云计算安全审计技术研究综述

王文娟 杜学绘 王 娜 单棣斌
(解放军信息工程大学网络空间安全学院 郑州 450001)
(数字工程与先进计算国家重点实验室 郑州 450001)

摘 要 目前安全问题已经成为阻碍云计算推广和发展的巨大障碍,云计算环境特有的数据和服务外包、虚拟化、多租户和跨域共享等特点使得其面临的安全威胁相比传统IT环境更复杂多样,对安全审计技术也提出了更高的要求。首先分析了云计算环境下安全审计面临的主要挑战,提出云环境下的安全审计参考框架,从用户维、业务维、数据维、设施维等4个维度上对云环境进行全方位的"体检"。然后针对不同维度,围绕日志审计、存储审计、配置审计3个方面的研究进行了评述,以期为我国未来云计算安全审计的发展研究提供有益的参考。

关键词 云计算,安全审计,日志审计,存储审计,配置审计
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.003

Review on Security Audit Technology for Cloud Computing

WANG Wen-juan DU Xue-hui WANG Na SHAN Di-bin
(College of Cyberspace Security, PLA Information Engineering University, Zhengzhou 450001, China)
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract Now the security concern has become a huge impediment to the development of cloud computing. Due to the specific characteristics such as data and service outsourcing, virtualization, multi-tenant and cross domain sharing, the cloud computing environment faces more complicated threats compared with traditional IT environment, and the security audit technology also needs higher demands. Firstly, this paper analyzed the main challenges that cloud security audit confronts with, proposed a security audit technology framework in cloud environment which provides all-around examination from four dimensions such as user dimension, business dimension, data dimension, infrastructure dimension. Then according to different dimensions, the studies were reviewed from three aspects including log audit, storage audit and configuration audit, in order to provide useful reference to the development research of security audit for cloud computing in our country.

Keywords Cloud computing, Security audit, Log audit, Storage audit, Configuration audit

1 引言

云计算[1]是一种基于互联网的新兴计算模式,通过将各种互联的计算资源进行有效整合并实现多层次的虚拟化与抽象,以可靠服务的形式提供给用户,从而将用户从复杂的底层硬件、软件和协议栈中解放出来。云计算的出现改变了用户的使用习惯、企业的销售方式、开发者的开发模式,从而改变了整个IT产业的游戏规则。虽然云计算已成为不可逆转的服务趋势,但也遇到很多问题亟待解决,其中,安全问题首当其冲。近年来,亚马逊、谷歌、微软等大型云服务提供商不断爆出各种安全事故,引起了业界的广泛关注,引发了人们对云计算的担心与质疑,安全问题已经成为阻碍云计算推广和发展的巨大障碍。云计算环境的开放性和商业性使得其面临的安全威胁相比传统IT环境更复杂多样,这也给云环境的安全保障提出了更为严峻的考验。

云计算环境中包含两类主体和两类客体,分别是云服务提供商、云租户、云端数据、云基础设施,它们之间不仅存在着服务与被服务关系、支撑与被支撑关系,还存在着复杂的攻击与被攻击关系。从CSA发布的《云计算面临的主要威胁》[2]报告以及引发的大量安全事件来看,云环境面临的安全威胁主要有两个方面(见表1):1)来自于云服务提供商的内部威胁。恶意云管理员可能侵入租户账户造成数据或隐私泄露;云管理员滥用虚拟机管理器(Virtual Machine Monitor, VMM)的Root权限安装和运行类似LibVMI[3]暴力软件进

到稿日期:2016-05-26 返修日期:2016-09-06 本文受国家863高技术研究发展计划基金项目:基于多维控制的云计算信息流追责、管控技术研究(2015AA011705)资助。

王文娟(1981-),女,博士生,副教授,主要研究方向为网络与信息安全、数据挖掘,E-mail:13526685747@139.com;杜学绘(1968-),女,博士,教授,主要研究方向为网络与信息安全;王 娜(1980-),女,博士,副教授,主要研究方向为网络与信息安全;单棣斌(1983-),男,硕士,讲师,主要研究方向为网络与信息安全。

入云基础设施内部观察正在运行的 VMs 的内存、CPU、磁盘或网络等。2)来自于云租户的外部威胁。非法租户访问盗取云计算资源，或者滥用云计算资源发动拒绝服务攻击使得云环境瘫痪。另外，VMM 存在的技术漏洞及错误配置使得租户操作系统有可能会控制或影响底层平台。可见，云租户对于云端数据及云基础设施产生着威胁，云服务提供商对于云端数据及租户 VM 同样构成了威胁，云基础设施自身存在的技术漏洞与未知风险也存在着安全隐患。

表 1　云计算面临的主要安全威胁

主体		威胁	客体
云服务提供商	内部威胁	恶意员工	云端数据、VMs
		数据丢失/数据泄露	
云租户	外部威胁	数据泄露	云端数据
		流量截获/账户劫持	云基础设施
		非法滥用云服务	
		不安全的 APIs	
		共享技术漏洞	
		未知风险	

因此，为了处理这些威胁，保障云计算环境安全可靠地运行，保证云计算服务被安全地访问和使用，引入传统 IT 安全审计的理念，借助安全审计技术对云计算环境的运行状态、服务访问、管理配置等进行详尽的记录和监管，从而防止有意或无意的操作错误，发现和响应发生在云计算环境中的安全事件，倒查和追溯安全问题根源或攻击者的行为轨迹。本文讨论的审计技术主要关注的是公有云，基础设施和平台软件由云服务提供商管理，而私有云由客户完全控制，可以采用传统的“无云的”审计解决方案。

2　云计算安全审计面临的挑战

传统的 IT 安全审计技术已经非常成熟，安全审计是对计算机系统和计算机网络中的各种信息进行实时采集、分析，以查证是否发生安全事件的一种安全技术。尽管传统 IT 安全审计和云计算安全审计在定义和安全观念上存在相同的观点，但是它并不能直接迁移至云计算环境。云计算环境特有的数据和服务外包、虚拟化、多租户和跨域共享等特征都给安全审计带来了一些非常具有挑战性的难题。这些难点和挑战主要表现在以下几个方面。

(1)多层服务模式带来的挑战。云计算主要提供 3 种服务模式：基础设施即服务(Infrastructure as a Service，IaaS)、平台即服务(Platform as a Service、PaaS)、软件即服务(Soft as a Service，SaaS)。其中，IaaS 是所有云服务的基础，提供硬件基础设施部署服务，为用户提供实体或虚拟的计算、存储和网络等资源；PaaS 建立在 IaaS 之上，是云计算应用程序的运行环境，提供应用程序部署与管理服务；SaaS 则建立在 PaaS 之上，提供基于互联网的应用程序服务。各个层次之间彼此独立又相互依存，构成一个动态、稳定的整体[4]。但是由于 IaaS，PaaS 和 SaaS 各层所提供的服务内容不同，用户的使用方式、行为轮廓也存在差异性。例如，使用 IaaS 服务的用户可能会租用一些硬件资源来配置环境，运行安装一些应用或上传数据进行存储；PaaS 面向的是开发人员，主要是利用数据处理平台计算处理用户数据或利用编程平台进行程序代码的开发测试；而 SaaS 面向的是普通用户，通过浏览器就可以使用某些应用而不需要进行安装等活动。因此，云计算安全审计需要根据各层不同的活动提取用户行为特征，建立行为轮廓库，然而云计算环境下用户数量巨大、服务需求各异、访问方式多样，这给正常行为特征的提取带来了前所未有的困难。

(2)数据外包存储带来了新的审计研究问题。云租户将自己的应用和数据迁移到云端，通过外包模式将用户从繁重的维护和管理任务中解放出来，使其不再受限于有限的本地设备资源，可以在任意时间、任意地点进行数据访问，数据外包存储已经成为了一种必然的趋势和潮流[5]。然而，外包即意味着用户数据控制权由用户自身向云服务提供商转移，数据的管理和维护完全由云服务提供商单方面来保证。事实上，云服务提供商是不能完全信任的，用户无法得知外包存储的数据是否确实已存储到云端并归数据所有者所有，除所有者和授权用户外是否有人更新数据，云服务提供商是否对数据所有者隐瞒数据丢失事故，例如由于云环境被恶意攻击或一些不可抗拒的客观原因而造成数据丢失，或者提供商丢弃了长时间内未被访问过或很少被访问的数据以达到节省存储空间的目的。因此，为了随时知晓数据是否被破坏或被丢失，数据所有者亟需一种安全可信的审计机制来确保数据被真实、完整地存储在云服务器中。在数据存放到本地或可信域中时安全审计较易实现，而一旦将数据外包存储到云中，安全审计就变成了难题。另外，在云计算环境下，用户对数据存储的实际物理地址知之甚少，因为云服务提供商需要隐藏数据的实际位置以方便其进行数据的转移和复制。因此，数据所有者需要一种能够有效定位其云端数据的技术，保证所有的数据包括其副本和备份存储在合同、法规允许的真实的物理存放位置。

(3)虚拟化、多租户特性带来的挑战。虚拟化是云计算的重要支撑技术之一，可以说是虚拟化为我们带来了“云”，通过虚拟化技术可将物理服务器分割成若干虚拟机并同时为多个用户服务，大大提高了服务器的资源利用率，实现了服务成本下降和可扩展性提高。但是，虚拟化在增加规模性的同时也戏剧性地增加了审计对象的数量。而且虚拟机的动态迁移将立即改变审计的网络结构拓扑，攻击者也很容易以打游击或控制“傀儡机”的模式在网络上迁移，使得追踪其行为轨迹、取证调查难度加大。另外，多租户共享资源也给恶意租户攻击其他租户、占用其他租户资源或利用其他租户实施攻击提供了便利。尽管从理论上来说，这些虚拟机之间是完全隔离并独立的，但由于共用相同的物理设备以及虚拟化技术、隔离技术等存在的漏洞都将导致这些虚拟机不能达到完全独立，因此需要对环境配置进行审计以发现安全隐患。

(4)云计算商业运营模式不成熟给责任认定带来了难度。事实上，当前租户与云服务提供商之间的责任与管理范围界定得并不清晰，在使用权限上可能存在冲突，当出现安全事故时就面临着责任认定和行为问责问题。服务提供商和用户根据所处云模型的层次不同，承担的责任有所不同[6]。首先，在 SaaS 层，服务提供商提供的应用服务最具集成化的功能和特性，用户对底层平台的可操作性最小，服务提供商承担主要的

安全职责；在 IaaS 层，底层基础设施和抽象层的安全保护属于服务提供商职责，而其他职责，如操作系统、应用和内容的管理和保护则属于用户；PaaS 则居于两者之间，用户在云平台上开发自己的应用，服务提供商要为平台自身提供安全保护，而平台上应用的安全性及如何安全地开发这些应用则由用户负责。因此，需要制定服务提供商和租户的行为规范，将资源的所有权、管理权及使用权明确下来，解决责任共担带来的职责不明确、行为问责难等问题。其次，云计算发展的趋势之一是 IT 服务专业化、产业化[7]，即云服务提供商通过购买服务的方式减少对非核心业务的投入，从而强化自身核心领域的竞争优势。服务提供商在对外提供服务的同时，自身也需要购买其他服务商所提供的服务。因此，租户所享用的云服务有可能间接涉及到多个服务提供商，这种多层转包无疑极大地增大了问题的复杂性，进一步增加了安全审计的难度。

综上所述，云计算安全审计是信息安全领域正在发生的重大变革。云计算安全审计不仅要保证云端数据的安全性，还要保障云计算支撑环境安全可靠地运行；既要检查云服务提供商的内部行为和内部过程，还要防止租户的恶意破坏等。因此，不存在“一体适用”的审计模型及机制，需要针对云计算开创新思维，从多个视角、多个维度建立云计算安全审计框架。

3 云计算安全审计框架建议

正如上文所述，云计算环境中包含云服务提供商、云租户两类主体和云端数据、基础设施两类客体，云环境面临的安全威胁是复杂多样的，为尽可能全面地审计云计算环境，应建立综合性的云计算安全审计框架，并积极开展其中各个安全审计的关键技术研究。本节提出了一个参考性的安全审计技术框架建议，如图 1 所示。该框架以服务提供商、云租户、云端数据、基础设施 4 个方面为出发点，在用户维、业务维、数据维、设施维 4 个维度上对云计算环境进行了全方位的“体检”。由于各个维度的审计数据来源和类型不同，不存在“一体适用”的审计机制。因此，针对不同维度有的放矢，采取有效适宜的审计机制。

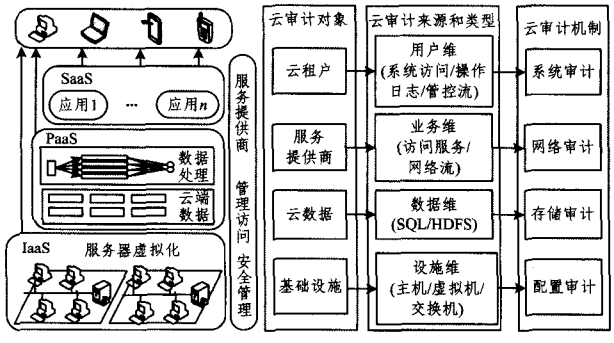

图 1 云计算安全审计框架

用户维侧重于租户和云管理员的操作行为。其审计数据来源于系统访问、文件操作、进程调用、控制流日志等，如图 2 所示。控制流日志是指云管理员操作虚拟机产生的管控日志，如打开、关闭 VM、在 VM 中安装软件等。租户对云环境资源的非法访问、恶意云管理员的特权滥用等都会产生日志记录，通过系统审计可以发现越权、操作失误等异常行为，或者寻找追踪攻击者留下的痕迹。

业务维侧重于租户的应用访问日志、物理网络信息流和 VM 间的网络信息流，如图 2 所示。通过网络审计可以发现流量截获/劫持、拒绝服务攻击等安全事件。但由于云计算底层架构通过虚拟化技术实现，虚拟机间的通信过程在物理机的共享内存中完成，流量并不经过传统的网络安全组件。因此，传统的网络数据获取手段不能完美地运用在云环境中，需要提出适应于虚拟化环境的网络审计解决方案。

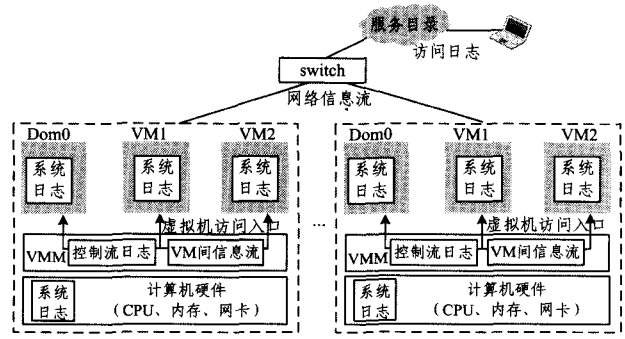

图 2 用户维和业务维审计数据来源

数据维侧重于租户的云端存储数据，如上传至云数据库、分布式文件系统中的数据。通过云存储审计使得租户对其数据的完整性进行验证，检查数据是否被破坏或丢失，保证云端数据的存储安全。

设施维侧重于云基础设施，包括服务器、交换机、防火墙等物理设备以及 VMs，vSwitch 等虚拟设备。云环境中网络结构配置错误、防火墙策略配置不当都会带来安全风险，虚拟化技术存在的技术漏洞也有可能被攻击者所利用造成安全隐患。因此，通过配置审计来发现网络结构、安全机制等配置问题。

该参考框架实现了多维度多元化的安全审计。系统审计属于一种消极审计，但具备对违规事件的“事后审查和取证”能力；网络审计能够近实时地发现网络攻击行为，属于“事中防护”。系统审计和网络审计统称为日志审计。云存储审计对租户的数据提供完整性保证，提高云服务提供商的信任性；配置审计通过对云环境的网络结构和安全策略进行配置核查，检验云环境的隔离性和合规性[8]。下面围绕日志审计、云存储审计、配置审计 3 个方面的研究进展分别进行评述。

4 云计算安全审计机制

4.1 日志审计

日志在信息系统运行管理中发挥着重要的作用，尤其在安全领域，日志记录了用户涉及安全操作的所有活动的过程，以备有违反安全规则的事件发生后能够有效地追查事件发生的时间、地点及过程，是安全事件追溯、取证分析的重要依据。但是当前关于云计算日志审计的研究成果比较少，因为云服务提供商的内部操作细节并不为用户所知，并且其限制提供日志记录和实施监控数据，审计日志所能获得的部分审计日志不足以对云计算安全审计进行全面的研究。

Shetty 等人[9]提出了一种审计恶意云租户的技术，通过

IP 定位和路由器 IP 分析技术，结合网络度量（平均时延、标准方差时延、跳数）和社会特征（城市人口密度）等因素能够确定云租户的真实地理位置。Shetty 等人开发了基于机器学习和控制理论模型的数据挖掘技术，能够自适应地调整检测阈值，实时分析云日志以发现云环境的异常事件。Birnbaum 等人[10]提出了一个基于行为建模的云计算安全审计框架，代替传统的基于特征的入侵检测技术或系统调用异常分析，主要用来分析云租户的审计数据。Birnbaum 等人提出的分析算法尤其在攻击同一物理机器上的客户 VMs 场景下验证了它的价值。Ganjali 等人[11]提出一种 H-one 审计机制来审计恶意云管理员，该机制给来源于 VMs 或管理员的所有信息流打上污点标签，利用污点跟踪技术跟踪信息流的传播过程。由于管理员的恶意行为有非法获取信息或篡改信息这一明显特征，因此，其能够识别管理员窃取用户隐私类等恶意行为，从而实现对云管理员的安全审计。另外由于大部分日志是经常出现且无害的，对大量日志进行跟踪、存储会浪费系统资源，针对这个问题设计了实时过滤守护进程，有效减少了对不必要日志的跟踪和存储开销。Wang 等人[12]设计并实现了一个云数据中心审计系统 CDCAS（Cloud Data Center Auditing System），能够满足云数据中心可扩展性和有效性的需求。这个系统中设计了一个分布式自治代理模型来收集各种多源异构日志，利用基于特征的方法和相关性分析算法比较审计日志和预配置或预定义的事件模式，从而发现非法行为，提取攻击、误用和错误事件。最后在真实的和仿真环境中评估、证实了该系统的有效性。

上述审计方法针对的审计对象或审计日志源都比较片面，大部分是单源单向审计，且未能全面地涉及云计算的多个主体及多源异构日志。如表 2 所列，Shetty 等人通过审计网络数据流来发现恶意租户的攻击，但难以发现恶意云管理员的行为，检测阈值难以确定；Birnbaum 等人的方案对租户正常行为建模比较困难；Ganjali 等人提出的 H-one 审计机制主要通过追踪管控信息流来审计恶意云管理员是否滥用管理员权限，但未讨论信息流分析方法及污点标签的管理技术；Wang 等人的方案能够实现多源双向审计，但网络审计集中在流量统计，未涉及网络行为审计和预定义规则库的设计。

表 2　日志审计中各方案对比分析

方案	关键技术	审计对象	数据源	存在不足
Shetty	IP 定位	云管理员	网络数据流	检测阈值难以确定
Birnbaum	污点跟踪	租户	系统日志	租户正常行为建模比较困难
Ganjali	行为建模	云管理员	管控信息流	未涉及信息流分析及污点标签管理
Wang	特征分析	双向	多源日志	未讨论网络行为审计和规则库设计

4.2　云存储审计

云存储审计[13]是指数据拥有者验证存储在云中数据的完整性和可用性的过程。为了提供可信、公平的审计结果，使数据所有者和云服务提供商都信服，第三方审计是比较合适的选择。第三方审计方案的设计面临诸多挑战：1）支持动态审计，即审计方案支持数据动态更新操作；2）支持批量审计，即审计方案支持多个审计任务进行合并处理，以提高审计效率；3）支持盲审计，即数据需要对第三方审计保密。

Ateniese 等人[14]首次提出了“可证明数据持有”PDP 方案，该方案只支持静态审计，将 RSA 密码与同态可验证标签结合起来。所有者先将数据分成块并加密，然后为每个数据块计算标签，并与加密后的数据一起保存在服务器上。审计者向服务器发出对数据块子集的质询而不需要检索整个文件。在后续的工作中，Ateniese[15]又设计了一种部分动态可证明（DPDP）的数据持有协议，在开始阶段预先计算一些元数据，其中每个元数据对应一个更新，其缺点是更新和验证次数有限且是预先固定的，不支持数据插入操作。由于采用耗时的 RSA 算法，PDP 方案中数据完整性证据的生成和验证效率很低。同年，Juels 等人[16]提出了“可检索的证明”POR 方案，在云存储服务器中利用抽样和纠错码来确保数据文件的持有性和可检索性，该方案只支持有限次的验证。这两种方案中验证数据完整性的算法基本相同，主要区别是 POR 方案在验证数据完整性的基础上加入了纠错码技术，以便恢复原始数据。Wang 等人[17]采用双线性配对技术基于离散对数问题提出了一种支持第三方验证的 PDP 协议，该协议利用随机屏蔽方法实现了盲审计，并利用同态标签的思想将数据标签聚合实现了批量审计。Wang 在另一个研究中[18]基于默克尔哈希树构造了一个允许数据动态变化的第三方审计 POR 协议，同时基于纠错码支持数据动态更新。Zhu 等人[19]基于双线性配对技术和索引表设计了一种支持数据动态变化的第三方审计 PDP 协议，该协议允许无限次验证并支持盲审计。He[20]和 Yang[21]等分别提出了支持多所有者多云服务器的批量审计方法，这些批量审计方法都是假设数据所有者只有一份文件。之后，He 等人[22]又提出了一种聚合盲审计方法，利用双线性对映射的性质在云端服务器将数据证据和标签证据加密后再合并，实现审计者在不知数据内容的情况下进行盲审计。在此基础上设计高效的索引机制来支持数据更新，同时实现了动态审计。针对多个审计请求，设计将不同的证据聚合的方法，以支持对多所有者多云服务器多文件的批量审计。

表 3 从动态审计、批量审计、盲审计等方面对上述方案进行了对比分析。可以看出，现有方案或多或少存在一些问题：有些方案不支持盲审计，有些方案不支持动态审计，而有些方案不支持多文件批量审计；计算开销和通信开销过高。但鉴于 POR 方案具有数据恢复功能，比 PDP 方案具有更高的实用价值，因此设计支持盲审计、动态审计和批量审计的 POR 协议是云存储审计研究的一个重要方向。

表 3　存储审计中各方案对比分析

方案	动态审计	批量审计			盲审计
		多所有者	多服务器	多文件	
PDP	—	—	—	—	—
POR	—	—	—	—	—
Wang	√	√	—	—	√
Zhu	√	—	√	—	√
Yang	√	√	√	—	√
He	√	√	√	√	√

4.3　配置审计

配置审计主要用来验证云基础设施的安全机制和静态结

构配置是否与标准、用户期望或安全策略一致。比如，在多租户共享资源的云基础设施中，防火墙配置的正确性非常重要，一旦防火墙配置出现问题，很可能导致数据的泄露或服务的非法使用。同样，在多租户环境下网络结构要素没有进行有效隔离也将导致数据被窃取。

Bleikertz 等人[23]提出了一种利用可达性图对虚拟机防火墙配置进行审计的方案。该方案根据多个虚拟机之间以及虚拟机与外界之间的可达性构建出整体的可达性图，Bleikertz 等人设计了两个算法，分别能够对任意的访问模式进行审计和验证可达性图是否包含某个可达性策略。对于给定的可达性策略集合，通过周期性地调用验证算法进行审计，能够保证所有的可达性策略都被满足。Bleikertz 在文献[24]中又延伸了先前的工作，提出了基于增量图的计算方法(如增加/删除结点和边)，能够近实时地检测影响安全的配置变化，通过在云基础设施中部署探测器来保持图模型的变化和实际的配置变化同步。Doelitzscher 等人[25-26]提出了一个基于自治代理的云计算安全审计系统，通过利用自治代理能够自动检测虚拟基础设施、VMs 的变化(例如新的 VMs 的打开/关闭和虚拟机迁移)和评估云环境的安全状态。该系统基于底层的业务流程模型还能够检测滥用云计算资源和租户账户、分布式拒绝服务攻击以及 VM 突破等攻击行为，克服了传统审计、入侵检测系统 IDS 和入侵防御系统 IPS 在频繁变化的云环境下的不足。Madi 等人[27]主要介绍了两类隔离配置机制：1)多租户无共同属主，如图 3 所示，Port_84 既属于租户 Beta 又属于租户 Alpha，该端口成为两个租户的共同资源；2)租户无共同驻留主机，如图 4 所示，虚拟机 VM_01 和 VM_02属于租户 Alpha，运行于物理主机 Compute Node_85 上，VM_03 属于租户 Beta，运行在物理主机 Compute Node_96 上。假定租户 Alpha 不信任租户 Beta，但是出于负载平衡原因，VM_02从 Compute Node_85 迁移到 Compute Node_96 上，与租户 Beta 共享同一物理主机，从而与租户 Alpha 的要求不符。这两种情况都将导致一个租户访问另一个租户的数据或资源从而造成隐私泄露，应该被及时审计并修改配置。

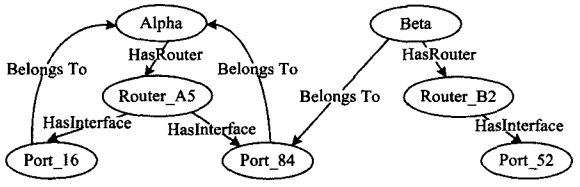

图 3 无共同属主

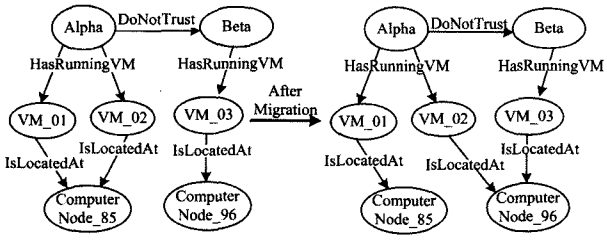

图 4 无共同驻留主机

结束语 如何保障云计算环境安全可靠地运行，确保云计算服务被安全地访问和使用是云计算面临的难题，它已严重阻碍了云计算的推广和发展。本文首先列举了云计算环境面临的主要威胁，深入分析了云计算安全审计面临的主要挑战。针对云计算威胁，以云服务提供商、云租户、云端数据、支撑环境 4 个方面为出发点，提出一个参考性的云计算安全审计框架建议，从用户维、业务维、数据维、设施维 4 个维度对云计算环境进行全方位的“体检”。并针对不同维度有的放矢，采取有效适宜的审计机制，围绕日志审计、云存储审计、配置审计 3 个方面的最新研究进展分别进行了评述，以期为我国未来云计算安全审计的发展研究提供有益的参考。

但是上述研究还存在若干问题需要进一步研究解决：

(1)云计算安全审计框架适用性问题。文中的审计框架提出了 3 种审计机制对应于不同的审计对象维度，但在实际环境中各审计机制如何设计、如何协同、是否存在跨多个维度的审计技术或系统还需进一步讨论和分析。

(2)云计算安全审计机制的灵活性问题。云计算面临的任务以及环境是不断变化的，这就需要安全审计机制有着更加灵活的解决方案，适应频繁变化的云环境，覆盖同一安全问题尽量多的意外状况。

(3)云计算安全审计的可信性问题。云计算存在双向审计问题，但是云服务提供商的内部操作细节并不为用户所知并且限制提供审计日志，因此，针对云管理员的审计准确性有待商榷，审计日志的隐私保护还需要进一步研究。

(4)云计算安全审计的大数据问题。云端存储的用户数据以及云计算环境中的审计日志数量巨大，日志的元结构和多维特性突出，而且更新动态性、处理实时性要求十分强烈，已经具备了大数据典型的“4V”特征。因此，将大数据技术应用到审计方法中，解决云计算安全审计可能面临的诸多问题是值得深入研究的课题。

(5)混合云的安全审计问题。混合云存在大量的云间服务协同和组合需求，因此引入了特定的安全审计问题。资源归属、管理责任认定、跨云基础架构监控、边界安全策略制定等是混合云安全审计问题的关键特征。

参 考 文 献

[1] MELL P, GRANCE T. NIST Definition of Cloud Computing, Sp [OL]. Publication 800-145. 2011. http://csrc. nist. gov/publications/nistpubs/800-145/SP800-145. pdf.

[2] The Notorious Nine: Cloud Computing Top Threats in 2013[EB/OL]. http://www.cloudsecurityalliance.org/group/top-threats.

[3] LibVMI[OL]. http://github. com/libvmi/ libvmi.

[4] LUO J Z, JIN J H, SONG A B, et al. Cloud computing: architecture and key technologies [J]. Journal on Communications, 2011, 32(7): 3-21. (in Chinese)
罗军舟，金嘉晖，宋爱波，等. 云计算：体系架构与关键技术[J]. 通信学报，2011，32(7)：3-21.

[5] FENG C S, QIN Z G, YUAN D. Techniques of Secure Storage for Cloud Data[J]. Chinese Juounal of Computer, 2015, 38(1): 150-163. (in Chinese)
冯朝胜，秦志光，袁丁. 云数据安全存储技术[J]. 计算机学报，2015，38(1)：150-163.

(下转第 30 页)

[9] Floodlight Controller[OL].https://floodlight.atlassian.net/wiki.

[10] BOTTA A,DAINOTTI A,PESCAPÉ A. A tool for the generation of realistic network workload for emerging networking scenarios[J]. Computer Networks (Elsevier), 2012, 56(15): 3531-3547.

[11] CAI Z P. Study on network measurement technology, model and algorithm based on active and passive measurement [D]. Changsha: National University of Defense Technology, 2005. (in Chinese)
蔡志平. 基于主动和被动测量的网络测量技术、模型和算法研究[D]. 长沙:国防科学技术大学,2005.

[12] CHENG G, WANG Y X, HU Y F, et al. Network Link Fault Diagnosis Based on OpenFlow[J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(5): 42-46. (in Chinese)
程光,王玉祥,胡一非,等. 基于 OpenFlow 的链路故障诊断方法[J]. 北京邮电大学学报,2015,38(5):42-46.

[13] CAI Z P, LIU F, ZHAO W T, et al. Network measurement deployment model and its optimization algorithm[J]. Journal of Software, 2008, 19(2): 419-431. (in Chinese)
蔡志平,刘芳,赵文涛,等. 网络测量部署模型及其优化算法[J]. 软件学报,2008,19(2):419-431.

(上接第 20 页)

[6] CHEN Y R. Research on User Behavior Authentication and Security Control in Cloud Computing[D]. Beijing: University of Science and Technology Beijing, 2012. (in Chinese)
陈亚睿. 云计算环境下用户行为认证与安全控制研究[D]. 北京:北京科技大学,2012.

[7] FENG D G, ZHANG M, ZHANG Y, et al. Study on Cloud Computing Security[J]. Journal of Software, 2011, 22(1): 71-83. (in Chinese)
冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71-83.

[8] LUNA G J, LANGENBERG R, SURI N. Benchmarking cloud security level agreements using quantitative policy trees[C]// ACM Workshop on Cloud Computing Security Workshop. 2012: 103-112.

[9] SHETTY S. Auditing and Analysis of Network Traffic in Cloud Environment[C]// IEEE Ninth World Congress on Services. 2013: 235-258.

[10] BIRNBAUM Z, LIU B, DOLGIKH A, et al. Cloud Security Auditing Based on Behavioral Modeling[J]. International Journal of Business Process Integration & Management, 2013, 7(2): 268-273.

[11] GANJALI A, LIE D. Auditing Cloud Administrators Using Information Flow Tracking[C]// Proceedings of the 7th ACM Workshop on Scalable Trusted Computing. 2012: 79-84.

[12] WANG X, ZHANG J, WANG M, et al. CDCAS: A Novel Cloud Data Center Security Auditing System[C]// IEEE International Conference on Services Computing. IEEE, 2014: 605-612.

[13] BIRK D, WEGENER C. Technical Issues of Forensic Investigations in Cloud Computing Environments[C]// IEEE Sixth International Workshop on Systematic Approaches To Digital Forensic Engineering. IEEE, 2011: 1-10.

[14] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores[C]// ACM Conference on Computer and Communications Security. ACM, 2007: 598-609.

[15] ATENIESE G, PIETRO R D, MANCINI L V, et al. Scalable and Efficient Provable Data Possession[C]// Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. ACM, 2008: 1-10.

[16] JUELS A, KALISKI B S. Pors: proofs of retrievability for large files[C]// ACM Conference on Computer and Communications Security. ACM, 2007: 584-597.

[17] WANG C, CHOW S S M, WANG Q, et al. Privacy-Preserving Public Auditing for Secure Cloud Storage[J]. IEEE Transactions on Computers, 2013, 2009(2): 362-375.

[18] WANG Q, WANG C, LI J, et al. Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing[C]// European Conference on Research in Computer Security. Springer-Verlag, 2009: 355-370.

[19] ZHU Y, WANG H, HU Z, et al. Dynamic audit services for integrity verification of outsourced storages in clouds[C]// Proc. of the 2011 ACM Symposium on Applied Computing (SAC). 2011: 1550-1557.

[20] KAI H, CHUANHE H, JINHAI W, et al. An Efficient Public Batch Auditing Protocol for Data Security in Multi-cloud Storage[C]// Chinagrid Conference. IEEE Computer Society, 2013: 51-56.

[21] YANG K, JIA X. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing[J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 24(9): 1717-1726.

[22] HE K, HUANG C H, WANG X M, et al. Aggregated privacy-preserving auditing for cloud data integrity[J]. Journal on Communications, 2015, 36(10): 119-132. (in Chinese)
何凯,黄传河,王小毛,等. 云存储中数据完整性的聚合盲审计方法[J]. 通信学报,2015,36(10):119-132.

[23] BLEIKERTZ S, SCHUNTER M. Security audits of multi-tier virtual infrastructures in public infrastructure clouds[C]// Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2010: 93-102.

[24] BLEIKERTZ S. Automated Security Analysis of Infrastructure Clouds[J]. Institutt for Telematikk, 2010, 18: 113-122.

[25] DOELITZSCHER F, FISHER C, MOSKAL D, et al. Validating Cloud Infrastructure Changes by Cloud Audits[C]// Services. 2012: 377-384.

[26] DOELITZSCHER F, REICH C, KNAHL M, et al. An agent based business aware incident detection system for cloud environments[J]. Journal of Cloud Computing, 2012, 1(1): 1-19.

[27] MADI T, MAJUMDAR S, WANG Y, et al. Auditing Security Compliance of the Virtualized Infrastructure in the Cloud: Application to OpenStack[C]// ACM Conference on Data and Application Security and Privacy. ACM, 2016: 195-206.