(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103365702 A
(43)申请公布日 2013.10.23

(21)申请号 201310290430.7

(22)申请日 2013.07.11

(71)申请人 中国科学院合肥物质科学研究院
地址 230000 安徽省合肥市蜀山湖路 350 号

(72)发明人 崔超远 施智平 乌云 王儒敬

(74)专利代理机构 安徽汇朴律师事务所 34116
代理人 方荣肖

(51)Int.Cl.
G06F 9/455(2006.01)
G06F 9/50(2006.01)

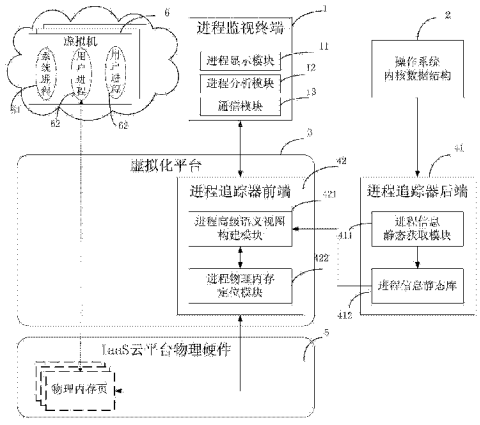
权利要求书2页 说明书7页 附图3页

(54)发明名称

IaaS 云环境下轻量级虚拟机进程追踪系统和方法

(57)摘要

本发明公开了 IaaS 云环境下轻量级虚拟机进程追踪系统和方法。所述追踪系统经由虚拟化平台从目标虚拟机外部实时追踪其内部进程，将进程追踪器分为进程追踪器后端和进程追踪器前端。在进程追踪启动前，预先构建进程追踪器后端进程信息库静态库。进程追踪开始后，在云平台虚拟化平台内部启动进程追踪器前端物理内存定位模块监视目标虚拟机内部事件，将从外部获得的硬件级字节信息还原为虚拟机内部的行为和事件特征，快速构建进程高级语义视图，实时捕获虚拟机内进程以及进程之间的关联关系。本发明无需在线解析操作系统内核，处理效率高，系统负荷小；当被监视虚拟机被入侵时，可保持对虚拟机的有效监控。



CN 103365702 A

1. IaaS 云环境下轻量级虚拟机进程追踪系统，包括进程监视终端和进程追踪器，所述进程监视终端通过有线或无线和云平台连接，其特征在于：

所述进程监视终端，包括通信模块和进程显示模块；

所述进程追踪器，包括进程追踪器前端和进程追踪器后端，功能上相互依存，实现上相互独立；

所述进程追踪器前端，嵌入到虚拟化平台内部，包括进程物理内存定位模块和进程高级语义视图构建模块；

所述进程追踪器后端，包括进程信息静态获取模块和进程信息静态库；

所述进程物理内存定位模块，用于在进程追踪任务启动之后，通过客户虚拟机的内核栈指针，定位当前进程控制块在所述客户虚拟机所依托宿主实体机的物理内存地址；

所述进程高级语义视图构建模块，用于根据所述进程物理内存定位模块获得的实体机物理内存地址，参照所述进程追踪器后端的进程信息静态库，解析物理内存，构建进程高级语义视图，还原所述客户虚拟机内部进程的语义内容；

所述进程信息静态获取模块，用于在所述进程追踪器前端启动之前执行并完成，解析客户虚拟机使用的操作系统的内核数据结构和进程控制块 PCB，获取描述进程的具体信息，并生成进程信息静态库，提供进程信息访问接口，所述描述进程的具体信息包括进程表示符、处理器状态、进程调度、进程控制；

所述进程信息静态库，用于接收来自所述进程追踪器前端传递的进程语义信息调用请求，并将请求处理结果向所述进程追踪器前端回复；

所述通信模块，用于向所述进程追踪器前端发出启动、挂起和停止的请求；接收所述进程追踪器前端返回的进程高级语义视图信息；

所述进程显示模块，用于显示所述进程追踪器前端返回的进程高级语义视图信息。

2. 根据权利要求 1 所述的 IaaS 云环境下轻量级虚拟机进程追踪系统：所述进程追踪器后端所在的操作系统为 Windows 或者 Linux。

3. 根据权利要求 1 所述的 IaaS 云环境下轻量级虚拟机进程追踪系统：所述进程监视终端还包括进程分析模块，用于分析进程对云平台整体以及客户机本身运行带来的影响。

4. 如权利要求 3 所述的 IaaS 云环境下轻量级虚拟机进程追踪系统的追踪方法，其特征在于：所述追踪方法包括进程监终端追踪 IaaS 云平台上客户虚拟机操作系统中任务所对应的进程的步骤：

步骤 101，启动进程追踪器的进程追踪器后端，针对虚拟机被采用的操作系统，解析所述操作系统的内核数据结构及进程控制块，生成描述进程信息的访问函数，构建进程信息静态库，该描述进程信息的访问函数包括进程描述信息调用接口、系统变量访问接口、系统调用和中断访问接口；

步骤 102，通过进程监视终端提交进程追踪请求；

步骤 103，嵌入虚拟化平台内部的进程追踪器前端接到请求，启动追踪任务，扫描 IaaS 云平台上所有的虚拟机；

步骤 104，进程追踪器前端的进程物理内存定位模块通过客户虚拟机 CPU 的控制寄存器，获取当前虚拟机操作系统的内核堆栈指针 ESP；进而定位当前客户虚拟机当前进程的进程控制块 PCB 的虚拟机的虚拟地址 GVA；

步骤 105，根据通过虚拟化平台的影子页表将虚拟机的虚拟地址 GVA 转化为宿主机物理地址 HPA ；

步骤 106，函数 API 实时调用进程追踪器后端进程信息静态库中的数据，进程追踪器前端进程高级语义视图构建模块开始解析 HPA，将 HPA 对应的硬件字节信息还原为客户虚拟机内部进程描述信息，该解析过程需要遍历进程控制块链表和进程树，将进程控制块 PCB 所对应的 HPA 传递给进程追踪器后端预先生成的进程信息静态库，获取当前进程所对应的进程号、进程名称 ；

步骤 107，搜索当前客户虚拟机的相邻的进程节点，判断是否存在相邻进程节点，若存在，进入步骤 104 ；若不存在，进入步骤 108 ；解析一台虚拟机的正在运行和待运行的所有进程信息 ；

步骤 108，搜索 IaaS 云平台上的其他客户虚拟机，判断是否存其他客户虚拟机，进入步骤 104 ；若不存在，进入步骤 109，解析 IaaS 云平台上的所有客户虚拟机的正在运行和待运行进程信息 ；

步骤 109，进程追踪器前端根据进程监视终端的请求，将解析结果传递到进程监视终端，供进程监视终端分析或显示用。

IaaS 云环境下轻量级虚拟机进程追踪系统和方法

技术领域

[0001] 本发明涉及 IaaS 云计算领域，特别涉及一种 IaaS 云环境下轻量级虚拟机内部进程追踪系统和方法。

背景技术

[0002] IaaS 云计算是一种将计算机基础设施资源通过互联网为用户提供服务的新型计算模式和商业模式。虚拟化作为支撑 IaaS 云模式的关键技术，通过对 CPU、内存、硬盘存储器等硬件的聚合和再分配，构建一个物理上异地分布、逻辑上单一呈现、功能上弹性伸缩的云环境，以虚拟机的形式响应用户的业务需求。云计算降低了资源使用者和资源实体之间的耦合程度，便于维护和管理，可以降低基础设施的运营成本，受到学术界和产业界的广泛关注，并且在许多行业得到应用和推广。

[0003] IaaS 云计算整合了大量计算机资源，为用户提供了资源无限利用的可能性。但是，资源规模的增大也产生了两个问题，即资源合理利用和资源安全利用的问题。

[0004] 首先，大规模资源如果不能合理分配和管理必然导致云提供商经济效益降低。目前，大多数数据中心的资源分配都是静态的，在申请时预先配置一定数量的设备，容易造成过度配置资源和过低配置资源两种极端情况。要实现资源优化，必须能够监视和预测用户资源的实时动态变化，根据负载的轻重程度追加或释放相关资源以达到提高资源使用效率和提高服务质量并降低成本的目标。业界现已提供的监视工具都是虚拟机系统级别的，这些工具的检测、管理粒度太大，不能确切地反映虚拟机的行为，只有进行细粒度进程级别的监视，才能准确把握操作系统的具体行为，进而判断虚拟机正在执行和将要执行的作业，正在消费和将要消费的资源，为资源优化提供量化的判断依据。

[0005] 其次，资源安全利用是云计算能否推广和普及的根本。那些规模庞大的基础设施除了被用于合法业务外，还同样可能为非法需求提供计算的可能性。例如，2011 年 4 月侵入索尼 PlayStation 游戏网络的黑客使用了亚马逊弹性计算云来破解一些加密密钥，从而窃取了数万用户的信用卡信息。云计算系统使有关部门和企业难于追查数字犯罪，一个主要原因是由于使用虚拟化技术导致的。用户租用的虚拟机可能实际上分布在云提供商数据中心内十几个甚至更多实体内存和实体硬盘驱动器上。假如一台虚拟机被关闭，它占用的存储空间很快就会被回收，犯罪信息就被随后的合法用户数据抹去，对数字犯罪的追踪也无从进行。因此，迫切需要一套虚拟机实时安全监视的解决方案，为 IaaS 云环境下虚拟机安全问题提供理论与方法支持。

[0006] IaaS 模式下关于虚拟机监视的技术和系统，主要集中在两个方面，即从虚拟机内部或外部进行检测。

[0007] 内部检测工具运行在被监视系统的内部，能够直接获取内核结构、进程、系统调用等高级语义信息，拥有高可见性，便于分析资源使用情况或判断安全状况。缺点是不仅会加重虚拟机运行负荷，还会由于因系统被攻击导致内部监控工具会暴露在攻击者的控制之下，获取不到系统的任何信息，甚至根本无法启动任何监控程序，不能发挥正常的监视功

能。

[0008] 外部检测工具运行在特权虚拟机或虚拟化平台上。现有技术中，有针对虚拟机进程识别的方法。2007 年，中国专利 200710118186.0 公开了一种虚拟机监视器识别客户操作系统中进程的方法和装置，它通过在进程切换时，由虚拟机监视器记录待运行进程页表信息和当前运行进程的标识信息来识别进程。该方法在实现过程中需要记录待运行进程和当前运行进程的上下文信息，如果面向云计算环境下数量庞大的用户和频繁的多任务作业时，这一方法会产生巨大的系统消耗，从而影响云平台的整体性能。2008 年，中国专利 200910237996.7 提供了一种通过虚拟机运行中应用程序的同步感知对虚拟机进行分类的技术，其中同步感知的方法也可以用于进程识别。但是，该方法在虚拟机进程识别时，需要反复解析每台虚拟机内核中的 task_struct 结构来获取进程信息，实时操作性差；而且这一方法在多用户多任务 IaaS 客户机时，重复解析 task_struct 结构会加重云平台的整体负荷。

[0009] 目前现有技术中，从虚拟机外部进行进程追踪的技术，功能上都可以识别运行中进程信息，但都需要实时解析不同操作系统内核数据结构，因此进程追踪不仅系统开销都很大，而且可移植性也不强。如果将这些技术用在 IaaS 云环境下的虚拟机监视，不仅要面对成千上万的虚拟客户机实例，还必须考虑不同类型不同版本的虚拟机操作系统内核结构，频繁进行在线实时内核解析将成为一项繁重而耗时的工作，必然会影响云平台的整体运行性能。因此这些技术都不易被接受和推广。

发明内容

[0010] 本发明正是针对现有技术的不足，提供一种 IaaS 云环境下轻量级虚拟机内部进程追踪的系统和方法。

[0011] 本发明是这样实现的，基于 IaaS 云环境下轻量级虚拟机进程追踪系统，包括进程监视终端、虚拟化平台和进程追踪器，所述进程监视终端通过有线或无线和云平台连接，其中，所述进程监视终端，包括通信模块和进程显示模块；所述进程追踪器，包括进程追踪器前端和进程追踪器后端，功能上相互依存，实现上相互独立；所述进程追踪器前端，嵌入到虚拟化平台内部，包括进程物理内存定位模块和进程高级语义视图构建模块；所述进程追踪器后端，包括进程信息静态获取模块和进程信息静态库；所述进程物理内存定位模块，用于在进程追踪任务启动之后，通过客户虚拟机的内核栈指针，定位当前进程控制块在所述客户虚拟机所依托宿主实体机的物理内存地址；所述进程高级语义视图构建模块，用于根据所述进程物理内存定位模块获得的实体机物理内存地址，参照所述进程追踪器后端的进程信息静态库，解析物理内存，构建进程高级语义视图，还原所述客户虚拟机内部进程的语义内容；所述进程信息静态获取模块，用于在所述进程追踪器前端启动之前执行并完成，解析客户虚拟机使用的操作系统的内核数据结构和进程控制块 PCB，获取描述进程的具体信息，并生成进程信息静态库，提供进程信息访问接口，所述描述进程的具体信息包括进程表示符、处理器状态、进程调度、进程控制；所述进程信息静态库，用于接收来自所述进程追踪器前端传递的进程语义信息调用请求，并将请求处理结果（即进程特定信息）向所述进程追踪器前端回复；所述通信模块，用于向所述进程追踪器前端发出启动、挂起和停止的请求；接收所述进程追踪器前端返回的进程高级语义视图信息；所述进程显示模块，用于显示所

述进程追踪器前端返回的进程高级语义视图信息。

[0012] 作为上述方案的进一步改进，所述进程追踪器后端所在的操作系统为 Windows 或者 Linux。

[0013] 作为上述方案的进一步改进，所述进程监视终端还包括进程分析模块，用于分析进程对云平台整体以及客户机本身运行带来的影响。

[0014] 本发明还提供上述 IaaS 云环境下轻量级虚拟机进程追踪系统的追踪方法，所述追踪方法包括进程监终端追踪 IaaS 云平台上客户虚拟机操作系统中任务所对应的进程的步骤：

[0015] 步骤 101，启动进程追踪器的进程追踪器后端，针对客户虚拟机被采用的操作系统，解析所述操作系统的内核数据结构及进程控制块，生成描述进程信息的访问函数，构建进程信息静态库，该描述进程信息的访问函数包括进程描述信息调用接口、系统变量访问接口、系统调用和中断访问接口；

[0016] 步骤 102，通过进程监视终端提交进程追踪请求；

[0017] 步骤 103，嵌入虚拟化平台内部的进程追踪器前端接到请求，启动追踪任务，扫描 IaaS 云平台上所有的客户虚拟机；

[0018] 步骤 104，进程追踪器前端的进程物理内存定位模块通过客户虚拟机 CPU 的控制寄存器，获取当前客户虚拟机操作系统的内核堆栈指针 ESP；进而定位当前客户虚拟机当前进程的进程控制块 PCB 的客户虚拟机的虚拟地址 GVA；

[0019] 步骤 105，根据通过虚拟化平台的影子页表将客户机虚拟机的虚拟地址 GVA 转化为宿主机物理地址 HPA；

[0020] 步骤 106，函数 API 实时调用进程追踪器后端进程信息静态库中的数据，进程追踪器前端进程高级语义视图构建模块开始解析 HPA，将 HPA 对应的硬件字节信息还原为客户虚拟机内部进程描述信息，该解析过程需要遍历进程控制块链表和进程树，将进程控制块 PCB 所对应的 HPA 传递给进程追踪器后端预先生成的进程信息静态库，获取当前进程所对应的进程号、进程名称；

[0021] 步骤 107，搜索当前客户虚拟机的相邻的进程节点，判断是否存在相邻进程节点，若存在，进入步骤 104；若不存在，进入步骤 108；解析一台虚拟机的正在运行和待运行的所有进程信息；

[0022] 步骤 108，搜索 IaaS 云平台上的其他客户虚拟机，判断是否存其他客户虚拟机，进入步骤 104；若不存在，进入步骤 109，解析 IaaS 云平台上的所有虚拟机的正在运行和待运行进程信息；

[0023] 步骤 109，进程追踪器前端根据进程监视终端的请求，将解析结果传递到进程监视终端，供进程监视终端分析或显示用。

[0024] 本发明相较于现有技术具有下列突出的优点和效果：

[0025] 本发明一种 IaaS 云环境下轻量级虚拟机内部进程追踪系统，将解析物理内存页和解析操作系统内核分开，进程追踪器分为进程追踪器前端和进程追踪器后端，进程追踪器后端用于预处理解析操作系统内核数据结构，进程追踪器前端用于实时解析宿主机物理内存，通过调用由进程追踪器后端生成的进程信息静态库，动态构建进程高级语义视图，进程追踪器前端在解析物理内存时，无需在线解析操作系统内核，处理效率高，系统负荷小，

是一种轻量级的追踪系统。

[0026] 本发明一种 IaaS 云环境下轻量级虚拟机内部进程追踪系统是一种细粒度的进程追踪系统，为 IaaS 云平台更准确的监控提供了可能。业界现已提供的成熟工具主要是虚拟机系统级别的，粒度大以至于不能够及时根据虚拟机的行为来采取补偿性甚至预测性的动作，如 Xen、KVM、VMware 只能监测到虚拟机操作系统类型、版本、运行状态机对应物理资源的信息，而不能提供虚拟机内部的任何信息。因此迫切需要一套细粒度，如模块、进程级别的虚拟机运维系统及工具。

[0027] 本发明的一种 IaaS 云环境下轻量级虚拟机内部进程追踪系统是一种从虚拟机外部监视虚拟机内部进程的系统，进程追踪模块嵌入到虚拟化平台中，在保持对被监视虚拟客户机高可见性的同时，保持着与被监控系统很好的隔离度。即使在被监控虚拟机被攻击者成功入侵的情况下，依然能够免于受到攻击的影响，保持对虚拟机有效的监控。

[0028] 本发明的一种 IaaS 云环境下轻量级虚拟机内部进程追踪方法是一种进程追踪模块化设计方法，进程追踪器后端预处理模块可针对任何操作系统，如 Windows、Linux 等，和任何虚拟化平台，如 Xen、KVM、Vmware 等，可移植性强，不仅可用于小型虚拟化平台，也可用于 IaaS 大型云平台，如 Eucalyptus、OpenStack 等架构，特别是用在大型 IaaS 平台下，更能体现出本发明的效果和效率。

[0029] 本发明的一种 IaaS 云环境下轻量级虚拟机内部进程追踪系统，提出”分别编译、组合链接”的实现方式，采用模块设计方案，在实施时避免了代码融合带来的定义冲突，限定了排错范围，使得进程追踪器的可移植性和复用性大大增强。

附图说明

[0030] 图 1 为本发明较佳实施方式提供的 IaaS 云环境下轻量级虚拟机内部进程追踪系统的体系结构框图。

[0031] 图 2 为本发明进程追踪器的进程追踪器前端和进程追踪器后端实施例示意图。

[0032] 图 3 为本发明的进程追踪器的扫描流程图。

具体实施方式

[0033] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0034] 如图 1 所示的较佳实施方式提供的 IaaS 云环境下轻量级虚拟机内部进程追踪系统的体系结构框图。

[0035] 所述基于 IaaS 云环境下轻量级虚拟机进程追踪系统包括进程追踪器、虚拟化平台 3 和进程监视终端 1。

[0036] 虚拟化平台 3 对 IaaS 云平台物理硬件 5 的物理内存页 2 进行管理，负责对对虚拟机提供硬件资源抽象，分配和管理这些资源，同时为其上运行的虚拟机 6 的操作系统提供硬件环境。虚拟化平台 3 根据实际需要将 IaaS 云平台物理硬件集合成一台虚拟机 6，或分配成多台虚拟机 6，虚拟机 6 有独立的系统进程 61 和至少一个用户进程 62。

[0037] 进程监视终端 1 包括通信模块 13、进程分析模块 12 和进程显示模块 11。

[0038] 进程追踪器包括进程追踪器前端 42 和进程追踪器后端 41，功能上相互依存，实现上相互独立。

[0039] 进程追踪器前端 42 嵌入虚拟化平台 3 的内部，利用虚拟化平台 3 对硬件和虚拟机的控制实现物理内存定位和解析。进程追踪器前端 42 包括进程物理内存定位模块 422 和进程高级语义视图构建模块 421。

[0040] 进程追踪器后端 41 位于虚拟化平台 3 的外部，架构上独立于虚拟化平台 3 包括进程信息静态获取模块 411 和进程信息静态库 412。

[0041] 所述进程物理内存定位模块 422 用于在进程追踪任务启动之后，通过虚拟机 6 的内核栈指针，定位当前进程控制块在虚拟机 6 所依托宿主实体机的物理内存页地址。

[0042] 进程高级语义视图构建模块 421 用于根据进程物理内存定位模块获得的实体机物理内存地址，参照进程追踪器后端 41 的进程信息静态库 412，解析物理内存，构建进程高级语义视图，还原虚拟机 6 内部进程的语义内容。

[0043] 进程信息静态获取模块 411 用于在进程追踪器前端 42 启动之前执行并完成，解析虚拟机 6 使用的操作系统的内核数据结构和进程控制块 PCB，获取进程表示符、处理器状态、进程调度、进程控制等描述进程的具体信息，并生成进程信息静态库，提供进程信息访问接口。

[0044] 进程信息静态库 412 用于接收和处理来自进程追踪器前端 42 传递的进程语义信息调用请求，并将进程号、进程状态等进程特定信息反馈给进程追踪器前端 42。

[0045] 通信模块 13 用于向进程追踪器前端 42 发送启动、挂起和停止的业务请求，并接收其实时构建的进程高级语义视图；进程分析模块 12 用于解析进程描述信息，如针对资源优化策略和系统安全策略等具体需求，分析进程对云平台整体以及客户机本身运行带来的影响；进程显示模块 11 用于显示所述进程追踪器前端 42 返回的进程高级语义视图信息，如进程 ID、进程名称、运行状态以及进程上下文信息等内容。

[0046] IaaS 云环境下轻量级虚拟机内部进程追踪系统实现从虚拟化平台 3 外部实时追踪虚拟化平台 3 内部虚拟机 6 的进程，将进程追踪器分为进程追踪器后端 41 和进程追踪器前端 42，在进程追踪启动前，预先构建进程追踪器后端 41 进程信息库静态库 412。进程追踪开始后，在云虚拟化平台 3 内部启动进程追踪器前端 42 物理内存定位模块 422 监视虚拟机 6 内部事件，将从外部获得的硬件级字节信息还原为虚拟机内部的行为和事件特征，快速构建进程高级语义视图，实时捕获虚拟机 6 的进程以及进程之间的关联关系。

[0047] 如图 2 所示的进程追踪器的进程追踪器前端和进程追踪器后端实施例示意图。

[0048] 进程追踪器的进程追踪器前端包括进程物理内存定位模块(hpa_location.c)、进程高级语义视图构建模块(hpa_analyzer.c)、用来声明在进程追踪器前端中要使用到的接口服务函数的一个 feedback.h 头文件、Makefile 和 Xen。Xen 源码没有引入任何来自操作系统内核源代码，进程追踪器前端嵌入虚拟化平台，完全不影响虚拟化平台的任何功能。

[0049] 进程追踪器的进程追踪器后端，有一个或多个“Feedback_X.c”，如 Feedback_Ubuntu.c、Feedback_Debian.c、Feedback_Fedora.c、Feedback_Centos.c、Feedback_Opensuse.c、Feedback_WinXP.c、Feedback_X.c 等。根据虚拟机的特定操作系统种类和内核版本来单独编译，按需作为进程追踪器前端的服务容器，数量上按需增减且不影响已有其它进程追踪器后端模块的工作，即该方法具有一定程度上的普适性和可扩展性；

[0050] 进程追踪器前端和进程追踪器后端的分工明确，进程追踪器前端模块只有一个，进程追踪器后端模块离线生成且按需增减，该方法保证进程追踪器轻量性的前提条件。

[0051] 如图 3 所示的较佳实施方式提供的 IaaS 云环境下轻量级虚拟机的进程追踪器扫描流程图。

[0052] 进程追踪器后端流程必须在执行虚拟机扫描前启动并完成相关操作。进程追踪器后端开始 301- 结束 305 中间包括流程：步骤 302，解析客户虚拟机操作系统内核数据结构；步骤 303，获取进程描述信息；步骤 304 建立进程信息静态库。生成的进程信息静态库供进程追踪器前端调用。

[0053] 进程追踪器前端开始的步骤 311- 结束的步骤 323 是进程追踪器前端接到进程监视终端的指令后，开始扫描虚拟机的详细过程。步骤 312-322 扫描 Iaas 云平台下所有虚拟机；步骤 313-317 首先定位包含进程详细信息的进程描述符所对应的物理内存页；步骤 313-321 是构建进程高级语义视图的详细过程；步骤 319 通过当前进程节点 task_struct 的成员 tasks 搜索与与其相邻的进程节点，获取其相邻节点 task_struct 的客户机虚拟地址，以此遍历所有进程。

[0054] 本实施例展示了虚拟机操作系统为 Linux 的进程追踪。追踪步骤具体如下：

[0055] 1、启动进程追踪器后端 41 的步骤 301-305，针对虚拟机 6 被采用的操作系统，解析其内核数据结构及进程控制块，生成进程描述信息调用接口、系统变量访问接口、系统调用和中断访问接口等描述进程信息的访问函数，构建进程信息静态库 412。

[0056] 2、云管理员通过进程监视终端 1 提交进程追踪请求；

[0057] 3、嵌入虚拟化平台 3 内部的进程追踪器前端 42 接到请求，执行步骤 311，启动追踪任务；执行步骤 312，扫描 IaaS 云平台上所有的虚拟机 6；

[0058] 4、即执行步骤 313，读取目标虚拟机内核堆栈指针 ESP，进程追踪器前端 42 的进程物理内存定位模块 422 通过虚拟机 6 的 CPU 的控制寄存器，获取当前虚拟机操作系统的内核堆栈指针 ESP；执行步骤 314，换算出结构体 thread_info 的客户机虚拟地址；执行步骤 315，定位 thread_info 的宿主机物理地址。thread_info 是位于进程内核栈栈底或栈顶(根据栈的增长方向)的一个结构体，它的成员 task 指向进程描述符 task_struct，进而定位当前虚拟机 6 的当前进程的进程控制块 PCB 的虚拟机 6 的虚拟地址 GVA；

[0059] 5、执行步骤 316 获取 task_struct 虚拟机机虚拟地址 GVA；执行步骤 317 定位 task_struct 物理地址，根据通过虚拟化平台 3 的影子页表将虚拟机 6 的虚拟地址 GVA 转化为宿主机物理地址 HPA；

[0060] 6、执行步骤 318，进程追踪器后端 41 调用函数 API 实时调用步骤 304 进程追踪器后端 41 生成的进程信息静态库 412 中的数据，进程追踪器前端 42 的进程高级语义视图构建模块 421 开始解析 HPA，将 HPA 对应的硬件字节信息还原为虚拟机 6 内部进程描述信息，该解析过程需要遍历进程控制块链表和进程树，将进程控制块 PCB 所对应的 HPA 传递给进程追踪器后端 41 预先生成的进程信息静态库 412，获取当前进程所对应的进程号、进程名称等；

[0061] 7、执行步骤 319，通过成员 tasks 搜索相进程节点，执行步骤 320，获取相进程节点 task_struct 的虚拟机 6 地址；执行步骤 321，判断是否完成所有节点搜素；若完成，执行步骤 322；若未完成，返回步骤 317；解析一台虚拟机的正在运行和待运行的所有进程信息；

[0062] 8、搜索 IaaS 云平台上的其他虚拟机，执行步骤 322，判断是否完成所有虚拟机扫描，若完成，进入步骤 9；若未完成，返回步骤 317，解析 IaaS 云平台上的所有客户虚拟机的正在运行和待运行进程信息；

[0063] 9、当步骤 322 判断完成所有虚拟机扫描时，进程追踪器前端 42 根据进程监视终端 1 的请求，将解析结果传递到进程监视终端 1，供进程监视终端 1 分析或显示用。

[0064] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

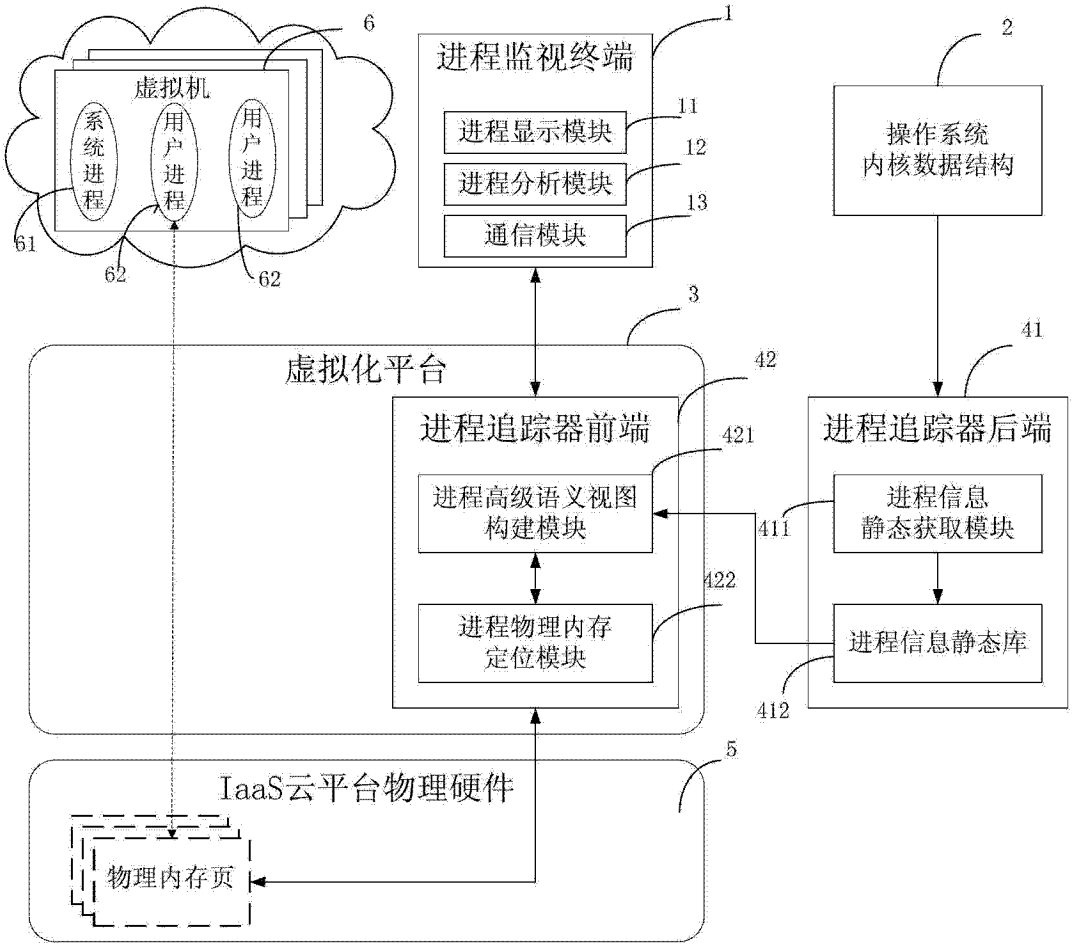

6
虚拟机
系统进程
用户进程
用户进程
61
62
62
进程监视终端
1
进程显示模块
11
进程分析模块
12
通信模块
13
2
操作系统
内核数据结构
3
虚拟化平台
42
进程追踪器前端
421
进程高级语义视图构建模块
422
进程物理内存定位模块
41
进程追踪器后端
411
进程信息静态获取模块
进程信息静态库
412
5
IaaS云平台物理硬件
物理内存页

图 1

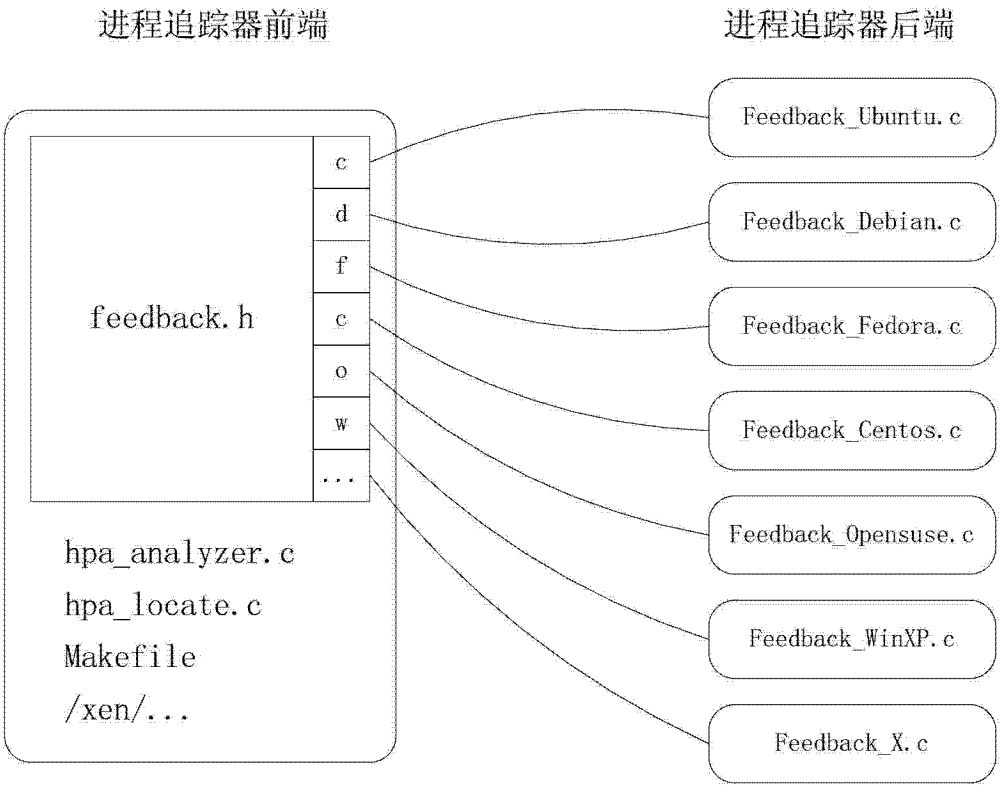

进程追踪器前端
进程追踪器后端
feedback.h
c
d
f
c
o
w
...
hpa_analyzer.c
hpa_locate.c
Makefile
/xen/...
Feedback_Ubuntu.c
Feedback_Debian.c
Feedback_Fedora.c
Feedback_Centos.c
Feedback_Opensuse.c
Feedback_WinXP.c
Feedback_X.c

图 2

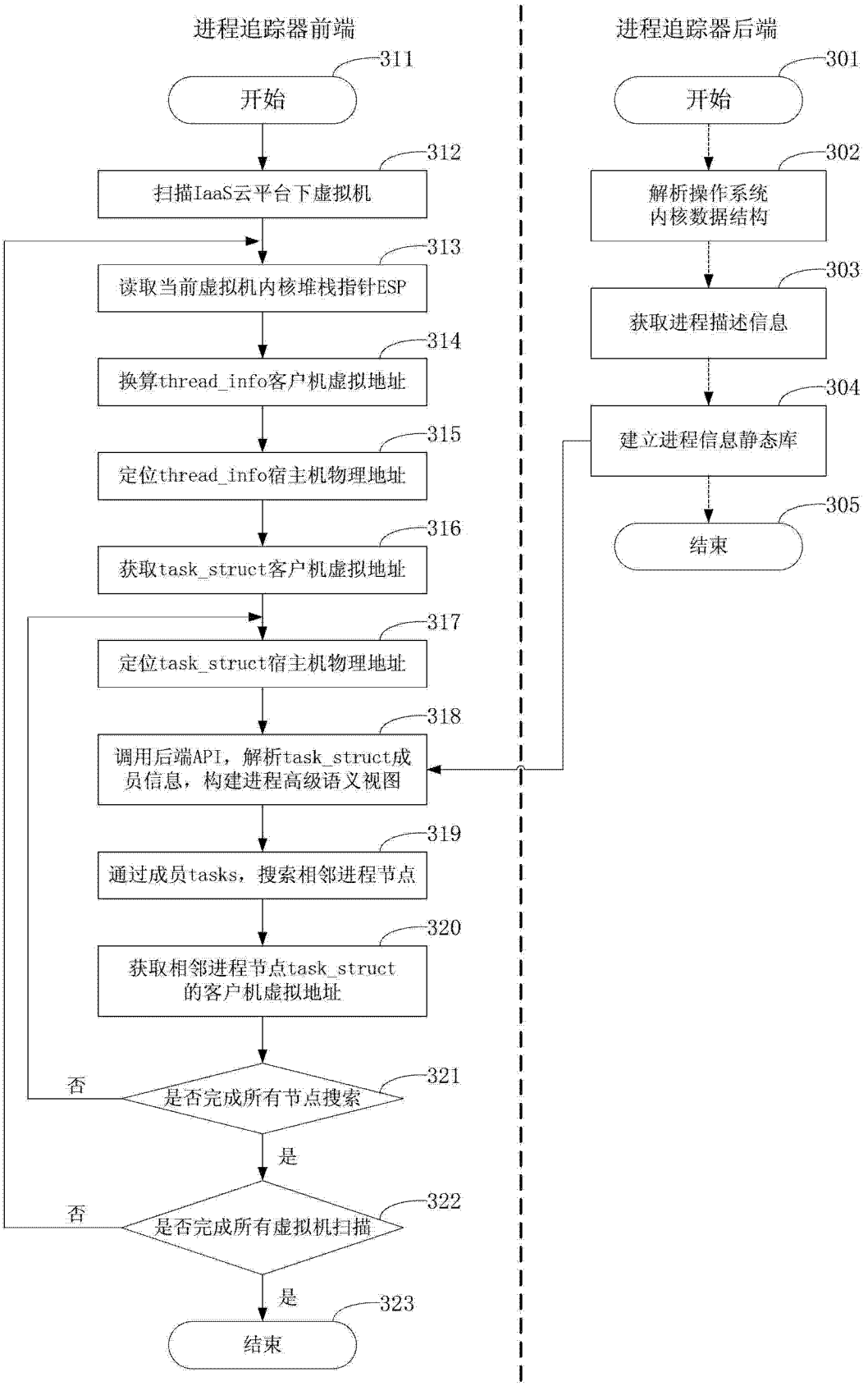

进程追踪器前端
进程追踪器后端
311
开始
312
扫描IaaS云平台下虚拟机
313
读取当前虚拟机内核堆栈指针ESP
314
换算thread_info客户机虚拟地址
315
定位thread_info宿主机物理地址
316
获取task_struct客户机虚拟地址
317
定位task_struct宿主机物理地址
318
调用后端API，解析task_struct成员信息，构建进程高级语义视图
319
通过成员tasks，搜索相邻进程节点
320
获取相邻进程节点task_struct的客户机虚拟地址
321
是否完成所有节点搜索
否
是
322
是否完成所有虚拟机扫描
否
是
323
结束
301
开始
302
解析操作系统内核数据结构
303
获取进程描述信息
304
建立进程信息静态库
305
结束

图 3