(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116848528 A
(43)申请公布日 2023.10.03

(21)申请号 202280015223.8
(22)申请日 2022.02.08
(30)优先权数据
17/177,159 2021.02.16 US
(85)PCT国际申请进入国家阶段日
2023.08.16
(86)PCT国际申请的申请数据
PCT/US2022/015608 2022.02.08
(87)PCT国际申请的公布数据
WO2022/177776 EN 2022.08.25
(71)申请人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 O·S·派克祖尔 H·A·弗斯凯特 R·G·克拉克
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 冯薇
(51)Int.Cl.
*G06F 21/62*(2006.01)

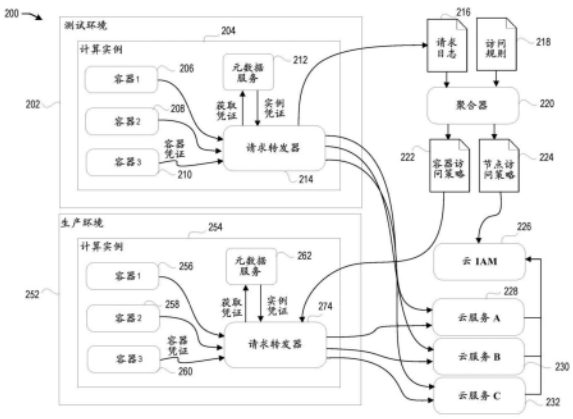
权利要求书3页 说明书31页 附图12页

(54)发明名称

用于自动配置用于容器应用的最小云服务访问权限的技术

(57)摘要

一种计算机系统可以接收对于访问一个或多个云服务(228、230、232)的一个或多个请求，并且可以将上述一个或多个请求存储在请求日志(216)中。计算机系统接收适用于云服务访问权限的一个或多个访问规则(218)。计算机系统聚合请求日志的上述一个或多个请求以确定针对容器(206、208、210)的访问要求，该容器被配置为存储一个或多个应用。计算机系统生成并存储定义容器和上述一个或多个云服务的访问的容器访问策略(222)，该容器访问策略至少部分地基于所聚合的一个或多个请求以及一个或多个访问规则。计算机系统将容器访问策略(222)发送到生产环境(252)中的计算实例的请求转发器(274)。




CN 116848528 A

1.一种方法,包括:

接收对于访问一个或多个云服务的一个或多个请求;

将所述一个或多个请求存储在请求日志中;

接收适用于云服务访问权限的一个或多个访问规则;

聚合请求日志的所述一个或多个请求以确定针对容器的访问要求,该容器被配置为存储一个或多个应用;

生成定义容器和所述一个或多个云服务的访问的容器访问策略,该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则;

将容器访问策略存储在存储器中;以及

将容器访问策略发送到生产环境中的计算实例的请求转发器,该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

2.如权利要求1所述的方法,还包括:

生成节点访问策略,该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略;以及

将容器访问策略存储在存储器中。

3.如权利要求2所述的方法,还包括:

授予与指派给所述节点的所述一个或多个容器的组合访问权等同的访问许可。

4.如权利要求2所述的方法,还包括:

将具有多个计算实例的计算实例分区成节点组,节点中的每个节点具有不同的访问权;以及

至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

5.如权利要求2所述的方法,其中节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

6.如权利要求1所述的方法,还包括:

测试云系统的访问要求;

至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障;以及

改变计算实例的许可来修复所述故障。

7.如权利要求1-6中的任一项所述的方法,还包括:

将生产环境中的每个容器类型的请求转发器设置为许可模式,该许可模式授予存储在容器中的所述一个或多个应用对所述一个或多个云服务的访问权;

从请求转发器接收所述一个或多个请求;以及

根据所述一个或多个请求的数量超过阈值要求,将请求转发器切换到限制模式,该限制模式至少部分地基于容器访问策略授予所述一个或多个应用对所述一个或多个云服务的访问权。

8.一种存储指令集的计算机可读介质,所述指令集包括:

一个或多个指令,该一个或多个指令在由计算机系统的一个或多个处理器执行时,使得计算机系统:

接收对于访问一个或多个云服务的一个或多个请求;

将所述一个或多个请求存储在请求日志中；

接收适用于云服务访问权限的一个或多个访问规则；

聚合请求日志的所述一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用；

生成定义容器和所述一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则；

将容器访问策略存储在存储器中；以及

将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

9.如权利要求8所述的计算机可读介质，其中所述一个或多个指令还使得计算机系统：

生成节点访问策略，该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略；以及

将容器访问策略存储在存储器中。

10.如权利要求9所述的计算机可读介质，其中所述一个或多个指令还使得计算机系统：

授予与指派给所述节点的所述一个或多个容器的组合访问权等同的访问许可。

11.如权利要求9所述的计算机可读介质，其中所述一个或多个指令还使得计算机系统：

将具有多个计算实例的计算实例分区成节点组，节点中的每个节点具有不同的访问权；以及

至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

12.如权利要求9所述的计算机可读介质，其中节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

13.如权利要求8-12中的任一项所述的计算机可读介质，其中所述一个或多个指令还使得计算机系统：

测试云系统的访问要求；

至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障；以及

改变计算实例的许可来修复所述故障。

14.如权利要求8-12中的任一项所述的计算机可读介质，其中所述一个或多个指令还使得计算机系统：

将生产环境中的每个容器类型的请求转发器设置为许可模式，该许可模式授予存储在容器中的所述一个或多个应用对所述一个或多个云服务的访问权；

从请求转发器接收所述一个或多个请求；以及

根据所述一个或多个请求的数量超过阈值要求，将请求转发器切换到限制模式，该限制模式至少部分地基于容器访问策略授予所述一个或多个应用对所述一个或多个云服务的访问权。

15.一种计算机系统，包括：

一个或多个存储器；以及

一个或多个处理器，通信地耦合到所述一个或多个存储器，被配置为执行包括以下的操作：

接收对于访问一个或多个云服务的一个或多个请求；

将所述一个或多个请求存储在请求日志中；

接收适用于云服务访问权限的一个或多个访问规则；

聚合请求日志的所述一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用；

生成定义容器和所述一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则；

将容器访问策略存储在存储器中；以及

将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

16.如权利要求15所述的计算机系统，其中所述一个或多个处理器还被配置为执行包括以下的操作：

生成节点访问策略，该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略；以及

将容器访问策略存储在一个或多个存储器中。

17.如权利要求16所述的计算机系统，其中所述一个或多个处理器还被配置为执行包括以下的操作：

授予与指派给所述节点的所述一个或多个容器的组合访问权等同的访问许可。

18.如权利要求16所述的计算机系统，其中所述一个或多个处理器还被配置为执行包括以下的操作：

将具有多个计算实例的计算实例分区成节点组，节点中的每个节点具有不同的访问权；以及

至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

19.如权利要求16所述的计算机系统，其中节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

20.如权利要求15-19中的任一项所述的计算机系统，其中所述一个或多个处理器还被配置为执行包括以下的操作：

测试云系统的访问要求；

至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障；以及

改变计算实例的许可来修复所述故障。

21.一种包括用于执行根据权利要求1-7中的任一项所述的步骤的部件的装置。

22.一种包括计算机指令的计算机程序产品，所述计算机指令在由处理器执行时，实现根据权利要求1-7中的任一项所述的方法的步骤。

# 用于自动配置用于容器应用的最小云服务访问权限的技术

[0001] 对先前申请的交叉引用

[0002] 本申请是于2021年2月16日提交的标题为“TECHNIQUES FOR AUTOMATICALLY CONFIGURING MINIMAL CLOUD SERVICE ACCESS RIGHTS FOR CONTAINER APPLICATIONS”的美国非临时申请17/177,159的PCT申请,并根据35U.S.C.119(e)声明其权益和优先权,其内容出于所有目的通过引用全文并入本文。

## 背景技术

[0003] 基础设施和平台即服务云提供商支持集成认证。特别地,托管在云提供商的基础设施上的客户工作负载可以使用它们被托管在其上的计算实例的身份进行认证。这个模型可以允许客户构建安全的工作负载。如果没有它,将要求客户在每次创建实例时用凭证引导其实例或在实例上运行的应用,并确保此类凭证被云服务识别出。

[0004] 客户访问规则可以限制计算实例或节点对某些服务或客户数据的访问,以防止所有容器对云基础设施具有相同级别的访问。为云服务建立连接性的现有系统常常可能使用过于宽松的许可规则,其中所有容器都对云基础设施具有相同级别的访问权。

## 发明内容

[0005] 本公开的某些实施例可以提供用于管理对基于云的服务的访问的方法、系统和计算机可读存储介质。本公开描述了在容器和云服务之间调解请求以便提供足够级别的访问控制的系统和技术。所公开的技术组合了云协调器的内部认证以识别容器调用者和云服务认证以认证对云服务进行的调用。在一些示例中,系统上运行的各个容器可能无法直接访问元数据服务或实例凭证。代替地,容器可以通过请求转发器组件来发送请求。该组件建立容器身份并核实特定容器是否有权与目标服务(例如,云服务)通信。请求转发器组件使用实例凭证来认证对目标服务的调用。可以以防止容器访问元数据服务的方式来配置计算实例。该技术有效地防止容器中的过程使用计算实例凭证。计算实例是虚拟处理器、云中的计算节点,或者甚至是裸机处理器(例如,物理硬件计算机)的示例。

[0006] 当容器被初始化时,容器编排器可以向其提供凭证。容器编排器除了替换节点、将容器替换为节点等之外,还可以使用凭证来识别容器。这个过程可以采取不同的形式。在一些情况下,该过程将导致凭证被存储在容器的文件系统上。根据本公开的一方面,在容器中执行的过程旨在调用云服务。该过程可以将对云服务的请求定向到请求转发器。该请求可以包括容器凭证。请求转发器可以接收请求并通过将容器凭证发送到容器编排器来确定容器的身份。请求转发器可以查阅系统上存储的一个或多个策略来核实是否允许容器访问目标云服务。请求转发器可以从元数据服务获得实例凭证。请求转发器可以将包括计算实例凭证的请求发送到目标云服务。云服务可以对照一个或多个存储的云策略核实该请求,以核实在容器中运行的实例是否被允许访问所请求的云服务。

[0007] 具体而言,容器可以执行可以请求访问云资源的一个或多个应用。例如,资源可以被用于创建虚拟机、或访问序列或数据对象、或管理密钥管理系统中的密钥、或将数据存储

在数据库中。云基础设施系统可以包括自己的集成访问管理机制。在访问管理系统中，可以向主体授予访问权。虽然在技术上有可能为每个容器创建主体，但该技术将需要包括授予对每个容器的访问权。这种技术难以大规模复制，因为它要求供应凭证并划分这些容器。这个问题只能使用计算节点来解决。计算节点有自己的第一类身份，并且可以授予对这些节点的访问权。因此，这些机器作为主体能够执行这些种类的动作。

[0008] 假设存在需要单独存储的两条数据，所公开的技术允许容器的隔离。例如，一个容器可以存储第一条数据，并且第二容器可以存储第二条数据。理想情况下，容器永远不会托管在同一机器上。以这种方式，如果一个容器中或容器隔离中存在违反或漏洞，那么该漏洞不会提供对其它容器中其它数据的访问。

[0009] 在一些方面，一种方法包括：(例如，从发送者)接收对于访问一个或多个云服务的一个或多个请求；将所述一个或多个请求存储在请求日志中；(例如，从不同发送者或相同发送者)接收适用于云服务访问权限的一个或多个访问规则；聚合请求日志的所述一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用；生成定义容器和所述一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则；将容器访问策略存储在存储器中；以及将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

[0010] 在一些方面，生成节点访问策略，该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略；以及将容器访问策略存储在存储器中。

[0011] 在一些方面，该方法包括授予与指派给所述节点的所述一个或多个容器的组合访问权等同的访问许可。

[0012] 在一些方面，该方法包括将具有多个计算实例的计算实例分区成节点组，节点中的每个节点具有不同的访问权；以及至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

[0013] 在一些方面，节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

[0014] 在一些方面，该方法包括测试云系统的访问要求；至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障；以及改变计算实例的许可来修复所述故障。

[0015] 在一些方面，该方法包括将生产环境中的每个容器类型的请求转发器设置为许可模式，该许可模式授予存储在容器中的所述一个或多个应用对所述一个或多个云服务的访问权；从请求转发器接收所述一个或多个请求；以及根据所述一个或多个请求的数量超过阈值要求，将请求转发器切换到限制模式，该限制模式至少部分地基于容器访问策略授予所述一个或多个应用对所述一个或多个云服务的访问权，将请求转发器切换到限制模式，该限制模式至少部分地基于容器访问策略授予所述一个或多个应用对所述一个或多个云服务的访问权。

[0016] 在一些方面，一种存储用于配置容器应用的云服务访问权限的指令集的非暂态计算机可读介质包括：一个或多个指令，该一个或多个指令在由计算机系统的一个或多个处理器执行时，使得计算机系统：(例如，从发送者)接收对于访问一个或多个云服务的一个或

多个请求;将所述一个或多个请求存储在请求日志中;(例如,从不同发送者或相同发送者)接收适用于云服务访问权限的一个或多个访问规则;聚合请求日志的所述一个或多个请求以确定针对容器的访问要求,该容器被配置为存储一个或多个应用;生成定义容器和所述一个或多个云服务的访问的容器访问策略,该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则;将容器访问策略存储在存储器中;以及将容器访问策略发送到生产环境中的计算实例的请求转发器,该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

[0017] 在一些方面,一个或多个指令还使得计算机系统:生成节点访问策略,该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略;以及将容器访问策略存储在存储器中。

[0018] 在一些方面,一个或多个指令还使得计算机系统:授予与指派给所述节点的所述一个或多个容器的组合访问权等同的访问许可。

[0019] 在一些方面,一个或多个指令还使得计算机系统:将具有多个计算实例的计算实例分区成节点组,节点中的每个节点具有不同的访问权;以及至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

[0020] 在一些方面,节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

[0021] 在一些方面,一个或多个指令还使得计算机系统:测试云系统的访问要求;至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障;以及改变计算实例的许可来修复所述故障。

[0022] 在一些方面,一个或多个指令还使得计算机系统:将生产环境中的每个容器类型的请求转发器设置为许可模式,该许可模式授予存储在容器中的所述一个或多个应用对所述一个或多个云服务的访问权;从请求转发器接收所述一个或多个请求;以及根据所述一个或多个请求的数量超过阈值要求,将请求转发器切换到限制模式,该限制模式至少部分地基于容器访问策略授予所述一个或多个应用对所述一个或多个云服务的访问权。

[0023] 在一些方面,一种计算机系统包括:一个或多个存储器;以及一个或多个处理器,通信地耦合到一个或多个存储器,被配置为执行用于配置用于容器应用的云服务访问权的操作,该操作包括:(例如,从发送者)接收对于访问一个或多个云服务的一个或多个请求;将所述一个或多个请求存储在请求日志中;(例如,从不同发送者或相同发送者)接收适用于云服务访问权限的一个或多个访问规则;聚合请求日志的所述一个或多个请求以确定针对容器的访问要求,该容器被配置为存储一个或多个应用;生成定义容器和所述一个或多个云服务的访问的容器访问策略,该容器访问策略至少部分地基于所聚合的一个或多个请求以及所述一个或多个访问规则;将容器访问策略存储在存储器中;以及将容器访问策略发送到生产环境中的计算实例的请求转发器,该请求转发器访问容器访问策略以授予容器对所述一个或多个云服务的访问权限。

[0024] 在一些方面,一个或多个处理器还被配置为执行包括以下的操作:生成节点访问策略,该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略;以及将容器访问策略存储在存储器中。

[0025] 在一些方面,一个或多个处理器还被配置为执行包括以下的操作:授予与指派给

所述节点的所述一个或多个容器的组合访问权等同的访问许可。

[0026] 在一些方面，一个或多个处理器还被配置为执行包括以下的操作：将具有多个计算实例的计算实例分区成节点组，节点中的每个节点具有不同的访问权；以及至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

[0027] 在一些方面，节点访问权是预先确定的并且每个节点内的容器访问权是动态配置的。

[0028] 在一些方面，一个或多个处理器还被配置为执行包括以下的操作：测试云系统的访问要求；至少部分地基于请求日志中的条目来检测特定应用访问所述一个或多个云服务的故障；以及改变计算实例的许可来修复所述故障。

[0029] 参考本说明书的其余部分(包括附图和权利要求)将实现所公开的实施例的其它特征和优点。下面关于附图来详细描述本公开的进一步特征和优点以及各种示例的结构和操作。在附图中，相似的附图标记可以指示完全相同或功能相似的元件。

[0030] 下面详细描述这些和其它实施例。例如，其它实施例针对与本文描述的方法相关联的系统、设备和计算机可读介质。

[0031] 参考以下具体实施方式和附图可以获得对于本公开的实施例的性质和优点的更好的理解。

## 附图说明

[0032] 图1图示了用于示例云网络体系架构的逻辑构造(logical construct)。

[0033] 图2图示了第二示例云网络体系架构的逻辑构造。

[0034] 图3是与用于自动配置用于容器应用的最小云服务访问权限的技术相关联的示例过程的流程图。

[0035] 图4图示了示出所公开的系统的被允许布置的示例布置图。

[0036] 图5图示了示出所公开的系统的被禁止布置的示例布置图。

[0037] 图6图示了被允许分组的示例图。

[0038] 图7是基于使用请求转发器作为服务的托管节点对云服务进行选择性容器访问的技术的简化流程图。

[0039] 图8是图示根据至少一个实施例的用于将云基础设施实现为服务系统的一种模式的框图。

[0040] 图9是图示根据至少一个实施例的用于将云基础设施实现为服务系统的另一种模式的框图。

[0041] 图10是图示根据至少一个实施例的用于将云基础设施实现为服务系统的另一种模式的框图。

[0042] 图11是图示根据至少一个实施例的用于将云基础设施实现为服务系统的另一种模式的框图。

[0043] 图12是图示根据至少一个实施例的示例计算机系统的框图。

## 具体实施方式

[0044] I.介绍

[0045] 现代计算框架提取机器的概念。机器可以被认为只是处理单元。现代应用越来越多地使用容器来构建,容器是与其依赖性和配置一起打包的微服务。容器管理/聚类服务是用于大规模部署和管理这些容器的软件。随着应用发展到跨多个服务器部署的多个容器,操作它们变得更加复杂。为了管理这种复杂性,容器管理/聚类服务提供了控制这些容器将如何运行以及在哪里运行的开源应用编程接口(API)。容器管理/聚类服务编排虚拟机的集群,并基于其可用的计算资源和每个容器的资源要求来调度容器在这些虚拟机上运行。容器被分组为群聚(pod)、用于容器管理/聚类服务的基本操作单元,并且这些群聚扩展到期望的状态。容器管理/聚类服务还自动管理服务发现、结合负载平衡、跟踪资源分配、基于计算利用率进行扩展、检查各个资源的健康状况、并且使得应用能够通过自动重启或复制容器来进行自我修复。

[0046] 网络编排器可以被用于为每个容器指派实例的数量。基于每个机器的繁忙程度,可以添加或移除容器以创建高工作负载密度,从而节省成本。可以针对高输入/输出(I/O)带宽来定制容器,以提高性能。

[0047] 云提供商可以为每个计算节点发布身份。以这种方式,节点就可以拥有自己的身份。存在获得该身份的标准机制。因此,如果容器正在节点上运行过程,那么系统可以调用例如特定的IP地址。这可以返回与该特定实例相关联的特定身份临时凭证。该凭证将具有多个参数,诸如特定机器是什么以及该机器所属的机器组。

[0048] 在示例中,客户可以使用来自云供应商的两种服务(例如,计算和对象存储)。客户的应用在计算实例上运行,并从对象存储桶中检索数据和存储数据。在没有集成认证机制的情况下,客户将被迫以与传统云前(pre-cloud)环境中相同的方式进行操作。也就是说,客户将需要:在其账户下创建用户;授予这些用户对对象存储的访问;并向应用提供用户的凭证。最后一步可能特别有问题。在应用可以变得可操作之前,必须将凭证放置在系统上。如果系统重启,或者添加新机器,那么必须重复这个步骤。它还必须由有权访问凭证的工程师手动执行,这增加了凭证暴露风险。为了使过程不那么麻烦,客户可以决定将凭证持久存储在机器本身上,或者多个机器可以访问它的位置。这可能进一步增加凭证泄露的风险。除了安全问题之外,此类过程无法针对复杂的大型工作负载进行扩展。对同步动作的要求(例如,凭证的创建、凭证的分发)给高度自动化的云工作负载带来了严重的问题。而且,每当客户想要改变凭证时,都必须重复该过程。

[0049] 现代云供应商提供高度集成的身份访问管理(IAM)解决方案。IAM是策略和技术的框架,用于确保企业中的合适人员能够适当地访问技术资源。IAM系统属于IT安全和数据管理的总体范畴。身份和访问管理系统不仅对将使用IT资源的个人进行识别、认证和授权,而且还对员工需要访问的硬件和应用进行识别、验证和授权。近年来,随着监管合规性要求变得越来越严格和复杂,身份和访问管理解决方案变得更加普遍和重要。

[0050] 它解决了确保跨日益异构的技术环境对资源的适当访问并满足日益严格的合规性要求的需要。计算实例以及专用于主机客户工作负载的其它资源(诸如无服务器功能)具有他们自己的由客户的账户下的云IAM识别的身份。客户可以直接将这些组件视为一类主体,将它们分组并授予它们所需的访问权。计算机器、功能和其它组件被自动设置有其托管过程可访问的短期凭证。应用检索这些凭证并使用它们来访问云资源。

[0051] 当客户打算在单个计算实例上托管多个异构过程时,可能出现问题。当计算节点

被用于运行由编排框架管理的容器(诸如在商用容器管理/聚类服务中使用的容器)时,这种情况是常见的。问题的核心是身份的最小粒度是单个机器。仅仅因为容器托管在同一计算机上,所以并不意味着它们旨在具有对云资源的相同访问权。但是,由于单个机器是最细粒度的身份,因此容器全都需要共享它。

[0052] 考虑以下示例。客户使用来自云供应商的两种服务:计算和对象存储。客户的应用在计算实例上运行,并从对象存储装置内的桶执行存储和检索数据操作。在没有集成认证机制的情况下,客户将被迫以与传统云前环境中相同的方式进行操作。云前系统将:(1)在其账户中创建用户;(2)授予用户对对象存储的访问权;以及(3)向应用提供用户的凭证。

[0053] 这最后一步是特别有问题的。在应用可以变得可操作之前,必须将凭证放置在系统上。如果系统重启,或者添加新机器,那么必须重复这个步骤。它还必须由有权访问凭证的工程师手动执行,这增加了凭证暴露风险。为了节省时间,客户可以决定将凭证持久存储在机器本身上,或者存储在多个机器可以访问它的位置,这进一步增加了凭证泄露的风险。

[0054] 除了安全问题之外,这个过程不能扩展以适应大的或复杂的工作负载。同步动作的要求(例如,凭证的创建或凭证的分发)可能给高度自动化的云工作负载带来问题。另外,每次客户想要改变凭证时,都必须重复该过程。

[0055] 专用于托管客户工作负载的计算实例和其它资源(诸如无服务器功能)具有由客户账户下的云IAM识别出的其自己的身份。客户可以直接将这些组件视为第一类主体,将它们分组并授予它们所需的访问权。计算实例、功能和其它组件被自动设置有短期凭证,能够访问它们托管的过程。然后,应用可以检索这些凭证并使用它们来访问云资源。

[0056] 在典型的实施方式中,计算实例包括本地可访问的网络服务,通常被称为元数据服务。这个服务允许系统上的本地工作负载访问由云供应商传播的各种信息,诸如表示计算实例的主体的凭证。元数据服务只能由这个特定计算机上运行的过程访问。过程向元数据服务发出请求,接收凭证,并使用它来访问其它云服务。其它服务使用云供应商的IAM服务来核实表示实例的主体是否有权执行所请求的操作。

[0057] 本公开的某些实施例可以提供用于管理对基于云的服务的访问的方法、系统和计算机可读介质。本文描述了两种类型的访问控制。首先,容器可以访问特定的云服务。这种访问可以基于称为服务的策略来确定容器是否具有许可。此外,第二访问控制是由计算实例对云服务进行的。因此,在容器上运行的过程需要该容器的许可才能访问云服务,但它也需要该容器作为其一部分的计算实例能访问该云服务的许可。

[0058] 本公开描述了在容器和云服务之间调解请求以便提供足够级别的访问控制的系统和技术。所公开的技术组合云编排器的内部认证以识别容器调用者和云服务认证以认证对云服务进行的调用。在一些示例中,系统上运行的各个容器可能无法直接访问元数据服务或实例凭证。代替地,容器可以通过请求转发器组件来发送请求。该组件建立容器身份并核实特定容器是否有权与目标服务进行通信。请求转发器组件使用实例凭证来认证对目标服务的调用。可以以防止容器访问元数据服务的方式配置计算实例。该技术有效地防止容器中的过程使用计算实例凭证。容器通过它在其上运行的机器获得对云服务的访问权,因为由于这些技术,容器无法被给予直接访问权。

[0059] 当容器被初始化时,容器编排器可以向其提供凭证。这个过程可以采取不同的形式,但最典型的将是导致凭证存储在容器的文件系统上的过程。根据本公开的一方面,在容

器中执行的过程旨在对云服务进行调用。该过程可以将对云服务的请求定向到请求转发器。该请求可以包括容器凭证。请求转发器可以接收请求并通过将容器凭证发送到容器编排器来确定容器的身份。请求转发器可以查阅系统上存储的一个或多个策略来核实是否允许容器访问目标云服务。请求转发器可以从元数据服务获得实例凭证。请求转发器可以将包括计算实例凭证的请求发送到目标云服务。云服务可以对照云策略来核实请求,以核实云服务是否允许实例执行给定操作。

[0060] 出于本公开的目的,实例(例如,计算实例)是在客户飞地(可公开获得)或服务飞地中运行的托管的服务器。如果该实例直接访问它在其上运行的硬件,那么可以将其视为裸机实例。如果实例和操作系统之间存在管理程序,那么可以将其视为虚拟实例。管理程序是一款软件,使用户能够同时创建和运行一个或多个虚拟机。管理程序也被称为虚拟机监视器(VMM)。管理程序提供的关键功能之一是隔离,这意味着访客无法影响主机或任何其它访客的操作,即使它崩溃了也是如此。管理程序可以是两种类型:类型1和类型2。类型1管理程序可以被称为本机或裸机管理程序,这种类型的管理程序直接在物理硬件之上运行。每个虚拟操作系统都在管理程序之上运行。裸机管理程序的示例可以是Oracle VM服务器、Vmware ESX/ESXi和Microsoft Hyper-V。类型2管理程序也可以被称为托管的管理程序。这种类型的管理程序作为软件应用安装在现有主机操作系统(OS)上。托管的管理程序的示例可以是Oracle VirtualBox、Microsoft Virtual PC、Vmware Server和Workstation。

[0061] 出于本公开的目的,容器是多租户容器数据库(CDB)中的模式、对象和相关结构的集合,其在逻辑上对于应用表现为单独的数据库。在CDB内,每个容器具有唯一的ID和名称。根和每个可插拔数据库(PDB)都被视为容器。PDB隔离数据和操作,因此,从用户或应用的角度来看,每个PDB看起来就像是传统的非CDB。

[0062] 图1图示了示例云网络体系架构100的逻辑构造。云网络体系架构可以包括一个或多个容器(例如,容器1 104、容器2 106和容器3 108)。在实施方式中,计算实例102可以包括本地可访问的网络服务,通常被称为元数据服务110。这个元数据服务110允许系统上的本地工作负载访问由云供应商传播的各种信息,包括表示计算实例102的主体的凭证。元数据服务110只能由在这个特定机器上运行的过程访问。过程可以联系元数据服务110以获得凭证并使用该凭证来访问其它云服务(例如,云服务A 112、云服务B 114或云服务C 116)。这些服务使用云供应商的IAM服务来核实表示实例的主体是否有权执行所请求的云操作。

[0063] 当客户打算在单个计算实例102上托管多个异构过程时,可能出现问题。当计算节点被用于运行由编排框架(例如,诸如容器管理/聚类服务等)管理的容器时,这可以是常见的。身份的最小粒度可以是单个机器。以前的技术可以只是将对一个或多个云服务的访问权指派给机器,而不一定指派给位于同一机器上的不同容器。仅仅因为容器托管在同一个计算机上,并不意味着它们具有对云资源的相同访问权。但是,由于单个机器是最细粒度的身份,因此它们都需要共享它。

[0064] 例如,如图1中所描绘的。容器1 104仅与云服务A 112通信。容器2 106与云服务A 112和云服务B 114通信。容器3 108与云服务C 116通信。在一种布置中,客户可以接受节点访问非预期云服务的风险。在这种布置中,计算节点被授予它们托管的任何容器可能需要的所有访问权,并且所有容器都接收访问节点凭证。这种方法实际上为了方便而牺牲了安全性。例如,在图1中所示的布置中,可以向计算实例102提供对云服务A 112、云服务B 114

和云服务C 116的访问。作为示例，可以禁止在容器1 104上运行的过程访问云服务C 116，可能是因为该服务属于竞争者实体。如果访问仅由计算实例控制，那么在容器1 104中运行的过程可能无意中获得对云服务C 116的访问，因为计算实例102为所有容器提供了访问所示的所有三个云服务的许可。

[0065] 在第二布置中，客户可以选择性地禁用元数据服务110对一些容器的访问。在这种布置中，不需要访问任何云资源的容器可以被禁止访问元数据服务110。这实现起来可以是简单的，但却是一种全有或全无的方法。这种布置对于具有不同访问需求的容器没有帮助。因此，使用防火墙规则或网络策略，用户可以决定仅允许这个容器访问整个元数据服务网络。此外，只有当该容器需要访问任何服务时，这才有效。因此，至少可以通过破坏容器获取凭证的路径来隔离不需要访问任何云服务的组件。

[0066] 在第三布置中，客户可以将容器分发到单独的机器。在这种布置中，客户可以创建一组计算节点并授予每组计算节点不同的访问权。客户随后可以配置容器编排器以将容器放置在具有与每个容器的需求匹配的访问权的节点上。节点可以被放入不同的组中。这些组为这些节点指派不同的访问权，然后在容器编排器中配置调度器以仅将特定容器指派给特定节点。这种方法在有限的情况下有效，但是，需要执行的次数越多，一组机器就会变得越分散，用户在机器上的损失就越大，总体工作负载密度就会受到影响。这种布置为容器提供了对云资源的定制访问。但是，这种布置可以更加复杂，并要求到节点以及节点到容器的细心的映射策略和规划，并且可能导致资源利用率低下。

[0067] 客户还可以使用这些选项的任何组合，从而增加访问管理的复杂性。上面提到的解决方案的缺点随着工作负载的规模和复杂性而增加，特别是不同容器的数量及其云服务访问需求。接受风险将导致对各个容器的访问范围越来越大，即使它们可能不需要它。分发大量容器可以导致所需的不同机器数量不断增加，并且会导致在每个节点上找到所需的正确访问权集合变得更加复杂。在极端情况下，客户可以决定为每种容器类型建立机器池，这将提供完美的访问限制，但会破坏使用容器管理服务的初衷，并且由于过程密度低而大大增加成本。

[0068] 一些提供商(诸如商业上可用的容器管理/聚类服务)在其管理的服务中利用其自己类型的主体来提供对容器(例如，群聚)的支持。因此，可以直接向容器本身授予访问权，而不是依赖元数据服务110。虽然这可以是有用的解决方案，但它仅限于给定的供应商和供应商的特定服务。想要管理自己的集群或想要使用不同框架的客户将无法实现这种解决方案。

[0069] II.云网络体系架构逻辑构造

[0070] 当云服务添加和移除容器或添加规则时，可以要求多种类型的实例。多种类型的实例可以向不同的实例授予不同级别的访问权。这个过程可能难以大规模执行，并且比简单的手动网络映射更为复杂。

[0071] 机器到云服务的访问可以由云IAM管理。所公开的技术可以确定两种策略。一种策略管理节点内的容器访问。第二种策略管理云内的节点访问。

[0072] 潜在的IAM解决方案可以建立可以识别对云服务进行调用的组件的请求转发器。组件可以使用自己的身份来调用云提供商服务。这种请求转发器可以访问一种或多种策略，这些策略可以确定配置以及哪些服务可以用哪些API以及用哪些凭证进行调用。

[0073] 这种系统可能难以大规模地实现或者难以用现代快节奏的软件交付范例来实现。新的或更新后的组件可以每天都被交付,每次都有与云服务通信的不同需求。这使得对各个组件策略的任何手动管理变得不切实际并且容易出错。进而,这可能导致过于宽松的许可策略,从而允许所有组件访问不需要的服务。计算节点本身的访问也必须受到管理,以确保它与节点上运行的所有容器的组合许可之间不存在差异。

[0074] 第二个问题可以是管理计算节点访问。上述讨论假设计算节点具有足够的访问权来处置来自位于该节点上的各种容器的所有请求。但是,管理计算节点访问也可以非常困难,尤其是在快速变化的环境中。原则上,计算节点必须具有在该节点上托管的所有容器的所有访问节点的联合的访问权。随着节点上的容器被添加、删除或重新定位,节点的访问要求发生改变。这通常会导致向计算节点授予过多的权限,以确保所有容器都具有所需的访问权。最佳安全实践要求将节点访问权授予尽可能小的集合。现在被正确地理解为与容器的访问权的管理不同的节点访问权的管理成为主要的运营障碍。

[0075] 本公开描述了一种自动推断针对容器和计算节点两者的访问需求的最小所需集合的系统。这些需求进一步被表示为提供给请求转发器和云IAM的策略。它还将组件的生命周期与策略本身的生命周期结合起来。另外,系统允许指定准则或访问规则,以控制如何将访问权指派给节点。因此,通过聚合请求日志的请求,系统可以确定访问需求的最小所需集合,这被用于确定容器的访问需求(例如,最小集合)。换句话说,访问要求可以等于容器(和/或容器的计算节点)的最小所需集合。

[0076] 利用这种系统,用户可以快速交付新组件并修改现有组件,同时确保授予云服务的访问权保持最小。在没有用于生成狭窄且特定策略的自动化机制的情况下,用户可能倾向于授予对容器(甚至更可能是计算实例)的过于宽松的许可访问权。可替代地,当期望高级别安全性时,手动预配置单个集中式策略可能对特征发布周期的性能产生负面影响。所公开的系统允许开发团队实现高速交付而不牺牲访问控制的高安全性。另外,由于能够指定访问规则,因此系统可以自动将容器划分为节点,自动为容器构建安全隔离边界。

[0077] 图2图示了用于第二云网络体系架构200的逻辑构造。所公开的系统在两个关键阶段中进行操作。在第一阶段,容器接受集成测试。测试环境被设置有请求转发器,该请求转发器被设置为在许可模式下运行。在持续交付和容器化系统中典型的此类测试执行容器的功能并触发对云提供商的调用。对云提供商的请求由请求转发器进行日志记录。然后聚合这个日志以创建特定于特定容器的云服务访问策略,以及托管该容器的计算节点(常常是节点组)的云服务访问策略。可以通过作为系统配置提供的访问规则来微调策略创建。例如,此类访问规则可以阻止一个节点访问两个特定的云服务。然后,策略与容器一起打包到单个部署包中。

[0078] 部署包由以下各项组成:容器、特定于容器的策略和节点策略。体系架构编排系统将节点访问策略224部署到云IAM 226,同时将容器和特定于容器的访问策略222部署到容器集群。然后,集群部署容器并将其策略发送到请求转发器。类似地,当容器被移除时,访问权(即,转发器中的容器访问权以及授予计算节点的策略中不必要的部分)也被移除。

[0079] 第二云网络体系架构200可以包括测试环境202。测试环境202可以包括一个或多个计算实例204。计算实例204可以包括一个或多个容器(例如,容器1 206、容器2 208和容器3 210)。每个容器都可以接收凭证来识别网络上的容器。在各种示例中,容器编排器可以

在创建时向容器提供身份。容器身份可以存储在容器的存储器中。

[0080] 如先前针对图1所讨论的，在计算实例204的容器中执行的过程可以请求云服务(例如，云服务A 228、云服务B 230或云服务C 232)。容器可以将其容器凭证发送到请求转发器214。请求转发器214可以充当容器和云服务之间的代理。请求转发器214负责获得凭证，使得机器上的组件可以使用实例凭证来调用云服务，这允许网络体系架构断开所有这些容器对该凭证的访问。因此，这些容器没有该凭证，并且现在容器必须通过请求转发器214进行所有调用，因为这是获得凭证的唯一方式。请求转发器214可以从容器接收包括容器凭证的请求。请求转发器214可以用控制平面中的容器编排器来核实凭证。请求转发器214可以将容器凭证发送到容器编排器并接收回容器身份。

[0081] 在测试环境202中，请求转发器214可以向元数据服务发送请求。该请求可以包括容器凭证。元数据服务212可以使用容器凭证来获取实例凭证。请求转发器214可以将对云服务的请求从一个或多个容器传输到请求日志216。该请求可以存储在请求日志216中。请求日志216数据可以存储在服务器上。聚合器220可以聚合一个或多个请求并将聚合的列表存储在服务器上。聚合器220还可以接收一个或多个访问规则218。聚合器220可以生成一个或多个容器访问策略222。聚合器220可以生成一个或多个节点访问策略224。

[0082] 生产环境252可以包括计算实例254。计算实例254可以包括一个或多个容器(例如，容器1 256、容器2 258和容器3 260)。每个容器都可以接收凭证来识别网络上的容器。在各种示例中，容器编排器可以在创建时向容器提供身份。容器身份可以存储在用于容器的存储器中。计算实例254可以包括请求转发器274。请求转发器274可以充当容器和云服务之间的代理。请求转发器274负责获得凭证，使得机器上的组件可以用实例凭证来调用云服务，这允许网络体系架构断开所有这些容器对该凭证的访问。因此，这些容器没有该凭证，并且现在容器必须通过请求转发器274进行所有调用，因为这是获得凭证的唯一方式。请求转发器274可以从容器接收包括容器凭证的请求。请求转发器274可以利用控制平面中的容器编排器来核实凭证。请求转发器274可以将容器凭证发送到容器编排器并接收回容器身份。

[0083] 计算实例254可以包括元数据服务262。请求转发器274可以向元数据服务262发送请求。该请求可以包括容器凭证。元数据服务262可以使用容器凭证来获得实例凭证。请求转发器274可以访问容器访问策略222。在各种实施例中，容器访问策略222可以存储在计算实例254上。在生产环境中，请求转发器274可以接收一个或多个容器访问策略222。容器访问策略222可以被用于确定容器被允许使用哪些云服务(如果有的话)。请求转发器274可以使用容器访问策略222来确定容器的许可。请求转发器274可以从元数据服务器222请求实例凭证。元数据服务器262可以基于容器的容器访问策略222来发送实例凭证信息。请求转发器274可以将请求发送到云服务(例如，云服务A 228、云服务B 230或云服务C232)。实例凭证可以附接到发送到云服务的请求。

[0084] 图3是与用于自动配置容器应用的最小云服务访问权限的技术相关联的示例过程300的流程图。在302处，过程300可以通过将新的或修改后的容器添加到云服务器基础设施来开始。

[0085] 在304处，容器可以进入测试环境。在测试环境中，可以将请求转发器设置为在许可模式下运行。测试环境不控制访问，而是被用于识别访问需求。在持续交付和容器化系统

中典型的此类测试执行容器的功能并触发对云提供商的调用。测试环境应当尽可能全面，否则测试可能存在差距并且可能无法捕获请求需求，因此将不会授予访问权。

[0086] 测试环境可以存在于云中。在测试环境内，可以存在基线策略，该基线策略提供系统可以拥有的最大允许访问权。例如，基线策略可以提供限制，诸如到功能即服务的连接(例如，出于安全考虑)。因此，在这种情况下，将不会向测试机器提供对功能即服务的访问权。因此，如果尝试通过该系统进行连接，并且采用其它许可策略，那么测试将失败，因为用于测试的计算机将不具有该访问权，并且测试将失败。这是为了让开发人员可以了解哪些访问是不可能的。

[0087] 在306处，可以接收测试结果。测试结果可以确定在容器上运行的一个或多个应用是否可以访问一个或多个云服务。如果测试结果是否定的，那么该过程不继续，因为或者容器已损坏或编码错误，或者基线策略禁止访问。

[0088] 在308处，对云提供商的请求可以由请求转发器记录在请求日志中。请求日志可以存储在服务器上。

[0089] 在310处，然后聚合请求日志以创建特定于特定容器的云服务访问策略以及用于托管容器的计算节点(常常是节点组)的云服务访问策略。这个过程可以通过一种类型的基础设施编排来执行。可以通过作为系统配置提供的访问规则来微调策略创建。例如，此类访问规则可以阻止一个节点访问两个特定的云服务。然后，策略与容器一起打包到单个部署包中。

[0090] 在312处，可以生成部署包。部署包可以包括容器、特定于容器的策略和节点策略。

[0091] 在314处，基础设施编排模块可以接收部署包。

[0092] 在316处，体系架构流程模块可以将节点访问策略部署到云IAM。节点访问策略提供机器访问。

[0093] 在318处，体系架构流程模块可以部署容器并且特定于容器的访问策略被部署到容器集群。

[0094] 在320处，容器集群可以部署容器。这里的容器带着策略去往容器集群或者容器，并且容器本身部署到容器上并且策略部署到请求转发上。因此，现在，请求转发器意识到在节点上运行的各个容器可以使用什么访问权并控制该访问权，并且云IAM现在具有允许这些计算机基于该配置运用该访问权的策略。

[0095] 在322处，容器集群将策略发送到请求转发器。类似地，当容器被移除时，访问权(即，转发器中的容器访问权以及授予计算节点的策略中不必要的部分)被移除。

[0096] 在示例操作中，新容器被识别以在应用中首次使用。为了继续进行，需要做两件事。首先，该过程需要允许该容器使用对象存储库的策略，因此节点将识别这个容器，但不能识别其它容器。这允许容器访问对象存储库，并且这个容器将在其上运行的机器必须有权访问对象存储库。因此，这两个策略被创建，并且与新容器打包在一起。现在，当部署容器并且体系架构编排将其解包时，可部署工件供给提供对云IAM的访问，以便机器和该容器将部署到机器组，这些机器现在有权访问对象存储库，这以前从未有过。此外，当该容器部署到容器集群时，请求转发器或控制此类访问的任何其它机制将知道该容器有权访问对象存储库。因此，即使该机器上可以运行着其它容器，这些容器也无权访问对象存储库，哪怕该机器在技术上可以访问对象存储库。

[0097] 容器集群可以散布在多个机器或多个计算实例(例如,Kubernetes、Docker Swarm或Openshift)上。容器编排器可以是在多个机器上放置和管理容器的系统。这些机器可以被抽象为工作者。这些机器可以由容器编排器添加或移除,如果一个机器坏掉,那么容器编排器将该容器提供给另一个机器。这些机器可以具有组(例如,机器组),这些组可以是这个容器可以在其上运行的机器的集合。从容器编排器的角度来看,这组机器也可以被称为节点。从云基础设施的角度来看,它们可以被称为实例。实例可以是虚拟机或裸机计算机。

[0098] 云IAM可以控制对容器集群设置的虚拟机组或裸机机器组或组合的访问。云IAM控制该云环境中的哪些主体有权访问云内的内容。机器通常被放置到组中,并且这些机器组被授予对云服务的访问权。组允许向上和向下扩展,以授予对计算机组的访问权,以在一个实例无法处置负载的情况下允许另一个计算机接管。

[0099] 图4图示了示例布置图400,其示出了所公开系统的允许的布置。该示例可以假设由六个容器组成的工作负载,并且在测试环境中识别出了以下连接需求。表1说明了容器/服务或资源图表。示例服务可以是Oracle云基础设施(OCI),它允许管理和扩展网络。另一个示例服务可以是VMware配置管理器(VCM)。服务内的资源可以是子网或负载平衡器。

[0100]

| 容器 | 服务/资源 |
|---|---|
| 容器 1 | 服务 A |
| 容器 2 | 服务 B |
| 容器 3 | 服务 B<br>服务 A |
| 容器 4 | 服务 C/资源 X |
| 容器 5 | 服务 A<br>服务 C/资源 Y |
| 容器 6 | 服务 D |

[0101] 表1

[0102] 在该示例中,访问规则可以由系统管理员指定以反映服务的安全性要求。示例访问规则可以要求从服务C/资源Y单独访问服务C/资源X。访问规则还可以要求从服务D单独访问服务A。这些规则提供对可以授予计算节点并调谐系统操作的访问权的限制。基于已知的通信路径和访问控制限制,系统可以识别哪些容器可以共同位于同一节点上。这在图4中所示的“允许的布置”图中进行了描绘。使用图操作,系统可以识别可以被共享的容器组和多个不同的节点。参考图4,容器1 402可以与容器2 404、容器3 406、容器4 408或容器5 410位于同一位置,但不与容器6 412位于同一位置。容器2可以与容器1 402、容器3 406、容器4 408、容器5 410或容器6 412位于同一位置。容器3 406可以与容器1 402、容器2 404、容器4 408或容器5 410位于同一位置。容器4 408可以与容器1 402、容器2 404、容器3 406或容器6 412位于同一位置。容器5可以与容器1 402、容器2 404或容器3 406位于同一位置。容器6可以与容器2 404或容器4 408位于同一位置。

[0103] 图5图示了示出所公开系统的禁止的布置的示例布置图500。图5遵循表1中指定并

在图4中讨论的相同访问规则。执行这个操作的一种方法是使用图来捕获容器的被禁止的布置。这在图5中的“禁止的布置”图中进行了描绘。给定禁止的布置，断开连接的图节点的任何集合都变成容器的有效分组。这在“允许的分组”中捕获，如图4中所示。应注意的是，容器2 504与每个节点都断开连接；因此，它可以被包括在任何容器分组中。而且，应注意的是，还存在未示出的其它可能布置。系统可以只提供用于容器分组的严格准则，从而允许容器编排器在这些约束内基于自己的算法并考虑其它因素来调度容器。如图5中所示，禁止容器1 502与容器6 512位于同一位置。不禁止容器2 504与任何其它容器位于同一位置。禁止容器6 512与容器1 502、容器3 506或容器5 510位于同一位置。禁止容器3 506与容器6 512位于同一位置。禁止容器5 510与容器6 512和容器4 508位于同一位置。禁止容器4 508与容器5 510位于同一位置。

[0104] 从上面的“允许的分组”示例中，识别出节点组的访问需求，其表示容器的访问需求的并集，并且可以如表2中所示进行调度：

[0105]

| 节点组 | 服务/请求 |
| --- | --- |
| 节点组 1 | 服务 B<br>服务 D<br>服务 C/资源 X |

[0106]

| | |
| --- | --- |
| 节点组 2 | 服务 A<br>服务 B<br>服务 C/资源 Y |

[0107] 表2

[0108] 图6图示了允许的分组的示例图600。这种分组遵循规定的访问规则。而且，这种分组提供了从规则中出现的容器的自然分离。各个容器以及节点组的访问需求被捕获在相应的策略中并与相应的容器一起打包。云编排系统(诸如Terraform)可以被用于自动将策略部署到云IAM，并使用特定于特定云基础设施的机制来执行任何所需的节点分组。如果系统在未设置计算节点策略的模式下操作，那么系统可以检查现有节点组，识别与容器匹配的节点组，然后报告许可不足或过多。

[0109] 图6图示了节点组1 602和节点组2 604。节点组1 602可以包括容器2 608、容器4 612和容器6 616。节点组2可以包括容器1606、容器3 610、容器5 614和容器2 608。

[0110] 允许的组图600是从实施方式的角度来看的。系统可以分析图600以确定允许的布置。例如，第一组机器可以托管容器2、6和4，而第二组机器可以托管容器1、3、5和2。如图所描绘的，容器2可以托管在组1和组2的机器中，这出于性能原因可以是有用的。例如，节点组2中可以存在多余的容量，可以将容器2放置在那里。这仅是一种可能性。

[0111] 在示例中，每个容器可以获得其自己的节点组。这也是有效的，但这不是最优的和有帮助的。由于系统知道这是容器的允许的分组，因此系统现在可以创建节点组；可以调度这些节点组中的容器；可以识别每个组的组合策略，因为系统知道容器的具体需求是什么；并且可以假设节点本身不需要任何访问。

[0112] 但一般而言，一组机器的组合需求只是该机器上的所有容器的需求。因此，节点组1可以访问服务BDC，并且资源X节点组2可以访问服务ABC资源Y。这产生策略。通过识别容器的需求，系统在应用内创建遵守这些规则的逻辑隔离。应用的逻辑隔离可以通过将容器放置在节点组中以及该节点组中的这些容器中进行创建，就像安全工程师在与团队一起审查时所做的那样。系统可以通过它想要实现的那些规则通过完全不同的机制推断出环境的逻辑分离。并且在例如系统不断添加具有其它访问需求的更多容器等的情况下，这些规则将被保留。

[0113] 可以存在无法以图方式解决这个问题的情况；这是一个容器违反其中一些规则的情况。如果系统将对服务C资源X的访问与服务资源Y分开，那么系统将具有访问服务中这两种资源的容器。这个问题无法解决，因为无法同时访问两个服务资源，并且系统将出现故障。它将在聚合步骤中出现故障，这可能是有益的。为此，系统将确定它实际上无法继续进行，因为设计者已经创建了违反系统已建立的规则的容器。

[0114] 图7是与用于自动配置容器应用的最小云服务访问权限的技术相关联的示例过程700的流程图。在一些实施方式中，图7的一个或多个过程方框可以由计算机系统(例如，如图12中所示的计算机系统1200)执行。附加地或替代地，图7的一个或多个过程方框可以由设备1200的一个或多个组件来执行，其中组件诸如处理单元1204、存储子系统1218、通信子系统1224、输入/输出子系统1208和总线子系统1202。处理单元1204可以包括子处理单元1232、1234。存储子系统1218可以包括系统存储器1210。系统存储器120可以包括应用程序1212、程序数据1214和操作系统1216。存储子系统1218可以包括计算机可读存储介质读取器1220和计算机可读存储介质1222。

[0115] 如图7中所示，过程700可以包括接收对于访问一个或多个云服务的一个或多个请求(方框710)。例如，计算机系统可以接收对于访问一个或多个云服务的一个或多个请求，如上所述。可以从一个或多个相同或不同的发送者接收请求。

[0116] 如图7中进一步所示，过程700可以包括将一个或多个请求存储在请求日志中(方框720)。例如，计算机系统可以将一个或多个请求存储在请求日志中，如上所述。

[0117] 如图7中进一步所示，过程700可以包括接收适用于云服务访问权限的一个或多个访问规则(方框730)。例如，计算机系统可以接收适用于云服务访问权限的一个或多个访问规则，如上所述。

[0118] 如图7中进一步所示，过程700可以包括聚合请求日志的一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用(方框740)。例如，计算机系统可以聚合请求日志的一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用，如上所述。

[0119] 如图7中进一步所示，过程700可以包括生成定义容器和一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于聚合的一个或多个请求和一个或多个访问规则(方框750)。例如，计算机系统可以生成定义容器和一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于聚合的一个或多个请求和一个或多个访问规则，如上所述。

[0120] 如图7进一步所示，过程700可以包括将容器访问策略存储在存储器中(方框760)。例如，计算机系统可以将容器访问策略存储在存储器中，如上所述。

[0121] 如图7中进一步所示，过程700可以包括将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对一个或多个云服务的访问权限(方框770)。例如，计算机系统可以将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对一个或多个云服务的访问权限，如上所述。

[0122] 过程700可以包括附加的实施方式，诸如下面描述的和/或与本文别处描述的一个或多个其它过程相结合的任何单个实施方式或实施方式的任何组合。

[0123] 过程700可以以两种模式操作。在第一模式下，过程700控制对云服务的访问。在第一节点中，容器的访问权以及节点的访问权都是由系统动态设置的。集群使用的容器和节点的所有访问要求都是自动配置的。系统可以被配置为调整如何授予节点访问权。最简单的情况是，所有节点都是平等的，并且任何容器都可以在任何节点上被调度。在这种情况下，每个节点需要的访问许可等同于所有容器的组合访问权。但是，应用设计者通常会分离容器，以便对一个容器(即，暴露程度较高或可信程度较低的容器)的攻击不会暴露同一节点中的其它容器。用于分离容器的过程可以是手动过程，并且取决于专家对系统和安全性约束的理解。在所公开的系统中，可以消除决定应当如何分离各个容器的要求。系统可以配置有关于应当如何授予访问权的一般规则(例如，一个系统不得访问两个特定服务或资源)。在制定此类规则后，系统自动将集群分区为具有不同访问权的节点组，并将容器指派给具有足够访问权的正确节点。同时，它保留了将可以在多个组中操作的容器指派给集群中的任何节点的灵活性。虽然这种机制有其益处，但一些用户可能强烈倾向于手动配置系统中的节点的访问权，或者可能不愿意将任何IAM访问管理委托给自动化系统。

[0124] 在第一实施方式中，过程700包括生成节点访问策略，该节点访问策略指定用于向计算实例组授予节点上的一个或多个容器的组合访问权的访问策略，并且过程700包括将容器访问策略存储在存储器中。

[0125] 在第二实施方式中，单独地或与第一实施方式组合，过程700包括授予与指派给节点的一个或多个容器的组合访问权等同的访问许可。

[0126] 在第三实施方式中，单独地或与第一实施方式和第二实施方式中的一个或多个组合，过程700包括将具有多个计算实例的计算实例分区成节点组，每个节点具有不同的访问权，并且至少部分地基于节点访问策略将一个或多个容器指派给具有足够访问权的节点。

[0127] 在第二模式下，过程700不控制节点对云服务的访问。在第四实施方式中，单独地或与第一实施方式至第三实施方式中的一个或多个组合，访问是预先确定的并且每个节点内的容器访问是动态配置的。当用户不愿意将访问管理委托给自动化系统时，节点的访问可以预先配置并为系统所知。在此，仅动态配置节点内授予的容器访问权。然后，系统可以在需要时将具有特定访问需求的容器放置到具有足够访问权的节点。因为授予计算节点的访问权是由系统预先定义且不可变的，所以可能发生容器需要集群中任何节点都不能允许的访问权的情况。这可以在测试阶段检测到。如果转发器发出请求失败，那么记录该失败，指示必须对计算实例的许可进行改变。有多种方式来确定转发器的请求是否失败。在测试环境中，假设测试实例和生产实例具有完全相同的许可，那么测试本身的失败就是足够的证明。

[0128] 在第五实施方式中，单独地或与第一实施方式至第四实施方式中的一个或多个组

合，过程700包括测试云系统的访问要求、至少部分地基于请求日志中的条目来检测特定应用访问一个或多个云服务的故障，并改变计算实例的许可来修复故障。在一些示例中，请求日志中的条目是先前存储的请求。例如，请求日志可以被配置为存储多个请求。并且，请求日志中的每个请求可以被视为条目。

[0129] 在第六实施方式中，单独地或与第一实施方式至第五实施方式中的一个或多个组合，过程700包括将生产环境中的每个容器类型的请求转发器设置为许可模式，该许可模式授予容器中存储的一个或多个应用对一个或多个云服务的访问权，从请求转发器接收一个或多个请求，并且根据该一个或多个请求的数量超过阈值要求而将请求转发器切换到限制模式，该限制模式部分地基于容器访问策略来授予一个或多个应用对一个或多个云服务的访问权。

[0130] 虽然图7示出了过程700的示例方框，但在一些实施方式中，过程700可以包括与图7中描绘的方框相比附加的方框、更少的方框、不同的方框或不同布置的方框。附加地或替代地，过程700的两个或更多个方框可以并行执行。

[0131] III.集中式请求转发器

[0132] 单独的集中式节点、或支持多个节点的单独的请求转发器集合、或节点的任何组合都是允许的。所公开的系统可以通过管理具有指派给该容器的转发器的容器策略以及托管该转发器的节点的节点策略来支持所有这些选项，而不管该节点位于何处。类似地，系统可以通过基于组合容器需求授予对该实体的访问权来支持请求转发器的集中式云版本。

[0133] 可以存在多种定位请求转发器的方式。在一个示例中，请求转发器可以位于中央。在另一个示例中，只要存在供给该策略并识别容器的机制，请求转发器就可以位于机器外部。在一些示例中，生产模型中可能不存在请求转发器。最后，容器策略可以获取生产环境中的容器策略。如果客户端认为测试不够全面或者没有测试环境，那么可以这样做。在这种情况下，该技术可以仅在最初具有许可模式的生产环境中实现，并且当接收到附加请求时，它获知访问需求。当已经识别出访问需求时，它获得足够的信息，使其了解所有访问需求，并且可以开始强制执行这些需求。

[0134] 在一个示例中，在最后数量的请求中，不存在新的请求。可以配置不同的阈值来表示已实现并识别出足够的访问权。然后系统开始强制执行访问权。系统一开始可能会以过于宽松的许可策略运行，但最终该策略会变得更加严格。这比永远在许可模式下运行要好。

[0135] 如果移除容器，那么可以移除访问权。如果为系统提供了新容器，那么访问权可能不可用，并且该过程将了解容器的生命周期，并移除先前建立的规则(例如，在部署了新版本的容器的情况下)。

[0136] 云网络体系架构可以包括多个计算实例。一个或多个计算实例可以存储各种容器。另一个单独的计算实例可以包括请求转发器、元数据服务和一个或多个策略。云网络体系架构可以包括各种云服务(例如，云服务A、云服务B、云服务C)。云网络体系架构还可以包括容器编排器。请求转发器可以集中用于多个节点，或者每个节点可以有自己的请求转发器。集中式/专用请求转发器节点意味着不同的节点(其可以包含多个容器)可以经由集中式节点将其请求转发到云服务。实例凭证不需要存储在每个节点上，只需存储在存在请求转发器的节点上即可。请求转发器不一定需要与其支持的容器位于同一节点上。

[0137] 这两种体系架构都有优点和缺点。关于集中式/专用请求转发器，节点的资源可以

专用于仅执行请求转发器的职责，而其它节点可以专注于使用其资源来执行其任务。除此之外，实例凭证不需要存储在每个节点上，只需存储在集中式实例上。但是，这种方法的缺点是集中式请求转发器充当单点故障。如果它宕机，那么所有容器都无法向云服务发出请求。至于在每个节点上都有请求转发器的情况，网络规则/体系架构的创建和运行将变得更加简单。每节点转发器的另一个优点是每个节点都有自己的请求转发器，导致每个节点仅处理其容器的工作负载。这种设计的一个缺点是必须维护每个节点的凭证才能访问云服务。这使得正确的密钥轮换和撤销问题变得更加困难，其程度取决于所涉及的节点数量。混合方法可以涉及使用集群节点的子集来托管请求转发器。

[0138] 在各种实施例中，生产中不存在请求转发器。该系统在生产中没有请求转发器的情况下也可以是有用的。在这种情况下，如果容器具有该节点所具有的所有访问权，那么无需为各个容器设置策略。但是，该节点的访问权将被限制为该节点上所有容器的并集。这虽然不会将容器访问限制在最低限度，但仍然会自动限制节点访问，这是优于手动配置访问的主要优势。

[0139] 在各种实施例中，容器策略可以在生产环境中获取。虽然该系统最有可能分两个阶段使用，其中构造策略所需的数据是在可信测试环境中获取的，然后与容器一起部署到生产系统，但仅在生产环境中替代机制是可能的。

[0140] 这种机制涉及针对生产环境中的每种容器类型单独地切换请求转发器的许可/限制模式。第一次部署容器时，请求转发器将所有请求发送到云服务，同时还产生请求的日志。在搜集到足够的数据之后，它切换到该特定容器的限制模式。这种实施方式不提供相同级别的安全性，因为在一段时间内允许对云服务的所有访问。但是，它确实降低了系统运营成本，并且对于一些用户来说可能就足够了，尤其是当容器周转率低时。何时获取足够的数据以切换模式的决定可以手动完成，或者基于时间，或者通过分析正在转发的新类型请求的数量来完成。例如，如果发送到转发器的所有请求在给定指定数量的请求的情况下不包含新请求，那么所收集的数据可以被认为是足够的。对节点的访问可以以类似的方式进行管理，从过度访问开始(在管理员设置的合理边界内)，然后减少到各个容器所需的特定权限，前提是完全建立了节点上所有容器的访问需求。

[0141] IV.基础设施即服务(IAAS)

[0142] 如上所述，基础设施即服务(IaaS)是一种特定类型的云计算。IaaS可以被配置为通过公共网络(例如，互联网)提供虚拟化计算资源。在IaaS模型中，云计算提供商可以托管基础设施组件(例如，服务器、存储设备、网络节点(例如，硬件)、部署软件、平台虚拟化(例如，管理程序层)等)。在一些情况下，IaaS提供商还可以提供各种服务来伴随这些基础设施组件(例如，计费、监视、日志记录、安全性、负载平衡和聚类等)。因此，由于这些服务可能是策略驱动的，因此IaaS用户可以能够实现策略来驱动负载平衡，以维持应用的可用性和性能。

[0143] 在一些情况下，IaaS客户可以通过诸如互联网之类的广域网(WAN)访问资源和服务，并且可以使用云提供商的服务来安装应用堆栈的剩余元素。例如，用户可以登录到IaaS平台以创建虚拟机(VM)、在每个VM上安装操作系统(OS)、部署诸如数据库之类的中间件、为工作负载和备份创建存储桶、甚至将企业软件安装到该VM中。然后，客户可以使用提供商的服务来执行各种功能，包括平衡网络流量、解决应用问题、监视性能、管理灾难恢复等。

[0144] 在大多数情况下，云计算模型将需要云提供商的参与。云提供商可以但不一定是专门提供(例如，供应、出租、销售)IaaS的第三方服务。实体也可能选择部署私有云，从而成为其自己的基础设施服务提供商。

[0145] 在一些示例中，IaaS部署是将新应用或应用的新版本放置到准备好的应用服务器等上的处理。它还可以包括准备服务器(例如，安装库、守护进程等)的处理。这通常由云提供商管理，位于管理程序层(例如，服务器、存储装置、网络硬件和虚拟化)之下。因此，客户可以负责处理(OS)、中间件和/或(例如，在(例如可以按需启动的)自助服务虚拟机上的)应用部署等。

[0146] 在一些示例中，IaaS供给可以指获取计算机或虚拟主机以供使用，甚至在它们上安装所需的库或服务。大多数情况下，部署不包括供给，并且供给可能需要被首先执行。

[0147] 在一些情况下，IaaS供给存在两个不同的问题。首先，在任何东西运行之前供给初始基础设施集合存在最初的挑战。其次，一旦所有东西已被供给，就存在演进现有基础设施(例如，添加新服务、更改服务、移除服务等)的挑战。在一些情况下，可以通过启用以声明方式定义基础设施的配置来解决这两个挑战。换句话说，基础设施(例如，需要哪些组件以及它们如何交互)可以由一个或多个配置文件来定义。因此，基础设施的总体拓扑(例如，哪些资源依赖于哪些资源，以及它们如何协同工作)可以以声明的方式描述。在一些情况下，一旦定义了拓扑，就可以生成创建和/或管理配置文件中描述的不同组件的工作流。

[0148] 在一些示例中，基础设施可以具有许多互连的元素。例如，可能存在一个或多个虚拟私有云(VPC)(例如，可配置和/或共享计算资源的潜在按需池)，也称为核心网络。在一些示例中，还可以供给一个或多个安全性组规则以定义将如何设置网络的安全性以及一个或多个虚拟机(VM)。也可以供给其它基础设施元素，诸如负载平衡器、数据库等。随着期望和/或添加越来越多的基础设施元素，基础设施可以逐步演进。

[0149] 在一些情况下，可以采用连续部署技术来使得能够跨各种虚拟计算环境来部署基础设施代码。此外，所描述的技术可以使得能够在这些环境内进行基础设施管理。在一些示例中，服务团队可以编写期望部署到一个或多个但通常是许多不同的生产环境(例如，跨各种不同的地理位置，有时跨越整个世界)的代码。但是，在一些示例中，必须首先设置将在其上部署代码的基础设施。在一些情况下，供给可以手动完成，可以利用供给工具来供给资源，和/或一旦供给基础设施就可以利用部署工具来部署代码。

[0150] 图8是图示根据至少一个实施例的IaaS体系架构的示例模式的框图800。服务运营商802可以通信地耦合到可以包括虚拟云网络(VCN)806和安全主机子网808的安全主机租赁804。在一些示例中，服务运营商802可以使用一个或多个客户端计算设备(客户端计算设备可以是便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如，Google **Glass®** 头戴式显示器))，运行软件(诸如Microsoft Windows **Mobile®**)和/或各种移动操作系统(诸如iOS、Windows Phone、Android、BlackBerry 8、Palm OS等)，并且支持互联网、电子邮件、短消息服务(SMS)、**Blackberry®**或其它通信协议。可替代地，客户端计算设备可以是通用个人计算机，包括例如运行各种版本的Microsoft **Windows®** 、Apple **Macintosh®** 和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行各种商业上可获得的

UNIX®或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统(诸如例如Google Chrome OS))中的任何操作系统的工作站计算机。替代地或附加地,客户端计算设备可以是任何其它电子设备,诸如瘦客户端计算机、支持互联网的游戏系统(例如,具有或不具有Kinect®手势输入设备的Microsoft Xbox游戏控制台)、和/或能够通过可以访问VCN 806和/或互联网的网络进行通信的个人消息传递设备。

[0151] VCN 806可以包括本地对等网关(LPG)810,该VCN 806可以经由包含在安全壳(SSH)VCN 812中的LPG 810通信地耦合到SSH VCN 812。SSH VCN 812可以包括SSH子网814,并且SSH VCN 812可以经由包含在控制平面VCN 816中的LPG 810通信地耦合到控制平面VCN 816。此外,SSH VCN 812可以经由LPG 810通信地耦合到数据平面VCN 818。控制平面VCN 816和数据平面VCN 818可以包含在可以由IaaS提供商拥有和/或操作的服务租赁819中。

[0152] 控制平面VCN 816可以包括充当外围网络(例如,公司内部网络和外部网络之间的公司网络的部分)的控制平面非军事区(DMZ)层820。基于DMZ的服务器可以承担有限责任并有助于控制安全性违规。此外,DMZ层820可以包括一个或多个负载平衡器(LB)子网822、可以包括(一个或多个)应用(app)子网826的控制平面应用层824、可以包括(一个或多个)数据库(DB)子网830(例如,(一个或多个)前端DB子网和/或(一个或多个)后端DB子网)的控制平面数据层828。包含在控制平面DMZ层820中的(一个或多个)LB子网822可以通信地耦合到包含在控制平面应用层824中的(一个或多个)应用子网826和可以包含在控制平面VCN 816中的互联网网关834,并且(一个或多个)应用子网826可以通信地耦合到包含在控制平面数据层828中的(一个或多个)DB子网830以及服务网关836和网络地址转换(NAT)网关838。控制平面VCN 816可以包括服务网关836和NAT网关838。

[0153] 控制平面VCN 816可以包括数据平面镜像应用层840,其可以包括(一个或多个)应用子网826。包含在数据平面镜像应用层840中的(一个或多个)应用子网826可以包括可以执行计算实例844的虚拟网络接口控制器(VNIC)842。计算实例844可以将数据平面镜像应用层840的(一个或多个)应用子网826通信地耦合到可以包含在数据平面应用层846中的(一个或多个)应用子网826。

[0154] 数据平面VCN 818可以包括数据平面应用层846、数据平面DMZ层848和数据平面数据层850。数据平面DMZ层848可以包括(一个或多个)LB子网822,其可以通信地耦合到数据平面应用层846的(一个或多个)应用子网826和数据平面VCN 818的互联网网关834。(一个或多个)应用子网826可以通信地耦合到数据平面VCN 818的服务网关836和数据平面VCN 818的NAT网关838。数据平面数据层850还可以包括可以通信地耦合到数据平面应用层846的(一个或多个)应用子网826的(一个或多个)DB子网830。

[0155] 控制平面VCN 816和数据平面VCN 818的互联网网关834可以通信地耦合到元数据管理服务852,该元数据管理服务852可以通信地耦合到公共互联网854。公共互联网854可以通信地耦合到控制平面VCN 816和数据平面VCN 818的NAT网关838。控制平面VCN 816和数据平面VCN 818的服务网关836可以通信地耦合到云服务856。

[0156] 在一些示例中,控制平面VCN 816或数据平面VCN 818的服务网关836可以对云服务856进行应用编程接口(API)调用,而无需通过公共互联网854。从服务网关836到云服务856的API调用可以是单向的:服务网关836可以对云服务856进行API调用,并且云服务856

可以将请求的数据发送到服务网关836。但是，云服务856可以不发起对服务网关836的API调用。

[0157] 在一些示例中，安全主机租赁804可以直接连接到服务租赁819，服务租赁819否则可以被隔离。安全主机子网808可以通过LPG 810与SSH子网814通信，LPG 810可以使得能够在否则隔离的系统上进行双向通信。将安全主机子网808连接到SSH子网814可以使安全主机子网808访问服务租赁819内的其它实体。

[0158] 控制平面VCN 816可以允许服务租赁819的用户设置或以其它方式供给期望资源。在控制平面VCN 816中供给的期望资源可以在数据平面VCN 818中部署或以其它方式使用。在一些示例中，控制平面VCN 816可以与数据平面VCN 818隔离，并且控制平面VCN 816的数据平面镜像应用层840可以经由VNIC 842与数据平面VCN 818的数据平面应用层846通信，VNIC 842可以包含在数据平面镜像应用层840和数据平面应用层846中。

[0159] 在一些示例中，系统的用户或客户可以通过可以将请求传送到元数据管理服务852的公共互联网854来做出请求，例如创建、读取、更新或删除(CRUD)操作。元数据管理服务852可以通过互联网网关834将请求传送到控制平面VCN 816。请求可以由包含在控制平面DMZ层820中的(一个或多个)LB子网822接收。(一个或多个)LB子网822可以确定请求是有效的，并且响应于该确定，(一个或多个)LB子网822可以将请求传输到包含在控制平面应用层824中的(一个或多个)应用子网826。如果请求被验证并且需要对公共互联网854的调用，那么对公共互联网854的调用可以被传输到可以对公共互联网854进行调用的NAT网关838。请求可能期望存储的存储器可以存储在(一个或多个)DB子网830中。

[0160] 在一些示例中，数据平面镜像应用层840可以促进控制平面VCN 816和数据平面VCN 818之间的直接通信。例如，可能期望对包含在数据平面VCN 818中的资源应用对配置的更改、更新或其它适当的修改。经由VNIC 842，控制平面VCN 816可以直接与包含在数据平面VCN 818中的资源通信，并且从而可以执行对这些资源的配置的更改、更新或其它适当的修改。

[0161] 在一些实施例中，控制平面VCN 816和数据平面VCN 818可以包含在服务租赁819中。在这种情况下，系统的用户或客户可能不拥有或操作控制平面VCN 816或数据平面VCN 818。替代地，IaaS提供商可以拥有或操作控制平面VCN 816和数据平面VCN818，这两种平面都可以包含在服务租赁819中。该实施例可以使得能够隔离可能阻止用户或客户与其它用户或其它客户的资源进行交互的网络。此外，该实施例可以允许系统的用户或客户私自存储数据库，而无需依赖可能不具有期望安全级别的公共互联网854以进行存储。

[0162] 在其它实施例中，包含在控制平面VCN 816中的(一个或多个)LB子网822可以被配置为从服务网关836接收信号。在这个实施例中，控制平面VCN 816和数据平面VCN 818可以被配置为由IaaS提供商的客户调用而无需调用公共互联网854。IaaS提供商的客户可能期望这个实施例，因为客户使用的(一个或多个)数据库可以由IaaS提供商控制并且可以存储在服务租赁819上，服务租赁819可能与公共互联网854隔离。

[0163] 图9是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图900。服务运营商902(例如，图8的服务运营商802)可以通信地耦合到安全主机租赁904(例如，图8的安全主机租赁804)，该安全主机租赁904可以包括虚拟云网络(VCN)906(例如，图8的VCN 806)和安全主机子网908(例如，图8的安全主机子网808)。VCN 906可以包括本地对等网关

(LPG)910(例如,图8的LPG 810),该VCN 906可以经由包含在安全壳(SSH)VCN 912(例如,图8的SSH VCN 812)中的LPG 810通信地耦合到SSH VCN 912。SSH VCN 912可以包括SSH子网914(例如,图8的SSH子网814),并且SSH VCN 912可以经由包含在控制平面VCN 916(例如,图8的控制平面VCN 816)中的LPG 910通信地耦合到控制平面VCN 916。控制平面VCN 916可以包含在服务租赁919(例如,图8的服务租赁819)中,并且数据平面VCN 918(例如,图8的数据平面VCN 818)可以包含在可能由系统的用户或客户拥有或操作的客户租赁921中。

[0164] 控制平面VCN 916可以包括控制平面DMZ层920(例如,图8的控制平面DMZ层820),其可以包括(一个或多个)LB子网922(例如,图8的(一个或多个)LB子网822)、可以包括(一个或多个)应用子网926(例如,图8的(一个或多个)应用子网826)的控制平面应用层924(例如,图8的控制平面应用层824)、可以包括(一个或多个)数据库(DB)子网930(例如,类似于图8的(一个或多个)DB子网830)的控制平面数据层928(例如,图8的控制平面数据层828)。包含在控制平面DMZ层920中的(一个或多个)LB子网922可以通信地耦合到包含在控制平面应用层924中的(一个或多个)应用子网926和可以包含在控制平面VCN 916中的互联网网关934(例如,图8的互联网网关834),并且(一个或多个)应用子网926可以通信地耦合到包含在控制平面数据层928中的(一个或多个)DB子网930以及服务网关936(例如,图8的服务网关)和网络地址转换(NAT)网关938(例如,图8的NAT网关838)。控制平面VCN 916可以包括服务网关936和NAT网关938。

[0165] 控制平面VCN 916可以包括可以包括(一个或多个)应用子网926的数据平面镜像应用层940(例如,图8的数据平面镜像应用层840)。包含在数据平面镜像应用层940中的(一个或多个)应用子网926可以包括可以执行计算实例944(例如,类似于图8的计算实例844)的虚拟网络接口控制器(VNIC)942(例如,VNIC 842)。计算实例944可以促进数据平面镜像应用层940的(一个或多个)应用子网926和可以包含在数据平面应用层946(例如,图8的数据平面应用层846)中的(一个或多个)应用子网926之间的经由包含在数据平面镜像应用层940中的VNIC 942以及包含在数据平面应用层946中的VNIC 942的通信。

[0166] 包含在控制平面VCN 916中的互联网网关934可以通信地耦合到元数据管理服务952(例如,图8的元数据管理服务852),该元数据管理服务952可以通信地耦合到公共互联网954(例如,图8的公共互联网854)。公共互联网954可以通信地耦合到包含在控制平面VCN 916中的NAT网关938。包含在控制平面VCN916中的服务网关936可以通信地耦合到云服务956(例如,图8的云服务856)。

[0167] 在一些示例中,数据平面VCN 918可以包含在客户租赁921中。在这种情况下,IaaS提供商可以为每个客户提供控制平面VCN 916,并且IaaS提供商可以为每个客户设置包含在服务租赁919中的唯一计算实例944。每个计算实例944可以允许包含在服务租赁919中的控制平面VCN 916和包含在客户租赁921中的数据平面VCN 918之间的通信。计算实例944可以允许在包含在服务租赁919中的控制平面VCN 916中供给的资源被部署或以其它方式用于包含在客户租赁921中的数据平面VCN 918中。

[0168] 在其它示例中,IaaS提供商的客户可以具有存在于客户租赁921中的数据库。在这个示例中,控制平面VCN 916可以包括数据平面镜像应用层940,该数据平面镜像应用层940可以包括(一个或多个)应用子网926。数据平面镜像应用层940可以驻留在数据平面VCN 918中,但数据平面镜像应用层940可能不在数据平面VCN 918中。换句话说,数据平面镜像

应用层940可以访问客户租赁921,但是数据平面镜像应用层940可能不存在于数据平面VCN 918中或者由IaaS提供商的客户拥有或操作。数据平面镜像应用层940可以被配置为对数据平面VCN 918进行调用,但可以不被配置为对包含在控制平面VCN 916中的任何实体进行调用。客户可能期望在数据平面VCN 918中部署或以其它方式使用在控制平面VCN 916中供给的资源,并且数据平面镜像应用层940可以促进客户的期望部署或资源的其它使用。

[0169] 在一些实施例中,IaaS提供商的客户可以将过滤器应用到数据平面VCN 918。在这个实施例中,客户可以确定数据平面VCN918可以访问什么,并且客户可以限制从数据平面VCN 918对公共互联网954的访问。IaaS提供商可能无法应用过滤器或以其它方式控制数据平面VCN 918对任何外部网络或数据库的访问。客户将过滤器和控制应用到包含在客户租赁921中的数据平面VCN918上可以帮助将数据平面VCN 918与其它客户和公共互联网954隔离开。

[0170] 在一些实施例中,云服务956可以由服务网关936调用以访问公共互联网954、控制平面VCN 916或数据平面VCN 918上可能不存在的服务。云服务956与控制平面VCN 916或数据平面VCN918之间的连接可以不是实时的或连续的。云服务956可以存在于由IaaS提供商拥有或操作的不同网络上。云服务956可以被配置为接收来自服务网关936的调用并且可以被配置为不接收来自公共互联网954的调用。一些云服务956可以与其它云服务956隔离,并且控制平面VCN 916可以与可能与控制平面VCN 916不在同一区域的云服务956隔离。例如,控制平面VCN 916可能位于“区域1”,并且云服务“部署6”可能位于区域1和“区域2”。如果包含在位于区域1中的控制平面VCN 916中的服务网关936对部署6进行调用,那么该调用可以被传输到区域1中的部署6。在这个示例中,控制平面VCN 916或区域1中的部署6可能不与区域2中的部署6通信地耦合或以其它方式通信。

[0171] 图10是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1000。服务运营商1002(例如,图8的服务运营商802)可以通信地耦合到安全主机租赁1004(例如,图8的安全主机租赁804),该安全主机租赁1004可以包括虚拟云网络(VCN)1006(例如,图8的VCN 806)和安全主机子网1008(例如,图8的安全主机子网808)。VCN 1006可以包括LPG 1010(例如,图8的LPG 810),该VCN 1006可以经由包含在SSH VCN 1012(例如,图8的SSH VCN 812)中的LPG 1010通信地耦合到SSH VCN 1012。SSH VCN 1012可以包括SSH子网1014(例如,图8的SSH子网814),并且SSH VCN 1012可以经由包含在控制平面VCN 1016(例如,图8的控制平面VCN 816)中的LPG 1010通信地耦合到控制平面VCN 1016并且经由包含在数据平面VCN1018(例如,图8的数据平面818)中的LPG 1010通信地耦合到数据平面VCN 1018。控制平面VCN 1016和数据平面VCN 1018可以包含在服务租赁1019(例如,图8的服务租赁819)中。

[0172] 控制平面VCN 1016可以包括可以包括(一个或多个)负载平衡器(LB)子网1022(例如,图8的(一个或多个)LB子网822)的控制平面DMZ层1020(例如,图8的控制平面DMZ层820)、可以包括(一个或多个)应用子网1026(例如,类似于图8的(一个或多个)应用子网1026)的控制平面应用层1024(例如,图8的控制平面应用层824)、可以包括(一个或多个)DB子网1030的控制平面数据层1028(例如,图8的控制平面数据层828)。包含在控制平面DMZ层1020中的(一个或多个)LB子网1022可以通信地耦合到包含在控制平面应用层1024中的(一个或多个)应用子网1026和可以包含在控制平面VCN 1016中的互联网网关1034(例如,图8

的互联网网关834)，并且(一个或多个)应用子网1026可以通信地耦合到包含在控制平面数据层1028中的(一个或多个)DB子网1030以及服务网关1036(例如，图8的服务网关)和网络地址转换(NAT)网关1038(例如，图8的NAT网关838)。控制平面VCN 1016可以包括服务网关1036和NAT网关1038。

[0173] 数据平面VCN 1018可以包括数据平面应用层1046(例如，图8的数据平面应用层846)、数据平面DMZ层1048(例如，图8的数据平面DMZ层848)，以及数据平面数据层1050(例如，图8的数据平面数据层850)。数据平面DMZ层1048可以包括可以通信地耦合到数据平面应用层1046的(一个或多个)可信应用子网1060和(一个或多个)不可信应用子网1062以及包含在数据平面VCN 1018中的互联网网关1034的(一个或多个)LB子网1022。(一个或多个)可信应用子网1060可以通信地耦合到包含在数据平面VCN 1018中的服务网关1036、包含在数据平面VCN1018中的NAT网关1038、以及包含在数据平面数据层1050中的(一个或多个)DB子网1030。(一个或多个)不可信应用子网1062可以通信地耦合到包含在数据平面VCN 1018中的服务网关1036和包含在数据平面数据层1050中的(一个或多个)DB子网1030。数据平面数据层1050可以包括可以通信地耦合到包含在数据平面VCN 1018中的服务网关1036的(一个或多个)DB子网1030。

[0174] (一个或多个)不可信应用子网1062可以包括可以通信地耦合到租户虚拟机(VM)1066(1)-(N)的一个或多个主VNIC1064(1)-(N)。每个租户VM 1066(1)-(N)可以通信地耦合到可以包含在相应容器出口VCN 1068(1)-(N)中的相应应用子网1067(1)-(N)，该相应容器出口VCN 1068(1)-(N)可以包含在相应客户租赁1070(1)-(N)中。相应辅VNIC 1072(1)-(N)可以促进包含在数据平面VCN 1018中的(一个或多个)不可信应用子网1062与包含在容器出口VCN 1068(1)-(N)中的应用子网之间的通信。每个容器出口VCN 1068(1)-(N)可以包括NAT网关1038，该NAT网关1038可以通信地耦合到公共互联网1054(例如，图8的公共互联网854)。

[0175] 包含在控制平面VCN 1016中以及包含在数据平面VCN 1018中的互联网网关1034可以通信地耦合到元数据管理服务1052(例如，图8的元数据管理系统852)，该元数据管理服务1052可以通信地耦合到公共互联网1054。公共互联网1054可以通信地耦合到包含在控制平面VCN 1016中以及包含在数据平面VCN 1018中的NAT网关1038。包含在控制平面VCN 1016中以及包含在数据平面VCN 1018中的服务网关1036可以通信地耦合到云服务1056。

[0176] 在一些实施例中，数据平面VCN 1018可以与客户租赁1070集成。在一些情况下，诸如在执行代码时可能期望支持的情况下，这种集成对于IaaS提供商的客户可能是有用的或期望的。客户可能提供可能具有破坏性、可能与其它客户资源通信或可能以其它方式导致非期望效果的代码来运行。作为对此的响应，IaaS提供商可以确定是否运行由客户给予IaaS提供商的代码。

[0177] 在一些示例中，IaaS提供商的客户可以向IaaS提供商授予临时网络访问，并请求附加到数据平面层应用1046的功能。运行该功能的代码可以在VM 1066(1)-(N)中执行，并且该代码可以不被配置为在数据平面VCN 1018上的其它任何地方运行。每个VM 1066(1)-(N)可以连接到一个客户租赁1070。包含在VM1066(1)-(N)中的相应容器1071(1)-(N)可以被配置为运行代码。在这种情况下，可以存在双重隔离(例如，容器1071(1)-(N)运行代码，其中容器1071(1)-(N)可能至少包含在(一个或多个)不可信应用子网1062中所包含的VM

1066(1)-(N)中),这可以帮助防止不正确的或以其它方式非期望的代码损坏IaaS提供商的网络或损坏不同客户的网络。容器1071(1)-(N)可以通信地耦合到客户租赁1070并且可以被配置为传输或接收来自客户租赁1070的数据。容器1071(1)-(N)可以不被配置为从数据平面VCN 1018中的任何其它实体传输或接收数据。在运行代码完成后,IaaS提供商可以终止或以其它方式处置容器1071(1)-(N)。

[0178] 在一些实施例中,(一个或多个)可信应用子网1060可以运行可以由IaaS提供商拥有或操作的代码。在这个实施例中,(一个或多个)可信应用子网1060可以通信地耦合到(一个或多个)DB子网1030并且被配置为在(一个或多个)DB子网1030中执行CRUD操作。(一个或多个)不可信应用子网1062可以通信地耦合到(一个或多个)DB子网1030,但是在这个实施例中,(一个或多个)不可信应用子网可以被配置为在(一个或多个)DB子网1030中执行读取操作。可以包含在每个客户的VM 1066(1)-(N)中并且可以运行来自客户的代码的容器1071(1)-(N)可以不与(一个或多个)DB子网1030通信地耦合。

[0179] 在其它实施例中,控制平面VCN 1016和数据平面VCN 1018可以不直接通信地耦合。在这个实施例中,控制平面VCN 1016和数据平面VCN 1018之间可能不存在直接通信。但是,通信可以通过至少一个方法而间接地发生。LPG 1010可以由IaaS提供商建立,其可以促进控制平面VCN 1016和数据平面VCN 1018之间的通信。在另一个示例中,控制平面VCN 1016或数据平面VCN1018可以经由服务网关1036对云服务1056进行调用。例如,从控制平面VCN 1016对云服务1056的调用可以包括对可以与数据平面VCN 1018通信的服务的请求。

[0180] 图11是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1100。服务运营商1102(例如,图8的服务运营商802)可以通信地耦合到安全主机租赁1104(例如,图8的安全主机租赁804),该安全主机租赁1104可以包括虚拟云网络(VCN)1106(例如,图8的VCN 806)和安全主机子网1108(例如,图8的安全主机子网808)。VCN 1106可以包括LPG 1110(例如,图8的LPG 810),该VCN 1106可以经由包含在SSH VCN 1112(例如,图8的SSH VCN 812)中的LPG 1110通信地耦合到SSH VCN 1112。SSH VCN 1112可以包括SSH子网1114(例如,图8的SSH子网814),并且SSH VCN 1112可以经由包含在控制平面VCN 1116(例如,图8的控制平面VCN 816)中的LPG 1110通信地耦合到控制平面VCN 1116并且经由包含在数据平面VCN1118(例如,图8的数据平面818)中的LPG 1110通信地耦合到数据平面VCN 1118。控制平面VCN 1116和数据平面VCN 1118可以包含在服务租赁1119(例如,图8的服务租赁819)中。

[0181] 控制平面VCN 1116可以包括可以包括(一个或多个)LB子网1122(例如,图8的(一个或多个)LB子网822)的控制平面DMZ层1120(例如,图8的控制平面DMZ层820)、可以包括(一个或多个)应用子网1126(例如,图8的(一个或多个)应用子网826)的控制平面应用层1124(例如,图8的控制平面应用层824)、可以包括(一个或多个)DB子网1130(例如,图8的(一个或多个)DB子网830)的控制平面数据层1128(例如,图8的控制平面数据层828)。包含在控制平面DMZ层1120中的(一个或多个)LB子网1122可以通信地耦合到包含在控制平面应用层1124中的(一个或多个)应用子网1126和可以包含在控制平面VCN 1116中的互联网网关1134(例如,图8的互联网网关834),并且(一个或多个)应用子网1126可以通信地耦合到包含在控制平面数据层1128中的(一个或多个)DB子网1130以及服务网关1136(例如,图8的服务网关)和网络地址转换(NAT)网关1138(例如,图8的NAT网关838)。控制平面VCN 1116可

以包括服务网关1136和NAT网关1138。

[0182] 数据平面VCN 1118可以包括数据平面应用层1146(例如,图8的数据平面应用层846)、数据平面DMZ层1148(例如,图8的数据平面DMZ层848)、以及数据平面数据层1150(例如,图8的数据平面数据层850)。数据平面DMZ层1148可以包括可以通信地耦合到数据平面应用层1146的(一个或多个)可信应用子网1160(例如,图8的(一个或多个)可信应用子网860)和(一个或多个)不可信应用子网1162(例如,图8的(一个或多个)不可信应用子网862)以及包含在数据平面VCN 1118中的互联网网关1134的(一个或多个)LB子网1122。(一个或多个)可信应用子网1160可以通信地耦合到包含在数据平面VCN 1118中的服务网关1136、包含在数据平面VCN 1118中的NAT网关1138以及包含在数据平面数据层1150中的(一个或多个)DB子网1130。(一个或多个)不可信应用子网1162可以通信地耦合到包含在数据平面VCN 1118中的服务网关1136和包含在数据平面数据层1150中的(一个或多个)DB子网1130。数据平面数据层1150可以包括可以通信地耦合到包含在数据平面VCN 1118中的服务网关1136的(一个或多个)DB子网1130。

[0183] (一个或多个)不可信应用子网1162可以包括可以通信地耦合到驻留在(一个或多个)不可信应用子网1162内的租户虚拟机(VM)1166(1)-(N)的主VNIC 1164(1)-(N)。每个租户VM 1166(1)-(N)可以运行相应容器1167(1)-(N)中的代码,并且可通信地耦合到可以包含在数据平面应用层1146中的应用子网1126,该数据平面应用层1146可以包含在容器出口VCN1168中。相应辅VNIC 1172(1)-(N)可以促进包含在数据平面VCN 1118中的(一个或多个)不可信应用子网1162和包含在容器出口VCN 1168中的应用子网之间的通信。容器出口VCN可以包括可以通信地耦合到公共互联网1154(例如,图8的公共互联网854)的NAT网关1138。

[0184] 包含在控制平面VCN 1116中以及包含在数据平面VCN 1118中的互联网网关1134可以通信地耦合到元数据管理服务1152(例如,图8的元数据管理系统852),该元数据管理服务1152可以通信地耦合到公共互联网1154。公共互联网1154可以通信地耦合到包含在控制平面VCN 1116中以及包含在数据平面VCN 1118中的NAT网关1138。包含在控制平面VCN 1116中以及包含在数据平面VCN 1118中的服务网关1136可以通信地耦合到云服务1156。

[0185] 在一些示例中,图11的框图1100的体系架构所示的模式可以被认为是图8的框图800的体系架构所示的模式的例外,并且在IaaS提供商不能直接与客户通信(例如,断开连接的区域)的情况下,这种模式可能是IaaS提供商的客户所期望的。客户可以实时访问每个客户的包含在VM 1166(1)-(N)中的相应容器1167(1)-(N)。容器1167(1)-(N)可以被配置为对包含在数据平面应用层1146的(一个或多个)应用子网1126中的相应辅VNIC 1172(1)-(N)进行调用,该数据平面应用层1146可以包含在容器出口VCN 1168中。辅VNIC 1172(1)-(N)可以将调用传输到NAT网关1138,该NAT网关1138可以将调用传输到公共互联网1154。在这个示例中,可以由客户实时访问的容器1167(1)-(N)可以与控制平面VCN 1116隔离,并且可以与包含在数据平面VCN 1118中的其它实体隔离。容器1167(1)-(N)也可以与来自其它客户的资源隔离。

[0186] 在其它示例中,客户可以使用容器1167(1)-(N)来调用云服务1156。在这个示例中,客户可以运行容器1167(1)-(N)中的从云服务1156请求服务的代码。容器1167(1)-(N)可以将该请求传输到辅VNIC 1172(1)-(N),该辅VNIC 1172(1)-(N)可以将请求传输到NAT

网关，该NAT网关可以将请求传输到公共互联网1154。公共互联网1154可以经由互联网网关1134将请求传输到包含在控制平面VCN 1116中的(一个或多个)LB子网1122。响应于确定请求有效，(一个或多个)LB子网可以将请求传输到(一个或多个)应用子网1126，该(一个或多个)应用子网1126可以经由服务网关1136将请求传输到云服务1156。

[0187] 应当认识到的是，各图中描绘的IaaS体系架构800、900、1000、1100可以具有除所描绘的组件之外的其它组件。另外，各图中所示的实施例仅仅是可以结合本公开的实施例的云基础设施系统的一些示例。在一些其它实施例中，IaaS系统可以具有比各图中所示更多或更少的组件、可以组合两个或更多个组件，或者可以具有不同的组件布置或配置。

[0188] 在某些实施例中，本文描述的IaaS系统可以包括以自助服务、基于订阅、弹性可伸缩、可靠、高度可用和安全的方式交付给客户的应用套件、中间件和数据库服务产品。此类IaaS系统的示例是本受让方提供的Oracle云基础设施(OCI)。

[0189] 图12图示了其中可以实现本公开的各种示例的示例计算机系统1200。系统1200可以用于实现上述任何计算机系统。如图所示，计算机系统1200包括经由总线子系统1202与多个外围子系统通信的处理单元1204。这些外围子系统可以包括处理加速单元1206、I/O子系统1208、存储子系统1218和通信子系统1224。存储子系统1218包括有形计算机可读存储介质1222和系统存储器1210。

[0190] 总线子系统1202提供用于让计算机系统1200的各种部件和子系统按意图彼此通信的机制。虽然总线子系统1202被示意性地示出为单条总线，但是总线子系统的替代实施例可以利用多条总线。总线子系统1202可以是若干种类型的总线结构中的任何一种，包括存储器总线或存储器控制器、外围总线、以及使用任何各种总线体系架构的局部总线。例如，这种体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线，其可以被实现为按IEEE P1386.1标准制造的Mezzanine总线。

[0191] 可以被实现为一个或多个集成电路(例如，常规微处理器或微控制器)的处理单元1204控制计算机系统1200的操作。一个或多个处理器可以被包括在处理单元1204中。这些处理器可以包括单核或多核处理器。在某些实施例中，处理单元1204可以被实现为一个或多个独立的处理单元1232和/或1234，其中在每个处理单元中包括单核或多核处理器。在其它实施例中，处理单元1204也可以被实现为通过将两个双核处理器集成到单个芯片中形成的四核处理单元。

[0192] 在各种实施例中，处理单元1204可以响应于程序代码执行各种程序并且可以维护多个并发执行的程序或进程。在任何给定的时间，要被执行的程序代码中的一些或全部代码可以驻留在(一个或多个)处理器1204中和/或存储子系统1218中。通过适当的编程，(一个或多个)处理器1204可以提供上述各种功能。计算机系统1200可以附加地包括处理加速单元1206，其可以包括数字信号处理器(DSP)、专用处理器，等等。

[0193] I/O子系统1208可以包括用户接口输入设备和用户接口输出设备。用户接口输入设备可以包括键盘、诸如鼠标或轨迹球的定点设备、结合到显示器中的触摸板或触摸屏、滚动轮、点击轮、拨盘、按钮、开关、键盘、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备可以包括例如运动感测和/或手势识别设备，诸如Microsoft **Kinect®** 运动传感器，其使得用户能够使用手势和语音命令通过自然用户接

口来控制诸如Microsoft**Xbox®**360游戏控制器的输入设备并与之交互。用户接口输入设备也可以包括眼睛姿势识别设备，诸如从用户检测眼睛活动(例如，当拍摄照片和/或做出菜单选择时的“眨眼”)并且将眼睛姿势转换为去往输入设备(例如，Google**Glass®**)的输入的Google**Glass®**眨眼检测器。此外，用户接口输入设备可以包括使用户能够通过语音命令与语音识别系统(例如，**Siri®**导航器)交互的语音识别感测设备。

[0194] 用户接口输入设备也可以包括但不限于三维(3D)鼠标、操纵杆或指向棒、游戏面板和绘图板、以及音频/视频设备，诸如扬声器、数码相机、数码摄录机、便携式媒体播放器、网络摄像头、图像扫描仪、指纹扫描仪、条形码阅读器3D扫描仪、3D打印机、激光测距仪和视线跟踪设备。此外，用户接口输入设备可以包括例如医学成像输入设备，诸如计算机断层扫描、磁共振成像、正电子发射断层摄影术、医疗超声设备。用户接口输入设备也可以包括例如音频输入设备，诸如MIDI键盘、数字乐器等。

[0195] 用户接口输出设备可以包括显示子系统、指示灯，或者诸如音频输出设备的非可视显示器等。显示子系统可以是阴极射线管(CRT)、诸如使用液晶显示器(LCD)或等离子显示器的平板设备、投影设备、触摸屏等。一般而言，术语“输出设备”的使用意在包括用于从计算机系统1200向用户或其它计算机输出信息的所有可能类型的设备和机制。例如，用户接口输出设备可以包括但不限于可视地传达文本、图形和音频/视频信息的各种显示设备，诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备、以及调制解调器。

[0196] 计算机系统1200可以包括包含软件元件、被示为当前位于系统存储器1210内的存储子系统1218。系统存储器1210可以存储在处理单元1204上可执行且可加载的程序指令，以及在这些程序的执行期间所产生的数据。

[0197] 取决于计算机系统1200的配置和类型，系统存储器1210可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存存储器等)。RAM通常包含可被处理单元1204立即访问和/或目前正被处理单元1204操作和执行的数据和/或程序模块。在一些实施方案中，系统存储器1210可以包括多种不同类型的存储器，诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。在一些实施方案中，包含有助于在诸如启动期间在计算机系统1200内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以被存储在ROM中。作为示例而非限制，系统存储器1210也示出了可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等的应用程序1212、程序数据1214、以及操作系统1216。作为示例，操作系统1216可以包括各种版本的Microsoft **Windows®**、Apple**Macintosh®**和/或Linux操作系统、各种可商业获得的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google**Chrome®**OS等)和/或诸如iOS、**Windows®**Phone、**Android®**OS、**BlackBerry®**10OS和**Palm®**OS操作系统的移动操作系统。

[0198] 存储子系统1218也可以提供用于存储提供一些实施例的功能的基本编程和数据构造的有形计算机可读存储介质。当被处理器执行时提供上述功能的软件(程序、代码模块、指令)可以被存储在存储子系统1218中。这些软件模块或指令可以被处理单元1204执行。存储子系统1218也可以提供用于存储根据本公开使用的数据的储存库。

[0199] 存储子系统1200也可以包括可被进一步连接到计算机可读存储介质1222的计算机可读存储介质读取器1220。与系统存储器1210一起，并且可选地与其相结合，计算机可读存储介质1222可以全面地表示用于临时和/或更持久地包含、存储、传输和检索计算机可读信息的远程、本地、固定和/或可移除的存储设备加存储介质。

[0200] 包含代码或代码的部分的计算机可读存储介质1222也可以包括本领域已知或使用的任何适当的介质，包括存储介质和通信介质，诸如但不限于：以用于信息的存储和/或传输的任何方法或技术实现的易失性和非易失性、可移除和不可移除的介质。这可以包括有形的计算机可读存储介质，诸如RAM、ROM、电可擦除可编程ROM(EEPROM)、闪存存储器或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光学存储装置、磁带盒、磁带、磁盘存储装置或其它磁存储设备，或者其它有形的计算机可读介质。这也可以包括非有形的计算机可读介质，诸如数据信号、数据传输、或者可以用于传输期望信息并且可以被计算系统1200访问的任何其它介质。

[0201] 举例来说，计算机可读存储介质1222可以包括从不可移除的非易失性磁介质读取或写到其的硬盘驱动器、从可移除的非易失性磁盘读取或写到其的磁盘驱动器、以及从可移除的非易失性光盘(诸如CD ROM、DVD和Blu-**Ray®**盘或其它光学介质)读取或写到其的光盘驱动器。计算机可读存储介质1222可以包括但不限于：**Zip®**驱动器、闪存卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质1222也可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态ROM等)、基于易失性存储器的SSD(诸如基于固态RAM、动态RAM、静态RAM、DRAM的SSD)、磁阻RAM(MRAM)SSD、以及使用基于DRAM的SSD和基于闪存存储器的SSD的组合的混合SSD。盘驱动器及其关联的计算机可读介质可以为计算机系统1200提供计算机可读指令、数据结构、程序模块及其它数据的非易失性存储。

[0202] 通信子系统1224提供到其它计算机系统和网络的接口。通信子系统1224用作用于从其它系统接收数据和从计算机系统1200向其它系统传输数据的接口。例如，通信子系统1224可以使计算机系统1200能够经由互联网连接到一个或多个设备。在一些实施例中，通信子系统1224可以包括用于访问无线语音和/或数据网络的射频(RF)收发器部件(例如，使用蜂窝电话技术、诸如3G、4G或EDGE(用于全球演进的增强型数据速率)的先进数据网络技术、WiFi(IEEE 802.11系列标准)、或其它移动通信技术、或其任何组合)、全球定位系统(GPS)接收器部件和/或其它部件。在一些实施例中，通信子系统1224可以提供有线网络连接(例如，以太网)，作为无线接口的附加或者替代。

[0203] 在一些实施例中，通信子系统1224也可以代表可以使用计算机系统1200的一个或多个用户接收结构化和/或非结构化的数据馈送1226、事件流1228、事件更新1230等形式的输入通信。

[0204] 举例来说，通信子系统1224可以被配置为实时地从社交网络和/或其它通信服务的用户接收数据馈送1226，诸如**Twitter®**馈送、**Facebook®**更新、诸如丰富站点摘要(RSS)馈送的web馈送和/或来自一个或多个第三方信息源的实时更新。

[0205] 此外，通信子系统1224也可以被配置为接收连续数据流形式的数据，这可以包括本质上可以是连续的或无界的没有明确终止的实时事件的事件流1228和/或事件更新

1230。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如,网络监视和流量管理应用)、点击流分析工具、汽车流量监视等。

[0206] 通信子系统1224也可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送1226、事件流1228、事件更新1230等,该一个或多个数据库可以与耦合到计算机系统1200的一个或多个流式传输数据源计算机进行通信。

[0207] 计算机系统1200可以是各种类型之一,包括手持便携式设备(例如,iPhone®蜂窝电话、iPad®计算平板电脑、PDA)、可穿戴设备(例如,Google Glass®头戴式显示器)、PC、工作站、大型机、信息站、服务器机架、或任何其它数据处理系统。

[0208] 由于计算机和网络的不断变化的本质,在图中绘出的计算机系统1200的描述仅仅旨在作为具体的示例。具有比图中绘出的系统更多或更少部件的许多其它配置是可能的。例如,定制的硬件也可以被使用和/或特定的元素可以用硬件、固件、软件(包括小应用程序(applets))或组合来实现。另外,可以采用到诸如网络输入/输出设备之类的其它计算设备的连接。基于本文提供的公开内容和教导,本领域普通技术人员将认识到实现各种实施例的其它方式和/或方法。

[0209] 本申请中描述的任何软件组件或功能可以被实现为由处理器执行的软件代码,该处理器使用任何合适的计算机语言(诸如例如,Java、C++或Perl),使用例如常规的或面向对象的技术。软件代码可以作为一系列指令或命令存储在计算机可读介质上用于存储和/或传输,合适的介质包括随机存取存储器(RAM)、只读存储器(ROM)、诸如硬盘驱动器或软盘之类的磁介质、或者诸如光盘(CD)或DVD(数字多功能盘)之类的光学介质、闪存等。计算机可读介质可以是此类存储或传输设备的任何组合。

[0210] 还可以使用适合于经由符合各种协议(包括互联网)的有线、光纤和/或无线网络传输的载波信号来编码和传输这样的程序。因此,可以使用利用此类程序编码的数据信号来创建根据本公开的实施例的计算机可读介质。用程序代码编码的计算机可读介质可以与兼容设备一起包装或者与其它设备分开提供(例如,经由互联网下载)。任何这样的计算机可读介质可以驻留在单个计算机程序产品(例如,硬盘驱动器或整个计算机系统)上或驻留在其内部,并且可以存在于系统或网络内的不同计算机程序产品上或其内部。计算机系统可以包括监视器、打印机或用于向用户提供本文提到的任何结果的其它合适的显示器。

[0211] 虽然已经描述了本公开的具体实施例,但是各种修改、变更、替代构造和等效形式也包含在本公开的范围内。本公开的实施例不限于在某些特定数据处理环境内操作,而是可以在多个数据处理环境内自由操作。此外,虽然已经使用特定系列的事务和步骤描述了本公开的实施例,但是本领域技术人员应该清楚本公开的范围不限于所描述系列的事务和步骤。上述实施例的各种特征和方面可以单独或联合使用。

[0212] 另外,虽然已经使用硬件和软件的特定组合描述了本公开的实施例,但是应当认识到硬件和软件的其它组合也在本公开的范围内。本公开的实施例可以仅用硬件、或仅用软件、或使用它们的组合来实现。本文描述的各种处理可以以任何组合在相同的处理器或在不同的处理器上实现。因而,在组件或模块被描述为被配置为执行某些操作的情况下,可以通过例如设计电子电路来执行操作、通过对可编程电子电路(诸如微处理器)进行编程来执行操作、或通过其任何组合来完成这样的配置。处理可以使用多种技术进行通信,包括但不限于用于进程间通信的常规技术,并且不同的进程对可以使用不同的技术,或者同一进

程对可以在不同时间使用不同的技术。

[0213] 因而，说明书和附图被认为是说明性的而不是限制性的意义。但是，在不脱离权利要求中阐述的更广泛的精神和范围的情况下，显然可以对其进行添加、减少、删除和其它修改和改变。因此，虽然已经描述了具体的公开实施例，但这些并不旨在进行限制。各种修改和等效形式都在以下权利要求的范围内。

[0214] 在描述所公开的实施例的上下文中(尤其在以下权利要求的上下文中)使用术语“一”和“一个”和“该”以及类似的指称应被解释为涵盖单数和复数两者，除非本文另有指示或与上下文明显矛盾。除非另有说明，否则术语“包括”、“具有”、“包含”和“含有”应被解释为开放式术语(即，意思是“包括但不限于”)。术语“连接”应被解释为部分或全部包含在内、附接到或连接在一起，即使中间存在一些东西。除非本文另有指示，否则本文中的值范围的描述仅旨在用作单独引用落入该范围内的每个单独值的简略方法，并且每个单独值被并入说明书中，就好像它在本文中单独描述一样。除非本文另有指示或与上下文明显矛盾，否则本文描述的所有方法都可以以任何合适的顺序执行。除非另有声明，否则本文提供的任何和全部示例或示例性语言(例如，“诸如”)的使用仅旨在更好地阐明本公开的实施例并且不对本公开的范围构成限制。说明书中的任何语言都不应被解释为指示任何未要求保护的元素对于本公开的实践是必不可少的。

[0215] 除非另有明确说明，否则析取(disjunctive)语言(诸如短语“X、Y或Z中的至少一个”)旨在在上下文中被理解为用作一般地表示项目、术语等可以是X、Y或Z中的任一者或者是它们的任何组合(例如，X、Y和/或Z)。因此，这种析取语言通常不旨在也不应暗示某些实施例需要X中的至少一个、Y中的至少一个或Z中的至少一个各自存在。

[0216] 本文描述了本公开的优选实施例，包括发明者已知用于实施本公开的最佳模式。这些优选实施例的变型对于本领域普通技术人员在阅读前述描述后会变得显而易见。发明者期望技术人员适当地采用这样的变型并且发明者旨在以不同于本文具体描述的方式来实践本公开。因而，本公开包括在适用法律允许的情况下对所附权利要求中记载的主题的所有修改和等效形式。此外，除非在本文中另有指示或与上下文明显矛盾，否则本公开包括上述元素在其所有可能的变型中的任何组合。

[0217] 本文引用的所有参考文献(包括出版物、专利申请和专利)均以相同的程度通过引用并入本文，就好像指示每个参考文献单独且具体地通过引用并入并且在本文中全文阐述一样。

[0218] 在前述的说明书中，本公开的各方面参考其具体实施例进行了描述，但本领域技术人员将认识到的是，本公开不限于此。上述公开的各个特征和方面可以被单独或联合使用。此外，在不脱离本说明书的更广泛精神和范围的情况下，实施例可以在除本文所述的环境和应用之外的任何数量的环境和应用中被使用。因而，本说明书和附图应当被认为是说明性而不是限制性的。

[0219] 在不脱离本公开的实施例的精神和范围的情况下，特定实施例的具体细节可以以任何合适的方式组合或者与本文所示和描述的细节不同。

[0220] 出于说明和描述的目的已经给出了本公开的示例性实施例的以上描述。其并非旨在是详尽的或将本公开限制到所描述的精确形式，并且根据以上教导，许多修改和变化是可能的。选择和描述实施例是为了最好地解释本公开的原理及其实际应用，从而使得本领

域其他技术人员能够在各种示例中以及通过适合于所设想的特定用途的各种修改来最好地利用本公开。

[0221] 本文引用的所有出版物、专利和专利申请均出于所有目的通过引用全文并入本文。

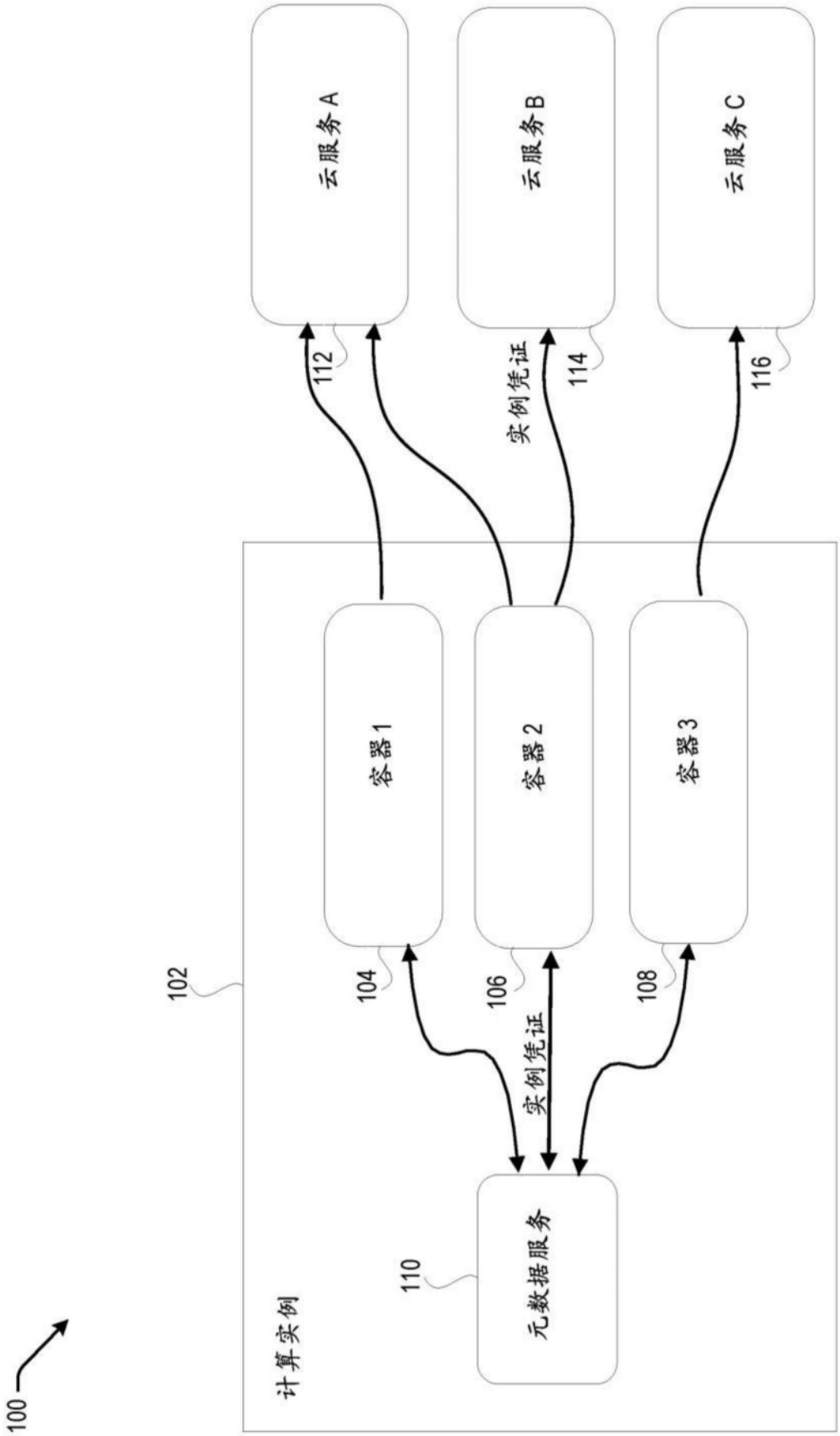

100
计算实例
102
元数据服务
110
容器1
容器2
容器3
104
106
108
实例凭证
实例凭证
云服务A
云服务B
云服务C
112
114
116

图1

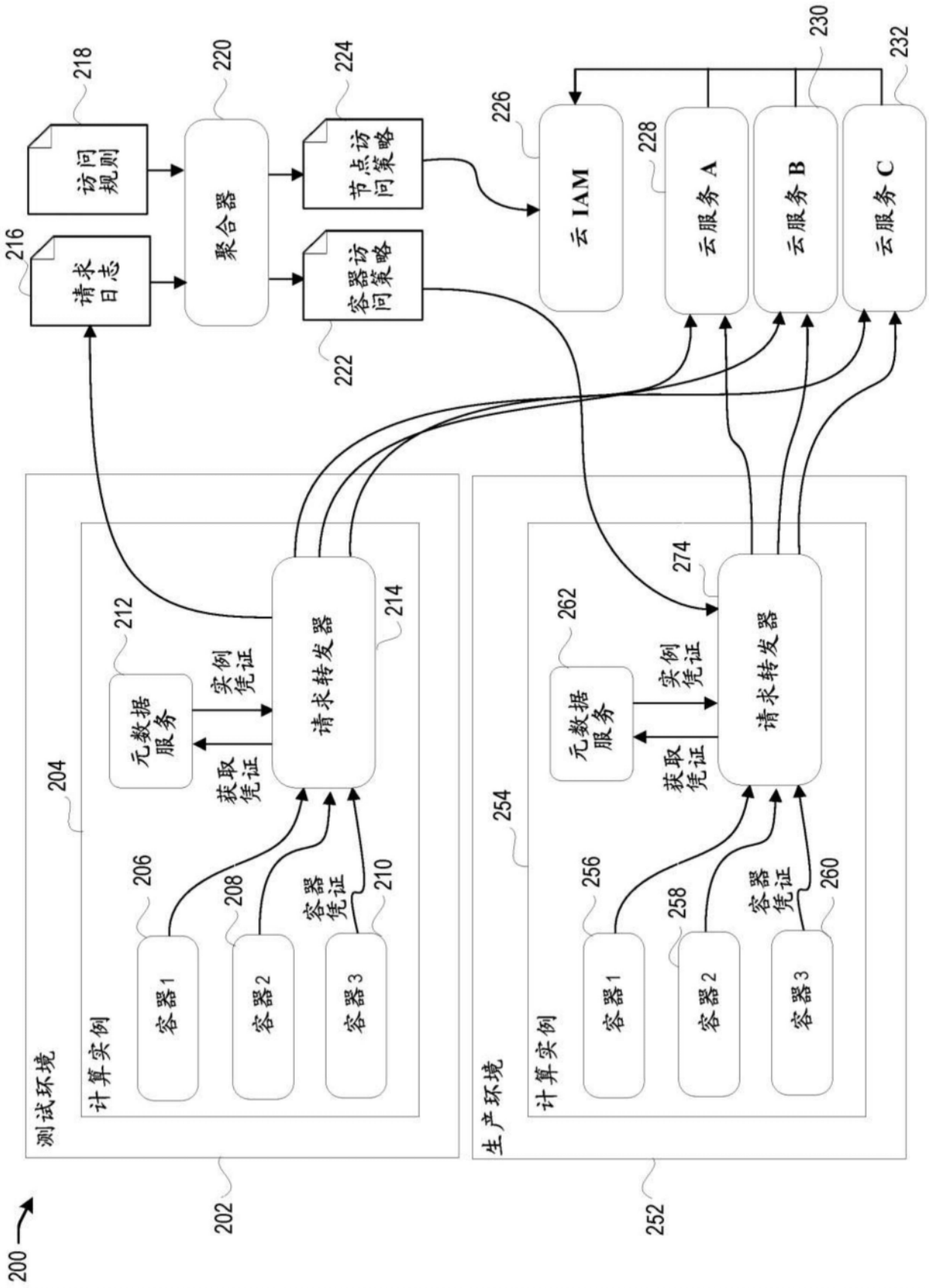

200
202
252
测试环境
计算实例
容器1
容器2
容器3
206
208
210
容器凭证
204
212
元数据服务
获取凭证
实例凭证
请求转发器
214
216
请求日志
218
访问规则
220
聚合器
222
容器访问策略
224
节点访问策略
226
云IAM
228
云服务A
230
云服务B
232
云服务C
生产环境
计算实例
容器1
容器2
容器3
256
258
260
容器凭证
254
262
元数据服务
获取凭证
实例凭证
请求转发器
274

图2

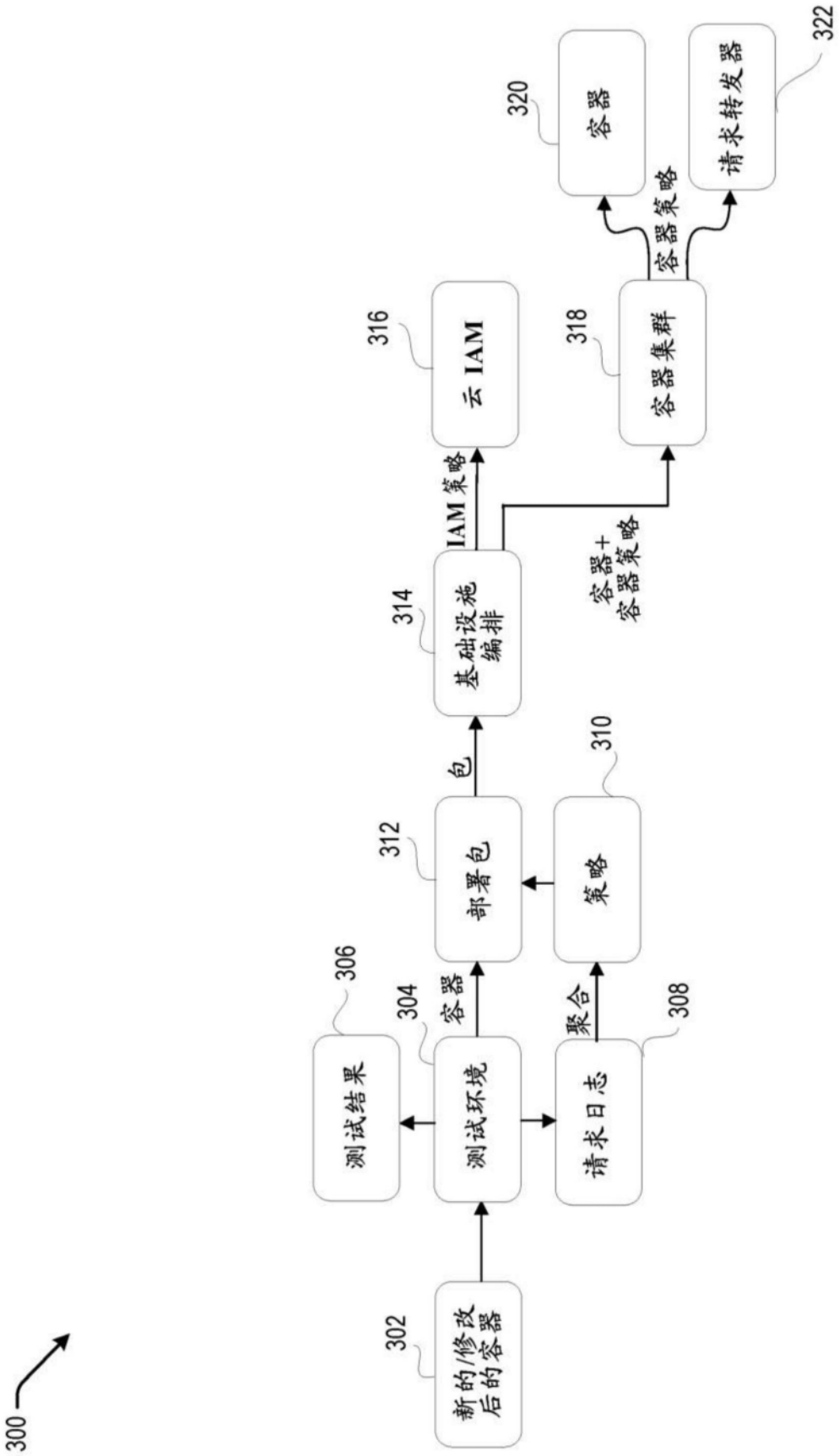

300
新的/修改后的容器
302
测试结果
306
测试环境
304
请求日志
308
容器
聚合
部署包
312
策略
310
包
基础设施编排
314
IAM策略
容器+容器策略
云 IAM
316
容器集群
318
容器策略
容器
320
请求转发器
322

图3

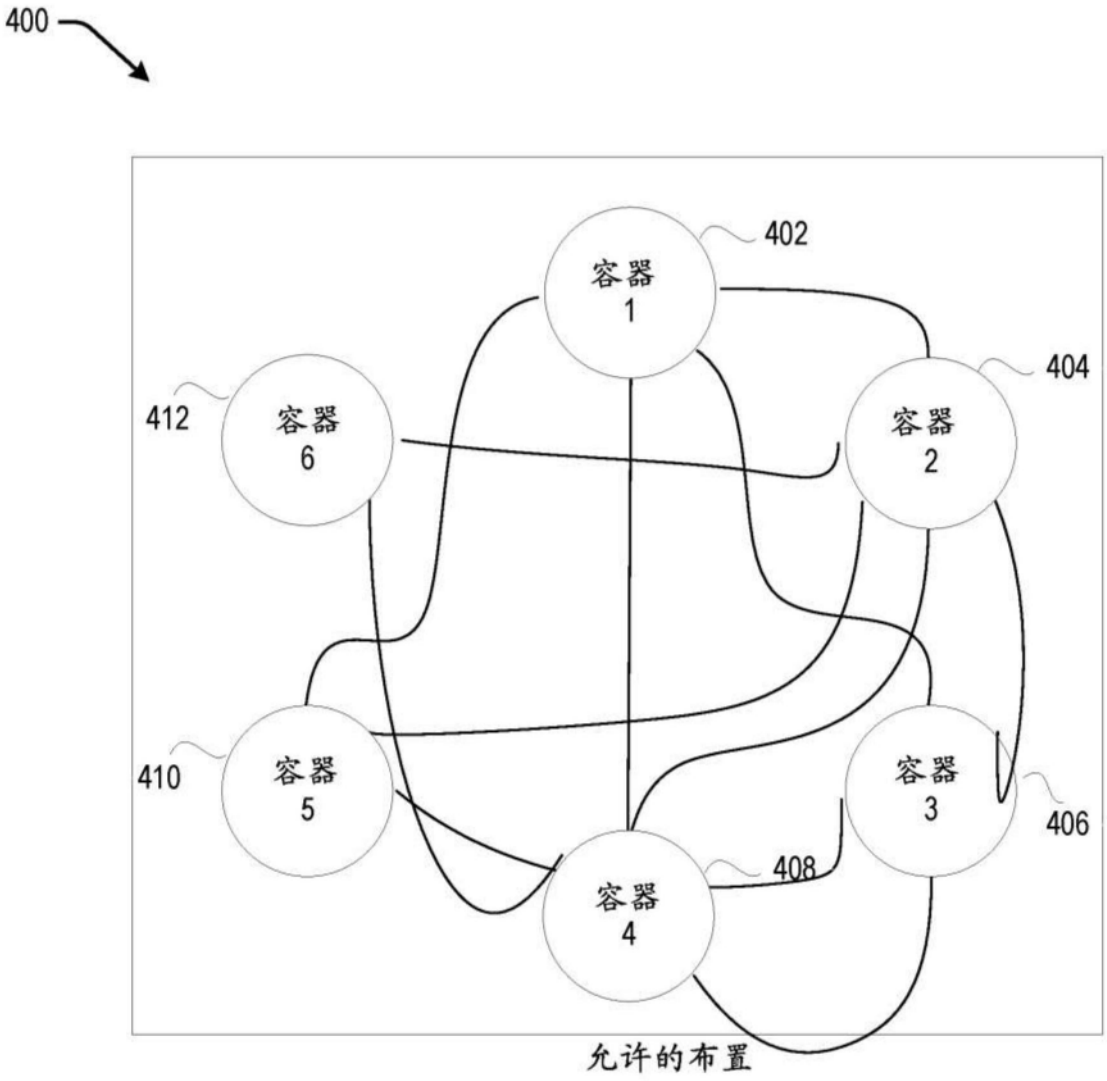



图4

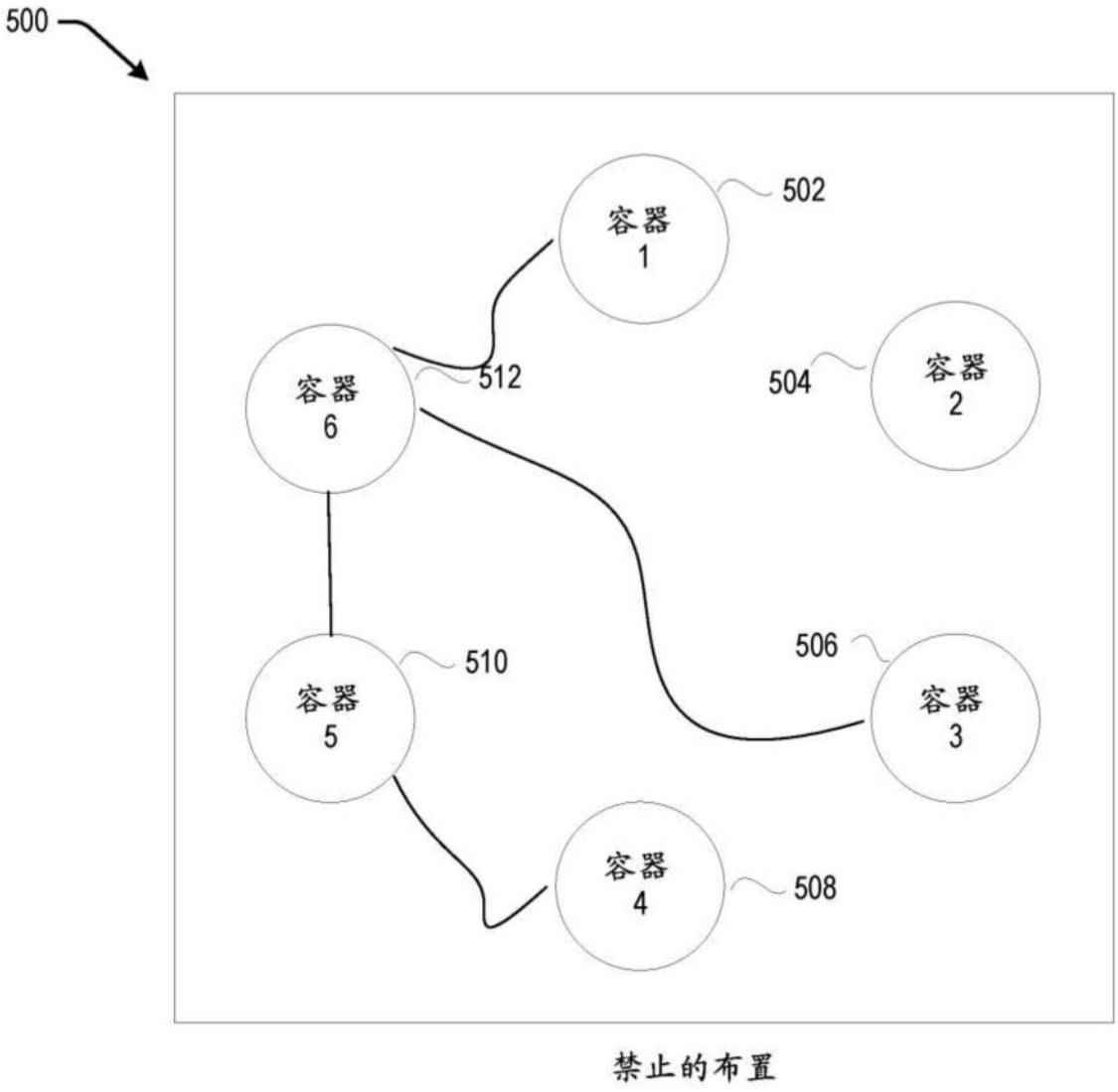



图5

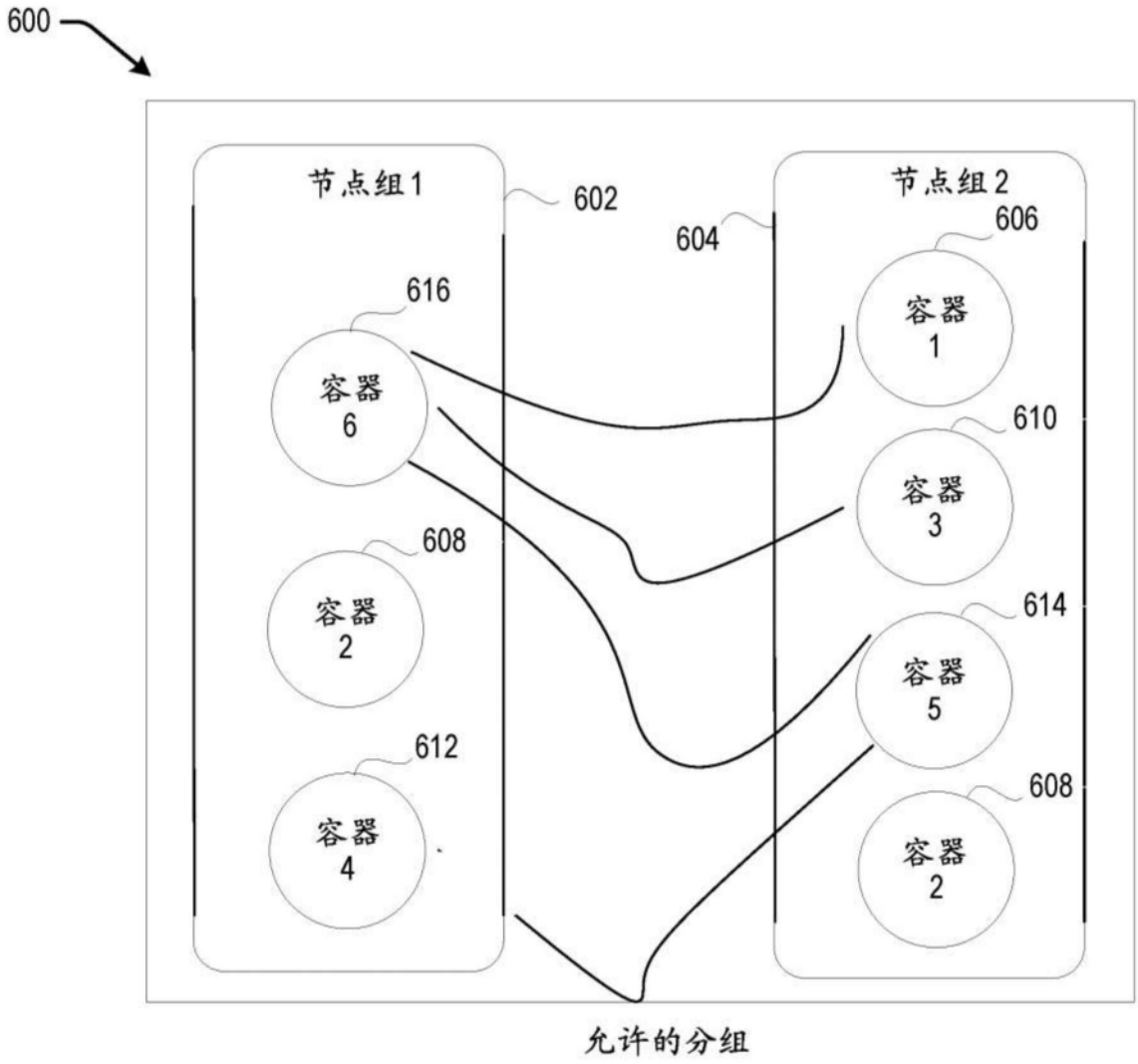

600
节点组1
602
604
节点组2
606
616
容器 6
容器 1
610
容器 3
608
容器 2
614
容器 5
612
容器 4
608
容器 2
允许的分组

图6

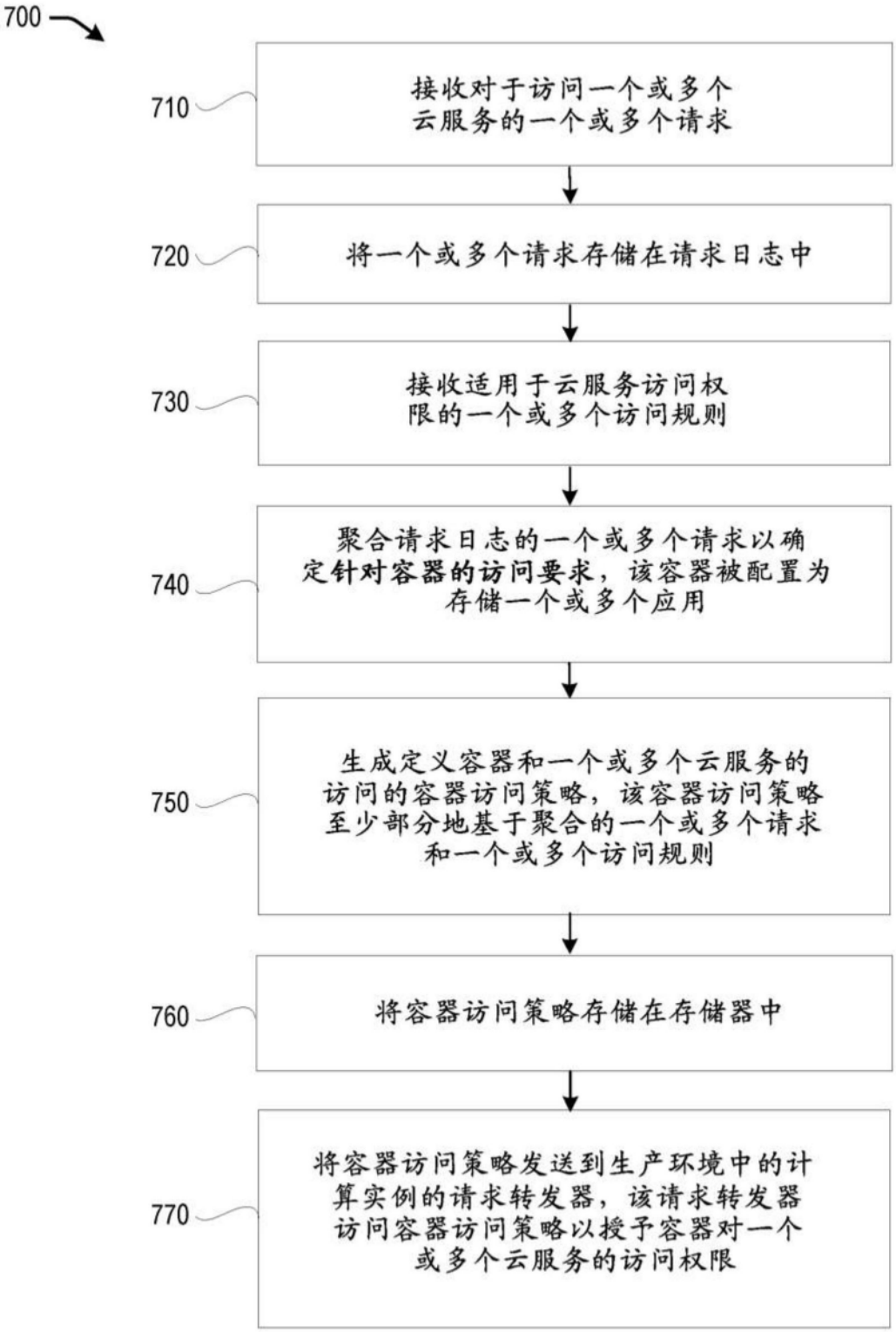

700
710
接收对于访问一个或多个云服务的一个或多个请求
720
将一个或多个请求存储在请求日志中
730
接收适用于云服务访问权限的一个或多个访问规则
740
聚合请求日志的一个或多个请求以确定针对容器的访问要求，该容器被配置为存储一个或多个应用
750
生成定义容器和一个或多个云服务的访问的容器访问策略，该容器访问策略至少部分地基于聚合的一个或多个请求和一个或多个访问规则
760
将容器访问策略存储在存储器中
770
将容器访问策略发送到生产环境中的计算实例的请求转发器，该请求转发器访问容器访问策略以授予容器对一个或多个云服务的访问权限

图7

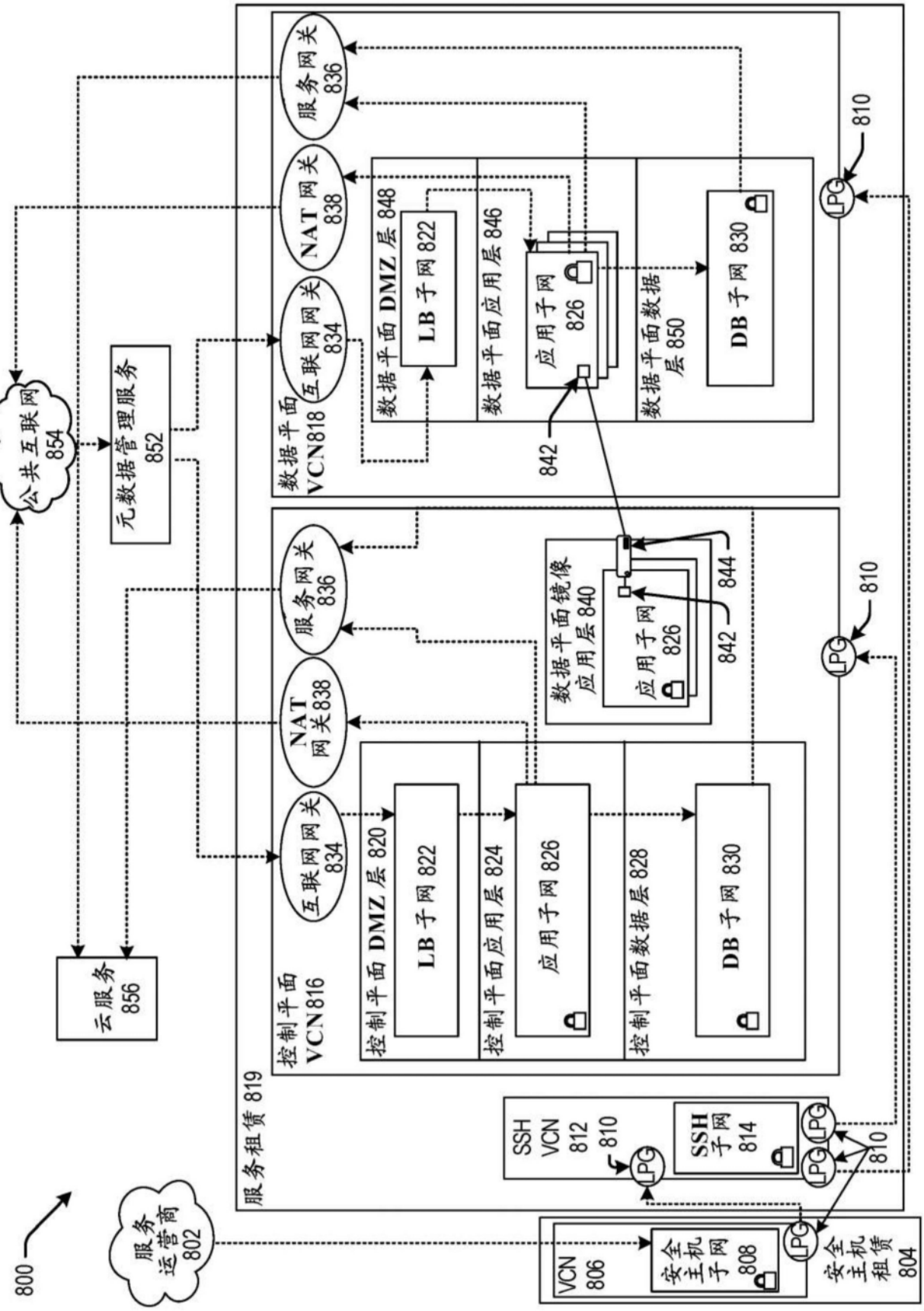

800
服务运营商 802
服务租赁 819
公共互联网 854
元数据管理服务 852
云服务 856
控制平面 VCN816
互联网网关 834
NAT 网关838
服务网关 836
控制平面 DMZ 层 820
LB 子网 822
控制平面应用层 824
应用子网 826
控制平面数据层 828
DB 子网 830
数据平面镜像应用层 840
842
844
数据平面 VCN818
互联网网关 834
NAT 网关 838
服务网关 836
数据平面 DMZ 层 848
LB 子网 822
数据平面应用层 846
应用子网 826
数据平面数据层 850
DB 子网 830
SSH VCN 812
SSH 子网 814
VCN 806
安全主机子网 808
安全主机租赁 804
LPG
810

图8

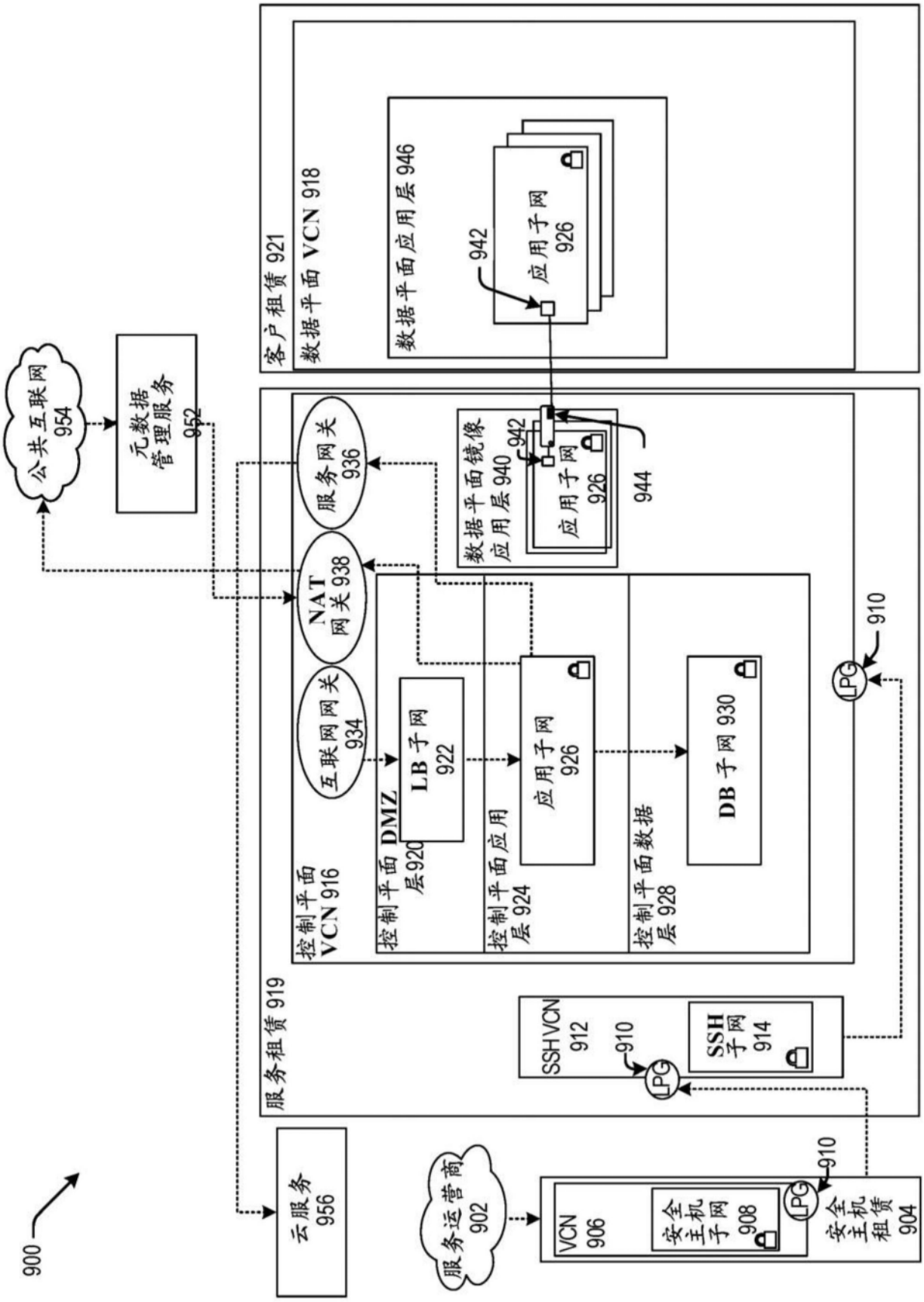

900
公共互联网 954
元数据管理服务 952
客户租赁 921
数据平面 VCN 918
数据平面应用层 946
942
应用子网 926
数据平面镜像应用层 940
942
应用子网 926
944
服务网关 936
NAT 网关 938
互联网网关 934
服务租赁 919
控制平面 VCN 916
控制平面 DMZ 层 920
LB 子网 922
控制平面应用层 924
应用子网 926
控制平面数据层 928
DB 子网 930
910
LPG
SSH VCN 912
910
LPG
SSH 子网 914
云服务 956
服务运营商 902
VCN 906
安全主机子网 908
910
LPG
安全主机租赁 904

图9

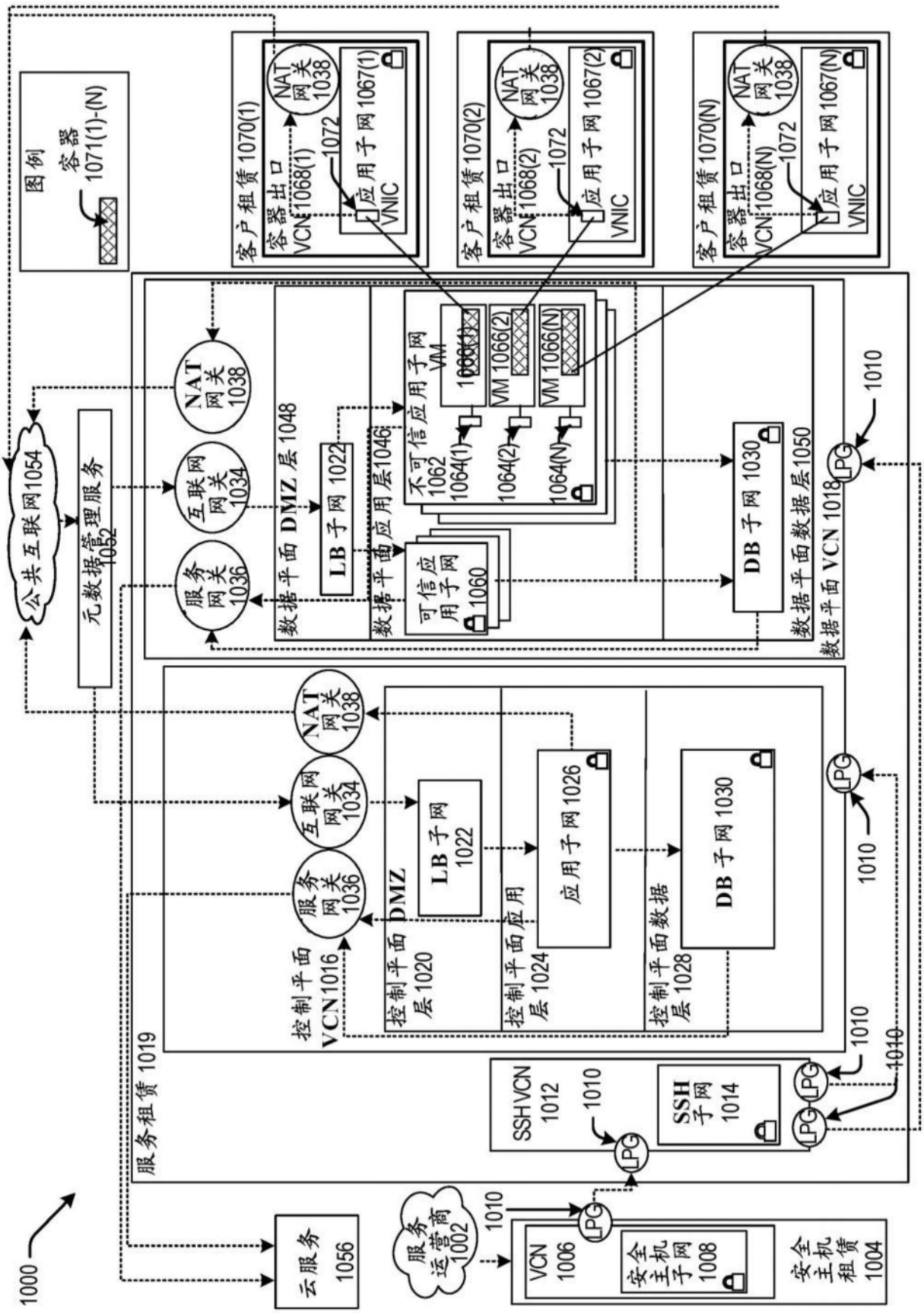

图例
容器 1071(1)-(N)
客户租赁 1070(1)
客户租赁 1070(2)
客户租赁 1070(N)
容器出口 VCN 1068(1)
容器出口 VCN 1068(2)
容器出口 VCN 1068(N)
NAT 网关 1038
应用子网 1067(1) VNIC
应用子网 1067(2) VNIC
应用子网 1067(N) VNIC
1072
公共互联网 1054
元数据管理服务 1052
互联网网关 1034
服务网关 1036
数据平面 DMZ 层 1048
LB 子网 1022
数据平面应用层 1046
可信应用子网 1060
不可信应用子网 VM 1062
VM 1066(1)
VM 1066(2)
VM 1066(N)
1064(1)
1064(2)
1064(N)
DB 子网 1030
数据平面数据层 1050
数据平面 VCN 1018
1010
LPG
服务租赁 1019
控制平面 VCN 1016
控制平面 DMZ 层 1020
控制平面应用层 1024
控制平面数据层 1028
应用子网 1026
SSH VCN 1012
SSH 子网 1014
服务运营商 1002
VCN 1006
安全主机子网 1008
安全主机租赁 1004
云服务 1056
1000

图10

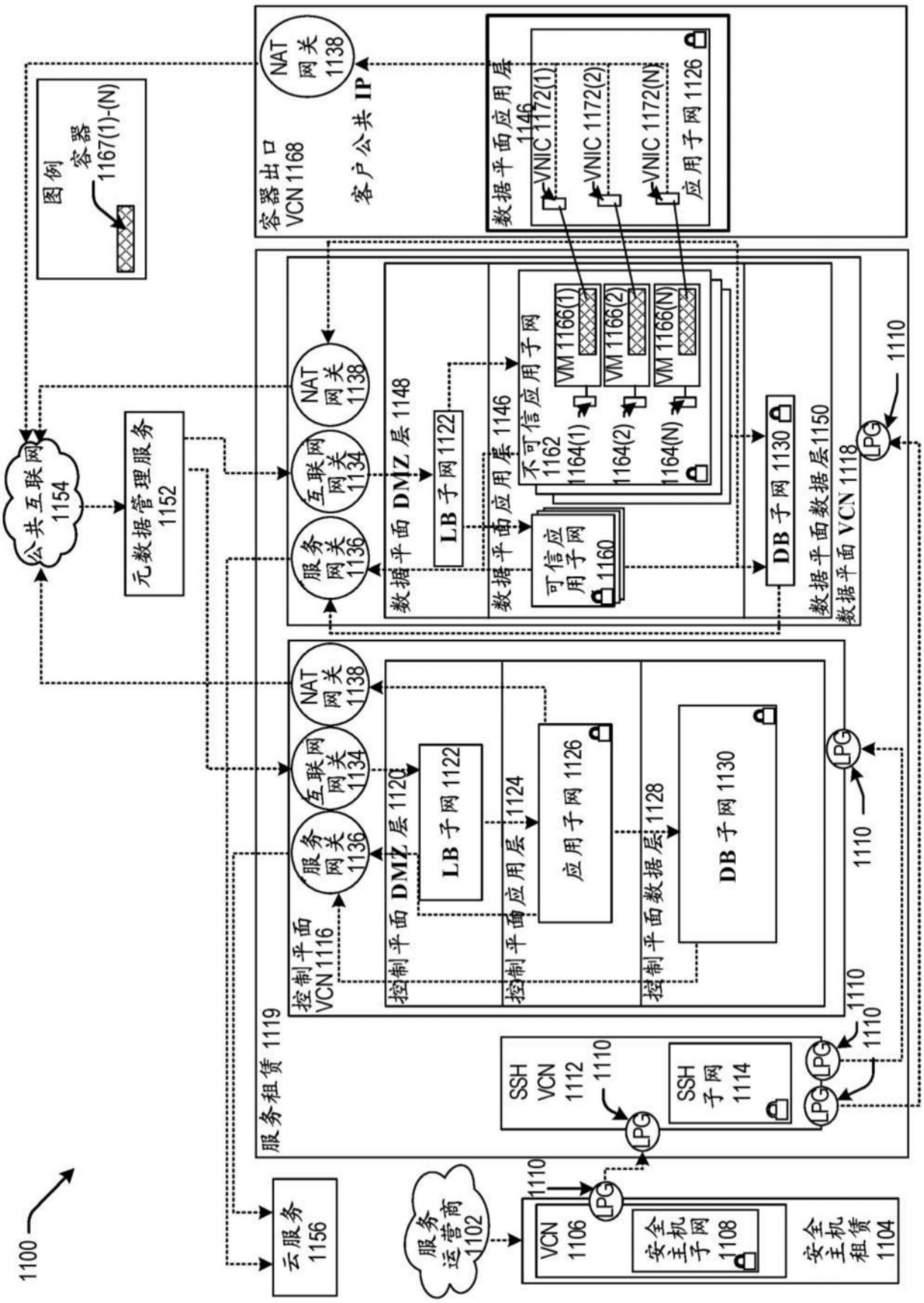

1100
图例
容器 1167(1)-(N)
公共互联网 1154
元数据管理服务 1152
云服务 1156
服务运营商 1102
服务租赁 1119
容器出口 VCN 1168
客户公共 IP
NAT 网关 1138
互联网网关 1134
服务网关 1136
数据平面应用层 1146
VNIC 1172(1)
VNIC 1172(2)
VNIC 1172(N)
应用子网 1126
数据平面 DMZ 层 1148
LB 子网 1122
不可信应用子网 1162
VM 1166(1)
VM 1166(2)
VM 1166(N)
1164(1)
1164(2)
1164(N)
可信应用子网 1160
DB 子网 1130
数据平面数据层 1150
数据平面 VCN 1118
1110
控制平面 VCN 1116
控制平面 DMZ 层 1120
控制平面应用层 1124
控制平面数据层 1128
SSH VCN 1112
SSH 子网 1114
LPG
VCN 1106
安全主机子网 1108
安全主机租赁 1104

图11

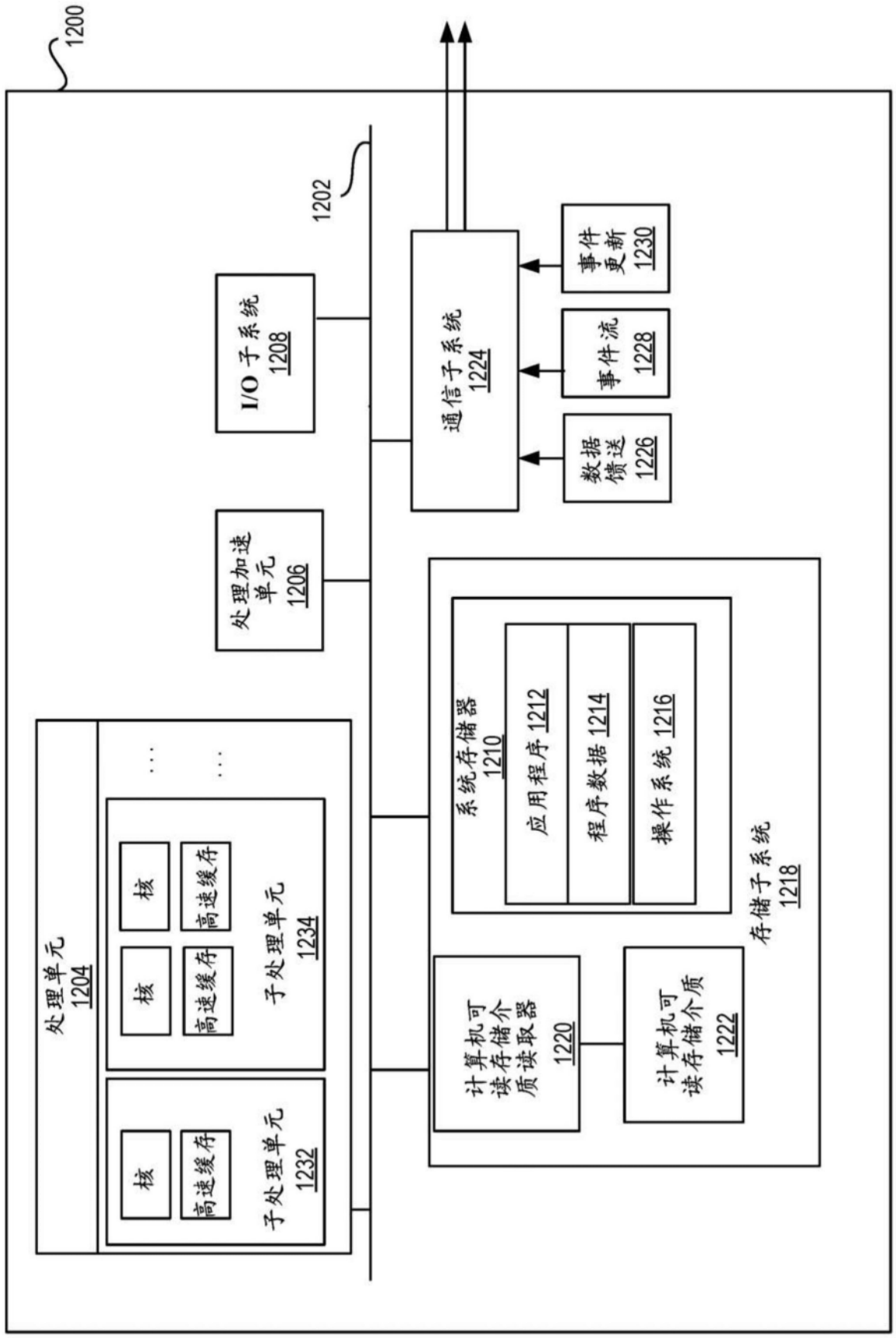

1200
1202
I/O 子系统 1208
处理加速单元 1206
通信子系统 1224
事件更新 1230
事件流 1228
数据馈送 1226
处理单元 1204
子处理单元 1232
核
高速缓存
子处理单元 1234
核
高速缓存
核
高速缓存
系统存储器 1210
应用程序 1212
程序数据 1214
操作系统 1216
存储子系统 1218
计算机可读存储介质读取器 1220
计算机可读存储介质 1222

图12