# 基于 vSphere 私有云的高校数据中心构建模式

鲍 陈,王海涛,汪千松,胡 冰
(安徽工程大学 现代教育技术中心,安徽 芜湖 241000)

**摘 要**:针对传统校园网数据中心 IT 资源配置模式存在的问题,转向虚拟化技术,在分析 vSphere 虚拟化架构基础上,从计算池、网络池、存储池、安全优化池的角度出发,提出一种基于 vSphere 私有云的高校数据中心构建模式,并详细介绍了私有云平台实施(IT 基础架构实施、虚拟化平台数据安全和 vCloud Directory 部署)。使用 vSphere 的私有云高校数据中心,降低了能源成本,提高了现有资源利用率,同时也提供自动化资源监控和按需分配、改进数据中心的灾难恢复方式和提高稳定性。实践证明,该模式构建的高校数据中心,优化了 IT 基础架构资源配置模式,提升了高校信息化建设水平,构建低碳、节能、减排、绿色的高校数据中心机房,增强了信息化系统的高可用性和安全性,也为其他高校同类建设项目提供了一个有意义的参考。

**关键词**:VMware vSphere;服务器虚拟化;私有云;IT 基础架构;vCloud Directory
**中图分类号**:TP311.52 **文献标识码**:A **文章编号**:1673-629X(2019)05-0182-05
doi:10.3969/j.issn.1673-629X.2019.05.038

# Campus Internet Data Center Deployment Mode Based on vSphere Private Cloud

BAO Chen, WANG Hai-tao, WANG Qian-song, HU Bing
(Modern Education Technology Center, Anhui Polytechnic University, Wuhu 241000, China)

**Abstract**: With regard to the problems related to IT resource allocation mode existed in the traditional campus network center, we present a vSphere private cloud-based construction mode for campus data center by means of virtualization technology and introduce the implementation of private cloud platform (the implementation of IT infrastructure, the data safety of virtualization platform and the allocation of vCloud Directory) in detail from the view of computation pool, network pool, storage pool and safety optimization pool on the basis of analyzing vSphere virtual infrastructure. The vSphere private cloud-based campus data center reduces energy costs, increases the utilization of existing resources, as well as realizes the monitoring and demand assignment of automated information resources, improves the disaster recovery methods of data center and the stability. The practice shows that the campus Internet data centers deployment mode optimizes the resource allocation mode of IT infrastructure, promotes the information construction level of universities, constructs low-carbon, energy-saving, emission-reduction and green campus Internet data centers, enhances the high availability and security of information system and also provides a meaningful reference for similar construction projection in other university.

**Key words**: VMware vSphere; server virtualization; private cloud; IT infrastructure; vCloud Directory

## 0 引 言

随着 PB 级大数据时代的到来,高校信息化建设也在迅速发展。传统的校园网数据中心采用“一套应用一套系统”的 IT 资源配置模式,面临管理复杂,资源利用率低,建设与运维成本高,业务的稳定性与连续性较差,安全控制和数据的灾备困难等问题,已经不能适应当前高校信息化的建设需求。云计算是一种采用虚拟化为基础架构,通过 IT 基础架构和软件向网络环境中的用户按需提供资源和服务的技术[1-2]。文中首先在分析 vSphere 虚拟化架构的基础上,提出了 vSphere 私有云基础架构,通过搭建高性能服务器集群和共享存储系统,利用 vSphere 的相关服务器虚拟化组件,对底层硬件进行整合利用,利用 vCloud Director 组件,将 IT 基础架构转变为私有云,构建新一代高可用性高校

**收稿日期**:2018-05-22 **修回日期**:2018-09-19 **网络出版时间**:2018-12-21
**基金项目**:安徽省自然科学基金资助项目(1508085ME70);安徽省高等教育提升计划项目(TSKJ2014B09);安徽工程大学计算机应用技术重点实验室开放基金项目(JSJKF201607);安徽工程大学校青年基金项目(2016YQ27)
**作者简介**:鲍 陈(1983-),男,助理工程师,硕士,研究方向为软件工程。
**网络出版地址**:http://kns.cnki.net/kcms/detail/61.1450.TP.20181221.1524.024.html

数据中心(Internet data center,IDC)。该方案有利于提高服务器整体利用率、简化管理与运维,实现信息化系统的高可用性和高安全性以及集群内主机和存储的负载均衡。

从经济效益和管理安全性考虑,vSphere 私有云基础架构的虚拟化构建是必要的。实践证明,该模式构建的高校数据中心,优化了 IT 基础架构服务模式,提升了高校信息化建设水平,也为其他高校同类建设项目提供了一个有意义的参考。

表 1　各种虚拟化技术对比

| 方式 | 性能 | 用户体验 | 形式 |
|---|---|---|---|
| 硬件仿真 | 30% - | 简单 | Hosted |
| 全虚拟化 | 30% -80% + | 简单 | Hosted/Hypervisor |
| 半虚拟化 | 80% + | 困难 | Hypervisor |
| 硬件辅助虚拟化 | 80% + | 一般 | Hosted/Hypervisor |
| 操作系统级虚拟化 | 80% | 困难 | 类似于 Hypervisor |

## 1　虚拟化技术

虚拟化技术[3-4]是通过映射或抽象的方式,通过虚拟化技术可以对包括基础设施、系统和软件等计算资源的表示,访问和管理进行简化,提高 IT 资源的利用率,如服务器、网络或存储设备,并且超出物理的局限性。虚拟化简化了资源管理,集中并共享了资源,使它们变成逻辑资源以最大限度地得到利用。

由于采用的虚拟化技术不同,可以将系统虚拟化分为五大类:硬件仿真、全虚拟化、半虚拟化、硬件辅助虚拟化、操作系统级虚拟化。各种虚拟化技术对比如表 1 所示。

## 2　vSphere 虚拟化架构分析

vSphere[5-6]是 VMware 公司首款云计算操作系统,以集成软件包的形式提供虚拟化、管理、资源优化、应用程序可用性和操作自动化等功能;并汇聚物理硬件资源(包括计算、存储和网络资源),允许用户创建通用管理服务的私有云,为高校数据中心提供高可用性、高安全性和可扩展性的虚拟资源解决方案。VMware vSphere 虚拟化架构如图 1 所示。VMware vSphere 在逻辑上由基础架构层(虚拟化层)、管理层和界面层构成,其中基础架构层包含基础架构和应用程序两个服务。

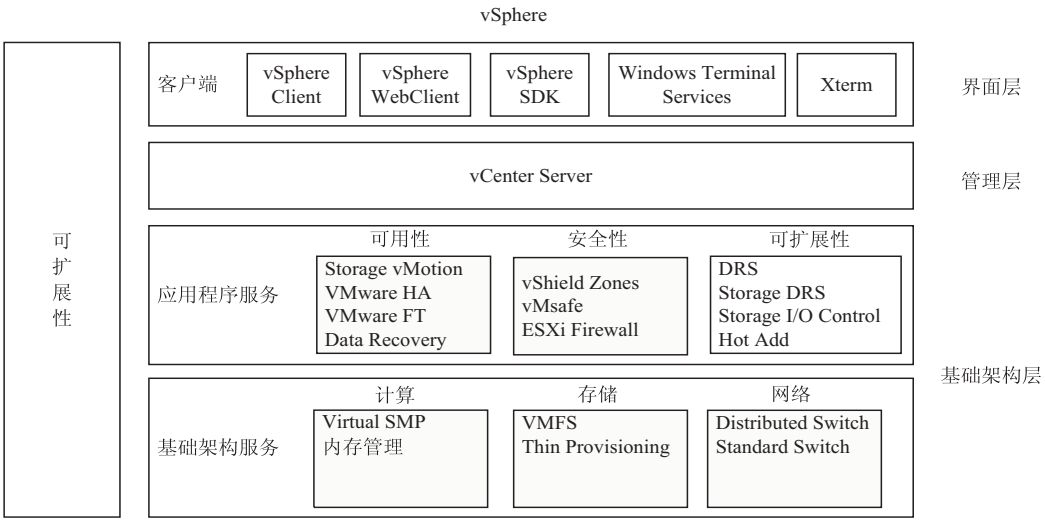



图 1　vSphere 虚拟化架构

(1)基础架构服务。VMware vSphere 通过基础架构服务抽象、聚合分配计算、存储和网络资源。①计算资源,即主机、集群和资源池;②存储资源,即数据存储和数据存储集群。其存储虚拟机的文件系统为 VMFS。数据存储技术包括 FC、FCoE、iSCSI、NAS 和 DAS;③网络资源,即使用虚拟交换机的主机和虚拟机提供网络连接。虚拟交换机分为标准虚拟交换机(vSS)和分布式虚拟交换机(vDS),支持 VMkernel 端口和虚拟端口组。

(2)应用程序服务。可用性是指提供应用、存储资源、基础架构和管理,包括高可用性 HA、故障容错 FT、数据保护、复制等。安全性是指提供安全虚拟应用程序防护,vShield 安全组件包括 vShield Manager(管理界面)、vShield App(网卡级防火墙)、vShield Edge(路由器)、vShield EndPoint(防病毒)和 vShield Data Security(数据安全),用来保护虚拟化数据中心。

(3)管理层。包含 vCenter Server。通过 vCenter Server 实现对数据中心进行单点控制,并提供基本的数据中心服务,如访问控制、性能监视以及配置。

(4)用户客户端。用户可通过 vSphere Client 和 vSphere Web Client 访问 vSphere 数据中心。利用 vSphere SDK 开发灵活、简洁并具有友好界面的

VMware vSphere 客户应用程序。

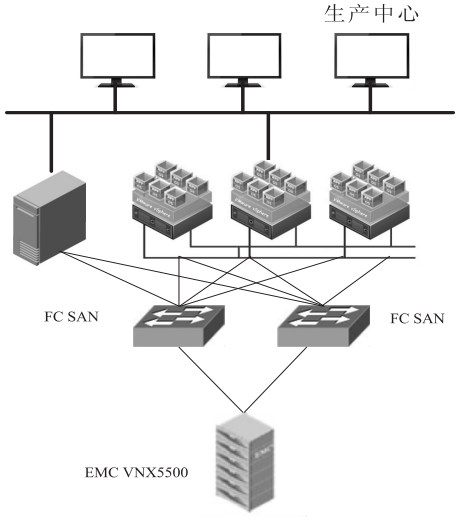
## 3 vSphere 私有云平台设计

### 3.1 存在问题与需求分析

随着高校信息化建设的不断深入,IT 系统的规模越发庞大,传统的校园网数据中心采用“一套应用一套系统”的 IT 资源配置模式,已经不能适应当前高校信息化建设需求。为了提高资源利用率,降低管理难度和系统维护风险,减少机房基础设施的投入,提高应用和系统部署的效率,转向虚拟化技术,提出以业务为中心“IT 即服务”私有云构建模式,对原有系统采用 P2V 迁移[7-8]。该私有云平台的构建,采用共享存储架构 FC SAN,实现了 CPU、内存与存储设备的分离,并利用 ESXi 组件对 IT 基础资源进行整合,构建虚拟化基础架构平台,同时使用 vShield(vCloud networking and security,vCNS)组件对虚拟机平台进行安全防护。在虚拟化基础架构平台上,利用 vCloud Director 组件,对虚拟化计算、存储、网络连接和安全性的虚拟数据中心实现安全配置,构建一种 vSphere 私有云,提供弹性计算的基础设施服务,从而达到新一代高校数据中心建设需求:高可用性基础架构,低成本,高 IT 资源利用率,管理和维护复杂度低,灵活、敏捷的 IT 服务交付。

### 3.2 总体架构

针对原有校园网中心机房设施以及新一代高校数据中心建设需求分析,目前该校的虚拟化平台物理架构由 8 台高性能 IBM 3650M4 服务器、FC SAN 存储系统(1 台 EMC VNX5500 存储和 2 台 FC 交换机 EMCDS300)组成。通过 vSphere 集群将所有 ESXi 主机整合起来,形成一个大的资源池,通过 vCenter Server 提供统一管理服务,配置 vShield 实现对虚拟数据中心的安全防护,并利用 vCloud Director 组件构建 vSphere 私有云。虚拟化平台的物理架构如图 2 所示。




**万方数据**虚拟化平台的物理架构

## 4 vSphere 私有云平台架构实施

### 4.1 IT 基础架构实施

(1)安装 ESXi 主机。

在每台物理服务器上安装虚拟化层 ESXi 操作系统,用于将服务器硬件资源进行抽象化处理,并允许多个虚拟机共享这些资源。相对于传统的 OS,ESXi 有更加严格的硬件限制,不是所有的存储控制器和网卡都支持,需要通过查询硬件兼容性列表 HCL。因为共享存储架构采用的是 FC SAN,需要每台服务器配置相应的万兆以太网卡和 HBA 卡,通过查找 HCL 列表,购买相应的万兆以太网卡和 HBA 卡。ESXi 系统安装完成后,配置需要服务器名和 IP 地址。文中的 8 台服务器名称为 ESXi01 ~ ESXi08,IP 地址为 192.168.168.2/26 ~ 192.168.168.9/25。

(2)配置 AD 域控制器。

安装活动目录 Active Directory 组件,并将此服务器提升为域控制器,添加 DNS 服务功能,并设置 DNS 转发器到当地 DNS 服务器上。DNS 服务器用集群中主机名。文中规划的 AD 域控制器 IP 地址为:192.168.168.14/25。

(3)部署 vCenter Server。

使用 vSphere Client 客户端连接到 ESXi01 服务器,在此服务器上安装 SUSE Linux 版的 vCenter Server Application。通过选择“File”(文件)→“Deploy OVF Template”(部署 OVF 模板),设备导入到虚拟基础架构的 ESXi 主机中。vCenter Server Application 部署完成后,可以通过控制台配置网络和时区。文中规划的 vCenter Server 的 IP 地址为:192.168.168.10/25。打开 Web 浏览器并键入:https://192.168.168.10:5480,登录后选择嵌入式数据库。单击“Start vCenter”(启动 vCenter),单击“Services”(服务)选项卡,启动停止相关服务等操作。vCenter 统一管理托管的 ESXi 主机。

(4)配置和管理虚拟网络。

虚拟网络为虚拟交换机的主机和虚拟机提供网络连接。虚拟交换机支持 VMkernel 端口(用于 IP 存储或 vMotion 迁移以及 ESXi 管理网络),一个或多个虚拟端口组。配置管理网络和 vMotion 网络,为了兼容不同 CPU 类型,需要在 vSphere Cluster 配置过程中开启 EVC 模式,并配置专用网络,在标准交换机 vSwitch0 中,启用 vMotion 和管理流量,迁移虚拟机。根据业务需求,添加标准交换机,通过端口组特性指定 VLAN ID 提供 VLAN 支持。新建分布式交换机,使得数据中心范围内的网络聚合起来集中进行网络资源调配、管理和监控。例如创建 vlan 201 的交换机支持 toInternet,配置上绑定 ESXi 主机业务网络物理网卡

NIC,NIC 网卡与上层核心交换机端口之间可以做成 Trunk 端口。

(5)配置 EMC 存储,并创建 VMFS 数据存储[9-11]。

文中采用 FC SAN 存储架构,包括一台 EMC VNX5500 存储系统,两台 FC 智能交换机。由于 EMC 存储系统价格较高,为了方便存储扩展,方案中的 FC 交换机支持 FC 端口和 IP 端口,方便将价格相对低廉的 IP SAN 存储网络接入网络存储系统中。配置 EMC 存储,输入 IP:https://1.1.1.1,进入 EMC VNX5500 配置界面,创建存储池,LUN 划分,注册主机,创建存储组并映射。在 vSphere Client 创建 VMFS 数据存储步骤如下:在 vCenter 的"Inventory"清单中,选择"Host and Clusters"视图,在"Configuration"面板中单击"Storage"链接,将显示现有数据存储,单击"Datastores"按钮,然后选择"Add Storage"链接,选择一个 LUN 来创建 VMFS5 数据存储。

(6)创建高可用性主机和群集。

vSphere Client 客户端登录 vCenter Server,在"Hosts and Clusters"(主机和群集)清单视图中,添加虚拟数据中心 vDC,在 vDC 下添加 8 台 ESXi 主机,打开 HA 和 DRS 功能。vSphere 的 vMotion、Storage vMotion、HA 和 DRS 功能支持群集的高可用性。vMotion 允许运行中的 VM 在相同 LUN 上的 ESXi 主机之间进行迁移,而 Storage vMotion 则允许运行在同一个 ESXi 主机上的 VM 从一个存储 LUN 转移到另一个存储 LUN 中。HA[12](high availability),则允许 vSphere HA 群集中打开 vSphere HA,当某台 ESXi 主机发生故障时,HA 会在其他主机上重启受影响的 VM;当 VM 停止发送心跳信号或 VM 进程崩溃时,HA 会重置 VM。

### 4.2　虚拟化平台安全

虚拟化平台安全包括网络安全、虚拟机安全、访问控制安全[13]。①网络安全。在 vSwitch(虚拟交换机)上进行 VLAN 配置,隔离不同网段,由于主机和网络之间的物理边界消失或模糊,无法通过硬件网关设备来提供服务,通过搭建 vShield 虚拟防火墙的保护端到端,边界到端点的数据安全(vShield 部署过程如下:通过 vSphere Client 端,通过 OVF 模板部署,导入 vShield-Manager-5.5.4 版本。vShield 虚拟机的 IP 规划为:192.168.168.39/25。通过浏览器配置 vCenter、DNS 和 NTP。并在每台 ESXi 主机上,安装 vShield App(防火墙),保护内部网络中 VM 之间通信,保护集群中的 VM。vShield Edge 组件可提供网络边缘安全和网关服务,用于隔离端口组、vDS 端口组。vShield Edge 同时通过提供 DHCP、VPN、NAT 和负载平衡并隔离末端网络连接到共享上行链路)。②虚拟机安全。vSphere 提供了一种虚拟机快照保存备份模式,可以依一次性实现服务器的灾难恢复,最大程度地保护虚拟机安全。③访问控制安全。vSphere 提供基于 RBAC[14]访问控制方式。管理员登录 vCenter 后,可以添加角色,并为角色添加特权。同时可以创建用户,并将该角色赋予这个用户。

### 4.3　私有云平台实施与监控

在虚拟化基础架构之上,通过 vCloud Directory 组件构建多租户云的私有云平台,实现弹性计算的基础设施服务。vCloud Directory 安装也是通过导入 OVF 模板的方式实现的。vCloud Directory 配置之前需要确保 vShield 和 vCloud Directory 都正常安装,安装步骤如下:创建提供者虚拟数据中心 vDC;创建虚拟分布式交换机 vDS,创建一个外部网络,配置外部网络;创建地址池;新建组织,并使用 LDAP 添加组织的用户,设置 vApp 租约策略;向组织分配资源,创建组织 vDC;创建目录(存储 vApp 模板文件和媒体文件)、配置存储、添加组织 vDC 网络,创建和使用 vApp,通过组织 URL,使用组织的用户账号登录,使用 vApp 模板创建 vApp 或者使用媒体文件创建 vApp(使用组织下配置存储和网络池),完成组织下的 VM 的创建。最后,在数据中心的 Network Virtualization 视图中,添加 vShield Edge(路由器),然后添加 Edge Interface(比如 toInternet 和 toIntranet),完成之后创建一个 Edge 的虚拟机,配置静态路由和 SNAT 规则,实现 Intranet 访问 Internet。完成上述实施步骤,就可以构建基于 vCloud 私有云,提供弹性计算的基础设施服务。

基于 vSphere 私有云平台部署完成后,为了保证原有业务系统的连续性,采用在原有物理主机上安装 VMware Converter 组件实现 P2V 物理机在线迁移[15]。通过性能监控 vCops(vCenter operations manager)组件,提供虚拟化环境(IT 基础架构中各 ESXi 主机、VM、存储和网络)的运行状况、容量和性能的可视化界面。经过一段时间的运行测试,达到以下效果:整合现有 IT 基础资源,实现资源统一管理;提高资源利用率、降低采购成本;提高平台数据安全性;降低总体拥有成本(TCO)、提高投资回报率(ROI)。

### 4.4　运维成本分析

此次 vSphere 应用部署中,配置了 8 台高性能 IBM 3650M4 服务器,电源总功率约为 750 W;IBM 3650M4 主机各自运行在校园网 DMZ 区,使用 vSphere 套件,在硬件服务器上安装 ESXi Server 平台,将原有系统迁移至虚拟机平台上。首先,从服务器耗电的角度,假设所有的服务器都是 24 小时不宕机运行,以每台服务器每小时耗电约 750 W,以每度电费

0.538 元计算,50 台电源的服务器每年所需电费约为:50×750×24×365×0.538÷1 000 = 176 733 元;虚拟化平台采用 8 台 ESXi 主机,其上运行 50 台虚拟机 VM,每年电费约为:8×750×24×365×0.538÷1 000 = 28 277.2 元。从空调制冷角度,数据中心电力消耗被转换为热能,制冷系统处理 1 W 的热量需要消耗电能约 0.8 W。虚拟化平台前 50 台服务器一年的制冷电力消耗电费为:176 733 元×0.8 = 141 386.4 元;虚拟化平台后 8 台 ESXi 主机一年制冷电力消耗电费为:28 277.2×0.8 = 22 621.76。Forrester 在《vCenter Operations TEI 研究》中认为,部署了 vSphere 私有云基础解决方案,可以使得 IT 成本资源使用量下降 30%,IT 工作效率上升 69%。

综上所述,通过 vSphere 私有云基础解决方案对数据中心服务器集群进行整合,大大减少了服务器数量,降低了数据中心能耗,节约了投资成本,减轻了管理难度。

## 5 结束语

提出一种高可用性的私有云基础架构解决方案,有效地解决了传统高校数据中心建设中存在的问题,该方案具有投资少、易于维护、安全可靠、业务的稳定性与连续性较好等特点。该方案从计算池、网络池、存储池、安全优化池的角度,提出了一套基于私有云数据中心的解决方案;采用共享存储架构 FC SAN,并通过 vSphere 集群[16]将所有 ESXi 主机进行整合,形成资源池,通过 vCenter Server 提供统一管理服务,配置 vShield 实现对虚拟数据中心的安全防护,并利用 vCloud Director 组件,从而实现了 vSphere 私有云。实践证明,该模式构建的高校数据中心,优化了 IT 基础架构服务模式,提升了高校信息化建设水平,构建了低碳、节能、减排、绿色的高校数据中心机房,增强了信息化系统的高可用性和安全性,也为其他高校同类建设项目提供了一个有意义的参考。

**参考文献:**


[1] 张 怡,孙志刚. 面向可信网络研究的虚拟化技术[J]. 计算机学报,2009,32(3):417-423.

[2] 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. [s. l. ]: ACM,2016:195-206.

[3] 辛 军,陈 康,郑纬民. 虚拟化的集群资源管理技术研究[J]. 计算科学与探索,2010,4(4):324-329.

[4] 陈煜嘉,郑斌斌. VMware vSphere 虚拟基础架构在 IDC 的应用[J]. 浙江树人大学学报,2011,11(1):1-6.

[5] PIAO A,YAN J. A networkaware virtual machine placement and migration approach in cloud computing[C]//Proceedings of the ninth international conference on grid and cloud computing. Nanjing,China:IEEE,2010:87-92.

[6] 钱琼芬,李春林,张小庆,等. 云数据中心虚拟资源管理研究综述[J]. 计算机应用研究,2012,29(7):2411-2415.

[7] 黄昊晶,崔志明. 一种以 vSphere 为核心的私有云基础架构设计方案[J]. 微电子学与计算机,2011,28(4):38-41.

[8] JANG J W,SEO E,JO H,et al. A low-overhead networking mechanism for virtualized high-performance computing systems[J]. Journal of Supercomputing,2012,59(1):443-468.

[9] 陆一飞,张震伟,陶 军,等. 基于控制中心的新型 SAN 架构的设计与实现[J]. 计算机研究与发展,2016,53(6):1292-1305.

[10] FUJIWARA I,AIDA K,ONO I. Applying double-sided combinational auctions to resource allocation in cloud computing[C]//2010 10th IEEE/IPSJ international symposium on applications and the internet. Seoul:IEEE,2010:7-14.

[11] 刘朝斌,谢长生,张 琨. 存储网络虚拟化关键技术的研究与实现[J]. 计算机科学,2004,31(5):38-40.

[12] 温少君,陈俊杰,郭 涛. 一种云平台中优化的虚拟机部署机制[J]. 计算机工程,2012,38(11):17-19.

[13] 赵晓东,曾庆凯. 基于系统虚拟化的安全技术研究[J]. 计算机工程与设计,2013,34(1):18-22.

[14] BERTINO E,BONATTI P A,FERRARI E. TRBAC:a temporal role-based access control model[J]. ACM Transactions on Information & System Security,2011,4(3):191-233.

[15] 江 雪,李小勇,等. 虚拟机动态迁移的研究[J]. 计算机应用,2008,28(9):2357-2377.

[16] FOSTER I,FREEMAN T,KEAHEY K,et al. Virtual clusters for grid communities[C]//Sixth IEEE international symposium on cluster computing and the grid. Singapore:IEEE,2006:513-520.