基于 Azure 的云安全研究

朱圣才
(上海市信息安全测评认证中心,上海 200011)

摘 要:随着云计算的进一步推进和发展,云计算面临的安全问题变得越来越突出,特别是在云计算带来的诸多利益下,如何满足用户在云计算环境下对用户数据的机密性、完整性等相关性能的需求,已成为云计算安全的首要难题。文中以微软 Azure 平台为基础,从云安全分析入手,针对 Windows Azure 云安全进行分析研究。在 Azure 架构下,探讨 Azure 云安全解决方案,分别从 IaaS、PaaS、SaaS 三个角度对微软 Azure 云平台安全方案给出应对措施,为进一步对微软 Azure 云平台进行更深层次的测评分析提供技术支持。

关键词:云计算;云安全;Windows Azure;Azure 安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)12-0143-04
doi:10.3969/j.issn.1673-629X.2013.12.034

Research on Cloud Computing Security Based on Windows Azure

ZHU Sheng-cai
(Shanghai Information Security Testing Evaluation and Certification Center, Shanghai 200011, China)

Abstract: With further promotion and development of cloud computing, the security problems faced by cloud computing are becoming more and more prominent, in particular, under the benefits of cloud computing, how to satisfy user requirement about the confidentiality and integrality of user data, and correlative capability in the cloud computing environment has become the primary security problem of cloud computing. Based on the Microsoft Azure platform, starting from the cloud security, research the security of the Windows Azure cloud. In the Azure architecture, to explore Azure cloud security solutions, respectively from three angles of IaaS, PaaS, SaaS on Microsoft Azure cloud platform security solution give the response measures, providing technical support for Microsoft's Azure cloud platform for a deeper evaluation analysis.

Key words: cloud computing; cloud security; Windows Azure; Azure security

0 引 言

在传统的计算模式下,用户对数据的存储与计算拥有完全的控制权;而在云计算模式下,用户数据与机器的管理将完全依赖于服务提供商,而用户仅仅保留对虚拟机的控制。因此,从用户的角度来说,如何保证存储数据与计算结果的安全性、私密性、可用性显得尤为重要[1-6]。从关注安全领域研究的从业者来看,目前的云计算技术充满了各种风险,特别是在整个架构上有着独有的脆弱性,云安全将成为云计算技术发展中最重要的关注点。

目前,对云计算安全进行研究和分析主要分为工业界和学术界,工业界主要还是综合运用传统的安全技术,学术界则围绕云计算的特点研究新的技术。文中主要从 Windows Azure 架构和云安全协议,以及云安全类型三个方面,分析研究微软 Windows Azure 云安全解决方案。

1 云安全

国际数据公司(IDC)的高级副总裁兼主要分析师 Frank Gens 在他的分析报告中指出云计算服务仍然处在早期发展阶段,对于云计算服务提供商来说,毫无疑问还有很多的问题需要解决。Frank Gens 指出目前用户最关心的是云计算的安全问题,当用户的商业信息和重要的 IT 资源放置在云上时,用户觉得很不安全[7-10]。

其实,关于云安全,早在云计算刚刚开始浮现的时候,国外的 IT 研究机构 Gartner 就提出了关于云安全风险的七个安全议题,对于云安全,主要可以通过 IaaS

收稿日期:2013-03-09 **修回日期**:2013-06-12 **网络出版时间**:2013-09-29
基金项目:国家科技支撑计划项目(2009BAH50B02)
作者简介:朱圣才(1986-),男,安徽安庆人,硕士,软件测试工程师,研究方向为信息安全、虚拟化与云计算。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130929.1544.044.html

安全、PaaS 安全、SaaS 安全三个部分来进行分析。

1.1 IaaS 安全

对于基础设施即服务的安全性,首先需要考虑的是数据中心的地理位置安全,在地理位置的选取上,要保证基础设施的安全性;其次,数据中心地理位置的选取主要依据该地理位置的网络衔接点与环境以及电力成本等因素;另外,自治系统在基础设施安全性方面也非常重要,因为自治系统不仅管理数据中心的所有硬件资源,还处理数据中心的大部分可自动化的系统管理工作。IaaS 安全性问题如表 1 所示。

表 1 IaaS 安全性问题

安全性	描 述
数据中心安全性	在云计算实体数据中心,云服务提供商在关键地点都设置了人员识别系统,并且配合了智能卡等设备管制人员的进出,自治系统会记录人员的操作记录,从而确保人员的操作不会影响数据中心与云平台的运作
硬件安全性	硬件设备作为数据中心的灵魂,主要包括服务器和网络设备两大类。云数据中心的所有服务器和网络设备都是预先规划好的,从而使得硬件设备在发生问题时,能够快速地发现问题解决问题
网络安全性	网络安全性中的拒绝服务器攻击以及其派生的分布式拒绝服务攻击都是利用暴增的流量导致服务应用程序超负荷工作而死机,目前云数据中心应对攻击的解决方案大多都是通过异常流量检测方式来拒绝服务攻击不至于影响所有用户

1.2 PaaS 安全

IaaS 安全主要是围绕实体层次的安全进行描述,PaaS 安全则是从软件和操作系统本身的安全进行研究,其中 PaaS 安全主要包括操作系统、访问控制、数据传输以及数据安全四个角度进行安全保障。PaaS 安全性问题如表 2 所示。

表 2 PaaS 安全性问题

安全性	描 述
操作系统	一般来说,操作系统安全是由开发商进行修复的;对于云计算数据中心,自治系统可以自动部署和修复文件,保证操作系统漏洞确实得到修复
访问控制	为了保护虚拟机不受恶意程序的攻击,位于虚拟机内的操作系统通常不会开放太大的权限给应用程序,当然,开放的权限一定能够确保应用程序正常运行;同时,不允许应用程序去修改操作系统的任何设置,所有对操作系统的设置只能由云服务提供商按照事先要求进行设置和管理
数据传输	对于云计算数据中心的所有数据传输,都使用了 SSL 功能,从而使得无论是跨越数据中心还是由客户端直接访问内部服务,都必须使用 SSL 在传输中加密数据,否则都会在服务的终结点被拦截
数据安全	对云计算安全的安全体系来讲,数据安全将是所有人最为关心的安全点

1.3 SaaS 安全

SaaS 安全依赖于 PaaS 所提供的云安全环境,同时还依赖于云应用程序开发人员对云应用程序开发时对安全的考虑和防护,所以在 SaaS 安全性方面除了 PaaS 提供的基础安全性以外,云应用程序开发人员在进行云应用软件设计时应该以信息安全为首要考虑。在 SaaS 安全中,除了多租户可能存在的问题外,针对 WEB 应用程序,都需要防范 OWASP 所公布的十大 WEB 安全性问题,常见的有注入、跨站脚本、失效的身份认证和会话管理、不安全的直接引用以及伪造跨站点请求等威胁。

2 Windows Azure

Windows Azure 是微软推出的云计算平台,Windows Azure 管理着微软数据中心的中控软件、虚拟机任务管理器以及虚拟机本身等组件,即管控整个数据中心所有的硬件和软件,包括云应用程序与计算资源使用情况以及容错机制等[11-15]。此节重点介绍 Windows Azure 的架构,从本质上认知 Windows Azure 平台。

Windows Azure 可以分为三部分,第一部分是部署在虚拟机上面的 Windows Azure Guest OS,该部分提供云应用程序所执行的环境,如图 1 所示。

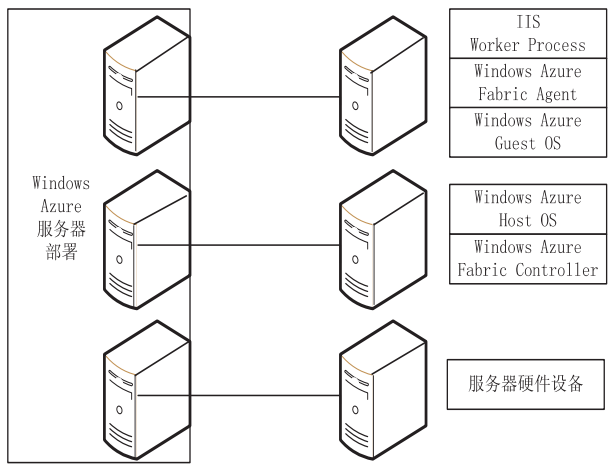

图 1 Windows Azure 虚拟机部署架构

第二部分是实体机上面的虚拟机 Windows Azure Host OS,该部分提供 Windows Azure 管理服务所需要的 Metadata 交换以及针对不同虚拟机通信所必须的负载均衡与容错功能,另外,Host OS 还有一个重要的任务就是在应用程序部署时,读取应用程序的服务定义文件,从而决定 Windows Azure Guest OS 的版本。Windows Azure Host OS 架构如图 2 所示。

第三部分是最底层的 Windows Azure 操作环境:Fabric Controller,它安装在数台中控服务器上,提供数据交换、配置管理与健康监控等功能,同时 Fabric Controller 是 Host OS 的主要执行者。

3 Azure 云安全解决方案

针对 Windows Azure 的架构和云安全所面临的问

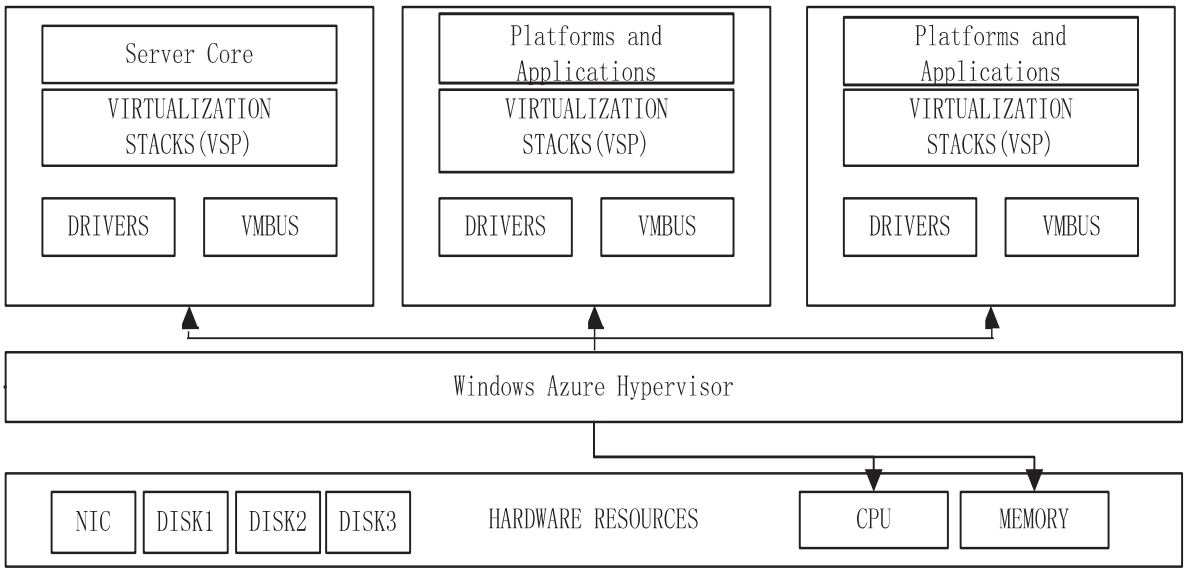

图 2　Windows Azure Hypervisor(Host OS)架构

题,微软 Windows Azure 开发团队为 Windows Azure 云平台在 IaaS、PaaS、SaaS 方面做了很多的防范和努力。此节介绍微软在 Azure 云安全方面提供的应对措施。

3.1　Azure IaaS 安全

在实体与基础设施的安全性方面,大多数数据中心所采用的方法基本相似,目前针对 Windows Azure IaaS 安全性,微软云数据中心是由 Microsoft Global Foundation Service 下的 Online Services Security and Compliance 团队负责,在 Azure IaaS 安全方面,Microsoft Global Foundation Service 为 Windows Azure 做了很多努力,对传统常见的攻击手段都给出了相应的应对措施,如表 3 所示。

表 3　Windows Azure IaaS 安全性应对措施

攻击方法	应对措施
端口扫描攻击	在每一个 Windows Azure 的实体服务器与 VM 中,只有要使用的通信端口被打开,而且默认禁止访问服务定义文件,在 Windows Azure Host OS 内的虚拟交换器都有特殊的数据包分析器,可以防止未授权的流量进入 VM
拒绝服务攻击	Windows Azure 的负载平衡器具有异常流量检测功能,在发现异常流量时会自动由 Fabric Controller 下令将连入服务所在的 VM 的 Virtual Public IP 关闭,并下令防火墙将异常流量挡在防火墙外面,以确保其他 Windows Azure 用户服务不会被影响
电子欺骗攻击	Windows Azure IaaS 都是以 VLAN 划分,可以防止异常的广播数据包以及多点传送数据包的攻击,Host OS 虚拟交换器会自动过滤异常的数据包
窃听截包攻击	Windows Azure IaaS 利用实体交换器限制针对同一个内部服务器群的网络数据包探测
多租户和边界攻击	Windows Azure IaaS 以特殊的算法,确保 VM 之间不会受到频率或内存缓存探测的攻击手段所产生的攻击
外部认证攻击	Windows Azure IaaS 的安全性,都委托两家外部的信息安全公司进行检测与问题报告,再由 Windows Azure 团队进行修正或调整

3.2　Azure PaaS 安全

此小节主要针对 Windows Azure 平台,在平台即服务模式中存在的威胁给出一系列的解决方案,并且这些解决方案都是用户可以靠自己的能力解决的,而不是向供应商求助。

PaaS 云服务最有可能会遇到以下威胁:系统配置不当、SSL 及部署缺陷、云数据中的非安全访问许可三个方面,尽管说 PaaS 云服务模式中还有很多其他风险和危险因素存在,但以上三条绝对是最有可能影响云服务部署工作的,也是 PaaS 安全性中最常见的问题。

(1)系统配置不当:Windows Azure 确保了 IIS、SQL Azure 和. NET 安全的能力,系统管理人员及时更新系统补丁,检查系统配置信息;

(2)SSL 及部署缺陷:对于应对 SSL 攻击而言,需要依靠 Windows Azure 正确配置及时进行系统配置和补丁更新,这里需要注意的是及时,确保 SSL 补丁和变更程序能够迅速发挥作用,从技术和管理两个方面预防 SSL 及部署缺陷;

(3)云数据中的非安全访问许可:Windows Azure 对 Office365 项目进行了详细的风险评估,在系统层面把安全工作做得更加稳固;同时 Windows Azure 应用很多行业内部的安全许可制度,对访问控制进行授权限制。

3.3　Azure SaaS 安全

在软件即服务模式中,用户往往依靠供应商来保证应用的安全。然而,PaaS 尽管可以保障云计算基础架构(防火墙、服务器、操作系统等等)的安全,但控制和保证应用安全的任务还是需要用户自己来承担;Azure SaaS 安全同样需要解决配置不当、非安全访问等相关威胁,如应用配置不当,Windows Azure 要求用户应该注意云应用安装后遗留下来的默认目录和实例文件,还有多余的服务以及默认的用户名和密码等。

Windows Azure SaaS 包括 Microsoft Exchange On-

line、Microsoft SharePoint Online、Microsoft Office Live Meeting、Microsoft Lync Online 以及 Microsoft Dynamic CRM 等软件即服务功能,也就是微软推出的 Microsoft Office365 项目,在操作系统与应用程序执行环境方面,Windows Azure 的 Guest OS 是以差异化磁盘进行操作系统部署,所有系统设置无法被应用程序更新。

4 结束语

云计算等开放网络服务环境的安全问题成为企业是否采用云计算等开放网络服务的重要疑虑之一。关注基于云计算等开放网络服务的 IT 应用中的安全设计,并去解决开放网络服务所引发的安全问题势在必行。文中基于 Windows Azure 云平台,结合微软 Office365 项目和微软 Azure 架构,研究 Windows Azure 云平台安全性要求,分别从 IaaS、PaaS、SaaS 三个角度分析研究了 Windows Azure 架构下云平台当下对云安全所提供的保护措施以及相应的解决方案,保证 Windows Azure 云平台的安全性,从而进一步促进云计算安全走向成熟。

参考文献:

[1] Jennings R. 云计算与 Azure 平台实战[M]. 王 鑫,丁斌,译. 北京:清华大学出版社,2011.

[2] 朱明中. Windows Azure 实战手记[M]. 北京:中国水利水电出版社,2011.

[3] 赵立伟,方国伟. 让云触手可及:微软云计算实践指南[M]. 北京:电子工业出版社,2010.

[4] 杨文志. 云计算技术指南-应用、平台与架构[M]. 北京:化学工业出版社,2010.

[5] 王 鹏. 云计算的关键技术与应用实例[M]. 北京:人民邮电出版社,2010.

[6] John R, James R. Cloud computing: Implementation, management, and security[M]. Beijing: China Machine Press, 2010.

[7] Rings T, Grabowski J, Schulz S. Grid and cloud computing: Opportunities for integration with the next generation network [J]. Grid computing, 2009(7): 375-393.

[8] Zhang Liangjie, Zhou Qun. CCOA: Cloud computing open-architecture[C]//Proc of 2009 IEEE international conference on Web Services. New York: IEEE Computer Society Press, 2009: 607-616.

[9] Yousef L, Bulrico M, Silva D. Toward a unified ontology of cloud computing [EB/OL]. 2010. http://www. collabogce. org/gce08/images/7/76/LamiaYousef. pdf.

[10] 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.

[11] 陈尚义. 浅谈云计算安全问题[J]. 网络安全技术与应用,2009(10):20-22.

[12] 李 玮. 云计算安全问题研究与探讨[J]. 电信工程技术与标准化,2012(4):44-49.

[13] 张爱玉,邱旭华,周卫东,等. 云计算与云计算安全[J]. 中国安防,2012(3):89-91.

[14] 杨 健,汪海航,王 剑,等. 云计算安全问题研究综述[J]. 小型微型计算机系统,2012,33(3):472-479.

[15] 陈 全,邓倩妮. 云计算及其关键技术[J]. 计算机应用,2009,29(9):2562-2567.

(上接第 142 页)

[J]. 计算机工程与应用,2012,48(20):112-116.

[4] Chen Lian. A kind of improved attribute reduction algorithm in intrusion detection application research based on rough sets theory[C]//Proc of international conference on computer science and automation engineering (CSAE). [s. l.]: [s. n.], 2011: 707-710.

[5] 樊爱京,杨照峰. 用于网络入侵检测的模式匹配新方法[J]. 计算机应用,2011,31(11):2961-2964.

[6] 汪淑丽. 基于支持向量机的无线传感器网络的入侵检测系统[J]. 传感器与微系统,2012,31(7):73-76.

[7] 汪 洁,杨 柳. 基于蜜罐的入侵检测系统的设计与实现[J]. 计算机应用研究,2012,29(2):667-671.

[8] 安辉耀,吴泽俊,王新安,等. 用于网络入侵检测的群体协同人工淋巴细胞模型[J]. 通信学报,2010,31(9):122-130.

[9] 李正洁,李永忠,徐 磊. 免疫 Agent 和量子粒子群优化的入侵检测方法研究[J]. 计算机工程与应用,2012,48(1):102-104.

[10] 余小华,黄灿辉,陈 瑛. 一种蚁群伏化的 WSN 分布式入侵检测模型[J]. 计算机工程与应用,2012,48(9):78-82.

[11] Ma C, Cao A, Zhou Y. Primary research on improved algorithm of ant colony clustering combination[J]. Journal of Shenyang Jianzhu university (natural science), 2011, 27(4): 798-803.

[12] Xi O, Bin T, Qi L, et al. A novel framework of defense system against DoS attacks in wireless sensor networks[C]//Proc of 2011 7th international conference on wireless communications, networking and mobile computing. [s. l.]: IEEE, 2011: 1-5.

基于Azure的云安全研究

作者： 朱圣才， ZHU Sheng-cai
作者单位： 上海市信息安全测评认证中心,上海,200011
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013(12)