doi: 10.3969/j.issn.1006-1576.2011.08.015

虚拟化主机技术在企业中的应用

孔思淇，潘泽友
（中国工程物理研究院计算机应用研究所，四川 绵阳 621900）

摘要：在分析虚拟化技术的发展历史和工作模式的基础上，针对企业级虚拟化主机的关键技术，介绍其实现原理、机制以及在云计算、桌面交付方面的应用，并分析虚拟化技术存在的不足。结果表明：虚拟化技术能为企业用户提供便捷、高效、安全和易管理的 IT 环境。

关键词：企业级虚拟化；云计算；桌面交付
中图分类号：TP391.98 **文献标志码**：A

Application of Virtualization-Host Technology in Enterprise

Kong Siqi, Pan Zeyou
(Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China)

Abstract: On the basis of analysis the development history and working mode of virtualization technology, aiming at the key technology of enterprise-level virtualization-host, introduce the realization principles, mechanisms and its application in cloud computing and desktop delivery, analysis the shortcoming of virtualization technology. The results show that virtualization can provide enterprise users with convenient, efficient, safe and manageable of the IT environment.

Keywords: enterprise-level virtualization; cloud computing; desktop delivery

0 引言

虚拟化（virtualization）是一个广义的术语，在计算机方面通常是指计算元件在虚拟的基础上而不是真实的基础上运行。抽象来说，虚拟化是资源的逻辑表示，不受物理限制的约束。具体来说，虚拟化技术的实现形式是在系统中加入一个虚拟化层，将下层的资源抽象成另一种形式的资源供上层使用[1]。

业界对虚拟化产生了很多种定义，侧重点各不相同，但都阐述了 3 层含义[2]：1) 虚拟化的对象是各种各样的资源；2) 经过虚拟化后的逻辑资源对用户隐藏了不必要的细节；3) 用户可以在虚拟环境中实现其在真实环境中的部分或者全部功能。因此，笔者对虚拟化主机技术在企业中的应用进行研究。

1 发展历史

1959 年，克里斯托弗在其于信息技术国际会议上发表的学术报告《Time Sharing in Large Fast Computers》中首次提出了虚拟化的概念。20 世纪 60 年代中期，IBM 的 Watson 研究中心为了验证“时间共享系统”的概念而开展了 M44/44X 工程，其架构基于虚拟机，定义了虚拟内存管理机制，可以在一台大型机上同时运行多个用户操作系统。此后直至 20 世纪 70 年代中期，IBM 提供了一系列应用了虚拟化技术的产品[3]，通过虚拟机监视器[1]技术在物理硬件上生成多个可以运行独立操作系统的虚拟机镜像。在 20 世纪 80 年代和 90 年代，随着 x86 架构的发展和 Windows 操作系统的广泛应用，主要用于大型机的虚拟化技术不再流行。但在 20 世纪 90 年代末期，x86 架构也显现出了利用率低、管理成本高和灾难防护不力等问题。1998 年，VMware 公司提出了针对 x86 平台的虚拟化技术，并加以实际演示。IBM 分别于 1999 年和 2002 年实现了“逻辑分区”和“动态逻辑分区”，允许在无需重启系统的情况下，将包括 CPU、内存的系统资源分配给独立的分区，使系统管理更加方便。2003 年，微软进入桌面虚拟化市场，至今不断提供操作系统层面的虚拟化产品。2006 年，Intel 和 AMD 陆续宣布从处理器层面支持虚拟化，至此，虚拟化又成为了 IT 行业的主流技术。

2 虚拟化的工作模式

虚拟化技术将物理资源进行逻辑表示以供给用户使用，在转换的过程中需要根据用户的需求，通过一些模式和方法将资源虚拟成符合要求的形态。在实现虚拟化时常常使用的模式和技术[4]如下。

2.1 单一资源的多个逻辑表示

这种模式是虚拟化最广泛使用的模式之一，它只包含一个物理资源，却向用户呈现出多个资源的

收稿日期：2011-04-23；修回日期：2011-05-16
作者简介：孔思淇（1986—），男，吉林人，硕士，从事网络应用技术研究。

形态，如图 1。

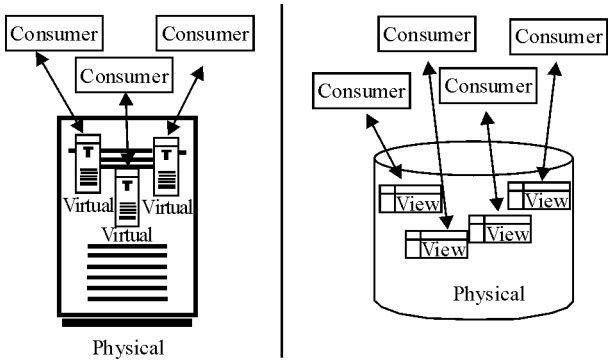

图 1　单一资源的多个逻辑表示[4]

2.2　多个资源的单一逻辑表示

这种模式将多类资源整合到一起，对外表示为提供单一接口的单个逻辑资源的形式。在利用多个简单功能来创建某种强大的系统时，这是一种非常有用的模式，存储虚拟化和集群技术就是这种模式的例子。多类资源都是通过一个接口呈现出来，用户只与一个系统进行交互，而实际上的计算则分布多个节点上，与网格比较类似，如图 2。

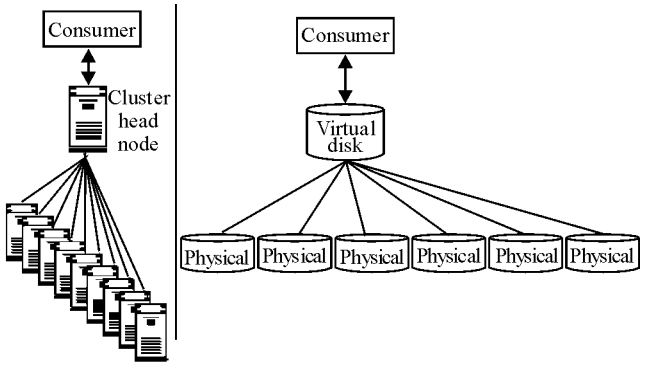

图 2　多个资源的单一逻辑表示[4]

2.3　在多个资源之间提供单一逻辑表示

这种模式可以将多个同类资源相融合，对外体现为单一逻辑资源的多副本形式。系统根据特定的条件来选择一个物理资源实现，例如资源利用率、延迟等。这种模式与上一种模式非常类似，但是它们之间的差别在于：这里每个物理资源都是一个完整的副本，彼此不依赖对方而存在；并且都可以提供逻辑表示所需要的所有功能。这种模式的一个例子是负载均衡。用户只需要提出事务请求，并不需要关心到底是哪一个资源副本在提供服务，如图 3。

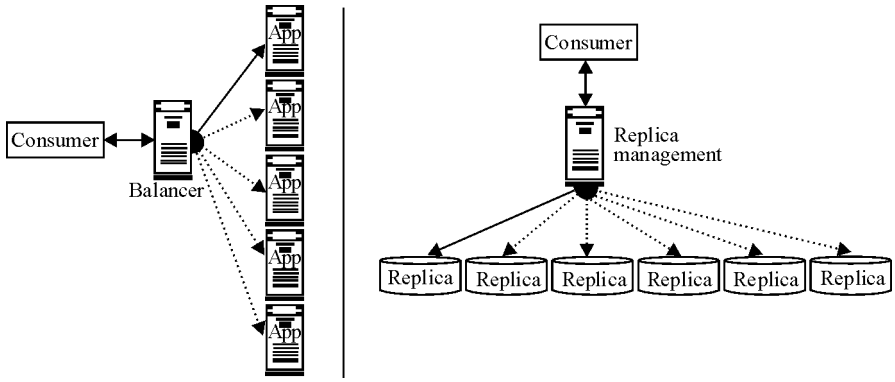

图 3　在多个资源之间提供单一逻辑表示[4]

2.4　单个资源的单一逻辑表示

这是用来表示单个资源的一种简单模式，将一种资源表示成另一种资源的形式。B/S模式就是一个常见的例子。创建一个前端来表示Web界面，它会映射到应用程序接口中，然后将后台服务器的内容通过可视化的方式呈递给用户，如图 4。

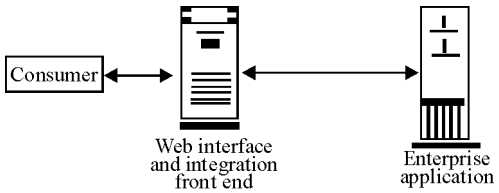

图 4　单个资源的单一逻辑表示[4]

虚拟化工作的基本模式是用物理资源来提供多种多样的逻辑资源集合，它们既可以独立执行为用户提供标准化、安全的接口，也可以组合执行以达到更好的效果。

3　企业级虚拟化主机技术

企业所需的 IT 环境必须安全、稳定、高可用性且方便管理。因此企业级虚拟化技术主要指系统方面的虚拟化，核心思想是使用虚拟化软件在一台物理机上虚拟出多台虚拟机；每台虚拟机分别运行在一个隔离环境中，均为具有完整硬件功能的逻辑计算机系统，且互相之间运行不同服务。这样既能提高资源利用率又能使各台虚拟机互不干扰地运行。

3.1　CPU虚拟化

CPU 虚拟化技术就是将物理 CPU 抽象成虚拟

CPU，且任意时刻一个物理 CPU 只能运行一个虚拟 CPU 的指令。这与多任务以及超线程技术完全不同[5]。CPU 虚拟化分为软件方案和硬件方案：软件方案中，关键资源的访问通过虚拟机监视器(virtual machine monitor，VMM)与底层硬件交互，因为虚拟机操作系统运行在非最高特权级，所以当其发出敏感指令[1]时会陷入到 VMM 中，VMM 会通过准确模拟物理处理器的行为，将其访问定位到 VMM 为其设计的与物理寄存器对应的“虚拟寄存器”上，进行软件模拟。当前纯软件的 CPU 虚拟化包括全虚拟化[6]和半虚拟化[7-8]。纯软件的 CPU 虚拟化虽然不要求对 x86 架构下的处理器本身进行改变，但是会增加系统的复杂性和性能开销。后来又提出了硬件辅助虚拟化技术，如 Intel VT[9]和 AMD-V[10]，支持虚拟化技术的 CPU 加入了特别优化过的指令集和处理器运行模式来控制虚拟过程，通过这些指令集，VMM 的性能得到了提升；而且硬件层面的虚拟化可以提供全新的操作系统运行模式，无需进行二进制转换[11]，也简化了 VMM 的设计。

3.2 存储虚拟化

存储虚拟化是对存储的物理设施和配置的逻辑抽象[3]。按照目前的主机结构来看，主要分为内存虚拟化和外存(硬盘)虚拟化。

3.2.1 内存虚拟化

内存虚拟化技术在大型机时代就已经被应用。由于当时计算机缺少运行程序或操作所需的随机存取内存(RAM)，于是操作系统使用虚拟内存(virtual memory)进行补偿。虚拟内存技术是指在磁盘存储空间中划分一部分作为内存的中转空间，负责存储内存中放不下且暂时不用的数据，当程序用到这些数据时，再将它们从磁盘换入到内存。虚拟内存技术屏蔽了程序所需内存空间的存储位置和访问方式等实现细节，向上提供透明服务，体现了虚拟化的核心理念，以一种透明的方式提供抽象了的底层资源。随着硬件技术的不断发展，在物理主机上运行多个虚拟机以提高硬件利用率成为了新的热点。内存虚拟化技术把物理机的真实物理内存统一管理，包装成多个虚拟的物理内存分别供虚拟机使用，使得每个虚拟机拥有各自独立的内存空间。不过由此带来了逻辑内存与物理内存互相转化的问题，二者的映射关系是由内存虚拟化管理单元来负责的，主要有影子页表法[12]和页表写入法[2] 2 种。影子页表法是指VMM为每个虚拟机维护着一个对应的页表，会随着客户操作系统页表的更新而更新。VMware 的产品均采用这种方法。页表写入法指的是当客户操作系统创建一个新页表时，需要向VMM注册该页表。客户操作系统对页表的每次修改都会陷入 VMM，由其来更新，保证其页表项记录的始终是真实的物理地址。Xen是采用该方法的典型代表。

3.2.2 外存虚拟化

随着信息业务的不断发展，网络存储系统已经成为企业数据中心的核心组件。存储网络平台性能的优劣，直接影响到企业业务的运行。因此，存储虚拟化技术(主要指硬盘方面)应运而生。独立冗余磁盘阵列(redundant array of independent disk，RAID)技术是外存虚拟化技术的雏形。它通过将多块物理磁盘以阵列方式组合起来，为上层提供一个统一的高性能的容错存储空间，大幅提高了存储系统的数据吞吐量。RAID主要包含RAID 0～RAID 7等数个规范，它们的侧重点各不相同，详见文献[13]。在RAID之后，随着数据量不断增加和对数据可用性要求的不断提高，出现了基于文件存储的NAS[14]和基于块设备访问的SAN[15]，二者均为基于网络的存储虚拟化技术的代表。网络附属存储(network attached storage，NAS)主要应用于以文件共享为基础的虚拟存储系统中。存储区域网络(storage area network，SAN)主要应用在以数据库应用为主的块级别的数据共享领域。存储虚拟化接替了物理存储设备的配置和管理的负担，同时使得存储资源的利用率更为高效。它可以使逻辑存储单元在广域网范围内整合，并且可以不需要停机就从一个磁盘阵列移动到另一个磁盘阵列上(实时迁移技术[16])。

3.3 I/O虚拟化

为满足多个虚拟机操作系统对外设资源的要求，VMM 通过 I/O 虚拟化的方式来复用有限的资源。系统将物理机真实的 I/O 统一管理，抽象成多个逻辑 I/O 以响应虚拟机的请求。I/O 虚拟化的优点在于可以降低布线的成本和复杂性，并减少基础设施的端口数量。

VMM 截获客户操作系统对设备的访问请求，然后通过软件模拟真实设备的效果，从而有效地实现了物理资源的复用。I/O 虚拟化要经过设备发现、访问截获和设备模拟交付 3 个过程。设备发现就是要让 VMM 提供一种方式，来让虚拟机操作系统发

现虚拟设备，这样虚拟机操作系统才能加载相关的驱动程序。当虚拟设备被虚拟机操作系统发现之后，驱动程序就会按照接口定义访问这个虚拟设备，VMM 需要截获客户机操作系统对虚拟设备的访问，并进行模拟，直至最终交付。

现有的 I/O 虚拟化技术大都是通过软件方式实现的。随着虚拟化的升温，Intel 和 AMD 逐渐支持了 IOMMU[17]技术，IOMMU 提供了设备之间的隔离，使得外部设备可以如同虚拟机一样使用客户物理地址进行寻址，简化 Hypervisor/VMM 的设计。

3.4　网络虚拟化

网络虚拟化是将软/硬件网络资源和网络功能整合在一起，并进行基于软件的实例化管理的过程。关于企业的网络虚拟化主要分为 2 部分：首先是虚拟专用网(VPN)，VPN 是对企业内部网的扩展，其核心是利用公共网络建立虚拟私有网，可以帮助远程用户与组织的内部网建立可信的安全连接，并保证数据的安全传输，是移动办公的一个重要支撑技术；其次是虚拟局域网(VLAN)，可以将一个物理局域网划分成多个 VLAN，也可以将多个物理局域网的节点划分到同一个 VLAN 中，VLAN 之间在无路由情况下不能互相通信，可以有效控制广播风暴并提高网络安全性。除上述之外，还有基于互联设备的虚拟化和基于路由器的虚拟化。前者通过使用标准的操作系统来统一管理网络互联设备和网络存储设备，实现数据与控制分离，增强系统鲁棒性；后者在固件上实现虚拟化功能，通过增加软件来提升路由器本身的性能和功能。

4　虚拟化技术在云计算中的应用

虚拟化技术在企业中的宏观应用体现在云计算中。云计算的定义多种多样，各厂商、网站、机构均从各个角度给出了不同的答案，但从本质上看，云计算以交付服务为根本，将软硬件资源封装并以透明的方式呈递给用户。

云计算的特征体现为虚拟化、分布式和动态可扩展。虚拟化是云计算最主要的特点，也是云计算最重要的技术基础与核心原动力。云计算的一个核心思想就是在共享资源的同时，提供隔离、安全、可信的工作环境。虚拟化后的资源可以按照云的实际情况进行动态调整，使每个用户都有独立的计算环境。此外，虚拟化简化了应用编写的工作，使得开发人员可以仅关注于业务逻辑，而不需要考虑底层资源的供给与调度。最后，云计算的易创建性使应用和服务可以拥有更多的虚拟机来进行容错和灾难恢复，从而提高了自身的可靠性和可用性。

虚拟化在云计算中的应用很广泛。在基础设施方面，通过虚拟化技术对物理资源进行抽象，实现内部流程自动化和资源管理优化，并为外部使用者提供各种各样的基础设施服务。如 Amazon EC2[18]，它采用 Xen 虚拟化技术，以虚拟机的形式向用户动态提供计算资源。它允许开发者创建基于 Linux 的虚拟机，这种创建过程既可以从零开始也可以使用预先构建好的映像文件。然后，使用 Web 服务 API 或该 API 的脚本封装器，可以快速部署任何数目的虚拟机。在平台层，虚拟化技术可以实现应用间隔离和用户间隔离，如 Google App Engine[19]，为用户提供托管平台，使不同应用、用户之间在运行时不会互相干扰。并且通过虚拟化技术对不同需求的服务器进行分别配置和扩展服务，实现可伸缩性。

5　虚拟化在桌面交付系统中的应用

虚拟化技术在企业中的微观应用体现在员工的桌面交付上。桌面交付系统的产生愿景就是一个人走到任何一个地方，只要打开一个连入网络的桌面终端就可以访问专用的桌面。其最大价值在于能真正让用户摆脱对设备的依赖，为不同的用户提供不同的资源，使计算从以设备为中心转向以用户为中心。

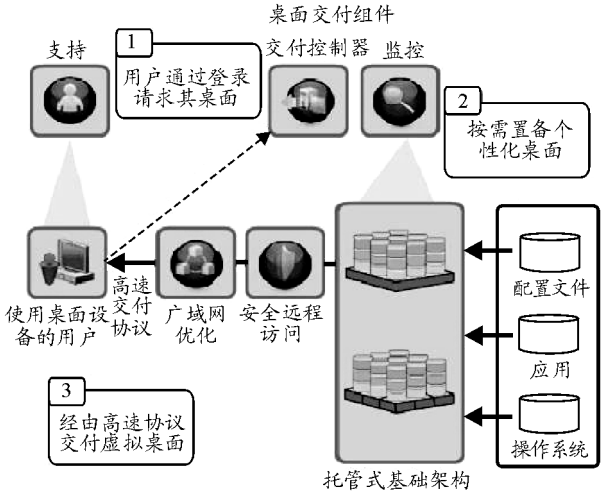

图 5　桌面虚拟交付基本结构[20]

桌面交付系统是系统虚拟化技术集成应用的实例，它将资源集合到后台数据中心，构建虚拟桌面架构 VDI[20]，在数据中心运行着多个 Virtual Desktops，为用户提供基于服务器的计算环境(镜像形式)，用户可以随时随地通过网络来访问存在于服务器上的桌面系统，就像本地使用物理机一样，其在前台所接收到的操作系统平台以及运行的应用程

序，全都是使用虚拟化技术制作出来的数据流；管理员能够接收用户请求，使用软件从集中位置来统一认证、配置、管理客户端设备。主要步骤有：访问验证、桌面配置和桌面交付，同时不断进行数据的安全性和访问控制，如图 5。

在交付系统中，利用虚拟化技术对软硬件资源进行了整合，通过智能运算体系将各种资源按需交付给用户，动态灵活的资源分配保证了用户桌面环境始终处于较高的可用性和有效性。

但上文所描述的仅仅是服务器端的可靠，如果企业的客户端存在不稳定因素，用户就无法通过自己的客户端正常访问高度可靠的数据中心提供的资源，那服务器端即使再可靠，对企业和用户来说也显得毫无意义。针对上述问题，桌面虚拟化借用“瘦客户端[21]”模型，如图 6，将企业中用户的存储资源集中管理。最常见的瘦客户端模型只为终端用户提供 GUI(图形用户接口)，其余功能由中央服务器提供，使用网络启动加载操作系统。

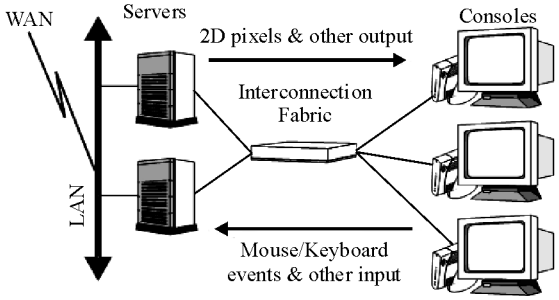

图 6 瘦客户端模型[21]

瘦客户端本地通常没有存储设备，不会存储任何文件数据以及外部的恶意代码，通过网络与服务器进行交互操作，一切数据资源的操作均在服务器上进行，其架构可以确保企业的数据安全。

6 存在的问题

虚拟化技术给企业带来了种种优势，可以将软硬件之间的关系解耦合，灵活构建计算环境，提高计算资源的使用效率，以达到为用户提供个性化和普适化的计算环境的目的。但是虚拟化依然在应用上存在着一些问题，主要体现在 3 个方面：

1) 业内没有一个统一的标准平台和开放协议，各厂商之间的解决方案存在兼容问题，不能在同一环境下实现整合，使企业系统的灵活性大大降低，同时也增加了管理成本。2) 虚拟化技术本身的风险，虚拟化技术的本意是高效利用资源，利用较少的设备实现较多的功能，这样势必会将多种应用放在同一台服务器上，如果服务器的容错能力不足，则其影响甚至远大于未虚拟化的服务器。3) 各服务器之间的负载均衡也是一个重要的问题，如果在同一时间有大量用户请求同一种应用，那么虚拟化技术怎样能够在用户满意度和服务器调度之间取得平衡也是下一步工作的要点。除了上述 3 点之外，初期成本高昂、短期回报少、对用户权限的限制以及虚拟系统本身的安全性都是企业级虚拟化技术的瓶颈问题[22]。总而言之，虚拟化技术为企业带来了巨大的竞争力，但是没有受到良好管理的虚拟化比不使用虚拟化更危险。

7 总结

总体来说，虚拟化技术通过将物理资源逻辑实现，为企业用户提供了便捷、高效、安全和易管理的IT环境，但依然存在着安全性、行业标准不一致和负载均衡等方面的问题。

参考文献：

[1] Intel 开源软件技术中心、复旦大学并行处理研究所. 系统虚拟化-原理与实现[M]. 北京: 清华大学出版社, 2009: 1-2.

[2] 王庆波, 金淳, 何乐, 等. 虚拟化与云计算[M]. 北京: 电子工业出版社, 2009: 27-28.

[3] Seawright L.H, MacKinnon R.A. VM/370: A Study of MultiPlicity and Usefulness[J]. IBM System Journal, 1979, 18(1): 4-17.

[4] Martin F. Maldonado. 虚拟化概述: 模式的观点[EB/OL]. (2006-07-03)[2011-03-10].http://www.ibm.com/developerworks/cn/grid/gr-virt/.

[5] 程伍端. 计算机虚拟化技术的分析与应用[J]. 计算机与数字工程, 2008, 36(11): 175-178.

[6] VMware. Understanding Full Virtualization, Paravirtualization, and Hardware Assist[EB/OL]. [2011-03-10]. http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf.

[7] Whitaker A, Shaw M, and Gribble S D. Denali: Lightweight virtual machines for distributed and networked applications[R]. Montery, California, USA: In Proc of the 2002 USENIX Annual Technical Conference. Technical Report 02-02-01, 2002.

[8] Paul Barham, Boris Dragovic, Keir Fraser, et al. Xen and the art of virtualization[C]. New York, NY, USA: In Proc of the nineteenth ACM symposium on Operating systems principles, 2003, 37(5): 164-177.

[9] Intel Corporation. Virtualization Technology [EB/OL]. [2011-03-10].http://www.intel.com/technology/virtualization/technology.htm?wapkw=(Intel+VT).

[10] AMD Corporation. AMD Virtualization (AMD-V^{TM}) Technology[EB/OL]. [2011-03-10]. http://sites.amd.com/us/business/it-solutions/virtualization/Pages/amd-v.aspx.

（下转第 57 页）