(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107577538 B
(45)授权公告日 2020.03.31

(21)申请号 201710995539.9

(22)申请日 2017.10.23

(65)同一申请的已公布的文献号
申请公布号 CN 107577538 A

(43)申请公布日 2018.01.12

(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 李铭轩 魏进武 张呈宇 张基恒 博格利

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 张子青 刘芳

(51)Int.Cl.
G06F 9/50(2006.01)
G06F 21/31(2013.01)

(56)对比文件
CN 105847045 A,2016.08.10,说明书第0001-0033段.
CN 106557690 A,2017.04.05,说明书第0001-0133段.
CN 106970822 A,2017.07.21,全文.
US 2016170721 A1,2016.06.16,全文.
wade&luffy.访问Docker仓库.《https://www.cnblogs.com/wade-luffy/p/6497502.html》.2017,第1-3页.

审查员 周真

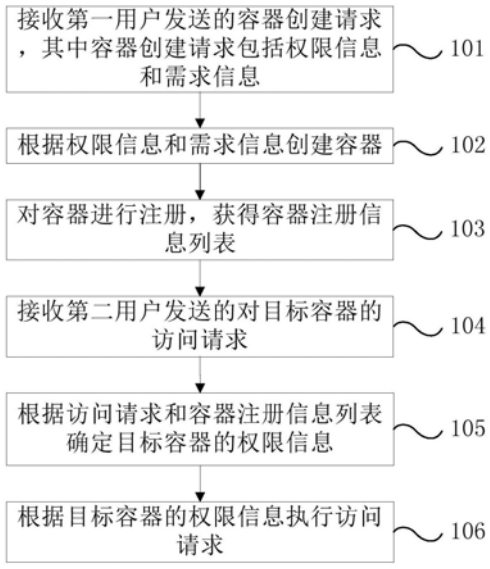
权利要求书2页 说明书9页 附图3页

(54)发明名称

容器资源管理方法及系统

(57)摘要

本发明提供的容器资源管理方法及系统,通过接收第一用户发送的容器创建请求,其中容器创建请求包括权限信息和需求信息,根据权限信息和需求信息创建容器,对容器进行注册,获得容器注册信息列表,接收第二用户发送的对目标容器的访问请求,根据访问请求和容器注册信息列表确定目标容器的权限信息,根据目标容器的权限信息执行访问请求。从而可在创建容器时,直接将容器的权限信息封装在容器中,进而可在用户访问容器时,直接根据容器中的权限信息执行访问,避免现有技术中由容器资源管理系统为用户分配容器的权限,一旦权限分配机制发生崩塌而造成的用户访问机制的紊乱的问题,保证了容器内的数据安全。



CN 107577538 B

1.一种容器资源管理方法,其特征在于,包括:

接收第一用户发送的容器创建请求,其中所述容器创建请求包括权限信息和需求信息;

根据所述权限信息和所述需求信息创建容器;

对所述容器进行注册,获得容器注册信息列表;

接收第二用户发送的对目标容器的访问请求;

根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息;

根据所述目标容器的权限信息执行所述访问请求;

所述根据所述权限信息和所述需求信息创建容器,包括:对所述权限信息进行加密,获得容器注解信息;根据所述需求信息创建容器副本,并对所述容器注解信息和所述容器副本进行封装,获得所述容器;

所述容器注册信息列表包括各容器的容器标识和对应的容器地址;所述访问请求包括目标容器标识;

相应的,所述根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息,包括:根据所述目标容器标识和所述容器注册信息列表中的各容器的容器标识确定所述目标容器的容器地址;根据所述目标容器的容器地址拉起所述目标容器并获取所述目标容器的容器注解信息;对所述目标容器的容器注解信息进行解密,获得所述目标容器的权限信息。

2.根据权利要求1所述的容器资源管理方法,其特征在于,所述接收第一用户发送的容器创建请求之前,还包括:

接收第一用户发送的身份认证请求,并对第一用户的用户身份进行安全认证;当所述第一用户的用户身份认证请求通过时,向所述第一用户发送认证通过消息,以供所述第一用户在接收到认证通过消息之后发送所述容器创建请求;

所述接收第二用户发送的访问请求之前,还包括:

接收第二用户发送的身份认证请求,并对第二用户的用户身份进行安全认证;当所述第二用户的用户身份认证请求通过时,向所述第二用户发送认证通过消息,以供所述第二用户在接收到认证通过消息之后发送所述访问请求。

3.根据权利要求1所述的容器资源管理方法,其特征在于,所述权限信息包括各用户标识和对应的操作权限;所述访问请求包括第二用户标识和访问操作;

相应的,所述根据所述目标容器的权限信息执行所述访问请求,包括:

判断所述目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识;

若是,则判断所述第二用户的访问操作是否与所述目标用户标识对应的操作权限匹配;若匹配,则执行所述访问操作。

4.根据权利要求1-3任一项所述的容器资源管理方法,其特征在于,所述需求信息包括容器副本数量和/或容器配置参数。

5.一种容器资源管理系统,其特征在于,包括:

收发单元,用于接收第一用户发送的容器创建请求,其中所述容器创建请求包括权限信息和需求信息;还用于接收第二用户发送的对目标容器的访问请求;

容器创建单元，用于根据所述权限信息和所述需求信息创建容器；对所述容器进行注册，获得容器注册信息列表；

容器访问单元，用于根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息；根据所述目标容器的权限信息执行所述访问请求；

所述容器创建单元，具体用于：

对所述权限信息进行加密，获得容器注解信息；

根据所述需求信息创建容器副本，并对所述容器注解信息和所述容器副本进行封装，获得所述容器；

所述容器注册信息列表包括各容器的容器标识和对应的容器地址；所述访问请求包括目标容器标识；

相应的，所述容器访问单元，具体用于：根据所述目标容器标识和所述容器注册信息列表中的各容器的容器标识确定所述目标容器的容器地址；根据所述目标容器的容器地址拉起所述目标容器并获取所述目标容器的容器注解信息；对所述目标容器的容器注解信息进行解密，获得所述目标容器的权限信息。

6.根据权利要求5所述的容器资源管理系统，其特征在于，还包括：身份认证单元；

所述身份认证单元用于对第一用户的用户身份进行安全认证；还用于对第二用户的用户身份进行安全认证；

相应的，所述收发单元还用于在接收第一用户发送的容器创建请求之前，接收第一用户发送的身份认证请求；当所述身份认证单元确定第一用户的用户身份认证请求通过时，所述收发单元还用于向所述第一用户发送认证通过消息，以供所述第一用户在接收到认证通过消息之后发送所述容器创建请求；

所述收发单元还用于在接收第二用户发送的访问请求之前，接收第二用户发送的身份认证请求；当所述身份认证单元确定所述第二用户的用户身份认证请求通过时，所述收发单元还用于向所述第二用户发送认证通过消息，以供所述第二用户在接收到认证通过消息之后发送所述访问请求。

7.根据权利要求5所述的容器资源管理系统，其特征在于，所述权限信息包括各用户标识和对应的操作权限；所述访问请求包括第二用户标识和访问操作；

相应的，所述容器访问单元，具体用于：判断所述目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识；若是，则判断所述第二用户的访问操作是否与所述目标用户标识对应的操作权限匹配；若匹配，则执行所述访问操作。

8.根据权利要求5-7任一项所述的容器资源管理系统，其特征在于，所述需求信息包括容器副本数量和/或容器配置参数。

容器资源管理方法及系统

技术领域

[0001] 本发明涉及数据安全领域，尤其涉及一种容器管理方法及系统。

背景技术

[0002] 随着数字化信息时代的到来，利用容器技术完成云存储成为热点。如何对基于多租户的容器资源进行管理成为研究重点。

[0003] 一般来说，多个容器将共享宿主机上的计算、存储、网络等资源。用户在访问容器之前，需要由系统层的容器资源管理系统为用户分配权限，然后由应用层面的操作系统对用户是否访问相应容器的权限进行判定。因此，在现有的容器资源管理方法中，用户对容器的访问权限是由容器资源管理系统分配的，而一旦权限分配机制发生崩塌，势必造成租户访问机制的紊乱，进而严重影响容器内的数据安全。

发明内容

[0004] 针对现有的容器管理系统的访问权限分配机制容易发生崩塌，严重影响容器内的数据安全的问题，本发明提供了一种容器管理方法及系统。

[0005] 一方面，本发明提供了一种容器管理方法，包括：

[0006] 接收第一用户发送的容器创建请求，其中所述容器创建请求包括权限信息和需求信息；

[0007] 根据所述权限信息和所述需求信息创建容器；

[0008] 对所述容器进行注册，获得容器注册信息列表；

[0009] 接收第二用户发送的对目标容器的访问请求；

[0010] 根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息；

[0011] 根据所述目标容器的权限信息执行所述访问请求。

[0012] 进一步地，所述根据所述权限信息和所述需求信息创建容器，包括：

[0013] 对所述权限信息进行加密，获得容器注解信息；

[0014] 根据所述需求信息创建容器副本，并对所述容器注解信息和所述容器副本进行封装，获得所述容器。

[0015] 进一步地，所述容器注册信息列表包括各容器的容器标识和对应的容器地址；所述访问请求包括目标容器标识；

[0016] 相应的，所述根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息，包括：

[0017] 根据所述目标容器标识和所述容器注册信息列表中的各容器的容器标识确定所述目标容器的容器地址；

[0018] 根据所述目标容器的容器地址拉起所述目标容器并获取所述目标容器的容器注解信息；

[0019] 对所述目标容器的容器注解信息进行解密，获得所述目标容器的权限信息。

[0020] 进一步地，所述接收第一用户发送的容器创建请求之前，还包括：

[0021] 接收第一用户发送的身份认证请求，并对第一用户的用户身份进行安全认证；当所述第一用户的用户身份认证请求通过时，向所述第一用户发送认证通过消息，以供所述第一用户在接收到认证通过消息之后发送所述容器创建请求；

[0022] 所述接收第二用户发送的访问请求之前，还包括：

[0023] 接收第二用户发送的身份认证请求，并对第二用户的用户身份进行安全认证；当所述第二用户的用户身份认证请求通过时，向所述第二用户发送认证通过消息，以供所述第二用户在接收到认证通过消息之后发送所述访问请求。

[0024] 进一步地，所述权限信息包括各用户标识和对应的操作权限；所述访问请求包括第二用户标识和访问操作；

[0025] 相应的，所述根据所述目标容器的权限信息执行所述访问请求，包括：

[0026] 判断所述目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识；

[0027] 若是，则判断所述第二用户的访问操作是否与所述目标用户标识对应的操作权限匹配；若匹配，则执行所述访问操作。

[0028] 进一步地，所述需求信息包括容器副本数量和/或容器配置参数。

[0029] 本发明还提供了一种容器资源管理系统，包括：

[0030] 收发单元，用于接收第一用户发送的容器创建请求，其中所述容器创建请求包括权限信息和需求信息；还用于接收第二用户发送的对目标容器的访问请求；

[0031] 容器创建单元，用于根据所述权限信息和所述需求信息创建容器；对所述容器进行注册，获得容器注册信息列表；

[0032] 容器访问单元，用于根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息；根据所述目标容器的权限信息执行所述访问请求。

[0033] 进一步地，所述容器创建单元，具体用于：

[0034] 对所述权限信息进行加密，获得容器注解信息；

[0035] 根据所述需求信息创建容器副本，并对所述容器注解信息和所述容器副本进行封装，获得所述容器。

[0036] 进一步地，所述容器注册信息列表包括各容器的容器标识和对应的容器地址；所述访问请求包括目标容器标识；

[0037] 相应的，所述容器访问单元，具体用于：根据所述目标容器标识和所述容器注册信息列表中的各容器的容器标识确定所述目标容器的容器地址；根据所述目标容器的容器地址拉起所述目标容器并获取所述目标容器的容器注解信息；对所述目标容器的容器注解信息进行解密，获得所述目标容器的权限信息。

[0038] 进一步地，所述容器资源管理系统还包括：身份认证单元；

[0039] 所述身份认证单元用于对第一用户的用户身份进行安全认证；还用于对第二用户的用户身份进行安全认证；

[0040] 相应的，所述收发单元还用于在接收第一用户发送的容器创建请求之前，接收第一用户发送的身份认证请求；当所述身份认证单元确定第一用户的用户身份认证请求通过时，所述收发单元还用于向所述第一用户发送认证通过消息，以供所述第一用户在接收到

认证通过消息之后发送所述容器创建请求；

[0041] 所述收发单元还用于在接收第二用户发送的访问请求之前，接收第二用户发送的身份认证请求；当所述身份认证单元确定所述第二用户的用户身份认证请求通过时，所述收发单元还用于向所述第二用户发送认证通过消息，以供所述第二用户在接收到认证通过消息之后发送所述访问请求。

[0042] 进一步地，所述权限信息包括各用户标识和对应的操作权限；所述访问请求包括第二用户标识和访问操作；

[0043] 相应的，所述容器访问单元，具体用于：判断所述目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识；若是，则判断所述第二用户的访问操作是否与所述目标用户标识对应的操作权限匹配；若匹配，则执行所述访问操作。

[0044] 进一步地，所述需求信息包括容器副本数量和/或容器配置参数。

[0045] 本发明提供的容器资源管理方法及系统，通过接收第一用户发送的容器创建请求，其中所述容器创建请求包括权限信息和需求信息，根据所述权限信息和所述需求信息创建容器，对所述容器进行注册，获得容器注册信息列表，接收第二用户发送的对目标容器的访问请求，根据所述访问请求和所述容器注册信息列表确定所述目标容器的权限信息，根据所述目标容器的权限信息执行所述访问请求。从而可在创建容器时，直接将容器的权限信息封装在容器中，进而可在用户访问容器时，直接根据容器中的权限信息执行访问，避免现有技术中由容器资源管理系统为用户分配容器的权限，一旦权限分配机制发生崩塌而造成的用户访问机制的紊乱的问题，从而保证了容器内的数据安全。

附图说明

[0046] 图1为本发明实施例一提供的一种容器资源管理方法的流程示意图；

[0047] 图2为本发明实施例二提供的一种容器资源管理方法的流程示意图；

[0048] 图3为本发明实施例三提供的一种容器资源管理系统的结构示意图。

具体实施方式

[0049] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。

[0050] 图1为本发明实施例一提供的一种容器资源管理方法的流程示意图，如图1所示，本发明实施例一提供的容器资源管理方法包括如下步骤：

[0051] 步骤101、接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息。

[0052] 需要说明的是，本发明的执行主体具体可为容器管理系统，其物理形态可为由处理器、存储器、逻辑电路、电子芯片等硬件组成的终端设备。

[0053] 具体来说，该容器管理系统可接收由第一用户发送的容器创建请求，该容器创建请求中包括有待创建容器的权限信息，以及待创建容器的需求信息。其中，权限信息具体可为用于表示与容器访问权限、容器修改权限等与容器管理权限相关的信息或标识，而需求信息则具体可为例如容器副本数量，和/ 或容器配置参数等在内的容器固有属性。

[0054] 此外，接收第一用户发送的容器创建请求的接收方式可采用接收指令输入的方式

实现，例如向第一用户提供一可视互动界面，以供第一用户在可视互动界面的指定位置输入相关信息；还可例如直接接收由第一用户输入的指令代码；本领域技术人员还可采用其他方式实现该接收第一用户发送的容器创建请求，本发明对此不进行限制。

[0055] 步骤102、根据权限信息和需求信息创建容器。

[0056] 步骤103、对容器进行注册，获得容器注册信息列表。

[0057] 具体来说，可根据第一用户输入的权限信息确定创建的容器的权限，并根据需求信息创建与需求信息匹配的容器。随后，对创建完成的容器进行注册，并获得容器注册信息列表。其中，该容器注册信息列表不仅包括有第一用户创建的容器的信息，还可包括有其他用户创建的容器的信息。

[0058] 步骤104、接收第二用户发送的对目标容器的访问请求。

[0059] 具体来说，该容器管理系统可接收由第二用户发送的对目标容器的访问请求。其中，该访问请求具体可为用于对目标容器进行数据存储、数据读取、容器状态查看、容器配置修改、删除容器等操作的请求。此外，第二用户可与第一用户为同一用户，也可与第一用户为不同用户，本发明对此不进行限制。

[0060] 此外，接收第二用户发送的访问请求的接收方式可采用接收指令输入的方式实现，例如向第二用户提供一可视互动界面，以供第二用户在可视互动界面的指定位置输入相关访问请求；还可例如直接接收由第二用户输入的指令代码；本领域技术人员还可采用其他方式实现该接收第二用户发送的容器创建请求，本发明对此不进行限制。

[0061] 步骤105、根据访问请求和容器注册信息列表确定目标容器的权限信息。

[0062] 步骤106、根据目标容器的权限信息执行访问请求。

[0063] 具体来说，可根据接收的第二用户的对目标容器的访问请求，在容器注册信息列表中查询并找到相应的目标容器的信息，然后根据目标容器的信息获取该目标容器的权限信息。随后，可根据该目标容器的权限信息判断该第二用户是否有对该目标容器进行访问的权限，若有，则可执行该访问请求，若没有，则可向第二用户返回拒绝访问的消息。

[0064] 也就是说，在本发明实施例一提供的容器资源管理方法中，在接收到第二用户对目标容器的访问请求之后，可直接获取预存在目标容器中的权限信息，并根据该权限信息对是否执行第二用户的访问请求进行判定，避免现有技术中存在的在接收到第二用户对目标容器的访问请求之后，还需要在系统层为第二用户分配容器权限，以供应用层对第二用户是否拥有访问容器的权限进行判定而造成的数据安全隐患。

[0065] 优选地，为了进一步保证数据安全，在步骤101的接收第一用户发送的容器创建请求之前，还可对第一用户的身份进行安全认证。具体来说，包括：接收第一用户发送的身份认证请求，并对第一用户的用户身份进行安全认证；当第一用户的用户身份认证请求通过时，向第一用户发送认证通过消息，以供第一用户在接收到认证通过消息之后发送容器创建请求。

[0066] 进一步来说，认证方式具体可采用证书认证或密钥认证，举例来说，可由容器资源管理系统向用户发送用户证书或用户密钥，以供用户利用该用户证书或该用户密钥完成身份认证，也可由第三方认证系统向用户发送用户证书或用户密钥，向容器资源管理系统发送与该用户证书匹配的系统证书或系统密钥，以供容器资源管理系统完成对用户的身份的认证。此外，当对第一用户通过认证时，可向第一用户发送认证通过消息，以供第一用户在

接收到认证通过消息之后发送容器创建请求；当对第一用户没有通过认证时，可向第一用户发送认证失败消息，第一用户可根据该认证失败消息重新发起身份认证请求。

[0067] 优选地，为了进一步保证数据安全，在步骤104的接收第二用户发送的访问请求之前，还可包括：接收第二用户发送的身份认证请求，并对第二用户的用户身份进行安全认证；当第二用户的用户身份认证请求通过时，向第二用户发送认证通过消息，以供第二用户在接收到认证通过消息之后发送访问请求。

[0068] 与上述类似的，认证方式具体可采用证书认证或密钥认证，举例来说，可由容器资源管理系统向用户发送用户证书或用户密钥，以供用户利用该用户证书或该用户密钥完成身份认证，也可由第三方认证系统向用户发送用户证书或用户密钥，向容器资源管理系统发送与该用户证书匹配的系统证书或系统密钥，以供容器资源管理系统完成对用户的身份的认证。此外，当对第二用户通过认证时，可向第二用户发送认证通过消息，以供第二 用户在接收到认证通过消息之后发送访问请求；当对第二用户没有通过认证时，可向第二用户发送认证失败消息，第二用户可根据该认证失败消息重新发起身份认证请求。

[0069] 本发明实施例一提供的容器资源管理方法，通过接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息，根据权限信息和需求信息创建容器，对容器进行注册，获得容器注册信息列表，接收第二用户发送的对目标容器的访问请求，根据访问请求和容器注册信息列表确定目标容器的权限信息，根据目标容器的权限信息执行访问请求。从而可在创建容器时，直接将容器的权限信息封装在容器中，进而可在用户访问容器时，直接根据容器中的权限信息执行访问，避免现有技术中由容器资源管理系统为用户分配容器的权限，一旦权限分配机制发生崩塌而造成的用户访问机制的紊乱的问题，从而保证了容器内的数据安全。

[0070] 在实施例一的基础上，为了进一步阐述本发明提供的容器资源管理方法，图2为本发明实施例二提供的一种容器资源管理方法的流程示意图。

[0071] 如图2所示，该容器资源管理方法包括：

[0072] 步骤201、接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息。

[0073] 与实施例一类似的是，该容器管理系统可接收由第一用户发送的容器创建请求，该容器创建请求中包括有待创建容器的权限信息，以及待创建容器的需求信息。其中，权限信息具体可为用于表示与容器访问权限、容器修改权限等与容器管理权限相关的信息或标识，而需求信息则具体可为例如容器副本数量，和/或容器配置参数等在内的容器固有属性。

[0074] 此外，接收第一用户发送的容器创建请求的接收方式可采用接收指令输入的方式实现，例如向第一用户提供一可视互动界面，以供第一用户在可视互动界面的指定位置输入相关信息；还可例如直接接收由第一用户输入的指令代码；本领域技术人员还可采用其他方式实现该接收第一用户发送的容器创建请求，本发明对此不进行限制。

[0075] 步骤202、对权限信息进行加密，获得容器注解信息。

[0076] 步骤203、根据需求信息创建容器副本，并对容器注解信息和容器副本进行封装，获得容器。

[0077] 具体来说，可采用加密技术对权限信息进行加密，生成容器注解信息，例如可采用

对称密钥加密，还可采用非对称密钥加密等加密技术，本发明对此不进行限制。

[0078] 此外，根据需求信息创建容器副本创建容器副本，并对容器注解信息和容器副本进行封装，获得容器。

[0079] 举例来说，当需求信息包括容器副本数量时，可创建与该容器副本数量相同数量的容器副本，并将容器注解信息和每个容器副本进行封装，获得容器；当需求信息包括容器配置参数时，可按照该容器配置参数创建容器副本，其中的容器配置参数具体可为容器存储容量、容器线程数等，将容器注解信息和每个容器副本进行封装，获得容器。

[0080] 步骤204、对容器进行注册，获得容器注册信息列表，其中，该容器注册信息列表包括各容器的容器标识和对应的容器地址。

[0081] 具体来说，对创建完成的容器进行注册，并获得容器注册信息列表。该容器注册信息列表不仅包括有第一用户创建的容器的信息，还可包括有其他用户创建的容器的信息，其中容器的信息包括容器标识和容器地址，此外，还可包括有对容器注解信息进行关键词提取所获得的信息等。

[0082] 步骤205、接收第二用户发送的对目标容器的访问请求，其中，该访问请求包括目标容器标识。

[0083] 具体来说，该容器管理系统可接收由第二用户发送的对目标容器的访问请求。其中，该访问请求中包括有目标容器标识。此外，该访问请求为用于对目标容器进行数据存储、数据读取、容器状态查看、容器配置修改、删除容器等操作的请求。此外，第二用户可与第一用户为同一用户，也可与第一用户为不同用户，本发明对此不进行限制。

[0084] 此外，接收第二用户发送的访问请求的接收方式可采用接收指令输入的方式实现，例如向第二用户提供一可视互动界面，以供第二用户在可视互动界面的指定位置输入相关访问请求；还可例如直接接收由第二用户输入的指令代码；本领域技术人员还可采用其他方式实现该接收第二用户发送的容器创建请求，本发明对此不进行限制。

[0085] 步骤206、根据目标容器标识和容器注册信息列表中的各容器的容器标识确定目标容器的容器地址。

[0086] 步骤207、根据目标容器的容器地址拉起目标容器并获取目标容器的容器注解信息。

[0087] 步骤208、对目标容器的容器注解信息进行解密，获得目标容器的权限信息。

[0088] 具体来说，在步骤206至步骤208中，容器资源管理系统在接收到第二用户发送的对目标容器的访问请求之后，将用该访问请求中的目标容器标识与容器注册信息列表中的各容器的容器标识一一进行比对，并在容器注册信息列表中确定该目标容器标识匹配的容器标识所对应的容器地址该容器地址则为目标容器的容器地址。根据获取到的目标容器的容器地址，可将目标容器从容器资源池中拉起，并读取封装在目标容器中的容器注解信息。采用与步骤202中的加密技术匹配的解密技术对容器注解信息进行解密，并获得目标容器的权限信息。

[0089] 步骤209、根据目标容器的权限信息执行访问请求。

[0090] 具体来说，根据该目标容器的权限信息判断该第二用户是否有对该目标容器进行访问的权限，若有，则可执行该访问请求，若没有，则可向第二用户返回拒绝访问的消息。

[0091] 进一步来说，权限信息中具体可包括有各用户标识和对应的操作权限，例如，第一

用户标识和对应的对容器进行修改、删除以及对容器中的数据进行存储和读取的权限等，还包括有第三用户标识和对应的对容器中的数据进行读取的权限等，此外，用户标识可采用单独用户标识的方式，即一个用户一个标识，也可采用群组标识的方式，即多个用户共享一个群组标识，本发明对此不进行限制。而相应的，访问请求还包括第二用户标识和访问操作，其中的访问操作具体则可为存储数据、读取数据、删除容器、修改容器等操作。步骤209可具体可为判断目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识。若目标容器的权限信息中存在有与第二用户标识匹配的目标用户标识，则获取与该目标用户标识对应的操作权限，并判断第二用户的访问操作是否与目标用户标识对应的操作权限匹配；若匹配，则执行访问操作。

[0092] 优选地，为了便于对各容器进行管理，本发明还接收由容器定其发送的容器运行状态信息，以供容器资源管理系统对容器的运行状态进行统计并汇总给用户，便于用户对容器进行管理。

[0093] 优选地，为了进一步保证数据安全，在步骤201的接收第一用户发送的容器创建请求之前，还可包括：接收第一用户发送的身份认证请求，并对第一用户的用户身份进行安全认证；当第一用户的用户身份认证请求通过时，向第一用户发送认证通过消息，以供第一用户在接收到认证通过消息之后发送容器创建请求。

[0094] 进一步来说，认证方式具体可采用证书认证或密钥认证，举例来说，可由容器资源管理系统向用户发送用户证书或用户密钥，以供用户利用该用户证书或该用户密钥完成身份认证，也可由第三方认证系统向用户发送用户证书或用户密钥，向容器资源管理系统发送与该用户证书匹配的系统证书或系统密钥，以供容器资源管理系统完成对用户的身份的认证。此外，当对第一用户通过认证时，可向第一用户发送认证通过消息，以供第一用户在接收到认证通过消息之后发送容器创建请求；当对第一用户没有通过认证时，可向第一用户发送认证失败消息，第一用户可根据该认证失败消息重新发起身份认证请求。

[0095] 优选地，为了进一步保证数据安全，在步骤205的接收第二用户发送的访问请求之前，还可包括：接收第二用户发送的身份认证请求，并对第二用户的用户身份进行安全认证；当第二用户的用户身份认证请求通过时，向第二用户发送认证通过消息，以供第二用户在接收到认证通过消息之后发送访问请求。

[0096] 与上述类似的，认证方式具体可采用证书认证或密钥认证，举例来说，可由容器资源管理系统向用户发送用户证书或用户密钥，以供用户利用该用户证书或该用户密钥完成身份认证，也可由第三方认证系统向用户发送用户证书或用户密钥，向容器资源管理系统发送与该用户证书匹配的系统证书或系统密钥，以供容器资源管理系统完成对用户的身份的认证。此外，当对第二用户通过认证时，可向第二用户发送认证通过消息，以供第二 用户在接收到认证通过消息之后发送访问请求；当对第二用户没有通过认证时，可向第二用户发送认证失败消息，第二用户可根据该认证失败消息重新发起身份认证请求。

[0097] 本发明实施例二提供的容器资源管理方法通过接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息，根据权限信息和需求信息创建容器，对容器进行注册，获得容器注册信息列表，接收第二用户发送的对目标容器的访问请求，根据访问请求和容器注册信息列表确定目标容器的权限信息，根据目标容器的权限信息执行访问请求。从而可在创建容器时，直接将容器的权限信息封装在容器中，进而可在用户访问容器

时，直接根据容器中的权限信息执行访问，避免现有技术中由容器资源管理系统为用户分配容器的权限，一旦权限分配机制发生崩塌而造成的用户访问机制的紊乱的问题，从而保证了容器内的数据安全。

[0098] 针对现有技术存在的访问权限分配机制容易发生崩塌，严重影响容器内的数据安全的问题，图3为本发明实施例三提供的一种容器管理系统的结构示意图。

[0099] 如图3所示，该容器管理系统包括：

[0100] 收发单元10用于接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息；还用于接收第二用户发送的对目标容器的访问请求。

[0101] 容器创建单元20用于根据权限信息和需求信息创建容器；对容器进行注册，获得容器注册信息列表。

[0102] 容器访问单元30用于根据访问请求和容器注册信息列表确定目标容器的权限信息；根据目标容器的权限信息执行访问请求。

[0103] 优选地，容器创建单元20，具体用于：对权限信息进行加密，获得容器注解信息；根据需求信息创建容器副本，并对容器注解信息和容器副本进行封装，获得容器。

[0104] 优选地，容器注册信息列表包括各容器的容器标识和对应的容器地址；访问请求包括目标容器标识；容器访问单元30，具体用于根据目标容器标识和容器注册信息列表中的各容器的容器标识确定目标容器的容器地址；根据目标容器的容器地址拉起目标容器并获取目标容器的容器注解信息；对目标容器的容器注解信息进行解密，获得目标容器的权限信息。

[0105] 优选地，权限信息包括各用户标识和对应的操作权限；访问请求包括第二用户标识和访问操作；容器访问单元30，具体用于判断目标容器的权限信息的各用户标识中是否有与第二用户标识匹配的目标用户标识；若是，则判断第二用户的访问操作是否与目标用户标识对应的操作权限匹配；若匹配，则执行访问操作。

[0106] 优选地，需求信息包括容器副本数量和/或容器配置参数。

[0107] 进一步地，为了进一步保证数据安全，本发明提供的容器资源管理系统还包括身份认证单元；

[0108] 身份认证单元用于对第一用户的用户身份进行安全认证；还用于对第二用户的用户身份进行安全认证；

[0109] 相应的，收发单元10还用于在接收第一用户发送的容器创建请求之前，接收第一用户发送的身份认证请求；当身份认证单元确定第一用户的用户身份认证请求通过时，收发单元10还用于向第一用户发送认证通过消息，以供第一用户在接收到认证通过消息之后发送容器创建请求；

[0110] 收发单元10还用于在接收第二用户发送的访问请求之前，接收第二用户发送的身份认证请求；当身份认证单元确定第二用户的用户身份认证请求通过时，收发单元10还用于向第二用户发送认证通过消息，以供第二用户在接收到认证通过消息之后发送访问请求。

[0111] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统的具体工作过程以及相应的有益效果，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0112] 本发明提供的容器资源管理方法及系统，通过接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息，根据权限信息和需求信息创建容器，对容器进行注册，获得容器注册信息列表，接收第二用户发送的对目标容器的访问请求，根据访问请求和容器注册信息列表确定目标容器的权限信息，根据目标容器的权限信息执行访问请求。从而可在创建容器时，直接将容器的权限信息封装在容器中，进而可在用户访问容器时，直接根据容器中的权限信息执行访问，避免现有技术中由容器资源管理系统为用户分配容器的权限，一旦权限分配机制发生崩塌而造成的用户访问机制的紊乱的问题，从而保证了容器内的数据安全。

[0113] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0114] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

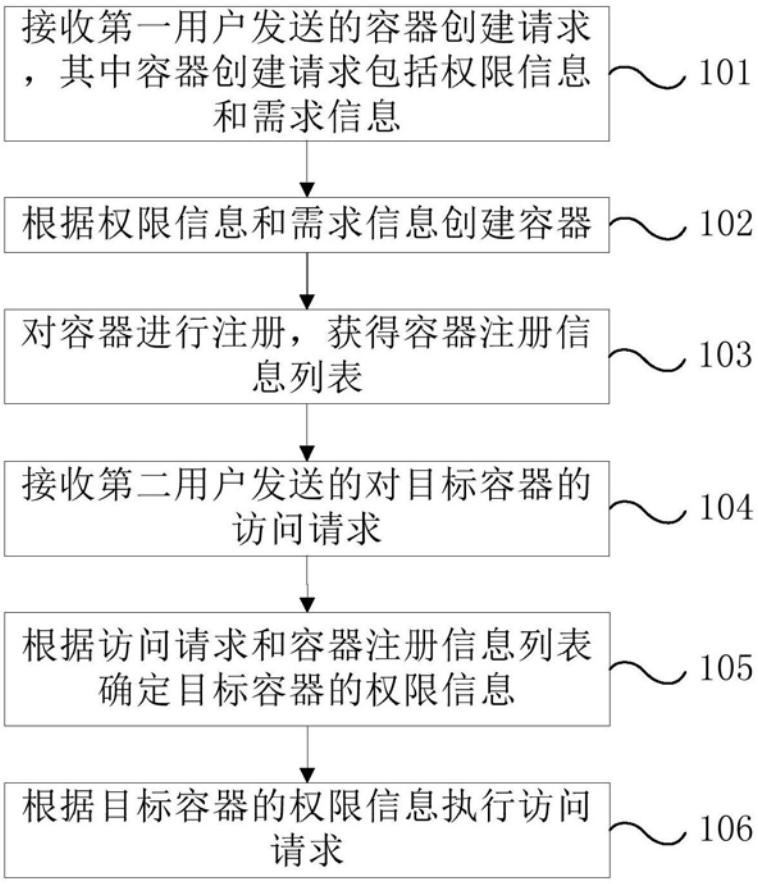

接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息
101
根据权限信息和需求信息创建容器
102
对容器进行注册，获得容器注册信息列表
103
接收第二用户发送的对目标容器的访问请求
104
根据访问请求和容器注册信息列表确定目标容器的权限信息
105
根据目标容器的权限信息执行访问请求
106

图1

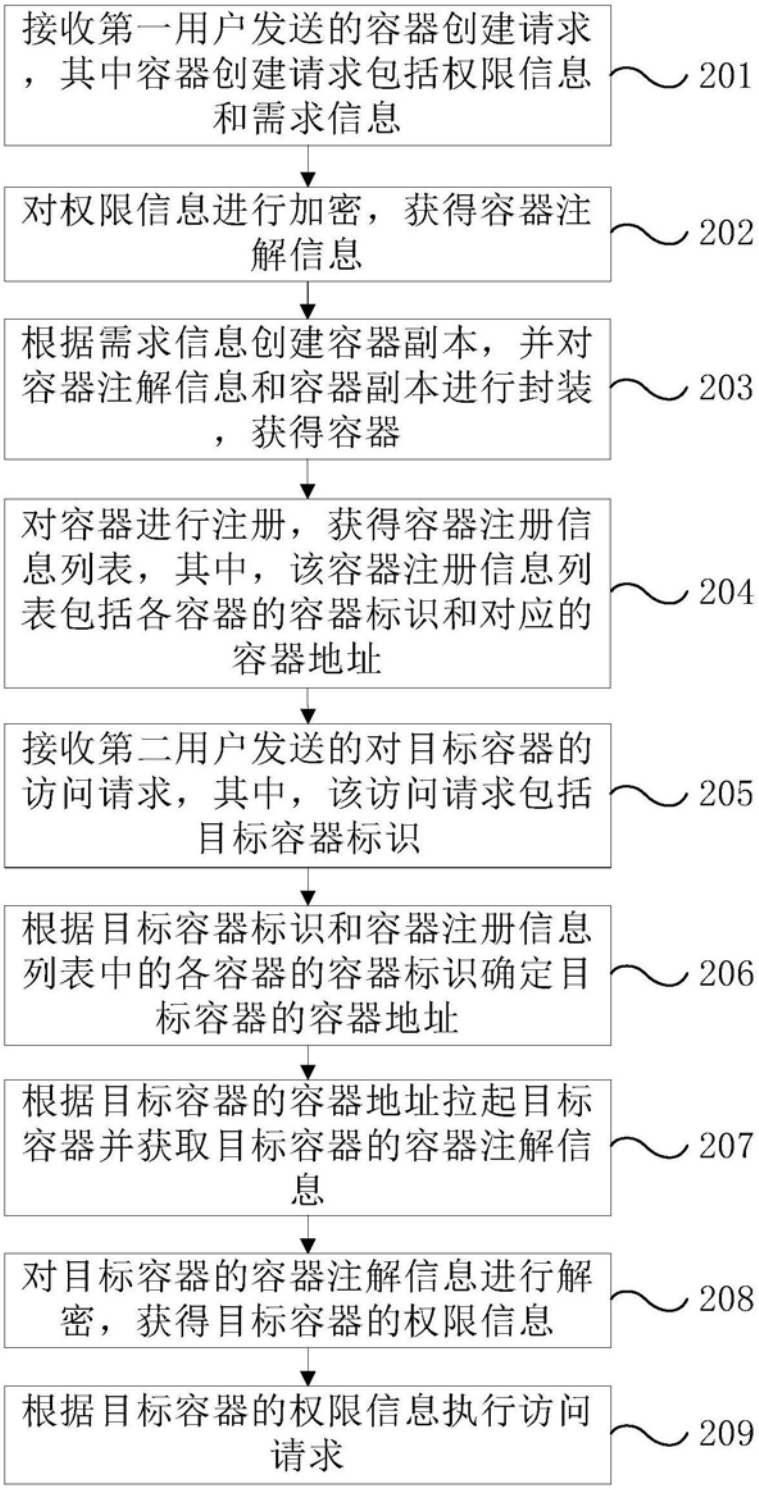

接收第一用户发送的容器创建请求，其中容器创建请求包括权限信息和需求信息
201
对权限信息进行加密，获得容器注解信息
202
根据需求信息创建容器副本，并对容器注解信息和容器副本进行封装，获得容器
203
对容器进行注册，获得容器注册信息列表，其中，该容器注册信息列表包括各容器的容器标识和对应的容器地址
204
接收第二用户发送的对目标容器的访问请求，其中，该访问请求包括目标容器标识
205
根据目标容器标识和容器注册信息列表中的各容器的容器标识确定目标容器的容器地址
206
根据目标容器的容器地址拉起目标容器并获取目标容器的容器注解信息
207
对目标容器的容器注解信息进行解密，获得目标容器的权限信息
208
根据目标容器的权限信息执行访问请求
209

图2

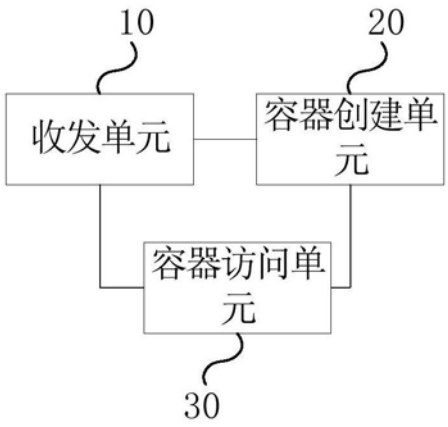


图3