

文件防护方法、规则配置方法以及计算设备

5 本申请要求于2023年08月24日提交中国专利局、申请号为202311080613.6、申请名称为“文件防护方法、规则配置方法以及计算设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10 本申请实施例涉及计算机技术领域，尤其涉及一种文件防护方法、规则配置方法及计算设备。

背景技术

云原生时代的带来，利用容器技术为用户提供安全便携的云服务成为发展趋势。如何保护容器中的文件不被恶意篡改也成为了需要解决的技术问题。

15 目前的K8s（Kubernetes，一种开源的容器管理平台）等容器管理工具虽然为容器之间提供了资源隔离功能，使得一个容器中的应用程序无法访问另一个容器中的文件，但是，这种文件防护方式只能实现容器之间的文件防护，仍然存在安全隐患，无法有效实现对容器文件的保护。

发明内容

20 本申请实施例提供一种文件防护方、规则配置方法以及计算设备，用以解决现有技术中容器文件存在安全隐患，无法有效实现文件保护的技术问题。

第一方面，本申请实施例中提供了一种文件防护方法，应用于内核中的驱动程序，所述方法包括：

- 25 检测应用程序发起的文件访问请求；
确定所述应用程序归属的目标容器的容器标识；
查找所述容器标识关联的容器标签；
根据所述容器标签，查找对应的至少一个文件防御规则；
按照所述至少一个文件防御规则，确定是否对所述文件访问请求执行防御动作。

30 第二方面，本申请实施例中提供了一种文件防护方法，应用于内核中的驱动程序，所述方法包括：

- 检测应用程序发起的文件访问请求，确定文件信息；
确定所述应用程序对应的目标容器的容器标识；
将所述容器标识及所述文件信息发送至防御程序，以供所述防御程序查找所述容器标识关联的容器标签，以及根据所述容器标签，查找对应的至少一个文件防御规则，以及根据所述文件信息与所述至少一个文件防御规则的匹配结果，生成指示信息；
- 35

- 根据所述防御程序发送的所述指示信息，确定是否对所述文件访问请求执行防御动作。
- 第三方面，本申请实施例中提供了一种文件防护方法，应用于防御程序，所述方法包括：
- 获取驱动程序发送的容器标识及文件信息；所述文件信息由所述驱动程序检测应用程序发起的文件访问请求而确定；所述容器标识基于所述应用程序查找获得；
- 5 查找所述容器标识关联的容器标签；
- 根据所述容器标签，查找对应的至少一个文件防御规则；
- 根据所述文件信息与所述至少一个文件防御规则的匹配结果，生成指示信息；
- 将所述指示信息发送至所述驱动程序；所述指示信息用以指示是否对所述文件访问请求
- 10 求执行防御动作。
- 第四方面，本申请实施例中提供了一种规则配置方法，包括：
- 在规则配置界面提供规则配置提示信息；
- 响应于用户配置操作，确定用户配置的文件防御规则，以及针对所述文件防御规则设置的容器标签；
- 15 将所述文件防御规则及所述容器标签发送至防御程序，以供所述防御程序确定所述文件防御规则与所述容器标签的关联关系；
- 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定所述应用程序对应的目标容器的容器标识；其中，所述容器标识用以确定关联的容器标签，所述容器标签用以通过查找所述关联关系确定对应的至少一个文件防御规则；所述至少一个文件防御规则用于确定是否对所述文件访问请求执行防御动作。
- 20 于确定是否对所述文件访问请求执行防御动作。
- 第五方面，本申请实施例中提供了一种文件防护方法，包括：
- 获取文件防御规则；
- 获取针对所述文件防御规则设置的容器标签；
- 确定所述文件防御规则与所述容器标签的关联关系；
- 25 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定所述应用程序对应的目标容器的容器标识；其中，所述容器标识用以确定关联的容器标签，所述容器标签用以通过查找所述关联关系确定对应的至少一个文件防御规则；所述至少一个文件防御规则用于确定是否对所述文件访问请求执行防御动作。
- 第六方面，本申请实施例中提供了一种计算设备，包括处理组件以及存储组件；
- 30 所述存储组件存储一个或多个计算机指令；所述一个或多个计算机指令用以被所述处理组件调用执行，以实现如上述第一方面所述的文件防护方法或者如上述第二方面所述的文件防护方法或者如上述第三方面所述的文件防护方法或者如上述第四方面所述的规则配置方法或者如上述第五方面所述的文件防护方法。
- 第七方面，本申请实施例中提供了一种计算机存储介质，存储有计算机程序，所述计算机程序被计算机执行时，实现如上述第一方面所述的文件防护方法或者如上述第二方面
- 35 算机程序被计算机执行时，实现如上述第一方面所述的文件防护方法或者如上述第二方面

所述的文件防护方法或者如上述第三方面所述的文件防护方法或者如上述第四方面所述的规则配置方法或者如上述第五方面所述的文件防护方法。

本申请实施例中，由内核中的驱动程序检测应用程序发起的文件访问请求，从而可以确定应用程序对来自的目标容器的容器标识，并可以根据该容器标识而确定对应的容器标
5 签，从而可以根据容器标签，查找对应的至少一个文件防御规则；按照至少一个文件防御规则，即可以确定是否对文件访问请求执行防御动作，基于容器标签设置了文件防御规则适用的防御范围，实现了不同防御范围的保护，实现了对容器文件的有效防护，且结合内核的驱动程序实现防御动作，提高了防护稳定性和防护效率。

本申请的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

10

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据
15 这些附图获得其他的附图。

- 图1示出了本申请实施例的技术方案应用于其中的一种系统架构图；
- 图2示出了本申请提供的一种文件防护方法一个实施例的流程图；
- 图3示出了本申请提供的一种文件防护方法又一个实施例的流程图；
- 图4示出了本申请提供的一种文件防护方法又一个实施例的流程图；
- 20 图5示出了本申请提供的一种规则配置方法一个实施例的流程图；
- 图6示出了本申请实施例在一个实际应用中的规则配置界面的显示示意图；
- 图7示出了本申请提供的一种文件防护方法又一个实施例的流程图；
- 图8示出了本申请提供的一种文件防护装置一个实施例的结构示意图；
- 图9示出了本申请提供的一种文件防护装置又一个实施例的结构示意图；
- 25 图10示出了本申请提供的一种文件防护装置又一个实施例的结构示意图；
- 图11示出了本申请提供的一种规则配置装置一个实施例的结构示意图；
- 图12示出了本申请提供的一种文件防护装置又一个实施例的结构示意图；
- 图13示出了本申请提供的一种计算设备一个实施例的结构示意图。

30 具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述。

在本申请的说明书和权利要求书及上述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101、102等，仅仅是用于区分各个不同的操作，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。

- 5 本申请实施例的技术方案适用于容器文件防护场景，比如云计算场景中的容器文件防护场景。容器可以是指运行在物理机中或者运行在物理机中所搭建的虚拟机中的容器，本申请对此不进行限定。

为了便于理解本申请的技术方案，下面首先对本申请中可能涉及的技术术语进行相应解释说明：

- 10 容器（Container）技术：有效的将单个操作系统的资源划分到孤立的组中，以便更好的在孤立的组之间平衡有冲突的资源使用需求，这种技术就是容器技术。基于容器技术创建的容器，类似于虚拟机，但是它们具有被放宽的隔离属性，可以在应用程序之间共享操作系统。本申请实施例中的容器可以创建于宿主机中，宿主机可以是物理主机中或者虚拟机，如云服务器中，本申请对此不进行限定。

- 15 Kubernetes：简称K8s，一种开源的容器管理平台，可以用于管理云计算平台中多个机器上的容器。

虚拟机（简称：VM，英文：Virtual machine）；通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在云计算场景中，虚拟机例如可以是指弹性云服务器等。

- 20 容器镜像：容器镜像和容器的关系，类似面向对象程序设计中的类和实例，镜像是静态的定义，容器可以是指容器镜像运行时的实体。

宿主机：可以是物理机或者虚拟机。它可以运行容器和其它应用程序。容器内部也可以运行应用程序，它与前者运行在宿主机的程序的区别是：除非容器进行了特殊配置，一般情况下它只能访问容器内特定的资源或者数据。

- 25 内核：操作系统的核心，是基于硬件的第一层软件扩充，提供操作系统的最基本的功能，是操作系统工作的基础，它负责管理系统的进程、内存、设备驱动程序、文件和网络系统，决定着系统的性能和稳定性。

- 应用层（用户态）：现代操作系统提供两种运行状态：用户态和内核态。所有的应用程序（进程）在一般情况下运行在用户态。此时进程不可以直接访问硬件资源或者系统数据。如果需要，则进程通过系统调用进入内核，通过内核继续获取相关资源或者数据。最后进程返回用户态继续运行。
- 30

- 系统调用（简称：syscall，英文全称：system call）：是计算机程序向执行该程序的操作系统（内核）请求服务的程序化方式。服务可能包括硬件相关服务（例如，访问硬盘驱动器或访问设备的相机）、新进程的创建和执行，以及与集成内核服务（如进程调度）的通信。系统调用提供了进程和操作系统之间的基本接口。本申请实施例中，应用程序的文
- 35

件访问操作都需要调用系统调用来实现。

应用程序：容器中所创建的执行程序，用以实现不同执行操作。每个应用程序对应一个进程。在云计算场景中，用户可以在一个或多个容器中运行不同的应用程序等。当然，应用程序也可以在容器外部运行的宿主机上创建并运行。

5 在一个实际应用中，本申请实施例的技术方案可以应用于云计算场景中，云计算是计算机技术发展最快的趋势之一，它涉及通过网络提供托管服务。云计算环境将计算和存储资源作为服务提供给最终用户。最终用户可以向提供的服务发出请求以进行处理。服务的处理能力通常受到配置资源的限制。

10 应当理解，尽管本申请包括关于云计算的详细描述，但本文所述教导的实现不限于云计算环境。相反，本申请的实施例能够结合现在已知或以后开发的任何其他类型的计算环境来实现。

云计算是一种服务交付模式，旨在实现，按需网络访问共享的可配置计算资源池（例如，网络、网络带宽、服务器、处理、内存、存储、应用程序、虚拟机和服务），这些资源可以通过最小的管理工作或与服务提供商的交互来快速调配和发布。

15 而云服务器是云计算提供方所提供的一种云计算服务，云计算提供方可以采用多租户模型将资源集中起来形成资源池以为多个租户提供服务。本文中所指的用户意即是指租户。可以通过出资购买云计算提供方的资源，以搭建符合自己需求的云服务器等，用户在云计算提供方可以注册用户账号，云计算提供方通过用户账号来区分不同用户。在一个云服务器中又可以创建一个或多个容器等。

20 发明人在实现本申请的过程中发现，目前的K8s（Kubernetes，一种开源的容器管理平台）等容器管理工具虽然为容器之间提供了资源隔离功能，使得一个容器中的应用程序无法访问另一个容器中的文件，但是，这种文件防护方式只能实现容器之间的文件防护，实际应用中，比如存在不希望一个容器中的特定文件不希望被某些应用程序进行恶意修改，这些应用程序不排除在同一个容器中，此时采用K8s提供的资源隔离方式，将无法有效保护文件，导致仍然存在安全隐患。

25 为了提高文件防护有效性，避免安全隐患，发明人经过一系列研究提出了本申请实施例的技术方案，在本申请实施例中，由内核中的驱动程序检测应用程序发起的文件访问请求，从而可以确定应用程序对来自的目标容器的容器标识，并可以根据该容器标识而确定对应的容器标签，从而可以根据容器标签，查找对应的至少一个文件防御规则；按照至少一个文件防御规则，即可以确定是否对文件访问请求执行防御动作，基于容器标签设置了文件防御规则适用的防御范围，实现了不同防御范围的保护，实现了对容器文件的有效防护，且结合内核的驱动程序实现防御动作，提高了防护稳定性和防护效率。

30 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，

都属于本申请保护的范围。

图1示出了一种本申请实施例的技术方案的可以应用于其中一种系统架构图，该系统架构可以包括服务端101，该服务端101中部署有操作系统以及至少一个容器102，操作系统可以包括内核103及应用层104，此外，操作系统包括不同系统类型，例如目前比较流行的Windows，Linux，MacOS等，本申请对此不进行限定。本申请适用于任何可以支持容器环境的系统，例如Linux。

其中，在每个容器102中可以运行一个或多个应用程序（进程）105。

在应用层104中可以部署防御程序106，防御程序106启动之后，可以在内核103中运行对应的驱动程序107。驱动程序107可以对内核中所有与文件访问相关的系统调用进行检测，以确定是否对来自任意容器中的任意应用程序所发起的文件访问请求执行防御动作。

本申请实施例中的，服务端101可以是指物理主机，当然也可以提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络(Content Delivery Network, CDN)、以及大数据和人工智能平台等基础云计算服务的云服务器，或者是带人工智能技术的智能云计算服务器或智能云主机。

需要说明的是，本申请实施例中可能会涉及到对用户数据的使用，在实际应用中，可以在符合所在国的适用法律法规要求的情况下（例如，用户明确同意，对用户切实通知，等），在适用法律法规允许的范围内在本文描述的方案中使用用户特定的个人数据。

以下对本申请实施例的技术方案的实现细节进行详细阐述。

图2为本申请实施例提供的一种文件防护方法一个实施例的流程图，本实施例的技术方案由内核中的驱动程序执行，该方法可以包括以下几个步骤：

201：检测应用程序发起的文件访问请求。

其中，应用程序可以调用内核中的系统调用而发起针对目标文件的文件访问请求。驱动程序可以通过检测内核中与文件访问操作相关的系统调用，以确定是否存在应用程序发起文件访问请求。

其中，文件访问请求中可以包括目标文件的文件信息，文件信息例如可以包括目标文件的文件路径、文件名称、文件类型和/或操作类型等，其中，操作类型用于指示不同文件访问操作，例如可以包括读操作、写操作、修改操作等等。

202：确定应用程序归属的目标容器的容器标识。

根据应用程序的进程信息可以查找到对应的容器标识。进程信息例如可以包括进程标识等。

可选地，可以从内核数据中，查找应用程序对应的容器标识。内核数据是指应用程序进入系统内核态后可以访问的系统内核里的数据。内核数据的current（内核数据中的一个信息字段）中包含了应用程序的进程相关信息，可以从该内核数据的current中找到对应的容器标识。发起文件访问请求的容器中的应用程序，通过系统调用进入内核。此时驱动程序通过访问内核数据中的current，即可以获取应用程序（进程）的数据，并根据这些

数据进一步确定应用程序归属的容器标识。

作为一种可选方式，容器标识可以采用容器ID（Identity document，身份认证标识）来表示。

5 作为另一种可选方式，由于容器ID通常为64 bytes（字节）的字符串，基于该容器ID进行信息查找，匹配开销较大，信息查找消息较慢。因此，可选地，可以采用命名空间标识来表示容器标识。命名空间标识通常为32 bits（比特）无符号整型数据，可以减少匹配开销，提高信息查找消息。

10 其中，命名空间标识例如可以采用网络命名空间标识（简称：net-ns，全称：network-namespace）、进程命名空间标识（简称：pid-ns，全称：Process Identifier - namespace）、文件命名空间（简称：mnt-ns，全称：mount-namespace）标识等。由于不同容器通常采用独立不同的文件命名空间，文件命名空间标识可以唯一标识文件系统，因此可以利用文件命名空间标识作为容器标识，以区分不同容器。

其中，上述目标容器可以是指应用程序归属的容器，为了方便描述，命名为“目标容器”。

15 203：查找容器标识关联的容器标签。

204：根据容器标签，查找对应的至少一个文件防御规则。

本申请实施例中，可以预先配置有不同文件防御规则对应的容器标签，容器标签用以限定文件防御规则的文件防御范围。其中，容器标签可以用以标识容器对应的集群、镜像、或者应用类型等，以限定文件防御范围。因此，可选地，容器标签可以包括用以标识应用类型的

20 应用标签、用以标识集群的集群标签、以及用以标识容器镜像的镜像标签中的至少一个。

其中，应用标签用以标识容器对应的应用类型，从而可以从应用维度进行文件防护。集群标签用以标识容器对应的集群，可以采用集群ID实现，从而可以从集群维度进行文件防护，镜像标识用以表示容器对应的镜像，可以采用镜像ID实现，从而可以实现从镜像维

25 度进行文件防护。

其中，由于防御程序可以检测获知任意容器的启动操作，从而可以确定容器所属集群的集群标签、所属镜像的镜像标签、所对应的容器的命名空间标识或者容器自身的容器标识等，据此可以生成容器相关信息而下发至驱动程序。因此，驱动程序可以是根据防御程序下发的容器相关信息，查找容器标识关联的容器标签。该容器相关信息可以包括容器标

30 识与容器标签的对应关系。容器标识为命名空间标识的情况下，容器相关信息即包括命名空间标识与容器标签的对应关系，防御程序可以关联容器标签与命名空间标识，生成容器相关信息而下发至驱动程序。该容器相关信息可以以数据表如哈希表、红黑树等形式存在等，当然本申请对此不进行限定。

其中，可选地，可以针对一种或多种标签而设置对应的文件防御规则。

35 容器标识关联的容器标签包括多种标签的情况下，针对其中的一种或多种标签而查找

是否存在对应的文件防御规则，从而可能获得至少一个文件防御规则。

实际应用中，可以首先在宿主机安装防御程序，防御程序安装并启动后，防御程序可以在内核安装驱动程序，以检测与文件操作相关的系统调用。防御程序可以把预先配置的不同文件防御规则对应的容器标签发送给驱动程序。

- 5 防御程序可以检测宿主机上的容器启动和停止。对于启动的容器，防御程序可以获取容器标识和容器标签，并把二者数据发送给驱动程序。对于停止的容器，防御程序可以依旧获取其容器标识，并可以发送给驱动程序删除其对应的关联标签。

因此，驱动程序可以是根据防御程序下发的相关联的容器标识和容器标签的，查找容器标识对应的容器标签，并根据防御程序下发的不同文件防御规则对应的容器标签，查找
10 容器标签所对应的文件防御规则等。

205：按照至少一个文件防御规则，确定是否对文件访问请求执行防御动作。

- 可选地，可以是判断文件访问请求中的文件信息是否匹配至少一个文件防御规则；根据判定结果，确定是否对文件访问请求执行防御动作。若判定结果为文件信息匹配任一个文件防御规则，则可以执行对文件访问请求的防御动作，若判定结果为文件信息与至少一个文件防御规则均不匹配，则可以放行该文件访问请求，从而使得可以实现在容器标签限
15 定的文件防御范围（如应用维度、集群维度或者镜像维度等）内实现对文件的防护，提高文件访问安全性，使得属于某个应用类型、某个集群、或某个镜像的应用程序无法实现对目标文件的文件访问操作。

- 其中，文件防御规则中可以包括待防御的文件路径、文件名称或者文件类型等。从而
20 可以根据文件访问请求中的文件信息，以及文件防御规则中待防御的文件路径、文件名称或者文件类型等，确定该文件访问请求是否命中文件防御规则，若命中，则文件信息匹配该文件防御规则，可以确定对该文件访问请求执行防御动作，否则即可以放行该文件访问请求，以调用内核继续执行对应的文件访问操作等。

- 此外，文件防御规则中还可以包括进程白名单，用以设置允许访问所设置的待防御的
25 文件路径、文件名称或者文件类型对应文件的的应用程序信息等，可选地，进程白名单可以为空。因此，按照文件防御规则，可以首先判断该应用程序是否位于进程白名单中，若是，则可以直接放行该文件访问请求，否则可以再结合文件访问请求中的文件信息，以及文件防御规则中待防御的文件路径、文件名称或者文件类型等，确定该文件访问请求是否命中文件防御规则。

- 30 此外，文件防御规则中还可以包括动作类型，用以设置命中该文件防御规则情况所执行的防御动作等，动作类型例如可以包括输出报警信息或者执行拦截操作等。因此，在确定对文件访问请求执行防御动作的情况下，可以按照文件防御规则中的动作类型，执行对应的防御动作，若文件信息命中多个文件防御规则，则可以按照多个文件防御规则分别对应的动作类型，而执行多个防御动作等。

- 35 此外，容器标签所包括的多种标签也可以设置有优先级，则可以按照优先级从高到低

的顺序，依次查找每种标签对应的文件防御规则，若存在对应的文件防御规则，则可以停止查找。该文件防御规则即为最终对应的文件防御规则。根据容器标识找到应用标签、以及集群标签的情况下，应用标签的优先级最高，可以优先查找是否存在应用标签对应的文件防御规则，若是，则利用该文件防御规则执行步骤205的操作，否则，可以再根据集群
5 标签查找对应的文件防御规则。

本实施例中，由内核中的驱动程序检测应用程序发起的文件访问请求，从而可以确定应用程序对来自的目标容器的容器标识，并可以根据该容器标识而确定对应的容器标签，从而可以根据容器标签，查找对应的文件防御规则；按照文件防御规则，即可以确定是否
10 对文件访问请求执行防御动作，基于容器标签设置了文件防御规则适用的防御范围，实现了不同防御范围的保护，实现了对容器文件的有效防护，且结合内核的驱动程序实现防御动作，提高了防护稳定性和防护效率。

一些实施例中，由上文描述可知，容器标签包括用以标识应用类型的应用标签、用以标识集群的集群标签、以及用以标识容器镜像的镜像标签中的至少一个；

该方法还可以包括：获取防御程序下发的文件防御规则与容器标签的关联关系；
15 上述根据容器标签，查找对应的文件防御规则可以包括：根据容器标签，查找关联关系以确定对应的文件防御规则。

也即防御程序可以获得用户配置信息，并将其中的文件防御规则与容器标签的关联关系下发至驱动程序，从而驱动程序可以据此查找对应的文件防御规则。

20 图3为本申请实施例提供的一种文件防护方法又一个实施例的流程图，本实施例的技术方案可以由于内核中的驱动程序执行，该方法可以包括以下几个步骤：

301：检测应用程序发起的文件访问请求，确定文件信息。
其中，应用程序可以调用内核中的系统调用而发起针对目标文件的文件访问请求。驱动程序可以通过检测内核中与文件访问操作相关的系统调用，以确定是否存在应用程序发
25 起文件访问请求。

其中，文件访问请求中可以包括文件信息，从而可以获得文件信息。文件信息例如可以包括文件路径、文件名称、文件类型和/或操作类型等，其中，操作类型用于指示不同文件访问操作，例如可以包括读操作、写操作、修改操作等等。

302：确定应用程序对应的目标容器的容器标识。
30 步骤302的具体执行操作可以详见步骤202中所述，此处不再重复赘述。

303：将容器标识及文件信息发送至防御程序，以供防御程序查找容器标识关联的容器标签，以及根据容器标签，查找对应的至少一个文件防御规则，以及根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息。

304：根据防御程序发送的指示信息，确定是否对文件访问请求执行防御动作。
35 本实施例与图2所示实施例不同之处在于，驱动程序将容器标识以及文件信息发放至

防御程序，由防御程序查找容器标签，并根据容器标签找到文件防御规则，并执行匹配操作。

其中，作为一种可选方式，指示信息可以包括匹配结果，驱动程序可以根据匹配结果，判断是否对文件访问请求执行防御动作，匹配结果表明文件信息与文件防御规则匹配的情况下，则执行对文件访问请求执行防御动作，否则则可以放行该文件访问请求。

作为另一种可选方式，防御程序可以根据匹配结果而生成执行指令，该指示信息即可以包括根据匹配结果而生成的执行指令。该执行指令可以指示驱动程序是否执行防御动作，从而无需驱动程序再执行判断操作等。

其中，防御程序中预先保存文件防御规则与容器标签的关联关系，从而可以根据容器标签，查找关联关系以确定对应的至少一个文件防御规则。

其中，防御程序在检测到任意容器的启动操作时，可以获得容器相关信息，从而可以根据容器相关信息，查找容器标识关联的容器标签。

其中，文件防御规则中可以包括待防御的文件路径、文件名称或者文件类型等。从而防御程序可以根据文件访问请求中的文件信息，以及文件防御规则中待防御的文件路径、文件名称或者文件类型等，确定该文件访问请求是否命中文件防御规则，若命中，则文件信息匹配该文件防御规则，否则认为文件信息与文件防御规则不匹配。

此外，文件防御规则中还可以包括进程白名单，用以设置允许访问所设置的待防御的文件路径、文件名称或者文件类型对应文件的应用程序信息等，可选地，进程白名单可以为空。因此，防御程序首先判断该应用程序是否位于进程白名单中，若是，则可以认为文件信息与文件防御规则不匹配，否则可以再结合文件信息，以及文件防御规则中待防御的文件路径、文件名称或者文件类型等，确定该文件访问请求是否命中文件防御规则。

此外，文件防御规则中还可以包括动作类型，用以设置命中该文件防御规则情况所执行的防御动作等，动作类型例如可以包括输出报警信息或者执行拦截操作等。因此，防御程序确定文件信息与至少一个文件防御规则匹配的情况下，还可以将动作类型发送至驱动程序，指示信息中可以包括该动作类型，以指示驱动程序按照动作类型，执行对应的防御动作。

本实施例中，由内核中的驱动程序检测应用程序发起的文件访问请求，从而可以确定应用程序对来自的目标容器的容器标识，并交由防御层序根据该容器标识而确定对应的容器标签，从而可以根据容器标签，查找对应的至少一个文件防御规则；按照至少一个文件防御规则，即可以确定是否对文件访问请求执行防御动作，基于容器标签设置了文件防御规则适用的防御范围，实现了不同防御范围的保护，实现了对容器文件的有效防护，且结合内核的驱动程序实现了防御动作，提高了防护稳定性和防护效率。

图4为本申请实施例提供的一种文件防护方法又一个实施例的流程图，本实施例的技术方案由防御程序执行，防御程序运行在操作系统的应用层，实际应用中，防御程序首先

安装在宿主机中，防御程序安装并启动后，防御程序可以在内核安装驱动程序，以用来检测与文件操作相关的系统调用，该方法可以包括以下几个步骤：

401：获取驱动程序发送的容器标识及文件信息。

其中，文件信息由驱动程序检测到应用程序发起的文件访问请求而确定；容器标识基于应用程序查找获得。驱动程序可以从内核数据中而确定该容器标识。

其中，容器标识可以采用命名空间标识实现，例如标识文件系统的文件命名空间标识等。

402：查找容器标识关联的容器标签。

403：根据容器标签，查找对应的至少一个文件防御规则。

10 防御程序可以检测宿主机上的容器启动和停止。对于启动的容器，防御程序可以获取容器标识和容器标签，由于防御程序可以检测获知任意容器的启动操作，从而可以确定容器所属集群的集群标签、所属镜像的镜像标签、所对应的命名空间标识或者容器自身的容器标识等，据此可以生成容器相关信息。因此，可以根据该容器相关信息，查找容器标识关联的容器标签。该容器相关信息可以包括容器标识与容器标签的对应关系。容器标识为命名空间标识的情况下，容器相关信息即包括命名空间标识与容器标签的对应关系，防御程序可以关联容器标签与命名空间标识，生成容器相关信息而下发至驱动程序。该容器相关信息可以以数据表如哈希表或者红黑树等形式存在等，当然本申请对此不进行限定。

404：根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息。

20 405：将指示信息发送至驱动程序；指示信息用以指示是否对文件访问请求执行防御动作。

其中，作为一种可选方式，指示信息可以包括匹配结果，驱动程序可以根据匹配结果，判断是否对文件访问请求执行防御动作，匹配结果表明文件信息与文件防御规则匹配的情况下，则执行对文件访问请求执行防御动作，否则则可以放行该文件访问请求。

25 作为另一种可选方式，防御程序可以根据匹配结果而生成执行指令，该指示信息即可以包括根据匹配结果而生成的执行指令。该执行指令可以指示驱动程序是否执行防御动作，从而无需驱动程序再执行判断操作等。

其中，防御程序中预先保存文件防御规则与容器标签的关联关系，从而可以根据容器标签，查找关联关系以确定对应的至少一个文件防御规则。

30 其中，防御程序在检测到任意容器的启动操作时，可以获得容器相关信息，从而可以根据容器相关信息，查找容器标识关联的容器标签。

本实施例中，由内核中的驱动程序检测应用程序发起的文件访问请求，从而可以确定应用程序对来自的目标容器的容器标识，并交由防御层序根据该容器标识而确定对应的容器标签，从而可以根据容器标签，查找对应的文件防御规则；按照文件防御规则，即可以确定是否对文件访问请求执行防御动作，基于容器标签设置了文件防御规则适用的防御范围，实现了不同防御范围的保护，实现了对容器文件的有效防护，且结合内核的驱动程序

实现文件访问请求的防御动作，提高了防护稳定性和防护效率。

此外，文件防御规则可以由用户配置获得，参见图5，为本申请实施例提供的一种规则配置方法一个实施例的流程图，本实施例的技术方案可以由用户端执行，该方法可以包括以下几个步骤：

5 501：在规则配置界面提供规则配置提示信息。
 该规则配置提示信息用于提示用户执行配置操作等。

 502：响应于用户配置操作，确定用户配置的文件防御规则，以及针对文件防御规则设置的容器标签。

10 该规则配置提示信息中例如可以包括规则设置提示信息以及标签设置提示信息等。
 规则设置提示信息中可以包括文件信息设置提示信息、白名单设置提示信息、动作设置提示信息等。

 文件信息设置提示信息用以提示用户配置文件信息，白名单设置提示信息用以提示用户配置进程白名单，动作设置提示信息用以提示用户配置动作类型等，从而可以结合文件信息，此外还可以结合进程白名单和/或动作类型而获得文件防御规则。

15 标签设置提示信息可以用以提示用户设置容器标签。
 503：将文件防御规则及容器标签发送至防御程序，以供防御程序确定文件防御规则与容器标签的关联关系。

 可选地，可以是通过控制端而将文件防御规则及容器标签发送至防御程序。
20 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识；其中，容器标识用以确定关联的容器标签，容器标签用以通过找关联关系确定对应的至少一个文件防御规则；至少一个文件防御规则用于确定是否对文件访问请求执行防御动作。

 作为一种可选方式，防御程序可以确定文件防御规则与容器标签的关联关系，并将文件防御规则以及关联关系下发至驱动程序；驱动程序用以检测到应用程序发起的文件访问请求，查找应用程序对应的目标容器的容器标识，以及根据容器标识关联的容器标签，查找关联关系确定对应的至少一个文件防御规则，并按照至少一个文件防御规则，确定是否对文件访问请求执行防御动作。

25 此外，防御程序可以检测宿主机上的容器启动和停止。对于启动的容器，防御程序可以获取容器标识和容器标签，并把二者数据发送给驱动程序。对于停止的容器，防御程序可以依旧获取其容器标识，并可以发送给驱动程序删除其对应的关联标签。

 因此，驱动程序可以是根据防御程序下发的相关联的容器标识和容器标签的，查找容器标识对应的容器标签，并根据防御程序下发的不同文件防御规则对应的容器标签，查找容器标签所对应的文件防御规则等。

35 作为一种可选方式，防御程序可以确定文件防御规则与容器标签的关联关系，以及获

取驱动程序发送的容器标识及文件信息，以及查找容器标识关联的容器标签；以及根据容器标签，查找对应的至少一个文件防御规则；以及根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息，并将指示信息发送至驱动程序。

5 驱动程序可以检测应用程序发起的文件访问请求，确定文件信息；确定应用程序对应的目标容器的容器标识；将容器标识及文件信息发送至防御程序，并根据防御程序发送的指示信息，而确定是否对文件访问请求执行防御动作。

10 为了便于理解，图6示出了规则配置界面的一种界面示意图，如图6所示的规则配置界面中可以包括规则设置提示信息以及标签设置提示信息601；其中，规则设置提示信息可以包括文件信息设置提示信息602、白名单设置提示信息603、动作设置提示信息604等。该规则配置界面中还可以包括确认提示信息，用以用户针对所配置的文件防御规则以及容器标签而执行确认操作，从而可以触发将文件防御规则及容器标签发送至防御程序。

其中，标签设置提示信息可以包括至少一个标签种类选择提示信息以及针对每个标签选择提示信息对应的标签输入提示信息，可以首先显示至少一个标签种类选择提示信息，响应于用户所选择的标签种类，可以再显示所选择的标签种类对应的标签输入提示信息等。

15 此外，一些实施例中，该方法还可以包括：

响应于针对文件防御规则的更新操作，执行对应的处理操作。

该更新操作例如可以包括删除或者修改等，其中，修改操作可以包括针对文件信息、进程白名单、动作类型或者对应的容器标签的修改操作等。

20 图7为本申请实施例提供的一种文件防护方法又一个实施例的流程图，本实施例的技术方案可以由防御程序执行，该方法可以包括以下几个步骤：

701：获取文件防御规则。

702：获取针对文件防御规则设置的容器标签。

25 其中，文件防御规则以及容器标签可以是用户端响应于用户配置操作而确定，用户端可以通过控制端而将文件防御规则以及容器标签发送至防御程序。

703：确定文件防御规则与容器标签的关联关系。

30 防御程序可以建立文件防御规则与容器标签的关联关系。从而，驱动程序检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识；其中，容器标识用以确定关联的容器标签，容器标签用以通过查找关联关系确定对应的至少一个文件防御规则；至少一个文件防御规则用于确定是否对文件访问请求执行防御动作。

35 作为一种可选方式，防御程序可以确定文件防御规则与容器标签的关联关系，并将文件防御规则以及关联关系下发至驱动程序；驱动程序用以检测到应用程序发起的文件访问请求，查找应用程序对应的目标容器的容器标识，以及根据容器标识关联的容器标签，查找关联关系确定对应的至少一个文件防御规则，并按照至少一个文件防御规则，确定是否对文件访问请求执行防御动作。

作为一种可选方式，防御程序可以确定文件防御规则与容器标签的关联关系，以及获取驱动程序发送的容器标识及文件信息，以及查找容器标识关联的容器标签；以及根据容器标签，查找对应的至少一个文件防御规则；以及根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息，并将指示信息发送至驱动程序。

5 驱动程序可以检测应用程序发起的文件访问请求，确定文件信息；确定应用程序对应的目标容器的容器标识；将容器标识及文件信息发送至防御程序，并根据防御程序发送的指示信息，而确定是否对文件访问请求执行防御动作。

一些实施例中，防御程序还可以将文件防御规则以及关联关系下发至驱动程序。

10 从而可以由驱动程序检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识，以及根据容器标识关联的容器标签，查找关联关系确定对应的文件防御规则，并按照文件防御规则，确定是否对文件访问请求执行防御动作。

一些实施例中，该方法还可以包括：

检测到任意容器的启动操作，将容器的容器相关信息下发至驱动程序；驱动程序根据容器相关信息，查找容器标识关联的容器标签。

15

图8为本申请实施例提供的一种文件防护装置一个实施例的结构示意图，该装置可以包括：

第一检测模块801，用于检测应用程序发起的文件访问请求；

第一确定模块802，用于确定应用程序归属的目标容器的容器标识；

20 第一查找模块803，用于查找容器标识关联的容器标签；

第二查找模块804，用于根据容器标签，查找对应的至少一个文件防御规则；

第一执行模块805，用于按照至少一个文件防御规则，确定是否对文件访问请求执行防御动作。

25 一些实施例中，第一查找模块具体是根据防御程序下发的容器相关信息，查找容器标识关联的容器标签；防御程序用以在检测到任意容器的启动操作时，将获取的对应的容器相关信息发送至驱动程序。

一些实施例中，容器标签包括用以标识应用类型的应用标签、用以标识集群的集群标签、以及用以标识容器镜像的镜像标签中的至少一个；

该装置还可以包括：

30 第一获取模块，用于获取防御程序下发的文件防御规则与容器标签的关联关系；

第二查找模型可以具体是根据容器标签，查找关联关系以确定对应的至少一个文件防御规则。

一些实施例中，第一确定模块可以具体是从内核数据中查找应用程序对应的命名空间标识；命名空间标识用以标识应用程序归属的目标容器。

35 一些实施例中，命名空间标识包括文件命名空间标识。

一些实施例中，第一执行模块可以具体是判断文件访问请求中的文件信息是否匹配至少一个文件防御规则；根据判定结果，确定是否对文件访问请求执行防御动作。

图8所述的文件防护装置可以执行图2所示实施例所述的文件防护方法，其实现原理和技术效果不再赘述。对于上述实施例中的文件防护装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图9为本申请实施例提供的一种文件防护装置又一个实施例的结构示意图，该装置可以包括：

- 第二检测模块901，用于检测应用程序发起的文件访问请求，确定文件信息；
- 10 第二确定模块902，用于确定应用程序对应的目标容器的容器标识；
- 第一发送模块903，用于将容器标识及文件信息发送至防御程序，以供防御程序查找容器标识关联的容器标签，以及根据容器标签，查找对应的至少一个文件防御规则，以及根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息；
- 15 第二执行模块904，用于根据防御程序发送的指示信息，确定是否对文件访问请求执行防御动作。

图9所述的文件防护装置可以执行图3所示实施例所述的文件防护方法，其实现原理和技术效果不再赘述。对于上述实施例中的文件防护装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图10为本申请实施例提供的一种文件防护装置又一个实施例的结构示意图，该装置可以包括：

- 20 第二获取模块1001，用于获取驱动程序发送的容器标识及文件信息；文件信息由驱动程序检测应用程序发起的文件访问请求而确定；容器标识基于应用程序查找获得；
- 第三查找模块1002，用于查找容器标识关联的容器标签；
- 第四查找模块1003，用于根据容器标签，查找对应的至少一个文件防御规则；
- 25 匹配模块1004，用于根据文件信息与至少一个文件防御规则的匹配结果，生成指示信息；
- 第二发送模块1005，用于将指示信息发送至驱动程序；指示信息用以指示是否对文件访问请求执行防御动作。

图10所述的文件防护装置可以执行图4所示实施例所述的文件防护方法，其实现原理和技术效果不再赘述。对于上述实施例中的文件防护装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图11为本申请实施例提供的一种规则配置装置一个实施例的结构示意图，该装置可以包括：

- 第一显示模块1101，用于在规则配置界面提供规则配置提示信息；
- 35 第一处理模块1102，用于响应于用户配置操作，确定用户配置的文件防御规则，以及

针对文件防御规则设置的容器标签；

第三发送模块1103，用于将文件防御规则及容器标签发送至防御程序，以供防御程序确定文件防御规则与容器标签的关联关系；

5 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识；其中，容器标识用以确定关联的容器标签，容器标签用以通过查找关联关系确定对应的至少一个文件防御规则；至少一个文件防御规则用于确定是否对文件访问请求执行防御动作。

10 图11所述的规则配置装置可以执行图5所示实施例所述的规则配置方法，其实现原理和技术效果不再赘述。对于上述实施例中的规则配置装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图12本申请实施例提供的一种文件防护装置又一个实施例的结构示意图，该装置可以包括：

第三获取模块1201，用于获取文件防御规则；以及获取针对文件防御规则设置的容器标签；

15 关系确定模块1202，用于确定文件防御规则与容器标签的关联关系；

其中，驱动程序用以检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识；其中，容器标识用以确定关联的容器标签，容器标签用以通过查找关联关系确定对应的至少一个文件防御规则；至少一个文件防御规则用于确定是否对文件访问请求执行防御动作。

20 一些实施例中，该装置还可以包括：

第四发送模块，用于将文件防御规则以及关联关系下发至驱动程序，以供驱动程序检测到应用程序发起的文件访问请求，确定应用程序对应的目标容器的容器标识，以及根据容器标识关联的容器标签，查找关联关系确定对应的至少一个文件防御规则，并按照至少一个文件防御规则，确定是否对文件访问请求执行防御动作。

25 一些实施例中，该装置还可以包括：

第五发送模块，用于检测到任意容器的启动操作，将容器的容器相关信息下发至驱动程序；驱动程序根据容器相关信息，查找容器标识关联的容器标签。

30 图12所述的文件防护装置可以执行图6所示实施例所述的文件防护方法，其实现原理和技术效果不再赘述。对于上述实施例中的文件防护装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

本申请实施例还提供了一种计算设备，如图所13示，该计算设备可以包括存储组件1301以及处理组件1302；

35 存储组件1301存储一条或多条计算机指令，其中，一条或多条计算机指令供处理组件1302调用执行，以实现如图2所示实施例的文件防护方法或者如图3所示实施例的文件防护方法或者如图4所示实施例的文件防5护方法或者如图所

图6所示实施例的文件防护方法。

其中，该计算设备可以运行一个或多个容器。

当然，计算设备必然还可以包括其他部件，例如输入/输出接口、显示组件、通信组件等。

- 5 在该计算设备中的处理组件用以实现如图4所示实施例的规则配置方法的情况下，该计算设备还可以包括显示组件，以执行对应的显示操作。

输入/输出接口为处理组件和外围接口模块之间提供接口，上述外围接口模块可以是输出设备、输入设备等。通信组件被配置为便于计算设备和其他设备之间有线或无线方式的通信等。

- 10 其中，处理组件可以包括一个或多个处理器来执行计算机指令，以完成上述的方法中的全部或部分步骤。当然处理组件也可以为一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

- 15 存储组件被配置为存储各种类型的数据以支持在终端的操作。存储组件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（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

- 20 显示组件可以为电致发光(EL)元件、液晶显示器或具有类似结构的微型显示器、或者视网膜可直接显示或类似的激光扫描式显示器。

- 需要说明的是，上述计算设备实现图2所示实施例的文件防护方法或图3所示实施例文件防护方法或者图4所示实施例的文件防护方法或者图6所示实施例的文件防护方法的情况下，其可以为物理设备或者云计算平台提供的弹性计算主机等。其可以实现成多个服务器或终端设备组成的分布式集群，也可以实现成单个服务器或单个终端设备。处理组件还可以是运行虚拟机，以由虚拟机实现图2所示实施例的文件防护方法或图3所示实施例文件防护方法或者图4所示实施例的文件防护方法或者图6所示实施例的文件防护方法等。
- 25

上述计算设备实现图5所示规则配置方法的情况下，其可以具体实现为电子设备，电子设备可以是指用户使用的，具有用户所需计算、上网、通信等功能的设备，例如可以是手机、平板电脑、个人电脑、穿戴设备等。

- 30 本申请实施例还提供了一种计算机可读存储介质，存储有计算机程序，所述计算机程序被计算机执行时可以实现上述图2所示实施例的文件防护方法或者如图3所示实施例的文件防护方法或者如图4所示实施例的文件防护方法或者如图5所示实施例的文件防护方法或者如图6所示实施例的文件防护方法。该计算机可读介质可以是上述实施例中描述的设备中所包含的；也可以是单独存在，而未装配入该电子设备中。

- 35 本申请实施例还提供了一种计算机程序产品，其包括承载在计算机可读存储介质上的

5 计算机程序，所述计算机程序被计算机执行时可以实现如上述图2所示实施例的文件防护方法或者如图3所示实施例的文件防护方法或者如图4所示实施例的文件防护方法或者如图5所示实施例的文件防护方法或者如图6所示实施例的文件防护方法。在这样的实施例中，计算机程序可以是

5 从网络上被下载和安装，和/或从可拆卸介质被安装。在该计算机程序被处理器执行时，执行本申请的系统中限定的各种功能。

需要说明的是，本申请实施例中可能会涉及到对用户数据的使用，在实际应用中，可以在符合所在国的适用法律法规要求的情况下（例如，用户明确同意，对用户切实通知，等），在适用法律法规允许的范围内在本文描述的方案中使用用户特定的个人数据。

10 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

15 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

20 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行各个实施例或者实施例的某些部分所述的方法。

25 最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权 利 要 求 书

- 1、一种文件防护方法，其特征在于，应用于内核中的驱动程序，所述方法包括：
检测应用程序发起的文件访问请求；
确定所述应用程序归属的目标容器的容器标识；
5 查找所述容器标识关联的容器标签；
根据所述容器标签，查找对应的至少一个文件防御规则；
按照所述至少一个文件防御规则，确定是否对所述文件访问请求执行防御动作。
- 2、根据权利要求1所述的方法，其特征在于，所述查找所述容器标识关联的容器标签包括：
10 根据防御程序下发的容器相关信息，查找所述容器标识关联的容器标签；所述防御程序用以在检测到任意容器的启动操作时，将获取的对应的容器相关信息发送至所述驱动程序。
- 3、根据权利要求1所述的方法，其特征在于，所述容器标签包括用以标识应用类型的应用标签、用以标识集群的集群标签、以及用以标识容器镜像的镜像标签中的至少一个；
15 所述方法还包括：
获取防御程序下发的文件防御规则与容器标签的关联关系；
所述根据所述容器标签，查找对应的至少一个文件防御规则包括：
根据所述容器标签，查找所述关联关系以确定对应的至少一个文件防御规则。
- 4、根据权利要求1所述的方法，其特征在于，所述确定所述应用程序归属的目标容器
20 的容器标识包括：
从内核数据中查找所述应用程序对应的命名空间标识；所述命名空间标识用以标识所述应用程序归属的目标容器。
- 5、根据权利要求4所述的方法，其特征在于，所述命名空间标识包括文件命名空间标识。
- 6、根据权利要求1所述的方法，其特征在于，所述按照所述文件防御规则，确定是否
25 对所述文件访问请求执行防御动作包括：
判断所述文件访问请求中的文件信息是否匹配所述至少一个文件防御规则；
根据判定结果，确定是否对所述文件访问请求执行防御动作。
- 7、一种文件防护方法，其特征在于，应用于内核中的驱动程序，所述方法包括：
30 检测应用程序发起的文件访问请求，确定文件信息；
确定所述应用程序对应的目标容器的容器标识；
将所述容器标识及所述文件信息发送至防御程序，以供所述防御程序查找所述容器标识关联的容器标签，以及根据所述容器标签，查找对应的至少一个文件防御规则，以及根据所述文件信息与所述至少一个文件防御规则的匹配结果，生成指示信息；
35 根据所述防御程序发送的所述指示信息，确定是否对所述文件访问请求执行防御动作。

- 8、一种文件防护方法，其特征在于，应用于防御程序，所述方法包括：
- 获取驱动程序发送的容器标识及文件信息；所述文件信息由所述驱动程序检测应用程序发起的文件访问请求而确定；所述容器标识基于所述应用程序查找获得；
- 5 查找所述容器标识关联的容器标签；
- 根据所述容器标签，查找对应的至少一个文件防御规则；
- 根据所述文件信息与所述至少一个文件防御规则的匹配结果，生成指示信息；
- 将所述指示信息发送至所述驱动程序；所述指示信息用以指示是否对所述文件访问请求执行防御动作。
- 9、一种规则配置方法，其特征在于，包括：
- 10 在规则配置界面提供规则配置提示信息；
- 响应于用户配置操作，确定用户配置的文件防御规则，以及针对所述文件防御规则设置的容器标签；
- 将所述文件防御规则及所述容器标签发送至防御程序，以供所述防御程序确定所述文件防御规则与所述容器标签的关联关系；
- 15 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定所述应用程序对应的目标容器的容器标识；其中，所述容器标识用以确定关联的容器标签，所述容器标签用以通过查找所述关联关系确定对应的至少一个文件防御规则；所述至少一个文件防御规则用于确定是否对所述文件访问请求执行防御动作。
- 10、一种文件防护方法，其特征在于，包括：
- 20 获取文件防御规则；
- 获取针对所述文件防御规则设置的容器标签；
- 确定所述文件防御规则与所述容器标签的关联关系；
- 其中，驱动程序用以检测到应用程序发起的文件访问请求，确定所述应用程序对应的目标容器的容器标识；其中，所述容器标识用以确定关联的容器标签，所述容器标签用以
- 25 通过查找所述关联关系确定对应的至少一个文件防御规则；所述至少一个文件防御规则用于确定是否对所述文件访问请求执行防御动作。
- 11、一种计算设备，其特征在于，包括处理组件以及存储组件；
- 所述存储组件存储一个或多个计算机指令；所述一个或多个计算机指令用以被所述处理组件调用执行，以实现如权利要求1~6任一项所述的文件防护方法或者如权利要求7所述
- 30 的文件防护方法或者如权利要求8所述的文件防护方法或者如权利要求9所述的规则配置方法或者如权利要求10所述的文件防护方法。
- 12、一种计算机存储介质，其特征在于，存储有计算机程序，所述计算机程序被计算机执行时，实现如权利要求1~6任一项所述的文件防护方法或者如权利要求7所述的文件防护方法或者如权利要求8所述的文件防护方法或者如权利要求9所述的规则配置方法或者如权利要求10所述的文件防护方法。
- 35