(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101449240 B
(45)授权公告日 2012.06.06

(21)申请号 200780017791.7
(22)申请日 2007.05.14
(30)优先权数据
11/383,455 2006.05.15 US
(85)PCT申请进入国家阶段日
2008.11.17
(86)PCT申请的申请数据
PCT/US2007/011545 2007.05.14
(87)PCT申请的公布数据
WO2007/133741 EN 2007.11.22
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 S·甘吉利 A·J·桑顿 J·F·维德赫纳 K·D·雷
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运
(51)Int.Cl.
G06F 9/44(2006.01)
G06F 17/00(2006.01)

(56)对比文件
US 20040139437 A1,2004.07.15, 全文.
US 20050055192 A1,2005.03.10, 全文.
CN 1541357 A,2004.10.27, 全文.
US 6892383 B1,2005.05.10, 第6栏第1-3段以及附图4.

审查员 张涛

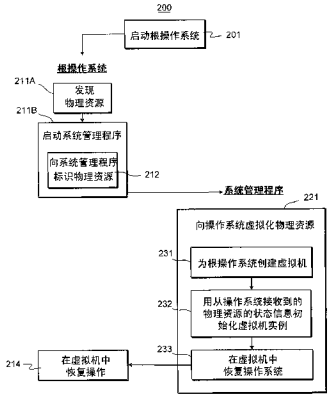
权利要求书 2 页 说明书 7 页 附图 6 页

(54)发明名称

在运行中的操作系统下启动系统管理程序

(57)摘要

在已有运行中的操作系统之后启动系统管理程序。操作系统自身可以启动系统管理程序。可以使用运行中的操作系统来取代系统管理程序来发现运行在计算系统上的物理资源。可以在系统管理程序工作之后启动其它操作系统或操作系统实例。



CN 101449240 B

1. 一种用于使用运行中的操作系统来启动系统管理程序的方法，所述方法包括：

操作系统 (401) 启动 (211B) 系统管理程序 (405) 的动作；以及

所启动的系统管理程序 (405) 向启动所述系统管理程序 (405) 的操作系统 (401) 虚拟化 (221) 计算系统 (100) 的至少一个物理资源 (402) 的动作。

2. 如权利要求 1 所述的方法，其特征在于，所述方法进一步包括以下动作：

所述操作系统发现所述至少一个物理资源的动作；以及

所述操作系统向所述系统管理程序提供关于所述至少一个物理资源的状态信息的动作，所述状态信息至少包括对应的物理资源的标识。

3. 如权利要求 2 所述的方法，其特征在于，所述方法进一步包括以下动作：

所述系统管理程序启动关于所述操作系统的虚拟机实例的动作；

用所述操作系统提供的状态信息来初始化所述虚拟机实例的动作；

在初始化所述虚拟机实例之后，所述系统管理程序恢复所述操作系统的动作；以及

在恢复了所述操作系统之后，所述系统管理程序使用所述虚拟机实例来虚拟化所述至少一个物理资源的动作。

4. 如权利要求 3 所述的方法，其特征在于，所述方法进一步包括为在所述计算系统上启动的每一附加操作系统执行以下动作：

所述系统管理程序启动关于每一附加操作系统的对应的虚拟机实例的动作；

在启动所述对应的虚拟机实例之后，启动所述对应的附加操作系统的动作；以及

所述系统管理程序使用所述对应的虚拟机实例来向所述对应的附加操作系统虚拟化所述至少一个物理资源的动作。

5. 如权利要求 1 所述的方法，其特征在于，所述方法进一步包括以下动作：

所启动的系统管理程序向启动所述系统管理程序的操作系统虚拟化所述计算系统的至少一个物理资源的动作。

6. 如权利要求 1 所述的方法，其特征在于，所述方法进一步包括：

所述操作系统创建临时虚拟机实例的动作；

用生成截取的指令来初始化所述临时虚拟机实例的动作；

在所述初始化动作之后恢复所述临时虚拟机实例的动作；

在检测到得自所述恢复所述临时虚拟机实例的动作的截取后，使用系统管理程序状态来启动所述临时虚拟机实例来操作的动作。

7. 如权利要求 6 所述的方法，其特征在于，所述方法进一步包括在创建所述临时虚拟机实例之前执行以下动作，所述动作包括：

使任何不可屏蔽中断无法起作用的动作。

8. 如权利要求 6 所述的方法，其特征在于，所述方法进一步包括在使用所述系统管理程序状态启动所述临时虚拟机实例之后执行以下动作，所述动作包括：

启动所述系统管理程序的动作；以及

毁去所述临时虚拟机实例的动作。

9. 如权利要求 8 所述的方法，其特征在于，所述操作系统和系统管理程序中的一个以 32 位模式操作，而所述操作系统和系统管理程序中的另一个以 64 位模式操作。

10. 如权利要求 8 所述的方法，其特征在于，所述操作系统和系统管理程序使用不同的

分页机制来操作。

11. 一种用于使用运行中的操作系统 (401) 来启动系统管理程序 (405) 的启动系统管理程序 (405) 的方法 (200)，所述方法包括：

系统管理程序 (405) 从根操作系统 (401) 接收表示所述操作系统 (401) 检测到的多个物理资源 (212) 的信息的动作；

所述系统管理程序 (401) 启动 (231) 关于所述根操作系统的虚拟机实例的动作；

用与所述表示所述操作系统检测到的所述多个物理资源的信息相一致的状态来初始化 (232) 所述虚拟机的动作；

恢复 (233) 所述根操作系统以使所述根操作系统经由使用所述状态初始化的所述虚拟机实例与所述多个物理资源间接地进行接口的动作。

12. 如权利要求 11 所述的方法，其特征在于，在所述系统管理程序运行后，还包括：

启动一个或多个附加操作系统的动作。

13. 如权利要求 12 所述的方法，其特征在于，还包括关于所述一个或多个附加操作系统的每一个的以下动作：

初始化对应的虚拟机实例以与所述对应的附加操作系统进行接口的动作。

在运行中的操作系统下启动系统管理程序

[0001] 背景技术

[0002] 操作系统的一个主要功能是与计算系统上的物理资源进行接口。典型的操作系统可以针对以不恰当的方式访问物理资源进行保护。例如，在应用程序使用特定存储器段时，操作系统可以保护该段存储器不被同一操作系统所管理的另一应用程序更改。否则，应用程序可能不能如所期望的那样工作。这种访问保护通常是基于该操作系统是运行于计算系统上的唯一操作系统的假设。

[0003] 然而，有时在同一计算系统上运行多个操作系统是有利的。在这种情况下，每一操作系统中的确保对资源的安全操作的固有保护可能不再足够。操作系统可能不能够控制另一操作系统对同一物理资源的访问，且甚至可能没有知晓其它运行中的操作系统的存在的机制。

[0004] 系统管理程序是被配置为插入到一个或多个运行中的操作系统和所保护的物理资源（如处理器、I/O 端口、存储器、中断等）之间的软件层。系统管理程序在功能上为操作系统多路复用受保护的物理资源，并以可视化的方式向每一操作系统显示资源。例如，作为一简单的示例，假定有两个操作系统正运行在具有一个处理器和 1 千兆字节 (GB) 随机存取存储器 (RAM) 的计算系统上。系统管理程序可以向每个操作系统各分配一半处理器周期，且向每个操作系统各分配一半存储器 (512 兆字节 (MB) RAM)。此外，系统管理程序可以提供定址到每个操作系统的虚拟化范围的 RAM，以便对两个操作系统看起来都只有 512MB RAM 可用。

[0005] 在操作系统尝试与物理资源进行通信以及物理资源尝试与操作系统进行通信时，系统管理程序执行适当的缓冲和变换以允许每个操作系统都仿佛其是运行在计算系统上的仅有的操作系统一样经历其环境。此外，系统管理程序以计算系统上的物理资源可由多个操作系统实例共享而仍被保护的方式来做到这点。

[0006] 通常，在运行操作系统之前启动系统管理程序。这允许系统管理程序通过呈现物理资源的虚拟化视图来在虚拟机中启动操作系统为立即在虚拟机中启动操作系统，系统管理程序包括用于发现物理资源及其本质特征的 大量代码。由于物理资源发现是在有任何运行中的操作系统之前完成的，所以操作系统不能依赖于该发现过程。因此，在系统管理程序中用于发现物理资源的代码可能相当复杂。

[0007] 发明内容

[0008] 虽然本发明的原理不限于该简要概述中概括的各实施例，但此处描述的某些实施例涉及在已有运行中的操作系统之后启动系统管理程序。尽管并非所需，但可以使用运行中的操作系统来取代系统管理程序来发现运行在计算系统上的物理资源。因此，如果需要，则系统管理程序可以依赖于操作系统来发现资源，而非必须具有执行相同功能的代码。

[0009] 提供本概述以便以简化的形式介绍将在以下详细描述中进一步描述的一些概念。该概述不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

[0010] 附图说明

[0011] 为了进一步阐明本发明的以上和其它优点与特征，将参考附图中示出的其具体实施例来呈现本发明的更具体描述。可以理解，这些附图只描绘本发明的典型实施例，因此将不被认为是对其范围的限制。将通过使用附图用附加特征和细节来描述和说明这些实施例，附图中：

[0012] 图 1 示出了可在其中采用本发明的各实施例的计算环境；

[0013] 图 2 示出用于使用运行中的操作系统来启动系统管理程序的方法的流程图；

[0014] 图 3 示出用于启动附加的操作系统实例的方法的流程图；

[0015] 图 4A 示出其中根操作系统在没有系统管理程序时与计算系统的物理资源进行直接通信的配置；

[0016] 图 4B 示出其中操作系统启动了系统管理程序以用作操作系统和物理资源之间的中介的配置；

[0017] 图 4C 示出其中系统管理程序启动并支持了附加的操作系统的配置；以及

[0018] 图 5 示出用于将操作系统传输到系统管理程序的环境的方法的流程图。

[0019] 具体实施方式

[0020] 根据本发明的各实施例，可以在已有运行中的操作系统之后启动系统管理程序。可以使用运行中的操作系统来取代系统管理程序来发现运行在计算系统上的物理资源。可以在系统管理程序工作之后启动其它操作系统实例。首先，将参考图 1 描述其中可实现本发明的原理的通用计算环境。然后，将参考后续附图描述关于本发明的各实施例的进一步的细节。

[0021] 计算系统现在越来越多地采用各种形式。例如，计算系统可以是手持式设备、电器、膝上型计算机、台式计算机、大型机、分布式计算系统或甚至常规上不被认为是计算系统的设备。在本说明书以及权利要求书中，术语“计算系统”被广义地定义为包括包含至少一个处理器以及其上能含有可由处理器执行的计算机可执行指令的存储器的任何设备或系统（或其组合）。存储器可采取任何形式，且可取决于计算系统的本质和形式。计算系统可在网络环境上分布，且可包括多个组成计算系统。

[0022] 参考图 1，在其最基本配置中，计算系统 100 一般包括至少一个处理单元 102 和存储器 104。存储器 104 可以是物理系统存储器，它可以是易失性的、非易失性的或两者的某种组合。易失性存储器的示例包括随机存取存储器 (RAM)。非易失性存储器的示例包括只读存储器 (ROM)、闪存等。术语“存储器”也可在此处用来指诸如物理存储介质等非易失性大容量存储。这样的存储可以是可移动或不可移动的，且可包括（但不限于）PCMCIA 卡、磁盘和光盘、磁带等。

[0023] 如此处所使用的，术语“模块”或“组件”可以指在计算系统上执行的软件对象或例程。此处描述的不同的组件、模块、引擎和服务可被实现为在计算系统上执行的对象或进程（例如，作为分开的线程）。尽管此处描述的系统和方法可用软件实现，但用硬件以及软件和硬件的组合的实现也是可能的且已被想到。

[0024] 在以下描述中，参考由一个或多个计算系统执行的动作描述本发明的各实施例。如果这样的动作用软件实现，则相关联计算系统中执行该动作的一个或多个处理器响应于执行了计算可执行指令而引导计算系统的操作。这样的操作的示例涉及对数据的操纵。计算机可执行指令（和所操纵的数据）可被存储在计算系统 100 的存储器 104 中。

[0025] 计算系统 100 还可包含允许计算系统 100 例如通过网络 110 与其它计算系统通信的通信信道 108。通信信道 108 是通信介质的示例。通信介质一般用诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据，并且包括任何信息传递介质。作为示例而非限制，通信介质包括有线介质，诸如有线网络或直接线连接，以及无线介质，诸如声学、无线电、红外线和其它无线介质。如此处所用的术语计算机可读介质既包括存储介质又包括通信介质。

[0026] 本发明的范围内的各实施例也包括用于承载或其上储存有计算机可执行指令或数据结构的计算机可读介质。这样的计算机可读介质可以是可由通用或专用计算机访问的任何可用介质。作为示例而非限制，这样的计算机可读介质可包括物理存储和 / 或存储器介质，诸如 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储、磁盘存储或其它磁存储设备、或可用于承载或存储计算机可执行指令或数据结构形式的所需程序代码装置且可由通用或专用计算机访问的任何其它介质。当信息通过网络或另一通信连接（硬连线、无线或硬连线或无线的组合）传输或提供给计算机时，该计算机将该连接完全视为计算机可读介质。因此，任何这样的连接被适当地称为计算机可读介质。以上的组合也应包括在计算机可读介质的范围之内。

[0027] 计算机可执行指令包括例如，使通用计算机、专用计算机、或专用处理设备执行某一功能或某组功能的指令和数据。尽管用对结构特征和 / 或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于在此所述的具体特征或动作。相反，在此所述的具体特征和动作是作为实现权利要求的示例形式公开的。

[0028] 图 2 示出用于运行中的操作系统启动系统管理程序的方法 200 的流程图。在本说明书和权利要求书中，“系统管理程序”是被配置为设置在一个或多个运行中的操作系统和受保护的物理资源之间的软件层。系统管理程序在功能上为操作系统多路复用受保护的物理资源，并以虚拟化的方式向每一操作系统显示资源。由此，系统管理程序用作操作系统和计算系统的物理资源之间的一种特殊的抽象层。

[0029] 例如，作为一简单的示例，假定有两个操作系统正运行在具有一个处理器和 1 千兆字节 (GB) 随机存取存储器 (RAM) 的计算系统上。系统管理程序可以向每个操作系统各分配一半处理器周期，且向每个操作系统各分配一半存储器 (512 兆字节 (MB)RAM)。此外，系统管理程序可以提供定址到每个操作系统的虚拟化范围的 RAM，以便对两个操作系统看起来都只有 512MBRAM 可用。在操作系统尝试与物理资源进行通信以及物理资源尝试与操作系统进行通信时，系统管理程序执行适当的缓冲和变换以允许每个操作系统都仿佛其是运行在计算系统上的仅有的操作系统一样经历其环境。

[0030] 不同于传统的系统管理程序配置，本发明的各实施例准许在操作系统启动之后启动系统管理程序，即使操作系统已经发现了计算系统的物理资源。开始系统管理程序的操作系统将表示所发现的物理资源的状态的信息传递给系统管理程序。由此，系统管理程序不必拥有发现计算系统的物理资源的独立的代码。

[0031] 一旦操作系统启动系统管理程序并将关于所发现的计算系统的物理资源的信息传递给系统管理程序之后，操作系统择可以暂停执行并将控制传递给系统管理程序。系统管理程序随后可以设置虚拟机实例来处理将来的对计算系统的物理资源的任何受保护资源的访问请求。用与受保护的物理资源的操作系统的概念相一致的状态来初始化虚拟机实

例。在完成之后，操作系统在虚拟机环境中恢复。然而，在虚拟机环境中，操作系统通过系统管理程序与物理资源间接地进行接口，而非直接地与物理资源进行接口。这一改变对操作系统来说是透明的，因为专用于与操作系统进行通信的虚拟机尊重操作系统先前发现的关于物理资源的信息。

[0032] 在某些情况下并对于某些受保护的物理资源，可能对操作系统来说不使用系统管理程序则不可能发现受保护的物理资源，并且因此也不可能以透明的方式稍后通过系统管理程序与同一受保护的物理资源间接地进行接口。在这种情况下，操作系统可被配置为理解其稍后将通过系统管理程序来操作，并且因而忽略稍后不能以透明的方式虚拟化的任何物理资源。例如，操作系统加载器可被配置为通知其它操作系统组件不要使用特定受保护的物理资源。

[0033] 回头参考图 2，方法 200 在根操作系统启动（动作 201）时开始。“根”操作系统是启动系统管理程序的操作系统，而非可在系统管理程序工作之后启动的操作系统。图 4A 示出在其中操作系统 401 在没有系统管理程序时与计算系统的物理资源 402 直接进行通信 404 的操作阶段的配置 400A。

[0034] 根操作系统随后执行在图 2 的左边一栏中栏标题“根操作系统”下示出的若干动作。例如，根操作系统发现至少一个物理资源（动作 211A）。操作系统通常具有在启动操作系统不久之后执行的发现计算系统的物理资源的指令。例如，参考图 4A，操作系统 401 发现物理资源状态 403。发现计算系统的物理资源可能是复杂的工作。

[0035] 为在启动系统管理程序之前的状态下恢复操作系统，操作系统捕获在启动系统管理程序之前的物理机器的状态。在一实施例中，所捕获的状态包括所有物理处理器和物理 APIC（高级可编程中断控制器）的状态。物理处理器状态包括：

[0036] 1. 通用寄存器。

[0037] 2. 浮点和 XMM 寄存器。

[0038] 3. 控制寄存器 (CR)。

[0039] 4. 调试寄存器 (DR)。

[0040] 5. 指令指针寄存器 (RIP)、栈指针寄存器 (RIP) 和标志寄存器 (RFLAGS)

[0041] 6. CS、DS、SS、ES、FS、GS 和 TR 段的段状态，包括段基础、限制和访问权限。

[0042] 7. 全局描述符表寄存器 (GDTR)、中断描述符表寄存器 (IDTR) 和局部描述符表寄存器 (LDTR)。

[0043] 8. 包括 KernelGsBase，Star，Lstar，Cstar，Sfmask，SysenterCs，SysenterEip，SysenterEsp 和 ApicBase MSR 的特定模型专用寄存器 (MSR)。

[0044] 物理本地 APIC 状态可以包括：

[0045] 1. 本地 APIC ID

[0046] 2. 请求寄存器

[0047] 3. 服务寄存器

[0048] 4. 任务优先级寄存器

[0049] 另外，在启动系统管理程序时，可以将硬件的某些其它方面作为引导参数提供给系统管理程序。这些可以包括：

[0050] 1. 当前和可能的逻辑处理器，包括可运行时热插入的那些

[0051] 2. 是否在 BIOS 中启用或禁用超线程

[0052] 3. 当前物理 RAM 范围—在引导系统管理程序时用 RAM 填充的系统物理地址范围

[0053] 4. 物理节点（包括在引导时不具有相关联的资源但可能在运行时填充的那些）

[0054] 5. 物理节点之间的存储器存取比率

[0055] 6. 系统管理程序必须访问的特定硬件特征（例如，电源管理定时器）的地址

[0056] 操作系统还启动要插入到操作系统和物理资源之间的系统管理程序（动作 211B）。例如，参考图 4B，系统管理程序 405 被插入到根操作系统 401 和物理资源 402 之间。作为该启动的一部分，操作系统向系统管理程序提供关于至少要被保护的物理资源的状态信息。该状态信息包括系统管理程序发现要由系统管理程序来防护的受保护的物理资源的相关状态所需的所有信息。在一实施例中，状态信息可以包括上述的捕获状态。至少，状态信息至少包括对应的物理资源的标识。

[0057] 同样，作为启动的一部分，操作系统将控制传递给系统管理程序。系统管理程序随后执行图 2 的右边一栏中标题“系统管理程序”下示出的动作。具体地，系统管理程序随后执行向根操作系统虚拟化计算系统的受保护的物理资源所必需的任务（动作 221）。

[0058] 例如，系统管理程序可以创建关于根操作系统的虚拟机实例（动作 231）。参考图 4B，框 421 表示关于操作系统 401 的虚拟机实例。一旦被初始化并工作之后，虚拟机实例 421 将用作关于操作系统 401 的物理资源 402 的代理。虚拟机实例 421 将从操作系统 401 接收对物理资源的服务请求，并将取决于虚拟机实例 421 可访问的状态信息来执行适当的请求变换和缓冲。虚拟机实例 421 随后将使得系统管理程序 405 从物理资源请求适当的服务。虚拟机实例 421 还可以视需要用适当的变换和缓冲来将请求结果报告回操作系统 401。

[0059] 取决于虚拟机实例可访问的状态信息，虚拟机实例 421 将不同地工作。系统管理程序尊重操作系统 401 已发现的关于物理资源 402 的状态信息。因此，系统管理程序 405 用操作系统提供的至少某些状态信息来初始化虚拟机实例 421（动作 232）。例如，系统管理程序 405 可以用操作系统所提供的捕获状态来初始化虚拟机。以此方式，用与表示操作系统所检测到的物理资源的信息相一致的状态初始化了虚拟机实例 421。随后在虚拟机环境中恢复操作系统（动作 233 和动作 214）。在该环境中，如图 4B 中可见的，取代操作系统 401 直接地与物理资源 402 进行接口，通过使用虚拟机实例 421 和系统管理程序 405 来为操作系统 401 虚拟化物理资源 402。由于虚拟机 421 所使用的状态信息与操作系统 401 所发现的状态信息相一致，所以在某些实施例中改变对于操作系统 401 来说是透明的。

[0060] 在一实施例中，经由仿真物理处理器行为的虚拟处理器抽象来提供虚拟化。类似地，其提供仿真物理 APIC 的行为的虚拟 APIC。这如下实现：

[0061] 1. 将虚拟处理器的状态初始化为所捕获的物理处理器的状态。

[0062] 2. 将虚拟 ACPI 的状态初始化为所捕获的物理本地 APIC 的状态。

[0063] 3. 系统管理程序安装截取来防止操作系统访问特许物理硬件资源。例如，本地 APIC 在启动系统管理程序之前所处的客物理地址被标记为不存在以使所有对本地 ACPI 的访问都被俘获到系统管理程序。

[0064] 在启动系统管理程序之后，系统管理程序可以启动附加操作系统，这些附加操作系统或是同一操作系统的实例或是不同的操作系统的实例。例如，参考图 4C，可以附加地启动操作系统 412 和 413 以及可能的由省略号 414 所表示的其它操作系统。图 3 示出用于

同样为附加操作系统虚拟化物理资源的方法 300 的流程图。在要启动附加操作系统时，系统管理程序首先启动对应的虚拟机实例（动作 301），随后通过该动作启动操作系统（动作 302）。系统管理程序使用对应的虚拟机实例来向对应的附加操作系统虚拟化物理资源（动作 303）。

[0065] 在启动操作系统后每一操作系统都执行物理资源的发现时，各种信息请求由对应的虚拟机实例来截取。取代找出与物理资源相关联的实际状态信息，对应的虚拟机向操作系统提供虚拟化的状态信息。

[0066] 有时，启动系统管理程序的操作系统可能处于不同的环境类型。例如，可能操作系统以 32 位模式操作，而要启动的系统管理程序要以 64 位模式操作，或相反。类似地，操作系统和系统管理程序能以不同的分页模式操作。即使操作系统和系统管理程序在不同的环境中操作时，本发明的某些实施例也允许操作系统启动系统管理程序。

[0067] 图 5 示出供操作系统进入系统管理程序的环境以准备启动系统管理程序的方法 500 的流程图。从图 5 的启动操作系统的动作 201，操作系统首先使任何不可屏蔽的中断无法起作用（动作 501），并屏蔽任何可屏蔽中断。能以多种不同的方法来使不可屏蔽中断无法起作用。毕竟，在操作系统转移到系统管理程序操作环境时，应该注意，要确保在加载系统管理程序的初始阶段之前没有中断和异常发生。如果在离开操作系统环境后而在进入系统管理程序环境前发生中断或异常，处理器可能不能够处理该中断或异常，因为没有中断描述符表或栈。大部分异常都可被容易地避免，因为它们是软件初始化的。可以在该过程期间通过将 RFLAGS 寄存器中的 IF 位清零来抑制可屏蔽的硬件中断。

[0068] 可以通过以下两种机制的任一种来抑制不可屏蔽中断（NMI）：

[0069] 1. 自传递一 NMI 并且不执行 IRET 指令：这可以通过临时地修改操作系统的中断描述符表中的 NMI 处理程序地址以指向不同的处理程序来达到。随后 NMI 可被传递到当前处理器。这将使得处理器跳转到 NMI 处理程序所提供的地址。在 NMI 处理程序中，可以还原原始 NMI 处理程序地址并继续。这将有效地屏蔽进一步的 NMI，因为在 x86 架构上，在接收到一个 NMI 之后则屏蔽各 NMI，直到执行了 IRET 指令为止。

[0070] 2. 总是以有效的中断描述符表（IDT）和栈来运行：这可通过创建临时 IDT 和栈来达到。临时页表可以将临时 IDT、NMI 处理程序地址和栈映射在其原始虚拟地址及其各自的物理地址。这确保如果 NMI 在处理器以临时页表运行时到达，则其将被正确地传递到处理程序。

[0071] 一旦中断被屏蔽或以其它方式变为无法起作用（动作 501），则创建临时虚拟机实例（动作 502）。操作系统随后用引起截取的指令来初始化临时虚拟机实例（动作 503）。截取是从操作系统到系统管理程序的控制传输。在恢复了临时虚拟机实例时（动作 504），该虚拟机实例执行引起截取的指令，且截 取被由此生成（动作 505）。因此，临时虚拟机实例开始使用系统管理程序状态来执行（动作 506），从而使得操作系统继续以系统管理程序模式操作（动作 507）。操作系统随后可以启动系统管理程序。可任选地，可以毁去临时虚拟机实例，因为其只是将操作系统置于启动系统管理程序所需要的系统管理程序模式所需要的。

[0072] 因此，本发明的各实施例即使在已有运行中的操作系统存在于计算系统上时仍准许启动系统管理程序。在某些实施例中，即使操作系统和系统管理程序处于不同的环境中，

操作系统也可以启动系统管理程序。

[0073] 本发明可具体化为其它具体形式而不背离其精神或本质特征。所述实施例在所有方面都应被认为仅是说明性而非限制性的。从而，本发明的范围由所附权利要求书而非前述描述指示。落入权利要求书的等效方式的含义和范围内的所有改变应被权利要求书的范围涵盖。

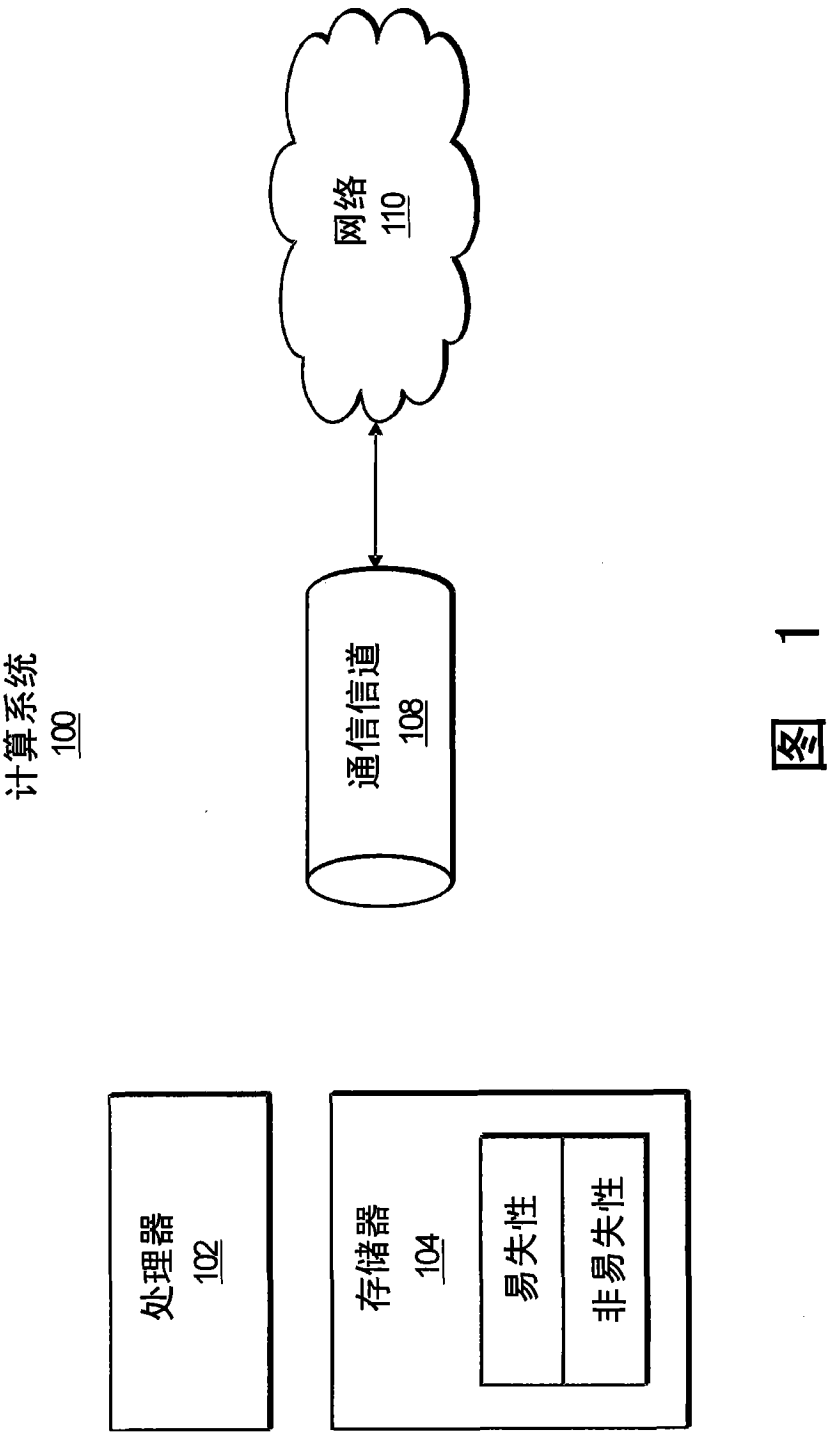


图 1

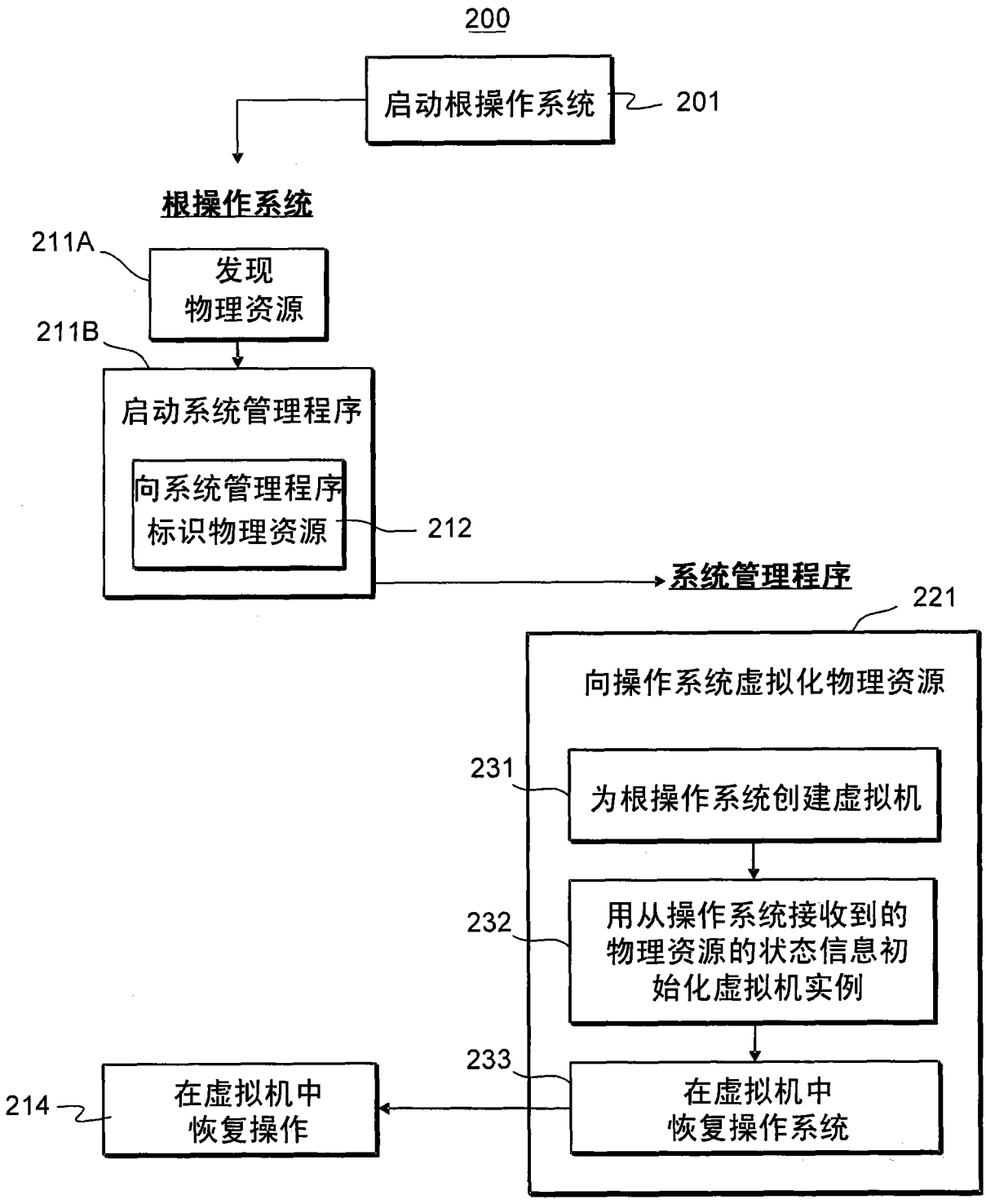

200
启动根操作系统
201
根操作系统
211A
发现
物理资源
211B
启动系统管理程序
向系统管理程序
标识物理资源
212
系统管理程序
221
向操作系统虚拟化物理资源
231
为根操作系统创建虚拟机
232
用从操作系统接收到的
物理资源的状态信息初
始化虚拟机实例
233
在虚拟机中
恢复操作系统
214
在虚拟机中
恢复操作

图 2

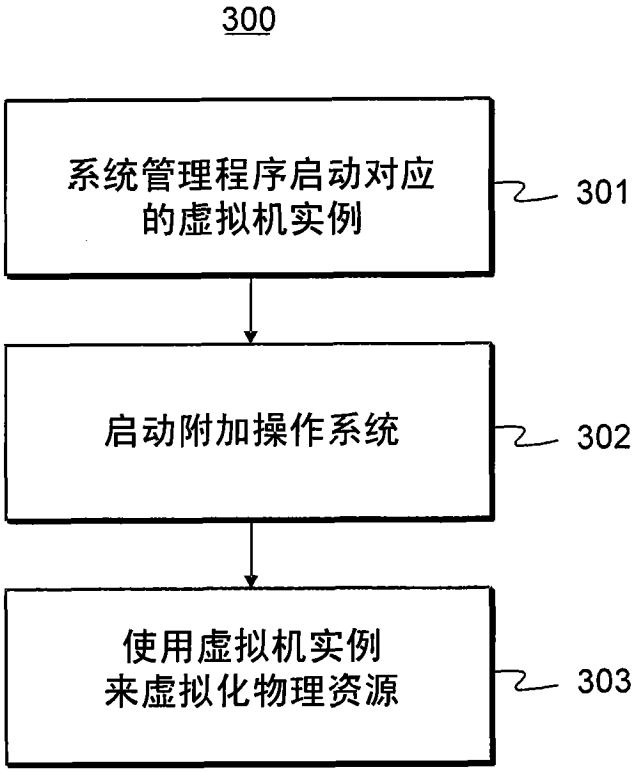

300
系统管理程序启动对应的虚拟机实例
301
启动附加操作系统
302
使用虚拟机实例来虚拟化物理资源
303

图 3

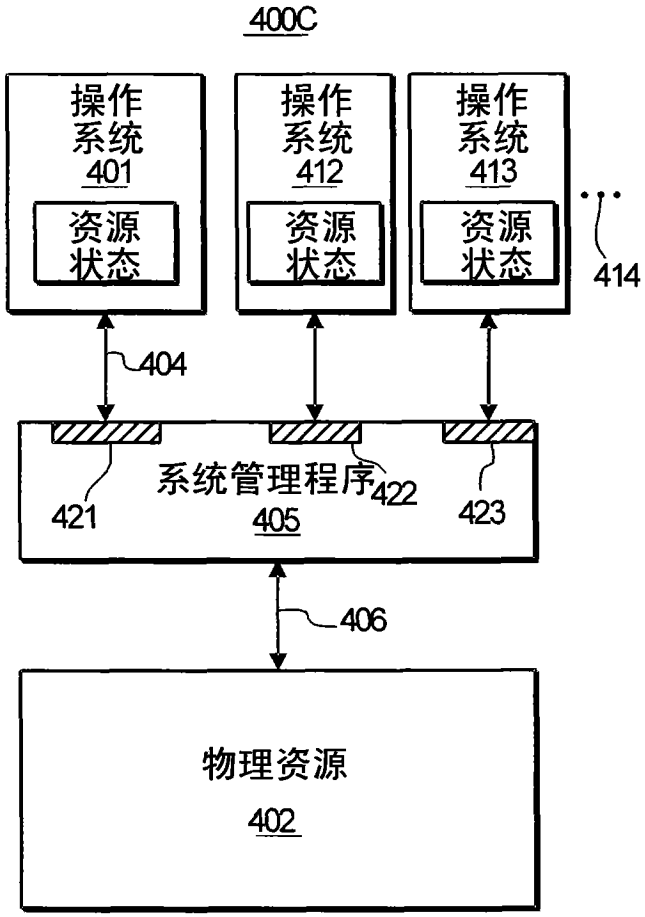

400C
操作系统 401
资源状态
操作系统 412
资源状态
操作系统 413
资源状态
414
404
421
系统管理程序 405
422
423
406
物理资源 402

图 4C

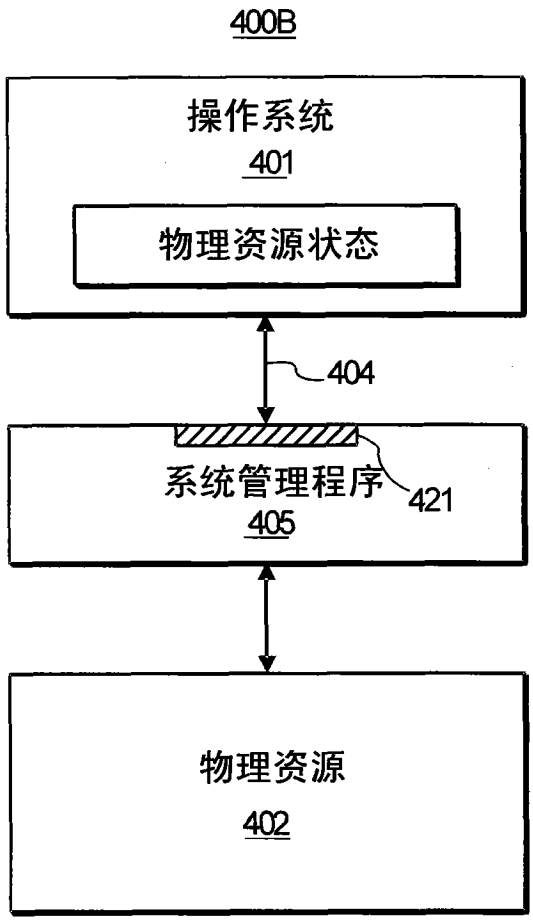

400B
操作系统
401
物理资源状态
404
系统管理程序
405
421
物理资源
402

图 4B

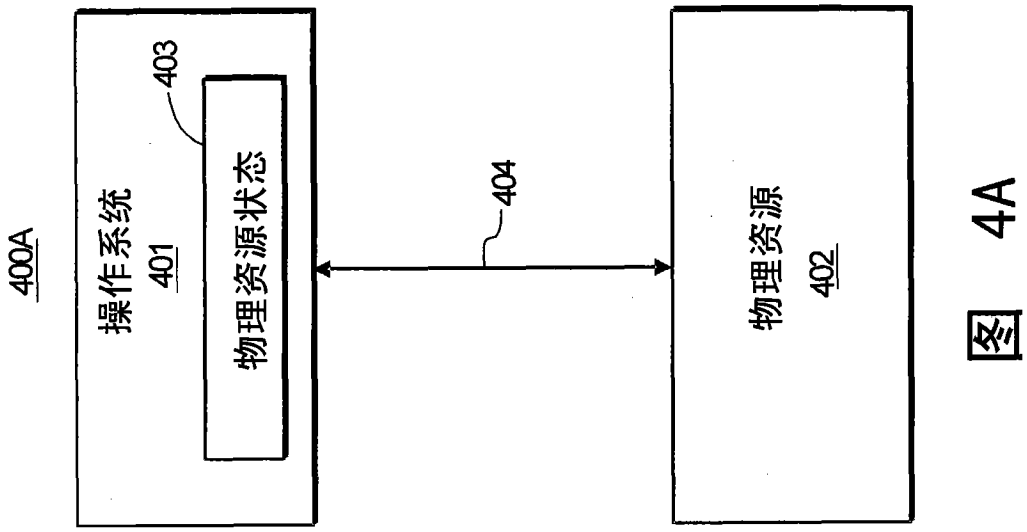

400A
操作系统
401
403
物理资源状态
404
物理资源
402

图 4A

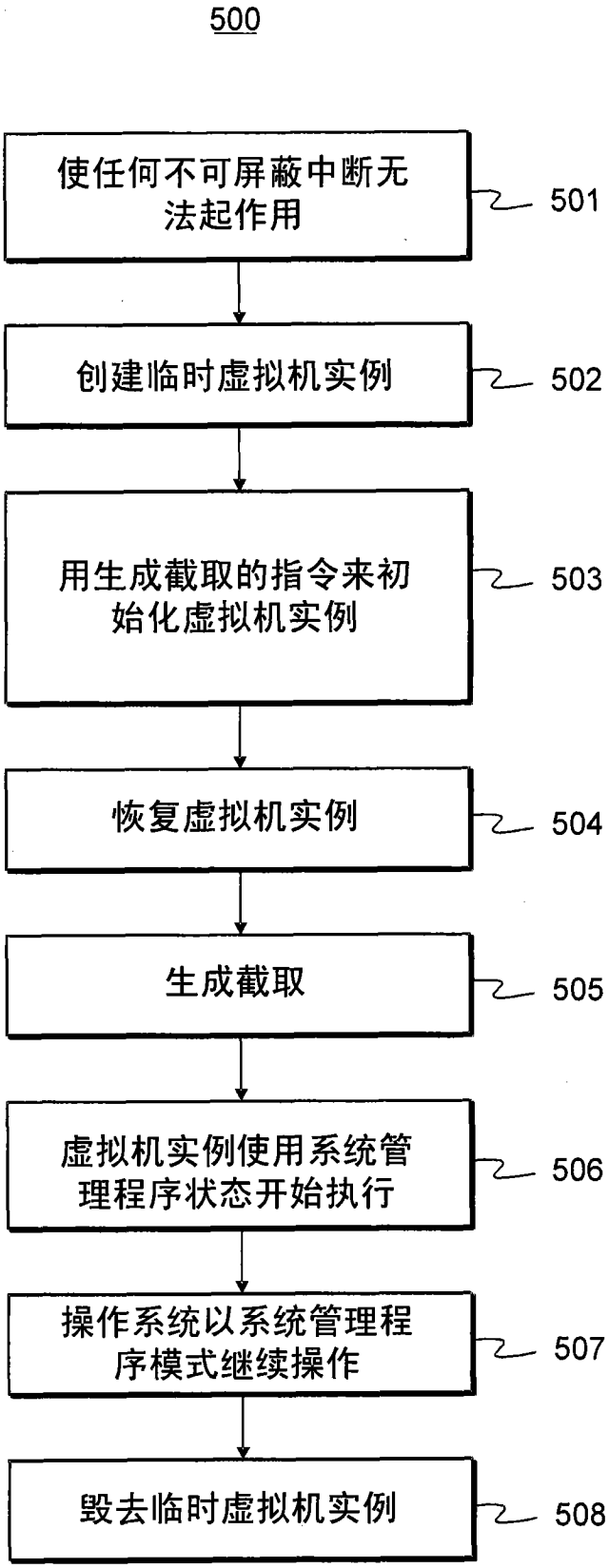

500
使任何不可屏蔽中断无法起作用
501
创建临时虚拟机实例
502
用生成截取的指令来初始化虚拟机实例
503
恢复虚拟机实例
504
生成截取
505
虚拟机实例使用系统管理程序状态开始执行
506
操作系统以系统管理程序模式继续操作
507
毁去临时虚拟机实例
508

图 5