

说明书

用于云计算的安全扫描方法、相关设备及存储介质

本公开要求于 2023 年 10 月 08 日提交中国专利局、申请号为 202311296787.6、申请名称为“用于云计算的安全扫描方法、相关设备及存储介质”的中国专利申请的优先权，其全部内
5 容通过引用结合在本公开中。

技术领域

本公开涉及云计算技术领域，尤其涉及一种用于云计算的安全扫描方法、相关设备
10 及存储介质。

背景技术

随着云计算技术的快速发展，以虚拟机（VM）为形态的云计算实例已经成为了现代化数据中心的核
心技术之一。随着云计算实例数量的增加，主机安全（Host Security）成为了云上安全对抗的重要场
景。在主机安全中，对主机的磁盘扫描是检测云计算实例对主机是否存在攻击行为，以及收集
15 恶意样本、还原攻击路径的重要信息收集手段。

业界的磁盘扫描方式主要包括带内代理扫描方式，即将用于磁盘扫描的代理程序内置在云计算实例内部来完成磁盘扫描动作，具有扫描效率高的优势。但是，由于用于扫描磁
盘的代理程序和云计算实例的进程、内核等运行在同一计算环境内，一方面容易受到入侵行为的影
响，另一方面也会侵占原本云计算实例的计算资源。
20

发明内容

本公开的多个方面提供一种用于云计算的安全扫描方法、相关设备及存储介质，使得安全扫描程序不易受到虚拟化实例内部进程的入侵干扰，也不会占用虚拟化实例的计算资源。

本公开实施例提供一种主机设备，主机设备上部署有虚拟化管理器和被虚拟化管理器管理的第一虚拟化实例，第一虚拟化实例具有目标物理存储空间，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作；虚拟化管理器，还用于在确定第一虚拟化实例使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给
25 安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描；其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作，所述共享队列不同于所述至少一个存储队列。
30

本公开实施例还提供一种用于云计算的安全扫描方法，应用于主机设备上的虚拟化管理器，虚拟化管理器管理主机设备上的第一虚拟化实例，该方法包括：在第一虚拟化实例

使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；第一虚拟化实例具有目标物理存储空间，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作；基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描；其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作，所述共享队列不同于所述至少一个存储队列。

本公开实施例还提供一种用于云计算的安全扫描方法，应用第一虚拟化实例外部的安全扫描程序，方法包括：在第一虚拟化实例对应的虚拟化管理器为安全扫描程序创建共享队列和共享内存的情况下，向共享队列写入读请求，以供虚拟化管理器基于读请求，从第一虚拟化实例的目标物理存储空间中读取目标数据，并将目标数据写入共享内存；从共享内存中读取目标数据，以及根据目标数据进行安全扫描；其中，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作，所述共享队列不同于所述至少一个存储队列。

本公开实施例还提供一种虚拟化管理装置，可作为主机设备中的虚拟化管理器实现，用于管理第一虚拟化实例，该装置包括：创建模块和提供模块；创建模块，用于在第一虚拟化实例使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；第一虚拟化实例具有目标物理存储空间，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作；提供模块，用于基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描；其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作，所述共享队列不同于所述至少一个存储队列。

本公开实施例还提供一种主机设备，包括存储器和处理器，存储器中存储有安全扫描程序，处理器，与存储器耦合，用于执行安全扫描程序，以实现本公开实施例提供的用于云计算的安全扫描方法中的步骤。

本公开实施例还提供一种存储有计算机程序的计算机可读存储介质，当计算机程序被处理器执行时，致使处理器实现本公开实施例提供的用于云计算的安全扫描方法中的各步骤。

本公开实施例提供一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述内用于云计算的安全扫描方法中的步骤。

在本公开实施例中，虚拟化实例的物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作，基于此，通过对虚拟化管理器进行功能拓展，虚拟化管理器除了为虚拟化实例创建对物理存储空间进行读写操作所需的存储队列之外，还能够为位于虚拟化实例外部的安全扫描程序创建共享队列和共享内存，进而基于共享队列和

共享内存能够将该物理存储空间中的数据提供给安全扫描程序，使得安全扫描程序能够基于虚拟化实例的物理存储空间中的数据进行主机安全扫描。由于安全扫描程序位于虚拟化实例外部，不易受到虚拟化实例内部进程的入侵干扰，也不会占用虚拟化实例的计算资源。另外，基于虚拟化实例的物理存储空间中的数据进行主机安全扫描，
5 能够做到实时、高效的扫描，能够对即时发生的入侵行为进行快速响应。

附图说明

此处所说明的附图用来提供对本公开的进一步理解，构成本公开的一部分，本公开的示意性实施例及其说明用于解释本公开，并不构成对本公开的不当限定。在附图
10 中：

- 图 1a 为本公开示例性实施例提供的主机设备的结构示意图；
- 图 1b 为本公开示例性实施例提供的主机设备和其它设备的结构示意图；
- 图 2 为本公开示例性实施例提供的另一种主机设备和安全扫描程序的结构示意图；
- 图 3 为本公开示例性实施例提供的另一种主机设备和安全扫描程序的内部结构示
15 意图；
- 图 4 为本公开示例性实施例提供的一种用于云计算的安全扫描方法的流程示意图；
- 图 5 为本公开示例性实施例提供的另一种用于云计算的安全扫描方法的流程示意图；
- 图 6 为本公开示例性实施例提供的一种虚拟化管理装置的结构示意图；
- 20 图 7 为本公开示例性实施例提供的一种主机设备的结构示意图。

具体实施方式

为使本公开的目的、技术方案和优点更加清楚，下面将结合本公开具体实施例及相应的附图对本公开技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本
25 公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范
围。

需要说明的是，本公开所涉及的用户信息（包括但不限于用户设备信息、用户个人信息等）和数据（包括但不限于用于分析的数据、存储的数据、展示的数据等），
30 均为经用户授权或者经过各方充分授权的信息和数据，并且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准，并提供有相应的操作入口，供
用户选择授权或者拒绝。

针对现有技术存在的问题，本公开实施例提供一种用于云计算的安全扫描方案，结合物理存储（如磁盘）读写时的多队列设计，利用虚拟化内存共享和物理存储（如
35 磁盘）协议的设计，将虚拟化实例的物理存储空间中的数据通过虚拟化方式共享给虚

拟化实例外部的安全扫描程序，供其进行安全扫描。

具体地，在本公开实施例中，虚拟化实例的物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作，基于此，通过对虚拟化管理器进行功能拓展，虚拟化管理器除了为虚拟化实例创建对物理存储空间进行读写操作所需的存储队列之外，还能够为位于虚拟化实例外部的安全扫描程序创建共享队列和共享内存，进而基于共享队列和共享内存能够将该物理存储空间中的数据提供给虚拟化实例外部的安全扫描程序，使其进行主机安全扫描。由于安全扫描程序位于虚拟化实例外部，不易受到虚拟化实例内部进程的入侵干扰，具有较好的隐藏性，也不会占用虚拟化实例的计算资源。另外，基于虚拟化实例的物理存储空间中的数据进行主机安全扫描，能够做到实时、高效的扫描，能够对即时发生的入侵行为进行快速响应，具有较高的时效性。

以下结合附图，对本公开实施例提供的一种解决方案进行详细说明。

图 1a 为本公开示例性实施例提供的主机设备的结构示意图。如图 1a 所示，该主机设备 101 上部署有虚拟化管理器 102 和被虚拟化管理器 102 管理的虚拟化实例 103。

在本实施例中，主机设备 101 可以是任何能够提供硬件资源的物理设备，例如可以是手机、笔记本、存储设备、传统服务器，也可以是云服务器、云主机等具有硬件资源的云端设备。在本实施例中，主机设备 101 负责提供虚拟化管理器 102 以及虚拟化实例运行所需的硬件资源，例如包括但不限于：处理器（Central Processing Unit, CPU）、存储器（例如内存）、网卡、持久存储器以及输入输出设备。

主机设备 101 不仅具有硬件资源，在硬件资源之上包括操作系统(Operating System, OS)，操作系统之上运行有虚拟化管理器 102。虚拟化管理器 102 用于在其所在主机设备上创建隔离运行环境，并在隔离运行环境中启动或创建以及管理虚拟化实例。虚拟化管理器 102 可以是任何能够在其所在主机设备上基于虚拟化技术创建隔离运行环境，并在隔离运行环境中启动或创建以及管理虚拟化实例的软件程序、组件或模块，虚拟化管理器 102 还可以对虚拟化实例提供独立的资源分配、访问控制和不同操作系统的支持。对此不做限定。可选地，虚拟化管理器 102 可以是虚拟机监视器（Virtual Machine Monitor, VMM），也可以称为 Hypervisor。可选地，Hypervisor 或 VMM 具体可实现为虚拟操作系统模拟器（Quick EMUlator, QEMU）或者 Vmware，但并不限于此。其中，虚拟化实例可以实现为云主机、弹性计算服务（Elastic Compute Service, ECS）、虚拟机（Virtual Machine, VM）或容器等。其中，一个虚拟化管理器 102 可以管理一个或多个虚拟化实例，每个虚拟化实例被一个虚拟化管理器 102 管理。在图 1a 中以一个虚拟化管理器对应一个虚拟化实例为例进行图示，但并不限于此。

在本实施例中，每个虚拟化管理器 102 对虚拟化实例进行管理的方式和过程相同或相似，在下面实施例中以其中任意一个虚拟化实例为例进行描述，为了便于区分和描述，将该任意一个虚拟化实例称为第一虚拟化实例 103。

在本实施例中，第一虚拟化实例提供隔离的运行环境，在该隔离的运行环境中可

以部署用户空间程序，用户空间程序也可以称为应用程序。除此之外，第一虚拟化实例具有目标物理存储空间，用于存储第一虚拟化实例 103 的操作系统、用户空间程序以及产生的各种数据。该目标物理存储空间是虚拟化管理器从主机设备的物理存储空间中为第一虚拟化实例分配的存储空间，主机设备的物理存储空间可以采用各种持久化存储介质，例如磁盘、闪存等。在后续实施例中，以主机设备的物理存储空间采用磁盘为例进行说明，但并不限于此；相应地，第一虚拟化实例分配到的目标物理存储空间也可以简称为第一虚拟化实例的磁盘空间。

在本实施例中，第一虚拟化实例中承载有用户空间程序，例如，社交类用户空间程序、购物类用户空间程序或者游戏类用户空间程序等；在运行用户空间程序的过程中会产生数据，需要将产生的数据写入目标物理存储空间中进行存储，当然，在用户空间程序启动或运行过程中也需要从目标物理存储空间中读取数据，这就涉及对目标物理存储控件的读写操作。为了实现对目标物理存储空间的读写操作，虚拟化管理器会针对目标物理存储空间创建存储设备，以及为第一虚拟化实例中的用户空间程序创建至少一个存储队列，其中，存储队列可以是在启动第一虚拟化实例的过程中由引导程序创建的。其中，虚拟化管理器可基于存储设备和至少一个存储队列，根据用户空间程序的读写请求，对目标物理存储空间以多队列读写方式进行读写操作，也就是说，目标物理存储空间支持虚拟化管理器以多队列读写方式对目标物理存储空间进行读写操作。其中，存储设备（例如，磁盘设备）可以是虚拟设备，也可以是物理存储设备。第一虚拟化实例中的用户空间程序将对目标物理存储空间的读写指令写入至少一个存储队列中的空闲存储队列中，至少一个存储队列的作用是接收并存储来自用户空间程序的读写指令，存储设备的作用之一是从至少一个存储队列中读取读写指令，根据所读取的读指令从目标物理存储空间中读取用户空间程序所需的数据，并将读取的数据返回给用户空间程序；以及根据所读取的写指令中的内存地址，从第一虚拟化实例的内存空间中读取相关数据，并将所读取的数据写入目标物理存储空间中。

下面结合图 2 所示的磁盘读写架构，介绍云计算场景中以多队列的方式进行磁盘读写的工作流程。在图 2 所示的磁盘读写架构中，涉及用户空间程序、第一虚拟化实例的目标物理存储空间（以磁盘空间为例）和目标物理存储空间对应的内核驱动（简称为磁盘的内核驱动）三部分。其中，磁盘的内核驱动属于第一虚拟化实例的操作系统。磁盘读写过程主要涉及三个步骤：①用户空间程序与该磁盘的内核驱动进行交互，通过磁盘的内核驱动向虚拟化管理器中的存储队列写入读写指令，并与磁盘设备（存储设备的示例）进行交互；②磁盘的内核驱动进一步包括核心协议模块和外设部件互连标准（Peripheral Component Interconnect, PCI）总线模块，核心协议模块通过 PCI 总线模块向存储对列中写入读写指令，并负责与磁盘设备进行交互；③由虚拟机管理器模拟的磁盘设备提供访问第一虚拟化实例的目标物理存储空间的能力。具体流程如下：

1) 用户空间程序基于第一虚拟化实例的操作系统调用访问文件系统，文件系统将针对目标物理存储空间的读写请求转发至内核驱动，由内核驱动和磁盘设备进行交互实现对目标物理存储空间的读写；

2) PCI 总线模块通过磁盘设备 IO 对目标物理存储空间进行命令控制，核心协议模块，分配内存空间，创建数据交互模块来进行协议命令的发送和执行结果的收集，最终完成对目标物理存储空间的数据传输。

3) 为提高 IO 数据交互效率，数据交互模块通常为多队列形式，例如，数据交互模块包括多个存储队列，PCI 总线模块将读写请求提交至任意空闲的存储队列中，并对任意返回了消息通知的存储队列进行处理，通过并发的方式提高 IO 效率。

4)、磁盘设备通过存储队列，提交读取目标物理存储空间上指定地址的命令，磁盘设备解析相应命令，将目标物理存储空间上指定地址的数据写入存储队列所指定的内存空间，并发送消息通知 PCI 总线模块读取相应数据。

随着云计算技术的快速发展，以虚拟机 (VM) 为形态的云计算实例已经成为了现代化数据中心的核心技术之一。随着云计算实例数量的增加,主机安全 (Host Security) 成为了云上安全对抗的重要场景。主机安全是基于对虚拟化实例的内存或磁盘等信息的收集和分析，对主机上的风险弱点、入侵行为进行检测的安全方法。在主机安全中，对主机的磁盘扫描是检测虚拟化实例对主机是否存在攻击行为，以及收集恶意样本、还原攻击路径的重要信息收集手段。

在本实施例中，创新性的在虚拟化外部提供安全扫描程序，借助于目标物理存储空间读写时的多队列设计，对虚拟化管理器进行功能拓展，使得虚拟化管理器可以配合第一虚拟化实例外部的安全扫描程序，针对第一虚拟化实例的目标物理存储空间中的数据进行主机安全扫描，保障主机设备的安全性。

其中，安全扫描程序 104 主要用于对第一虚拟化实例 103 的目标物理存储空间进行安全扫描。例如，第一虚拟化实例实现为虚拟机的情况下，安全扫描程序实现为虚拟机安全管理者 (Secure VM Supervisor)。

其中，安全扫描程序属于无代理扫描 (Agentless Scanning)，无代理扫描是虚拟机主机安全检测技术的一种技术分支。通过虚拟化技术提供的接口，无代理扫描能够无需在被扫描的虚拟化实例中安装任何代理软件的情况下，对虚拟化实例的运行状态进行收集和分析。无代理扫描能够避免虚拟化实例内对代理的拒绝服务攻击 (Denial of Service, DoS)、篡改行为的攻击，也不受网络连接要求或虚拟化实例自身性能影响、不需要考虑当下愈发复杂的入侵对抗防御手段，数据可信度、服务稳定性高。

其中，安全扫描程序的部署方式并不限定，安全扫描程序可以部署在第一虚拟化实例所在的主机设备上，与可以部署在与主机设备通信连接的其它设备上。可选地，安全扫描程序实现为部署在主机设备上的第二虚拟化实例，进一步，安全扫描程序实现为部署在主机设备上的第二虚拟化实例中的用户空间程序。第二虚拟化实例和第一

虚拟化实例可以由同一虚拟化模拟器管理，也可以由不同的虚拟化管理器进行管理。或者，安全扫描程序实现为其它设备上的第二虚拟化实例，进一步实现为其它设备上的第二虚拟化实例中的用户空间程序。当然，安全扫描程序也可以作为用户空间程序直接部署在第一虚拟化实例所在的主机设备上，或者其它设备上。在图 1a 以及图 2-3 中以安全扫描程序部署主机设备上为例进行图示，但并不限于此，在图 1b 中以安全扫描程序部署在与主机设备通信连接的其它设备上为例进行图示，但并不限于此。

在本实施例中，虚拟化管理器 102 在对目标存储空间以多队列的方式进行读写的情况下，除了为第一虚拟化实例 103 创建至少一个存储队列之外，还为位于第一虚拟化实例外部的安全扫描程序创建共享队列，以及共享内存，基于该共享队列和共享内存，以通常用户空间程序正常读取目标物理存储空间的方式，将该目标物理存储空间中的数据提供给安全扫描程序，使得安全扫描程序能够在第一虚拟化实例的操作系统以及用户空间程序无感知的情况下，基于第一虚拟化实例的目标物理存储空间中的数据进行主机安全扫描，保障主机设备以及第一虚拟化实例的安全性。由于安全扫描程序位于虚拟化实例外部，不易受到第一虚拟化实例内部进程的入侵干扰，也不会占用第一虚拟化实例的计算资源。

其中，共享队列的功能不同于至少一个存储队列的功能。共享队列主要将目标物理存储空间中的数据共享给安全扫描程序，以供安全扫描程序能够在第一虚拟化实例的操作系统以及用户空间程序无感知的情况下，基于第一虚拟化实例的目标物理存储空间中的数据进行主机安全扫描，保障主机设备以及第一虚拟化实例的安全性。存储队列主要是供第一虚拟化实例上的用户空间程序读写目标物理存储空间中的数据。

其中，在本实施例中，在不修改虚拟化实例的任何上层组件（例如，第一虚拟化实例的操作系统，及该操作系统之上的磁盘驱动、用户空间程序等）的前提下，在虚拟机管理器中对虚拟化实例的目标物理存储空间的数据通信进行截获，并将转发至安全扫描程序，完成对虚拟化实例的磁盘扫描工作。

另外，基于第一虚拟化实例的目标物理存储空间中的数据进行主机安全扫描，能够做到实时、高效的扫描，能够对即时发生的入侵行为进行快速响应。

另外，基于共享队列和共享内存将该目标物理存储空间中的数据提供给安全扫描程序，不需要对第一虚拟化实例的存储进行快照或磁盘镜像的留存，也就无需为这些磁盘镜像或快照提供存储空间，节省了存储空间，还能够保证主机安全扫描的效率。

进一步，利用云计算虚拟化的特性，对第一虚拟化实例上的操作系统、用户空间程序的操作以及存储设备有良好的带外控制，能够有效抵抗带内的入侵攻击干扰，同时对已可能发生的攻击行为有较好的隐蔽性，帮助安全人员更好地对入侵行为进行针对性检测和分析。

进一步，深度利用了云计算虚拟化的特性，可以将安全扫描程序封装在一个独立的虚拟化实例（如，VM）当中，通过特制的内核（kernel）驱动实现对其他虚拟化实

例的磁盘扫描，利用云计算虚拟机管理器对部署安全扫描程序的虚拟化实例的进行资源控制，限制安全扫描程序的计算资源消耗，并利用云计算方便实现的资源共享能力实现单安全扫描程序多虚拟化实例扫描对象的一对多扫描框架，可扩展性强。

在本实施例中，虚拟化管理器 102 为安全扫描程序创建共享队列的实施方式并不
5 限定，主要包括直接方式和间接方式，直接方式是指在由引导程序启动第一虚拟化实例之后，由虚拟化管理器 102 为安全扫描程序创建共享队列，间接方式是指在第一虚拟化实例启动过程中，由虚拟化管理器 102 控制引导程序为安全扫描程序创建共享队列。本公开实施例中的引导程序包括但不限于：基本输入输出系统（Basic Input Output System, BIOS）或统一可扩展固件接口（Unified Extensible Firmware Interface, UEFI）。

10 在一可选实施例中，直接方式：在虚拟化管理器 102 在第一虚拟化实例启动之后，为安全扫描程序创建共享队列的情况下，虚拟化管理器 102 采用 IO 虚拟化协议，为安全扫描程序创建共享队列，其中，IO 虚拟化协议是一种针对虚拟化平台的 IO 虚拟化技术，其提供了一种标准化的接口来实现虚拟化实例和宿主机之间的高性能、低开销的 IO 通信，其支持多队列，使得其可以同时处理多个 I/O 请求。基于 IO 虚拟化协议的
15 的磁盘读写方式可以通过虚拟机管理器，通过共享队列将第一虚拟化实例的磁盘数据映射到第一虚拟化实例外部的安全扫描程序来实现磁盘读写的共享，从而实现安全扫描程序对第一虚拟化实例的磁盘空间的扫描。具体地，虚拟化管理器 102 采用 IO 虚拟化协议的情况下，执行第一虚拟化实例对应的第一引导程序，以启动第一虚拟化实例，第一引导程序是启动虚拟化实例所需的引导程序，基于第一引导程序启动第一虚拟化
20 实例 103 的过程中未创建共享队列，在启动第一虚拟化实例之后，由虚拟化管理器 102 为安全扫描程序创建共享队列。可选地，IO 虚拟化协议可以实现为 Virtio 协议，Virtio 协议是一种针对虚拟化平台的 IO 虚拟化技术，属于虚拟化管理器 102 对磁盘的一种管理方式，Virtio 提供了一种标准化的接口来实现虚拟化实例与主机设备之间的高性能、低开销的 IO 通信。Virtio 支持多队列，同时处理多个 I/O 请求。在 Virtio 中，每个队
25 列都有自己的独立控制结构和缓冲区，可以与不同的处理器核心或线程相关联，从而实现并发处理。

在另一可选实施例中，间接方式：虚拟化管理器 102 在第一虚拟化实例启动过程中控制引导程序为安全扫描程序创建共享队列。直通的非易失性存储器快速通道
30 （Non-Volatile Memory Express, NVMe）协议是针对磁盘设备通信的一种协议，其能够满足对读写效率的高需求，NVMe 协议具备多队列、面向高速串行计算机扩展总线标准（PCI-express, PCIe）的设计，是当今快速块设备，尤其是固态硬盘设备充分发挥性能的协议更优选。支持 NVMe 协议的设备称为 NVMe 设备。NVMe 协议是磁盘固有的属性，需要虚拟化管理器的配合，对磁盘进行多队列读写操作或控制。基于设备直通的 NVMe 协议的
35 磁盘读写方式则可以通过目标物理存储空间所支持的多队列磁盘协议，创建多个存储队列，并通过共享队列将第一虚拟化实例的磁盘数据映射到第一虚拟化实例外部的安全扫描程

序来实现磁盘读写的共享，从而达到同样的效果。具体地，在采用基于设备直通的 NVMe 协议的情况下，对启动第一虚拟化实例的引导程序进行改进，使得改进后的第二启动程序可以在启动第一虚拟化实例的过程中创建共享队列；其中，第一引导程序与第二引导程序不同，虚拟化管理器执行第一虚拟化实例对应的第二引导程序，以启动第一虚拟化实例，并在启动过程中，由第二引导程序为安全扫描程序创建共享队列，创建共享队列之后，第二引导程序将对第一虚拟化实例的控制权返回给第一虚拟化实例的操作系统。其中，第二引导程序是独立于第一虚拟化实例的操作系统以及用户空间程序的一个独立软件。在云计算场景，第二引导程序由云厂商控制，第一虚拟化实例的操作系统和用户空间程序并不感知。

10 在此说明，无论是第一引导程序还是第二引导程序可视为是虚拟化管理器的一部分。

在一可选实施例中，无论是上述哪种创建共享队列的实施方式，虚拟化管理器创建共享内存的实施方式可以实现为：从第一虚拟化实例的内存中为安全扫描程序分配目标内存，并针对安全扫描程序设置目标内存为共享属性，以得到共享内存。

15 在一可选实施例中，虚拟化管理器基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序的实施方式并不限定。下面提供一种具体的实施方式：安全扫描程序在需要进行安全扫描的情况下，基于共享队列向虚拟化管理器发送读请求，例如，在共享队列中写入读请求。相应地，虚拟化管理器基于共享队列接收安全扫描程序发送的读请求，根据读请求，从目标物理存储空间中读取目标数据。例如，读请求中包含：第一虚拟化实例的目标物理存储空间的地址信息和数据长度，该地址信息为逻辑地址，磁盘设备对读请求进行解析，将读请求中的逻辑地址转换成物理地址，根据物理地址从目标存储空间中读取目标数据；将该目标数据写入共享内存中，以供安全扫描程序从共享内存中读取目标数据。例如，采用中断重转发机制，将目标数据写入共享内存之后，产生中断，不再将向用户空间程序发送通知信息，而是向安全扫描程序发送通知信息，以通知安全扫描程序从共享内存中读取目标数据进行安全扫描。

25 在本实施例中，第一虚拟化实例可以使用安全扫描服务，也可以不使用安全扫描服务，并不限定使用安全扫描服务的实施方式。在一可选实施例中，面向用户提供人机交互界面，用户可以在该人机交互界面上选择其购买的虚拟化实例是否使用安全扫描服务。针对第一虚拟化实例，在用户确定第一虚拟化实例使用安全扫描服务的情况下，虚拟化管理器可以获取第一虚拟化实例的配置信息，该配置信息中包括：第一虚拟化实例使用安全扫描服务的指示信息，根据指示信息确定第一虚拟化实例使用安全扫描服务，相应地，虚拟化管理器为第一虚拟化实例创建共享队列和共享内存。在另一可选实施例中，预先建立安全扫描程序与第一虚拟化实例之间的安全扫描服务绑定关系，安全扫描程序不断检测处于启动状态的虚拟化实例，向处于启动状态且与其建立有安全扫描服务绑定关系的虚拟化实例对应的虚拟化管理器发送指示创建共享队列

和共享内存的命令；虚拟化管理器接收该指示创建共享队列和共享内存的命令，在接收到命令的情况下，确定第一虚拟化实例使用安全扫描服务，并在启动虚拟化实例的过程中，通过第二引导程序为安全扫描程序创建共享队列，或者，在执行第一引导程序启动第一虚拟化实例之后，为安全扫描程序由虚拟化管理器创建共享队列。

5 在一可选实施例中，并不对虚拟化管理器的内部结构进行限定，下面示例性提供一种虚拟化管理器的内部结构，如图3所示，该虚拟化管理器102包括：创建模块102a、第一通信模块102b以及为第一虚拟化实例分配的存储设备102c。其中，存储设备对应于磁盘设备。

10 其中，创建模块102a在第一虚拟化实例使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存，并将共享队列和共享内存的地址信息提供给第一通信模块102b。

15 其中，第一通信模块102b负责与安全扫描程序进行通信，接收安全扫描程序发送的读请求，将读请求写入共享队列中，以供存储设备102c从共享队列中读取该读请求；其中，存储设备102c从共享队列中读取读请求，根据读请求从目标物理存储空间中读取目标数据，并将目标数据写入共享内存中。进一步，第一通信模块102b从共享内存中读取目标数据并将目标数据发送给安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描。

20 在此说明，存储设备102c除了从共享队列中读取读请求，根据读请求从目标物理存储空间中读取目标数据，并将目标数据写入共享内存中之外，还可以根据至少一个存储队列中来自第一虚拟化实例中用户空间程序的读写请求，对目标物理存储空间进行读写操作。存储设备102c可以定期轮询或者根据中断信号，从对应存储队列中获取来自用户空间程序的读请求或写请求，对于来自用户空间程序的读请求，从目标物理存储空间中获取用户空间程序所需读取的第一数据，并将该第一数据写入第一虚拟化实例的内存空间（非共享内存）中，并通过存储队列通知内核驱动读取该第一数据并将第一数据发送给用户空间程序；对于来自用户空间程序的写请求，从第一虚拟化实例的内存空间中获取用户空间程序所需写入的第二数据，将该第二数据写入目标物理存储空间中，并通过存储队列通知内核驱动写入完毕，由内核驱动通知用户空间程序已经将第二数据写入目标物理存储空间。其中，共享队列不同于至少一个存储队列。

25 相应地，本实施例还示例性提供一种安全扫描程序104的内部结构，如图3所示，该安全扫描程序104包括：第二通信模块104a、扫描模块104b和数据分析模块104c。

30 其中，数据分析模块104c响应安全扫描指令或事件，确定第一虚拟化实例的磁盘地址信息和数据长度。其中，可以设定实时扫描，实时产生安全扫描指令，或者设定扫描周期进行扫描，在扫描周期到达时生成安全扫描指令；其中，特定事件并不限定，例如可以是监测到目标物理存储空间发生写入事件。根据这些信息生成读请求并将读请求提供给扫描模块104b；扫描模块104b将该读请求提供给第二通信模块104a；由

第二通信模块 104a 将该读请求发送给第一通信模块 102b；第一通信模块 102b 接收安全扫描程序发送的读请求，将读请求写入共享队列中，以供存储设备 102c 从共享队列中读取该读请求；存储设备 102c 从共享队列中读取读请求，根据读请求从目标物理存储空间中读取目标数据，并将目标数据写入共享内存中；第一通信模块 102b 从共享内存中读取目标数据，将目标数据发送给第二通信模块 104a，第二通信模块 104a 将目标数据提供给扫描模块 104b，由扫描模块 104b 将目标数据提供给数据分析模块 104c。数据分析模块 104c 根据目标数据检测是否发生主机入侵行为，并在发生主机入侵行为的情况下，向用户进行告警。关于根据目标数据监测是否发生主机入侵行为的方式包括但不限于：确定目标数据中是否存在病毒库或风险库中的数据、确定目标数据中包含的日志信息是否被清空、确定目标数据中是否包含异常流程流量、确定目标数据中是否存在异常登录的账户等。

本方案提出的安全扫描方案能达到以下技术效果：

强时效性：通过与虚拟化实例内的共享队列进行交互，安全扫描程序以通常用户空间程序正常读取文件的方式获取目标数据并进行扫描，即时、针对性地对虚拟化实例中需要扫描的数据进行读取，而不需要将整个虚拟化实例的镜像或快照数据保存后再进行扫描，因此可以做到快速定位风险文件和溯源攻击行为。

资源隔离：利用云计算虚拟化的特性，本方案中所有与扫描相关的高 IO、计算负载组件均运行在虚拟化实例之外，使用独立的特殊虚拟化实例运行，例如，安全扫描程序独立于第一虚拟换实例实现，可以与第一虚拟化实例运行在相同的主机设备上，也可以与第一虚拟化实例运行在不同的主机设备上。用户购买虚拟化实例后，不会因带内扫描代理（部署在虚拟化实例内部的安全扫描程序）的运行影响其购买的计算资源使用，也不会因代理的扫描行为出现明显的 IO 波动，能够对服务资源做到很好的隔离保护。

用户数据控制：与使用镜像/快照进行带外的扫描方法相比，本方案不会使用额外的存储资源来保存虚拟化实例的磁盘镜像或快照，一方面可以节省云厂商为保存用户数据所付出的存储资源，另一方面也可以避免对用户数据的拷贝和数据泄漏，保护用户数据不离开原始计算区域。

虚拟化实例无感知：在本实施例中，由于改造均在虚拟化实例之下的虚拟化管理器一层，方案可以实现对虚拟化实例的操作系统及其上层应用隐藏，该操作系统及其上层的内核模块、用户空间进程均无感知。同时由于性能开销在虚拟化实例的虚拟化管理器当中，不会直接对虚拟化实例内运行的代码产生性能影响；不占用虚拟化实例的操作系统的 IO 队列，对 IO 性能影响较小，进一步降低通过性能分析来判断代理存在的可能性。

本公开实施例除了提供主机设备实施例之外，还提供了用于云计算的安全扫描方法，下面对本公开实施例提供的用于云计算的安全扫描方法的过程进行说明。

图 4 为本公开示例性实施例提供的一种用于云计算的安全扫描方法的流程示意图，该方法应用于主机设备上的虚拟化管理器，虚拟化管理器管理该主机设备上的第一虚拟化实例，如图 4 所示，该方法包括：

5 401、在第一虚拟化实例使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；第一虚拟化实例具有目标物理存储空间，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作；

402、基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描；其中，第一虚拟化实例通过至少一个存储队列对目标物理存储空间进行读写操作。

10 在一可选实施例中，基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序，包括：基于共享队列接收安全扫描程序发送的读请求，根据读请求，从目标物理存储空间中读取目标数据；将目标数据写入共享内存中，以供安全扫描程序从共享内存中读取目标数据。

15 在一可选实施例中，本公开实施例提供的方法还包括：获取第一虚拟化实例的配置信息，配置信息中包括第一虚拟化实例使用安全扫描服务的指示信息，根据指示信息确定第一虚拟化实例使用安全扫描服务；或者接收安全扫描程序发送的指示创建共享队列和共享内存的命令，在接收到命令的情况下，确定第一虚拟化实例使用安全扫描服务，命令是在安全扫描程序与第一虚拟化实例建立安全扫描服务绑定关系的情况下发送的。

20 在一可选实施例中，为位于第一虚拟化实例外部的安全扫描程序创建共享队列，包括：在采用 IO 虚拟化协议（例如 Virtio 协议）的情况下，执行第一虚拟化实例对应的第一引导程序，以启动第一虚拟化实例，并在启动第一虚拟化实例之后，为安全扫描程序创建共享队列；或者在采用基于设备直通的 NVMe 协议的情况下，执行第一虚拟化实例对应的第二引导程序，以启动第一虚拟化实例，并在启动过程中，由第二引导程序为安全扫描程序创建共享队列。

25 图 5 为本公开示例性实施例提供的另一种用于云计算的安全扫描方法，该方法应用第一虚拟化实例外部的安全扫描程序，如图 5 所示，该方法包括：

501、在第一虚拟化实例对应的虚拟化管理器为安全扫描程序创建共享队列和共享内存的情况下，向共享队列写入读请求，以供虚拟化管理器基于读请求，从第一虚拟化实例的目标物理存储空间中读取目标数据，并将目标数据写入共享内存；

30 502、从共享内存中读取目标数据，以及根据目标数据进行安全扫描；其中，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作，第一虚拟化实例通过至少一个存储队列对目标物理存储空间进行读写操作。

35 在一可选实施例中，本公开提供的方法还包括：向虚拟化管理器发送的指示创建共享队列和共享内存的命令，以供虚拟化管理器在接收到命令的情况下，确定第一虚拟化实例使用安全扫描服务，命令是在安全扫描程序与第一虚拟化实例建立安全扫描服务绑定关系

的情况下发送的。

关于本公开实施例提供的图 4-5 所示方法中各步骤的详细实施方式以及有益效果已经在前述实施例中进行了详细描述，此处将不做详细阐述说明。

- 需要说明的是，上述实施例所提供方法的各步骤的执行主体均可以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤 501 至步骤 502 的执行主体可以为设备 A；又比如，步骤 501 的执行主体可以为设备 A，步骤 502 的执行主体可以为设备 B；等等。

- 另外，在上述实施例及附图中的描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的序号如 501、502 等，仅仅是用于区分开各个不同的操作，序号本身不代表任何的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。需要说明的是，本文中的“第一”、“第二”等描述，是用于区分不同的消息、设备、模块等，不代表先后顺序，也不限定“第一”和“第二”是不同的类型。

- 图 6 为本公开示例性实施例提供的一种虚拟化管理装置的结构示意图，该装置可作为主机设备中的虚拟化管理器实现，用于管理第一虚拟化实例，如图 6 所示，该装置包括：创建模块 61 和提供模块 62。

- 创建模块 61，用于在第一虚拟化实例使用安全扫描服务的情况下，为位于第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；第一虚拟化实例具有目标物理存储空间，目标物理存储空间支持虚拟化管理器以多队列读写方式对其进行读写操作；

提供模块 62，用于基于共享队列和共享内存，将目标物理存储空间中的目标数据提供给安全扫描程序，以供安全扫描程序根据目标数据对主机设备进行安全扫描；其中，第一虚拟化实例通过至少一个存储队列对目标物理存储空间进行读写操作，共享队列不同于至少一个存储队列。

- 在一可选实施例中，提供模块 62 具体用于：基于共享队列接收安全扫描程序发送的读请求，根据读请求，从目标物理存储空间中读取目标数据；将目标数据写入共享内存中，以供安全扫描程序从共享内存中读取目标数据。

- 在一可选实施例中，本公开实施例提供的虚拟化管理装置还包括：获取模块、确定模块和接收模块；获取模块，用于获取第一虚拟化实例的配置信息，配置信息中包括第一虚拟化实例使用安全扫描服务的指示信息，确定模块，用于根据指示信息确定第一虚拟化实例使用安全扫描服务；或者接收模块，用于接收安全扫描程序发送的指示创建共享队列和共享内存的命令，确定模块，用于在接收到命令的情况下，确定第一虚拟化实例使用安全扫描服务，命令是在安全扫描程序与第一虚拟化实例建立安全扫描服务绑定关系的情况下发送的。

- 在一可选实施例中，创建模块，具体用于：在采用 IO 虚拟化协议（如 virtio 协议）

的情况下，执行第一虚拟化实例对应的第一引导程序，以启动第一虚拟化实例，并在启动第一虚拟化实例之后，为安全扫描程序创建共享队列；或者在采用基于设备直通的 NVMe 协议的情况下，执行第一虚拟化实例对应的第二引导程序，以启动第一虚拟化实例，并在启动过程中，由第二引导程序为安全扫描程序创建共享队列。

5 关于本公开实施例提供的图 6 所示装置中各步骤的详细实施方式以及有益效果已经在前述实施例中进行了详细描述，此处将不做详细阐述说明。

图 7 为本公开示例性实施例提供的另一种主机设备的结构示意图，如图 7 所示，该设备包括：存储器 74 和处理器 75。

10 存储器 74，用于存储安全扫描程序，并可被配置为存储其它各种数据以支持在主机设备上的操作。这些数据的示例包括用于在主机设备上操作的任何应用程序或方法的指令等。

处理器 75，与存储器 74 耦合，用于执行存储器 74 中的安全扫描程序，以用于：在第一虚拟化实例对应的虚拟化管理器为安全扫描程序创建共享队列和共享内存的情况下，向共享队列写入读请求，以供虚拟化管理器基于读请求，从第一虚拟化实例的目标物理存储空间中读取目标数据，并将目标数据写入共享内存；从共享内存中读取目标数据，以及根据目标数据对主机设备进行安全扫描；其中，所述目标物理存储空间支持所述虚拟化管理器以多队列读写方式对其进行读写操作，第一虚拟化实例通过至少一个存储队列对目标物理存储空间进行读写操作，共享队列不同于至少一个存储队列。

15

在一可选实施例中，处理器 75 还用于向虚拟化管理器发送的指示创建共享队列和共享内存的命令，以供虚拟化管理器在接收到命令的情况下，确定第一虚拟化实例使用安全扫描服务，命令是在安全扫描程序与第一虚拟化实例建立安全扫描服务绑定关系的情况下发送的。

20

在一可选实施例中，安全扫描程序是部署在主机设备上或其它设备上的第二虚拟化实例中的用户空间程序，或者安全扫描程序是直接部署在主机设备上或其它设备上的用户空间程序。

25 关于本公开实施例提供的图 7 所示设备中各步骤的详细实施方式以及有益效果已经在前述实施例中进行了详细描述，此处将不做详细阐述说明。

进一步，如图 7 所示，该主机设备还包括：通信组件 76 和电源组件 78 等其它组件。图 7 中仅示意性给出部分组件，并不意味着主机设备只包括图 7 所示组件。本实施例的主机设备实现为云服务器。

30 关于本公开实施例提供的主机设备的详细实施方式以及有益效果已经在前述实施例中进行了详细描述，此处将不做详细阐述说明。

相应地，本公开实施例还提供一种存储有计算机程序的计算机可读存储介质，计算机程序被处理器执行时能够实现上述图 4-5 所示方法中的各步骤。

相应地，本公开实施例还提供一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述图 4-5 所示方法中的各步骤。

35

上述存储器可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（Static Random-Access Memory，SRAM），电可擦除可编程只读存储器（Electrically Erasable Programmable Read Only Memory，EEPROM），可擦除可编程只读存储器（Erasable Programmable Read Only Memory，EPROM），可编程只读存储器（Programmable Read-Only Memory，PROM），只读存储器（Read-Only Memory，ROM），磁存储器，快闪存储器，磁盘或光盘。

上述通信组件被配置为便于通信组件所在设备和其他设备之间有线或无线方式的通信。通信组件所在设备可以接入基于通信标准的无线网络，如 WiFi、2G、3G、4G/LTE、5G 等移动通信网络，或它们的组合。在一个示例性实施例中，通信组件经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，通信组件还包括近场通信（Near Field Communication，NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（Radio Frequency Identification，RFID）技术，红外数据协会（Infrared Data Association，IrDA）技术，超宽带（Ultra Wide Band，UWB）技术，蓝牙（BlueTooth，BT）技术和其他技术来实现。

上述显示器包括屏幕，其屏幕可以包括液晶显示器（Liquid Crystal Display，LCD）和触摸面板（TouchPanel，TP）。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与触摸或滑动操作相关的持续时间和压力。

上述电源组件，为电源组件所在设备的各种组件提供电力。电源组件可以包括电源管理系统，一个或多个电源，及其他与为电源组件所在设备生成、管理和分配电力相关联的组件。

上述音频组件，可被配置为输出和/或输入音频信号。例如，音频组件包括一个麦克风（Microphone，MIC），当音频组件所在设备处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器或经由通信组件发送。在一些实施例中，音频组件还包括一个扬声器，用于输出音频信号。

本领域内的技术人员应明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开可采用在一个或多个其中包含有计算机可用程序代码的计算机可读存储介质（包括但不限于磁盘存储器、只读光盘（Compact Disc Read-Only Memory，CD-ROM）、光学存储器等）上实施的计算机程序产品的形式。

本公开是参照根据本公开实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提

供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

- 5 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

- 10 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器（Central Processing Unit, CPU）、输入/输出接口、网络接口和内存。

- 15 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（Random Access Memory, RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

- 20 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（Phase-change Random Access Memory, PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（Dynamic Random Access Memory, DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（Digital Video Disc, DVD）或其他光学存储、磁盒式磁带，磁带磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

- 25 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

- 30 以上仅为本公开的实施例而已，并不用于限制本公开。对于本领域技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本公开的权利要求范围之内。
- 35

权 利 要 求 书

- 1、一种主机设备，其中，所述主机设备上部署有虚拟化管理器和被所述虚拟化管理器管理的第一虚拟化实例，所述第一虚拟化实例具有目标物理存储空间，所述目标物理存储空间支持所述虚拟化管理器以多队列读写方式对其进行读写操作；
- 5 所述虚拟化管理器，还用于在确定所述第一虚拟化实例使用安全扫描服务的情况下，为位于所述第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；基于所述共享队列和共享内存，将所述目标物理存储空间中的目标数据提供给所述安全扫描程序，以供所述安全扫描程序根据所述目标数据对所述主机设备进行安全扫描；
- 10 其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作。
- 2、根据权利要求 1 所述的主机设备，其中，所述虚拟化管理器在基于所述共享队列和共享内存，将所述目标物理存储空间中的目标数据提供给所述安全扫描程序时，具体用于：
- 15 基于所述共享队列接收所述安全扫描程序发送的读请求，根据所述读请求，从所述目标物理存储空间中读取目标数据；
- 将所述目标数据写入所述共享内存中，以供所述安全扫描程序从所述共享内存中读取所述目标数据。
- 3、根据权利要求 1 或 2 所述的主机设备，其中，所述虚拟化管理器还用于：
- 20 获取所述第一虚拟化实例的配置信息，所述配置信息中包括所述第一虚拟化实例使用安全扫描服务的指示信息，根据所述指示信息确定所述第一虚拟化实例使用安全扫描服务；
- 或者
- 接收所述安全扫描程序发送的指示创建共享队列和共享内存的命令，在接收到所述命令的情况下，确定所述第一虚拟化实例使用安全扫描服务，所述命令是在所述安全扫描程序与所述第一虚拟化实例建立安全扫描服务绑定关系的情况下发送的。
- 25 4、根据权利要求 1-3 任一项所述的主机设备，其中，所述虚拟化管理器在为位于所述第一虚拟化实例外部的安全扫描程序创建共享队列时，具体用于：
- 在采用 IO 虚拟化协议的情况下，执行所述第一虚拟化实例对应的第一引导程序，以启动所述第一虚拟化实例，并在启动所述第一虚拟化实例之后，为所述安全扫描程序创建共享队列；
- 30 或者
- 在采用基于设备直通的非易失性存储器快速通道 NVMe 协议的情况下，执行所述第一虚拟化实例对应的第二引导程序，以启动所述第一虚拟化实例，并在启动过程中，由所述第二引导程序为所述安全扫描程序创建共享队列。
- 5、根据权利要求 1-4 任一项所述的主机设备，其中，所述虚拟化管理器包括：
- 35 创建模块，用于在所述第一虚拟化实例使用安全扫描服务的情况下，为位于所述第一

虚拟化实例外部的安全扫描程序创建共享队列和共享内存；

通信模块，用于接收所述安全扫描程序发送的读请求，将所述读请求写入所述共享队列中；以及从所述共享内存中读取所述目标数据并将所述目标数据发送给所述安全扫描程序，以供所述安全扫描程序根据所述目标数据对所述主机设备进行安全扫描；

- 5 为所述第一虚拟化实例分配的存储设备，用于从所述共享队列中读取所述读请求，根据所述读请求从所述目标物理存储空间中读取所述目标数据，并将所述目标数据写入所述共享内存中；以及根据所述至少一个存储队列中来自所述第一虚拟化实例中用户空间程序的读写请求，对所述目标物理存储空间进行读写操作。

- 10 6、根据权利要求 1-5 任一项所述的主机设备，其中，所述安全扫描程序是部署在所述主机设备或其它设备上的第二虚拟化实例。

7、一种用于云计算的安全扫描方法，其中，应用于主机设备上的虚拟化管理器，所述虚拟化管理器管理所述主机设备上的第一虚拟化实例，所述方法包括：

- 15 在第一虚拟化实例使用安全扫描服务的情况下，为位于所述第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；所述第一虚拟化实例具有目标物理存储空间，所述目标物理存储空间支持所述虚拟化管理器以多队列读写方式对其进行读写操作；

基于所述共享队列和共享内存，将所述目标物理存储空间中的目标数据提供给所述安全扫描程序，以供所述安全扫描程序根据所述目标数据对所述主机设备进行安全扫描；

其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作。

- 20 8、根据权利要求 7 所述的方法，其中，包括：基于所述共享队列和共享内存，将所述目标物理存储空间中的目标数据提供给所述安全扫描程序，包括：

基于所述共享队列接收所述安全扫描程序发送的读请求，根据所述读请求，从所述目标物理存储空间中读取目标数据；

- 25 将所述目标数据写入所述共享内存中，以供所述安全扫描程序从所述共享内存中读取所述目标数据。

9、根据权利要求 7 或 8 所述的方法，其中，为位于所述第一虚拟化实例外部的安全扫描程序创建共享队列，包括：

- 30 在采用 IO 虚拟化协议的情况下，执行所述第一虚拟化实例对应的第一引导程序，以启动所述第一虚拟化实例，并在启动所述第一虚拟化实例之后，为所述安全扫描程序创建共享队列；

或者

在采用基于设备直通的非易失性存储器快速通道 NVMe 协议的情况下，执行所述第一虚拟化实例对应的第二引导程序，以启动所述第一虚拟化实例，并在启动过程中，由所述第二引导程序为所述安全扫描程序创建共享队列。

- 35 10、一种用于云计算的安全扫描方法，其中，应用第一虚拟化实例外部的安全扫描程

序，所述方法包括：

在所述第一虚拟化实例对应的虚拟化管理器为所述安全扫描程序创建共享队列和共享内存的情况下，向所述共享队列写入读请求，以供所述虚拟化管理器基于所述读请求，从所述第一虚拟化实例的目标物理存储空间中读取目标数据，并将目标数据写入所述共享内存；

从所述共享内存中读取所述目标数据，以及根据所述目标数据进行安全扫描；

其中，所述目标物理存储空间支持所述虚拟化管理器以多队列读写方式对其进行读写操作，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作。

11、一种虚拟化管理装置，其中，可作为主机设备中的虚拟化管理器实现，用于管理所述主机设备中的第一虚拟化实例，所述装置包括：创建模块和提供模块；

所述创建模块，用于在第一虚拟化实例使用安全扫描服务的情况下，为位于所述第一虚拟化实例外部的安全扫描程序创建共享队列和共享内存；所述第一虚拟化实例具有目标物理存储空间，所述目标物理存储空间支持所述虚拟化管理器以多队列读写方式对其进行读写操作；

15 所述提供模块，用于基于所述共享队列和共享内存，将所述目标物理存储空间中的目标数据提供给所述安全扫描程序，以供所述安全扫描程序根据所述目标数据对所述主机设备进行安全扫描；其中，所述第一虚拟化实例通过至少一个存储队列对所述目标物理存储空间进行读写操作。

12、一种主机设备，其中，包括存储器和处理器，所述存储器中存储有安全扫描程序，所述处理器，与所述存储器耦合，用于执行所述安全扫描程序，以实现权利要求 10 中任一项所述方法中的步骤。

13、一种存储有计算机程序的计算机可读存储介质，其中，当所述计算机程序被处理器执行时，致使所述处理器实现权利要求 7-10 中任一项所述方法中的步骤。

14、一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现如权利要求 7-10 任一项所述方法中的步骤。