

文章编号: 1001-9081(2013)12-3350-04

doi: 10.11772/j.issn.1001-9081.2013.12.3350

基于云计算的电子邮件安全服务系统的设计与实现

戴瑾¹, 刘波^{2*}, 卞皓宇³

(1. 南京大学金陵学院, 南京 210089; 2. 趋势科技中国研发中心, 南京 210012; 3. 南京大学 软件学院, 南京 210098)

(*通信作者电子邮箱: cn.liubo@gmail.com)

摘要: 目前电子邮件安全扫描软件正在被广泛使用, 随着用户数量和系统流量的激增, 传统的紧耦合同步处理IMHS系统整体效能、健壮性、可维护性、可扩充性上都存在着难以克服的问题。针对海量用户压力之下存在的系统瓶颈, 确立了以“松耦合、异步、无状态”为设计原则, 通过融合云计算及面向服务体系结构(SOA)技术, 设计并实现了一个基于P2P协同的对等化电子邮件安全云服务系统。该系统支持服务过程动态协同, 有效提高了资源使用效率和系统可伸缩性。最后在实际系统中通过典型操作实例测试分析了系统性能, 验证了系统架构的可行性和有效性。

关键词: 云计算; 电子邮件安全服务; 面向服务体系结构; 对等网络; 表达性状态转移

中图分类号: TP393.027; TP393.098 文献标志码: A

Design and implementation of E-mail security service system with cloud computing

DAI Jin¹, LIU Bo^{2*}, BIAN Haoyu³

(1. Jinling College, Nanjing University, Nanjing Jiangsu 210089, China;

2. Trend Micro China Development Center, Nanjing Jiangsu 210012, China;

3. Software Institute, Nanjing University, NanJing Jiangsu 210098, China)

Abstract: E-mail security scanning software is being widely used. With the rapid increase of user number and system flow, there are insurmountable problems in terms of performance, robustness, maintainability and scalability in the traditional tightly-coupled and synchronous IMHS (Inter-scan Message Hosted Security) system. With regards to the system bottleneck by the mass users, a loosely-coupled, asynchronous, stateless principle was proposed for system design. Through the integration of cloud computing and Service Oriented Architecture (SOA) technique, a P2P-based E-mail secure cloud service system was designed and implemented. The system supports dynamic collaborative process, and effectively improves the efficiency of resource use and system scalability. The results and analysis of typical operation tests in real system verify the feasibility and effectiveness of the system architecture.

Key words: cloud computing; E-mail security service; Service Oriented Architecture (SOA); Peer-to-Peer (P2P); REpresentational State Transfer (REST)

0 引言

电子邮件是互联网上历史最为悠久, 使用最为广泛的通信手段。当前, 互联网中各种垃圾邮件泛滥, 病毒猖獗, 然而传统的电子邮件安全扫描软件安装维护复杂, 运行成本高昂, 严重影响了服务质量。因此, 如何提高电子邮件安全扫描软件的可部署性和优化软件系统性能成为相关技术研究的热点问题之一。作为分布式计算技术的最新发展, 云计算为有效聚集可用资源、实现动态资源共享提供了商业实现模式, 相关技术研究受到学术界及产业界的高度重视^[1]。

目前市面上广泛应用的邮件安全服务系统如IMHS(Inter-scan Message Hosted Security)系统都是基于传统网关扫描软件架构基础构建而成的。在海量用户压力之下, 此类系统存在效率低下、扩充困难、鲁棒性差、维护困难等一系列问题。

为了从根本上消除上述问题, 本文提出了以“松耦合、异步、无状态”为原则的新型电子邮件安全云服务系统架构方案, 设计和实现了基于云计算的电子邮件安全服务系统。该系统以对等化为贯彻上述原则的切入点, 在云端引入基于对等网络(Peer-to-Peer, P2P)的分布式计算模式的云服务节点

资源共享模型, 实现了基于面向服务的体系结构(Service Oriented Architecture, SOA)的云服务软件动态协同机制^[2]。

1 系统架构设计优化方案

1.1 紧耦合同步处理系统存在的问题

目前市场上使用的邮件安全服务系统软件都不是按照分布式系统的要求设计和实现的, 而是在原有网关扫描产品的同步架构的基础上设计实现的, 是一个典型的三明治结构, 如图1所示。整个系统基本上依据传统的邮件递送系统的思想, 由邮件递送服务器、内容扫描系统、用户交互系统等一系列子系统构成。子系统包括接收MTA(Mail Transfer Agent)、扫描服务器(Scanner)、发送MTA、Web用户界面、策略服务器、日志服务器、邮件隔离服务器、数据库及其他后台支撑系统。各子系统之间相互紧密耦合, 任何独立的子系统都不能单独工作。

这种设计方式具有结构简单、处理流程直接、单封邮件处理时间短的优点。但它的缺点在于, 主要的子系统都是通过简单邮件传输协议(Simple Message Transfer Protocol, SMTP)直接或间接连接在一起, 紧耦合同步处理方式造成了在系统整体效能、健壮性、可维护性、可扩充性上存在难以克服的困难。

收稿日期: 2013-08-05; 修回日期: 2013-08-09。 基金项目: 国家自然科学基金面上项目(61170069)。

作者简介: 戴瑾(1973-), 女, 浙江绍兴人, 讲师, 硕士, CCF会员, 主要研究方向: 分布式计算、并行处理; 刘波(1973-), 男, 江苏南京人, 工程师, 硕士, 主要研究方向: 云安全系统; 卞皓宇(1992-), 男, 江苏南通人, 主要研究方向: 分布式计算。

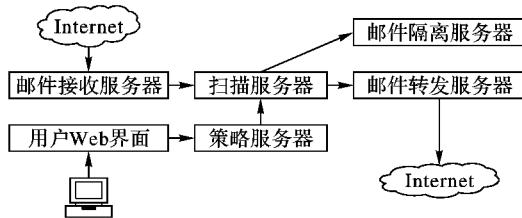


图 1 传统的 IMHS 系统结构

例如,扫描服务器(Scanner)接收到 Inbound MTA 的连接请求后立刻发出连接 Outbound MTA 的请求,只有收到 Outbound MTA 的回应后,才能返回对应的回应给 Inbound MTA。每一个 SMTP 的命令处理都要经过相同的流程。

这种严格同步机制,使整个系统的吞吐率严重依赖于模块的瞬间性能,任何一个模块的性能瓶颈都会造成这个系统性能的大幅度下降,也导致对系统整体容量的评估异常困难^[3]。一旦基础设施有任何的不稳定,都可能导致系统出现吞吐量下降、响应缓慢等问题。此外,各模块间的依赖很复杂,也会造成系统出现故障时,无法快速定位故障发生点并进行排除,十分不利于日常维护。

1.2 确立解决方案

针对上述问题,本文在优化系统的设计中提出了三个基本设计原则:松耦合、异步和无状态^[4]。

1.2.1 松耦合

依据松耦合的原则将系统划分为多个互相之间耦合度最小的子系统,保证子系统的独立性和自闭性,既有利于系统的实现和测试,也有利于将来对服务的扩充。

1.2.2 异步

整个系统数据流和控制流在各子系统之间的传输尽量采用异步模式,提高对硬件的使用效率,减少系统瓶颈,提高系统伸缩性。

1.2.3 无状态

无状态原则是指系统的各模块必须尽量做到不保存状态,这样当某些服务器软硬件发生故障时,可以将事务迅速转移到其他服务器上,不需要做复杂的状态迁移。这种设计有利于实现计算的虚拟化,无状态意味着事务在这台或那台服务器上完成并无区别,计算并不依赖具体的软硬件,当需要扩充容量时,只需要向计算资源池内投入更多的服务器就可以实现系统处理能力的无缝伸缩。

基于这三个设计原则,设计并实现了基于云计算的电子邮件安全服务系统。在优化设计中,采用 P2P 系统架构为系统解耦,通过 SOA 的软件架构设计保证系统的异步性和无状态性。也正是系统的松耦合、无状态和异步设计使得系统硬件部署上得以借助云计算的平台技术来实现,使系统性能得到更好的发挥。

2 对等化电子邮件安全云服务系统的设计

2.1 系统异步处理架构——P2P 对等网络

前面分析了各模块间的紧耦合和同步处理是造成很多问题的根源。遵循松耦合的原则,首先从优化网络架构的角度提出了 P2P 对等网络架构的解决方案。图 2 所示的是我们所采用的基于 P2P 对等网络的 IMHS 分布式处理的设计和实现方案,通过取消原有的集中式 IMHS 系统的中心节点,以 P2P 的平行结构取而代之,这种设计可以最大限度地消除系统的瓶颈,提高整个系统的可靠性。重要的是这种设计不依赖特定的软硬件,可以方便地部署到虚拟化的环境中,特别适合在

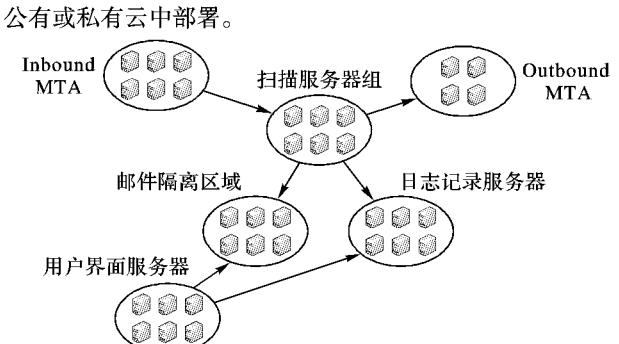


图 2 P2P 对等网络分布式处理 IMHS 系统

该方案将整个系统按功能分成若干个子系统,每个子系统由一组功能同构的服务器组成。整个系统各个节点都是平等的,没有中心节点,计算和存储任务由各个节点自行协调分配到最适合的节点处理;节点不保存状态,每个任务由某个节点处理;节点之间没有依赖关系,每个节点都拥有完成自身处理任务所必须的数据和资源^[5]。扩展系统处理能力只需要线性地增加服务器就可以做到,并且在添加服务器时,系统的处理能力和存储能力都同步得到扩充。

2.2 系统动态资源共享——云计算技术实现模式

2.2.1 云安全服务的实现策略

传统电子邮件安全服务系统方案允许垃圾邮件和病毒下载到公司内部后再处理,存在潜在威胁,系统需不断地投入资金和技术人员进行升级和维护。为有效地解决该问题,在 P2P 对等网系统架构上,将云计算模式和电子邮件安全扫描功能相结合,建立电子邮件安全云。云计算技术可以有效聚集可用资源和实现动态资源共享。如图 3 所示,服务采用 SaaS(Software as a Service)模式,用户只需提供邮件服务的请求,并提交服务的输入,就可以直接得到服务的结果。这样既可以有效保证系统运行的稳定性、高效性及实时性,还可大大降低用户的处理成本和管理成本。



图 3 电子邮件云安全服务模式

在电子邮件云安全服务中,用户在使用了系统提供的云安全扫描服务以后,通过设置域名服务器(Domain Name Service,DNS)记录,将自己的邮件流中转到系统提供的安全云入口。邮件在经过扫描以后转发给用户的邮件服务器。在这个过程中,大约 95% 以上的垃圾邮件和病毒邮件在云端被过滤掉,不会下载到用户端,也不会占用用户的带宽和处理资源。用户所有的配置信息和安全策略以及安全统计信息都保存在云端,用户还可以通过浏览器登录到系统来修改和配置自己的安全策略,查看统计信息等。

2.2.2 云安全服务的部署

本文系统使用的是趋势科技的云平台,安全服务部署于分布在北美和欧洲的四个不同的数据中心内,每个数据中心都具有完全独立的服务器集群提供服务。这些服务器和数据中心对于用户来说是完全透明的。趋势科技负责管理所有数据中心的服务器系统,并保证用户的邮件能够得到及时有效的处理。

数据中心内的服务器集群采用多租户冗余设计,当一台

服务器发生故障时,用户的邮件会被自动切换到正常的服务器上。分别部署在美国东西海岸的两个数据中心互为备份,用户的帐户和配置信息在两个数据中心之间实时同步,在最坏的情况下,如因为基础设施的故障,整个数据中心发生问题时,另一个数据中心能够自动接管所有的邮件流量,保证用户的电子邮件不受影响。同样部署于欧洲的数据中心也具有同样的结构。

系统充分发挥了云计算的优势,把所有的资源都通过互联网连接成一个虚拟的云服务系统。通过对服务的虚拟化,云安全系统可以为用户提供 24 小时不间断的可靠服务,保证用户的业务任何时候都不会因为各种事件和故障而中断。

2.3 基于 SOA 的软件构架方案设计

系统的整体设计采用的是 SOA 软件架构,它是一种粗粒度、松耦合服务架构,系统以 Web Service 作为内部的通信接口,运用代理技术将系统的主被动部分分开^[6],实现异步处理。

2.3.1 系统解耦设计方案

只有降低系统各部件之间的耦合度之后,才能把系统有效分割为几个子系统分别进行调试和优化。从软件设计角度对传统 IMHS 系统详细分析,发现主要耦合部分在以下三个方面:1)从 Inbound MTA 到 Scaner 的 SMTP 连接;2)从 Scaner 到 Outbound MTA 的 SMTP 连接;3)Scaner 内部的一些慢速的处理。

这三个部分形成了一个串行化处理路径 Inbound MTA→Scaner→Outbound MTA,路径上的部件互相牵制,互相制约,其峰值处理能力在最佳情况下,也远远小于路径中最慢的部件的处理能力。只需将这个路径上的同步处理通过解耦分成三个独立的处理过程,并在它们之间建立缓冲队列以平衡任务的峰值和谷值,那么系统的处理能力应该接近或等于性能最差部件的峰值处理能力。由此可通过提高最慢的子系统的处理能力来消除瓶颈,提高系统整体性能。

因此在三者之间加入异步转送邮件的模块,切断 MTA 和扫描服务器之间的紧密耦合,将同步过程转变为异步过程,并通过缓冲队列来调节数据流的峰谷值之间的平衡,以获得最大平均性能。

系统的解耦方案如图 4 所示。在 MTA 和扫描服务器(Scaner)之间插入两个转发代理及一个缓冲队列,同时取消 MTA 和扫描服务器(Scaner)之间的 SMTP 连接。系统工作流程将按如下方式进行:Inbound MTA 收到邮件之后不再启动 SMTP 连接去发送,而是直接保留在自己本地的磁盘里;转发代理 1 检索到这些文件后,将它们通过网络转发到扫描服务器上,邮件被保存在扫描服务器上的缓冲队列里;扫描服务器的工作进程定期查询缓冲队列来检索新的任务,一旦发现有新的邮件到达,即将新邮件提交;完成扫描的邮件被回送到缓冲队列中,由转发代理 2 将这些邮件转发给 Outbound MTA,随后从缓冲队列中删除这些邮件,完成处理过程。

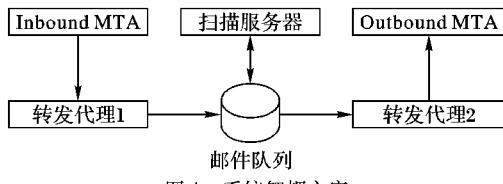


图 4 系统解耦方案

IMHS 系统内存在多个 Agent 和 Service,需要考虑如何来管理这些动态的组件,让 Agent 和 Service 之间实现直接的 P2P 通信,这种对等网的软件架构如图 5 所示。完全对等网状通信结构更有利于负荷的均匀分配^[7],系统的扩充也较为

容易。添加新功能时,只需要加入新的 Agent 和 Web Service;性能不足时,只需添加相应的服务器。P2P 的扁平层次结构更适合一个大型动态环境,是可不断进行动态扩充的系统^[8]。

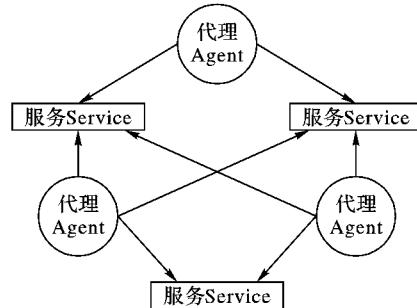


图 5 基于对等网的软件架构

考虑到松耦合和异步通信的设计原则,在接口的设计风格上遵照高负载分布式系统的设计基本原则,通过对流行的 SOA 的分析,选择了 RESTful(REpresentation State Transfer) 式的 Web 服务^[9]。这种以数据为中心的设计架构,服务器尽量保持无状态的设计,服务器之间的通信通过 Agent 的异步传输来实现,服务器之间没有直接的耦合关系,较好地解决了扩展性、可靠性以及低成本之间的矛盾,效能也比旧架构有较大的提高^[10]。组件之间通过注册服务器建立逻辑关系,每个注册服务器都保存一张所有组件的状态表。组件是在异步模式下工作的,通过 HTTP 协议,建立输入输出队列来交互数据。

2.3.2 系统功能逻辑设计

系统经过解耦后,可以划分为 12 个主要组件,每个组件都由一个独立的 Web Service 来实现,这些组件可分别驻留在不同服务器上,也可以让多个组件共享一台服务器,还可在多个服务器部署同一组件的多个副本来自滑峰值负载。图 6 为系统主要部件和子系统关系图。

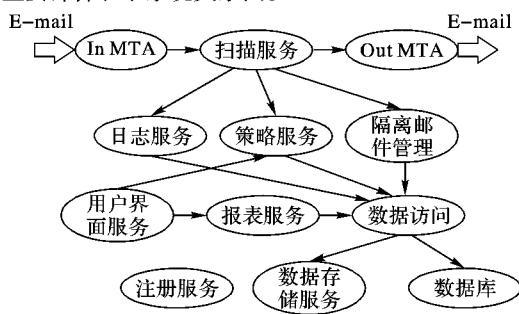


图 6 系统主要部件

2.3.3 系统性能的扩展

在用户大量增加、系统现有容量不敷使用时,需要通过添加新的服务器来扩充系统的容量。本系统的设计可以允许用户采用即插即用的方式扩充系统,免去了繁琐的重新配置和调试的过程。首先,需要分析系统的瓶颈在哪里。由于本系统采用了完全异步的处理方式,判断瓶颈的工作变得非常简单,只要检查任务在哪一个服务处堆积,就能找到瓶颈。然后用户只需购买相应的硬件,安装软件后设置好注册服务器的地址,即可使新服务器自动投入运行。

3 系统性能测试与分析

基于“松耦合、异步、无状态”的原则,依据 SOA 软件设计架构设计和实现了基于云计算的对等化电子邮件安全服务系统,并对它和传统的邮件安全云服务系统进行了性能比较。

3.1 测试系统配置

测试服务器采用 DELL 2950, 操作系统为 CentOS 5.3, MTA 服务器安装 Postfix 2.3.3。选择了处理邮件的主要流程和组件, 即从输入 MTA 到扫描服务器再到输出 MTA 的流程。利用思博伦通信的 Avalanche 2900 测试仪模拟网络负载, 它是目前测试云系统的可靠工具。系统测试持续时间为 60 min, 邮件的测试样本采用纯文本的邮件, 其样本大小分布如表 1 所示, 该分布和实际运行的系统上观察到的分布基本一致, 可以较准确地反映系统在真实环境下的处理能力。

用来进行对比测试的系统是趋势科技运营的第一代云安全服务产品 IMHS 1.0, 采用传统架构设计, 该产品应用广泛, 目前已拥有了数百万的注册用户。

表 1 测试样本分布表

邮件大小/KB	样本分布/%	邮件大小/KB	样本分布/%
1	10	64	14
4	55	256	4
16	16	1 024	1

3.2 测试结果

经对比测试, 趋势科技运 IMHS 1.0 系统运行结果每秒处理邮件能力在 30 到 60 封范围内, 对等化架构的 IMHS 运行结果是系统每秒处理邮件能力在 60 到 180 封范围内。

传统架构的 IMHS 和对等化架构的 IMHS 两种系统 1 h 收邮件测试结果汇总如表 2 所示。

表 2 系统性能对比

系统	流量(成功连接次数)	吞吐速率/(封·s ⁻¹)	CPU 占用率/%	内存容量/GB
传统架构的 IMHS	160 438	≈50	≈10	≈5
对等化架构的 IMHS	399 705	≈120	≈25	≈7

3.3 结果分析

从表 2 可以看出, 与传统架构的 IMHS 相比, 本文提出的对等化架构的 IMHS 系统对 CPU 和内存的占用略有上升, 但性能却有 100% 以上的提高, 由于两个系统中扫描服务器本身的代码并未改变, 这个性能上的提高可以看作是新的体系架构所带来的。主要原因在于新的异步通信策略解放了扫描服务器, 使之不用等待上下游其他组件的响应, 可以全力投入对数据的扫描服务。同时, 异步的通信要求较少的通信线程, 这部分资源也可以投入到扫描服务中。所以, 尽管异步通信

引入了更多的 I/O 操作, 但是服务器的整体效能还是得到了提高。另外, 从结果可以看出, 整个系统的吞吐速率约等于最慢的部件——扫描服务器的吞吐速率, 添加更多的扫描服务器就可以提高系统的吞吐速率。

4 结语

本文探讨了高负载分布式系统的设计基本原则, 确立了松耦合、异步传输和无状态服务器的重要设计原则。基于这些原则, 通过对流行的 SOA 的分析, 设计建立了基于云计算的节点资源共享模型的对等化电子邮件安全服务系统。实际性能测试结果表明, 新系统设计达到了预期效果。在以后工作中, 我们还将进一步完善系统功能, 优化性能, 对自适应分组和动态调整服务器等方面展开进一步的研究, 为优化邮件系统的部署、提供个性化服务提供支持。

参考文献:

- [1] 郑纬民, 胡进峰, 代亚非, 等. 对等计算研究概论 [J]. 中国计算机学会通讯, 2004(2): 38–51.
- [2] JOSUTTIS N M. SOA in practice [M]. 程桦, 译. 北京: 电子工业出版社, 2008.
- [3] 张媛, 卢泽新, 刘亚萍. NFS over Lustre 性能评测与分析 [J]. 计算机工程, 2007, 33(10): 274–276.
- [4] 刘波, 杨强. 低成本分布式邮件备份系统的设计与实现 [J]. 微型机与应用, 2011, 31(5): 79–83.
- [5] 戴瑾, 谭良良, 王钦辉, 等. 一种基于聚类算法的 P2P 流媒体服务平台可视化监控系统的设计与实现 [J]. 微电子学与计算机, 2012, 29(12): 184–188.
- [6] ROCHARDSON L, RUBY S. RESTful Web Services [M]. 徐涵, 李红军, 胡伟, 译. 北京: 电子工业出版社, 2008.
- [7] 邹德清, 金海, 吴松, 等. 面向网格的协作式网络计算平台 [J]. 计算机学报, 2004, 24(12): 1617–1625.
- [8] RIPEANU M. Peer-to-peer architecture case study: Gnutella network [C]// Proceedings of the First International Conference on Peer-to-Peer Computing. Washington, DC: IEEE Computer Society, 2001: 99–100.
- [9] SLETTEN B. Resource-oriented architecture : the rest of REST [EB/OL]. [2009-03-12]. <http://www.infoq.com/articles/roa-rest-of-rest>.
- [10] ROBERTO L. Resource oriented architecture and REST [EB/OL]. [2013-02-22]. http://en.wikipedia.org/wiki/Resource_oriented_architecture.

(上接第 3334 页)

- [7] 李冰. 云计算环境下动态资源管理关键技术研究 [D]. 北京: 北京邮电大学, 2012.
- [8] 冯伟. 多目标优化的虚拟机调度模型与关键算法研究 [D]. 上海: 复旦大学, 2012.
- [9] 许力, 曾智斌, 姚川. 云计算环境中虚拟资源分配优化策略研究 [J]. 通信学报, 2012, 33(Z1): 9–16.
- [10] 谢文静. 云计算环境下虚拟机资源分配优化方法研究 [D]. 长沙: 湖南大学, 2011.
- [11] BELOGLAZOV A, BUYYA R. Energy efficient allocation of virtual machines in cloud data centers [C]// Processing of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing. Piscataway: IEEE, 2010: 577–578.
- [12] BELOGLAZOV A, BUYYA R. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers

[J]. Concurrency and Computation: Practice and Experience, 2012, 24(13): 1397–1420.

- [13] SHI Y X, JIANG X H, YE K J. An energy-efficient scheme for cloud resource provisioning based on CloudSim [C]// Proceedings of the 2011 IEEE International Conference on Cluster Computing. Piscataway: IEEE, 2011: 595–599.
- [14] Standard Performance Evaluation Corporation, Inc. SPECpower_ssj2008 result file fields [EB/OL]. [2012-11-24]. http://www.spec.org/power/docs/SPECpower_ssj2008-Result_File_Fields.html#Ratio.
- [15] Standard Performance Evaluation Corporation, Inc. SPECpower_ssj2008 [EB/OL]. [2012-11-18]. http://www.spec.org/power_ssj2008/index.html.
- [16] PARK K S, PAI V S. CoMon: a mostly-scalable monitoring system for PlanetLab [J]. ACM SIGOPS Operating Systems Review, 2006, 40(1): 65–74.