领域提供全自动化管理、一站式交付、支持与企业ITIL无缝集成融合、TCO最优化的端到端解决方案，实现企业传统IT基础设施及应用的改造、扩容和新建；

✎ 面向中小型企业(SMB)，提供支持多租户安全隔离与动态发放、超大规模资源池调度管理、可最大限度发挥规模经济效益的公有云托管解决方案。

无论上述哪一类形态，企业云计算IT基础设施平台均可定位于基础设施、中间层云平台服务、云计算业务发放与维护管理。针对云平台