US 20250258940A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0258940 A1**

WEI (43) **Pub. Date: Aug. 14, 2025**

(54) **CONTAINER OPERATION CONTROL METHOD AND APPARATUS**

(71) Applicant: **Beijing Volcano Engine Technology Co., Ltd.**, Beijing (CN)

(72) Inventor: **Wei WEI**, Beijing (CN)

(21) Appl. No.: **18/843,232**

(22) PCT Filed: **May 29, 2023**

(86) PCT No.: **PCT/CN2023/096771**

§ 371 (c)(1),
(2) Date: **Aug. 30, 2024**

(30) **Foreign Application Priority Data**

Jul. 21, 2022 (CN) 202210865142.9

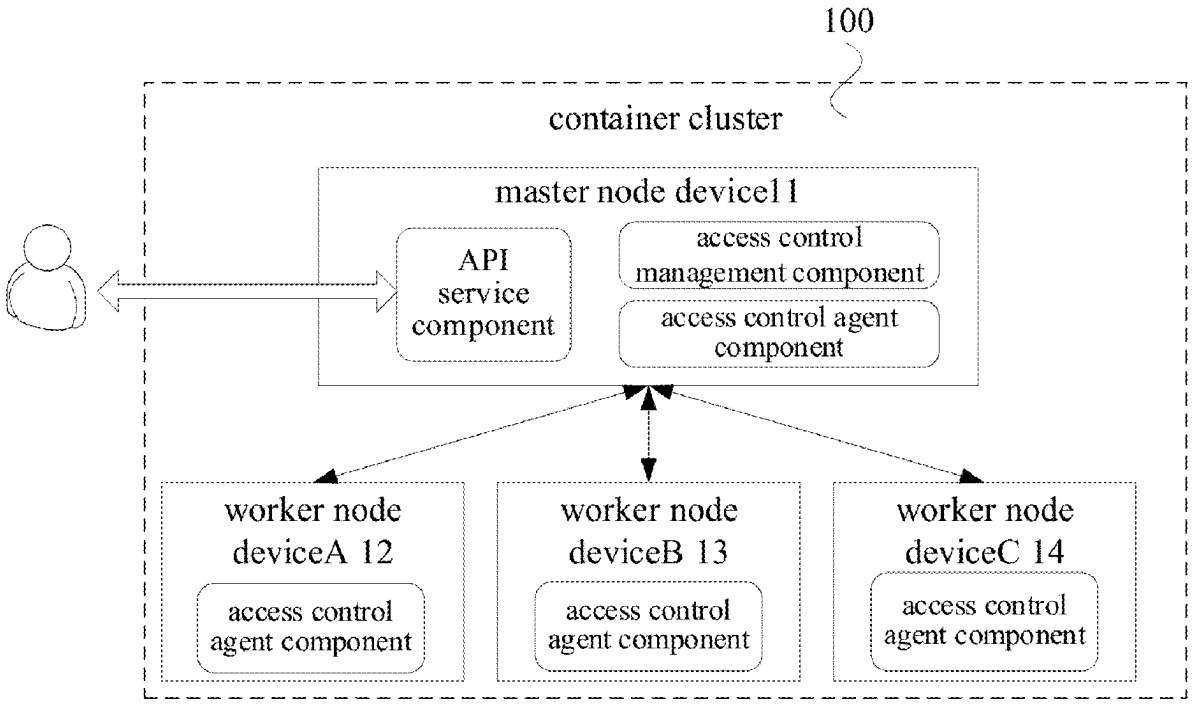
Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/604*** (2013.01); *G06F 2221/2141* (2013.01)

(57) **ABSTRACT**

The embodiments of the present disclosure relate to the technical field of computers. Provided are a container operation control method and apparatus. The method further comprises: providing at least one type of container security protection profile, which can be selected and configured by a user, wherein the at least one type of container security protection profile comprises: a container security protection profile based on a container security baseline and/or for a specified vulnerability in a container environment; receiving a profile configuration request, which is initiated on the basis of the at least one type of container security protection profile, wherein the profile configuration request comprises a profile identifier of a target container security protection profile and object information of a target protection object related to a container, and the profile configuration request is used for requesting to perform security protection on the target protection object on the basis of the target container security protection profile; and in response to the profile configuration request, starting the target container security protection profile for the target protection object, so as to perform access control on an access request on the basis of the target container security protection profile.



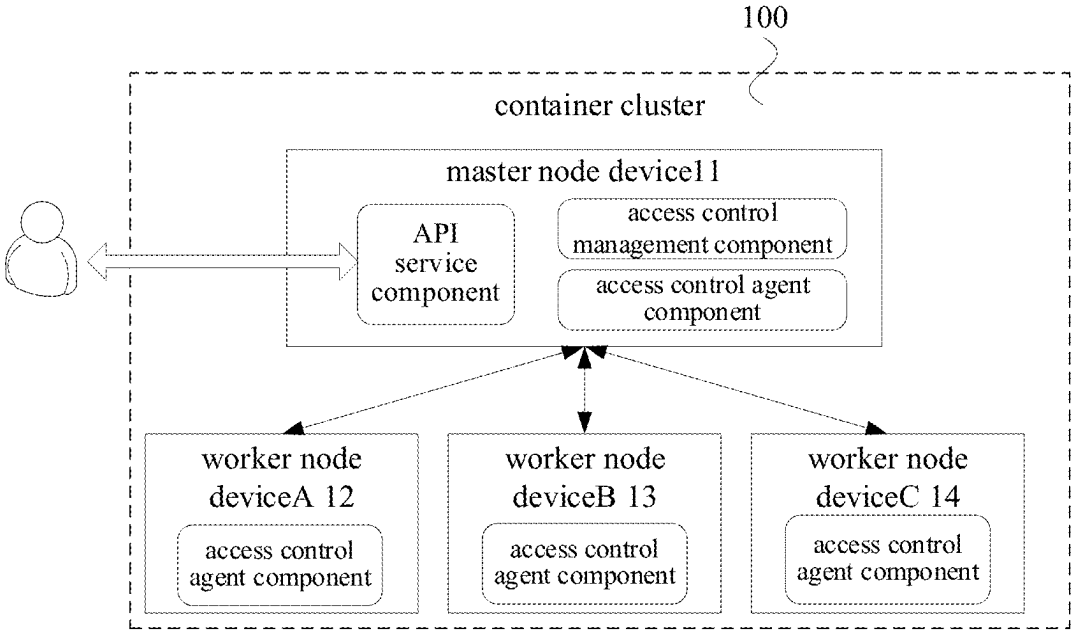

100
container cluster
master node device11
API service component
access control management component
access control agent component
worker node deviceA 12
access control agent component
worker node deviceB 13
access control agent component
worker node deviceC 14
access control agent component

FIG. 1

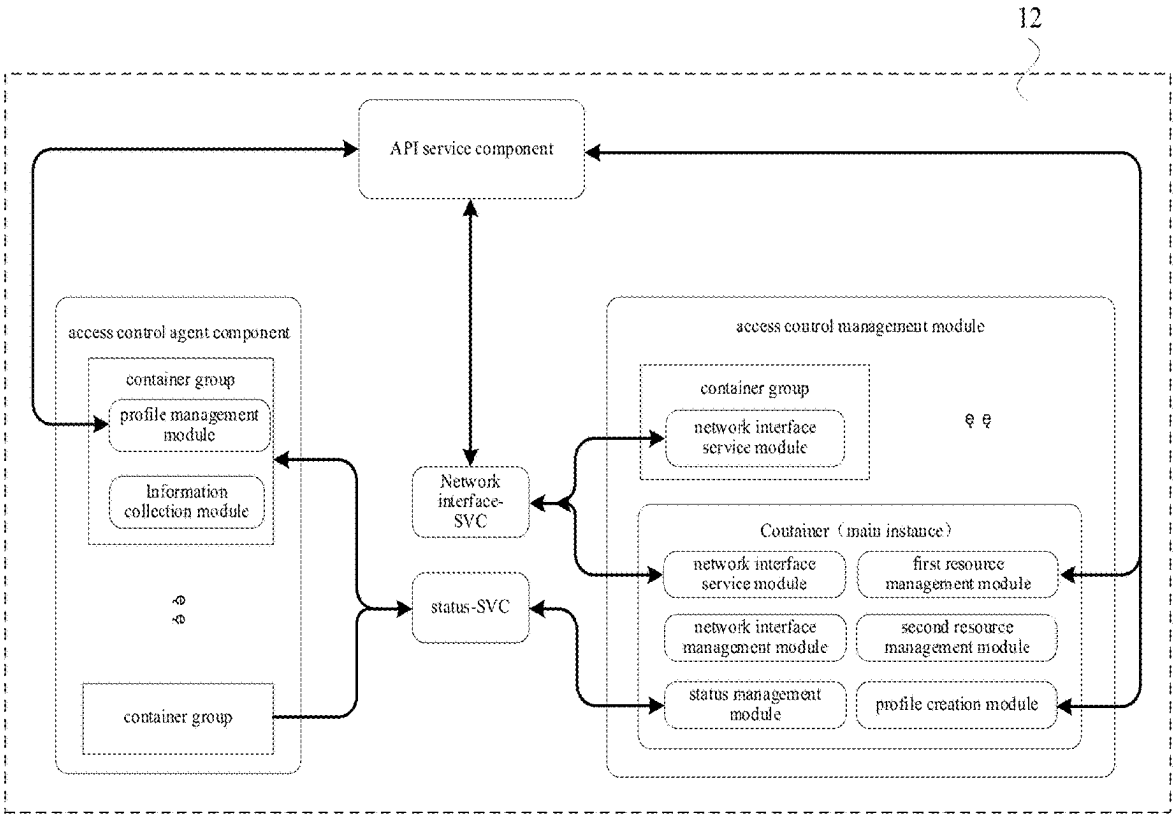

12
API service component
access control agent component
container group
profile management module
Information collection module
container group
Network interface-SVC
status-SVC
access control management module
container group
network interface service module
Container（main instance）
network interface service module
first resource management module
network interface management module
second resource management module
status management module
profile creation module

FIG. 2

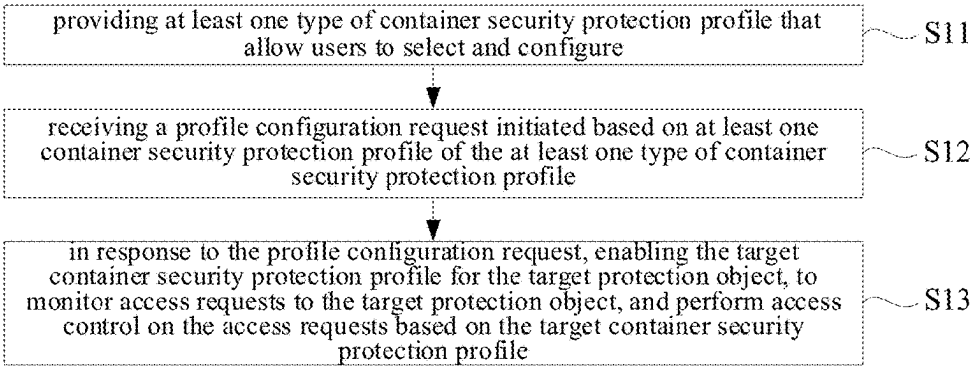

providing at least one type of container security protection profile that allow users to select and configure
S11
receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile
S12
in response to the profile configuration request, enabling the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile
S13

FIG. 3

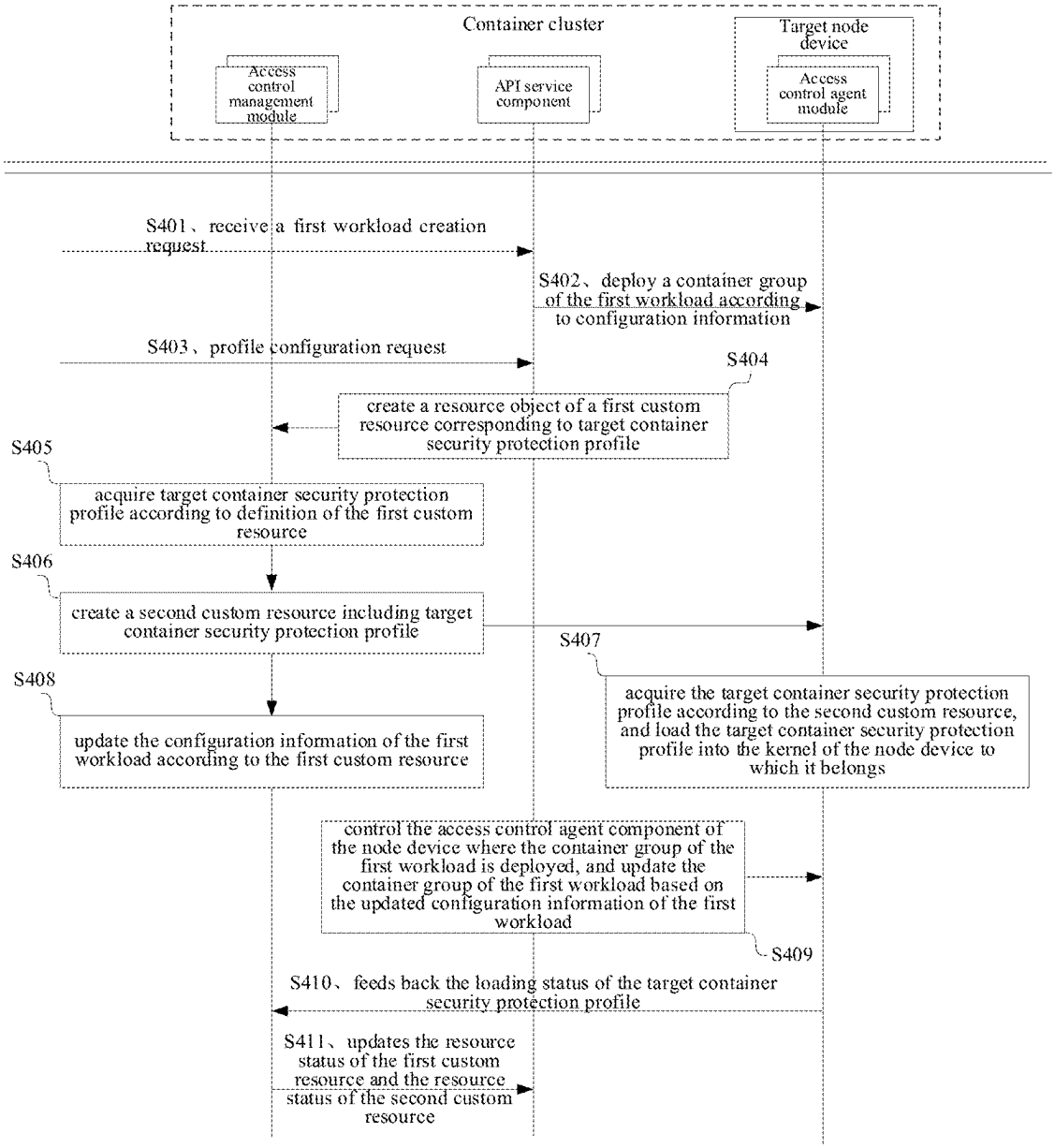

Container cluster
Target node device
Access control management module
API service component
Access control agent module
S401、receive a first workload creation request
S402、deploy a container group of the first workload according to configuration information
S403、profile configuration request
S404
create a resource object of a first custom resource corresponding to target container security protection profile
S405
acquire target container security protection profile according to definition of the first custom resource
S406
create a second custom resource including target container security protection profile
S407
acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into the kernel of the node device to which it belongs
S408
update the configuration information of the first workload according to the first custom resource
control the access control agent component of the node device where the container group of the first workload is deployed, and update the container group of the first workload based on the updated configuration information of the first workload
S409
S410、feeds back the loading status of the target container security protection profile
S411、updates the resource status of the first custom resource and the resource status of the second custom resource

FIG. 4

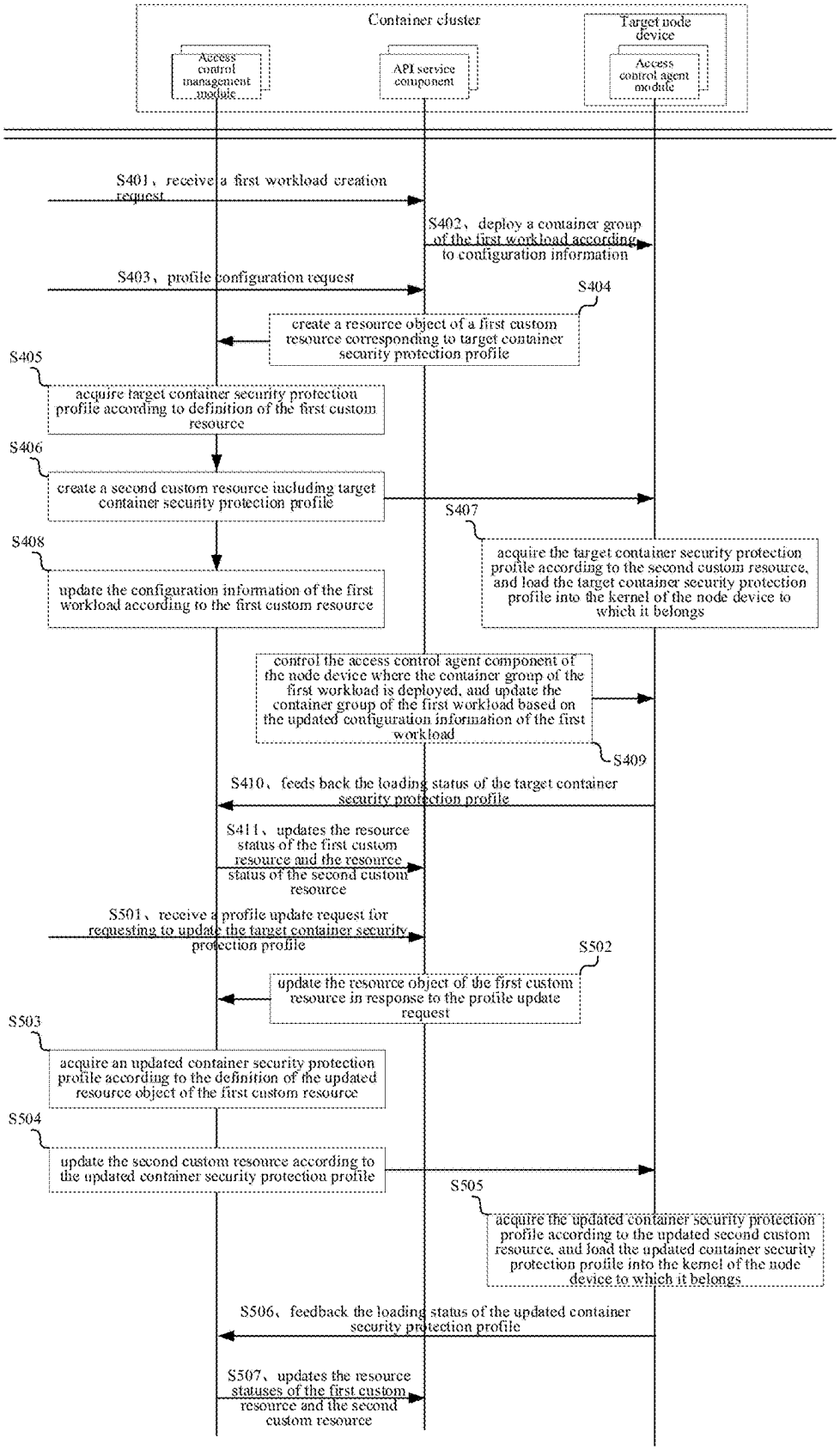

Container cluster
Target node device
Access control management module
API service component
Access control agent module
S401、receive a first workload creation request
S402、deploy a container group of the first workload according to configuration information
S403、profile configuration request
S404
create a resource object of a first custom resource corresponding to target container security protection profile
S405
acquire target container security protection profile according to definition of the first custom resource
S406
create a second custom resource including target container security protection profile
S407
acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into the kernel of the node device to which it belongs
S408
update the configuration information of the first workload according to the first custom resource
control the access control agent component of the node device where the container group of the first workload is deployed, and update the container group of the first workload based on the updated configuration information of the first workload
S409
S410、feeds back the loading status of the target container security protection profile
S411、updates the resource status of the first custom resource and the resource status of the second custom resource
S501、receive a profile update request for requesting to update the target container security protection profile
S502
update the resource object of the first custom resource in response to the profile update request
S503
acquire an updated container security protection profile according to the definition of the updated resource object of the first custom resource
S504
update the second custom resource according to the updated container security protection profile
S505
acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs
S506、feedback the loading status of the updated container security protection profile
S507、updates the resource statuses of the first custom resource and the second custom resource

FIG. 5

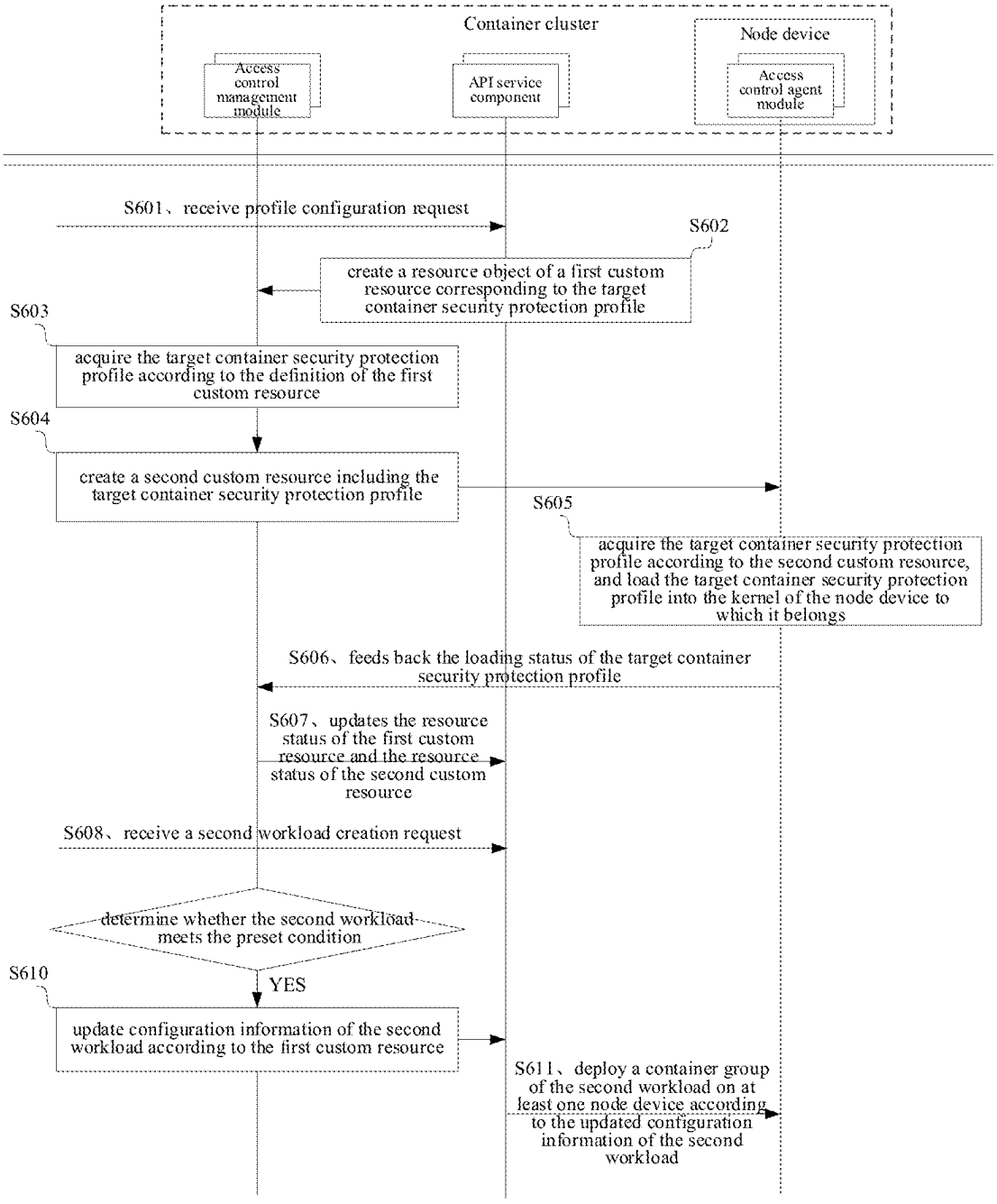

Container cluster
Node device
Access control management module
API service component
Access control agent module
S601、receive profile configuration request
S602
create a resource object of a first custom resource corresponding to the target container security protection profile
S603
acquire the target container security protection profile according to the definition of the first custom resource
S604
create a second custom resource including the target container security protection profile
S605
acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into the kernel of the node device to which it belongs
S606、feeds back the loading status of the target container security protection profile
S607、updates the resource status of the first custom resource and the resource status of the second custom resource
S608、receive a second workload creation request
determine whether the second workload meets the preset condition
YES
S610
update configuration information of the second workload according to the first custom resource
S611、deploy a container group of the second workload on at least one node device according to the updated configuration information of the second workload

FIG. 6

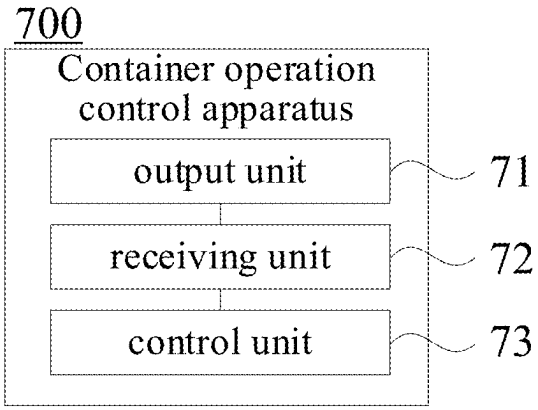

700
Container operation control apparatus
output unit
71
receiving unit
72
control unit
73

FIG. 7

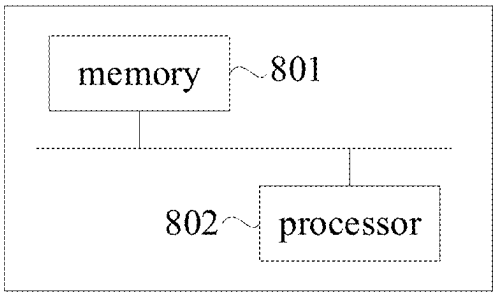

memory
801
802
processor

FIG. 8

CONTAINER OPERATION CONTROL METHOD AND APPARATUS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority to and is based on a Chinese application with an application number 202210865142.9 and a filing date of Jul. 21, 2022, the aforementioned application is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present disclosure relates to the field of computer technology, and in particular to a container operation control method and apparatus.

BACKGROUND

[0003] AppArmor is a Mandatory Access Control (MAC) system implemented based on a Linux Security Module (LSM) and is used to restrict the behavior of application processes based on Discretionary Access Control (DAC).

DISCLOSURE OF THE INVENTION

[0004] Embodiments of the present disclosure provide a container operation control method and apparatus.

[0005] The technical solutions provided by the embodiments of the present disclosure are as follows:

[0006] In a first aspect, an embodiment of the present disclosure provides a container operation control method, including:

[0007] providing at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

[0008] receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

[0009] in response to the profile configuration request, enabling the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile.

[0010] In a second aspect, an embodiment of the present disclosure provides a container operation control apparatus, including:

[0011] an output unit, configured to provide at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

[0012] a receiving unit, configured to receive a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

[0013] a control unit, configured to, in response to the profile configuration request, enable the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile.

[0014] In a third aspect, an embodiment of the present disclosure provides an electronic device, comprising: a memory and a processor, wherein the memory is configured to store a computer program; and the processor is configured to execute the computer program, so as to cause the electronic device to implement the container operation control method described in any of the above embodiments.

[0015] In a fourth aspect, an embodiment of the present disclosure provides a computer-readable storage medium, a computer program, when executed by a computing device, causes the computing device to implement the container operation control method described in any of the above embodiments.

[0016] In a fifth aspect, an embodiment of the present disclosure provides a computer program product which, when running on a computer, causes the computer to implement the container operation control method described in any of the above embodiments.

[0017] The container operation control method provided by embodiments of the present disclosure first provides at least one type of container security protection profile that allow users to select and configure, then receive a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, in response to the profile configuration request, enables the target container security protection profile for the target protection object, and monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile.

DESCRIPTION OF THE DRAWINGS

[0018] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments according to the present disclosure, and together with the description, serve to explain the principles of the present disclosure.

[0019] In order to more clearly illustrate the technical solutions in the embodiments of the present disclosure or related technologies, the drawings required for use in the embodiments or related technical descriptions are briefly introduced below, and it is obvious for ordinary skilled in the art that other drawings can be derived based on these drawings without paying any creative labor.

[0020] FIG. **1** is a first architecture diagram of the container operation control method provided by an embodiment of the present disclosure;

[0021] FIG. **2** is a second architecture diagram of the container operation control method provided by an embodiment of the present disclosure;

[0022] FIG. **3** is a first interactive flowchart diagram of the container operation control method provided by an embodiment of the present disclosure;

[0023] FIG. **4** is a second interactive flowchart diagram of the container operation control method provided by an embodiment of the present disclosure;

[0024] FIG. **5** is a third interactive flowchart diagram of the container operation control method provided by an embodiment of the present disclosure;

[0025] FIG. **6** is a fourth interactive flowchart diagram of the container operation control method provided by an embodiment of the present disclosure;

[0026] FIG. **7** is a schematic structural diagram of the container operation control apparatus provided by an embodiment of the present disclosure;

[0027] FIG. **8** is a schematic diagram of the hardware structure of an electronic device provided in an embodiment of the present disclosure.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0028] In order to more clearly understand the above objects, features and advantages of the present disclosure, the scheme of the present disclosure will be further described below. It should be noted that, in the absence of conflict, the embodiments of the present disclosure and the features therein may be combined with each other.

[0029] In the following description, many specific details are set forth to facilitate a full understanding of the present disclosure, but the present disclosure may also be implemented in other ways different from those described herein; it is obvious that the embodiments in the specification are only part of the embodiments of the present disclosure, rather than all of the embodiments.

[0030] In embodiments of the present disclosure, words such as "exemplary" or "for example" are used to indicate examples, instances or illustrations. Any embodiment or design scheme described as "exemplary" or "for example" in the embodiments of the present disclosure should not be construed as preferred or advantageous over other embodiments or designs. Rather, invocations of words such as "exemplary" or "such as" are intended to present relevant concepts in a concrete manner. Furthermore, in the description of the embodiments of the present disclosure, unless otherwise specified, "plurality" means two or more.

[0031] Currently, cloud products usually adopt default universal security protection strategies, which have relatively weak protection capabilities, resulting in serious container security risks, if users want to improve security protection capabilities, they need to write their own security protection strategies for configuration, however, writing and configuring strategies face very high technical thresholds, and are difficult to implement universally. Therefore, a container security solution with higher applicability and security is required.

[0032] AppArmor restricts the behavior of a process by, on a kernel call path of the process, acquiring a container security protection profile (AppArmor Profile) that the process should follow based on a process security context label, and then performing mandatory access control based on the container security protection profile to decide whether to allow the process to perform a corresponding operation. Currently, when a mainstream container operates, the component may have a built-in default container security protection profile (Default AppArmor Profile), during the runtime when the component detects that the operating system supports AppArmor, it will enable sandbox protection for a container based on the default container security protection profile when the container is built. However, since the default container security protection profile needs to be applicable to various scenarios, it only contains very basic container security protection policies, which results in the protection strength of AppArmor being very limited, and during the container operates, component will not enable protection for a privileged container.

[0033] To enhance the protection strength of AppArmor, a certain container cluster, such as Kubernetes, etc., already supports setting a custom container security profile for a workload. However, current container clusters do not provide management and loading of custom container security policies. Before enabling a custom container security protection profile for a protection object, users are required to complete the writing, testing, loading, and configuration of the custom container security protection policies, then the custom container security protection policies can be used for security protection for custom container of a workload, which has a high threshold for use. To solve the above problem, the container operation control method provided in an embodiment of the present disclosure pre-creates at least one type of container security protection profile that allow users to select and configure, when a user needs to perform access control on the target protection object through a custom container security protection profile (target container security protection profile), the user only needs to select the container security protection profile to be used from the container security protection policies that allow users to select and configure provided by the container cluster, and carry a profile identifier of the container security protection profile to be used in the profile configuration request, then the container cluster can obtain the corresponding container security protection profile according to the profile identifier carried in the profile configuration request, and then enable the container security protection profile for the target protection object, to monitor an access request to the target protection object, and perform access control on the access request of the target protection object based on the container security protection profile to be used, there is no need for the user to write, test, load, and configure a custom container security protection profile, therefore, the embodiment of the present disclosure can lower the threshold for using containers in the container cluster corresponding to AppArmor for security protection.

[0034] The following first describes a scenario architecture of the container operation control method provided by an embodiment of the present disclosure.

[0035] Referring to FIG. **1**, the scenario architecture of the container operation control method provided by the embodiment of the present disclosure includes: a container cluster **100**.

[0036] The container cluster **100** includes: a master node device **11** and multiple worker node devices. In FIG. **1**, the container cluster **100** includes a worker node device A **12**, a worker node device B **13**, and a worker node device C **14**, as an example.

[0037] The master node device **11** runs an application programming interface (API) service component, an access control management component (Manager) and an access control agent component (Agent) for a container cluster, and each worker node device runs an access control agent component thereon. The access control management component belongs to a stateless service, is deployed in Deployment mode, and enables multiple copies, its main functions include: 1. managing custom resources as a Custom Resource Define (CRD) management module; 2. communicating with the access control agent component as a server to manage resource status; 3. creating a container security protection profile for a workload; 4. serving as an admission control network interface server (admission controller webhook server), mutating the configuration information of the workload according to the built container security protection profile, specifying the container security protection profile for the workload, and thus enabling sandbox protection for the workload. The access control agent component belongs to a stateless service and is deployed to each node device in the container cluster in DaemonSet mode. The main functions of the access control agent component include: 1. monitoring CRD resources to manage container security protection policies; 2. managing extended Berkeley Packet Filter (eBPF) & audit function (auditd) to monitor and collect workload behaviors; 3. feedbacking the status and behavior information to the master node device.

[0038] Further, referring to FIG. **2** which is schematic structural diagram of another type of container cluster. The container cluster **100** includes: an API service component, an access control management component, and an access control agent component.

[0039] Among them, the access control management component mainly includes the following functional modules:

[0040] 1. Network interface service module (Webhook Server): this module is managed by all instances of the access control management component. It is mainly used to: maintain the container security protection profile cache, receive admission request initiated by the API service component, and mutate the configuration information about the workload according to the container security protection profile to be used when the workload is built or updated, so as to set the container security protection profile (AppArmor Profile) to be used for the workload.

[0041] 2. Network interface service management module (Webhook Manager): This module is managed by a main instance of the access control management component, and is mainly used to perform management, generation and updating of certificate for the network interface configuration of the container cluster, register mutating network interface configuration (Mutating Webhook Configuration) resources, etc., for the Webhook Server, and dynamically adjust matching rules for the network interfaces according to the configured container security protection profile, thereby determining which access requests will be sent from the API service component to the network interface service.

[0042] 3. Status management module (Status Manager): This module is managed by the main instance of the access control management component and is used to manage a status service. The status service is used to receive status reporting information from the access control agent component, and maintain component status, the status of container security protection profile for each node device, or the like.

[0043] 4. First resource management module (VarmorPolicy Operator): This module is managed by the main instance of the access control management component and is mainly used to manage a first type of custom resources (VarmorPolicy) in the container cluster. The way in which the first resource management module manages the first type of custom resources includes: in response to creation of the first type of custom resources, calling a profile creation module (Profile Builder) to generate a container security protection profile, then creating corresponding second type of custom resources (ArmorProfile), and maintaining the status of the second type of custom resources.

[0044] 5. Second resource management module (ArmorPolicy Operator): This module is managed by the main instance of the access control management component and is mainly used to maintain the status of the second type of custom resources in the cluster.

[0045] 6. Profile creation module (Profile Builder): This module is managed by the main instance of the access control management component; the profile creation module generates container security protection policies based on the first type of custom resources built by the user and encapsulates them into the second type of custom resources.

[0046] The access control agent component mainly includes the following functional modules:

[0047] 1. Profile Management Module (Profile Manager): This module is managed by the access control agent component on each node device in the container cluster, is responsible for monitoring the resource objects of the second type of custom resources and managing the creation, updating, loading, and unloading of container security protection policies on a host machine based on definitions of the monitored resource objects of the second type of custom resources.

[0048] 2. Information recording module (Recorder): This module is managed by the access control agent component on each node device in the container cluster, and is responsible for collecting status and behavior information of the node devices and containers, and reporting it to the access control management component.

[0049] An execution subject of the container operation control method provided in the embodiment of the present disclosure may be a container cluster; for example: Kubernetes (abbreviated as K8s or Kube).

[0050] Based on the above system architecture, an embodiment of the present disclosure provides a container operation control method. As shown in FIG. **3**, the container operation control method may include the following steps:

[0051] S**11**. providing at least one type of container security protection profile that allow users to select and configure.

[0052] Wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment.

[0053] In some embodiments, the container cluster may provide the user with at least one type of container security protection profile that allow users to select and configure through a profile selection-configuration interface.

[0054] The container security baseline in the embodiment of the present disclosure refers to a minimum-security requirement in the container environment.

[0055] In a scenario where a container cluster is running, the security of the container cluster is strongly related to the workloads and resources deployed in the container cluster. Unsafe workload configurations can bring varying degrees of security risks, some of which can even directly cause serious hazards such as container escape. Therefore, configuration information about the workload is an important factor affecting the security of a container cluster. The security standard and practice for a container cluster provide requirements and guidance for the secure configuration of workload to reduce security risks introduced by the workload configuration information and ensure the isolation of the container. However, in a large number of production environments, such these important security requirements are still not followed or cannot be followed due to various reasons. For example: privileges are configured for workloads without following the least privilege principle, privileges are incorrectly configured due to lack of understanding of related security risks, and some components require privileges to operate normally. These workloads that do not meet the security baseline will impact a greater potential safety hazard to the cluster. Based on this, the present disclosure provides, in some embodiments, container security protection strategies based on container security baselines for users to select and configure, so that users can reinforce workloads with security risks, thereby providing protection capabilities before the workloads are redesigned, rectified, and redeployed, thereby achieving goals of blocking attack vectors commonly used by attackers, increasing utilization costs, and enhancing container isolation.

[0056] As an optional implementation of the embodiment of the present disclosure, the container security protection strategy based on the container security baseline includes at least one of the following container security protection strategies ①-⑩:

[0057] ①. It is prohibited to rewrite kernel parameters of the host.

[0058] The path of kernel parameters of the host is /proc/sys/kernel/core_pattern, therefore, the host's kernel parameters can be prohibited from being rewritten by prohibiting rewriting of files with the file path of /proc/sys/kernel/core_pattern, thereby blocking the container escaping due to rewriting the host's kernel parameters.

[0059] ②. It is prohibited to mount a process file system (procfs) with read and write permissions.

[0060] ③. It is prohibited to mount the host disk device with read and write permissions.

[0061] ④. It is prohibited to read and write the host disk device.

[0062] ⑤. It is prohibited to rewrite an agent release file of a subsystem of the host control group.

[0063] ⑥. It is prohibited to mount a subsystem of the host control group;

[0064] ⑦. It is prohibited to use specified privileged capabilities.

[0065] The privileged capabilities include CAP_AUDIT_CONTROL, CAP_AUDIT_READ, CAP_AUDIT_WRITE, CAP_BLOCK_SUSPEND, etc., therefore, it is prohibited to use each privileged capability separately as a container security protection strategy, or privileged capabilities can be combined, and it is prohibited to use multiple privileged capabilities after combination as a container security protection strategy.

[0066] ⑧. It is prohibited to use privileged capabilities in a namespace.

[0067] That is, any privileged capability is prohibited from being used within the namespace.

[0068] ⑨. It is prohibited to use specified privileged capabilities in a namespace.

[0069] Similarly, it is prohibited to use each privileged capability separately as a container security protection strategy in the namespace, or privileged capabilities can be combined, and it is prohibited to use multiple privileged capabilities after combination as a container security protection strategy in the namespace.

[0070] ⑩. It is prohibited to use AF_PACKET protocol family to create sockets.

[0071] That is, the container security protection strategies based on the container security baseline and their security protection effects can be shown in Table 1 below:

TABLE 1

container security protection strategy	security protection effect of container security protection strategy
Forbidden to rewrite kernel parameters of the host	block container escaping due to rewriting the host's kernel parameters
Forbidden to mount a process file system with read and write permissions	block mounting a process file system (procfs) with read and write permissions and carrying out information leakage and container escaping
Forbidden to mount the host disk device with read and write permissions	block mounting the host disk device and carrying out host information leakage and/or container escaping (Note: the path of the magnetic disk can be acquired dynamically, such as /dev/sda*)
Forbidden to read and write the host disk device	block reading and writing files in disk through writing and reading the host disk device and carry outing host information leakage and/or container escaping
Forbidden to rewrite an agent release file of a subsystem of the host control group	block carrying out container escaping by rewriting agent releasing file of a sub-system of a host control group (/sys/fs/cgroup/*/release-agent in cgroups)
Forbidden to mount a subsystem of the host control group	block carrying out container escaping by mounting the sub-system in a host device control group

TABLE 1-continued

Forbidden to use specified privileged capabilities	forbidden to strengthen container and reduce attack face by using one or more of following privileged capabilities CAP_AUDIT_CONTROL, CAP_AUDIT_READ, CAP_AUDIT_WRITE, CAP_BLOCK_SUSPEND, CAP_BPF, CAP_CHECKPOINT_RESTORE, CAP_CHOWN, CAP_DAC_OVERRIDE, CAP_DAC_READ_SEARCH. CAP_FOWNER, CAP_FSETID, CAP_IPC_LOCK,
Forbidden to use privileged capabilities in a namespace	CAP_IPC_OWNER, CAP_KILL, CAP_LEASE, CAP_LINUX_IMMUTABLE, CAP_MAC_ADMIN, CAP_MAC_OVERRIDE, CAP_MKNOD, CAP_NET_ADMIN, CAP_NET_BIND_SERVICE, CAP_NET_BROADCAST, CAP_NET_RAW, CAP_PERFMON, CAP_SETGID, CAP_SETFCAP, CAP_SETPCAP, CAP_SETUID, CAP_SYS_ADMIN, CAP_SYS_BOOT, CAP_SYS_CHROOT,
Forbidden to use specified privileged capabilities in a namespace	CAP_SYS_MODULE, CAP_SYS_NICE, CAP_SYS_PACCT, CAP_SYS_PTRACE, CAP_SYS_RAWIO, CAP_SYS_ RESOURCE, CAP_SYS_TIME, CAP_SYS_TTY_CONFIG, CAP_SYSLOG, CAP_WAKE_ALARM
Forbidden to use AF_PACKET protocol family to build sockets	block using AF_PACKET protocol family to build sockets and perform network sniffing

[0072] Software vulnerabilities cannot be completely eliminated and will continue to emerge as software changes. In the rapidly developing cloud-native field, some newly discovered vulnerabilities (0 day vulnerabilities) with serious consequences often appear. Some of these software vulnerabilities can only be fixed by migrating services and restarting the host or container, while some are caused by design flaws in related components and lack a thorough repair solution, and yet others are even introduced by the features or functions of the software and cannot be fixed. These different types of vulnerabilities may pose security risks to the user's online environment due to reasons such as difficulty in repairing, long repair cycles, and inability to repair completely, and so on. The method and system provided by the present disclosure can block or mitigate (increase the cost of vulnerability exploitation) the exploitation (attack) of some specific vulnerabilities through a sandbox mechanism, thereby minimizing the security risks in the window period before the vulnerability is fixed.

[0073] As an optional implementation of the embodiment of the present disclosure, the container security protection strategy for a specified vulnerability in a container environment includes at least one of the following container security protection strategies I-X:

[0074] I. it is prohibited to read the credential for communicating with the container cluster's API service.

[0075] The path of the credential for communicating with the container cluster's API service is/run/secrets/kubernetes.io/serviceaccount/token, therefore, by prohibiting the reading of the file with the file path/run/secrets/kubernetes.io/serviceaccount/token, an attack method of acquiring the credential for communicating with the container cluster's API service can be blocked.

[0076] II. it is prohibited to read the path of the container in the host machine.

[0077] The path of the container in the host is generally stored in files with the paths /proc/mounts, /proc/[PID]/mounts, and /proc/[PID]/mountinfo, therefore, the reading of the path of the container in the host can be blocked by prohibiting reading of files with the paths /proc/mounts, /proc/[PID]/mounts, and /proc/[PID]/mountinfo.

[0078] III. It is prohibited to read the disk device number of the host machine.

[0079] IV. It is prohibited to read the network protocol IP address of the host machine.

[0080] V. It is prohibited to execute specified executable files.

[0081] The executable files specified in the embodiment of the present disclosure can be set according to the executable file to be used in each attack manner. Exemplarily, the specified executable files may include: /bin/sh file, /bin/bash file, /bin/dash file, /bin/busybox file, /usr/bin/wget file, /bin/wget file, etc.

[0082] VI. It is prohibited to modify file permissions.

[0083] VII. It is prohibited to rewrite the directory and configuration files of system configuration files.

[0084] VIII. It is prohibited to escalate permissions.

[0085] IX. It is prohibited to perform local inter-process communication via UNIX sockets.

[0086] X. It is prohibited to access to specified files through NGINX service.

[0087] In the embodiment of the present disclosure, any file that needs to be kept strictly confidential or that would cause serious consequences if stolen can be set as a specified file. For example, the specified files may include: the path of the container in the host machine, the IP address of the host machine, the MAC address of the host machine, etc.

TABLE 2

container security protection strategy	security protection effect of container security protection strategy
prohibited to read credential for communicating with API service of container cluster	block acquiring credential for communicating with API service of container cluster by reading the file with the file path /run/secrets/kubernetes.io/serviceaccount/token
prohibited to read path of container in the host machine	block acquiring path of container in the host machine by reading files such as /proc/mounts, /proc/[PID]/mounts, and /proc/[PID]/mountinfo
prohibited to read disk device number of the host machine	block acquiring disk device number of the host machine by reading files such as /proc/[PID]/mountinfo, /proc/partitions

TABLE 2-continued

prohibited to read network protocol IP address of the host machine	block acquiring the host IP by reading files such as /proc/net/arp, /proc/[PID]/net/arp
prohibited to execute specified executable files	the executable files may include one or more of: /bin/sh file, /bin/bash file, /bin/dash file, /bin/busybox file, /usr/bin/wget file, /bin/wget file, to block shell utilization, downloading of external files, issuance of network request
prohibited to modify file permissions	block modifying file permissions by executing /bin/chmod (Note: in some scenarios, it shall be utilized along with a category "prohibited to execute busybox command")
prohibited to rewrite configuration file directory and configuration files	block writing operation on configuration file directory (/etc directory) and configuration file (/etc) to prevent attacks such as premission escalation, persistence
prohibited to escalate permissions	block writing operation on configuration file directory (/etc directory) to prevent attacks such as premission escalation, persistence
prohibited to perform local inter-process communication via UNIX sockets	mitigate attack utilizing CVE-2020-15257 vulnerability
prohibited to access to specified files through NGINX service	mitigate attack utilizing vulnerability of Kubernetes Ingress-nginx component

[0088] S**12**. receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile.

[0089] Wherein the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile.

[0090] In the embodiment of the present disclosure, the target protection object may be a specific workload or a container group or a container or an application in a container. In actual use, the target protection object can be specified through information about the workload or container group or container or application, such as, label, type, namespace, name and other. That is, the object information of the target protection object may be a label, type, namespace, name, etc. of a workload or a container group or a container or an application.

[0091] In the embodiment of the present disclosure, the target protection object may also be a workload or a container group or a container or an application that meets preset conditions, and the target protection object can be specified by setting the preset conditions. When creating a workload, it can be determined whether the currently built or built workload or container group or container or application belongs to the target protection object by judging whether the workload or container group or container or application meets the preset conditions. That is, the object information of the target protection object may be the condition that the target protection object needs to meet.

[0092] S**13**. in response to the profile configuration request, enabling the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile.

[0093] The container operation control method provided by the embodiment of the present disclosure first provides at least one type of container security protection profile that allow users to select and configure, then receives a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, in response to the profile configuration request, enable the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile. Since the container operation control method provided by the embodiment of the present disclosure provides a user with at least one type of container security protection profile that allow users to select and configure, when the user needs to perform access control on a target protection object through a target container security protection profile, the user only needs to select the target container security protection profile from the provided container security protection profiles that allow users to select and configure, without needing to write the target container security protection profile, therefore, the embodiment of the present disclosure can reduce the user's writing of container security protection policies, thereby lowering the threshold for using container sandbox protection.

[0094] As an optional implementation of the embodiment of the present disclosure, the above step S**13** (in response to the profile configuration request, enable the target container security protection profile for the target protection object) includes:

[0095] based on the object information of the target protection object, enabling the target container security protection profile for the container group of the target protection object, the container of the target protection object, or the application of the target protection object.

[0096] That is, the minimum access control granularity for the target container security protection profile in the embodiment of the present disclosure is an application in the container.

[0097] Although the above at least one type of container security protection profile that allow users to select and configure provided by the container cluster can provide

security protection against specific risks or specific attack manners, in some cases the container security protection profile may conflict with the needs of the application service itself, resulting in the normal operation of the application service being blocked by the container security protection profile. For example, an application service may need to read a credential (Service Account token) for communicating with the container cluster's API service and then interact with the container cluster's API service, while if the target container security profile includes a container security profile that prohibits reading the credential for communicating with the container cluster's API service, the container security profile will prevent the application service from reading the credential for communicating with the container cluster's API service, thereby causing that the application service cannot interact with the API service. For another example, an application service may need to execute a bash executable file, if a container security protection profile that prohibits the execution of bash executable files is selected, the container security protection profile will prevent the application service from executing bash.

[0098] The target protection object of the target container security protection strategy described in the above embodiment can be a container group of the target protection object or a container in the container group or an application in the container. Therefore, the above embodiment can enable the target container security protection strategy for only the container group or container or application that will not conflict with the behavior of the application service itself, thereby blocking penetration and increasement of penetration costs without affecting the normal operation of the application service.

[0099] As an expansion and refinement of the above embodiment, the present disclosure provides another container operation control method. As shown in FIG. **4**, the container operation control method includes:

[0100] S**401**: An API service component of a container cluster receives a first workload creation request.

[0101] Where, the first workload creation request carries configuration information of the first workload, and is used to request creation of the first workload according to the configuration information.

[0102] The first workload in the embodiment of the present disclosure may be a resource of a namespace type such as Deployment, DaemonSet, or StatusfulSet, etc., and the system interfaces that also are of the namespace type may correspond one-to-one with the workloads.

[0103] S**402**: The API service component deploys a container group of the first workload on at least one target node device of the container cluster according to the configuration information.

[0104] It should be noted that the target node device may be a master node device in the container cluster, or a worker node device in the container cluster, or may include both a master node device and a worker node device.

[0105] S**403**: The API service component receives a profile configuration request.

[0106] Among them, the profile configuration request includes a profile identifier of the target container security protection profile and object information of a target protection object related to the container, and the profile configuration request is used to request security protection for the target protection object based on the target container security protection profile; the target protection object includes the first workload.

[0107] S**404**. The API service component creates a resource object of a first custom resource corresponding to the target container security protection profile.

[0108] Since the definition of the first custom resource includes declaration information of each target protection object, the definition of the first custom resource includes declaration information of the first workload.

[0109] The first custom resource in the embodiment of the present disclosure is a first type of custom resource (VarmorProfile), and may be a namespace type of resource that is consistent with the namespace of the target protection object. The target protection object is used to define the workload to be performed access control, and may include: resource type, name, container group/container/application name list, or label selector, to enable sandbox protection for eligible workloads through the label mechanism.

[0110] S**405**. The access control management component of the container cluster acquires the target container security protection profile according to the definition of the first custom resource.

[0111] In some embodiments, an access control management component of a container cluster may monitor an object of a resource object of a first custom resource in real time, and in response to the resource object of the first custom resource being created, a target container security protection profile can be acquired according to a definition of the first custom resource.

[0112] S**406**: The access control management component of the container cluster creates a second custom resource including the target container security protection profile.

[0113] The target container security protection profile is managed in the container cluster system in a resource manner, so the second custom resource is the target container security protection profile.

[0114] In some embodiments, the access control management component encapsulates the target container security protection profile into a second type of custom resource to generate a second custom resource.

[0115] As an optional implementation of the embodiment of the present disclosure, the first custom resource, the second custom resource, and the target protection object are resources in the same namespace.

[0116] The second custom resource in the embodiment of the present disclosure is a second type of custom resource (ArmorProfile), and is a namespace type of resource that is consistent with the namespace of the target protection object. The second type of custom resource shields underlying logic, is only used in the system internally and is mainly used to define target protection objects and target container security protection policies.

[0117] In some embodiments, the first custom resource, the second custom resource, and the target protection object are resources in the same namespace.

[0118] Since the first custom resource, the second custom resource, and the target protection object are resources in the same namespace, the embodiment of the present disclosure can allow users to operate the first custom resource in the corresponding namespace and perform access control on the workload in the namespace; at the same time, it can restrict users of other namespaces from operating the first custom

resource and the second custom resource in the namespace, thereby further improving the security and usability of the access control scheme.

[0119] S**407**. The access control agent component of the node device (the at least one target node device) in the container cluster, where the container group of the first workload is deployed, acquires the target container security protection profile according to the second custom resource, and loads the target container security protection profile into the kernel of the node device to which it belongs.

[0120] S**408**: The access control management component updates the configuration information of the first workload according to the first custom resource.

[0121] It should be noted that the execution order of the above steps S**407** and S**408** is not limited in the embodiment of the present disclosure, S**407** may be executed first and then S**408**, or S**407** and S**408** may be executed in parallel.

[0122] S**409**. The API service component controls the access control agent component of the node device (the at least one target node device), where the container group of the first workload is deployed, and updates the container group of the first workload based on the updated configuration information of the first workload.

[0123] As an optional implementation of the embodiment of the present disclosure, in the above step S**409** (the API service component controls the access control agent component of the node device, where the container group of the first workload is deployed, and updates the container group of the first workload based on the updated configuration information of the first workload), it includes:

[0124] in response to the configuration information of the first workload being updated, the API service component controls the node device (the at least one target node device), where the container group of the first workload is deployed, to perform a rolling update on the container group of the first workload.

[0125] S**410**. The access control agent component of the node device, where the container group of the first workload is deployed, respectively feeds back the loading status of the target container security protection profile into the corresponding node device to the access control management component.

[0126] S**411**. The access control management component updates the resource status of the first custom resource and the resource status of the second custom resource according to the loading status of the target container security protection profile fed back by respective node devices, where the container group of the first workload is deployed.

[0127] The embodiment shown in FIG. **4** above provides an implementation method for enabling sandbox protection for an existing workload (first workload), and because the above embodiment converts the target container security protection profile into resources in the container cluster, the above embodiment can make the use of the container sandbox cloud-native, thereby obtaining a user experience consistent with that of other resources in the container cluster.

[0128] As an optional implementation of the embodiment of the present disclosure, as shown in FIG. **5**, based on the embodiment shown in FIG. **4** above, the method provided in the embodiment of the present disclosure may further includes the following steps:

[0129] S**501**. The API service component receives a profile update request for requesting to update the target container security protection profile.

[0130] S**502**: The API service component updates the resource object of the first custom resource in response to the profile update request.

[0131] S**503**: The access control management component acquires an updated container security protection profile according to the definition of the updated resource object of the first custom resource.

[0132] S**504**: The access control management component updates the second custom resource according to the updated container security protection profile.

[0133] S**505**. Control the access control agent component of the node device (the at least one target node device) where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

[0134] S**506**. Control the access control agent component of the node device (the at least one target node device) where the container group of the target protection object is deployed, to feedback the loading status of the updated container security protection profile into the corresponding node device to the access control management component respectively.

[0135] S**507**: The access control management component updates the resource status of the first custom resource and the second custom resource according to the loading status of the updated container security protection profile into each target node device.

[0136] The embodiment shown in FIG. **5** above provides an implementation method for changing the container security protection profile for a workload (first workload) that has sandbox protection enabled, and there is no need to restart the first workload during the change of the first workload, which solves the limitation that the workload must be restarted when changing the container sandbox profile and improves the flexibility when using the container sandbox.

[0137] As an expansion and refinement of the above embodiment, the present disclosure provides another container operation control method. As shown in FIG. **6**, the container operation control method includes:

[0138] S**601**: The API service component of the container cluster receives a profile configuration request.

[0139] Among them, the profile configuration request includes a profile identifier of the target container security protection profile and object information of a target protection object related to the container, the profile configuration request is used to request security protection for the target protection object based on the target container security protection profile, the target protection object includes a workload that meets a preset condition.

[0140] S**602**. The API service component creates a resource object of a first custom resource corresponding to the target container security protection profile.

[0141] S**603**: The access control management component of the container cluster acquires the target container security protection profile according to the definition of the first custom resource.

[0142] S**604**: The access control management component of the container cluster creates a second custom resource including the target container security protection profile.

[0143] So far, the resources including the target container security protection profile are created.

[0144] S**605**: The access control agent component of each node device of the container cluster acquires the target container security protection profile according to the second custom resource, and loads the target container security protection profile into the kernel of the node device to which it belongs.

[0145] S**606**: The access control agent component of each node device of the container cluster feeds back the loading status of the target container security protection profile into the corresponding node device to the access control management component.

[0146] S**607**: The access control management component updates the resource status of the first custom resource and the resource status of the second custom resource according to the loading status of the target container security protection profile fed back by each node device.

[0147] S**608**. The API service component receives a second workload creation request.

[0148] The second workload creation request carries configuration information of the second workload, and is used to request creation of the second workload according to the configuration information.

[0149] S**609**: The access control management component determines whether the second workload meets the preset condition.

[0150] If the access control management component determines that the second workload does not meet the preset condition, the container group of the second workload is directly deployed on at least one node device of the container cluster according to the configuration information, just like the existing workload creation scheme, if the access control management component determines that the second workload meets the preset condition, the following steps are executed:

[0151] S**610**. The access control management component updates configuration information of the second workload according to the first custom resource.

[0152] S**611**. The API service component deploys a container group of the second workload on at least one node device according to the updated configuration information of the second workload.

[0153] The embodiment shown in FIG. **6** above provides a solution of first defining a protection strategy (target container security protection strategy), and when a workload (the second workload) that meets the condition is created, then enabling sandbox protection for the workload.

[0154] It should be noted that, based on the embodiment shown in FIG. **6**, the container operation control method provided by the present disclosure can also change the container security protection strategy for the second workload. The implementation scheme for changing the container security protection profile (target container security protection profile) for the second workload is similar to the embodiment shown in FIG. **5**, and to avoid redundancy, it will not be repeated here.

[0155] Based on the same inventive concept, as an implementation of the above method, the embodiment of the present disclosure also provides a container operation control apparatus, which corresponds to the above method embodiment, for ease of reading, this embodiment will no longer repeat the details of the above method embodiment one by one, but it should be clear that the container operation control apparatus in this embodiment can correspond to all the contents in the above method embodiment.

[0156] The embodiment of the present disclosure provides a container operation control apparatus. FIG. **7** is a schematic structural diagram of the container operation control device. As shown in FIG. **7**, the container operation control apparatus **700** includes:

[0157] an output unit **71**, configured to provide at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

[0158] a receiving unit **72**, configured to receive a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

[0159] a control unit **73**, configured to, in response to the profile configuration request, enable the target container security protection profile for the target protection object, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile.

[0160] As an optional implementation of the embodiment of the present disclosure, the container security protection strategy based on the container security baseline includes at least one of the following container security protection strategies:

[0161] It is prohibited to rewrite kernel parameters of a host.

[0162] It is prohibited to mount a process file system with read and write permissions.

[0163] It is prohibited to mount a host disk device with read and write permissions.

[0164] It is prohibited to read and write the host disk device.

[0165] It is prohibited to rewrite an agent release file of a subsystem of the host control group.

[0166] It is prohibited to mount a subsystem of the host control group;

[0167] It is prohibited to use specified privileged capabilities.

[0168] It is prohibited to use privileged capabilities in a namespace.

[0169] It is prohibited to use specified privileged capabilities in a namespace.

[0170] It is prohibited to use AF_PACKET protocol family to create sockets.

[0171] As an optional implementation of the embodiment of the present disclosure, the container security protection strategy for a specified vulnerability in a container environment includes at least one of the following container security protection strategies:

[0172] It is prohibited to read the credential for communicating with the container cluster's API service.

[0173] It is prohibited to read the path of the container in the host machine.

[0174] It is prohibited to read the disk device number of the host machine.

[0175] It is prohibited to read the network protocol IP address of the host machine.

[0176] It is prohibited to execute specified executable files.

[0177] It is prohibited to modify file permissions.

[0178] It is prohibited to rewrite the directory and configuration files of system configuration files.

[0179] It is prohibited to escalate permissions.

[0180] It is prohibited to perform local inter-process communication via UNIX sockets.

[0181] It is prohibited to access to specified files through NGINX service.

[0182] As an optional implementation of the embodiment of the present disclosure, the control unit **73** is specifically configured to enable the target container security protection profile for the container group of the target protection object or the container of the target protection object or the application of the target protection object based on the object information of the target protection object.

[0183] As an optional implementation of the embodiment of the present disclosure,

[0184] The receiving unit **71** is specifically configured to receive a profile configuration request through an API service component of the container cluster;

[0185] The control unit **73** is further configured to, before in response to the profile configuration request, enable the target container security protection profile for the target protection object, create a resource object of a first custom resource corresponding to the target container security protection profile through the API service component, acquire the target container security protection profile according to the definition of the first custom resource, and create a second custom resource including the target container security protection profile through the access control management component of the container cluster.

[0186] As an optional implementation of the embodiment of the present disclosure, the first custom resource, the second custom resource, and the target protection object are resources in the same namespace.

[0187] As an optional implementation of the embodiment of the present disclosure, the target protection object includes a first workload created in the container cluster before the profile configuration request is received;

[0188] The control unit **73** is specifically configured to control an access control agent component of a node device in the container cluster where the container group of the first workload is deployed, obtain the target container security protection profile according to the second custom resource, and load the target container security protection profile into the kernel of the node device to which it belongs; update the configuration information of the first workload according to the first custom resource through the access control management component; control the access control agent component of the node device of the container group where the first workload is deployed, and update the container group of the first workload according to the updated configuration information of the first workload.

[0189] As an optional implementation of the embodiment of the present disclosure, the target protection object includes a workload that meets a preset condition;

[0190] The receiving unit **71** is further configured to, after creating a second custom resource according to the target container security protection profile, receive a second workload creation request through the API service component, the second workload creation request carries configuration information of the second workload, and is used to request creation of the second workload according to the configuration information.

[0191] The control unit **73** is specifically configured to, if it is determined that the second workload meets the preset condition, update configuration information of the second workload according to the first custom resource through the access control management component; deploy a container group of the second workload on at least one node device according to the updated configuration information of the second workload through the API service component.

[0192] As an optional implementation of the embodiment of the present disclosure,

[0193] The receiving unit **71** is further configured to receive, through the API service component, a profile update request for requesting to update the security protection profile of the target container;

[0194] The control unit **73** is also used to update the resource object of the first custom resource in response to the profile update request; acquire the updated container security protection profile according to the definition of the updated resource object of the first custom resource through the access control management component, and update the second custom resource according to the updated container security protection profile; control the access control agent component of the node device where the container group of the target protection object is deployed, acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

[0195] The container operation control apparatus provided in this embodiment can execute the container operation control method provided in the above method embodiment, their implementation principle and technical effect are similar and will not be repeated here.

[0196] Based on the same inventive concept, an embodiment of the present disclosure also provides an electronic device. FIG. **8** is a schematic structural diagram of an electronic device provided in an embodiment of the present disclosure. As shown in FIG. **8**, the electronic device provided in this embodiment includes: a memory **801** and a processor **802**, wherein the memory **801** is used to store a computer program; and the processor **802** is used to execute the container operation control method provided in the above embodiment when executing the computer program.

[0197] Based on the same inventive concept, an embodiment of the present disclosure further provides a computer-readable storage medium, on which a computer program is stored. When the computer program is executed by a processor, the computing device implements the container operation control method provided in the above embodiments.

[0198] Based on the same inventive concept, an embodiment of the present disclosure further provides a computer program product, when the computer program product is

executed on a computer, a computing device implements the container operation control method provided in the above embodiments.

[0199] Those skilled in the art should appreciate that the embodiments of the present disclosure may be provided as methods, systems, or computer program products. Accordingly, the present disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, the present disclosure may take the form of a computer program product embodied in one or more computer usable storage mediums having computer usable program code embodied therein.

[0200] The processor can be a central processing unit (CPU), or other general-purpose processors, digital signal processors (DSP), application-specific integrated circuits (ASIC), field-programmable gate arrays (FPGA) or other programmable logic devices, discrete gate or transistor logic devices, discrete hardware components, etc. A general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like.

[0201] The memory may include non-permanent memory in a computer-readable medium, random-access memory (RAM) and/or non-volatile memory, such as, read-only memory (ROM) or flash RAM. Memory is an example of a computer-readable medium.

[0202] Computer readable media include permanent and non-permanent, removable and non-removable storage media. The storage medium can implement information storage by any method or technology, and the information can be computer-readable instructions, data structures, program modules or other data. Examples of computer storage media include, but not limited to, phase change memory (PRAM), static random access memory (SRAM), dynamic random access memory (DRAM), other types of random access memory (RAM), read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), flash memory or other memory technology, compact disk-read-only memory (CD-ROM), digital versatile disk (DVD) or other optical storage, magnetic cassettes, magnetic disk storage or other magnetic storage devices, or any other non-transmission medium that can be used to store information that can be accessed by a computing device. According to definition in this document, computer-readable media do not include temporary computer-readable media (transitory media), such as modulated data signals and carrier waves.

[0203] Finally, it should be noted that the above embodiments are only used to illustrate the technical solutions of the present disclosure, instead of limiting them. Although the present disclosure has been described in detail with reference to the aforementioned embodiments, those skilled in the art should understand that they can still modify the technical solutions described in the aforementioned embodiments, or replace some or all of the technical features therein by equivalents. However, these modifications or replacements do not cause the essence of the corresponding technical solutions to deviate from the scope of the technical solutions of the embodiments of the present disclosure.

1. A container operation control method, including:

providing at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, through an application programing interface API service component of a container cluster, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

creating a resource object of a first custom resource corresponding to the target container security protection profile through the API service component;

acquiring the target container security protection profile according to a definition of the first custom resource, and creating a second custom resource including the target container security protection profile, through an access control management component of the container cluster;

enabling the target container security protection profile for the target protection object in response to the profile configuration request, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile,

the target protection object includes a first workload created in the container cluster before the profile configuration request is received;

the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

controlling an access control agent component of a node device in the container cluster where the container group of the first workload is deployed, to acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into a kernel of the node device to which it belongs.

2. The method of claim **1**, wherein, the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

enabling the target container security protection profile for the container group of the target protection object or the container of the target protection object or the application of the target protection object, based on the object information of the target protection object.

3. (canceled)

4. The method of claim **1**, wherein, the first custom resource, the second custom resource, and the target protection object are resources in the same namespace.

5. The method of claim **1**, wherein, the method further comprises:

updating configuration information of the first workload according to the first custom resource through the access control management component;

controlling the access control agent component of the node device where the container group of the first workload is deployed, to update the container group of

the first workload according to the updated configuration information of the first workload, through the API service component.

6. The method of claim **1**, wherein, the target protection object includes a workload that meets a preset condition;

after creating the second custom resource according to the target container security protection profile, the method further comprises:

receiving a second workload creation request through the API service component, the second workload creation request carries configuration information of the second workload, and is used to request creation of the second workload according to the configuration information;

if it is determined that the second workload meets the preset condition, updating configuration information of the second workload according to the first custom resource through the access control management component;

deploying a container group of the second workload on at least one node device according to the updated configuration information of the second workload through the API service component.

7. The method of claim **5**, wherein, the method further comprises:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

8. (canceled)

9. An electronic device, comprising: a memory and a processor, wherein the memory is configured to store a computer program; and the processor is configured to execute the computer program, so as to cause the electronic device to implement:

providing at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, through an application programing interface API service component of a container cluster, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

creating a resource object of a first custom resource corresponding to the target container security protection profile through the API service component; acquiring the target container security protection profile according to a definition of the first custom resource, and creating a second custom resource including the target container security protection profile, through an access control management component of the container cluster;

enabling the target container security protection profile for the target protection object in response to the profile configuration request, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile,

the target protection object includes a first workload created in the container cluster before the profile configuration request is received;

the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

controlling an access control agent component of a node device in the container cluster where the container group of the first workload is deployed, to acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into a kernel of the node device to which it belongs.

10. A non-transitory computer-readable storage medium, storing a computer program, which when executed by a computing device, causes the computing device to implement:

providing at least one type of container security protection profile that allow users to select and configure, wherein the at least one type of container security protection profile includes: a container security protection profile based on a container security baseline and/or a container security protection profile for a specified vulnerability in a container environment;

receiving a profile configuration request initiated based on at least one container security protection profile of the at least one type of container security protection profile, through an application programing interface API service component of a container cluster, the profile configuration request including a profile identifier of a target container security protection profile and object information about a target protection object related to the container, the profile configuration request being used to request security protection for the target protection object based on the target container security protection profile;

creating a resource object of a first custom resource corresponding to the target container security protection profile through the API service component; acquiring the target container security protection profile according to a definition of the first custom resource, and creating a second custom resource including the target container security protection profile, through an access control management component of the container cluster;

enabling the target container security protection profile for the target protection object in response to the profile configuration request, to monitor access requests to the target protection object, and perform access control on the access requests based on the target container security protection profile,

the target protection object includes a first workload created in the container cluster before the profile configuration request is received;

the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

controlling an access control agent component of a node device in the container cluster where the container group of the first workload is deployed, to acquire the target container security protection profile according to the second custom resource, and load the target container security protection profile into a kernel of the node device to which it belongs.

11-12. (canceled)

13. The method of claim **6**, wherein, the method further comprises:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

14. The electronic device of claim **9**, wherein, the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

enabling the target container security protection profile for the container group of the target protection object or the container of the target protection object or the application of the target protection object, based on the object information of the target protection object.

15. The electronic device of claim **9**, wherein, the first custom resource, the second custom resource, and the target protection object are resources in the same namespace.

16. The electronic device of claim **9**, wherein, the processor is configured to execute the computer program, so as to cause the electronic device to further implement:

updating configuration information of the first workload according to the first custom resource through the access control management component;

controlling the access control agent component of the node device where the container group of the first workload is deployed, to update the container group of the first workload according to the updated configuration information of the first workload, through the API service component.

17. The electronic device of claim **9**, wherein, the target protection object includes a workload that meets a preset condition;

wherein the processor is configured to execute the computer program, so as to cause the electronic device to further implement, after creating the second custom resource according to the target container security protection profile:

receiving a second workload creation request through the API service component, the second workload creation request carries configuration information of the second workload, and is used to request creation of the second workload according to the configuration information;

if it is determined that the second workload meets the preset condition, updating configuration information of the second workload according to the first custom resource through the access control management component;

deploying a container group of the second workload on at least one node device according to the updated configuration information of the second workload through the API service component.

18. The electronic device of claim **16**, wherein, the processor is configured to execute the computer program, so as to cause the electronic device to further implement:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

19. The electronic device of claim **17**, wherein, the processor is configured to execute the computer program, so as to cause the electronic device to further implement:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

20. The non-transitory computer-readable storage medium of claim **10**, wherein, wherein, the enabling the target container security protection profile for the target protection object in response to the profile configuration request, comprises:

enabling the target container security protection profile for the container group of the target protection object or the container of the target protection object or the application of the target protection object, based on the object information of the target protection object.

21. The non-transitory computer-readable storage medium of claim **10**, wherein, the computer program, which when executed by a computing device, causes the computing device to further implement:

updating configuration information of the first workload according to the first custom resource through the access control management component;

controlling the access control agent component of the node device where the container group of the first workload is deployed, to update the container group of the first workload according to the updated configuration information of the first workload, through the API service component.

22. The non-transitory computer-readable storage medium of claim **10**, wherein, the target protection object includes a workload that meets a preset condition;

wherein the computer program, which when executed by a computing device, causes the computing device to further implement, after creating the second custom resource according to the target container security protection profile:

receiving a second workload creation request through the API service component, the second workload creation request carries configuration information of the second workload, and is used to request creation of the second workload according to the configuration information;

if it is determined that the second workload meets the preset condition, updating configuration information of the second workload according to the first custom resource through the access control management component;

deploying a container group of the second workload on at least one node device according to the updated configuration information of the second workload through the API service component.

23. The non-transitory computer-readable storage medium of claim **21**, wherein, the computer program, which when executed by a computing device, causes the computing device to further implement:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

24. The non-transitory computer-readable storage medium of claim **22**, wherein, the computer program, which when executed by a computing device, causes the computing device to further implement:

receiving a profile update request for requesting to update the security protection profile of the target container, and updating the resource object of the first custom resource in response to the profile update request, through the API service component;

acquiring the updated container security protection profile according to a definition of the updated resource object of the first custom resource, and updating the second custom resource according to the updated container security protection profile, through the access control management component;

controlling the access control agent component of the node device where the container group of the target protection object is deployed, to acquire the updated container security protection profile according to the updated second custom resource, and load the updated container security protection profile into the kernel of the node device to which it belongs.

* * * * *