云服务的安全运维平台

汤 涛
(北京世纪互联宽带数据中心有限公司蓝云事业部 北京 100016)
(tang.tao2@oe.21vianet.com)

Secure Operation Platform for Cloud Service

Tang Tao
(*BlueCloud Department of Beijing 21Vianet Co. Ltd., Beijing* 100016)

Abstract Cloud Service is a very popular IT service in the past years. The service quality of Cloud Service typically depends largely on the quality of Cloud Service Operation. How to provide reliable, trusted and secure Cloud Service to customer, will crucially rely on a secure operation platform. In this article, transformation from traditional IT operation to Cloud operation and its differences are briefed. The secure operation platform model and core content are elaborated. And then all components of secure operation platform are analyzed and explained. Meanwhile, Cloud security and compliance are elaborated.

Key words cloud service; operation platform; cloud security; cloud compliance; cloud service operation

摘 要 云服务作为一种近年相当热门的IT服务,云服务的服务质量往往取决于运维的质量.如何为用户提供可靠的、可信的、安全的云服务,安全的运维平台就尤为重要.针对云运维的要点、难点和重点,介绍了从传统IT运维到云运维的变迁及其差异,阐述了安全的运维平台的模型和核心内容,并且对安全运维平台的各个组成部分进行了分析解释,同时还阐述了云安全与云合规.

关键词 云服务;运维平台;云安全;云合规;云运维

中图法分类号 TP309.2

早在2015年1月,国务院印发《关于促进云计算创新发展培育信息产业新业态的意见》[1],为促进创业兴业、释放创新活力提供有力支持,为经济社会持续健康发展注入新的动力.《意见》提出,要加快发展云计算,打造信息产业新业态,推动传统产业升级和新兴产业成长,培育形成新的增长点,促进国民经济提质增效升级.到目前,我国云计算服务能力大幅提升,创新能力明显增强,在降低创业门槛、服务民生、培育新业态、探索电子政务建设新模式等方面取得积极成效,云计算数据中心区域布局初步优化,发展环境更加安全可靠.预计到2020年,云计算成为我国信息化重要形态和建设网络强国的重要支撑.

云计算是一种新兴的计算模型,它是在网格

收稿日期:2017-04-15

计算的基础上发展起来的[2]. 目前已经在社会各个领域发挥着多方面的作用,从支持网站的发布、支撑企业应用、移动互联网、物联网、大数据等等这些往往在底层都离不开云计算的支持. 云计算本质上是一种按使用量付费的服务模式,类似于水电等公共服务,这种服务模式可以为用户提供无所不在、便捷的、按需的网络访问,进入可配置的计算资源共享池(包括网络、服务器、存储、应用和服务),这些资源在只需投入微乎其微的管理工作,或与云服务提供商进行极少的交互就能被快速获取或者释放[3].

云计算作为一种服务,必然会深刻影响和改变软件开发、软件架构、软件测试、系统运维等包括整个软件生命周期的各个阶段各个方面. 随着云计算的不断发展壮大,云又可以按照共享的模型分为公有云、私有云和混合云等. 本文从多个角度多层面探讨公有云的云运维、云安全以及与传统 IT 运维的关系和区别.

1 云时代运维的变迁

由于云计算服务与传统的 IT 计算有所不同,传统 IT 是硬件厂商提供硬件,平台软件服务商提供平台软件,应用软件服务商提供应用软件,通常由企业 IT 部门负责企业的这些硬件、平台软件和应用软件的运行维护. 而在云计算应用场景中,这些运行维护通常就会切分成由云计算服务商和企业 IT 部门分别负责各自的服务. 一般而言,由云服务商负责机房、网络硬件、服务器硬件、云平台、虚拟机以及一些相关的网络服务等组成部分的运维;而由用户负责虚机内的操作系统、应用程序等的运行维护. 由于云本身通常又分为 3 层,即基础结构即服务(infrastructure as a service, IaaS)、平台即服务(platform as a service, PaaS)和软件即服务(software as a service, SaaS)[4]. 在云服务这 3 个层面,云服务商和用户各自负责的部分又有差异,如图 1 所示.

其中,IaaS 在虚拟机及虚拟机以下,皆由云服务商负责运维,而虚机内的操作系统以及之上的部分则由用户自主负责管理. 对于 PaaS 而言,在运行时以及以下部分是由云服务商负责运维,而用户只需要负责数据和应用. 如果是使用 SaaS,对于用户而言就会变得相对简单,因为用户基本上不需要负责与应用相关的任何运维,都是由云服务商提供,也就是说就这些系统而言,用户的 IT 部门基本上不需要任何相关的运维.

因此,在云时代,就 IaaS 和 PaaS 而言,传统的 IT 运维发生了根本性的变化,原有的运维体系切分成 2 部分,云平台部分由云运营商负责,而云平台之上的部分则由用户的 IT 部门负责. 对于 SaaS,传统的 IT 运维则完全转移到云运营商负责.

同时对于云服务商而言,为了满足多用户的不同需求,使得云平台底层硬件和数据中心的规模都需要扩大,数据中心机房、机架、核心路由设

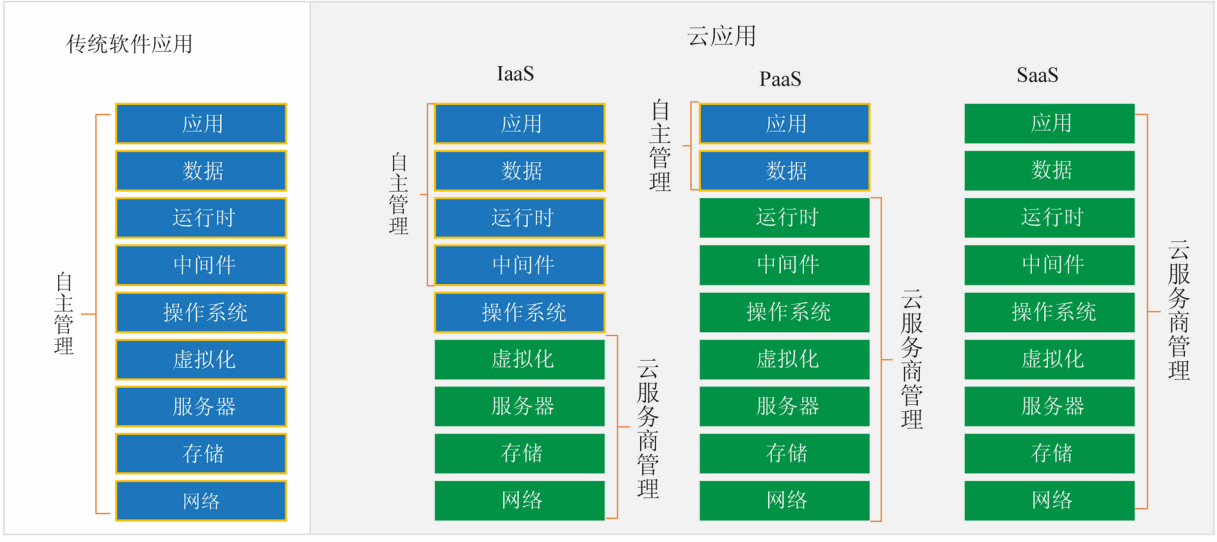

图 1 传统软件应用与云应用

备和服务器等硬件基础设施也需要相应地投入，这就与之前传统互联网数据中心(Internet Data Center，IDC)的运维又不一样. 正是由于云服务需要大量的物理基础设施，因此，对于传统的IDC在业务模型上向云转移更有得天独厚的优势，同时由于云业务的兴起和蓬勃发展，也在一定程度上倒逼传统的IDC在云业务方面通过多种不同方式在转型.

2 云运维与传统运维

传统IT运维本质上而言是面向单服务器机或者服务器聚群的运维，而云运维则是相当于把整个数据中心甚至多个数据中心当成一套大而全的物理硬件设备，在其上部署云操作系统，实现在云操作系统的虚拟主机内部署客户的应用程序，如图2所示[5].

由此，传统IT运维向云运维的转变就不再是简单的单服务器到多服务器，而是涉及大规模硬件、云操作系统、虚拟主机、虚拟网络、跨虚拟主机的协同等等多层面多方位的增加. 同时云服务的业务模型也决定了云运维与传统运维的差异，本质上云运维是综合了IDC基础设施运维和企业级IT运维，涉及面从底层IDC基础设施运维，即业内常说的风火水电等，到服务器物理硬件，再到云操作系统，然后是虚拟网络、虚拟机等等，一整套全方位多层面的运维体系. 如果直接给一个相应的定义，云运维就包含了IDC基础设施运维、传统企业级IT运维的底层部分，当然其规模要大出很多，以及云业务相关的一系列外围系统. 由于云业务与传统IDC以及企业IT业务也完全不同，因此，还需要很多额外的外围系统作为云业务的支撑，这些系统也是云运维的一个重要组成部分. 这些外围系统通常就包括业务和运维支撑服务系统(business and operation support service，BOSS)，或者也会经常拆分成业务支撑服务系统(business support service，BSS)和运维支撑服务系统(operation support service，OSS)，如图3所示.

在云时代，运维模型发生了根本性变化，云技术提供商与传统解决方案技术提供商类似，但是由于云本身的特殊性，需要不断地在生产环境，即云环境中升级底层应用系统. 这就使得云技术提供商需要更多的团队来管理和分发部署包，而且是在生产环境中升级，不像之前企业级IT运维那样，可以随时对某部分服务器停机来升级，就有点类似于给行驶中的汽车换轮胎，需要多工种一起协同才能达成. 这样就需要增加很多不同的角色来负责协调和管理，比如云服务整合经理和云服务提供经理等等诸多传统IT并不需要的一些角色. 云产品交付后也不再是直接交给用户去使用和运行维护，而是交付给云服务提供商. 而云服务提供商则需要比传统IT扩充更多的角色，不单单是增加BOSS系统，而且更为重要的是需要增加云服务和业务服务、客户支持、部署管理、过渡和迁移管理、运维管理、安全和风险管理等等诸多涉及跨用户的服务. 而这其中大部分服务都需要7×24×365的支持. 因为云服务上的用户多种多样，业务系统也多种多样，有的用户要求高，有的用户要求低，有的用户可以接受5×8(5个工作日，每天8h支持)，有的客户则需要7×24(全天候支持)等等，作为基础服务平台的运维而言，往往就只能选择最高的要求作为服务基线. 就像五星级酒店一样，不管客户什么时候来，什么时候需要热水等等都可以随时提供服务.

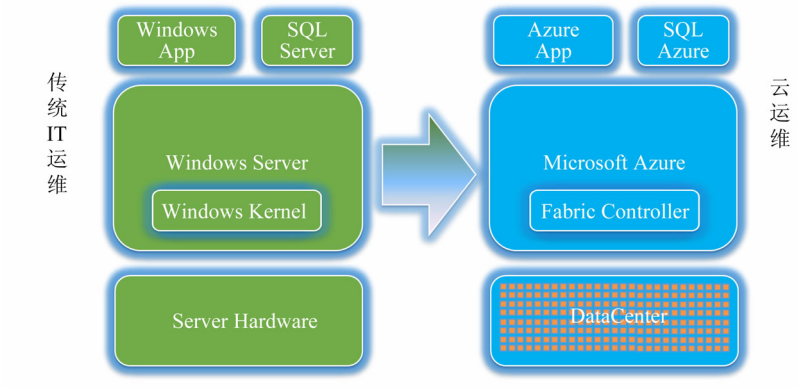

图2 传统IT运维与云运维

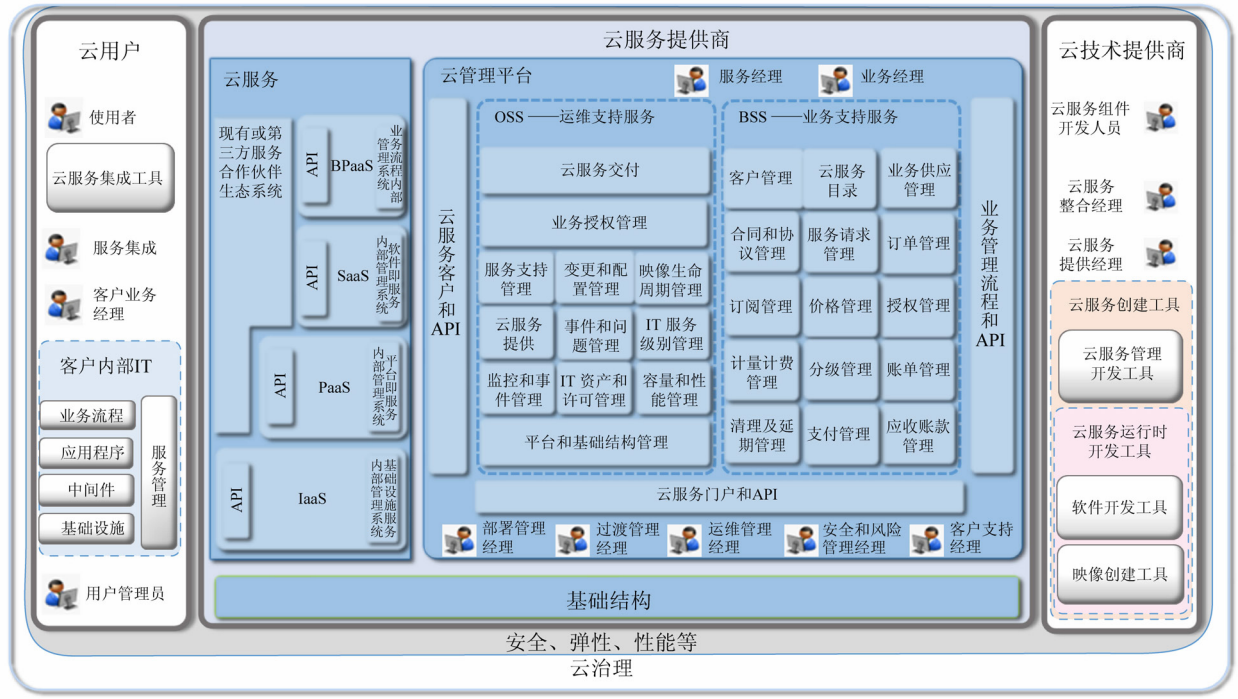

图 3　云服务模型

对于云用户而言，就不再像以前那样需要完整的运维系统及运维人员，云用户只需要关心应用解决方案层面的运维，也就是说更专注于业务系统，而不再需要关心什么时候需要采购扩充物理硬件. 这样一来，对于云运维而言，就比传统 IT 运维提出了更高的要求，也对云运维从业工程师提出了更高的要求，传统 IT 运维往往只需要考量单个或者基于群集的多台服务器，而在云运维阶段，云运维工程师需要考虑更多云服务组件的部署、多租户的资源分配、虚拟主机和网络协同等等，对工程师的要求也更高. 就云运维而言，这就需要通盘考虑，特别是不能在停机的情况下升级系统等等，这是一个很典型地从量变到质变的过程.

3　云运维平台

云运维的广度和复杂度在一定程度上就决定了对运维人员和相关运维系统的要求高度. 如何能保障云平台的稳定可靠，就需要有相关的外围系统的支撑，这些系统主要包含云平台管理系统和云服务系统，如图 3 所示，其中，云平台管理系统又可以分为如下 4 个类别：

1）运维支持服务系统. 运维支持服务系统主要提供云平台后台的运维支持相关服务. 比如，云平台的监控和事件管理、变更和配置管理、容量和性能管理、IT 资产和许可管理、平台和基础结构管理等等，其功能通常如表 1 所示.

2）业务支持服务系统. 业务支持服务系统通常包括与客户相关的商务和服务系统，比如客户管理系统、合同和协议管理系统、订阅管理和价格管理等等，这些相关系统以及其功能描述如表 2 所示.

3）业务管理流程及 API 管理系统. 由于云服务涉及多样化的流程，甚至是跨业务部门的流程，因此，业务流程的管理和各个系统之间以及系统内的 API 管理就很重要. 业务流程有的可以整合到云运维平台中，即是系统对系统的业务流程，有的可能是信息系统与纸质或者邮件的结合.

4）云服务内部管理和/或第三方合作伙伴管理系统. 云服务运维平台通常可能需要提供管理第三方合作伙伴的系统等，以及内部的管理系统，比如内部办公系统、内部邮件系统等等. 这些与常规的企业内部信息化管理系统类似，在此不再一一复述.

表 1　运维支持服务系统

系统名称	基本功能描述
监控和事件管理	负责监控云平台的各种状态和指标，并且在遇到异常情况时能自动触发生成相应事件. 运维工程师可以在系统中记录相应的事件处理过程，并且可以最终关闭事件.
IT 资产和许可管理	记录整个云平台和与平台相关的 IT 资产信息，以及各种许可的管理等等.
容量和性能管理	检索、查看和调配云平台的容量和性能的管理系统，通常需要与监控和事件管理系统对接，以便能在性能或者容量触及阈值时产生报警，并将报警信息写入到监控和事件管理系统，以便运维工程师及时处理. 该系统也有人机界面或者相应的 API 接口，以便能方便二次开发性能和容量的自动化管理.
事件和问题管理	负责记录云平台相关的事件和问题的系统，这些事件和问题往往不是由监控传感器自动发现的，而是通过日常工作中遇到或者发现的一些事件和问题，具有相对主观性.
服务级别管理	可被度量的服务绩效的管理，这些服务可以被恰当地设计以便满足定义在服务级别需求中的那些期望. 通过该系统可以更好地控制资源管理，降低使用成本，提高客户满意度以及建立更好的客户关系.
变更和配置管理	云平台规模往往比较大，系统也比较负责，如何更好地管理不同的系统配置，部署以及变更就需要一套完善的变更和配置管理系统来实现.
云服务提供管理	无论是 IaaS，PaaS 还是 SaaS 都会包含多种多样的服务，比如虚机、存储、数据库或者是各种不同的应用级服务，这些不同的服务又会有不同的规格，比如虚机可能有共享核的，有单核的，有双核的，等等. 云服务提供管理就是管理这些多样化的服务.
映像生命周期管理	映像是 IaaS 和 PaaS 平台下重要的组成部分，通过映像模板，用户可以随时快速创建所需要的虚机或者服务，映像生命周期管理就是管理这些映像的系统.
服务支持管理	用户使用过程中遇到的各种问题可能会需要云平台相关的服务支持，服务支持管理系统就是用于管理这些用户相关的支持服务的.
业务授权管理	不同的用户根据其采购的云服务，授权其可以使用的云服务的范围.
平台和基础结构管理	平台和基础结构管理通常包括数据中心、机架、电源、空调、硬件服务器、网络设备等等相关的管理.

表 2　业务支持服务系统

系统名称	基本功能描述
客户管理系统	管理所有的客户基本信息，包括用户的分类、用户的级别、用户的联系方式等等.
云服务目录管理系统	管理云服务中具体有哪些组件，这些不同组件都分属于哪些类别.
业务供应管理系统	哪些组件提供生产环境的服务，其服务的环境如何，以及对应于哪个或者哪些数据中心等等.
合同和协议管理系统	管理与用户线下合同和协议，以及合同相关的流程等等.
服务请求管理系统	针对用户的服务请求，创建相应的流程实例，并且在规定的服务级别的时间内给用户解决相应请求问题.
订单管理系统	管理用户的订单，包括有可能的多种不同级别的订单.
订阅管理系统	管理用户账户下的订阅，通常对于使用云计算服务比较多的用户，用户账户下可能包含多个订阅.
价格管理系统	管理云服务内的不同产品的价格.
授权管理系统	授权不同级别的用户能有不同的资源访问权限.
计量计费管理系统	负责对云服务的内容进行计量计费的管理.
账单管理系统	管理云服务的用户账单.
清理及延期管理系统	由于云服务有很多是先使用后付费的情况，该系统负责对于延期未付费的用户的清理和管理.
支付管理系统	管理线上线下的支付.
应收账款管理系统	管理用户的应收账款.

4　云安全与合规

云安全是一个比较大的范畴的问题，涉及到云的安全防护，比如反病毒、防攻击、防渗透等外来攻击，还涵盖用户的数据安全，比如防泄露、防监守自盗等多方面. 这些问题都是云运维中不可避免，而且需要着重强调和考虑的.

通常在云平台中，需要有多重的防 DDOS 攻击和黑客攻击渗透的工具和手段. 在防 DDOS 方面通常业界有比较流行的处理方法，比如软硬防火墙、协议分析、流量清洗、黑洞等等. 由于云平台

的用户多样性和复杂性，不仅要防由外而内的攻击，还需要注意由内向外的攻击，这种往往就是用户的虚拟机被劫持或者是恶意用户通过云平台对外的 DDOS 攻击. 而防黑客攻击方面，包含日常的漏洞扫描，及时打补丁，针对一些开源技术的可能漏洞进行跟踪. 为了防止账号和服务等的劫持，除了采用必要的双因子认证以外，还需要加强对堡垒机的安全加固，并且构建威胁分析模型，对所有可能的威胁作全面的分析，必要时执行包含白客扫描在内的多样化扫描的模拟攻击，以便找到并堵住这些潜在的风险和漏洞.

在用户之间做好严格的隔离也非常重要，比如在 Azure 平台中就有多方面的隔离措施，首先在网络上有完全的逻辑隔离技术，内网 IP 在跨用户账户之间不可以访问，在用户访问权限上有逻辑隔离，而且在数据存储上也通过加密及读写隔离措施防止用户访问之前磁盘上别的用户存储的但已逻辑删除的数据等.

再次就是增强用户数据的安全性方面，需要提供多种加密方式可以供用户选择用于保护用户存储的数据. 将所有数据访问活动记入日志，并且让用户可以访问自己的日志也是用户数据安全防护的重要手段之一. 数据的异地同步、异地容灾也有利于增强用户数据的安全性. 云运维工程师对客户数据无常设的访问权限，只有在客户提供书面授权的情况下才按照客户要求访问客户的数据，而且用户的书面授权书和相应的操作日志都完整保存，并保证可追溯. 这样也是满足国家信息安全三级等级的审计要求，以及满足工信部可信云认证的要求的重要保障，同时也是防止监守自盗的重要方法，用户对于这样的用户数据安全性就会比较有信心.

在云合规方面，根据国家法律法规的要求，不仅需要把数据物理上保存在境内，而且需要严格地提供针对各种相关法律法规的要求，以及政策方面的要求的十分严格又易于理解的解释，以便用户了解能做什么不能做什么. 按照这些要求，针对用户的数据进行存储和管理. 在合规方面还需要定期开展第三方独立审计，以便满足上述不同的合规要求. 由于云平台作为底层平台，用户部署在其上的系统需要满足合规的要求时，云服务商往往也可能需要配合并满足用户相关的合规要求.

5 结　　语

云服务的质量不仅仅取决于技术的先进性，同样重要的是也取决于云运维的服务质量. 本文从云运维的变迁入手，简要地描述了云运维与传统运维的区别，着重描述了云运维平台的各个系统以及这些系统的基本功能，同时也简明扼要地阐述了云安全以及云合规的基本要求. 这些都是云运维的重要组成部分，也是云服务商日常需要考虑和涉及的. 世纪互联全资子公司上海蓝云网络科技有限公司在 4 年多来提供 Azure 和 O365 云服务过程，一直致力于为国内用户提供世界级的云技术和云服务，为提升国内云技术和服务水平，为促进国内经济和社会的发展起到了积极作用.

参　考　文　献

[1] 中华人民共和国国务院. 国务院关于促进云计算创新发展培育信息产业新业态的意见[EB/OL]. (2015-01-30)[2017-04-15]. http://www.gov.cn/zhengce/content/2015-01/30/content_9440.htm

[2] 陈全，邓倩妮. 云计算及其关键技术[J]. 计算机应用，2009，29(9)：2562-2566

[3] National Institute of Standards and Technology. Cloud Computing [EB/OL]. [2017-04-15]. https://www.nist.gov/programs-projects/cloud-computing

[4] Mell P M，Grance T. The NIST definition of cloud computing [G]. Special Publication (NIST SP)-800-145. Gaithersburg，USA：NIST，2011

[5] Namit. Inside Azure-Deployment workflow with Fabric Controller and Red Dog Front End [EB/OL]. [2016-05-05]. https://blog.kloud.com.au/2016/05/05/inside-azure-deployment-workflow-with-fabric-controller-and-rdfe/

汤　涛

硕士，北京世纪互联宽带数据中心有限公司蓝云事业部技术运维总经理，主要研究方向为云运维云安全合规.

tang.tao2@oe.21vianet.com