

云计算服务持续监管研究

陈兴蜀, 葛龙, 罗永刚, 李想

(四川大学网络空间安全研究院, 四川 成都 610065)

摘要: 云计算环境的复杂性和动态性, 难以及时掌握云计算服务安全运行状态、评估云计算服务风险。为确保云计算服务的安全能力持续符合国家相关标准要求, 对云计算服务持续监管相关内容进行了研究, 定义了云服务商、客户和持续监管方角色, 明确各角色的监管责任、评估指标体系以及接口规范, 确保政府部门、重点行业客户稳定且安全地使用云计算服务。

关键词: 云计算; 持续监管; 云计算安全

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00105

Research on continuous monitoring of cloud computing service

CHEN Xing-shu, GE Long, LUO Yong-gang, LI Xiang

(Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China)

Abstract: The complexity and dynamism of cloud computing environment hardly lead to timely awareness of cloud computing service's operating state and assessment of cloud computing service risk. In order to ensure that the security of cloud service abidingly conforms to relevant national standard, continuous monitoring of cloud computing service was researched, and the role of cloud service provider was defined, customer, and continuous monitoring, described their supervising responsibility, and assessed index system and interface specification, thus guaranteeing stable and secure employment of cloud computing service by government department and key industries.

Key words: cloud computing, continuous monitoring, cloud computing security

1 引言

云计算是一种计算资源的新型利用模式, 客户以购买服务的方式, 通过网络获得计算、存储、软件等不同类型的资源^[1]。云计算服务以其快速伸缩、泛在接入、自助按需、资源池化、服务可计量的创新服务特性很快成为业内关注的焦点, 各地政府部门、重点行业纷纷进行规划部署。积极推进云计算服务在政府部门的应用, 获取和采用以社会化方式提供的云计算服务, 有利于减少各部门、各地方分散重复建设, 有利于降低信息化成本、提高资源利用率^[2]。

云计算的应用也带来了一些安全问题, 因此产生了对云计算安全的需求。2014年5月22日, 中国政府宣布实施网络安全审查制度。政府部门云计算服务安全审查制度作为网络安全审查制度的组成部分, 目前正在加快推进。GB/T 31167-2014《信息安全技术 云计算服务安全指南》(以下简称《指南》)和GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》(以下简称《要求》)两项国家标准作为支撑云计算服务安全审查工作的技术标准, 已于2014年9月3日发布。

《指南》和《要求》两项标准对政府部门采用云计算服务提出了安全的技术和管理要求, 促进

了云计算在政府部门的安全应用。但由于云计算服务是在线、动态地为客户提供服务,其安全能力随云计算环境的技术、管理、外部因素等的变化而改变。如何让客户安全地使用云计算服务,则需要研究对云计算服务的持续监管技术和管理方法。

2 研究现状

虽然云计算安全方面的标准研究已受到了广泛重视,但目前国际和国内都还缺少云计算服务持续监管方面相应的技术和规范标准。云安全联盟(CSA, Cloud Security Alliance)虽然提出了相关的初步框架,但后续没有具体可操作性的标准或规范推出。我国在云计算服务持续监管上的研究仍是空白,目前主要存在以下问题。

1) 缺乏在运行监管中各角色的监管责任和管理边界的界定。可能因运行监管的责任不履行或过度监管导致持续监管不能有效进行,造成安全问题处理延误及各角色相互推诿责任等问题。

2) 缺乏有效、科学的监管数据接口定义。监管分析所需的数据、接口没有统一规范的定义,会导致监管方难以从云计算环境获得所需的监管数据。另一方面,云服务提供商配合提供监管数据需要修改云计算平台,过度监管将导致监管成本过高。

3) 缺乏持续监管的评价指标体系。如何通过监管接口(以下简称监管API)获得监管数据,对云计算服务的安全能力进行有效评价,形成客观的评价结果,也是持续监管的关键难点。

本文主要讨论云计算服务持续监管框架、各角色的关系及监管责任、安全责任,持续监管的评估指标体系以及接口规范。主要目的是希望通过制定云计算服务持续监管框架及技术规范标准,让主管云计算服务安全审查的部门及时掌握政府部门、重点行业采用云计算服务的情况,有效评估云服务商所提供服务的**安全能力和安全风险,明确云计算服务环境中各角色安全责任和监管责任,从而保障客户的业务及数据安全。

3 云计算服务持续监管框架

本文提出的云计算服务持续监管框架如图1所

示,包含3个角色:云服务商(以下简称CSP)、云服务客户(主要指政府部门和重点行业的客户,以下简称客户)、持续监管方(CMO, continuous monitoring organization)。

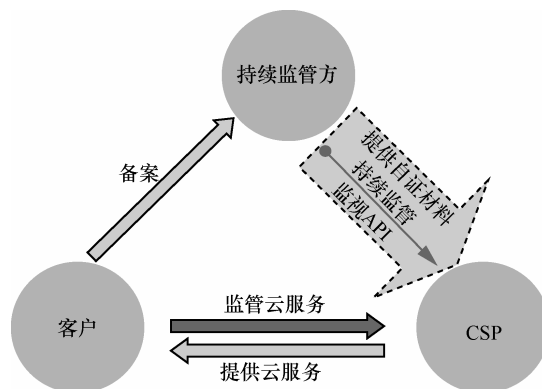


图1 云计算服务持续监管框架

3.1 各角色的监管责任

客户:租用CSP提供的云计算服务,向持续监管方提供部署在云计算服务平台上的业务、数据和安全相关备案信息,通过对CSP的持续监管掌握云计算服务质量和安全状态,并通过对自身的安全监管,保障云计算服务平台上部署的业务和数据的安全。

CSP:为客户提供云计算服务的持续监管接口,接受持续监管部门的监管,关心自身平台的运行状态与安全态势,向客户保证服务质量。

CMO:受CSP和客户的信任,评估CSP的云计算服务质量和安全状态,实时为党政用户、重点行业用户提供云计算服务的持续监管,全面掌握客户的云服务使用情况。

3.2 云计算服务持续监管实现方式

CMO应按照政府信息安全相关规章制度和标准对CSP和客户进行持续监管,CSP、客户应积极参与并配合CMO的持续监管活动。

3.2.1 对CSP的持续监管

CMO对CSP进行持续监管的主要目的是为了验证CSP是否持续实施其承诺的云服务相关安全措施,是否持续履行《指南》中所要求的安全监管责任和义务,是否持续符合《要求》中的安全能力要求。

验证方式主要通过自证和被证的方式实现,如图2所示。

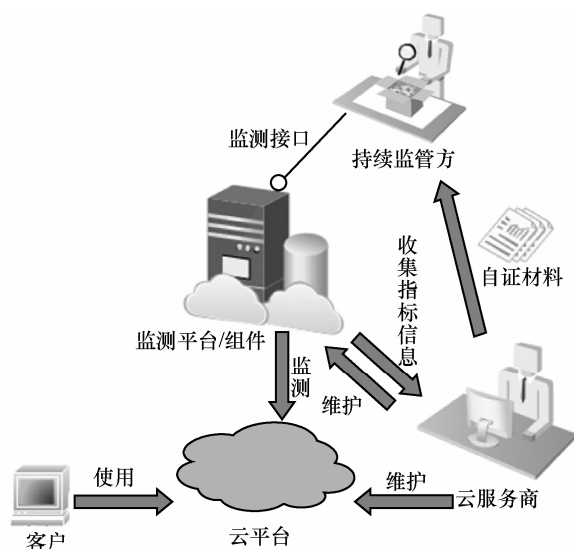


图 2 持续监管方对 CSP 的监管方式

CSP 应在本地建立并维护一个监测平台或组件用于监测云计算平台，通过制定并实施监管策略、对自身平台开展周期性的风险评估和监测、不断收集并分析指标信息以及对内持续开展信息安全教育等方式保证自身云平台的安全性。CSP 以报告的形式向 CMO 提交其制定的监管策略内容及实施的成果、或风险评估和检测方法及相关材料，实现自证。其中，CSP 提交的自证材料应根据 CMO 要求的格式和指标进行整理，并按和 CMO 协商的频率提交。

CSP 应提供监测接口给 CMO，以便 CMO 可以通过监测接口获取云平台相关数据信息，以验证 CSP 提供的自证材料的准确性，从而实现被证。

如果 CMO 对 CSP 的验证结果与 CSP 提供的自证材料的误差在可接受范围内（CMO 与 CSP 协商），则证明 CSP 满足 CMO 的监管要求，否则，应按照《要求》规定的要求及时整改，直到符合要求为止。

3.2.2 对客户的持续监管

CMO 对客户进行持续监管的主要目的是为了验证客户是否持续符合《指南》中所要求的安全监管责任和义务。

验证方式主要是通过客户向 CMO 备案的方式实现，如图 3 所示。客户应向 CMO 提交其使用云服务的基本情况（包括但不限于部门名称、部门属性、使用的云服务厂商、服务模式、

部署模式、业务和数据类型等）、自身负责的云计算环境及客户端实施的安全措施及成果等相关材料。客户提交的材料应根据 CMO 要求的格式和内容进行整理，并按和 CMO 协商的频率提交。CMO 对客户进行备案，以便国家有关部门了解当前已部署云服务的党政机关的情况和安全状态。

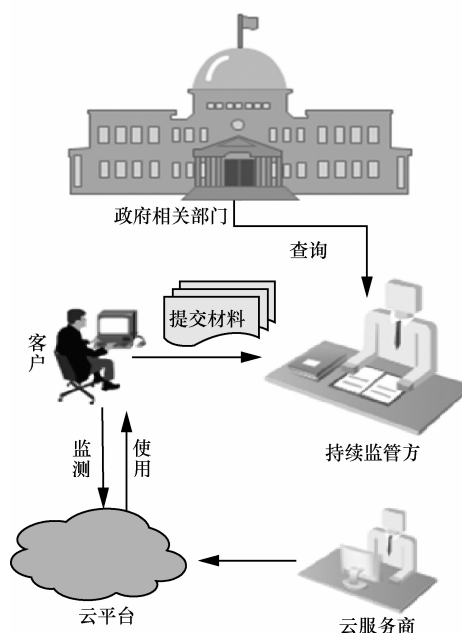


图 3 CMO 对客户的监管方式

客户所使用的云计算环境及客户端的安全应由客户负责，客户可根据《指南》中客户的监管责任对 CSP 进行监管以保证自己使用的云平台的安全性。因此，客户对 CSP 的监管不在本文讨论范围内。

如果客户云平台出现重大变更或信息安全事件，应及时通知 CMO，CMO 更新备案信息。

4 持续监管各角色的安全责任

在持续监管框架中，云计算环境的安全性由 CSP 和客户共同承担。在某些情况下，CSP 还要依靠其他组织提供计算资源和服务，其他组织也应承担安全责任。因此，云计算安全措施的实施主体有多个，各类主体的安全责任因不同的云计算服务模式而异。

本文参考《指南》中的相关内容，划分了客户和 CSP 的安全责任范围，如图 4 所示。

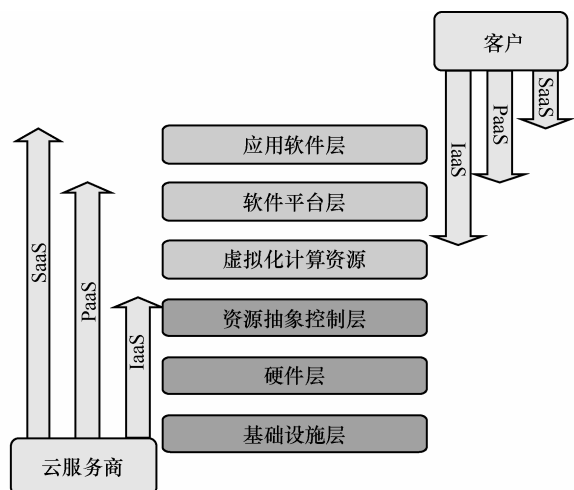


图4 服务模式与安全责任控制范围

云计算根据服务模式可以分为软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）。不同服务模式下 CSP 和客户对计算资源的控制范围不同，控制范围则决定了安全责任的边界。如图4所示，图4中两侧的箭头表示 CSP 和客户的控制范围，具体如下。

1) 在 SaaS 模式下，用户承担客户端安全相关责任；CSP 承担服务端安全责任。

2) 在 PaaS 模式下，用户承担自己开发和部署的应用及其运行环境的安全责任，其他安全由 CSP 负责。

3) 在 IaaS 模式下，用户负责分配到的虚拟网络安全，自己部署的操作系统、运行环境和应用的安全，对这些资源的操作、更新、配置的安全和可靠性负责。CSP 负责虚拟化计算资源层及底层资源的安全。

考虑到云服务商可能还需要其他组织提供的服务，如 SaaS 或 PaaS 服务模式中，如果 SaaS 或 PaaS 服务基础资源是由 IaaS 服务提供商提供的，在这种情况下，一些安全措施由其他组织提供。因此，云计算安全责任模型可归纳为如图5所示的模型。

5 云计算服务持续监管评估指标体系

评估指标体系是 CMO 监管 CSP 及客户是否符合监管要求的重要依据，评估指标的制定直接影响持续监管的实现方式。CMO 应依据《要求》中对 CSP 的安全能力的要求制定指标，并遵循由

大到小、由粗到细的方式对指标进行分类。例如，可以根据云平台的运行状态将指标分为静态指标（文档类）和动态指标（接口类），然后将静态指标具体分为信息安全策略文档、安全培训报告或记录、安全评估报告等形式。同时可以将动态指标具体分为配置信息、负载信息、流量信息等，然后再根据每个项对指标进行细化。

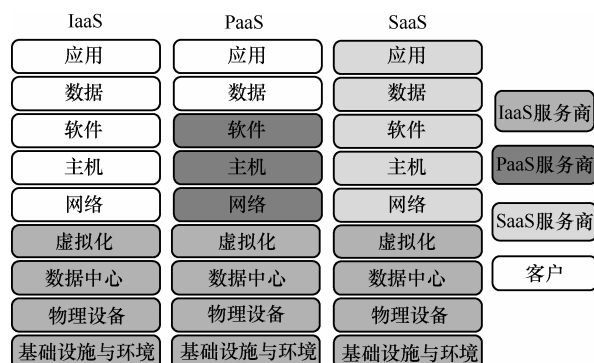


图5 持续监管角色安全责任模型

CMO 应与 CSP 或客户关于每一项指标的合理性以及实现技术或手段进行讨论，最后与 CSP 或客户对合理且可实现的指标达成一致意见，并制定成评估指标体系。指标体系应以 CMO 与 CSP 或客户协商的频率，定期更新。表1列举了《要求》中对 CSP 的安全能力的所有类别，鉴于当前指标制定工作还在进行中，当前列出来的一些指标只是初步设想，具体的指标内容还有待讨论与更进一步的研究，因此表2仅列举了针对《要求》中的“系统与通信保护”项制定的指标，其他项的具体指标还在研究中。

表1 安全能力类别

类别	安全要求项数
系统开发与供应链安全	17
系统与通信保护	15
访问控制	26
配置管理	7
维护	9
应急响应与灾备	13
审计	11
风险评估与持续监控	6
安全组织与人员	12
物理与环境保护	15

表 2

系统与通信保护指标

安全能力	类型	监管指标类型
策略与规程	文档类 接口类	系统与通信保护策略：包含但不限于以下子项内容 包含但不限于以下子项接口
边界保护	文档类	1) 客户业务系统隔离策略 2) 边界通信监控机制 3) 内外部网络安全隔离机制 4) 外部电信服务的安全管理措施 5) 外部通信接口授权策略 6) 远程维护管理策略 7) 边界保护策略失效响应机制
	接口类	1) 边界保护设备的配置信息 2) 外部电信服务接口传输的信息流采样
传输保密性和完整性	文档类	1) 通信加密和签名验签算法及设施策略 2) 通信加密和签名验签设施的证书、测评报告
	接口类	无
网络中断	文档类	不活动时间定义及应对措施
	接口类	无
可信路径	文档类	平台用户与系统安全功能之间建立可信通信路径的相关措施
	接口类	无
密码使用和管理	文档类	1) 密钥的生成、使用和管理策略及记录 2) 密码设施的管理和使用记录
	接口类	无
协同计算设备	文档类	协同计算设备禁用策略
	接口类	无
移动代码	文档类	移动代码使用及限制策略
	接口类	无
会话认证	文档类	会话认证策略
	接口类	无
移动设备的物理连接	文档类	移动设备的管理和使用策略
	接口类	无
恶意代码防护	文档类	1) 恶意代码防护设备及防护机制 2) 恶意代码防护设备的维护更新记录 3) 恶意代码的检测和处理机制 4) 恶意代码误报率的分析机制和误报分析影响记录
	接口类	1) 恶意代码防护设备的配置信息 2) 恶意代码的实时告警 3) 恶意代码防护设备的特征库及策略库版本信息
内存防护	文档类	内存申请、使用、释放等防护机制
	接口类	内存信息
系统虚拟化安全性	文档类	1) 虚拟机实时监控机制 2) 虚拟机镜像安全机制 3) 虚拟机安全隔离机制 4) 虚拟化平台资源隔离机制
	接口类	1) 资源隔离失败告警 2) 虚拟镜像模板的配置信息
网络虚拟化安全性	文档类	1) 虚拟网络逻辑隔离策略 2) 虚拟网络访问控制机制
	接口类	虚拟网络资源配置信息
存储虚拟化安全性	文档类	1) 存储数据的安全控制机制 2) 物理存储实体访问机制 3) 虚拟存储资源之间逻辑隔离机制 4) 用户的存储数据清除机制 5) 虚拟存储数据访问控制策略 6) 虚拟存储数据的审计机制 7) 虚拟存储冗余备份支持机制 8) 第三方加密及密钥管理策略
	接口类	1) 用户数据清除记录信息 2) 虚拟存储备份信息 3) 数据加密方案信息

6 云计算服务持续监管 API 规范

监管 API 是 CMO 实现监管 CSP 的重要手段。CMO 应遵循通用、简单、易于实现、可交互等特点制定接口规范。CSP 应根据 CMO 制定的接口规范提供相应功能的接口。接口规范的制定可以参考 RESTful (representational state transfer) 协议, CMO 可以通过典型的“查询—响应”的方式向 CSP 查询云服务当前相关的安全属性。例如当前服务的脆弱性等级或最新的脆弱性评估信息等。CMO 也可以使用标准的基于 XMPP^[1] (extensible messaging and presence protocol) 的通知机制定义“触发器”, 在满足特定条件时接收告警事件。

需要重点强调的是, CMO 应采用统一标准来制定接口规范。监管 API 不能替代用于收集、存储及分析事件的监控设备和相关技术。

通过几个简单的例子来说明持续监管 API 的作用。如图 6 所示, CMO 使用某个查询接口向 CSP 查询其承诺的服务可用性等级指标, 此指标通常会被写入到 SLA 中。查询结果以 CMO 规定的形式返回给 CMO。

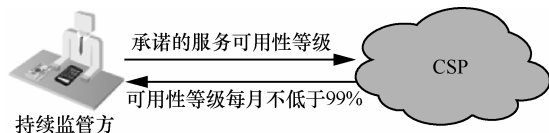


图 6 查询 CSP 承诺的服务可用性等级

如图 7 所示, CMO 向 CSP 查询上个月实际达到的服务可用性等级。查询结果被称作“测量结果”, 因为它表示的是服务等级测量的结果, 此结果是由 CSP 上报的。

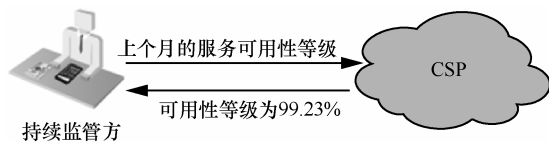


图 7 查询上个月的服务可用性等级

如图 8 所示, CMO 要求 CSP 在某个特定情况被证实时发送告警, 这被称为“触发器”。此外, CSP 也会在本地图录此次告警的细节, 以便客户或 CMO 后期咨询。

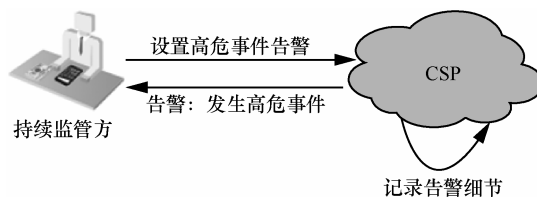


图 8 高危事件上报并记录

可以根据接口的功能或类型将其划分为不同集合, 并将集合作为功能组件来使用。例如, 将接口按功能分为以下几类, 如图 9 所示。

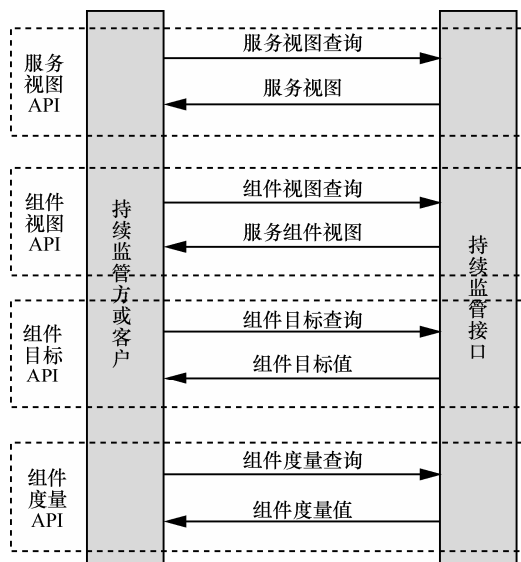


图 9 监管 API 接口分类

1) 服务视图 API: 获得特定云计算服务的服务视图, 如服务的名称、服务 ID 等相关信息。

2) 组件视图 API: 通过服务 ID 获得该服务的相关组件信息。

3) 组件目标 API: 获得组件的预期目标, 如可用性。

4) 组件度量 API: 获得组件的度量值, 可以是定性或定量值。通过与组件目标值比较可以确定组件性能或安全是否满足要求。

7 结束语

本文所描述的云计算服务持续监管内容是在研究国际、国内云计算服务持续监管相关标准、技术和管理成果之上, 结合我国政府部门、重点行业使用云计算服务的安全要求, 提出云计算服务中持续监管的角色和安全责任边界, 形成云计算服务持续监管框架, 并研究、初步提出了云计

算服务的评估指标体系与接口规范。

云计算服务持续监管框架及技术规范标准, 是对我国云计算服务安全标准体系的完善, 能有效支撑云计算服务安全审查的工作, 保障涉及党政、重点行业的云计算服务快速、稳健、持续地发展。

随着云计算服务在党政机关、企事业单位以及国家重点行业中的应用不断发展, 云计算服务持续监管技术将成为今后云计算领域中的研究热点, 如何实时监管云计算服务平台将会成为今后的重点研究课题。

参考文献:

- [1] 中国国家标准化管理委员会. 信息安全技术 云计算服务安全指南: GB/T 31161-2014[S]. 北京: 中国标准出版社, 2014.
Standardization Administration of China. Information security technology of cloud computing services security guidelines: GB/T 31161-2014[S]. Beijing: China Standards Press, 2014.
- [2] 中国国家标准化管理委员会. 信息安全技术 云计算服务安全能力要求: GB/T 31168-2014[S]. 北京: 中国标准出版社, 2014.
Standardization Administration of China. Cloud computing service security capacity requirements of information security technology: GB/T 31168-2014[S]. Beijing: China Standards Press, 2014.
- [3] FedRAMP Office. Continuous monitoring strategy & guide. Version 2.0[S]. 2014.
- [4] NIST Special Publication 800-137. Information security continuous monitoring (ISCM) for federal information systems and

organizations[S]. 2011.

- [5] NIST Special Publication 800-37. Guide for applying the risk management framework to federal information systems[S]. 2010.
- [6] CSA(Cloud Security Alliance). Auditing the cloud controls matrix[S]. 2014.
- [7] CSA. Defined categories of security as a service[S]. 2016.
- [8] NIST Special Publication 800-145. The NIST definition of cloud computing[S]. 2011.
- [9] CSA. CTP data model and API[S]. 2015.

作者简介:



陈兴蜀(1968-), 女, 四川自贡人, 博士, 四川大学教授, 主要研究方向为网络空间安全。

葛龙(1976-), 男, 江苏丹阳人, 博士, 四川大学讲师, 主要研究方向为云计算安全。

罗永刚(1980-), 男, 贵州瓮安人, 博士, 四川大学讲师, 主要研究方向为云计算、大数据安全。

李想(1987-), 男, 河南郑州人, 四川大学博士生, 主要研究方向为云计算安全。