(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113297589 B
(45)授权公告日 2024.04.16

(21)申请号 202110352368.4

(22)申请日 2021.03.31

(65)同一申请的已公布的文献号
申请公布号 CN 113297589 A

(43)申请公布日 2021.08.24

(73)专利权人 阿里巴巴创新公司
地址 新加坡勿拉士峇沙路51号来赞达一号大厦#03-06

(72)发明人 匡大虎 黄竹刚 李鹏

(74)专利代理机构 北京智信禾专利代理有限公司 11637
专利代理师 吴肖肖

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

(56)对比文件
CN 102088360 A,2011.06.08
CN 104394141 A,2015.03.04
CN 104537488 A,2015.04.22
CN 106161462 A,2016.11.23
CN 109033809 A,2018.12.18
CN 109643242 A,2019.04.16
CN 112333244 A,2021.02.05
CN 112417379 A,2021.02.26
KR 20120065783 A,2012.06.21
US 2011167483 A1,2011.07.07
US 2014245461 A1,2014.08.28
US 2017346807 A1,2017.11.30
US 2018262510 A1,2018.09.13
US 2019340360 A1,2019.11.07
US 7336790 B1,2008.02.26
US 9594922 B1,2017.03.14
CN 110990150 A,2020.04.10
CN 109327477 A,2019.02.12
CN 104125219 A,2014.10.29
CN 107835181 A,2018.03.23

审查员 吴银娥

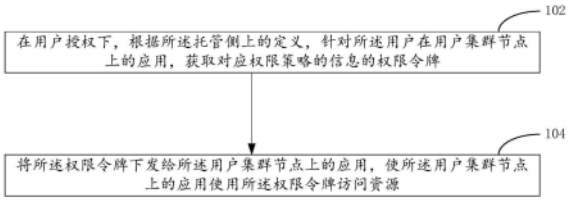
权利要求书3页 说明书10页 附图5页

(54)发明名称

设置集群权限的方法、装置及系统

(57)摘要

本说明书实施例提供设置集群权限的方法、装置及系统,其中所述设置集群权限的方法应用于托管侧,所述托管侧上定义了一个或多个应用各自所需权限策略的信息,所述方法包括:在用户授权下,根据托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,将所述权限令牌下发给所述用户集群节点上的应用。



CN 113297589 B

1.一种设置集群权限的方法,应用于托管侧,所述托管侧上从应用维度进行权限的拆分,定义了用户在用户集群节点上的一个或多个应用各自所需权限策略的信息,所述权限策略的信息包括权限策略对应的角色,所述方法包括:

在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;

所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:

在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌;

将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源;

所述将权限令牌下发给所述用户集群节点上的应用,包括:

将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源。

2.根据权利要求1所述的方法,所述将角色令牌下发给所述用户集群节点上的应用,包括:

对所述角色令牌进行加密;

将加密后的角色令牌以秘钥凭据的形式下发给所述用户集群节点的应用。

3.根据权利要求1所述的方法,所述应用包括:系统组件应用和/或用户自定义组件应用。

4.根据权利要求1所述的方法,所述托管侧上定义了一个或多个应用各自所需权限策略的信息,包括:

所述托管侧上设置了自定义资源对象,使所述用户集群节点具有对应的自定义资源实例部署,所述自定义资源实例,用于声明用户集群节点上的一个或多个应用所需权限策略的信息。

5.根据权利要求4所述的方法,还包括:

响应于监听到所述自定义资源实例中一个或多个应用所需权限策略的信息的更新,根据所述更新,相应向所述用户集群节点中对应的应用下发对应的权限令牌、吊销对应的权限令牌的下发凭证、或更新对应的权限令牌。

6.根据权利要求5所述的方法,还包括:

接收用户集群节点针对所述应用发出的权限设置请求;

根据所述权限设置请求,相应为所述用户集群节点上的应用下发或者吊销权限令牌。

7.根据权利要求6所述的方法,所述权限设置请求触发所述自定义资源实例中对应应用所需权限策略的信息的更新。

8.根据权利要求1所述的方法,还包括:

在下发的权限令牌具有对应的有效期的情况下,托管侧根据所述有效期以及应用的需要,对下发的权限令牌进行轮转更新。

9.一种设置集群权限的装置,配置于托管侧,所述托管侧上从应用维度进行权限的拆分,定义了用户在用户集群节点上的一个或多个应用各自所需权限策略的信息,所述权限

策略的信息包括权限策略对应的角色,所述装置包括:

令牌获取模块,被配置为在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌;

令牌下发模块,被配置为将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源;所述将权限令牌下发给所述用户集群节点上的应用,包括:将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源。

10.一种设置集群权限的系统,包括:托管侧以及用户集群侧,所述用户集群侧包括若干个用户集群节点,其中,所述用户集群节点上设置了应用,所述托管侧上从应用维度进行权限的拆分,定义了用户在用户集群节点上的一个或多个应用各自所需权限策略的信息,所述权限策略的信息包括权限策略对应的角色;

所述托管侧,被配置为在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;将所述权限令牌下发给所述用户集群节点上的应用,所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌;所述将权限令牌下发给所述用户集群节点上的应用,包括:将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源;

所述应用,被配置为获取所述托管侧下发的权限令牌,使用所述权限令牌访问资源。

11.一种计算设备,包括:

存储器和处理器;

所述存储器用于存储计算机可执行指令,所述处理器用于执行所述计算机可执行指令:

在用户授权下,根据托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;所述托管侧上从应用维度进行权限的拆分,定义了用户在用户集群节点上的一个或多个应用各自所需权限策略的信息;

所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:

在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌;

将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源;

所述将权限令牌下发给所述用户集群节点上的应用,包括:

将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使

用所述角色令牌访问资源。

12.一种计算机可读存储介质,其存储有计算机指令,该计算机指令被处理器执行时实现权利要求1至8任意一项所述设置集群权限的方法的步骤。

设置集群权限的方法、装置及系统

技术领域

[0001] 本说明书实施例涉及计算机技术领域,特别涉及一种设置集群权限的方法。本说明书一个或者多个实施例同时涉及一种设置集群权限的装置,一种计算设备,一种计算机可读存储介质及设置集群权限的系统。

背景技术

[0002] 云服务,是一种基于互联网提供安全、可靠的计算和数据处理能力的服务。云服务的租户们可以使用云上资源来实现自己的项目。目前,在各云服务商部署的容器集群中,通过将权限绑定在用户集群节点上,使用户集群节点上的租户和云服务商的系统能够获取云资源信息。

[0003] 但是,将权限绑定在用户集群节点上的管理方式容易发生越权风险。

发明内容

[0004] 有鉴于此,本说明书实施例提供了一种设置集群权限的方法。本说明书一个或者多个实施例同时涉及一种设置集群权限的装置,一种计算设备,一种计算机可读存储介质及设置集群权限的系统,以解决现有技术中存在的技术缺陷。

[0005] 根据本说明书实施例的第一方面,提供了一种设置集群权限的方法,应用于托管侧,所述托管侧上定义了一个或多个应用各自所需权限策略的信息,所述方法包括:在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源。

[0006] 可选地,所述权限策略的信息为权限策略对应的角色。所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌。所述将权限令牌下发给所述用户集群节点上的应用,包括:将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源。

[0007] 可选地,所述将角色令牌下发给所述用户集群节点上的应用,包括:对所述角色令牌进行加密;将加密后的角色令牌以秘钥凭据的形式下发给所述用户集群节点的应用。

[0008] 可选地,所述应用包括:系统组件应用和/或用户自定义组件应用。

[0009] 可选地,所述托管侧上定义了一个或多个应用各自所需权限策略的信息,包括:所述托管侧上设置了自定义资源对象,使所述用户集群节点具有对应的自定义资源实例部署,所述自定义资源实例,用于声明用户集群节点上的一个或多个应用所需权限策略的信息。

[0010] 可选地,所述方法还包括:响应于监听到所述自定义资源实例中一个或多个应用

所需权限策略的信息的更新，根据所述更新，相应向所述用户集群节点中对应的应用下发对应的权限令牌、吊销对应的权限令牌的下发凭证、或更新对应的权限令牌。

[0011] 可选地，所述方法还包括：接收用户集群节点针对所述应用发出的权限设置请求；根据所述权限设置请求，相应为所述用户集群节点上的应用下发或者吊销权限令牌。

[0012] 可选地，所述权限设置请求触发所述自定义资源实例中对应应用所需权限策略的信息的更新。

[0013] 可选地，所述方法还包括：在下发的权限令牌具有对应的有效期的情况下，托管侧根据所述有效期以及应用的需要，对下发的权限令牌进行轮转更新。

[0014] 根据本说明书实施例的第二方面，提供了一种设置集群权限的装置，配置于托管侧，所述托管侧上定义了一个或多个应用各自所需权限策略的信息，所述装置包括：令牌获取模块，被配置为在用户授权下，根据所述托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌。令牌下发模块，被配置为将所述权限令牌下发给所述用户集群节点上的应用，使所述用户集群节点上的应用使用所述权限令牌访问资源。

[0015] 根据本说明书实施例的第三方面，提供了一种设置集群权限的系统，包括：托管侧以及用户集群侧，所述用户集群侧包括若干个用户集群节点，其中，所述用户集群节点上设置了应用。所述托管侧，被配置为在用户授权下，根据所述托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌；将所述权限令牌下发给所述用户集群节点上的应用。所述应用，被配置为获取所述托管侧下发的权限令牌，使用所述权限令牌访问资源。

[0016] 根据本说明书实施例的第四方面，提供了一种计算设备，包括：存储器和处理器；所述存储器用于存储计算机可执行指令，所述处理器用于执行所述计算机可执行指令：在用户授权下，根据托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌；所述托管侧上定义了一个或多个应用各自所需权限策略的信息；将所述权限令牌下发给所述用户集群节点上的应用。

[0017] 根据本说明书实施例的第五方面，提供了一种计算机可读存储介质，其存储有计算机指令，该计算机指令被处理器执行时实现本说明书任意实施例所述设置集群权限的方法的步骤。

[0018] 本说明书一个实施例提供了设置集群权限的方法，由于托管侧上定义了一个或多个应用各自所需权限策略的信息，无需用户进行复杂的权限部署，只要用户授权，托管侧即可根据所述托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌，将所述权限令牌下发给所述用户集群节点上的应用，使所述用户集群节点上的应用使用所述权限令牌访问资源，因此，托管侧从应用维度进行权限的拆分定义，根据定义下发权限令牌给用户集群节点的应用，不仅减少了用户操作，而且实现了集群的节点基础服务权限的权限收敛和保护，避免同一节点上的租户共享同一权限产生越权风险。

附图说明

[0019] 图1是本说明书一个实施例提供的一种设置集群权限的方法的流程图；

[0020] 图2是本说明书一个实施例提供的设置集群权限的系统部署架构图；

[0021] 图3是本说明书一个实施例提供的一种设置集群权限的装置的结构示意图；

[0022] 图4是本说明书另一个实施例提供的一种设置集群权限的装置的结构示意图；

[0023] 图5是本说明书一个实施例提供的一种设置集群权限的系统的结构示意图；

[0024] 图6是本说明书一个实施例提供的一种计算设备的结构框图。

具体实施方式

[0025] 在下面的描述中阐述了很多具体细节以便于充分理解本说明书。但是本说明书能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本说明书内涵的情况下做类似推广，因此本说明书不受下面公开的具体实施的限制。

[0026] 在本说明书一个或多个实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本说明书一个或多个实施例中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0027] 应当理解，尽管在本说明书一个或多个实施例中可能采用术语第一、第二等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一也可以被称为第二，类似地，第二也可以被称为第一。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0028] 首先，对本说明书一个或多个实施例涉及的名词术语进行解释。

[0029] 角色访问控制机制，是一种提供身份管理与资源访问权限的机制。例如，角色访问控制机制可以允许创建并管理多个角色并按需分配权限策略，从而实现不同角色拥有不同资源访问权限的目的。

[0030] 节点基础服务权限：用于云服务商部署的集群节点上的系统组件或用户后续部署的应用容器访问基础服务的资源模型或OpenAPI。

[0031] 权限收敛：遵循权限最小化原则设置权限策略的权限大小和作用域。

[0032] 在本说明书中，提供了一种设置集群权限的方法，本说明书同时涉及一种设置集群权限的装置，一种计算设备，一种计算机可读存储介质以及一种集群系统，在下面的实施例中逐一进行详细说明。

[0033] 图1示出了根据本说明书一个实施例提供的一种设置集群权限的方法的流程图。所述方法应用于托管侧，所述托管侧上定义了一个或多个应用各自所需权限策略的信息。所述方法包括步骤102至步骤104。

[0034] 步骤102：在用户授权下，根据所述托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌。

[0035] 步骤104：将所述权限令牌下发给所述用户集群节点上的应用，使所述用户集群节点上的应用使用所述权限令牌访问资源。

[0036] 可见，由于托管侧上定义了一个或多个应用各自所需权限策略的信息，无需用户进行复杂的权限部署，只要用户授权，托管侧即可根据所述托管侧上的定义，针对所述用户

在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源,因此,托管侧从应用维度进行权限的拆分定义,根据定义下发权限令牌给用户集群节点的应用,不仅减少了用户操作,而且实现了集群的节点基础服务权限的权限收敛和保护,避免同一节点上的租户共享同一权限产生越权风险。另外,由于根据本实施例提供的方法,权限收敛在托管侧,无需在用户集群节点中部署多余的权限管理工具,对用户集群节点的容器无需侵入式修改,也无需在客户集群引入额外组件,用户无需负责权限管理工具的稳定性和大规模弹性场景下的可用性,因此,用户没有额外的运维负担。

[0037] 例如,根据上述实施例提供的方法,可以在用户侧提供一键授权的功能选项,用户无需了解应用的工作细节,也无需自定义多个基础服务角色和绑定,也无需修改组件部署模板,只需要完成一键授权即可由托管侧进行基础服务权限的托管和相应凭证的下发,吊销等操作。由于用户无需进行复杂的模板配置和应用的权限部署,只需要调用统一的权限设置的接口一键授权即可完成权限设置,易用性和安全性更强。另外,对于用户集群节点来说,由于基础服务的系统组件的权限可以由托管侧托管统一管理,用户集群节点可以默认无任何权限,均可以由托管侧管理。当然,根据场景需要,用户集群节点可以保留例如删除秘钥凭据的能力。例如,在Kubernetes集群中,用户可以删除用户节点上的secret以直接按需吊销权限。

[0038] 需要说明的是,本说明书实施例提供的方法对于权限策略的信息以及权限下发的具体实现方式,并不进行限制。例如,根据角色访问控制机制,可以在托管侧上定义一个或多个应用各自所需权限策略对应的角色,通过下发角色令牌的方式下发权限。具体地,例如,所述权限策略的信息为权限策略对应的角色。所述在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,包括:在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌。所述将权限令牌下发给所述用户集群节点上的应用,包括:将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源。

[0039] 为了更进一步保证下发角色令牌的安全,本说明书一个或多个实施例中,所述将角色令牌下发给所述用户集群节点上的应用,包括:对所述角色令牌进行加密;将加密后的角色令牌以秘钥凭据的形式下发给所述用户集群节点的应用。在该实施例中,托管侧下发的角色令牌经过加密,配合集群的秘钥凭据这一访问控制策略保护下发凭证的安全性。其中,秘钥凭据,用于保存扮演应用所需权限策略的角色令牌。其中对角色令牌加密可以采用AES(Advanced Encryption Standard,高级加密标准)加密方式。

[0040] 根据上述实施例,集群节点的权限收敛到托管侧统一管理,并且以应用维度进行权限的拆分定义。每一个应用可以对应一个或多个secret(秘钥凭据)来下发权限。例如系统应用、用户选装的自定义应用等都可以由托管侧负责对应角色令牌的下发、更新轮转和吊销。所有下发到用户集群节点的角色令牌都经过托管侧内部加密处理,并且由托管侧负责定义轮转更新或吊销。可见,通过集群节点上的应用所需权限被托管侧收敛,以应用维度细粒度拆分了节点基础服务访问权限以及可选自定义应用,支持细粒度的应用的权限下发,增强了对节点权限管理的安全性,配合角色访问控制策略可以实现多租场景下的基础

服务权限隔离,降低了权限泄露的风险,从而达到了安全上的增强。

[0041] 需要说明的是,本说明书实施例提供的方法对于所述应用的具体形式并不进行限制。例如,所述应用可以包括:系统组件应用和/或用户自定义组件应用。可见,该实施例由使集群节点默认的系统组件应用的基础服务权限和后续可能添加到节点的用户自定义组件应用的可选组件权限均被收敛到托管侧,在多租场景下很好的提升了用户账号下云资源安全性。

[0042] 为了托管侧的安全性和易用性,本说明书一个或多个实施例中,所述托管侧上定义了一个或多个应用各自所需权限策略的信息,包括:所述托管侧上设置了自定义资源对象,使所述用户集群节点具有对应的自定义资源实例部署,所述自定义资源实例,用于声明用户集群节点上的一个或多个应用所需权限策略的信息。在该实施例中,通过集群节点的自定义资源实例声明的方式对应用所需权限策略的信息进行定义,实现了声明式的管理,用户在使用上只需要一键授权,避免了大量的权限定义和管理工作,使托管侧的安全性和易用性都得以增强。

[0043] 可以理解的是,由于实现了声明式的管理,在实例中的应用对应的权限策略的信息更新时(例如,托管侧根据系统需要更新权限或者按用户需要更新权限等场景),托管侧可以响应于该更新,自动对权限进行下发、更新或吊销,进一步增强托管侧的安全性和易用性。具体地,例如,所述方法还可以包括,响应于监听到所述自定义资源实例中一个或多个应用所需权限策略的信息的更新,根据所述更新,相应向所述用户集群节点中对应的应用下发对应的权限令牌、吊销对应的权限令牌的下发凭证、或更新对应的权限令牌。

[0044] 另外,为了便于用户下发自定义应用的权限,本说明书一个或多个实施例中,还可以包括:接收用户集群节点针对所述应用发出的权限设置请求;根据所述权限设置请求,相应为所述用户集群节点上的应用下发或者吊销权限。例如,可以接收用户集群节点针对所述应用发出的权限吊销请求;根据所述权限吊销请求,吊销所述权限的下发凭证,再例如,可以接收用户集群节点发出的权限下发请求,确定所述权限下发请求针对的应用所需的权限策略的信息,根据确定的权限策略的信息,下发对应权限给所述用户集群节点上的应用。下发凭证,是一种数字资料,其中的内容可以包括赋与凭证所有者权限的权限策略的信息。例如,在应用于Kubernetes集群的应用场景下,下发凭证可以以秘钥凭据secret的形式实现。

[0045] 结合监听自定义资源实例更新的实施方式,所述权限设置请求可以相应触发所述自定义资源实例中对应应用所需权限策略的信息的更新。所述根据权限设置请求,相应为所述用户集群节点上的应用下发或者吊销权限令牌的步骤,具体可以通过托管侧监听自定义资源实例的更新来实现。由于权限设置请求可以作用到自定义资源实例中配置的权限的更新,托管侧可以监听到该更新并发起调协下发新凭证或吊销凭证。例如,当用户自定义的组件不需要权限时,用户集群节点发出的针对该组件发出的权限吊销请求,可以触发对应CR实例的更新,使托管侧监听到该更新,进而取消该组件的凭证secret的下发。

[0046] 考虑到某些场景下,应用的权限令牌可能存在有效期的要求,因此,本说明书一个或多个实施例中,所述方法还包括:在下发的权限令牌具有对应的有效期的情况下,托管侧根据所述有效期以及应用的需要,对下发的权限令牌进行轮转更新或吊销。通过该实施例,使得托管侧对用户集群节点中的应用的权限管理更加贴合场景需要。

[0047] 下述结合附图2,以本说明书提供的设置集群权限的方法结合Kubernetes的托管组件(operator组件)对用户集群节点上的组件基于角色访问控制机制进行权限设置的具体实现为例,对所述设置集群权限的方法进行进一步说明。托管组件,是Kubernetes的扩展软件,它可以利用定制资源管理应用及其组件。图2示出了本说明书一个实施例提供的设置集群权限的系统部署架构图。在该设置集群权限的系统中,托管侧可以是云服务商托管的Kubernetes托管侧节点,即如图2所示的托管VPC(Virtual Private Cloud,虚拟私有云),用户集群节点即如图2所示的用户VPC。

[0048] 如图2所示,托管侧的operator组件“addon-token-operator”从集群节点上必须安装的系统组件出发以组件维度做权限的拆分,每一个组件对应一个或多个系统角色,从而便于管理各系统组件所需的权限列表,做到细粒度的收敛,另一个目的是缩小权限泄露后的攻击面。在权限拆分的基础上,可以在托管侧集群中定义用于声明用户集群节点所需基础服务范围的K8s CRD(即自定义资源对象),使每个用户集群节点都可以有一个与之对应的CR实例部署。如图2所示,CR实例中包括对角色配置“addon-token”的声明。“addon-token-operator”可以利用元集群托管组件来感应集群创建,依据CR实例中声明的角色配置,相应向用户集群节点的应用下发角色令牌。

[0049] 另外,用户还可以通过可选组件权限管理,自定义授权托管侧下发可选组件的角色权限或取消指定角色对应的权限。在某些应用场景下,也可以按需向用户展示托管侧定义的必装系统组件对应的角色,以便用户对必装系统组件对应的角色进行个性化调整。

[0050] “addon-token-operator”可以监听每个用户集群节点CR实例的更新,当CR实例中发生角色配置的变更时,“addon-token-operator”可以根据新的权限配置自动重新调协,调协过程中“addon-token-operator”可以重新扮演CR实例中声明的新角色,成功扮演获取的角色令牌可以以K8s secret即秘钥凭据的形式下发到用户集群中。

[0051] “addon-token-operator”在下发角色令牌之前,可以对角色令牌以AES方式加密。另外,还可以基于访问控制策略保护下发凭证的安全性,具体地,例如,可以结合用户集群托管主节点的原生组件“control-plane”创建秘钥凭据,用户集群secret,用来保存加密后的角色令牌。

[0052] 基于应用场景的需要,下发的角色令牌可以具有有效期,例如,三个小时的有效期。“addon-token-operator”可以负责维护角色令牌的自动轮转和新凭证的再下发。

[0053] 另外,当托管侧接收到用户的选装组件请求时,请求同样可以作用到CR实例进行权限的更新,“addon-token-operator”同样会监听该请求并发起调协完成新凭证的下发。当自选组件不需要权限时,通过集群绑定CR实例的修改同样可以由“addon-token-operator”吊销secret的下发。

[0054] 下面,对“addon-token-operator”角色令牌的下发、轮转更新、吊销的过程进行示例性说明。

[0055] 下发:例如,用户创建集群可能会部署如图2中用户VPC侧的一系列组件“存储组件”、“网络组件”、“日志组件”、“监控组件”等。这些组件需要访问云上自身账号下面的资源,因此,需要相应的权限。“addon-token-operator”响应于集群创建,根据声明的权限配置确定这些组件所需权限策略对应的角色,调用角色访问控制服务,获得角色令牌。“addon-token-operator”对角色令牌通过AES加密后以secret的形式,下发给用户集群节

点上的这些组件。这些组件运行时,可以从下发的secret里得到角色令牌。其中,解密角色令牌的秘钥可以同时被下发在secret里,组件根据一定的算法来进行解密,解密后即可使用角色令牌去访问云上资源。

[0056] 轮转更新:例如,“addon-token-operator”内可以设置有secret管理工具,该secret管理工具可以用于维护用户集群节点的secret及对应的有效期。在有效期过期之前,“addon-token-operator”会重新调用角色访问控制机制获得具有新的有效期的角色令牌。其中,该有效期可以是“addon-token-operator”根据场景需要设置具体有效期长度的。例如,“addon-token-operator”可以通过向角色访问控制机制传入有效期参数来使角色访问控制机制返回具有相应有效期的角色令牌。“addon-token-operator”更新用户VPC下的secret,使其保存具有新的有效期的角色令牌。

[0057] 吊销:例如,“addon-token-operator”可以直接触发用户集群节点删除相应的secret即可达到吊销权限的目的。

[0058] 通过上述实施例可见,在各云服务商部署的Kubernetes集群中,托管侧从应用维度进行权限的拆分定义,根据定义下发权限给用户集群节点的应用,从而云服务商自身部署在集群节点中的系统组件等应用能够正常获取到指定用户账号下的云资源信息,不必给集群节点绑定权限过大的基础服务权限,减少安全风险。而且各租户在通过Kubernetes集群部署自己的项目应用时,无需自己给节点绑定复杂的自定义权限,使用托管侧为应用下发的权限访问资源即可满足项目应用对基础服务云资源的访问权限要求,不仅减少用户操作,而且节点上部署的应用不存在通过其他租户给节点绑定的自定义权限跨租户访问的越权风险,保证租户管理的云资源的安全。因此,本说明书实施例提供的方法能够充分保证Kubernetes集群节点资源访问权限的收敛和保护。

[0059] 与上述方法实施例相对应,本说明书还提供了设置集群权限的装置实施例,图3示出了本说明书一个实施例提供的一种设置集群权限的装置的结构示意图。所述装置可以配置于托管侧,所述托管侧上定义了一个或多个应用各自所需权限策略的信息。如图3所示,该装置包括:令牌获取模块302及令牌下发模块304。

[0060] 该令牌获取模块302,被配置为在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;

[0061] 该令牌下发模块304,被配置为将所述权限令牌下发给所述用户集群节点上的应用。

[0062] 由于托管侧上定义了一个或多个应用各自所需权限策略的信息,无需用户进行复杂的权限部署,只要用户授权,托管侧即可根据所述托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌,将所述权限令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述权限令牌访问资源,因此,托管侧从应用维度进行权限的拆分定义,根据定义下发权限令牌给用户集群节点的应用,不仅减少了用户操作,而且实现了集群的节点基础服务权限的权限收敛和保护,避免同一节点上的租户共享同一权限产生越权风险。

[0063] 图4示出了本说明书另一个实施例提供的一种设置集群权限的装置的结构示意图。在该实施例中,所述权限策略的信息为权限策略对应的角色。所述令牌获取模块302,可以被配置为在用户授权下,根据所述托管侧上定义的一个或多个应用各自所需权限策略对

应的角色,针对所述用户在用户集群节点上的应用,基于角色访问控制机制获得对应的角色令牌。所述令牌下发模块304,可以被配置为将所述角色令牌下发给所述用户集群节点上的应用,使所述用户集群节点上的应用使用所述角色令牌访问资源。

[0064] 为了更进一步保证下发角色令牌的安全,本说明书一个或多个实施例中,所述令牌下发模块304,包括:令牌加密子模块3042及凭据下发子模块3044。

[0065] 该令牌加密子模块3042,可以被配置为对所述角色令牌进行加密。

[0066] 该凭据下发子模块3044,可以被配置为将加密后的角色令牌以秘钥凭据的形式下发给所述用户集群节点的应用。

[0067] 本说明书实施例通过集群节点上的应用所需权限被托管侧收敛,以应用维度细粒度拆分了节点基础服务访问权限以及可选自定义应用,支持细粒度的应用的权限下发,增强了对节点权限管理的安全性,配合角色访问控制策略可以实现多租场景下的基础服务权限隔离,降低了权限泄露的风险,从而达到了安全上的增强。

[0068] 需要说明的是,本说明书实施例提供的方法对于所述应用的具体形式并不进行限制。例如,所述应用可以包括:系统组件应用和/或用户自定义组件应用。为了托管侧的安全性和易用性,本说明书一个或多个实施例中,所述托管侧上设置了自定义资源对象,使所述用户集群节点具有对应的自定义资源实例部署,所述自定义资源实例,用于声明用户集群节点上的一个或多个应用所需权限策略的信息。相应地,该装置的令牌下发模块304还可以被配置为响应于监听到所述自定义资源实例中一个或多个应用所需权限策略的信息的更新,根据所述更新,相应向所述用户集群节点中对应的应用下发对应的权限令牌、吊销对应的权限令牌的下发凭证、或更新对应的权限令牌。

[0069] 另外,为了便于用户下发自定义应用的权限,本说明书一个或多个实施例中,该装置还可以包括:请求接收模块306,可以被配置为接收用户集群节点针对所述应用发出的权限设置请求。所述令牌下发模块304还可以被配置为根据所述权限设置请求,相应为所述用户集群节点上的应用下发或者吊销权限令牌。

[0070] 结合监听自定义资源实例更新的实施方式,所述权限设置请求可以触发所述自定义资源实例中对应应用所需权限策略的信息的更新。

[0071] 考虑到某些场景下,应用的权限令牌可能存在有效期的要求,因此,本说明书一个或多个实施例中,所述令牌下发模块304还可以被配置为在下发的权限令牌具有对应的有效期的情况下,根据所述有效期以及应用的需要,对下发的权限令牌进行轮转更新。

[0072] 上述为本实施例的一种设置集群权限的装置的示意性方案。需要说明的是,该设置集群权限的装置的技术方案与上述的设置集群权限的方法的技术方案属于同一构思,设置集群权限的装置的技术方案未详细描述的细节内容,均可以参见上述设置集群权限的方法的技术方案的描述。

[0073] 图5示出了本说明书一个实施例提供的一种设置集群权限的系统的结构示意图。如图5所示,该设置集群权限的系统可以包括:托管侧502以及用户集群侧504,所述用户集群侧504包括若干个用户集群节点506,其中,所述用户集群节点506上设置了应用508。

[0074] 所述托管侧502,可以被配置为在用户授权下,根据所述托管侧上的定义,针对所述用户在用户集群节点506上的应用508,获取对应权限策略的信息的权限令牌;将所述权限令牌下发给所述用户集群节点506上的应用508。

[0075] 所述应用508,可以被配置为获取所述托管侧502下发的权限令牌,使用所述权限令牌访问资源。

[0076] 由于托管侧502上定义了一个或多个应用各自所需权限策略的信息,无需用户进行复杂的权限部署,只要用户授权,托管侧502即可根据所述托管侧上的定义,针对所述用户在用户集群节点506上的应用508,获取对应权限策略的信息,根据获取的权限策略的信息,下发对应权限给所述用户集群节点506上的应用508,使所述用户集群节点506上的应用508使用该权限访问资源,因此,托管侧502从应用维度进行权限的拆分定义,根据定义下发权限给用户集群节点506的应用508,不仅减少了用户操作,而且实现了集群的权限收敛和保护,避免同一节点上的租户共享同一权限产生越权风险。

[0077] 可以理解的是,所述用户集群节点506可以是用户集群侧504中的任一个或多个用户集群节点,所述应用508可以是用户集群节点506中的任一个或多个应用。

[0078] 图6示出了根据本说明书一个实施例提供的一种计算设备600的结构框图。该计算设备600的部件包括但不限于存储器610和处理器620。处理器620与存储器610通过总线630相连接,数据库650用于保存数据。

[0079] 计算设备600还包括接入设备640,接入设备640使得计算设备600能够经由一个或多个网络660通信。这些网络的示例包括公用交换电话网(PSTN)、局域网(LAN)、广域网(WAN)、个域网(PAN)或诸如因特网的通信网络的组合。接入设备640可以包括有线或无线的任何类型的网络接口(例如,网络接口卡(NIC))中的一个或多个,诸如IEEE802.11无线局域网(WLAN)无线接口、全球微波互联接入(Wi-MAX)接口、以太网接口、通用串行总线(USB)接口、蜂窝网络接口、蓝牙接口、近场通信(NFC)接口,等等。

[0080] 在本说明书的一个实施例中,计算设备600的上述部件以及图6中未示出的其他部件也可以彼此相连接,例如通过总线。应当理解,图6所示的计算设备结构框图仅仅是出于示例的目的,而不是对本说明书范围的限制。本领域技术人员可以根据需要,增添或替换其他部件。

[0081] 计算设备600可以是任何类型的静止或移动计算设备,包括移动计算机或移动计算设备(例如,平板计算机、个人数字助理、膝上型计算机、笔记本计算机、上网本等)、移动电话(例如,智能手机)、可佩戴的计算设备(例如,智能手表、智能眼镜等)或其他类型的移动设备,或者诸如台式计算机或PC的静止计算设备。计算设备600还可以是移动式或静止式的服务器。

[0082] 其中,处理器620用于执行如下计算机可执行指令:

[0083] 在用户授权下,根据托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;所述托管侧上定义了一个或多个应用各自所需权限策略的信息;

[0084] 将所述权限令牌下发给所述用户集群节点上的应用。

[0085] 上述为本实施例的一种计算设备的示意性方案。需要说明的是,该计算设备的技术方案与上述的设置集群权限的方法的技术方案属于同一构思,计算设备的技术方案未详细描述的细节内容,均可以参见上述设置集群权限的方法的技术方案的描述。

[0086] 本说明书一实施例还提供一种计算机可读存储介质,其存储有计算机指令,该指令被处理器执行时以用于:

[0087] 在用户授权下,根据托管侧上的定义,针对所述用户在用户集群节点上的应用,获取对应权限策略的信息的权限令牌;所述托管侧上定义了一个或多个应用各自所需权限策略的信息;

[0088] 将所述权限令牌下发给所述用户集群节点上的应用。

[0089] 上述为本实施例的一种计算机可读存储介质的示意性方案。需要说明的是,该存储介质的技术方案与上述的设置集群权限的方法的技术方案属于同一构思,存储介质的技术方案未详细描述的细节内容,均可以参见上述设置集群权限的方法的技术方案的描述。

[0090] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0091] 所述计算机指令包括计算机程序代码,所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括:能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、电载波信号、电信信号以及软件分发介质等。需要说明的是,所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减,例如在某些司法管辖区,根据立法和专利实践,计算机可读介质不包括电载波信号和电信信号。

[0092] 需要说明的是,对于前述的各方法实施例,为了简便描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本说明书实施例并不受所描述的动作顺序的限制,因为依据本说明书实施例,某些步骤可以采用其它顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定都是本说明书实施例所必须的。

[0093] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其它实施例的相关描述。

[0094] 以上公开的本说明书优选实施例只是用于帮助阐述本说明书。可选实施例并没有详尽叙述所有的细节,也不限制该发明仅为所述的具体实施方式。显然,根据本说明书实施例的内容,可作很多的修改和变化。本说明书选取并具体描述这些实施例,是为了更好地解释本说明书实施例的原理和实际应用,从而使所属技术领域技术人员能很好地理解和利用本说明书。本说明书仅受权利要求书及其全部范围和等效物的限制。

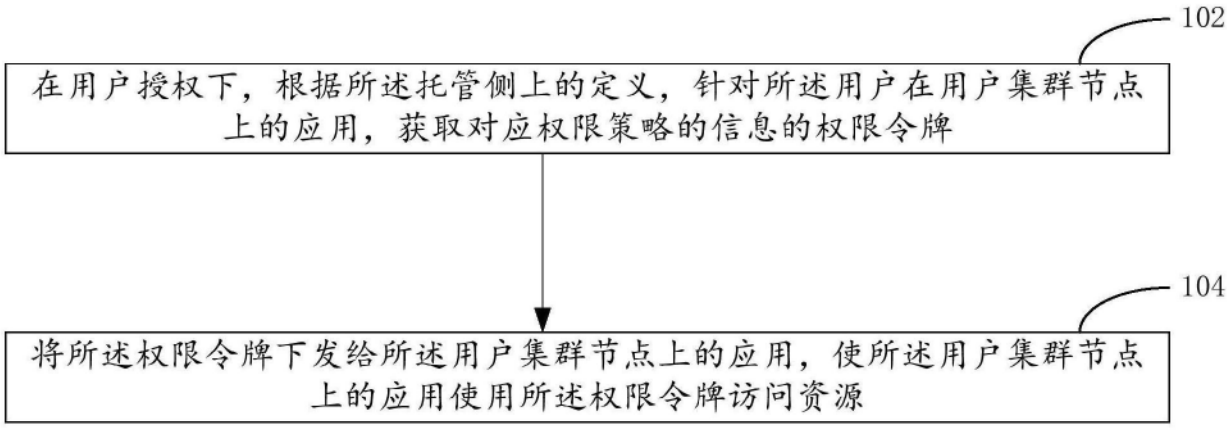

102
在用户授权下，根据所述托管侧上的定义，针对所述用户在用户集群节点上的应用，获取对应权限策略的信息的权限令牌
104
将所述权限令牌下发给所述用户集群节点上的应用，使所述用户集群节点上的应用使用所述权限令牌访问资源

图1

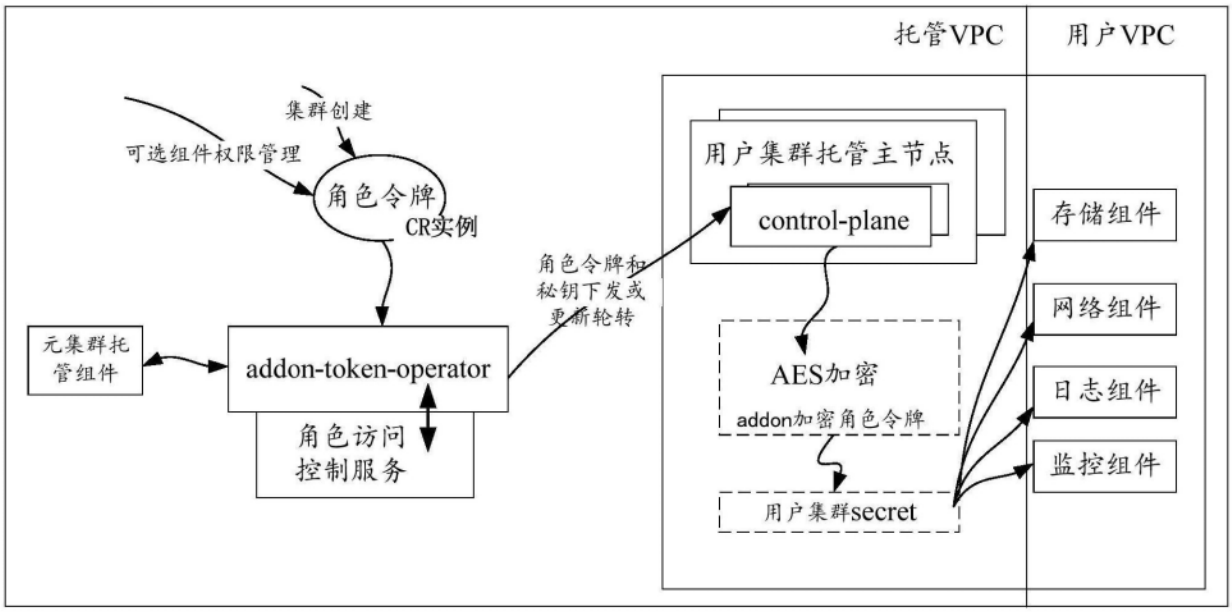

托管VPC
用户VPC
集群创建
可选组件权限管理
角色令牌
CR实例
元集群托管组件
addon-token-operator
角色访问控制服务
角色令牌和秘钥下发或更新轮转
用户集群托管主节点
control-plane
AES加密
addon加密角色令牌
用户集群secret
存储组件
网络组件
日志组件
监控组件

图2

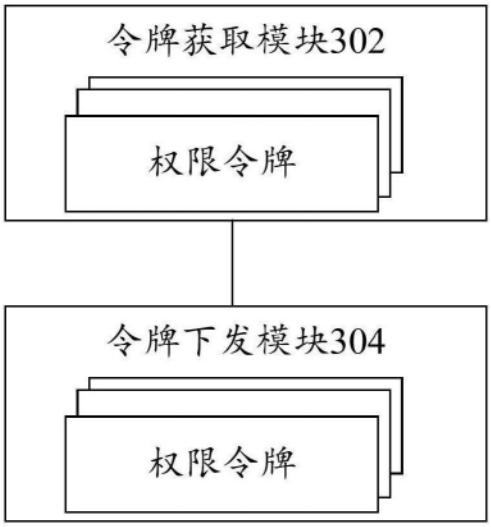


图3

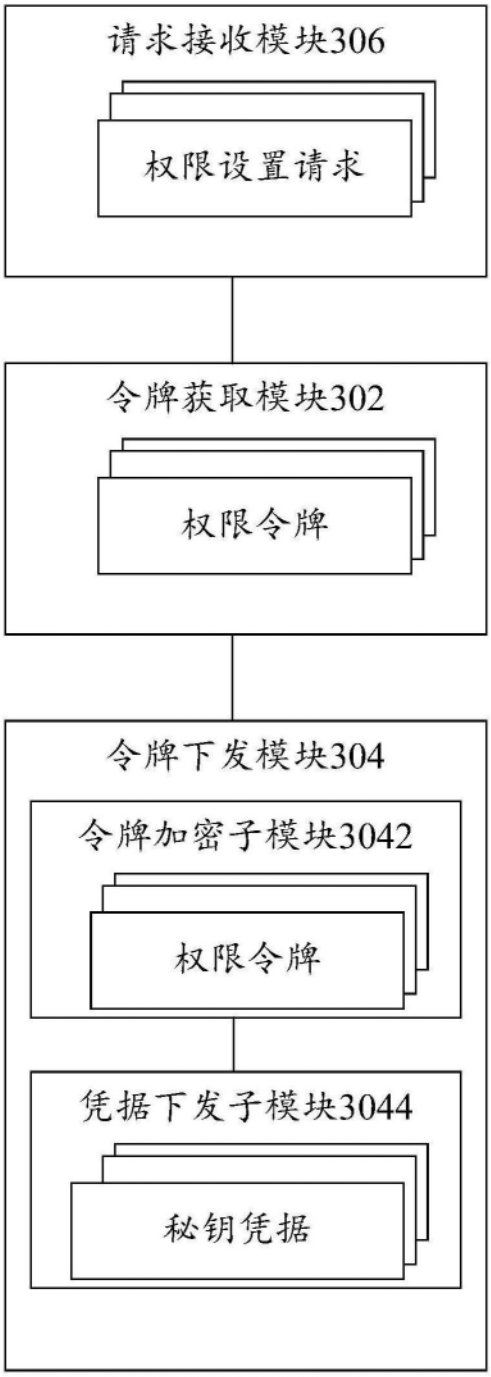

请求接收模块306
权限设置请求
令牌获取模块302
权限令牌
令牌下发模块304
令牌加密子模块3042
权限令牌
凭据下发子模块3044
秘钥凭据

图4

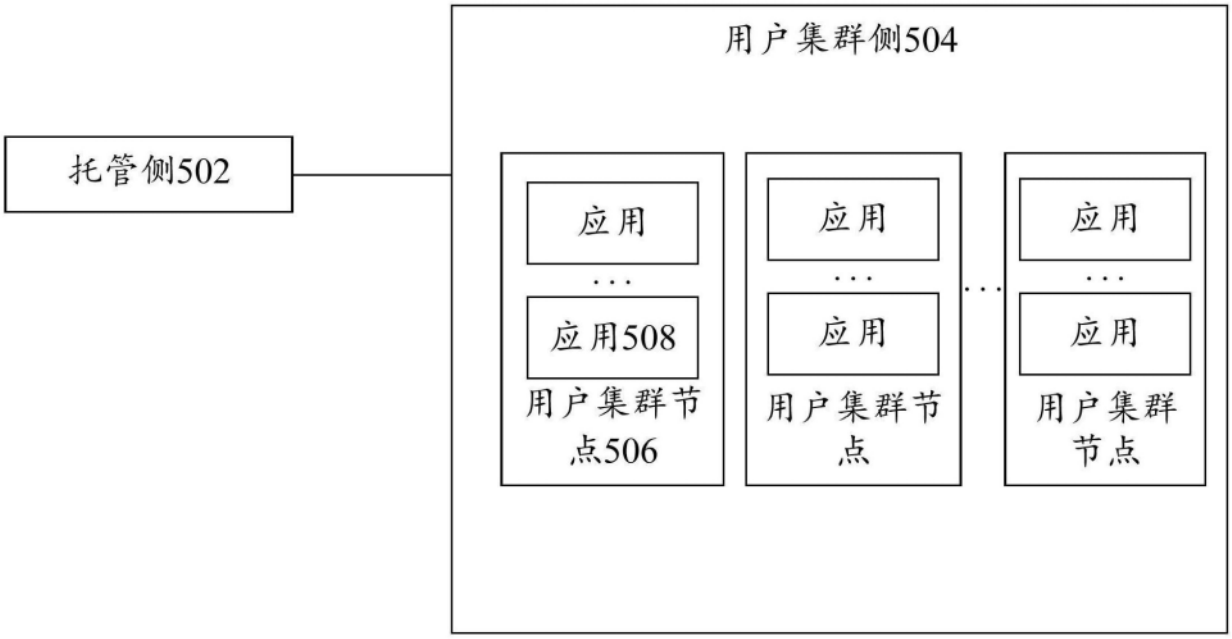

用户集群侧504
托管侧502
应用
应用
应用508
用户集群节点506
应用
应用
用户集群节点
应用
应用
用户集群节点

图5

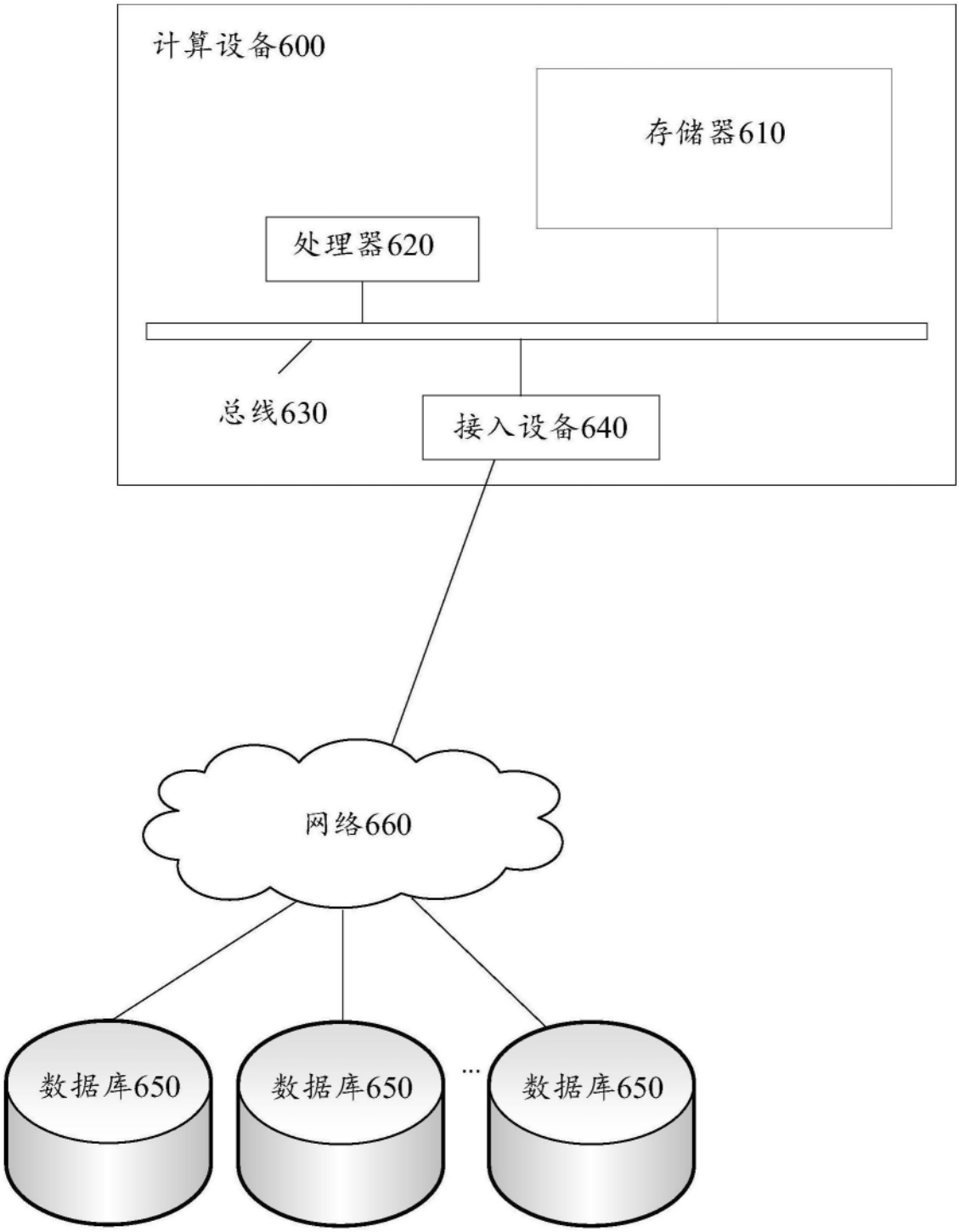

计算设备600
存储器610
处理器620
总线630
接入设备640
网络660
数据库650
数据库650
...
数据库650

图6