增强英特尔®架构服务器上的虚拟化

提高效用、改进管理、降低成本

在基于英特尔® 处理器的平台上实施的服务器虚拟化已经能够帮助企业加快服务器整合、简化测试和开发环境、降低总成本、提高响应多变工作负载要求的速度。英特尔虚拟化技术将可以为目前的纯软件解决方案提供基础性的架构支持。通过推动技术创新的步伐和增进虚拟化解决方案的功能、互操作性与支持，它必将使虚拟化发挥出更多的优势。

2005年3月

目录

要点综述

“……企业现在应该开始重视虚拟化技术了。”

——《服务器采购与部署的远景》，
Andrew Butler，Gartner副总裁兼服务器技术研究领域负责人，2004年3月18日。

虚拟化技术已经开始转变许多IT机构供应和管理其系统和应用的方式。服务器虚拟化技术可实现多个操作系统和应用，灵活、安全地向单个平台的整合。这样的整合可进而降低服务器的数量、提高效用、简化IT基础设施并降低管理成本。如果与快速的软件供应工具结合使用，它还可以灵活动态地管理硬件资源以满足不断变化的工作负载要求。这些能力已经为许多企业带来了巨大的价值，预计它在今后几年的采用率将急速上涨。据IDC估计，2003年发运的服务器中有8%已带有供应和虚拟化特性，这一比例预计到2007年将增至40%[1]。

英特尔® 虚拟化技术（之前称之为英特尔Vanderpool技术）将提供旨在增加当前纯软件虚拟化解决方案的价值的硬件支持。这一英特尔架构扩展将有力帮助IT机构：

- 降低实施服务器虚拟化解决方案的成本和风险。
- 提高应用在虚拟分区上的可靠性、可用性和安全性。
- 增强与传统软件的互操作性。

英特尔虚拟化技术还将简化虚拟化软件的开发工作，进而加快创新的进度。其规范已经发布。英特尔® 安腾® 2处理器架构平台中的硬件支持预计将于2005年实现；64位英特尔® 至强™ 处理器架构平台中的硬件支持预计将于2006年上半年实现。英特尔目前正与多个业界领先的第三方厂商展开密切合作，以便能够更早地推出能有效利用这一全新架构改进的下一代虚拟化软件。

虚拟化是一项革新技术，英特尔正准备在英特尔架构上提供市场上领先的虚拟化能力。这些能力将与其它重点在于解决当今主要IT难题的英特尔平台创新形成有效的互补。将它们相组合，这些技术将继续提高英特尔架构的灵活性、可靠性、安全性和可管理性，并将进而带来更多可满足各种IT需求的商业价值。

[1] 资料来源：《IDC适应性资源管理报告》（2004年）。

高昂的IT运营成本

“迄至2008年，不利用虚拟化的企业将多支付40%以上的采购成本，并还将多支付约20%以上的管理费用……”

——《服务器虚拟化远景》， T. Bittman，Gartner Research Note，2003年7月17日。

虚拟化是一项革新技术，英特尔正准备在英特尔架构上提供市场上领先的虚拟化能力。这些能力将与其它重点在于解决当今主要IT难题的英特尔平台创新形成有效的互补。将它们相组合，这些技术将继续提高英特尔架构的灵活性、可靠性、安全性和可管理性，并将进而带来更多可满足各种IT需求的商业价值。

一般的IT机构通常会将其70－80%的预算用做现有系统和应用的管理开支[2]。其中一项开支就是管理每个数据中心都会配备的、大量未充分利用的服务器。过去，IT机构总是倾向于使用一台服务器运转一个应用。考虑到工业标准服务器价格的可承受性，这的确是一种经济高效的战略，因为它不仅可简化部署工作，还可减少潜在的软件冲突。然而全球范围的服务器数量在过去十年间已经剧增了将近150倍，与维护这些系统相关的成本也相应地发生了急剧增长[3]。同时服务器的平均性能也明显有所提高。当前服务器的性能已经是十年前服务器的十多倍。通过将多个应用和操作系统整合到单个平台，虚拟化可以帮助IT机构充分利用这一提升的性能，进而提高服务器的利用率并同时降低管理、功耗和散热要求[4]。当前的解决方案还能够灵活分配计算资源，以备不时之需。借助这些工具，许多IT机构均将能够大幅降低他们的服务器相关成本（包括投资和运营），并同时有效地提高其数据中心的灵活性（图1）。

服务器虚拟化软件的领先开发商Vmware，证实了通过虚拟化和整合客户可在服务器总保有成本上节省的具体成本[5]：

- 硬件成本降低： 28-53%
- 运营成本降低： 72-79%
- 总共成本降低： 29-64%

Vmware还证实，虚拟化可在软件授权成本上再节省20%的成本[6]。鉴于如此巨大的优势，服务器虚拟化技术将在今后几年被广泛采用就不足为奇了。

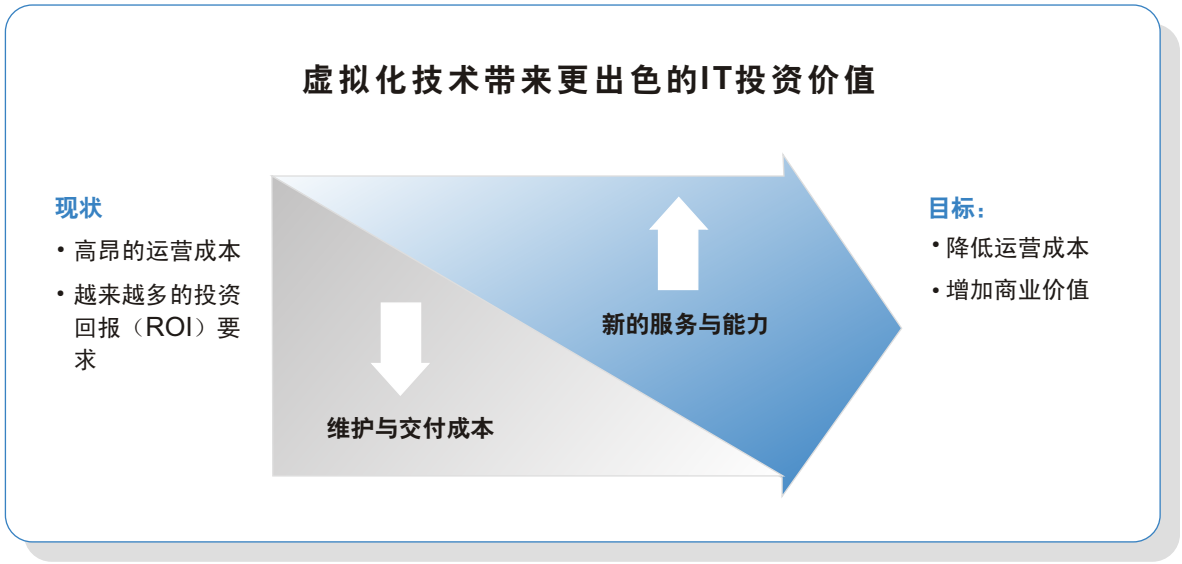

图1。随着802.16a标准（Wi-MAX）得到批准，现在可以采用经济高效的标准技术在整个城区部署全面、安全且易管理的无线

[2] 基于戴尔公司总裁兼首席运营官（COO）Kevin Rollins在《戴尔与Sun Offer的不同远景》中的引言，引自Larry Greenemeier的《InformationWeek.com》，2003年9月17日。

[3] “尽管处理能力的成本相对较低（并且越来越低），但是空间、功耗、安装、集成和管理的费用却很高……”资料来源：《服务器虚拟化的远景》，T. Bittman，Gartner Research Note，2003年7月17日。

[4] 注：服务器虚拟化可分为几种，包括操作系统模拟（如：Java虚拟机）和工作负载管理（多个应用共享一个操作系统）。本白皮书主要侧重的是资源管理，它能够支持多个操作系统共享平台资源。如欲了解有关其它虚拟化模式的更多信息，请参阅《服务器虚拟化的远景》，T. Bittman，a Gartner Research Note，2003年7月17日。

[5] 如欲了解详细信息，请访问VMware网站：http://www.vmware.com/solutions/consolidation/mission_critical.html

[6] 资料来源：Michael Mullany，VMware市场推广副总裁，引自Mark Hall所著文章《MAC引来新支持……》，计算机世界，2005年1月10日），网站地址：http://www.computerworld.com/softwaretopics/os/macos/story/0,10801,98824,00.html

虚拟化一项革新的技术

“虚拟化技术可以帮助公司有效地将逻辑单元的使用（如操作系统或存储容量）和物理单元的操作（服务器或磁盘）分立开来。这可以让企业实现最高的使用率—并获得管理和运转资产的巨大灵活性。”

——*Organic IT 2004：《降低IT成本，加速企业增长》*，Frank E. Gillett，Forrester Research，2004年5月18日。

一般意义下的虚拟化能够将软件和其下面的硬件基础设施抽象开来。实际上，虚拟化切断了具体软件堆栈与具体服务器之间的联系。这就为控制硬件和软件资源带来了更大的灵活性，并进而带来了可满足各种IT需求的出色价值（图2）。

整合和标准化服务器基础设施

目前的各种虚拟化解决方案均支持跨所有英特尔处理器架构平台的整合。它们可以用来提高小型双路服务器的利用率，或用来支持4、8、16路或更多路平台上的传统应用。

平台资源（如处理能力、内存、输入/输出和存储）可以根据业务和应用的需要，按需进行分配和排序。这至关重要，因为应用可能具有截然不同的工作负载要求。灵活地进行资源分配可以增强性能、提高整合率并为新的平台采购带来更丰厚的回报。

借助虚拟化，多种不同的操作系统可以共用一个平台，这样可大幅简化企业标准化硬件基础设施的创建工作。再加上整合，这就可以从根本上显著地简化数据中心环境并降低总保有成本（TCO）[7]。

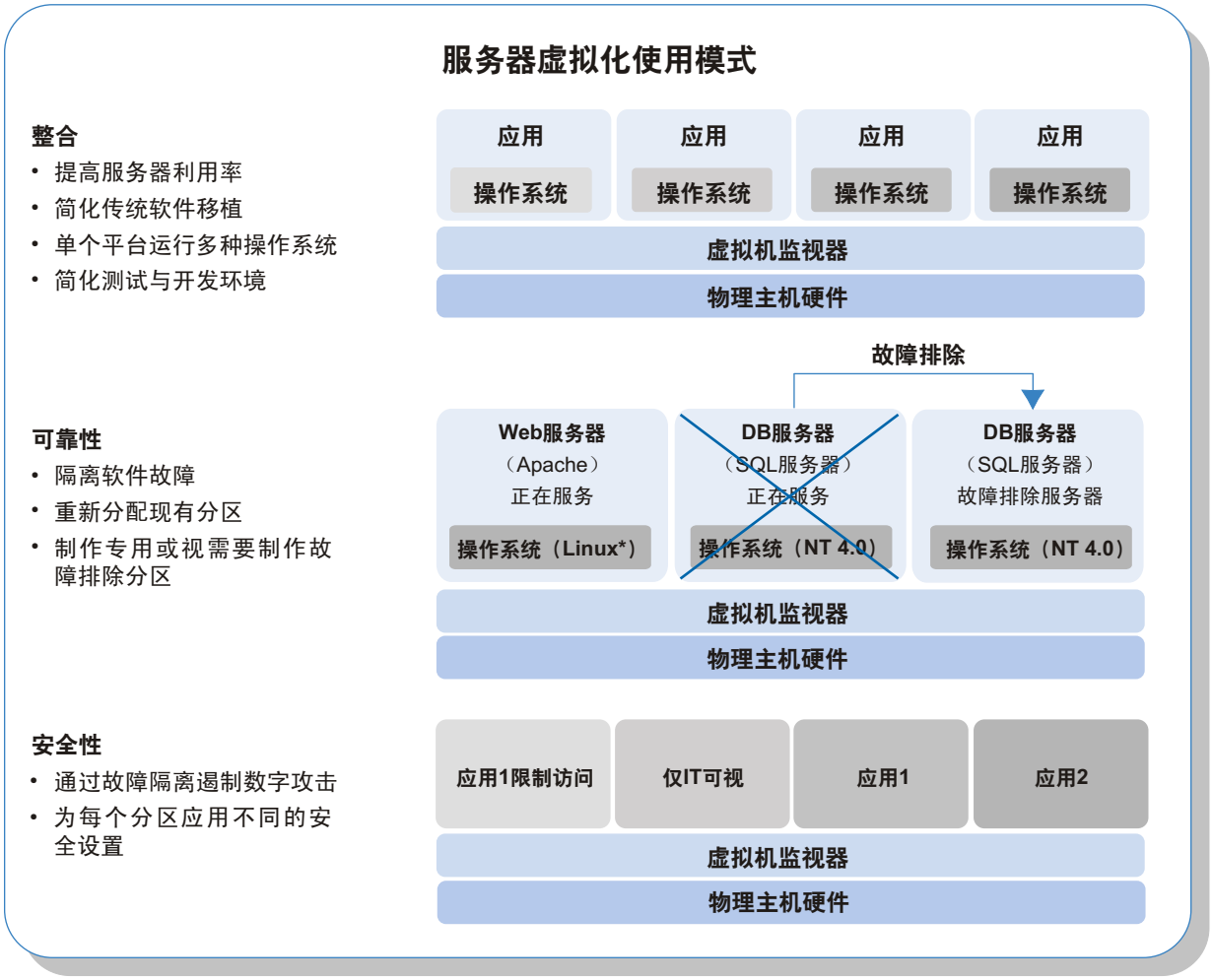

图2：服务器虚拟化可以用来提高服务器的利用率、可靠性和安全性，同时也可以用来提高企业的灵活性并降低运营成本。

[1] 如欲了解详细的讨论信息，请参阅《标准化在简化IT基础设施中的作用》，IDC高层研讨会简报，2004年9月。

提高可用性和安全性

虚拟化技术可通过以下几种主要方式提高可用性和安全性：

- **故障隔离**－大多数应用故障均由软件故障而起。虚拟化可以在虚拟分区之间进行逻辑隔离，这样一个分区的软件故障就基本不会影响到另一分区的应用。逻辑隔离还能帮助遏制数字攻击，有效增强整合环境中的安全性。
- **灵活的故障排除**－通过配置，各个虚拟分区可以为一个或多个应用提供自动故障排除。由于目前基于英特尔安腾2处理器的平台和基于多路英特尔至强处理器MP的平台均带有多项高可用性特性，如果要满足所有服务层要求，通常只需通过在平台上以基本应用的方式提供故障排除分区即可实现。如果要求更高的可用性，可将故障排除分区设置在单独的平台上。
- **不同的安全设置**－每台虚拟机可以应用不同的安全设置，这样IT机构就能够长期具备比最终用户更高的控制能力和管理特权。

简化操作系统与硬件移植

虚拟化的一项主要优势是它可以简化传统应用到新平台的移植，以进而提高性能、可靠性和可管理性。在这种情况下，应用不必移植到新的操作系统下，反而可以留存在新平台虚拟分区中的现有操作系统下，而且也不需进行软件修改。这种战略常用来延长传统应用的使用时间，而且其成本和风险均相对较低。

简化测试和开发

虚拟化为开发与测试环境提供了同样巨大的优势。连续重复的软件堆栈（包括生产版本）可以放存于同一平台的不同虚拟分区之中。这可以提高硬件的利用率并简化整个产品周期的管理。在多数情况下，IT机构能够在现有的生产平台上测试新的和升级的解决方案，无需调整生产环境。这不仅可简化移植过程，同时还可以进一步降低成本（因为不必进行环境重建）。

提高企业灵活性

供应或重新调整虚拟分区的大小远比购买和部署新的硬件平台容易得多。当前的自动化供应解决方案具备这一优势，所以能够显著地提高IT响应能力。企业由此就可以部署更少的平台，但却可以更灵活地借助它们来满足不断变化的需要。

新时代的电脑灵活性：台式机和工作站的虚拟化

客户端平台也将集成英特尔虚拟化技术，相应的支持预计将于2005年开始实现。其主要优势如下：

- **增强可用性与可管理性**－关键的IT管理与网络安全工具可单独放在安全的分区之中，以防止未经授权的篡改。这样可以提高可用性和增强恢复能力，并能够在断开最终用户的前提下，实现升级、维护和管理。这些能力将与英特尔主动管理技术的能力形成有效的互补，（它们大致将在同一时间推出，如欲了解更多信息，请访问：http://www.intel.com/technology/manage/iamt/）。
- **增强电脑的安全**－虚拟分区可以用来限制多用户机器中的个人台式机访问，并可以有效遏制各种数字攻击（病毒、蠕虫、黑客等）。比如： 浏览网页和查看电子邮件可以放在不同的分区中，从而对商务应用和数据的潜在攻击就将被有效地遏制。
- **提高IT灵活性**－ 一台电脑划出多个安全、独立的分区，以支持多个用户， 还可以部署多个操作系统支持各种不同的功能（如：Unix用于工程应用、Windows用于个人办公套件）。 在可以将个人和企业的应用同时放在一台计算机上，并通过分区保持高度的安全性和可用性。
- **实现桌面便携性**－用户的桌面可以被压缩，并方便地移动至另一电脑上的安全、虚拟分区。

困境之中的数据中心中小型企业的虚拟化

目前，服务器虚拟化在企业数据中心中的应用已经非常普遍。随着时间的推移，它有可能在中小型企业中得到同样广泛的应用。通过将应用分置在不同的虚拟分区中，虚拟化技术必将为中小型企业带来更高的可靠性、可用性和安全性。

中小型企业用户还可以配置故障排除分区来进一步增强可用性，并可以通过添置分区或重新分配平台资源获得极其灵活的可扩充能力。随着企业的发展和硬件能力需求的加剧，应用还可以经过压缩轻松地移植到新系统的虚拟分区。

英特尔架构上的服务器虚拟化

“英特尔服务器的利用率将在2003年和2008年间提高一倍。”

——《*预测2004年：服务器虚拟化正在迅速演进*》，T. Bittman，Gartner Research Note，2003年11月14日。

VMware*和Microsoft*现在已经推出了各自的虚拟化软件，可为基于英特尔架构的服务器提供之前仅大型机拥有的强大能力。许多企业正以20：1或者甚至30：1的整合比率将传统的应用纷纷向4路至16路的英特尔处理器架构平台[8]移植。

随着英特尔双内核处理器的上市，虚拟化的重要性将更加显然。结合英特尔的超线程（HT）技术‡，采用双内核处理器的两路平台将可以支持高达8个软件线程；4路平台将高达16个；8路平台高达32个；16路平台则更可支持高达64个线程。这将为多个应用在单个平台上的高效运行提供极大的灵活性。

如何实现

在服务器上创建虚拟分区时，一个被称之为虚拟机监视器（VMM）的薄软件层会直接在服务器硬件上运行。在VMM之上然后才是一个或多个Guest OS和应用堆栈（图3）。

虚拟机监视器（VMM）：

- **模拟**为每个软件堆栈模拟一个完整的硬件环境——虚拟机。理论上，操作系统和应用完全不知道它们正在同其它的应用共享硬件资源。
- **隔离**每个虚拟机上的应用执行，以提供高度的安全性和可用性。
- **分配平台资源**（处理、内存、I/O、存储等）以优化性能并按业务需求调整服务层级。
- **压缩软件堆栈**（包括操作系统和状态信息），以便能够轻松地将它们复制并移动至同一或其它平台上的新虚拟机。

现在的虚拟化解决方案已具备所有这些功能。但是，这些纯软件解决方案通常需要复杂的工作区。为实现更好更经济高效的虚拟化，和便于更轻松地进行软件开发，英特尔已与业界领先的VMM厂商展开了密切的合作，并共同确立了一套新的架构标准。这些标准统称为英特尔虚拟化技术，并且已经发布，以帮助加速在基于英特尔架构的企业平台上的虚拟化解决方案创新。

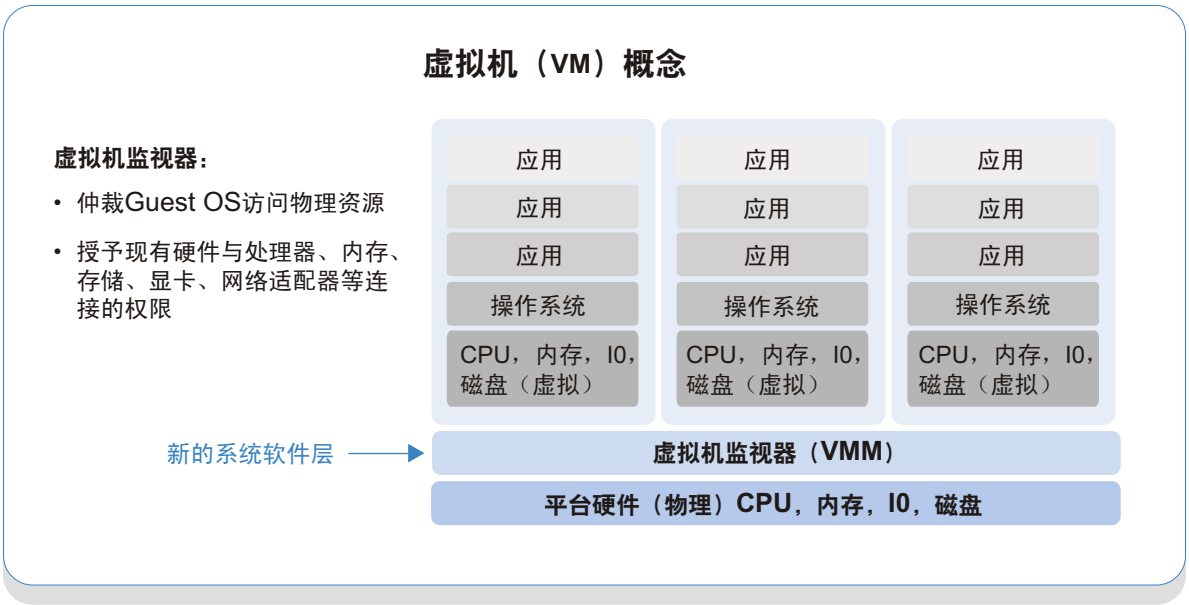

图3：服务器虚拟化的关键是虚拟机监视器（VMM），它是一种能够管理硬件资源和仲裁多个操作系统和应用堆栈的请求的软件应用。

[8] 如欲了解更多信息，请访问英特尔网站http://www.intel.com/business/bss/products/server/consolidation/index.htm；或参阅英特尔白皮书：《英特尔架构上的20：1整合》，网址：http://cache-www.intel.com/cd/00/00/14/88/148803_148803.pdf

面向下一代解决方案的硬件辅助虚拟化

> *“英特尔Vanderpool技术[现在已称为英特尔虚拟化技术]将使诸如Vmware和虚拟电脑等产品更加高效、强大、安全和灵活。”*
>
> ——*《英特尔Vanderpool将推动虚拟化创新》*，Martin Reynolds，Gartner Research，2005年1月21日

在一般的平台环境中，通常会有一个单独的操作系统来控制平台资源，和仲裁一个或多个应用的请求。在虚拟化的平台环境中，可能会存在多个运行在VMM软件之上的Guest OS。为避免冲突，VMM必须把持关键平台资源的控制权限，而且应该是在必要的时候才向每个Guest OS让出有限的控制权限。这些转接的效率和完整性对于实现最佳的性能和可靠性至关重要。

挑战

在当前的32位英特尔架构中，所有软件的运行位置可分为四个“特权级”或“环”（0环到3环）。操作系统一般在0环中运行，该环提供了最多的处理器与平台资源访问特权。单独的应用通常在3环中运行，这一环限制了一些可能会影响其它应用的功能（例如内存映射）。操作系统就是以这种方式保留了控制权限，以确保系统顺畅地运行。

因为VMM必须具备控制平台资源的特权，所以一般的解决方案就是在0环中运行VMM，在1环或3环中运行Guest OS。但是，目前的操作系统均是专为在0环中运行而设计的。由此便产生了挑战。具体而言，能够控制关键平台资源的有17条“特权”指令。现有的绝大多数操作系统版本中均会时不时地运行这些指令。当操作系统不在0环中运行时，这些指令中的任何一条指令都能制造冲突，导致系统故障或者响应错误。

纯软件解决方案

通常有两种方法来处理这17条特权指令。

1. **Guest OS运行时调整**——在这种情况下，VMM负责监视运行期间的操作，一旦Guest OS中出现17条指令中的任一条指令，就即可完全控制处理器。VMM处理完冲突之后，再将控制权限交给Guest OS。
2. **Guest OS静态修改（半虚拟化）**——这种情况是在运行之前对Guest OS进行调整。

这两种方法都有不足之处。运行时调整迫使VMM不得不在运行期间提供复杂的工作区，这可能会影响性能。半虚拟化下，VMM又不能支持未经调整的（传统）Guest OS。这两种方法均需要VMM厂商、操作系统厂商、或两者同时投入巨大的软件开发工作。它们还需要VMM和操作系统软件进行升级，这无疑将增加IT支持的成本和复杂性。

采用英特尔®虚拟化技术的更佳解决方案

英特尔虚拟化技术通过扩展内核平台架构，可消除当前虚拟化解决方案中的鸿沟。增强特性包括：

1. **面向虚拟机监视器（VMM）的全新特权环**——这使得guest OS和应用在专为其设计的环内运行，同时确保VMM拥有对平台资源的特许控制权。从而可消除许多潜在的冲突，简化VMM要求，并提高与未更改的传统操作系统的兼容性。
2. **基于硬件的转换**——在硬件中支持VMM与guest OS之间的切换。这可减少对于复杂的计算密集型软件转换的需求。
3. **基于硬件的内存保护**——在专用地址空间为VMM和所有guest OS保留处理器状态信息。这可帮助加快转换，并确保这一流程的完整性。

这些增强特性将可为软件厂商和IT部门带来重要优势，其中包括：

- **降低IT部门的成本和风险**——不依赖于VMM和操作系统软件，将可改进与传统操作系统的互操作性。它还有助于减少同步升级和修补数据中心的需求。支持成本将会降低，IT部门将能够在一致的硬件和VMM平台上支持更广泛的操作系统版本。
- **提高了可靠性和可用性**——降低VMM的大小和复杂性，使之独立于其guest OS，从而减少潜在的软件冲突，避免运行速度降低甚至中断。
- **增强安全性**——在硬件而非软件中管理VMM转换，以帮助增强虚拟分区的逻辑隔离。更小、更简单的VMM还可以更好地防御软件攻击。
- **更简单的VMM开发**——英特尔虚拟化技术的主要目标在于使VMM软件独立于操作系统软件。这将使VMM供应商从“根据操作系统补丁和升级需求调整代码”这种资源密集型工作中解放出来。它还能够在尽可能减少VMM开发和优化的情况下，使现有解决方案更轻松地充分利用最新平台能力。企业有望能够从更快推出的新特性和能力中获益。

不断创新

“……企业应该了解其服务器厂商的虚拟化产品和战略，并使之成为其选择服务器时考虑的一个方面。”

——《预测2004年：服务器虚拟化快速发展》，
T. Bittman，Gartner Research注释，
2003年11月14日

英特尔目前正将英特尔虚拟化技术集成到其所有服务器平台中。

- 预计到2005年下半年基于英特尔安腾2 处理器的平台将支持该技术。
- 预计到2006年上半年基于64位英特尔至强处理器的平台将支持该技术。
- 英特尔还在加速该技术在客户机平台中的集成，预计到2005年将可支持台式机，2006年将可支持笔记本电脑（参见侧栏，电脑灵活性新纪元，第5页）。

英特尔虚拟化技术只是一系列平台创新的第一步，将为先进虚拟化解决方案提供更全面的支持。英特尔工程师目前正在评估I/O虚拟化替代方案，这将使VMM能够在运行于同一硬件平台上的众多应用之间更轻松地管理和分配I/O带宽。

英特尔还将继续与领先VMM和操作系统开发商（第三方和开放源代码方）合作，以为其开发工作提供更强大基础，并确保未来增强特性能够满足商业客户最苛刻的要求。在未来几年，英特尔架构虚拟化解决方案将继续改进，以为IT部门提供日益强大的工具，来整合应用、降低成本和优化业务灵活性。

始终致力于在工业标准英特尔架构服务器上提供全面的市场领先平台技术，其中就包括英特尔虚拟化技术。当前有众多可用技术，包括超线程（HT）技术‡（已讨论过）和英特尔64位扩展技术，能够在单一平台上同时为32位和64位提供最佳支持。未来创新还将包括：英特尔主动管理技术和LaGrande技术，分别致力于平台管理和安全保障。这些先进平台能力完美组合在一起，将能够帮助IT企业解决某些最严峻的挑战，并提高其IT投资的业务价值。

结论

“……未来几年，虚拟化将彻底改变我们运行企业基础设施的方式，并赋予我们更广泛的选择范，以创建更完善的解决方案。”

——《虚拟化之约》（Betting on Virtualization），
Mark Gibbs，Network World，2004年
11月15日。

虚拟化代表了未来优化硬件使用和数据库灵活性的潮流。利用VMware和Microsoft提供的软件，英特尔架构现在可提供灵活、经济高效的虚拟化解决方案。这些解决方案已经为广泛的生产环境带来了出色的价值。

英特尔虚拟化技术将可增加这些优势，从而使基于英特尔处理器的平台能够以集成和无缝的方式支持虚拟化。通过提供全新的VMM软件特权层，以及在硬件中支持主要虚拟化功能，英特尔虚拟化技术将可简化VMM开发和维护，改进与传统操作系统的互操作性，增强安全性和可靠性，并降低实施成本和风险。

英特尔虚拟化技术是一系列平台增强性能之一，英特尔将在未来几年提供重要支持，以增强数据中心灵活性、可管理性和安全性。除了性能和性价比的不断提高，这些创新还将全面提升所有英特尔架构服务器的业务价值。

如欲了解有关英特尔虚拟化技术的更多信息，请访问英特尔网站：http://www.intel.com/technology/ computing/vptech/

英特尔、Intel标识、英特尔安腾、Intel Itanium和英特尔至强、Intel Xeon是英特尔公司及其在美国和其他国家（地区）的子公司之商标或注册商标。

* 文中涉及的其它名称及商标属于各自所有者资产。此处提供的第三方产品信息仅供培训之用。英特尔对第三方产品的性能或支持不承担任何责任，也不就这些设备或产品的质量、可靠性、功能或兼容性做出任何声明或担保。

‡ 超线程（HT）技术要求计算机具备：3.06 GHz或更高主频的含超线程（HT）技术的英特尔奔腾4处理器、支持超线程（HT）技术的芯片组与基本输入/输出系统（BIOS）、以及将超线程（HT）技术最优化的操作系统。实际性能会因您使用的具体硬件和软件的不同而有所差异。如欲了解更多信息，请访问：

http://www.intel.com/cn/gb/homepage/land/hyperthreading.htm

304266-001P