(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2023 年 6 月 15 日 (15.06.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/103992 A1

(51) 国际专利分类号:
G06F 21/31 (2013.01)

(21) 国际申请号: PCT/CN2022/136683

(22) 国际申请日: 2022 年 12 月 5 日 (05.12.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111484516.4 2021年12月7日 (07.12.2021) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 冉小凯 (RAN, Xiaokai); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 蒋学鑫 (JIANG, Xuexin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 杨洋 (YANG, Yang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区西丽街道松坪山社区松坪山路3号奥特迅电力大厦201, Guangdong 518052 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,

(54) **Title:** CONTAINER OPERATION METHOD AND APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 容器运行方法、装置、电子设备和存储介质

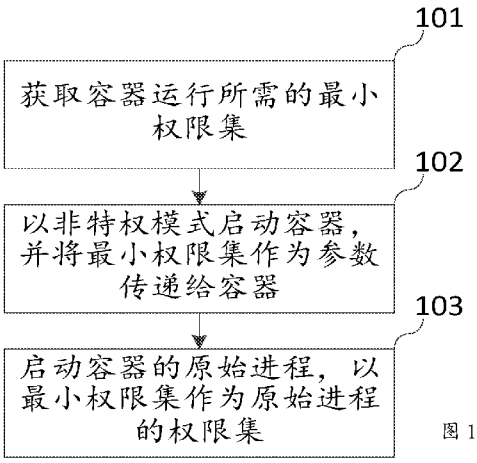

图 1

101 Obtain the minimum set of permissions required for operation of a container

102 Start the container in an unprivileged mode, and transfer the minimum set of permissions to the container as a parameter

103 Start an original process of the container, and use the minimum set of permissions as a set of permissions of the original process

(57) **Abstract:** Embodiments of the present application relate to the technical field of computer processing, and in particular, to a container operation method and apparatus, an electronic device, and a storage medium. The container operation method comprises: obtaining the minimum set of permissions required for operation of a container; starting the container in an unprivileged mode, and transferring the minimum set of permissions to the container as a parameter; and starting an original process of the container, and using the minimum set of permissions as a set of permissions of the original process.

(57) **摘要**: 本申请实施例涉及计算机处理技术领域，特别涉及一种容器运行方法、装置、电子设备和存储介质。其中，容器运行方法，包括：获取容器运行所需的最小权限集；以非特权模式启动容器，并将最小权限集作为参数传递给容器；启动容器的原始进程，以最小权限集作为原始进程的权限集。

WO 2023/103992 A1

[见续页]

SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

容器运行方法、装置、电子设备和存储介质

相关申请

本申请要求于 2021 年 12 月 07 号申请的、申请号为 202111484516.4 的中国专利申请的优先权。

技术领域

本申请实施例涉及计算机处理技术领域，特别涉及一种容器运行方法、装置、电子设备和存储介质。

背景技术

容器技术是指，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。也就是产生资源隔离，用于解决多操作系统/应用程序堆栈的问题。

而特权容器（特权模式的容器）几乎拥有系统全部权限，可以直接修改主机运行参数，不受限制的使用系统内存、CPU 资源，访问、修改主机敏感数据，删除主机关键文件。特权容器拥有对系统全局资源的访问权限，也打破了容器技术的设计初衷：资源隔离，即容器只能访问容器命名空间内的局部资源。因此，运行异常的特权容器将对系统安全构成重大威胁。

发明内容

本申请实施例的主要目的在于提出一种容器运行方法，回收特权容器的多余权限，保障系统资源的安全性。

为实现上述目的，本申请实施例提供了一种容器运行方法，包括：获取容器运行所需的最小权限集；以非特权模式启动容器，并将最小权限集作为参数传递给容器；启动容器的原始进程，以最小权限集作为原始进程的权限集。

为实现上述目的，本申请实施例还提供一种容器运行系统，包括：获取模块，用于获取容器运行所需的最小权限集；传递模块，用于以非特权模式启动容器，并将最小权限集作为参数传递给容器；启动模块，用于启动容器的原始进程，以最小权限集作为原始进程的权限集。

为实现上述目的，本申请实施例还提供了一种电子设备，包括：至少一个处理器；以及，与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行上述的容器运行方法。

为实现上述目的，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，所述计算机程序被处理器执行时实现上述的容器运行方法。

本申请实施例中，提供了一种容器运行方法，对于特权容器，筛选出容器正常运行所需最小权限集，以非特权模式启动容器，将所述最小权限集作为参数传递给容器，在启动容器的原始进程后，容器仅具有最小权限集中的权限。从而删除了非必须权限，将特权容器转换

为非特权容器，降低特权容器运行异常对系统安全的威胁。

附图说明

图 1 是根据本申请一个实施例中所提供的容器运行方法的流程图；

图 2 是根据本申请一个实施例中所提供的容器运行装置的流程图；

图 3 是根据本申请一个实施例中提供的一种电子设备的结构示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合附图对本申请的各实施例进行详细的阐述。然而，本领域的普通技术人员可以理解，在本申请各实施例中，为了使读者更好地理解本申请而提出了许多技术细节。但是，即使没有这些技术细节和基于以下各实施例的种种变化和修改，也可以实现本申请所要求保护的技术方案。以下各个实施例的划分是为了描述方便，不应对本申请的具体实现方式构成任何限定，各个实施例在不矛盾的前提下可以相互结合相互引用。

本申请的一个实施例涉及一种容器运行方法，具体流程如图 1 所示，至少包括以下步骤：

步骤 101，获取容器运行所需的最小权限集；

步骤 102，以非特权模式启动容器，并将最小权限集作为参数传递给容器；

步骤 103，启动容器的原始进程，以最小权限集作为原始进程的权限集。

下面对本实施例的容器运行方法的实现细节进行具体的说明，以下内容仅为方便理解提供的实现细节，并非实施本方案的必须。

在步骤 101 中，获取容器运行所需的最小权限集。由于容器的产生是为了完成或实现相应业务，容器运行所需的最小权限集也就是该业务正常运作所需的最小权限。

在一个例子中，获取容器运行所需的最小权限集，包括：将容器的最小权限集初始化为空，并将容器运行在非特权模式下；在容器的运行过程中，获取容器在非特权模式下向系统请求的用于进行特权操作的权限，并将请求的权限加入最小权限集，赋予所述容器所述请求的权限，保证所述容器的正常运行；在满足预设的初始化结束条件后，关闭容器的运行，输出最小权限集。其中，将容器运行在非特权模式下，即容器最开始无法实现特权操作，由于最开始将容器的最小权限集清空，容器不具备任何进行特权操作的权限；但容器在生成时存在对应需要完成的业务，所以在运行过程中仍然会向系统请求实现该业务的特权操作的权限，系统根据请求赋予容器相应的权限，使得容器能够继续进行其他权限的请求，并将系统赋予的该权限加入当前容器的最小权限集，逐渐充实容器的最小权限集的内容。在满足预设的初始化结束条件后，关闭容器的运行，将得到的最终的最小权限集输出。此处容器的正常运行可以是容器进行权限请求的过程正常运行。

在一个例子中，预设的初始化结束条件包括：容器请求的权限均处于最小权限集内。其中，对于容器请求的权限均处于最小权限集内的判断方式，例如为连续 N 次请求的权限（N 不小于预设的第一阈值）过程中，所请求的权限均在最小权限集内，则判断容器请求的权限均处于最小权限集内；或，对权限连续请求的时间不小于预设的第二阈值的过程中，所请求的权限均在最小权限集内，则判断容器请求的权限均处于最小权限集内。

在一个具体实现中，首先系统开启权限测调功能，即为容器权限的请求做好预处理，以

非特权模式启动容器，启动后容器尝试调用特权操作，即对于系统请求特权操作的权限；系统根据所收到的请求进程确定进行请求的容器，并获取容器信息，在收到权限请求时，判断容器信息中的最小权限集是否包含该权限，若不包含，则将该请求权限加入最小权限集，并继续接收容器的下一次权限请求；若包含，则接收容器的下一次特权请求，在连续请求次数不小于第一阈值的过程中，所有请求的权限均在最小权限集内，或连续请求时长不小于第二阈值的过程中，所有请求的权限均在最小权限集内，则判断容器所需的权限均处于最小权限集内，当前最小权限集为最终的最小权限集，可输出。

在另一个例子中，预设的初始化结束条件还例如：将请求的权限加入所述最小权限集，直到容器对应的业务实现运行，其中，所述容器对应的业务在所述容器建立时产生。由于容器在生成时存在需要实现的业务（即容器对应的业务），在一直在向最小权限集中加入请求的权限，直到检测到所需要实现的业务首次正常执行的情况下，判定当前容器请求的权限均处于最小权限集内。该需要执行的业务若存在多个阶段，每个阶段所需的权限不完全一致，则对应的初始化结束条件是需要遍历所述多个阶段，检测到所述多个阶段均正常运行，才判定所述容器对应的业务实现运行；例如存在三个阶段，则需要这三个阶段首次均实现正常执行后，判定当前容器所请求的权限均在最小权限集内。此处的检测业务是否实现运行的条件支持预设及自定义。

此外，赋予容器请求的权限，主要是为了获取最小权限集，即并不是永久赋予权限，当最小权限集形成并输出后，当前容器被赋予的权限会被收回。也就是说所请求的权限是暂时的赋予容器。

在一个具体实现中，在收到权限请求时，判断特权容器信息中的最小权限集是否包含该权限，若不包含，则临时赋予容器该权限，且将该权限置入最小权限集中。当容器所需要实现的业务正常运行时，表示容器所必要的权限均已获取，也就是容器正常运行的必要权限均处于最小权限集内，则已完成最小权限集的生成，所获取的最小权限集可输出。上述临时赋予容器权限，指的是在最小权限集输出之前，在最小权限集正在进行生成但未完成的过程中赋予权限。在容器对应的业务能够正常执行时判断最小权限集获取成功，不需要设置阈值判断最小权限集是否已完成获取，减少需要实施的准备工作，并且直接由业务的执行状况判断，所获取的最小权限集更准确，提升用户体验。

在步骤 102 中，以非特权模式启动容器，并将最小权限集作为参数传递给容器。即，在获取最小权限集后，以非特权模式重新启动容器，容器初始运行于不具有任何特权操作的权限的状态下。此时，将步骤 101 获取的最小权限集作为参数，赋予当前容器，即，容器能够获取上述最小权限集中的权限。避免容器获取非必要权限，从而威胁到系统中其他数据的安全。

在步骤 103 中，启动容器的原始进程，以最小权限集作为原始进程的权限集。按照容器的原始进程启动容器，即容器按照原需要实现的业务运行，在运行过程中具有所获取的最小权限集中的权限。其中，在上述获取最小权限集时，容器运行于第一状态，该第一状态只用于获取最小权限集，不实际进行业务运行，例如可称为测试状态；在本步骤中，启动后容器运行于第二状态，第二状态通常为实际执行业务，例如可称为生产状态；此外，第一状态与第二状态的运行环境并不进行限定，第一状态和第二状态可运行于同一环境中，或者运行在不同环境中；第一状态与第二状态的切换可以根据预设转换条件触发，例如最小权限集的生

成或传递，或接到人工输入的转换指令，或人为按动转换按钮等。

在一个例子中，启动容器的原始进程，以最小权限集作为原始进程的权限集，包括：将系统工具映射到容器的空间内；运行系统工具作为容器的初始化进程，将最小权限集作为系统工具的权限集；通过系统工具启动容器的原始进程，并将系统工具的权限集继承给原始进程的权限集。具体地，用非特权模式启动容器，将最小权限集作为参数传递给容器，也就是为容器赋予最小权限集中的权限；使用映射的方式将系统工具映射到容器的空间，运行系统工具作为容器的初始化进程；系统工具接收容器传递的最小权限集，并使用该权限集设置自己的权限集，例如将最小权限集作为自己的权限集；系统工具调用执行文件启动容器的原始进程，根据权限继承规则，系统工具的权限集通过继承的方式成为容器的原始进程的执行文件的权限集，即最小权限集作为容器的原始进程的执行文件的权限集；容器的原始进程获取正常运行所需的最小权限集，容器在运行过程中，非必须权限被删除，即容器在运行过程中不具备非必须权限，用于限制容器的数据获取权限，提高系统中其他数据的安全性。

在一个例子中，系统工具包括：capinit 工具。具体地，本实施例提供一个二级制系统工具 capinit，该工具接受启动容器时传递的最小权限集，并将该最小权限集传递给容器的原始进程，也就是传递给容器内的业务进程，例如：capinit 接收一个最小权限集作为运行时参数；使用权限设置（setcap）命令赋予 capinit 工具 CAP_SETPCAP 权限，CAP_SETPCAP 为允许向其他进程转移能力以及删除其他进程的能力，此时即使普通用户运行 capinit，也可以变更自己的权限；capinit 使用启动容器时传递的最小权限集提升自己的环境（ambient）权限；capinit 调用执行文件（execve）启动容器进程。

在一个具体实现过程中，当系统工具为 capinit 工具时，再获取容器运行所需的最小权限集之后，例如：用非特权模式启动容器，将最小权限集作为参数传递给当前容器；使用映射的方式将 capinit 映射到容器空间，运行 capinit 以完成容器的初始化进程；capinit 工具接受容器传递的最小权限集，并使用该权限集设置自己的 ambient 权限集，例如将自己的 ambient 权限集与最小权限集设置为一致；capinit 工具调用 execve 启动容器的原始进程，根据权限继承规则，capinit 的 ambient 权限集通过继承的方式成为容器的原始进程的 effective 权限集，例如，该容器的原始进程的 effective 权限集变为与最小权限集一致。从而容器的原始进程获取到正常运行所需的最小权限集，原特权容器的非必须权限被删除，避免容器无限制的请求非必要的数据，提高了系统中数据的安全性。

本实施方式中，提供了一种容器运行方法，对于特权容器，筛选出容器正常运行所需最小权限集，并在无需制作容器镜像的情况下，赋予容器必须的最小权限集合，删除非必须权限，将特权容器转换为非特权容器，降低特权容器运行异常对系统安全的威胁。

本申请的另一个实施例涉及一种容器运行装置，下面对本实施例的调度系统的细节进行具体的说明，以下内容仅为方便理解提供的实现细节，并非实施本例的必须，图 2 是本实施例所述的容器运行装置的示意图，包括：

获取模块 201，用于获取容器运行所需的最小权限集；

传递模块 202，用于以非特权模式启动容器，并将最小权限集作为参数传递给容器；

启动模块 203，用于启动容器的原始进程，以最小权限集作为原始进程的权限集。

对于获取模块 201，在一个例子中，获取容器运行所需的最小权限集，包括：将容器的最小权限集初始化为空，并将容器运行在非特权模式下；在容器的运行过程中，获取容器在

非特权模式下向系统请求的用于进行特权操作的权限，并将请求的权限加入最小权限集，赋予所述容器所述请求的权限，保证所述容器的正常运行；在满足预设的初始化结束条件后，关闭容器的运行，输出最小权限集。

在一个例子中，预设的初始化结束条件包括：容器请求的权限均处于最小权限集内。

在另一个例子中，预设的初始化结束条件包括：将所述请求的权限加入所述最小权限集，直到容器对应的业务实现运行，其中，容器对应的业务在容器建立时产生。

对于启动模块 203，启动容器的原始进程，以最小权限集作为原始进程的权限集，例如：将系统工具映射到容器的空间内；运行系统工具作为容器的初始化进程，将最小权限集作为系统工具的权限集；通过系统工具启动容器的原始进程，并将系统工具的权限集继承给原始进程的权限集。

在一个例子中，系统工具包括：capinit 工具。

本实施方式中，提供了一种容器运行装置，对于特权容器，筛选出容器正常运行所需最小权限集，并在无需制作容器镜像的情况下，赋予容器必须的最小权限集合，删除非必须权限，将特权容器转换为非特权容器，降低特权容器运行异常对系统安全的威胁。

不难发现，本实施例为与上述方法实施例对应的系统实施例，本实施例可以与上述方法实施例互相配合实施。上述实施例中提到的相关技术细节和技术效果在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在上述实施例中。

值得一提的是，本实施例中所涉及到的各模块均为逻辑模块，在实际应用中，一个逻辑单元可以是一个物理单元，也可以是一个物理单元的一部分，还可以以多个物理单元的组合实现。此外，为了突出本申请的创新部分，本实施例中并没有将与解决本申请所提出的技术问题关系不太密切的单元引入，但这并不表明本实施例中不存在其它的单元。

本申请另一个实施例涉及一种电子设备，如图 3 所示，包括：至少一个处理器 301；以及，与所述至少一个处理器 301 通信连接的存储器 302；其中，所述存储器 302 存储有可被所述至少一个处理器 301 执行的指令，所述指令被所述至少一个处理器 301 执行，以使所述至少一个处理器 301 能够执行上述各实施例中的容器运行方法。

其中，存储器和处理器采用总线方式连接，总线可以包括任意数量的互联的总线和桥，总线将一个或多个处理器和存储器的各种电路连接在一起。总线还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路连接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口在总线和收发机之间提供接口。收发机可以是一个元件，也可以是多个元件，比如多个接收器和发送器，提供用于在传输介质上与各种其他装置通信的单元。经处理器处理的数据通过天线在无线介质上进行传输，进一步，天线还接收数据并将数据传送给处理器。

处理器负责管理总线和通常的处理，还可以提供各种功能，包括定时，外围接口，电压调节、电源管理以及其他控制功能。而存储器可以被用于存储处理器在执行操作时所使用的数据。

本申请另一个实施例涉及一种计算机可读存储介质，存储有计算机程序。计算机程序被处理器执行时实现上述方法实施例。

即，本领域技术人员可以理解，实现上述实施例方法中的全部或部分步骤是可以通过程

序来指令相关的硬件来完成，该程序存储在一个存储介质中，包括若干指令用以使得一个设备（可以是单片机，芯片等）或处理器（processor）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

本领域的普通技术人员可以理解，上述各实施方式是实现本申请的具体实施例，而在实际应用中，可以在形式上和细节上对其作各种改变，而不偏离本申请的精神和范围。

权 利 要 求 书

1. 一种容器运行方法，包括：

获取容器运行所需的最小权限集；

以非特权模式启动所述容器，并将所述最小权限集作为参数传递给所述容器；

启动所述容器的原始进程，以所述最小权限集作为所述原始进程的权限集。

2. 根据权利要求 1 所述的容器运行方法，其中，所述获取容器运行所需的最小权限集，包括：

将所述容器的最小权限集初始化为空，并将所述容器运行在非特权模式下；

在所述容器的运行过程中，获取所述容器在所述非特权模式下向系统请求的用于进行特权操作的权限，并将所述请求的权限加入所述最小权限集，赋予所述容器所述请求的权限，保证所述容器的正常运行；

在满足预设的初始化结束条件后，关闭所述容器的运行，输出所述最小权限集。

3. 根据权利要求 2 所述的容器运行方法，其中，所述预设的初始化结束条件包括：

所述容器请求的权限均处于所述最小权限集内。

4. 根据权利要求 2 所述的容器运行方法，其中，所述预设的初始化结束条件包括：

将所述请求的权限加入所述最小权限集，直到所述容器对应的业务实现运行，其中，所述容器对应的业务在所述容器建立时产生。

5. 根据权利要求 1 至 4 中任一项所述的容器运行方法，其中，所述启动所述容器的原始进程，以所述最小权限集作为所述原始进程的权限集，包括：

将系统工具映射到所述容器的空间内；

运行所述系统工具作为所述容器的初始化进程，将所述最小权限集作为所述系统工具的权限集；

通过所述系统工具启动所述容器的原始进程，并将所述系统工具的权限集继承给所述原始进程的权限集。

6. 根据权利要求 5 所述的容器运行方法，其中，所述系统工具包括：capinit 工具。

7. 一种容器运行装置，包括：

获取模块，用于获取容器运行所需的最小权限集；

传递模块，用于以非特权模式启动所述容器，并将所述最小权限集作为参数传递给所述容器；

启动模块，用于启动所述容器的原始进程，以所述最小权限集作为所述原始进程的权限集。

8．一种电子设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行如权利要求1至6中任一项所述的容器运行方法。

9．一种计算机可读存储介质，存储有计算机程序，其中，所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的容器运行方法。

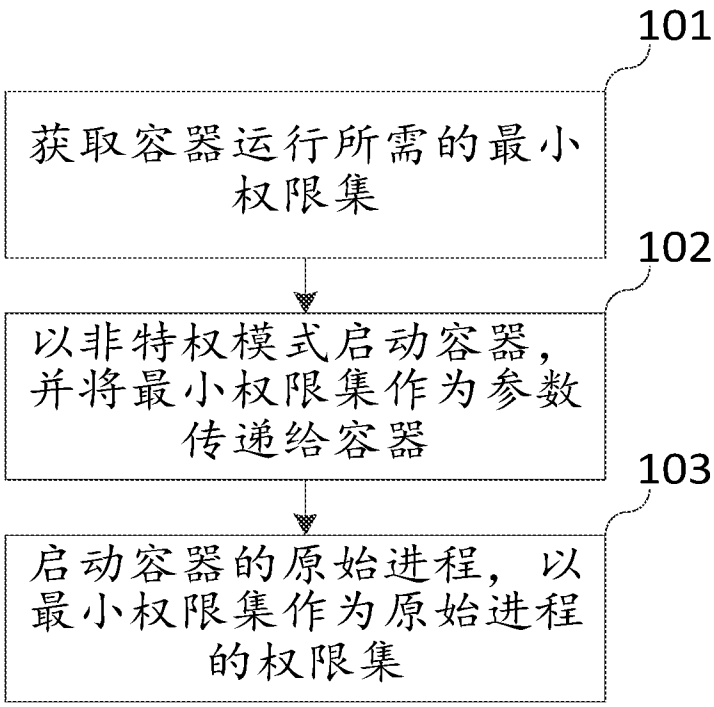
101
获取容器运行所需的最小权限集
102
以非特权模式启动容器，并将最小权限集作为参数传递给容器
103
启动容器的原始进程，以最小权限集作为原始进程的权限集

图 1

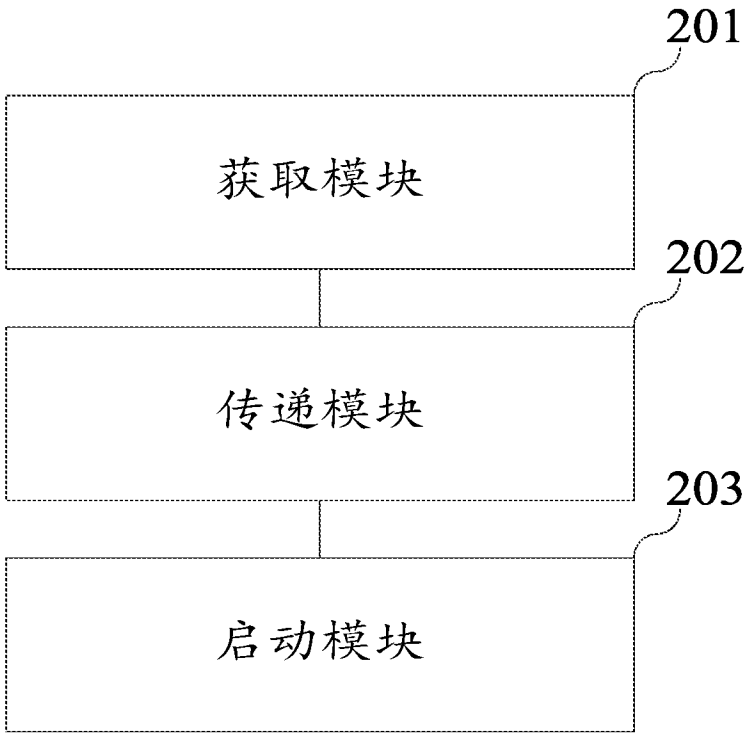

图 2

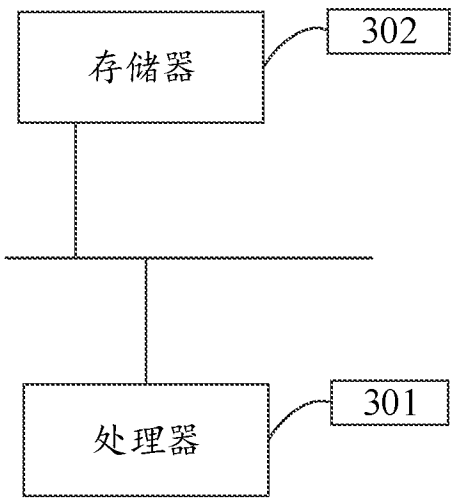

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/136683

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/31(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 容器, 特权, 最小权限, 最小权限集, docker, authority, least, target, work

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106845183 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 13 June 2017 (2017-06-13) description, paragraphs 0030-0040	1-9
Y	CN 113672974 A (BEIJING QIYI CENTURY SCIENCE & TECHNOLOGY CO., LTD.) 19 November 2021 (2021-11-19) description, paragraphs 0006-0010 and 0140-0151	1-9
A	CN 109802955 A (360 ENTERPRISE SECURITY TECHNOLOGY (ZHUHAI) CO., LTD.; BEIJING QIANXIN TECHNOLOGY CO., LTD.) 24 May 2019 (2019-05-24) entire document	1-9
A	CN 113065108 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 02 July 2021 (2021-07-02) entire document	1-9
A	CN 113221103 A (SHANDONG YINGXIN COMPUTER TECHNOLOGY CO., LTD.) 06 August 2021 (2021-08-06) entire document	1-9

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 February 2023	**20 February 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	
Facsimile No. **(86-10)62019451**	Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016366104 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 15 December 2016 (2016-12-15) entire document	1-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/136683

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106845183 A	13 June 2017	None	
CN 113672974 A	19 November 2021	None	
CN 109802955 A	24 May 2019	None	
CN 113065108 A	02 July 2021	None	
CN 113221103 A	06 August 2021	None	
US 2016366104 A1	15 December 2016	None	

国际检索报告

国际申请号
PCT/CN2022/136683

A. 主题的分类

G06F21/31(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE：容器，特权，最小权限，最小权限集，docker, authority, least, target, work

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 106845183 A (郑州云海信息技术有限公司) 2017年6月13日 (2017-06-13) 说明书第0030-0040段	1-9
Y	CN 113672974 A (北京奇艺世纪科技有限公司) 2021年11月19日 (2021-11-19) 说明书第0006-0010、0140-0151段	1-9
A	CN 109802955 A (360企业安全技术(珠海)有限公司 北京奇安信科技有限公司) 2019年5月24日 (2019-05-24) 全文	1-9
A	CN 113065108 A (支付宝（杭州）信息技术有限公司) 2021年7月2日 (2021-07-02) 全文	1-9
A	CN 113221103 A (山东英信计算机技术有限公司) 2021年8月6日 (2021-08-06) 全文	1-9
A	US 2016366104 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2016年12月15日 (2016-12-15) 全文	1-9

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"D" 申请人在国际申请中引证的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年2月15日	2023年2月20日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 高民芳 电话号码 (+86) 010-53961520

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/136683

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 106845183 A	2017年6月13日	无	
CN 113672974 A	2021年11月19日	无	
CN 109802955 A	2019年5月24日	无	
CN 113065108 A	2021年7月2日	无	
CN 113221103 A	2021年8月6日	无	
US 2016366104 A1	2016年12月15日	无	