(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116194917 A
(43)申请公布日 2023.05.30

(21)申请号 202180038982.1
(22)申请日 2021.10.20
(30)优先权数据
63/106,150 2020.10.27 US
17/497,386 2021.10.08 US
(85)PCT国际申请进入国家阶段日
2022.11.29
(86)PCT国际申请的申请数据
PCT/US2021/055746 2021.10.20
(87)PCT国际申请的公布数据
WO2022/093585 EN 2022.05.05
(71)申请人 谷歌有限责任公司
地址 美国加利福尼亚州
(72)发明人 阿图尔·古尔 迪甘塔·帕拉迪 马诺伊·夏尔马 毛利奥·科梅托
(74)专利代理机构 上海华诚知识产权代理有限公司 31300
专利代理师 肖华
(51)Int.Cl.
G06F 21/55(2006.01)

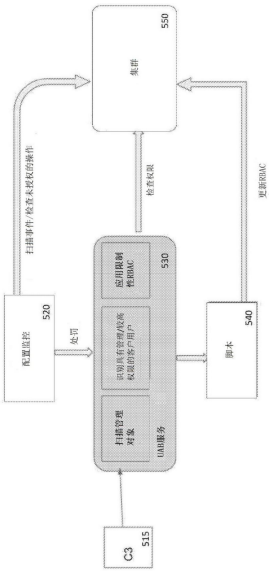
权利要求书2页 说明书8页 附图6页

(54)发明名称

第三方即服务解决方案中安全地支持客户安全策略的系统和方法

(57)摘要

本公开描述了未授权阻塞角色(UAB)的体系结构和设计。UAB是防止云托管软件的较高权限用户对例如管理对象的受保护对象执行未授权活动的机制。UAB通过定期监控客户用户在管理软件中的对象层级中的关键管理对象上的权限来工作。如果检测到客户用户具有的权限高于用户应该在那些对象上具有的权限，则UAB在用户上应用限制性的基于角色的访问控制(RBAC)。类似地，UAB还监控受保护的主体和受保护的角色，以确保其权限不被客户用户修改。



CN 116194917 A

1.一种在分布式计算系统中防止未授权活动的方法,其特征在于,包括:

利用一个或多个处理器周期性地扫描云计算系统的管理软件中的对象;

利用所述一个或多个处理器基于所述扫描来识别具有管理权限的客户用户;以及

利用所述一个或多个处理器为所识别的所述客户用户应用基于角色的访问控制(RBAC)。

2.如权利要求1所述的方法,其特征在于,所述周期性地扫描在未授权活动的事件之前执行,使得所述应用RBAC作为预防性措施执行。

3.如权利要求1所述的方法,其特征在于,所述应用RBAC在检测到未授权的事件之后作为处罚措施来执行。

4.如权利要求1所述的方法,其特征在于,应用所述RBAC包括:

遍历云计算平台对象层级;

对于所述层级中的每个对象,将所识别的所述用户的许可分类至一个或多个桶;

对于每个对象,评估所述桶中的所述许可;

确定未授权的活动阻止器(UAB)部署;以及

应用UAB更新。

5.如权利要求4所述的方法,其特征在于,所述一个或多个桶包括UAB许可桶,直接用户级许可桶,继承用户级许可桶,直接组级许可桶,或继承组级许可桶中的至少一个。

6.如权利要求4所述的方法,其特征在于,评估许可包括生成所述对象的有效用户许可映射。

7.如权利要求4所述的方法,其特征在于,评估许可包括在所述一个或多个桶中比较所识别的所述用户的条目。

8.如权利要求4所述的方法,其特征在于,确定所述UAB部署包括基于对所述许可的所述评估来确定是否应新应用,保留或修改UAB许可。

9.如权利要求4所述的方法,其特征在于,应用UAB更新包括调用管理应用编程接口。

10.如权利要求1所述的方法,其特征在于,识别具有管理权限的客户用户包括检测客户的权限的升级。

11.如权利要求1所述的方法,其特征在于,识别具有管理权限的客户用户包括检测由另一客户用户创建所述具有管理权限的客户用户。

12.一种在云计算系统中防止未授权活动的系统,其特征在于,包括:

一个或多个处理器,被配置为:

周期性地扫描所述云计算系统的管理软件中的对象;

基于所述扫描来识别具有管理权限的客户用户;以及

为所识别的所述客户用户应用基于角色的访问控制(RBAC)。

13.如权利要求12所述的系统,其特征在于,所述周期性地扫描在未授权活动的事件之前执行,使得所述应用RBAC作为预防性措施执行。

14.如权利要求12所述的系统,其特征在于,所述应用RBAC在检测到未授权的事件之后作为处罚措施来执行。

15.如权利要求12所述的系统,其特征在于,在应用所述RBAC时,所述一个或多个处理器还被配置为:

遍历云计算平台对象层级；

对于所述层级中的每个对象，将所识别的所述用户的许可分类至一个或多个桶；

对于每个对象，评估所述桶中的所述许可；

确定未授权的活动阻止器(UAB)部署；以及

应用UAB更新。

16.如权利要求15所述的系统，其特征在于，所述一个或多个桶包括UAB许可桶，直接用户级许可桶，继承用户级许可桶，直接组级许可桶，或继承组级许可桶中的至少一个。

17.如权利要求15所述的系统，其特征在于，为了评估许可，所述一个或多个处理器还被配置为生成所述对象的有效用户许可映射。

18.如权利要求15所述的系统，其特征在于，为了评估许可，所述一个或多个处理器还被配置为在所述一个或多个桶中比较所识别的所述用户的条目。

19.如权利要求15所述的系统，其特征在于，为了确定所述UAB部署，所述一个或多个处理器还被配置为基于对所述许可的所述评估来确定是否应新应用，保留或修改UAB许可。

20.如权利要求15所述的系统，其特征在于，为了应用UAB更新，所述一个或多个处理器还被配置为调用管理应用编程接口。

21.如权利要求12所述的系统，其特征在于，为了识别具有管理权限的客户用户，所述一个或多个处理器还被配置为检测客户的权限的升级。

22.如权利要求12所述的系统，其特征在于，为了识别具有管理权限的客户用户，所述一个或多个处理器还被配置为检测由另一客户用户创建所述具有管理权限的客户用户。

23.一种存储可由一个或多个处理器执行的指令的非暂态计算机可读介质，所述指令用于执行在云计算系统中防止未授权活动的方法，其特征在于，所述指令包括：

周期性地扫描所述云计算系统的管理软件中的对象；

基于所述扫描来识别具有管理权限的客户用户；以及

为所识别的所述客户用户应用基于角色的访问控制(RBAC)。

第三方即服务解决方案中安全地支持客户安全策略的系统和方法

相关申请的交叉引用

[0001] 本申请是2021年10月8日提交的美国专利申请No.17/497,386的接续申请,其要求申请日为2020年10月27日提交的美国临时专利申请No.63/106,150的优先权,其公开内容通过引用并入本文。

背景技术

[0002] 企业客户可以使用升降(lift-and-shift)用例移动到云,其中客户可以将可执行程序从企业内部(on-premises)机器提升到云,而对部署在他们自己数据中心的应用和基础设施生态系统进行最小修改或不进行修改。对于这些用例,企业内部客户通常希望保留他们现有的工作流,安全策略和管理模型。由于客户具有在企业内部部署解决方案的管理权限,因此在使用云供应商以“即服务(as-as-a-service)”消费模型提供的相同企业软件或解决方案时,他们往往希望拥有相同的权限。对于在裸机(bare-metal)运行的软件应用来说,这可能是有问题的,因为获得管理权限意味着可以自由地修改解决方案的核心配置。例如,获得这种管理权限的客户用户可以执行未授权的动作,例如删除宿主机,改变管理虚拟机的配置等。

[0003] 一些现有的解决方案依赖于监控已经发生的和可能未被授权的事件。这些解决方案的一个大缺点是它们是事后检测方法。它们实际上不能阻止未授权的活动或操作的发生,这可能导致潜在灾难性的配置改变和/或由于客户产生的错误而导致的数据丢失。

发明内容

[0004] 本公开描述了未授权阻塞角色(Unauthorized-Blocking-Role,UAB)的体系结构和设计。UAB是一种防止云托管软件的较高权限用户在管理或受保护对象上执行未授权的活动的机制。

[0005] 本公开的一个方面提供了一种在分布式计算系统中防止未授权活动的方法。该方法包括利用一个或多个处理器周期性地扫描云计算系统的管理软件中的对象;利用所述一个或多个处理器基于所述扫描来识别具有管理权限的客户用户;以及利用所述一个或多个处理器为所识别的所述客户用户应用基于角色的访问控制(RBAC)。周期性地扫描可以在未授权活动的事件之前执行,使得所述应用RBAC作为预防性措施执行,或者作为在检测到未授权事件之后的处罚措施执行。

[0006] 应用所述RBAC包括:遍历云计算平台对象层级;对于所述层级中的每个对象,将所识别的所述用户的许可分类至一个或多个桶;对于每个对象,评估所述桶中的所述许可;确定未授权的活动阻止器(UAB)部署;以及应用UAB更新。所述一个或多个桶包括UAB许可桶,直接用户级许可桶,继承用户级许可桶,直接组级许可桶,或继承组级许可桶中的至少一个。在一些示例中,评估许可包括生成所述对象的有效用户许可映射。在其它示例中,评估许可包括在所述一个或多个桶中比较所识别的用户的条目。确定所述UAB部署包括基于对

所述许可的所述评估来确定是否应新应用,保留或修改UAB许可。应用UAB更新包括调用管理应用编程接口。

[0007] 根据一些示例,识别具有管理权限的客户用户包括检测客户的权限的升级。在其它示例中,它包括检测由另一客户用户创建所述具有管理权限的客户用户。

[0008] 本公开的另一方面提供了一种在云计算系统中防止未授权活动的系统。该系统可以包括一个或多个处理器,被配置为:周期性地扫描所述云计算系统的管理软件中的对象;基于所述扫描来识别具有管理权限的客户用户;以及为所识别的所述客户用户应用基于角色的访问控制(RBAC)。所述周期性地扫描在未授权活动的事件之前执行,使得所述应用RBAC作为预防性措施执行,或者作为在检测到未授权事件之后的处罚措施执行。

[0009] 在应用所述RBAC时,所述一个或多个处理器还被配置为遍历云计算平台对象层级;对于所述层级中的每个对象,将所识别的所述用户的许可分类至一个或多个桶;对于每个对象,评估所述桶中的所述许可;确定未授权的活动阻止器(UAB)部署;以及应用UAB更新。所述一个或多个桶包括UAB许可桶,直接用户级许可桶,继承用户级许可桶,直接组级许可桶,或继承组级许可桶中的至少一个。为了评估许可,所述一个或多个处理器还被配置为生成所述对象的有效用户许可映射,和/或在所述一个或多个桶中比较所识别的所述用户的条目。为了确定UAB部署,所述一个或多个处理器还被配置为基于对所述许可的所述评估来确定是否应新应用,保留或修改UAB许可。为了应用UAB更新,所述一个或多个处理器还被配置为调用管理应用编程接口。

[0010] 为了识别具有管理权限的客户用户,所述一个或多个处理器还可以被配置为检测客户的权限的升级,和/或检测由另一客户用户创建所述具有管理权限的客户用户。

[0011] 本发明的另一方面提供一种存储可由一个或多个处理器执行的指令的非暂态计算机可读介质,所述指令用于执行在云计算系统中防止未授权活动的方法。指令可以包括周期性地扫描所述云计算系统的管理软件中的对象;基于所述扫描来识别具有管理权限的客户用户;以及为所识别的所述客户用户应用基于角色的访问控制(RBAC)。

附图说明

[0012] 图1是根据本公开的各方面的示例系统的框图。

[0013] 图2是示出根据本公开的各方面的示例性过程的关系框图。

[0014] 图3是根据本公开的各方面的示例性层级结构的框图。

[0015] 图4是示出了根据本公开的各方面对所选对象的保护的示例性层级对象树的框图。

[0016] 图5是示出根据本公开的各方面的另一示例性过程的关系框图。

[0017] 图6是示出根据本公开的各方面的示例方法的流程图。

具体实施方式

[0018] 未授权的活动阻止器(Unauthorized Activity Blocker,UAB)通过定期监控客户用户对管理软件中的对象层级结构中的关键管理或者受保护对象的权限来工作。如果检测到客户用户在这些对象上的权限高于他应该拥有的权限,则UAB在用户上应用限制性的基于角色的访问控制(Restrictive role-Based Access Controls,RBAC)。类似地,UAB还监

控受保护的主体和受保护的角色,以确保其权限不被客户用户修改。

[0019] UAB可以在诸如云计算系统的系统中实施。系统可以包括多个硬件计算设备和第三方服务器虚拟化软件。第三方虚拟化软件可以包括管理软件。下面结合图1描述这种系统的一个示例。系统可以被配置为托管先前在客户自己的物理设施的硬件上实施的服务,并且因此作为第三方即服务(third party as a service,3PaaS)解决方案发挥作用。

[0020] 图1示出了包括分布式计算环境的示例系统。分布式计算环境可以包括专用云即服务(Private Cloud as a Service,PCaaS)计算环境。多个数据中心160,170,180可以例如通过网络150通信地耦合。数据中心160,170,180还可以通过网络150与例如客户端110的一个或多个客户端设备通信。因此,例如,客户端110可以在“云”中执行操作。在一些示例中,数据中心160,170,180还可以与控制器190通信。

[0021] 每个客户端110可以是个人计算机或移动设备,旨在供人使用,具有通常在个人计算机中发现的所有内部组件,例如中央处理单元(CPU)、CD-ROM、硬盘驱动器和显示设备,例如具有屏幕的显示器、投影仪、触摸屏、小型LCD屏幕、电视、或其它设备,例如可以操作来显示由处理器120处理的信息的电气设备、扬声器、调制解调器和/或网络接口设备、用户输入,例如鼠标,键盘,触摸屏或麦克风,以及用于将这些元件彼此连接的所有部件。此外,根据本文所述的系统和方法的计算机可包括能够处理指令并向/从人类和其它计算机传输数据的设备,包括通用计算机、PDA、平板电脑、移动电话、智能手表、缺乏本地存储能力的网络计算机、电视的机顶盒和其它联网设备。

[0022] 客户端110可以包含处理器120、存储器130、和通常存在于通用计算机中的其它部件。存储器130可以存储处理器120可访问的信息,包括可以由处理器120执行的指令132。存储器还可包括可由处理器120检索,操纵或存储的数据134。存储器130可以是能够存储处理器120可访问的信息的非暂态计算机可读介质,例如硬盘驱动器、固态驱动器、磁带驱动器、光存储、存储卡、ROM、RAM、DVD、CD-ROM、可写和只读存储器。处理器120可以是众所周知的处理器或其它不太知名的处理器类型。或者,处理器120可以是专用控制器,例如ASIC。

[0023] 指令132可以是由处理器120直接执行的指令集合,例如机器码,或间接执行的指令,例如脚本。在这方面,术语“指令”、“步骤”和“程序”在此可以互换使用。指令132可以以目标代码格式存储,用于由处理器120直接处理,或其它类型的计算机语言,包括按需解释或预先编译的独立源代码模块的脚本或集合。

[0024] 数据134可由处理器120根据指令132检索,存储或修改。例如,尽管系统和方法不受特定数据结构的限制,但是数据134可以被存储在计算机寄存器中,在数据存储中作为具有多个不同字段和记录的结构、或文档、或缓冲器。数据134也可以被格式化为计算机可读格式,例如但不限于二进制值,ASCII或Unicode。此外,数据134可以包括足以标识相关信息的信息,诸如数字,描述性文本,专有代码,指针,对存储在其它存储器(包括其它网络位置)中的数据的引用,或者由函数用来计算相关数据的信息。

[0025] 尽管图1在功能上将处理器120和存储器130示为在同一框内,但是处理器120和存储器130实际上可以包括多个处理器和存储器,这些处理器和存储器可以或可以不存储在同一物理壳体内。例如,指令132和数据134中的一些可存储在可移除CD-ROM上,而其它可存储在只读计算机芯片内。指令和数据中的一些或全部可存储在物理上远离处理器120但仍可由处理器120存取的位置中。类似地,处理器120实际上可包括处理器的集合,其可并行或

不并行操作。

[0026] 数据中心160-180可以彼此相距相当远的距离。例如，数据中心可以位于世界各国。每个数据中心160,170,180可以包括一个或多个计算设备，诸如处理器，服务器，分片(Shard)等。例如，如图1所示，数据中心160包括计算设备162,164，数据中心170包括计算设备172，并且数据中心180包括计算设备181-186。

[0027] 根据一些示例，计算设备可以包括运行在宿主机上的一个或多个虚拟机。例如，计算设备162可以是支持运行操作系统和应用的多个虚拟机166,167的宿主机。虽然在图1中仅示出了几个虚拟机166,167，但是应当理解，任意数量的宿主计算设备可以支持任意数量的虚拟机。此外，应当理解，图1中所示的配置仅仅是示例，并且示例数据中心160-180中的每一个中的计算设备可以具有彼此相同或不同的各种结构和部件。

[0028] 根据一些示例，计算设备还可以包括管理工具，例如管理管理程序(management hypervisor)164。管理管理管理程序164可以在管理服务器(未示出)上执行，并且可以执行一个或多个管理虚拟机(未示出)。管理管理程序164可以为在数据中心160中执行的专用云提供管理服务。这样的管理服务可以包括，例如，资源管理，虚拟机管理，虚拟机部署，任务调度，统计，记录，服务器管理等。管理服务可以使用第三方虚拟化软件来执行。虽然仅示出了一个管理管理程序164，但是应当理解，数据中心160,170,180中的任何一个或全部可以具有任何数量的管理工具。

[0029] 在一些示例中，管理工具可以包括与数据中心160-180中的计算设备通信的独立的控制器190。例如，控制器190可以跟踪每个计算设备的容量，状态，工作负荷或其它信息，并使用这些信息来分配任务。控制器190可以包括处理器198和存储器192，包括数据194和指令196，类似于上述客户端110。控制器190可以被配置为在整个分布式数据存储中保持授权参数的一致性。例如，保持一致性可以包括由监听设备监听特定事件，设备在检测到该特定事件时向存储器发送消息。同步设备可以读取存储的消息，并处理该消息，包括更新建立在分布式数据存储器上的后端系统。监听设备和同步设备可以是相同的设备或不同的设备。例如，控制器190可以用作监听设备和同步设备中的一个或两个。根据其它示例，网络的其它节点用作监听设备和同步设备中的一个或两个。仅作为示例，多个节点，例如每个数据中心160-180中的一个，可以被指定为监听设备。进一步对于该示例，控制器190可以作为同步设备，处理对每个后端系统的授权更新。

[0030] 例如，可以在计算设备上执行程序，使得一些操作由第一数据中心的一个或多个计算设备执行，而其它操作由第二数据中心的一个或多个计算设备执行。在一些示例中，各种数据中心中的计算设备可以具有不同的容量。例如，不同的计算设备可以具有不同的处理速度，工作负荷等。虽然仅示出了这些计算设备中的几个，但是应当理解，每个数据中心160,170,180可以包括任意数量的计算设备，并且第一数据中心的计算设备的数量可以不同于第二数据中心中的计算设备的数量。此外，应当理解，每个数据中心160-180中的计算设备的数量可以随时间变化，例如，随着硬件的移除，替换，升级或扩展。

[0031] 此外，可以在分布式数据存储上建立各种后端系统。例如，身份管理系统，域名服务器(DNS)设置管理系统等。这种后端系统在某种程度上可以是相互关联的。例如，DNS设置管理系统的用户可以使用由身份管理系统管理的标识登录。在这方面，提供对这种后端系统的访问的授权参数应该是一致的。因此，影响对一个后端系统或对分布式数据存储的另

一部分的访问的更新应该被有效地渗透到相互关联的后端系统，从而确保授权参数是一致的。

[0032] 在一些示例中，每个数据中心160-180还可以包括多个存储设备(未示出)，例如硬盘驱动器，随机存取存储器，磁盘，磁盘阵列，磁带驱动器或任何其它类型的存储设备。数据中心160-180可以实现多种体系结构和技术中的任何一种，包括但不限于直接连接存储(DAS)，网络连接存储(NAS)，存储区域网络(SAN)，光纤信道(FC)，以太网上的光纤信道(FCoE)，混合体系结构网络等。数据中心可以包括除存储设备之外的多个其它设备，例如电缆，路由器等。此外，在一些示例中，数据中心160-180可以是虚拟化环境。此外，虽然仅示出了几个数据中心160-180，但是许多数据中心可以通过网络150和/或其它网络耦合。

[0033] 客户端110，数据中心160-180和控制器190能够直接和间接通信，例如通过网络150。例如，使用因特网套接字，客户端110可以通过因特网协议套件连接到在远程服务器上操作的服务。服务器可以建立监听套接字，套接字可以接受用于发送和接收信息的发起连接。网络150和中间的节点可以包括各种配置和协议，包括因特网，万维网，内联网，虚拟专用网，广域网，局域网，使用一个或多个公司的专用通信协议的专用网络，以太网，WiFi(例如，702.71，702.71b，g，n，或其它此类标准)，以及RPC，HTTP，以及前述的各种组合。这种通信可以由能够与其它计算机之间的传输数据的设备，如调制解调器(例如，拨号，电缆或光纤)和无线接口来促进。

[0034] 客户端110可以代表多个客户端设备。云系统或专用云可以为多个用户帐户提供环境，其中用户帐户通过客户端设备110访问云系统。每个用户帐户可以被分配指定的权限以执行特定的命令或程序。根据一些示例，一些用户帐户可以获得管理权限。管理权限的示例包括添加用户，升级软件等的权限。管理权限可以永久地或在指定的临时持续时间内获得。

[0035] UAB与第三方软件配置监控携手并进，第三方软件负责对客户用户执行的潜在未授权的活动进行事后监控。它为客户可能获得管理权限的情况提供保护，例如云主机引擎提供的明确手段，让客户成为第三方软件的管理员。它还为作为管理员的客户用户创建另一个具有管理员权限的客户用户的情况提供保护。

[0036] UAB还可以用作由多个组件组成的系统中的安全监控工具，其中用户可以临时请求较高的权限访问以对某些对象执行专门的操作。

[0037] 图2示出了触发UAB的流程。如图所示，UAB可以以预防模式(preventive mode)或处罚模式(penalizing mode)触发。在预防模式中，一旦检测到具有更高权限的客户用户，就应用限制性RBAC。这种模式能够最大限度地安全和防止未授权的动作。处罚模式在检测到未授权活动时应用限制性RBAC，例如未授权活动由配置监控解决方案检测到的情况。在某些场景下，可以选择这种模式，即必须信任某些解决方案的用户来访问受保护的管理对象，并且权限不够细化，无法阻止一组操作同时允许其它操作。在这种情况下，默认的假设是用户表现良好并且将在授权的操作范围内操作。然而，如果检测到用户有违规行为，则对用户采取处罚动作，在受保护的管理对象应用UAB权限。

[0038] 如图2所示，在框210中，客户用户通过权限升级202或通过由另一客户用户204创建来获取管理权限。如果客户用户执行未授权的活动，则在框220中通过配置监控服务来检测该活动。这样的服务可以扫描管理事件(框222)，生成对未授权活动的警报(框224)，和/

或警告客户或纠正未授权活动做出的改变(框226)。在检测之后,可以应用UAB(框230)作为处罚动作。

[0039] UAB可以附加地或替代地完全防止未授权的活动。例如,在某些情况下,对于不同的对象,不同的用户等可能需要不同的保护策略。因此,UAB可以用作某些策略的惩罚,以及用作其它策略的预防。在预防的情况中,UAB可以周期性地扫描管理对象(框232),识别具有管理权限的客户用户(框234),并且对所识别的用户应用限制的基于角色的访问控制(RBAC)(框236)。

[0040] 周期性扫描可以包括周期性地监控客户用户在管理软件对象层级(hierarchy)结构中的关键管理对象的许可。例如,可以每分钟一次,每小时一次,每天一次或以任何其它频率执行扫描。

[0041] 基于扫描,识别具有较高权限的客户用户,例如管理权限。可以确定被识别的用户的管理权限高于用户应该具有的管理权限。

[0042] 如果检测到客户用户的权限高于他在给定对象上应该具有的权限,则UAB在用户上应用限制性RBAC。例如,UAB限制所识别的客户用户的访问。类似地,UAB还监控受保护的主体和受保护的角色,以确保其权限不被客户用户修改。

[0043] UAB权限可以直接应用于对象层级结构的任何部分的用户级,或者应用于组级,或者作为组合。这确保了在用户是其他组的成员,而这些组(也具有对给定对象的权限)的情况下,用户的净有效权限将对应于UAB权限。

[0044] 根据一些示例,可以定义新的角色来应用UAB权限。每个角色都是构成了应用在管理对象上的限制性RBAC的权限的集合。在一个示例中,可以定义多个角色。例如,多个角色可以帮助持久地区分“有效”权限的原始源,从而确保在删除UAB时可以有效地恢复权限。角色的示例包括UAB角色,UAB间接用户角色和UAB直接用户角色。在一些示例中,当较高权限的有效源是组成员时,应用UAB角色。当较高权限的有效源是继承的直接用户权限时,应用UAB间接用户角色。这有助于容易地检测源。当较高权限的有效源是相关对象上的直接用户权限时,应用UAB直接用户角色。

[0045] 图3示出了描述各种对象及其关系的云计算平台库存层级。一些管理服务器许可模型可以基于对云计算平台对象层级结构中的此类对象分配许可。每个许可在给定对象上为用户或组提供一组权限,称为角色。用户可以获得关于对象的直接用户级许可,关于对象的继承的用户级许可,关于对象的直接组级许可,其中用户是组的成员,或者关于对象的继承的组级许可,其中用户是组的成员。

[0046] 在某些情况下,多个用户和组级许可可以适用于一个用户。在一些示例中,可以使用一个或多个规则来计算用户的有效许可。作为示例,这种规则可以包括:(1)用户级许可覆盖组级许可;(2)直接组级许可覆盖继承的组级许可;(3)如果不能基于规则1和2来确定许可,并且用户是多个组的成员,则将有效许可计算为成员组的许可的总和。

[0047] 图4示出了在层级结构中的对象周围创建的保护的示例。如图所示,示例性层级对象树400包括根节点410,配置节点410,上层对象节点420和下层对象节点430。

[0048] 根据一些示例,UAB可以在对象层级结构中的对象子集周围创建保护。例如,这样的子集可以包括任何一个或多个对象的分组。在所示的示例中,第一子集452包括对象032,第二子集454包括来自层级结构的两个不同级的对象023和035。第三子集456包括来自三个

不同级别的节点。当UAB保护被应用于子集452,454,456中的节点时,那些节点可以被认为是“受保护的”。虽然客户用户可以在树中的所有对象上具有管理权限,但是UAB可以应用于表示受保护对象的子集452,454,456中的任何一个或多个。即使在动态对象树配置中也是如此,在动态对象树配置中,由于云提供商管理程序或客户管理程序发起的操作,新对象或对象子树可以稍后添加。

[0049] 图5示出了UAB服务530的示例性实施方式。在该示例中,UAB服务530作为独立容器运行在监控空间中的容器组合(pod)中,例如Kubernetes pod。它从配置,集合,缓存(C3)服务515中检索必须被监视的专用云的列表,并检查在集群550上的列表中的对象的权限。集群550例如可以是第三方软件集群,例如VMware集群。

[0050] UAB服务530还与脚本540集合交互。脚本540用于在第三方软件集群550上实现改变。脚本540的一个示例可以包括Ansible Tower Playbooks。UAB服务530与脚本540交互,以实现许可改变,例如通过应用限制性RBAC。

[0051] 第三方软件配置监控服务520扫描事件并检查集群550中的未授权操作。配置监控服务520通知UAB 530应当针对较高权限用户采取处罚动作。UAB服务530依次采取诸如应用限制性RBAC的动作。

[0052] 图6示出了在受保护对象的层级结构上应用UAB的示例方法600,一旦用户的权限被取消,就删除UAB权限。云计算平台安全模型允许在对象树下层级传播,也允许在对象级的直接许可分配,以及基于用户和/或组成员的许可。虽然以特定的顺序描述了操作,但是应当理解,可以以不同的顺序或同时执行操作。另外,可以添加或删除操作。

[0053] 在框610,处理全局许可。例如,处理应用于层级结构中所有对象的权限。

[0054] 在框620中,遍历对象层级,例如,以考虑每个单独的对象。可使用多种算法中的任何一种来遍历所述层级,例如宽度优先搜索(Breadth-First-Search,BFS)算法。在BFS算法中,创建BFS级别,每个级别都有对象。例如,数据中心对象可以在顶层,之后是集群对象等。

[0055] 在框630,为每个对象的用户许可进行分类。许可可以被分类到不同的桶(bucket)中。例如,对于每个“受保护的”对象,扫描该组许可,并且将该许可所应用的相关用户分配给特定的桶。桶的示例可以包括UAB许可桶,直接用户级许可桶,继承的用户级许可桶,直接组级许可桶和继承的组级许可桶。UAB许可桶可以包含具有直接用户级权限的用户和角色之间的映射,其中角色与UAB角色之一匹配。直接用户级许可桶可以包括在对象上具有直接用户级权限的用户和角色之间的映射。继承的用户级许可桶可以包括在对象上具有继承的用户级许可的用户和角色之间的映射。直接组级许可桶可以包括在对象上具有直接组级许可的组的用户和角色之间的映射。继承的组级许可桶可以包括在对象上具有继承的组级许可的组的用户和角色之间的映射。应当理解,这些仅仅是示例,并且可以使用另外的或更少的桶,以及不同类型的桶。此外,可以将用户分配给多个桶。

[0056] 在框640中,对于每个对象,按照特定的优先级顺序在桶中评估许可。许可评估可能需要检查对象的父对象的桶。评估的结果是更新的每个对象的UAB许可桶和有效的用户权限映射。

[0057] 例如,对于每个受保护对象,有效的用户权限权限映射被初始化,其中该映射存储用于相关客户用户的权限配置。仅作为示例,映射的模式可以是:

user-effective-priv[object]＝{"user-x":{"priv-level-hi":"true/false",

bucket:B/C/D/E},"user-y":{"priv-level-hi":"true/false",bucket:B/C/D/E},…}

[0058] 该映射最初可以被设置为NULL,并且在为每个对象解析桶时被填充。

[0059] 在评估UAB角色桶时,对于桶中的每个条目可以设置默认值,假设UAB许可将被删除,除非对象上的另一个更高级别的权限加强了保持UAB权限完整的需要。如果用户具有直接许可,或者如果用户具有继承许可并且其父级保留许可,则用户可以保留许可。否则,可以删除用户的UAB角色。

[0060] 在评估直接用户级许可桶和间接用户级许可桶时,对于各个桶中的每个用户,可以将条目添加到“user-effective-priv”对象,该对象指示对应于用户的角色是否具有适当的权限。同一用户不能在直接和间接用户级许可桶中。

[0061] 在评估直接组级许可桶时,对于桶中的每个用户,检查user-effective-priv对象中是否已经存在条目。如果条目存在于直接或间接用户级许可桶中的任一个中,则可以忽略用户。然而,如果该条目存在于别处,并且被解析的桶条目的“角色”具有更高的权限,则用指示权限级别的更新值来修改该条目。如果用户还不存在,则可以创建新的条目。

[0062] 评估间接组级许可桶可以类似于评估直接组级许可桶。特别地,对于桶中的每个用户,检查在user-effective-priv对象中是否已经存在条目。如果条目存在于任何直接或间接用户级许可桶或直接组级许可中,则可以忽略用户。然而,如果该条目存在于别处,并且被解析的桶条目的“角色”具有更高的权限,则用指示权限级别的更新值来修改该条目。如果用户还不存在,则可以创建新的条目。

[0063] 在框650中,确定UAB部署。例如,该过程可以迭代遍历每个对象的有效用户权限映射,以确定UAB权限是否应该被新应用于该对象,或被保留,或被修改。UAB许可桶可以相应地被更新。

[0064] 如果用户尚未在UAB许可桶中,则可以确定应该新应用UAB许可。在这种情况下,可以基于对象的有效用户权限映射中的桶计算的新UAB来添加用户。

[0065] 当用户已经在UAB许可桶中时,并且用户的新角色对应于在UAB许可桶中标识的角色,则可以确定应该保留UAB权限。如果用户已经在UAB许可桶中,但是用户的新角色在那里没有被识别,则可以确定应该修改UAB许可。

[0066] 在框660中,应用UAB更新。例如,迭代每个对象的UAB许可桶,以基于前面的块中的评估来确定是否必须应用或删除UAB许可。可以调用管理应用程序编程接口(API)来实现改变。

[0067] 上述技术是有利的,因为它们可以减小升降用例转移到云的摩擦。此外,他们允许客户保留他们在企业内部的配置中习惯的安全策略,但是以安全的方式。此外,它们提供了一种基于其行为灵活地控制客户用户的访问权限的方法。

[0068] 除非另有说明,否则上述替代示例不是相互排斥的,而是可以以各种组合来实现,以实现独特的优点。由于在不脱离由权利要求限定的主题的情况下,可以利用以上讨论的特征的这些和其它变化和组合,因此实施例的上述描述应当以说明的方式而不是以对由权利要求限定的主题的限制的方式来进行。此外,提供本文所述的实施例,以及措辞为“诸如”、“包括”等的条款,不应被解释为将权利要求的主题限制为具体实施例;相反,这些实施例仅用于说明许多可能的实施方案中的一个。此外,不同附图中的相同附图标记可以标识相同或相似的元件。

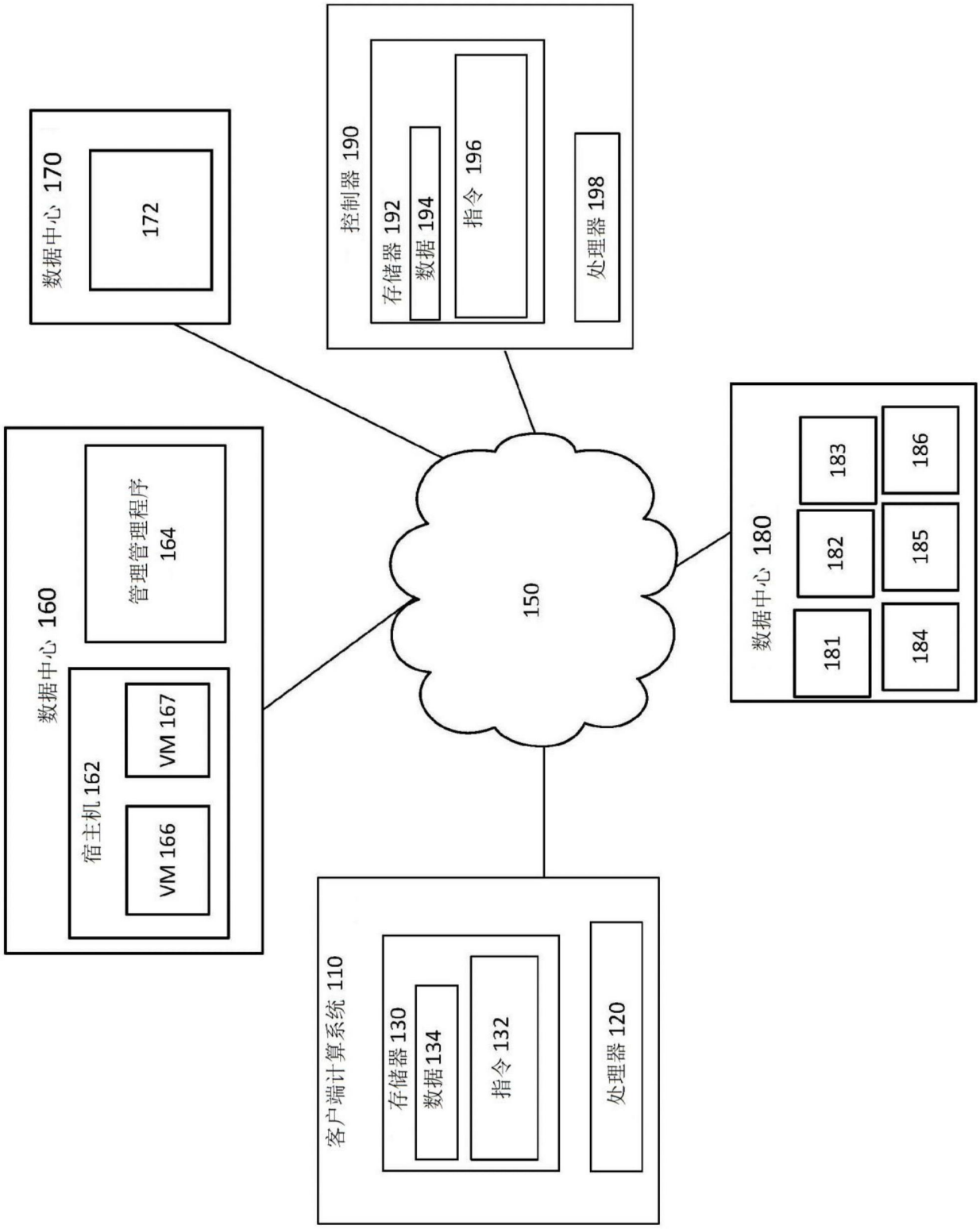

数据中心 170
172
控制器 190
存储器 192
数据 194
指令 196
处理器 198
数据中心 160
管理管理程序
164
宿主机 162
VM 166
VM 167
150
数据中心 180
181
182
183
184
185
186
客户端计算系统 110
存储器 130
数据 134
指令 132
处理器 120

图1

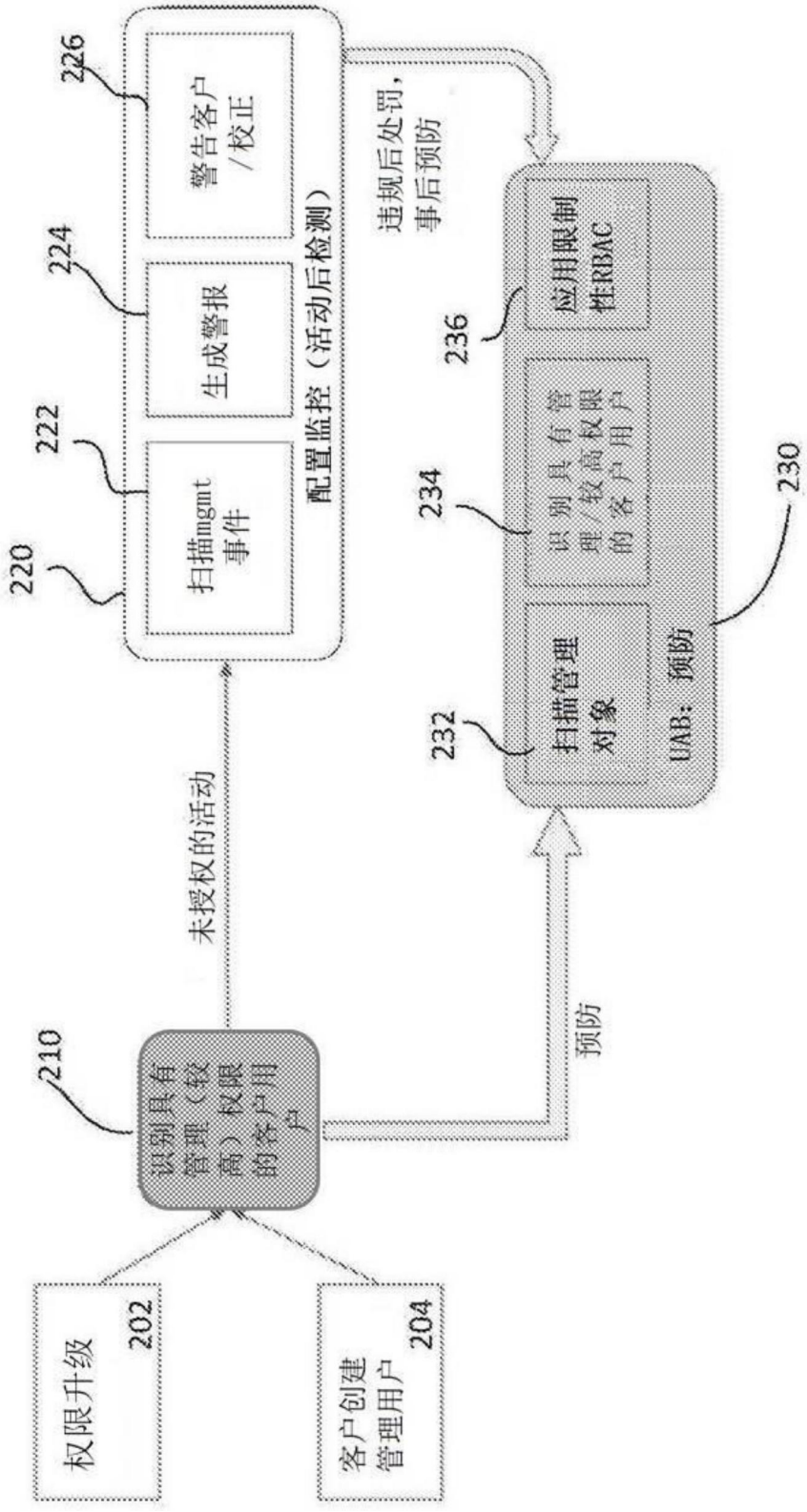

权限升级
202
客户创建管理用户
204
识别具有管理（较高）权限的客户用户
210
预防
未授权的活动
配置监控（活动后检测）
220
扫描mgmt事件
222
生成警报
224
警告客户/校正
226
违规后处罚，事后预防
扫描管理对象
232
识别具有管理/较高权限的客户用户
234
应用限制性RBAC
236
UAB：预防
230

图2

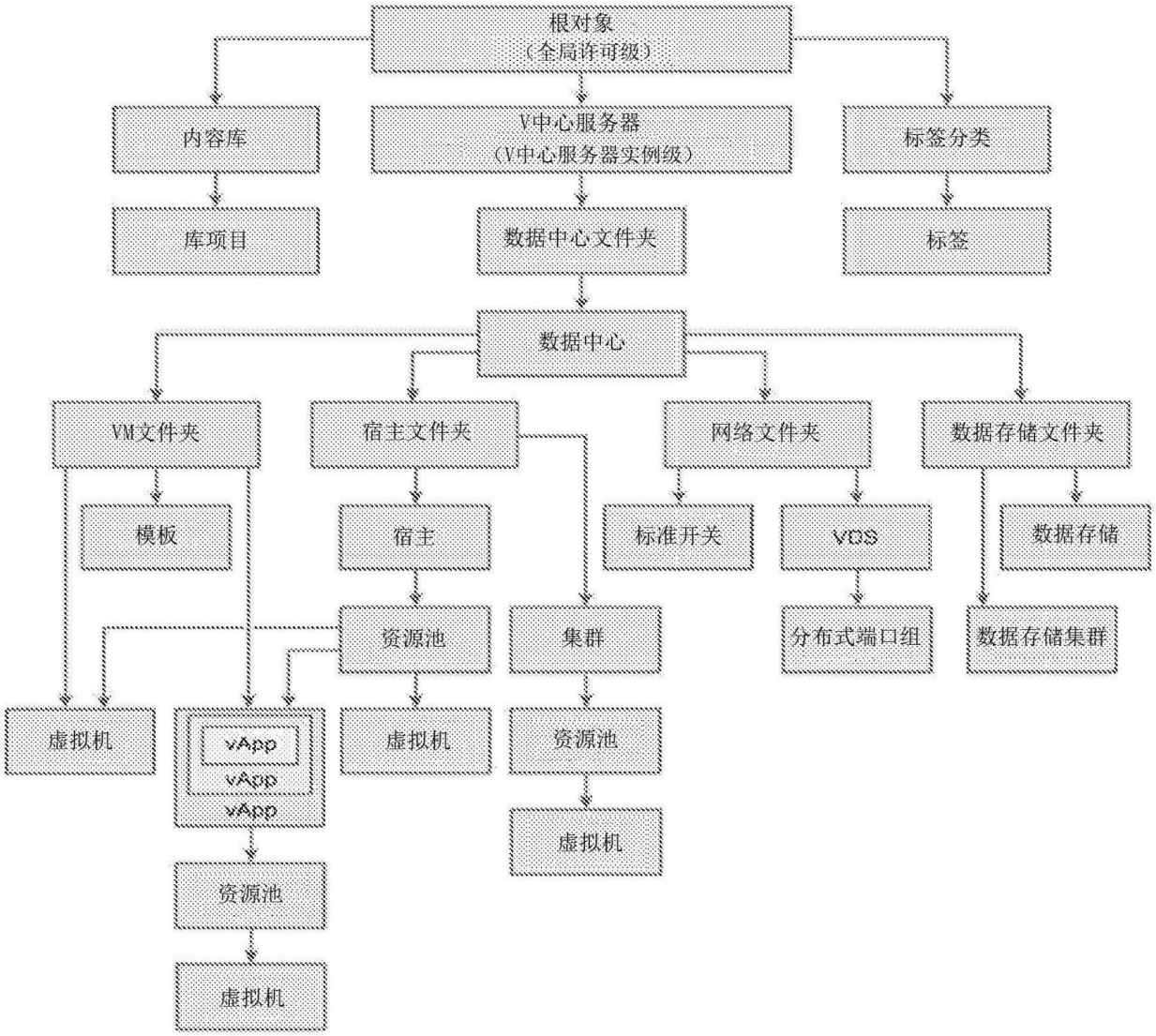

根对象
（全局许可级）
内容库
V中心服务器
（V中心服务器实例级）
标签分类
库项目
数据中心文件夹
标签
数据中心
VM文件夹
宿主文件夹
网络文件夹
数据存储文件夹
模板
宿主
标准开关
VDS
数据存储
资源池
集群
分布式端口组
数据存储集群
虚拟机
vApp
vApp
vApp
虚拟机
资源池
虚拟机
资源池
虚拟机

图3

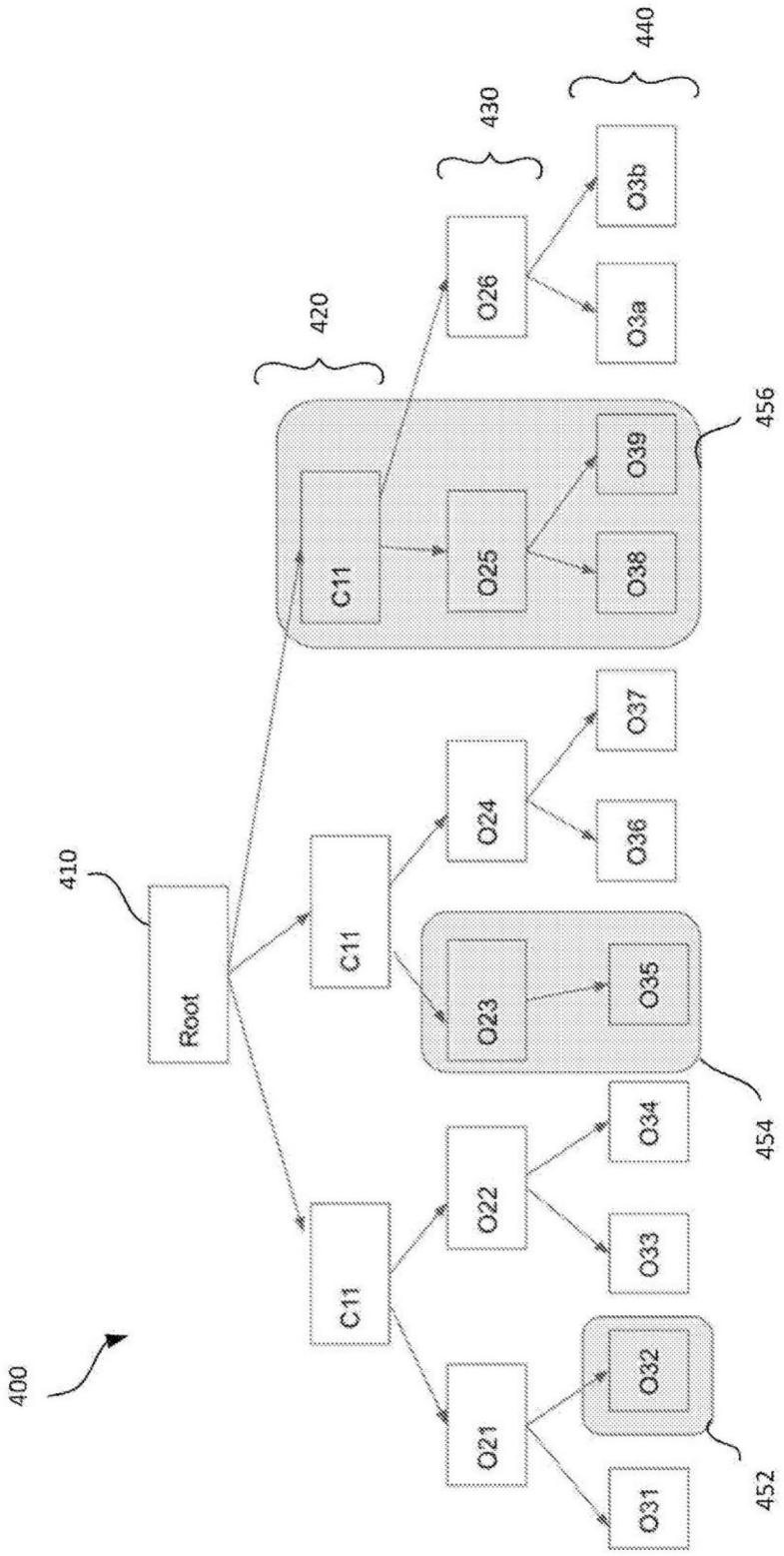

400
410
Root
C11
C11
C11
420
430
440
456
454
452
O26
O3b
O3a
C11
O25
O39
O38
O24
O37
O36
O23
O35
O22
O34
O33
O21
O32
O31

图4

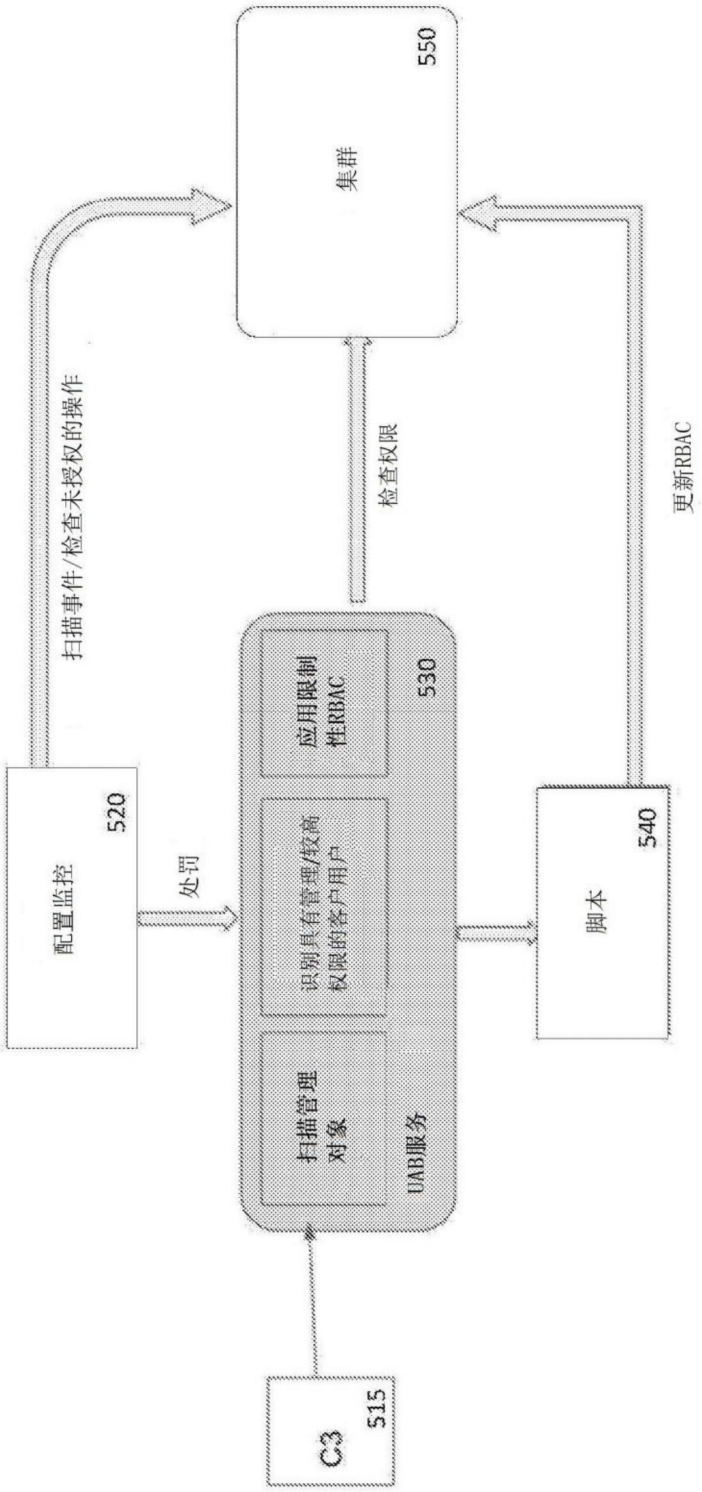

550
集群
扫描事件/检查未授权的操作
检查权限
更新RBAC
530
应用限制性RBAC
识别具有管理/较高权限的客户用户
扫描管理对象
UAB服务
520
配置监控
处罚
540
脚本
C3
515

图5

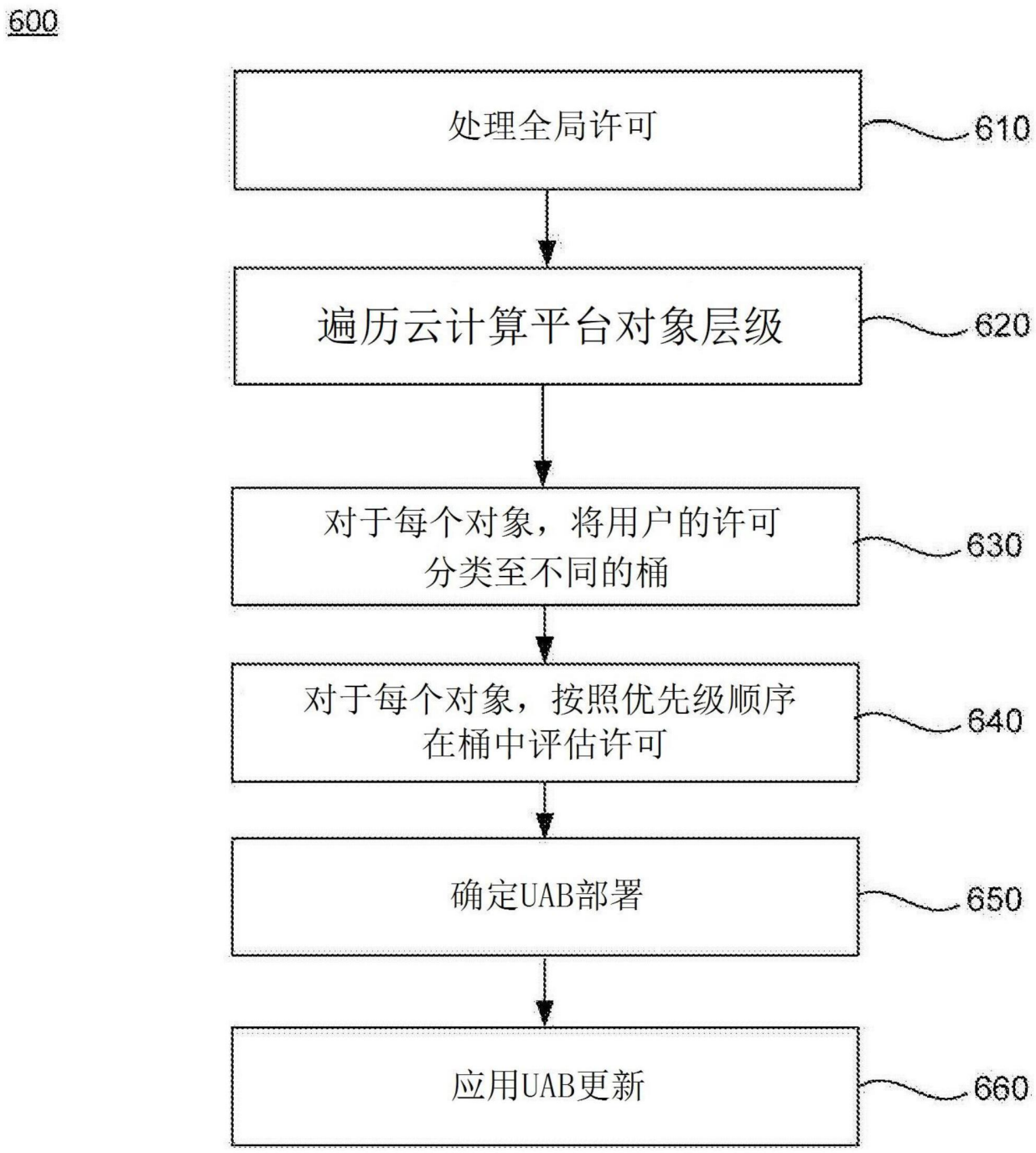

600
处理全局许可
610
遍历云计算平台对象层级
620
对于每个对象，将用户的许可
分类至不同的桶
630
对于每个对象，按照优先级顺序
在桶中评估许可
640
确定UAB部署
650
应用UAB更新
660

图6