

基于 KVM 的虚拟化研究及应用

崔泽永¹, 赵会群²

(1. 北方工业大学 经济管理实验中心, 北京 100144;

2. 北方工业大学 信息工程学院, 北京 100144)

摘要:文中解释了基于硬件虚拟化技术解决方案 Kernel-based Virtual Machine(KVM)的系统架构,分析了 KVM 的虚拟化拓扑结构灵活、硬件配置方案简单以及数据统一集中管理,如针对实践教学数据中心教学应用数量庞大、环境复杂,尤其使用加密狗作为加密手段的应用较多的特点,详细给出通过 KVM 解决上述问题的虚拟化设计方案,并通过一个案例具体说明了虚拟化部署过程中的重点及注意事项。该方案不但能满足教学正常进行的需求,成本低廉,而且能提高服务器的稳定性和利用率,降低数据中心的维护成本和复杂度。

关键词:虚拟化;KVM;桥接;USB 加密狗

中图分类号:TP391.9

文献标识码:A

文章编号:1673-629X(2011)06-0108-04

Research and Application of Virtualization Based on KVM

CUI Ze-yong¹, ZHAO Hui-qun²

(1. Experimental Centre of Economics & Management, North China University of Technology, Beijing 100144, China;

2. College of Information Engineering, North China University of Technology, Beijing 100144, China)

Abstract: Explain the system architecture of the Kernel-based Virtual Machine (KVM), which is a hardware-based virtualization solution. Indicate that flexible of the topology structure, convenient hardware configuration and data central management are main features and advantages of the KVM. In connection with the real situation, the author mentions that data center of the experimental center are applying a large numbers of teaching applications, existing in complex environment and using USB Dongles as encryption. Consequently, problems such as inefficient of servers and USB Dongle conflictions are obstructing the teaching order and development of the experimental center. Therefore, present a solution to solve these problems through the KVM virtualization design and specify the focus and precautions in virtualization deployment process through a case. The program not only meets the needs of normal teaching, low cost, but also improves the stability and efficiency of servers, reduces data center maintenance costs and complexity.

Key words: virtualization; KVM; network bridge; USB soft dog

0 引言

虚拟化技术是 IBM 在 20 世纪 70 年代首先应用在 IBM/370 大型机上,这项技术极大地提高了大型机资源利用率。随着软硬件技术的迅速发展,这项属于大型机及专利的技术开始在普通 X86 计算机上应用并成为当前计算机发展和研究的一个热点方向。目前,虚拟化技术在高校数据中心虚拟化^[1,2]、计算机教学^[3-5]、数字图书馆^[6,7]等各方面都有所应用并取得了较好的效果。文中提出基于 KVM 的教学平台虚拟化方案设计,较好地解决了使用加密狗作为加密手段的应用虚拟化问题。

1 KVM 虚拟化技术概述

虚拟化技术能够在一台计算机上运行多个操作系统,每个系统上运行自己独立的应用软件^[8]。虚拟化技术可以对这些系统进行有效隔离,对资源进行按需分配,从而保证每个系统的安全性和性能^[9]。目前虚拟化技术已经形成从硬件到软件一整套的解决方案。基于 X86 架构的硬件技术主要是由 Intel 和 AMD 提供的 Virtualization Technology (VT) 和 Pacifica (AMD-V) 虚拟化技术,该技术对处理器进行了扩展,从而实现了处理器的虚拟化^[10,11]。软件方面主要有 VMware 公司的 VSpere 和 VMware Workstation、Microsoft 公司的 Hyper-V 和 Virtual PC 以及 Linux 系统下的 Xen 和 KVM 等。前两个软件是已经商业化的系统,Xen 也开始了商业化运作,KVM 是免费的开源系统并在迅速发展当中,是目前唯一进入 Linux 核心的虚拟化解决方案。

KVM 是由以色列的一个名为 Qumrant 的开源组

收稿日期:2010-10-28;修回日期:2011-01-27

基金项目:北京市自然科学基金(4062012)

作者简介:崔泽永(1977-),男,河北安国人,实验师,研究方向为系统信息化和系统建模;赵会群,博士,教授,研究方向为可信网络和可信软件。

织于 2006 年 10 月提出的基于硬件虚拟化的虚拟机 (Virtual Machine, VM) 实现方案, 2007 年 2 月发布的 Linux 2.6.20 内核第一次包含了 KVM。实际上 KVM 只是虚拟化解决方案的一部分, 其底层需要处理器支持, 为多个操作系统提供虚拟化处理器, I/O 通过 QEMU 进行, 其架构如图 1 所示。

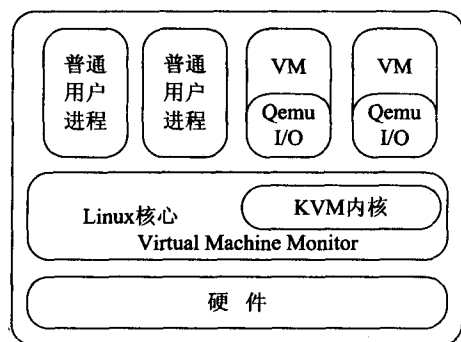


图 1 KVM 系统架构

KVM 包含内核模块和处理器模块两部分, 内核模块 `kvm.ko` 提供核心的虚拟化支持, 处理器模块 `kvm-intel.ko` 和 `kvm-amd.ko` 分别提供了对 Intel 和 AMD 处理器虚拟化技术的支持。KVM 通过加载 `kvm.ko` 内核模块将 Linux 内核转换为一个 Virtual Machine Monitor (VMM, Hypervisor), 因此 KVM 可以随着 Linux 标准内核的升级而获得性能提升 (如调度程序、内存支持等)^[12]。虚拟机对应成为标准的 Linux 进程, 因而可以用标准的 Linux 进程管理机制进行管理。

在普通的 Linux 进程有内核模式和用户模式两种运行模式, 内核模式表示代码执行的特权模式, 用户模式表示代码执行的非特权模式。在 KVM 系统中为 Linux 引入了一种新的进程模式, 新的模式称为客户模式, 客户模式用来执行虚拟机操作系统非 I/O 代码。在客户模式中包含内核模式和用户模式两种标准模式, VM 操作系统可在内核模式下运行标准的内核, 在用户模式下支持自己的内核和用户空间应用程序。

虚拟机操作系统的 I/O 操作是由修改过的 QEMU 支持的。QEMU 是一种用动态翻译技术实现的快速指令集层虚拟机, 它支持整个计算机系统的模拟, 包括多种处理器 (X86、ARM、PowerPC 等)、磁盘、图形适配器和网络设备等。KVM 是用硬件虚拟化技术代替了 QEMU 的动态翻译技术, 实现虚拟机操作系统代码直接由硬件处理从而提高系统性能。VM 操作系统生成的 I/O 请求会被截获并转发到用户空间, 由 QEMU 的设备模型来模拟 I/O 操作, 在需要的情况下触发真实的 I/O 操作。

2 KVM 教学平台虚拟化应用系统设计

随着经济模式的转变和信息技术的发展, 社会对

复合型人才的数量和质量要求越来越高。为了适应这种变化, 高等教育不断重视和加强实践教学, 利用现代计算技术贴近现实成为其中最重要的手段之一。国内大部分院校均已建立起一定规模的实践教学环境, 初步建立了教学、科研等各种网络应用系统。这些系统在实践教学秩序的稳定性和教学质量的提升等方面发挥了重要作用。

一般实践教学数据中心服务器拓扑结构如图 2 所示, 其中包括目录服务器、数据库服务器、文件服务器、WEB 服务器及专业教学软件应用服务器, 部分院校还部署了防火墙、负载均衡等扩展设备, 以保证服务器的安全性、高性能和高可靠性。

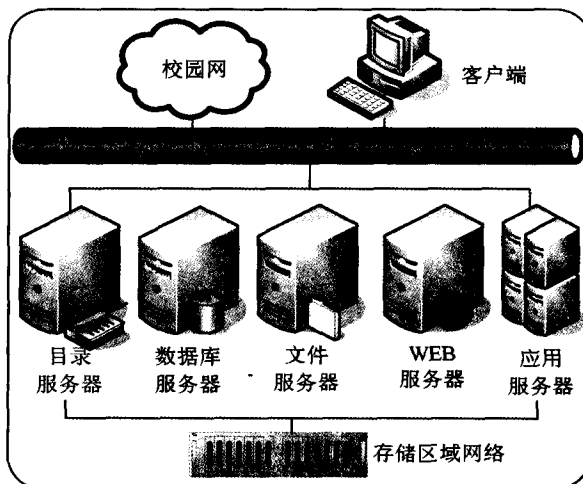


图 2 实践教学数据中心服务器拓扑结构

在实践教学快速发展过程中, 各院校的数据中心在建设和管理上也面临着许多困难和问题。①服务器数量越来越庞大, 经常是一个建设项目建立一套服务器系统, 在此情况下服务器利用率相当低; ②服务器资源争夺, 有时为了提高服务器利用率, 将不同系统部署在同一台服务器上, 造成不同应用系统之间的冲突, 比如加密狗之间的冲突、端口之间的争夺、环境资源冲突等。虚拟化技术的应用为解决这些问题提供了一条很好的思路。

2.1 KVM 技术在虚拟化中的优势

KVM 虚拟化技术具有较强的灵活性, 能较好地根据不同操作系统和特殊硬件设备加以利用, 降低不同系统间维护的复杂度。

KVM 支持 VM 操作系统种类多, 常见的基于 X86 架构的 Windows、Linux、Unix 操作系统绝大部分可以稳定运行。

KVM 本身运行在 Linux 系统内核当中, 属于瘦虚拟化方案, KVM 本身体积很小, 其支持硬件取决于 Linux 系统本身对硬件的支持。目前主流硬件设备均有对应的 Linux 驱动, 这也就决定了 KVM 可以在最广

泛的硬件系统之上运行。

KVM 可以直接使用指定的硬件设备,如 USB 端口等。利用此项功能,可以直接将特定应用 USB 加密狗与运行该应用的 VM 绑定,从而解决加密狗冲突的问题。

同时 KVM 具有优良的系统性能和稳定性,系统更新便捷。

2.2 虚拟化设计的原则

现有系统的分类整合,对目前应用系统按照技术架构进行分类,分析其应用特性,将类似的系统进行合并服务器处理,以利于将应用迁移到虚拟主机上。对将来要增加的应用系统进行预测,以保证系统的扩展性满足未来的需求。

数据集中存储,将虚拟机文件及数据库集中存储到存储设备中,实现数据的集中统一管理。

2.3 服务器虚拟化方案设计

根据现有应用系统的性质将其分为两大类,一类为教学服务器,专门运行教学相关的专业软件。另一类为环境支持系统,包括域服务器、网站服务器、文件服务器。教学服务器平时压力并不大,但是当展开教学活动时,服务器负载会迅速提高。鉴于教学系统的特点,将教学系统服务器作为首先进行虚拟化的部分,系统结构如图 3 所示。

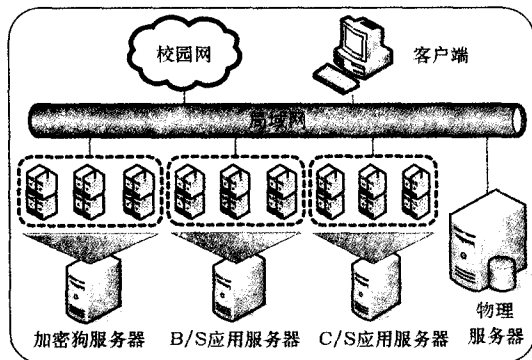


图 3 应用服务器虚拟化架构

将教学系统服务器按资源利用率分为两部分,利用率超过 20% 的系统将单独设置虚拟机,利用率在 20% 以下的按照提供服务种类组合在不同虚拟机中。按服务性质将服务分为纯加密保护验证类、B/S 应用服务类、C/S 应用服务类、自有专用服务类等四类。

在教学系统中大量应用使用 USB 加密狗进行版权保护,为避免加密狗之间相互冲突,将加密狗对应 USB 端口直接指向对应的虚拟机,使之成为私有端口,不被主机系统和其它虚拟机系统所识别和使用,从而达到消除冲突的目的。

依据数据集中存储的原则,采用 SAN(存储区域网络)集中存储方式,将虚拟机镜像文件部署在 SAN

共享存储阵列中。当物理主机发生故障时,可通过集群转移或者指定其他物理主机重新运行虚拟机,缩短应用中断时间。

通过分析应用系统的运行原理,建立分布式数据库,使其与应用分离,数据库集中存储在数据库服务器上。应用采用虚拟机多机备份机制,保证在应用的安全性。对于部分数据库和应用不能分离的业务,采用多级备份的方式,以降低风险发生时造成的损失。

3 KVM 虚拟化应用系统部署

采用 Ubuntu910 系统,基于 KVM84 对服务器进行虚拟化,设置 CPU、内存、硬盘、网络等硬件环境,安装操作系统及应用,加载相应 USB 加密狗,实现从虚拟化平台到软件应用的完整虚拟化解方案。

3.1 环境检查及软件配置

KVM 是基于 CPU 硬件虚拟化基础之上的,在安装 KVM 之前必须确认 CPU 支持虚拟化技术。使用 `cat /proc/cpuinfo | grep -E '(vmx|svm)'` 命令进行检测,有输出结果说明 CPU 支持虚拟化。部分服务器默认是关闭虚拟化技术的,需要进入 BIOS 打开 CPU 的虚拟化支持。

Linux 内核是从 2.6.20 版本开始集成 KVM,因此 Linux 内核版本必须在此之上。使用 `uname-a` 命令查看 Linux 内核版本。

在 Ubuntu 下安装 KVM 模块和安装其他软件类似,使用 `apt-get install kvm` 安装 KVM 模块并添加到 Linux 核心。`lsmod` 命令可查看 KVM 模块是否加载成功,如果未加载成功可以使用命令 `modprobe kvm` 载入。

3.2 VM 操作系统实例化

3.2.1 建立虚拟磁盘镜像

虚拟磁盘镜像在逻辑上是提供给虚拟机使用的硬盘,在物理上可以是 Linux 系统内一普通镜像文件,也可以是真实的物理磁盘或分区。本方案设计中将虚拟机集中存储在 SAN 存储阵列中,采用文件方式,用 `dd` 命令创建如下

```
dd if=/dev/zero of=hdisk.img bs=1G count=10
```

`dd` 命令创建一个名为 `hdisk.img` 的容量为 10G 的虚拟磁盘。虚拟磁盘并不会立即分配全部空间,而是根据使用情况在不超过 10G 范围内动态分配。

3.2.2 配置虚拟网络

KVM 有 NAT 和 TUN/TAP 两种网络接入方式。NAT 方式下主机操作系统和虚拟机操作系统不需要进行特殊设置,虚拟机操作系统内网卡采用内部 DHCP 方式获取私有 IP 地址,可以与外部网络通讯,但是虚拟机不能向外提供服务,也不能与主机进行通信。

TUN/TAP 方式是采用网桥连接,虚拟机与主机、虚拟机与外部网络通讯都正常,其拓扑结构如图 4 所示。

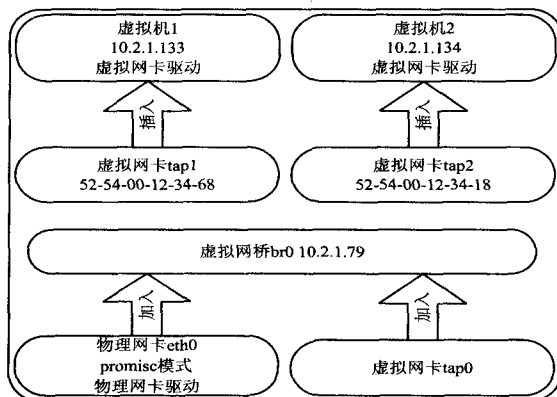


图 4 KVM 网络桥接模式拓扑图

TUN/TAP 模式是将物理网卡 eth0 设置成混杂模式,建立一个虚拟网桥 br0 和虚拟网卡 tap0,然后将虚拟网卡 tap0 和物理网卡 eth0 加入网桥,设置成网桥端口并激活虚拟网卡 tap0。网桥 IP 设置成原主机 IP 地址,这时主机操作系统可正常通讯。当虚拟机操作系统启动时将自动以 tap0 为模板建立所需数量的虚拟网卡并插入系统,VM 操作系统启动后可按正常系统 DHCP 方式或手工指定方式设置网卡 IP 地址。

3.2.3 部署操作系统

KVM 虚拟机硬件配置的设定或更改非常灵活,KVM 通过虚拟机启动命令参数指定虚拟机所对应的 CPU、内存、硬盘、网卡、声卡、系统时钟等硬件配置。使用启动命令将虚拟磁盘文件和虚拟机关联起来,启动后开始安装操作系统。

```
kvm-m 512-hda /home/kvm/hdisk.img-cdrom /dev/cdrom-boot d -localtime
```

此命令是设置虚拟机使用磁盘镜像文件/home/kvm/hdisk.img 作为硬盘,设置内存容量为 512 兆,从光驱启动虚拟机安装操作系统,安装界面出现后和在物理机器上正常安装操作系统一致。

安装完将启动命令中的 -boot d 参数修改为 -boot c 即可实现从磁盘镜像正常启动虚拟机。

3.3 虚拟机的优化和统一集中管理

Virtio 是一套 Linux 下用于虚拟 I/O 的通用框架^[13],采用半虚拟化技术以提高 I/O 性能,通过在 VM 内加载 virtio 驱动以支持网卡、块存取设备、PCI 等设备。启用 virtio 虚拟千兆网卡替换 KVM 默认的 Realtek RTL8029 虚拟网卡,可大幅度提高虚拟网卡的性能和稳定性。如选用 virtio 网卡并指定网卡物理地址,可使用 -net nic, model=virtio, mac=52:54:00:12:34:68 参数。虚拟机启动后安装对应的网卡驱动即可正常使用。虚拟机系统调试完毕后可将复杂的启动命令存为脚本,避免出错并提高管理效率。

KVM 虚拟机是针对服务器虚拟化进行设计和开发的虚拟化方案,因此 KVM 虚拟机对虚拟显卡支持相对较弱。但是 KVM 提供了不在物理服务器端启动虚拟机图形界面,而是通过 VNC 远程访问的方式对虚拟机进行管理的工作机制。如使用远程管理启动虚拟机,可使用 -vnc 172.16.32.3:3 参数启动 VNC 服务器,VNC 客户端通过访问 172.16.32.3:5093 地址对虚拟机进行远程管理控制,为不同虚拟机指定不同端口,形成统一的集中管理。

3.4 部署 USB 加密设备

在部署应用过程中,加密狗冲突问题可以利用 KVM 硬件端口指定技术将不同 USB 设备与特定虚拟机绑定,主机操作系统不需要安装相应 USB 驱动,由此可解决 USB 加密狗在同一系统下冲突的问题。

KVM 可使用 -usbdevice host *. * 参数将所有主机上的 USB 设备全部指定转接到虚拟机上,此时主机将无法正常使用 USB 设备。因此,必须向 KVM 说明哪些 USB 设备由客户机控制。这里需要使用到的是 USB 设备的 vid 和 pid 两个参数,每个 usb 设备都有这两个 id,vid 代表生产商,pid 代表产品。可以通过 lsusb 命令来察看 USB 设备的这两个参数,其中一条结果如下

```
Bus 001 Device 007: ID 0a5c:2110 Broadcom Corp
```

在启动命令里边修改 -usbdevice 选项,增加该 USB 设备 -usbdevice host:0a5c:2110,操作系统启动后再加载相应 USB 加密狗驱动即可正常使用。

3.5 虚拟化应用效果分析

目前实验中心实际运行的教学专用应用中符合虚拟化条件的为 37 个,分布在 13 台服务器上,通过虚拟化部署共建立虚拟机 12 个,分布在 4 台服务器上,有效提高了服务器的资源利用率。其它服务器中 3 台服役时间已超过 6 年,实施虚拟化后随着服务器的压力减小,故障率明显降低,故障修复周期也大幅缩短,保障了教学秩序的稳定。

KVM 虚拟机只依赖于虚拟磁盘镜像文件,其他配置在 Linux 系统中完成。因此只需要复制磁盘镜像文件,修改对应启动命令即可完成一台新服务器的部署,有效缩短部署新服务器的工作周期,极大地降低部署复杂程度,提高工作效率。服务器数据备份是管理员日常工作的一个重要组成部分,实施虚拟化后只需备份虚拟磁盘文件,恢复时将虚拟磁盘文件复制回来即可实现应用和数据的完整恢复。

4 结束语

KVM 是一个发展时间比较短,但是性能和稳定性

(下转第 115 页)

4 结束语

对于句子的划分和成分的提取,文中使用的是计算所汉语词法分析系统 ICTCLAS,使用 ICTCLAS 系统可以直接实现对于一个或一段中文文本的词性的划分和提取。

文中在粗糙集理论属性约简的基础上初步研究了中文主客观文本判别的问题。文中,初步判断句子只有主客观之分,没有那种介于主观和客观之间的模糊或是粗糙的概念。粗糙集理论运用于文本,根本作用是用于约简,减少系统的时间代价。通过观察大量的主客观语句,提取出主观语句的结构特征,根据设定的阈值,选取几率较大的模式,最后用粗糙集约简模式,达到在确保查准率的前提下,提高系统对主客观句子的判定效率的目的。实验表明,基于粗糙集的中文文本主客观性研究无论是在查准率还是在时间代价上,都有了很大的改善。对于那些同存在于主观和客观句中的模型,无论是保留还是约简,都会影响系统在执行时判断主观或是客观的查全率和查准率,后期将继续研究怎么处理这些模型。

参考文献:

- [1] 苗夺谦,李道国.粗糙集理论、算法与应用[M].北京:清华大学出版社,2008.
- [2] 叶强,张紫琼,罗振雄.面向互联网评论情感分析的中文

主观性自动判别方法的研究[J].信息系统学报,2007,1(1):79-91.

- [3] Aas K, Eikvil L. Text categorization: a survey [M]. Norwegian: Norwegian Computer Center, 1999.
- [4] Lahtinen T. Automatic indexing: an approach using an index term corpus and combining linguistic and statistical methods: [D]. Finland: University of Helsinki, 2000.
- [5] Hochsztain E. A granular approach for analyzing the degree of affability of website [C] // Lecture Notes in Computer Science. [s. l.]: [s. n.], 2002: 479-485.
- [6] 张雪英.基于粗糙集理论的文本自动分类研究[D].南京:南京理工大学,2005.
- [7] 樊娜,蔡皖东,赵煜.基于最大熵模型的观点句主观关系提取[J].计算机工程,2010,36(2):4-6.
- [8] 杨彩梅.关系化——一种识别句子主观性语言实现的形式手段[J].现代外语,2007,30(1):1-10.
- [9] Yang Ying, Liu Xin. A reexamination of text categorization methods [C] // Proceedings of ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR99). Berkeley, Cal.: [s. n.], 1999.
- [10] 姚天防,娄德成.汉语语句主题语义倾向分析方法的研究[J].中文信息学报,2007,21(5):73-79.
- [11] 李钝,曹付元,曹元大,等.基于短语模式的文本情感分类研究[J].计算机科学,2008,35(4):132-134.
- [12] 吴月萍,陈玉泉.基于Web的概念属性抽取的研究[J].中国管理信息化,2009,12(10):98-101.

(上接第111页)

表现优秀的虚拟化解决方案。文中通过一个实例介绍了KVM在虚拟化过程中的具体应用,其灵活的网络拓扑结构、简便的硬件配置方案、集中统一管理可满足于大多数数据中心虚拟化实践。当然KVM也有很多不足,对一些虚拟化扩展特性,如泛虚拟化支持、虚拟机动态迁移、图形化管理界面等新功能正在进一步研究和开发当中。

参考文献:

- [1] 何禹,胡宇鸿,王一波.虚拟化技术在校园网数据中心的应用[J].电子科技大学学报,2007,16(12):1461-1464.
- [2] 周俐军,林泽东,刘伟科.基于VMware的高校数据中心虚拟化管理探究[J].中国管理信息化,2009,12(16):65-66.
- [3] 李馥娟.虚拟机技术在复杂网络实验中的应用[J].实验技术与管理,2009,26(12):79-83.
- [4] 王建军.VMware虚拟机技术在计算机机房管理中的应用[J].科技信息,2009(1):96-97.
- [5] 徐红,刘羽.计算机专业虚拟实验教学环境的改革与

实践[J].实验技术与管理,2009,26(2):90-92.

- [6] 董秋生,黄文,马骏涛,等.服务器虚拟化技术在数字图书馆服务器整合中的应用[J].情报理论与实践,2009,32(1):119-122.
- [7] 刘荣发.服务器虚拟化技术在图书馆数字化服务中的应用[J].现代图书情报技术,2007(4):79-83.
- [8] 刘爱军,耿国华.基于x86的虚拟机技术现状、应用及展望[J].计算机技术与发展,2007,17(11):250-253.
- [9] 董耀祖,周正伟.基于X86架构的系统虚拟机技术与应用[J].计算机工程,2006,32:71-73.
- [10] 陈文智,姚远,杨建华,等.Pcanel/V2——基于Intel VT-x的VMM架构[J].计算机学报,2009,32:1131-1139.
- [11] 顾晓峰,王健.基于Intel VT-x的XEN全虚拟化实现[J].计算机技术与发展,2009,19(9):242-245.
- [12] Kivity A, Kamay Y, Laor D, et al. Kvm: the Linux virtual machine monitor [C] // The 2007 Ottawa Linux Symposium. Ottawa, Ontario, Canada: Cisco Unwires Linux Symposium, 2007: 225-230.
- [13] Russell R. virtio: towards a de-facto standard for virtual I/O devices[J]. SIGOPS Oper. Syst. Rev., 2008, 42(5): 95-103.