(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119173871 A
(43)申请公布日 2024.12.20

(21)申请号 202380039552.0

(22)申请日 2023.05.02

(30)优先权数据
17/742,472 2022.05.12 US

(85)PCT国际申请进入国家阶段日
2024.11.11

(86)PCT国际申请的申请数据
PCT/US2023/020663 2023.05.02

(87)PCT国际申请的公布数据
WO2023/219829 EN 2023.11.16

(71)申请人 甲骨文国际公司
地址 美国

(72)发明人 H·K·凯利 S·瓦维拉帕利

(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 刘前红

(51)Int.Cl.
G06F 21/62(2006.01)
H04L 9/40(2006.01)

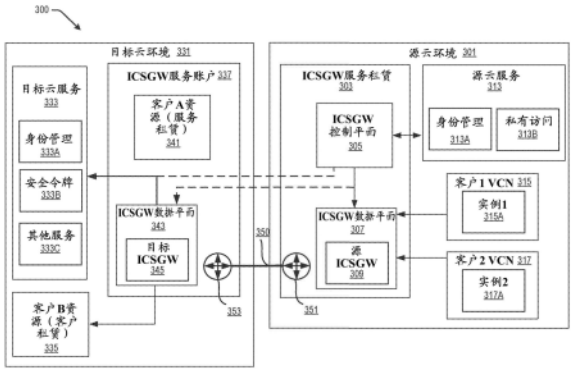
权利要求书3页 说明书22页 附图12页

(54)发明名称

云间服务网关

(57)摘要

本文讨论了针对在源云环境中部署的资源促进对在目标云环境中提供的服务的访问的框架。源云环境不同于并且独立于目标云环境。在源云环境中执行的计算实例生成使用目标云环境中提供的服务的请求。该请求通过云间服务网关从源云环境传送到目标云环境。基于与计算实例相关联的访问角色在目标云环境中执行该服务。



CN 119173871 A

1.一种方法,包括:

由在源云环境中执行的计算实例生成使用在目标云环境中提供的服务的请求,所述源云环境不同于所述目标云环境;

经由云间服务网关将所述请求从所述源云环境传送到所述目标云环境;以及

基于与所述计算实例相关联的访问角色在所述目标云环境中执行所述服务。

2.根据权利要求1所述的方法,还包括:

由所述计算实例将所述请求发送到设置在所述源云环境中的源云间服务网关,所述请求包括与所述计算实例相关联的身份主体;以及

由所述源云间服务网关验证所述计算实例的所述身份主体。

3.根据权利要求2所述的方法,其中验证所述身份主体包括核实所述计算实例是否被准许访问所述目标云环境中的所述服务。

4.根据权利要求2所述的方法,还包括:

响应于所述身份主体被成功验证,由所述源云间服务网关从存储在所述源云环境中的预配置信息中获得与所述计算实例相关联的所述访问角色。

5.根据权利要求4所述的方法,还包括:

响应于所述身份主体被成功验证,由所述源云间服务网关修改所述请求以生成经修改请求,其中所述修改包括移除所述请求的元数据中包括的所述身份主体,以及将与所述计算实例相关联的所述访问角色合并到所述元数据中;以及

由所述源云间服务网关将所述经修改请求发送给设置在所述目标云环境中的目标云间服务网关。

6.根据权利要求5所述的方法,其中所述源云间服务网关设置在所述源云环境的第一数据平面中,并且所述目标云间服务网关设置在所述目标云环境的第二数据平面中,所述源云间服务网关经由可信通信通道通信地耦合到所述目标云间服务网关。

7.根据权利要求5所述的方法,还包括:

由所述目标云间服务网关从所述经修改请求中提取与所述计算实例相关联的所述访问角色;以及

由所述目标云间服务网关从所述目标云环境中包括的管理服务获得与所述访问角色相关联的令牌。

8.根据权利要求7所述的方法,还包括:

由所述目标云间服务网关用与所述访问角色相关联的所述令牌对所述经修改请求进行签名,以形成被签名的经修改请求;以及

将所述被签名的经修改请求转发到期望由所述计算实例使用的所述服务。

9.根据权利要求8所述的方法,还包括:

由所述服务基于所述令牌来验证所述被签名的经修改请求;以及

响应于成功验证,由所述服务执行所述请求。

10.一种存储特定计算机可执行指令的计算机可读介质,所述特定计算机可执行指令在由处理器执行时使计算机系统至少:

由在源云环境中执行的计算实例生成使用在目标云环境中提供的服务的请求,所述源云环境不同于所述目标云环境;

经由云间服务网关将所述请求从所述源云环境传送到所述目标云环境;以及

基于与所述计算实例相关联的访问角色在所述目标云环境中执行所述服务。

11.根据权利要求10所述的存储特定计算机可执行指令的计算机可读介质,其中所述计算机系统还被配置为:

由所述计算实例将所述请求发送到设置在所述源云环境中的源云间服务网关,所述请求包括与所述计算实例相关联的身份主体;以及

由所述源云间服务网关验证所述计算实例的所述身份主体。

12.根据权利要求11所述的存储特定计算机可执行指令的计算机可读介质,其中验证所述身份主体包括核实所述计算实例是否被准许访问所述目标云环境中的所述服务。

13.根据权利要求11所述的存储特定计算机可执行指令的计算机可读介质,其中所述计算机系统还被配置为:

响应于所述身份主体被成功验证,由所述源云间服务网关从存储在所述源云环境中的预配置信息中获得与所述计算实例相关联的所述访问角色。

14.根据权利要求13所述的存储特定计算机可执行指令的计算机可读介质,其中所述计算机系统还被配置为:

响应于所述身份主体被成功验证,由所述源云间服务网关修改所述请求以生成经修改请求,其中所述修改包括移除所述请求的元数据中包括的所述身份主体,以及将与所述计算实例相关联的所述访问角色合并到所述元数据中;以及

由所述源云间服务网关将所述经修改请求发送给设置在所述目标云环境中的目标云间服务网关。

15.根据权利要求14所述的存储特定计算机可执行指令的计算机可读介质,其中所述源云间服务网关设置在所述源云环境的第一数据平面中,并且所述目标云间服务网关设置在所述目标云环境的第二数据平面中,所述源云间服务网关经由可信通信通道通信地耦合到所述目标云间服务网关。

16.根据权利要求14所述的存储特定计算机可执行指令的计算机可读介质,其中所述计算机系统还被配置为:

由所述目标云间服务网关从所述经修改请求中提取与所述计算实例相关联的所述访问角色;以及

由所述目标云间服务网关从所述目标云环境中包括的管理服务获得与所述访问角色相关联的令牌。

17.根据权利要求16所述的存储特定计算机可执行指令的计算机可读介质,其中所述计算机系统还被配置为:

由所述目标云间服务网关用与所述访问角色相关联的所述令牌对所述经修改请求进行签名,以形成被签名的经修改请求;以及

将所述被签名的经修改请求转发到期望由所述计算实例使用的所述服务。

18.一种系统,包括:

处理器;以及

包括指令的存储器,所述指令当用所述处理器执行时使所述系统至少:

由在源云环境中执行的计算实例生成使用在目标云环境中提供的服务的请求,所述源

云环境不同于所述目标云环境;

经由云间服务网关将所述请求从所述源云环境传送到所述目标云环境;以及

基于与所述计算实例相关联的访问角色在所述目标云环境中执行所述服务。

19.根据权利要求18所述的系统,还配置为:

由所述计算实例将所述请求发送到设置在所述源云环境中的源云间服务网关,所述请求包括与所述计算实例相关联的身份主体;以及

由所述源云间服务网关验证所述计算实例的所述身份主体。

20.根据权利要求19所述的系统,其中所述系统被配置为通过核实所述计算实例是否被准许访问所述目标云环境中的所述服务来验证所述身份主体。

云间服务网关

[0001] 对相关申请的交叉引用

[0002] 本申请要求2022年5月12日提交的美国非临时申请第17/742472号的申请日的利益,其内容通过引用整体并入本文以用于所有目的。

技术领域

[0003] 本公开涉及一种云间服务网关,其提供针对部署在第二云环境(例如,第二公共云)中的资源促进对在第一云环境(例如,第一公共云)中提供的服务的访问的框架。在不交换或共享与两个云环境之间的资源相关联的身份主体(例如,证书或凭证)的情况下提供对服务的访问。

背景技术

[0004] 公共云的用户或客户想要从各种云服务提供商获得最佳的同类服务。在云环境中,此类服务设计的当前范例鼓励在云环境提供的本地服务之上进行构建。跨云或云间服务访问不是容易获得的。因此,用户设计他们自己的定制解决方案以从第一云环境访问在不同于第一云环境且独立于第一云环境的第二云环境中提供的服务。为了获得对另一云服务提供商提供的服务的访问而设计的典型解决方案耗时、易出错并且昂贵。此外,典型访问解决方案的主要缺点之一是凭证管理。具体地,从部署在第二云环境中的资源访问在第一云环境中提供的服务涉及在两个云环境之间建立网络连接。在这样的框架中,访问第一云环境的服务涉及用户通过云基础设施分发他们的凭证。这样的解决方案本质上是不安全且不方便的。

[0005] 本文描述的实施例解决与在不同云环境之间迁移应用有关的这些和其他问题。

发明内容

[0006] 本公开总体上涉及一种云间服务网关,其提供针对部署在第二云环境(例如,第二公共云)中的资源促进对在第一云环境(例如,第一公共云)中提供的服务的访问的框架。在不交换或共享与两个云环境之间的资源相关联的身份主体(例如,证书或凭证)的情况下提供对服务的访问。本文描述了各种实施例,包括方法、系统、存储可由一个或多个处理器执行的程序、代码或指令的非瞬态计算机可读存储介质等。提及这些说明性实施例不是为了限制或定义本公开,而是为了提供帮助理解的示例。在具体实施方式部分中讨论了其他实施例,并且在其中提供了进一步的描述。

[0007] 本公开的一方面提供了一种方法,包括:由在源云环境中执行的计算实例生成使用在目标云环境中提供的服务的请求,源云环境不同于目标云环境;经由云间服务网关将请求从源云环境发送到目标云环境;以及基于与计算实例相关联的访问角色在目标云环境中执行服务。

[0008] 本公开的另一个方面提供了一种存储特定计算机可执行指令的计算机可读介质,所述特定计算机可执行指令在由处理器执行时使计算机系统至少:由在源云环境中执行的

计算实例生成使用在目标云环境中提供的服务的请求,源云环境不同于目标云环境;经由云间服务网关将请求从源云环境发送到目标云环境;以及基于与计算实例相关联的访问角色在目标云环境中执行服务。

[0009] 本公开的一个方面提供了一种包括处理器和存储器的系统,存储器包括指令,指令当由处理器执行时使系统至少:由在源云环境中执行的计算实例生成使用在目标云环境中提供的服务的请求,源云环境不同于目标云环境;经由云间服务网关将请求从源云环境发送到目标云环境;以及基于与计算实例相关联的访问角色在目标云环境中执行服务。

[0010] 在参考下面的说明书、权利要求和附图时,前述以及其他特征和实施例将变得更加明显。

附图说明

[0011] 图1描绘了根据各种实施例的云间服务网关(ICSGW)的示例性高层架构。

[0012] 图2描绘了根据各种实施例的由云间服务网关(ICSGW)执行的过程的流程图。

[0013] 图3A描绘了根据各种实施例的云间服务网关(ICSGW)的详细架构。

[0014] 图3B描绘了根据某些实施例的由源云间服务网关执行的过程的流程图。

[0015] 图3C描绘了根据某些实施例的由目标云间服务网关执行的过程的流程图。

[0016] 图4A描绘了根据一些实施例的在源云环境中执行的计算实例利用目标云环境中提供的服务的示例性过程。

[0017] 图4B描绘了根据一些实施例的利用目标云环境中提供的服务在源云环境中执行的计算实例的另一示例性过程。

[0018] 图5是描绘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。

[0019] 图6是描绘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模式的框图。

[0020] 图7是描绘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模式的框图。

[0021] 图8是描绘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模式的框图。

[0022] 图9是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

[0023] 在下面的描述中,将描述各种实施例。出于解释的目的,阐述了具体的配置和细节以提供对实施例的透彻理解。然而,本领域技术人员将明白,可以在没有具体细节的情况下实施实施例。此外,为了不模糊所描述的实施例,可以简化众所周知的特征。

[0024] 在云计算中,云是云客户通过通信网络(例如,互联网)访问的服务器的集合。为客户提供各种服务的云服务提供商(CSP)管理云的基础设施。相比之下,多云环境通常涉及几个云基础设施的使用,每个云基础设施由唯一的CSP管理。多云部署有多种用途。多云部署可以利用多个基础设施即服务(IaaS)供应商,或者它可以将不同的供应商用于IaaS、平台即服务(PaaS)和软件即服务(SaaS)服务。多云可以纯粹出于冗余和系统备份的目的,或者

多云部署可以针对不同的服务并入不同的云供应商。

[0025] 到目前为止,大多数多云解决方案主要侧重于简化网络访问。拥有不同CSP的账户的用户或客户可以基于身份联盟(即用户的身份联盟)访问不同云中的资源。具体地,身份联盟是一种在双方之间建立信任的系统,目的是对用户进行身份验证并传递授权其访问资源所需的信息。然而,这种框架并不会自然扩展到在资源(即非用户行为者,诸如计算实例、VM、功能)之间建立信任。

[0026] 此外,客户尽可能偏向于将其从计算工作负载(即,VM、容器、功能)到云服务的业务保持为私有,并避免将其长期使用的凭证分发给这些计算工作负载中。客户可以实现这种类型的通信,但仅在各自的云提供环境中,即在单个云环境中。目前还没有在云间环境中实现类似通信模式的机制。本公开的实施例提供了一种云间服务网关(ICSGW),其旨在提供一种框架,使用该框架,客户可以在一个云环境(例如,由第一CSP管理)中配置他们的计算工作负载或计算实例,从而以更安全的方式访问不同云环境(即,由第二CSP管理)中的服务。

[0027] 图1描绘了根据各种实施例的云间服务网关(ICSGW)的示例性高层架构。图1中描绘的高层架构100包括云间服务网关105,云间服务网关105是无缝地设置在源云环境101和目标云环境107之间的多租户服务。具体地,ICSGW 105在源云环境101和目标云环境107两者中都具有足迹。

[0028] 源云环境101包括托管一个或多个计算实例102(例如,虚拟机(VM)、容器、功能)的一个或多个客户虚拟云网络(例如,客户VCN 103)。这样的计算实例102可以利用由目标云环境107经由ICSGW 105提供的服务109。应当理解,目标云环境107提供的服务109可由在目标云环境107中具有租赁(即,目标云环境107中的客户账户)的客户以及没有客户租赁的客户使用。

[0029] 根据一些实施例,当计算工作负载(例如,源云环境101中的计算实例102)利用源云环境101中本地可用的身份主体(即,对应于资源的身份的资源主体)访问目标云环境中的目标服务109时,ICSGW 105服务执行一组动作。在一个实现中,该组动作至少包括:(i)拦截计算工作负载和目标服务之间的请求/响应;(ii)验证与计算实例相关联的身份主体;(iii)将身份主体转换为计算实例在目标云环境中的访问角色;以及(iv)将请求转发到目标云环境中的最终目的地(例如,期望的服务)。换言之,源云环境中的计算实例102生成访问目标云环境中的服务109的请求。该请求进一步通过安全通信信道从源云环境101传送到目标云环境107。基于与源云环境101中的计算实例相关联的访问角色(即,一个或多个特权)在目标云环境107中执行服务。此外,下面参考图3A至3C详细描述关于ICSGW 105的架构以及(在目标云环境中)发起服务以供源云环境中的计算实例使用的过程。

[0030] 图2描绘了根据各种实施例的由云间服务网关(ICSGW)执行的过程的高层流程图。具体地,图2示出了配备在源云环境中执行的计算实例(例如,虚拟机、容器、函数)经由ICSGW访问在目标云环境中提供的服务的步骤的过程。图2描绘的处理可以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合中实现。软件可以存储在非易失性存储介质上(例如,存储器设备上)。图2中呈现并在下面描述的方法旨在是说明性的和非限制性的。尽管图2描绘了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些备选实施例中,这些步骤可以以某种不同的次序来

执行,或者某些步骤也可以并行地执行。

[0031] 该过程开始于步骤201,其中在源云环境中执行的计算实例(例如,在源云环境中的客户VCN中执行的计算实例)生成使用在目标云环境中提供的服务的请求。需要注意的是,目标云环境与源云环境不同且独立。

[0032] 在步骤203中,计算实例生成的请求经由云间服务网关从源云环境传送到目标云环境。具体地,如稍后将参考图3A描述的,将请求从源云间服务网关(部署在源云环境中)传送到目标云间服务网关(部署在目标云环境中),源云间服务网关和目标云间服务网关经由可信通信信道(例如,快速连接(Fastconnect)通信信道)通信地耦合。在将请求传送到目标云环境后,在步骤205中,基于与计算实例相关联的访问角色在目标云环境中执行服务。

[0033] 现在转到图3A,描绘了根据各种实施例的云间服务网关(ICSGW)的详细架构。ICSGW提供了一种服务框架,该服务框架针对部署在第二公共云(即,本文称为源云环境)中的资源促进对在第一公共云(即,本文称为目标云环境)中提供的服务的访问,而无需跨两个云环境共享身份主体。

[0034] ICSGW的架构300包括源云环境301和目标云环境331。源云环境301包括ICSGW服务租赁303、源云服务313以及一个或多个客户虚拟云网络(VCN)(例如,客户1VCN 315、客户2VCN 317)。ICSGW服务租赁303包括控制平面组件(即,ICSGW控制平面305)和数据平面组件(即,ICSGW数据平面307)。源ICSGW 309被托管在ICSGW数据平面307中。源云服务313包括多个服务,包括身份和管理服务313A以及私有访问服务313B。每个客户VCN包括在其中执行的计算实例(例如,客户1VCN 315包括计算实例315A,并且客户2VCN 317包括另一计算实例317A)。

[0035] 目标云环境331包括ICSGW服务账户(或服务租赁)337和目标云服务333。ICSGW服务账户337包括托管目标ICSGW 345的数据平面组件(即,ICSGW数据平面343)。目标云服务可以包括服务,诸如身份管理333A、安全令牌服务333B和其他服务333C(例如,队列服务、存储服务)。源云环境301经由可信、高带宽和低延时的通信链路350(例如,快速连接通信链路)通信地耦合到目标云环境331。具体地,通过一个实施例,通过经由一对路由器(例如,支持快速连接的动态路由网关(DRG))将源ICSGW 309(设置在源云环境301的数据平面307中)连接到目标ICSGW 345(设置在目标云环境331的数据平面343中)来建立可信通信链路350。例如,如图3A中所示,源云环境301中的ICSGW服务租赁303包括支持快速连接的第一DRG 351,其通信地耦合到被包括在目标云环境331的ICSGW服务租赁337中的支持快速连接的第二DRG 353。

[0036] 源ICSGW 309与目标ICSGW 345一起提供促进在源云环境301中执行的计算实例(例如,计算实例315A和317A)访问在目标云环境331中提供的服务(例如,其他服务333C)的框架。应当注意,在目标云环境331中提供的服务对于在目标云环境331中具有租赁(或账户)的源云环境301的客户(例如,客户B租赁335)以及对于在目标云环境中没有租赁的源云环境301的客户是可用的。需要注意的是,对于在目标云环境331中没有租赁的客户,源云环境301的ICSGW控制平面305被配置为在目标云环境的ICSGW服务账户337中实例化用于该客户的资源组(例如,客户A资源组)。资源组包括诸如队列、存储桶、访问角色等资源。将理解,图3A的上述实施例不以任何方式限制本公开的范围。相反,对云间服务网关(ICSGW)的架构的修改完全在本公开的范围内。例如,根据一些实施例,(源云环境301中的)ICSGW数据平面

307可以包括源ICSGW池,并且(在目标云环境331的)ICSGW数据平面343可以包括目标ICSGW池。在这样的设置中,可以基于某些条件(例如,系统中的当前业务负载)动态地选择源ICSGW池中的一个源ICSGW以及目标ICSGW池中的一个目标ICSGW,以将请求从源云环境301传送到目标云环境331。

[0037] 在下文中,提供了关于在源云环境中执行的资源(例如,计算实例315A)如何访问目标云环境331中的服务的详细描述。在操作中,促进对目标云环境331中的服务和源云环境301中的资源的访问的过程包括两个操作阶段:建立阶段和执行阶段。在建立阶段,在源云环境中创建动态组。动态组提供以类似于将用户分组到用户组中的方式将计算实例作为主要行为者进行分组。策略是在建立阶段创建的,其准许动态组中的计算实例发布API调用以从目标云环境获得服务。动态组中的成员资格可以由被称为匹配规则的一组标准来确定。满足匹配规则的云基础设施资源(例如,计算实例)被包括为动态组的成员。

[0038] 此外,在建立阶段,每个动态组被分配与动态组的成员可以在目标云环境中享有的一组特权相对应的角色(本文称为访问角色)。此外,在建立阶段,客户可以提供关于客户是否在目标云环境中具有租赁(即,账户)的信息。这样的信息可以包括目标云环境的标识符、目标云环境的区域、客户的租赁在目标云环境中的账户ID等。应当理解,在客户在目标云环境中没有租赁的情况下,(源云环境301中包括的)ICSGW控制平面305可以在建立阶段为客户(例如,客户A资源组341)建立资源组。注意,资源组是在目标云环境331的ICSGW服务账户337中创建的。

[0039] 根据一些实施例,在建立阶段,源云环境301的ICSGW控制平面305利用私有访问服务313B来提供源云环境(例如,客户1VCN 315、客户2VCN 317)的客户租赁中的客户VCN到ICSGW数据平面307的私有连接。此外,ICSGW控制平面305可以利用VCN/DNS基础设施服务来对客户VCN中的域名系统(DNS)解析器进行编程,以将去往目标云环境中的服务的客户业务重新路由到ICSGW数据平面307。

[0040] 在执行阶段,在客户VCN中执行的计算实例(例如,计算实例315A)发送请求,请求使用在目标云环境331中提供的服务。这样的请求被源ICSGW 309拦截。在一个实现中,该请求包括与计算实例相关联的身份主体(例如,证书或凭证)。源ICSGW从请求中提取身份主体,并执行与计算实例相关联的准许的验证。例如,源ICSGW 309与源云环境301的身份管理服务313A通信以核实特定计算实例是否被准许发出请求,请求由目标云环境提供的服务。

[0041] 在成功验证之后,源ICSGW 309获得为计算实例预配置(即,在建立阶段)的访问角色。然后,源ICSGW 309修改从计算实例接收的请求,并将经修改请求转发给目标云环境中包括的目标ICSGW 345。注意,经修改请求通过在建立阶段中建立的可信通信信道(例如,通信信道350)从源云环境301传送到目标云环境。在一个实现中,源ICSGW 309通过从请求中剥离(即,移除)身份主体并将访问角色合并到请求中来修改请求以形成经修改请求。以此方式,确保与源云环境301的资源相关联的身份主体不被发送到目标云环境331。

[0042] 目标ICSGW 345在接收源ICSGW 309发送的经修改请求后,提取经修改请求中包括的访问角色(与计算实例相关联)。在一个实施例中,目标ICSGW 345与管理服务(例如,目标云环境331中包括的身份管理服务333A或安全令牌服务333B)通信以获得与计算实例的访问角色相关联的凭证(例如,令牌)。目标ICSGW 345用获得的凭证对经修改请求进行签名,并将被签名的请求转发给期望由计算实例使用的服务(例如,服务333C)。在一个实施例中,

所期望的服务可以与目标云环境331的管理服务(例如,身份管理服务333A)通信以确定用于对请求进行签名的凭证是否具有足够的特权来执行所请求的动作。在成功验证之后,在目标云环境331中包括的客户租赁中执行服务,即,在客户B租赁335中执行请求(在客户在目标云环境中具有租赁的情况下),或者在客户A资源组341中执行请求(在客户在目标云环境中没有其自己的租赁的情况下)。

[0043] 图3B示出了根据某些实施例的由源云间服务网关(ICSGW)执行的过程的流程图。图3B中所示的处理可以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合中实现。软件可以存储在非易失性存储介质上(例如,存储器设备上)。图3B中呈现并在下面描述的方法旨在是说明性的和非限制性的。尽管图3B示出了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些备选实施例中,这些步骤可以以某种不同的次序来执行,或者某些步骤也可以并行地执行。

[0044] 该过程开始于步骤361,其中源ICSGW从在源云环境中执行的计算实例接收请求。该请求对应于计算实例请求使用由目标云环境提供的服务。在一个实现中,该请求包括与计算实例相关联的身份主体(例如,证书或凭证)。在步骤363中,源ICSGW从请求中提取身份主体,并执行与计算实例相关联的准许的验证。例如,源ICSGW验证特定计算实例是否被准许发出请求,请求由目标云环境提供的服务。

[0045] 在步骤365中,源ICSGW执行查询以确定与和计算实例相关联的身份主体相关联的准许的验证是否成功。如果对查询的响应是肯定的(即,计算实例被准许请求由目标云环境提供的服务),则过程移动到步骤367。然而,如果在步骤365中对查询的响应是否定的(即,计算实例不被准许请求由目标云环境提供的服务),则过程移动到步骤366。应当理解,源ICSGW可以根据源云环境的管理服务(例如,身份访问管理服务)来验证与计算实例相关联的身份主体。

[0046] 在步骤366中(即,在确定对步骤365的查询的否定响应之后),源ICSGW提供对由计算实例发送的请求的响应。例如,源ICSGW向计算实例发送响应消息,指示计算实例的身份主体未被成功验证,因此目标云环境的所请求的服务不能被提供给计算实例(即,服务访问失败)。在步骤366中发送响应消息后,图3A中的过程终止。

[0047] 在确定对步骤365的查询的肯定响应后,过程移动到步骤376。在该步骤中,源ICSGW从预配置信息(例如,与建立阶段相关联的信息)获得与所请求的服务的计算实例相关联的访问角色。访问角色指示与目标云环境中的计算实例相关联的特权(例如,读写特权、只读特权)。

[0048] 该过程然后进行到步骤369,其中源ICSGW修改从计算实例获得的请求以生成经修改请求。在一个实现中,源ICSGW从请求中移除与计算实例相关联的身份主体,并在请求中包括与计算实例相关联的访问角色(在步骤367中获得)以生成经修改请求。此后,源ICSGW将经修改请求发送到目标ICSGW。参考图3A,可以理解,经修改请求经由在源云环境和目标云环境之间建立的可信通信通道350从源ICSGW传送到目标ICSGW。

[0049] 图3C示出了根据某些实施例的由目标云间服务网关(ICSGW)执行的过程的流程图。图3C中示出的处理可以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合中实现。软件可以存储在非易失性存储介质上(例如,存储器设备上)。图3C中呈现并在下面描述的方法旨在是说明性的和非限制性的。尽

管图3C示出了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些备选实施例中,这些步骤可以以某种不同的次序来执行,或者某些步骤也可以并行地执行。

[0050] 该过程开始于步骤371,其中目标ICSGW接收源ICSGW发送的经修改请求(即,在图3B的步骤370中由源ICSGW发送的请求)。在步骤373中,目标ICSGW提取经修改请求中包括的访问角色。该过程然后移动到步骤375,其中目标ICSGW与目标云环境中包括的管理服务(例如,图3B的安全令牌服务333B)通信。具体地,目标ICSGW与管理服务通信以获得与计算实例的访问角色相关联的凭证(例如,令牌)。

[0051] 在步骤377中,目标ICSGW利用在步骤375中获得的凭证对经修改请求进行签名,并在步骤379中将被签名的请求转发给期望由计算实例使用的服务。该过程然后移动到步骤381,在该步骤中执行查询以确定凭证的有效性。例如,在一个实现中,所期望的服务可以与目标云环境的管理服务(例如,身份管理服务)通信以确定用于对请求进行签名的凭证是否具有足够的特权来执行所请求的动作。如果在步骤381中对查询的响应是肯定的(即,凭证具有足够的特权来执行动作),则过程移至步骤383。然而,如果对步骤381的查询的响应是否定的,则过程移至步骤385。

[0052] 在步骤385中,服务用指示对要由服务执行的所请求的动作(例如,读、写、更新)的访问失败的消息进行响应。换句话说,该服务通知目标ICSGW由于特权不足而无法执行所请求的动作。在一些实现中,目标ICSGW可以经由可信通信信道将获得的响应转发到部署在源云环境中的计算实例。然而,响应于步骤381中凭证的成功验证,步骤383中的过程继续执行所期望的服务的请求。此后,图3B中示出的过程终止。

[0053] 现在转到图4A和图4B,根据一些实施例,示出了在源云环境中执行的计算实例利用在目标云环境中提供的服务的示例性过程。参考图4A,示出了源云环境401和目标云环境451。源云环境401包括托管两个应用(即,应用1 405A和应用2 405B)的客户虚拟云网络(即,客户VCN 403)。此外,源云环境401包括与目标云环境451中包括的目标ICSGW 459通信地耦合的源ICSGW 407。

[0054] 目标云环境451包括目标云服务461、客户租赁或账户463、以及其他目标云服务453。其他目标云服务453可以包括附加服务,诸如身份管理服务453A、安全令牌服务453B等。为了说明,目标云环境451中期望由计算实例(即,源云环境401中的应用1 405A和应用2 405B)使用的目标云服务461被示出为S3服务和SQS服务。S3服务(即,简单存储服务)是将数据作为对象存储在桶中的对象存储服务。对象是文件和描述该文件的任何元数据。桶是对象的容器。SQS(即简单队列服务)是受管理的消息队列服务,其用于异步发送、存储和检索各种大小的多个消息。

[0055] 根据一些实施例,在建立阶段在源云环境中创建动态组。动态组以类似于将用户分组到用户组中的方式提供将计算实例作为主要参与者进行分组。可以在建立阶段创建准许动态组内的计算实例发出API调用以获得服务的策略。可以理解,动态组中的成员资格可以由被称为匹配规则的一组标准来确定。满足匹配规则的云基础设施资源被包括为动态组的成员。例如,如图4A中所示,应用1 405A被包括在第一动态组(DG1)中,而应用2 405B被包括在第二动态组(DG2)中。

[0056] 此外,在建立阶段,每个动态组可以被分配与动态组的成员可以在目标云环境中享有的一组特权相对应的角色(本文也称为访问角色)。例如,如图4A中所示,属于动态组1

(DG1)的应用1 405A被分配第一角色(标记为IAM-角色1),并且属于动态组2(DG2)的应用2 405B被分配第二角色(标记为IAM-角色2)。为简单起见,与第一角色相关联的特权对应于读和写特权,而与第二角色相关联的特权对应于只读特权。以这种方式构建的动态组集合在图4A中以虚框409示出。如图4A中所示,应当理解,在建立阶段,还在目标云环境中的客户账户463中实例化被分配给不同动态组的角色。具体地,在建立阶段,客户指定客户是否在目标云环境中拥有客户租赁。在客户在目标云环境中具有客户租赁(例如,目标云环境451中的客户账户463)的情况下,在建立阶段中指定指定目标云环境、目标云环境中的客户租赁、分配给客户VCN的动态组的不同角色等的信息。

[0057] 此外,通过一些实施例,每个动态组中的计算实例可以被编程为向与该动态组相关联的端点发送对于目标云环境中提供的服务的请求。端点将请求转发到源ICSGW,源ICSGW进一步通过安全通信通道将请求转发到目标ICSGW。例如,如图4A中所示,DG1中包括的应用1 405A将由应用发出的请求(即,请求目标云环境中提供的服务的请求)转发到ICSGW 1端点406A,而DG2中包括的应用2 405B将由应用发出的请求转发到ICSGW 2端点406B。

[0058] 在下文中,参考图4A,详细描述与由客户VCN 403中包括的计算实例发出的四个不同请求(针对目标云环境所提供的服务)有关的流程。具体地,流程1(具有标记为1.1到1.5的步骤)对应于应用1405A发出请求以访问目标云环境中的S3桶从而上传文件的场景。流程2(具有标记为2.1到2.5的步骤)对应于应用1 405A发出请求以调用SQS服务从而发送消息的场景。流程3(具有标记为3.1至3.5的步骤)对应于应用2 405B轮询SQS队列以确定消息的存在的场景,而流程4(具有标记为4.1至4.5的步骤)对应于应用2 405B发出读取文件的请求的场景。

[0059] 参考流程1,在步骤1.1中,应用1 405A发出上传文件的请求。该请求经由ICSGW 1端点406A被转发给源ICSGW 407。源ICSGW 407终止该请求并执行验证检查以确定与应用1 405A相关联的身份主体是否被准许做出这样的请求。在成功验证之后,源ICSGW 407修改该请求以在该请求中包括与应用1 405A相关联的访问角色(例如,IAM角色1)。在步骤1.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。注意,经修改请求在源云环境401和目标云环境451之间建立的安全通信通道(例如,快速连接)上转发。在步骤1.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务(例如,目标云服务453中包括的安全令牌服务453B)通信以获得与访问角色相关联的凭证。在步骤1.4中,目标ICSGW 459用获得的凭证对经修改请求进行签名(步骤1.3),并将被签名的请求转发给服务(例如,期望由应用1405A使用的服务461)。在步骤1.5中,目标服务461可以执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,上传文件)的足够特权相关联。此外,由于应用1 405A与具有读写特权的访问角色相关联,因此在步骤1.5中,文件被上传到客户租赁463中的S3桶中。

[0060] 现在参考流程2,在步骤2.1中,应用1 405A发出请求以调用目标云环境中的SQS服务发送消息(例如,发送到SQS队列)。该请求经由ICSGW 1端点406A被转发给源ICSGW 407。源ICSGW 407终止该请求并执行验证检查以确定与应用1 405A相关联的身份主体是否被准许做出这样的请求。在成功验证之后,源ICSGW 407修改该请求以在该请求中包括与应用1 405A相关联的访问角色(例如,IAM角色1)。在步骤2.2中,源ICSGW 407将经修改请求转发到

目标ICSGW 459。在步骤2.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务(例如,目标云服务453中包括的安全令牌服务453B)通信以获得与访问角色相关联的凭证。在步骤2.4中,目标ICSGW 459用获得的凭证对经修改请求进行签名(步骤1.3),并将被签名的请求转发给服务(例如,期望由应用1 405A使用的SQS服务461)。在步骤2.5中,目标服务461可以执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,在SQS队列上发送消息)的足够特权相关联。此外,由于应用1 405A与具有读写特权的访问角色相关联,因此在步骤2.5中,将消息添加到客户租赁463中的SQS队列。

[0061] 现在参考流程3,其对应于应用2 405B轮询SQS队列以确定消息的存在(即,从SQS队列读取消息)的场景。在步骤3.1中,应用2 405B发出从SQS队列获取消息的请求。该请求经由ICSGW 2端点406B被转发给源ICSGW 407。源ICSGW 407终止该请求并如上所述执行验证检查。在成功验证之后,源ICSGW 407修改请求以在请求中包括与应用2 405B相关联的访问角色(例如,IAM角色2)。在步骤3.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤3.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务通信以获得与访问角色相关联的凭证。在步骤3.4中,目标ICSGW 459用获得的凭证对经修改请求进行签名(步骤3.3),并将被签名的请求转发给服务(例如,期望由应用2 405B使用的SQS服务461)。在步骤3.5中,目标服务461可以执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,从SQS队列获取消息)的足够特权相关联。此外,由于应用2 405B与具有读特权的访问角色相关联,因此在步骤3.5中,从客户租赁463中的SQS队列中获取消息。

[0062] 现在参考流程4,其对应于应用2 405B调用对S3服务的调用以从S3桶获取对象的场景。在步骤4.1中,应用2 405B发出从S3桶获取对象的请求。该请求经由ICSGW 2端点406B被转发给源ICSGW407。源ICSGW 407终止该请求并如上所述执行验证检查。在成功验证之后,源ICSGW 407修改请求以在请求中包括与应用2 405B相关联的访问角色(例如,IAM角色2)。在步骤4.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤4.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务通信以获得与访问角色相关联的凭证。在步骤4.4中,目标ICSGW 459用获得的凭证(步骤4.3)对经修改请求进行签名,并将被签名的请求转发给服务(例如,期望由应用2405B使用的S3服务461)。在步骤4.5中,目标服务461可以执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,从S3桶获得对象)的足够特权相关联。此外,由于应用2 405B与具有读特权的访问角色相关联,因此在步骤4.5中,从客户租赁463中的S3桶中获取对象。

[0063] 现在参考图4B,详细描述与客户VCN 403中包括的计算实例发出的四个不同请求(针对目标云环境所提供的服务)有关的流程。具体地,流程5(具有标记为5.1到5.4的步骤)对应于应用2 405B发出将文件上传在S3存储桶中的请求的场景。流程6(具有标记为6.1到6.4的步骤)对应于应用2 405B发出从SQS队列删除消息的请求的场景。流程7(具有标记为7.1至7.5的步骤)对应于应用1 405A发出从SQS队列删除消息的请求的场景,而流程8(具有标记为8.1至8.5的步骤)对应于应用1 405A发出从S3存储桶删除文件的请求的场景。

[0064] 现在参考流程5,其对应于应用2 405B发出将文件上传在S3桶中的请求的场景。在

步骤5.1中,应用2 405B发出将文件上传在S3存储桶中的请求。该请求经由ICSGW 2端点406B被转发给源ICSGW 407。源ICSGW 407终止该请求并如上所述执行验证检查。在成功验证之后,源ICSGW 407修改请求以在请求中包括与应用2405B相关联的访问角色(例如,IAM角色2)。在步骤5.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤5.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务通信以获得与访问角色相关联的凭证。在步骤5.4中,目标ICSGW 459用获得的凭证对经修改请求进行签名(步骤5.3),并将被签名的请求转发给服务(例如,期望由应用2 405B使用的S3服务461)。目标服务461执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,将文件上传到S3桶)的足够特权相关联。由于应用2 405B与具有只读特权的访问角色相关联,因此目标云环境中的S3服务拒绝将文件上传在S3存储桶中的请求(步骤5.4)。因此,客户账户463中的服务461不执行该请求。

[0065] 现在参考流程6,其对应于应用2 405B发出从SQS队列中删除消息的请求的场景。在步骤6.1中,应用2 405B发出从SQS队列中删除消息的请求。该请求经由ICSGW 2端点406B被转发给源ICSGW 407。源ICSGW 407终止该请求并如上所述执行验证检查。在成功验证之后,源ICSGW 407修改请求以在请求中包括与应用2405B相关联的访问角色(例如,IAM角色2)。在步骤6.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤6.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与管理服务通信以获得与访问角色相关联的凭证。在步骤6.4中,目标ICSGW 459用(步骤6.3的)获得的凭证对经修改请求进行签名,并将被签名的请求转发给服务(例如,期望由应用2 405B使用的SQS服务461)。目标服务461执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,从SQS队列中删除消息)的足够特权相关联。由于应用2405B与具有只读特权的访问角色相关联,因此目标云环境中的SQS服务拒绝删除消息的请求(步骤6.4)。因此,客户账户463中的服务461不执行该请求。

[0066] 现在转到流程7,在步骤7.1中,应用1 405A发出从SQS队列中删除消息的请求。该请求经由ICSGW 1端点406A被转发给源ICSGW 407。源ICSGW 407终止该请求并执行验证检查以确定与应用1 405A相关联的身份主体是否被准许做出这样的请求。在成功验证之后,源ICSGW 407修改该请求以在该请求中包括与应用1 405A相关联的访问角色(例如,IAM角色1)。在步骤7.2,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤7.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与目标云环境的管理服务(例如,目标云服务453中包括的安全令牌服务453B)通信以获得与访问角色相关联的凭证。在步骤7.4中,目标ICSGW 459用(步骤7.3的)获得的凭证对经修改请求进行签名,并将被签名的请求转发给服务(例如,期望由应用1 405A使用的SQS服务461)。在步骤7.5中,目标服务461可以执行检查以确定(从目标ICSGW 459获得的)凭证是否与执行所请求的动作(即,删除消息)的足够特权相关联。此外,由于应用1 405A与具有读写特权的访问角色相关联,在步骤7.5中,从客户租赁463中的SQS队列中删除该消息。

[0067] 流程8(具有标记为8.1到8.5的步骤)对应于应用1 405A发出从S3桶中删除文件的请求的场景。在步骤8.1中,应用1 405A发出从S3存储桶中删除文件的请求。该请求经由ICSGW 1端点406A被转发给源ICSGW 407。源ICSGW 407终止该请求并执行验证检查以确定与应用1 405A相关联的身份主体是否被准许做出这样的请求。在成功验证之后,源ICSGW

407修改该请求以在该请求中包括与应用1 405A相关联的访问角色(例如,IAM角色1)。在步骤8.2中,源ICSGW 407将经修改请求转发到目标ICSGW 459。在步骤8.3中,目标ICSGW 459从自源ICSGW 407接收的经修改请求中提取对应的访问角色。目标ICSGW 459与目标云环境的管理服务(例如,目标云服务453中包括的安全令牌服务453B)通信以获得与访问角色相关联的凭证。在步骤8.4中,目标ICSGW 459用(步骤8.3的)获得的凭证对经修改请求进行签名,并将被签名的请求转发给服务(例如,期望由应用1 405A使用的S3服务461)。在步骤8.5中,目标服务461执行检查以确定凭证(从目标ICSGW 459获得)是否与执行所请求的动作(即,从S3存储桶中删除文件)的足够特权相关联。此外,由于应用1 405A与具有读写特权的访问角色相关联,因此在步骤8.5中,从客户租赁463中的S3桶中删除消息。

[0068] 注意,图4A和图4B中描绘的示例性场景对应于客户具有租赁的情况,即目标云环境中的客户账户(例如,图3A的客户B租赁335)。在这种情况下,ICSGW服务账户337被配置为代表在源云环境中执行的计算实例来(在目标云环境中)管理服务。可以理解,对于客户在目标云环境中没有租赁的情况,可以实现一组类似的场景。在这种情况下,ICSGW控制平面(图3A中的305)可以被配置为在目标云环境的ICSGW服务账户337内设置客户资源组(例如,客户A资源组341)。

[0069] 示例云基础架构

[0070] 图5是示出根据至少一个实施例的IaaS架构的示例模式的框图500。服务运营商502可以通信地耦合到安全主机租赁504,安全主机租赁504可以包括虚拟云网络(VCN)506和安全主机子网508。在一些示例中,服务运营商502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®、计算平板电脑、个人数字助理(PDA))或可穿戴设备(例如,Google Glass®头戴式显示器),运行诸如Microsoft Windows Mobile®的软件、和/或诸如iOS、Windows Phone、Android、BlackBerry 8、Palm OS等的各种移动操作系统,并且支持互联网、电子邮件、短消息服务(SMS)、Blackberry®或其他通信协议。备选地,客户端计算设备可以是通用个人计算机,例如包括运行各种版本的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市场上可获得的UNIX®或类UNIX操作系统中的任何操作系统的工作站计算机,包括但不限于GNU/Linux操作系统的种类,例如Google Chrome OS。备选地或另外地,客户端计算设备可以是能够通过可以访问VCN 506和/或互联网的网络进行通信的任何其他电子设备,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/或个人消息收发设备。

[0071] VCN 506可以包括本地对等网关(LPG)510,其可以经由安全外壳(SSH)VCN 512中包含的LPG 510通信地耦合到SSH VCN 512。SSH VCN 512可以包括SSH子网514,并且SSH VCN 512可以经由控制平面VCN 516中包含的LPG 510通信地耦合到控制平面VCN 516。此外,SSH VCN 512可以经由LPG 510通信地耦合到数据平面VCN 518。控制平面VCN 516和数据平面VCN 518可以被包含在服务租赁519中,服务租赁519可以由IaaS提供商拥有和/或运营。

[0072] 控制平面VCN 516可以包括用作外围网络(例如,公司内联网和外部网络之间的公

司网络的一部分)的控制平面非军事区(DMZ)层520。基于DMZ的服务器可能具有受限的责任,并有助于遏制安全漏洞。此外,DMZ层520可以包括一个或多个负载均衡器(LB)子网522、可包括(多个)app子网526的控制平面app层524、可包括(多个)数据库(DB)子网530(例如,(多个)前端DB子网和/或(多个)后端DB子网)的控制平面数据层528。控制平面DMZ层520中包含的(多个)LB子网522可以通信地耦合到控制平面app层524中包含的(多个)app子网526和可包含在控制平面VCN 516中的互联网网关534,并且(多个)app子网526可以通信地耦合到控制平面数据层528中包含的(多个)DB子网530,以及服务网关536和网络地址转换(NAT)网关538。控制平面VCN 516可以包括服务网关536和NAT网关538。

[0073] 控制平面VCN 516可以包括可包括(多个)app子网526的数据平面镜像app层540。数据平面镜像app层540中包含的(多个)app子网526可以包括可执行计算实例544的虚拟网络接口控制器(VNIC)542。计算实例544可以通信地将数据平面镜像app层540的(多个)app子网526耦合到可包含在数据平面app层546中的(多个)app子网526。

[0074] 数据平面VCN 518可以包括数据平面app层546、数据平面DMZ层548和数据平面数据层550。数据平面DMZ层548可以包括可通信地耦合到数据平面app层546的(多个)app子网526和数据平面VCN 518的互联网网关534的(多个)LB子网522。(多个)app子网526可以通信地耦合到数据平面VCN 518的服务网关536和数据平面VCN 518的NAT网关538。数据平面数据层550还可以包括可通信地耦合到数据平面app层546的(多个)app子网526的(多个)DB子网530。

[0075] 控制平面VCN 516和数据平面VCN 518的互联网网关534可以通信地耦合到元数据管理服务552,元数据管理服务552可以通信地耦合到公共互联网554。公共互联网554可以通信地耦合到控制平面VCN 516和数据平面VCN 518的NAT网关538。控制平面VCN 516和数据平面VCN 518的服务网关536可以通信地耦合到云服务556。

[0076] 在一些示例中,控制平面VCN 516或数据平面VCN 518的服务网关536可以对云服务556进行应用编程接口(API)调用,而无需通过公共互联网554。从服务网关536到云服务556的API调用可以是单向的:服务网关536可以对云服务556进行API调用,并且云服务556可以向服务网关536发送所请求的数据。但是,云服务556不可以向服务网关536发起API调用。

[0077] 在一些示例中,安全主机租赁504可以直接连接到服务租赁519,服务租赁519可以在其他情况下是隔离的。安全主机子网508可以通过LPG 510与SSH子网514通信,LPG 510可以支持在其他情况下隔离的系统上的双向通信。将安全主机子网508连接到SSH子网514可以给予安全主机子网508对服务租赁519内的其他实体的访问。

[0078] 控制平面VCN 516可以允许服务租赁519的用户建立或以其他方式供应期望的资源。可以在数据平面VCN 518中部署或以其他方式使用在控制平面VCN 516中供应的期望资源。在一些示例中,控制平面VCN 516可以与数据平面VCN 518隔离,并且控制平面VCN 516的数据平面镜像app层540可以经由可包含在数据平面镜像app层540和数据平面app层546中的VNIC 542与数据平面VCN 518的数据平面app层546通信。

[0079] 在一些示例中,系统的用户或客户可以通过公共互联网554做出请求,例如创建、读取、更新或删除(CRUD)操作,公共互联网554可以将请求传送到元数据管理服务552。元数据管理服务552可以通过互联网网关534将请求传送到控制平面VCN 516。该请求可以由控

制平面DMZ层520中包含的(多个)LB子网522接收。(多个)LB子网522可以确定该请求有效,并且响应于该确定,(多个)LB子网522可以将该请求发送到包含在控制平面app层524中的(多个)app子网526。如果该请求被验证并且需要对公共互联网554的调用,则可以将对公共互联网554的调用发送到可对公共互联网554进行调用的NAT网关538。请求可能期望存储的存储器可以存储在(多个)DB子网530中。

[0080] 在一些示例中,数据平面镜像app层540可以促进控制平面VCN 516和数据平面VCN 518之间的直接通信。例如,可能期望将对配置的改变、更新或其他适当修改应用于数据平面VCN 518中包含的资源。经由VNIC 542,控制平面VCN 516可以直接与数据平面VCN 518中包含的资源通信,并且从而可以执行对数据平面VCN 518中包含的资源的改变、更新或对配置的其他适当修改。

[0081] 在一些实施例中,控制平面VCN 516和数据平面VCN 518可以包含在服务租赁519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 516或数据平面VCN 518。相反,IaaS提供商可以拥有或操作控制平面VCN 516和数据平面VCN 518,这两者都可以包含在服务租赁519中。该实施例可以实现网络隔离,这可以阻止用户或客户与其他用户或其他客户的资源交互。此外,该实施例可以允许系统的用户或客户私下存储数据库,而不需要依赖可能不具有期望的安全级别的公共互联网654来存储。

[0082] 在其他实施例中,控制平面VCN 516中包含的(多个)LB子网522可以被配置为接收来自服务网关536的信号。在该实施例中,控制平面VCN 516和数据平面VCN 518可以被配置为由IaaS提供商的客户调用,而不调用公共互联网554。IaaS提供商的客户可能期望该实施例,因为客户使用的(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519上,该服务租赁519可以与公共互联网554隔离。

[0083] 图6是示出根据至少一个实施例的IaaS架构的另一示例模式的框图600。服务运营商602(例如,图5的服务运营商502)可以通信地耦合到安全主机租赁604(例如,图5的安全主机租赁504),该安全主机租赁604可以包括虚拟云网络(VCN)606(例如,图5的VCN 506)和安全主机子网608(例如,图5的安全主机子网508)。VCN 606可以包括本地对等网关(LPG)610(例如,图5的LPG 510),其可以经由安全外壳(SSH)VCN 612中包含的LPG 510通信地耦合到安全外壳(SSH)VCN 612(例如,图5的SSH VCN 512)。SSH VCN 612可以包括SSH子网614(例如,图5的SSH子网514),并且SSH VCN 612可以经由控制平面VCN 616中包含的LPG 610通信地耦合到控制平面VCN 616(例如,图5的控制平面VCN 516)。控制平面VCN 616可以包含在服务租赁619中(例如,图5的服务租赁519),并且数据平面VCN 618(例如,图5的数据平面VCN 518)可以包含在可由系统的用户或客户拥有或运营的客户租赁621中。

[0084] 控制平面VCN 616可以包括可包括(多个)LB子网622(例如,图5的(多个)LB子网522)的控制平面DMZ层620(例如,图5的控制平面DMZ层520)、可包括(多个)app子网626(例如,图5的(多个)app子网526)的控制平面app层624(例如,图5的控制平面app层524)、可包括(多个)数据库(DB)子网630(例如,类似于图5的(多个)DB子网530)的控制平面数据层628(例如,图5的控制平面数据层528)。控制平面DMZ层620中包含的(多个)LB子网622可以通信地耦合到控制平面app层624中包含的(多个)app子网626和可包含在控制平面VCN 616中的互联网网关634(例如,图5的互联网网关534),并且(多个)app子网626可以通信地耦合到控制平面数据层628中包含的(多个)DB子网630以及服务网关636(例如图5的服务网关)和网

络地址转换(NAT)网关638(例如图5的NAT网关538)。控制平面VCN 616可以包括服务网关636和NAT网关638。

[0085] 控制平面VCN 616可以包括数据平面镜像app层640(例如,图5的数据平面镜像app层540),数据平面镜像app层640可以包括(多个)app子网626。数据平面镜像app层640中包含的(多个)app子网626可以包括可执行计算实例644(例如,类似于图5的计算实例544)的虚拟网络接口控制器(VNIC)642(例如,VNIC 542)。计算实例644可以促进数据平面镜像app层640的(多个)app子网626和可包含在数据平面app层646(例如,图5的数据平面app层546)中的(多个)app子网626之间经由数据平面镜像app层640中包含的VNIC 642和数据平面app层646中包含的VNIC 642的通信。

[0086] 控制平面VCN 616中包含的互联网网关634可以通信地耦合到元数据管理服务652(例如,图5的元数据管理服务552),元数据管理服务652可以通信地耦合到公共互联网654(例如,图5的公共互联网554)。公共互联网654可以通信地耦合到控制平面VCN 616中包含的NAT网关638。控制平面VCN 616中包含的服务网关636可以通信地耦合到云服务656(例如,图5的云服务556)。

[0087] 在一些示例中,数据平面VCN 618可以包含在客户租赁621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 616,并且IaaS提供商可以为每个客户建立在服务租赁619中包含的唯一计算实例644。每个计算实例644可以允许服务租赁619中包含的控制平面VCN 616和在客户租赁621中包含的数据平面VCN 618之间的通信。计算实例644可以允许在服务租赁619中包含的控制平面VCN 616中供应的资源在客户租赁621中包含的数据平面VCN 618中部署或以其他方式使用。

[0088] 在其他示例中,IaaS提供商的客户可以具有驻留在客户租赁621中的数据库。在该示例中,控制平面VCN 616可以包括可包括(多个)app子网626的数据平面镜像app层640。数据平面镜像app层640可以驻留在数据平面VCN 618中,但是数据平面镜像app层640可以不驻留在数据平面VCN 618中。也就是说,数据平面镜像app层640可以访问客户租赁621,但是数据平面镜像app层640可以不存在于数据平面VCN 618中或者由IaaS提供商的客户拥有或运营。数据平面镜像app层640可以被配置为对数据平面VCN 618进行调用,但可以不被配置为对控制平面VCN 616中包含的任何实体进行调用。客户可能期望部署或以其他方式使用在控制平面VCN 616中供应的数据平面VCN 618中的资源,并且数据平面镜像app层640可以促进客户的期望部署或资源的其他使用。

[0089] 在一些实施例中,IaaS提供商的客户可以将过滤器应用于数据平面VCN 618。在该实施例中,客户可以确定数据平面VCN 618可以访问什么,并且客户可以限制从数据平面VCN 618对公共互联网654的访问。IaaS提供商可能不能应用过滤器或以其他方式控制数据平面VCN 618对任何外部网络或数据库的访问。由客户将过滤器和控制应用于包含在客户租赁621中的数据平面VCN 618上,可以帮助将数据平面VCN 618与其他客户和公共互联网654隔离。

[0090] 在一些实施例中,云服务656可以由服务网关636调用以访问可能不存在于公共互联网654、控制平面VCN 616或数据平面VCN 618上的服务。云服务656和控制平面VCN 616或数据平面VCN 618之间的连接可能不是实时的或连续的。云服务656可以存在于由IaaS提供商拥有或运营的不同网络上。云服务656可以被配置为从服务网关636接收调用,并且可以

被配置为不接收来自公共互联网654的调用。一些云服务656可以与其他云服务656隔离，并且控制平面VCN 616可以与可能与控制平面VCN 616不在同一区域中的云服务656隔离。例如，控制平面VCN 616可以位于“区域1”中，而云服务“部署6”可以位于区域1和“区域2”中。如果位于区域1中的控制平面VCN 616中包含的服务网关636对部署6进行调用，则该调用可以被传输到区域1中的部署6。在该示例中，控制平面VCN 616或区域1中的部署6可以通信地耦合到区域2中的部署6，或者以其他方式与区域2中的部署6通信。

[0091] 图7是示出根据至少一个实施例的IaaS架构的另一示例模式的框图700。服务运营商702(例如，图5的服务运营商502)可以通信地耦合到安全主机租赁704(例如，图5的安全主机租赁504)，该安全主机租赁704可以包括虚拟云网络(VCN)706(例如，图5的VCN 506)和安全主机子网708(例如，图5的安全主机子网508)。VCN 706可以包括LPG 710(例如，图5的LPG 510)，其可以经由SSH VCN 712中包含的LPG 710通信地耦合到SSH VCN 712(例如，图5的SSH VCN 512)。SSH VCN 712可以包括SSH子网714(例如，图5的SSH子网514)，并且SSH VCN 712可以经由控制平面VCN 716中包含的LPG 710通信地耦合到控制平面VCN 716(例如，图5的控制平面VCN 516)，并且可以经由数据平面VCN 718中包含的LPG 710来通信地耦合到数据平面VCN 718(例如，图5的数据平面518)。控制平面VCN 716和数据平面VCN 718可以包含在服务租赁719(例如，图5的服务租赁519)中。

[0092] 控制平面VCN 716可以包括可包括(多个)负载均衡器(LB)子网722(例如，图5的(多个)LB子网522)的控制平面DMZ层720(例如，图5的控制平面DMZ层520)、可包括(多个)app子网726(例如，类似于图5的(多个)app子网526)的控制平面app层724(例如，图5的控制平面app层524)、可包括(多个)DB子网730的控制平面数据层728(例如，图5的控制平面数据层528)。控制平面DMZ层720中包含的(多个)LB子网722可以通信地耦合到控制平面app层724中包含的(多个)app子网726以及可包含在控制平面VCN 716中的互联网网关734(例如，图5的互联网网关534)，并且(多个)app子网726可以通信地耦合到控制平面数据层728中包含的(多个)DB子网730以及服务网关736(例如，图5的服务网关)和网络地址转换(NAT)网关738(例如，图5的NAT网关538)。控制平面VCN 716可以包括服务网关736和NAT网关738。

[0093] 数据平面VCN 718可以包括数据平面app层746(例如，图5的数据平面app层546)、数据平面DMZ层748(例如，图5的数据平面DMZ层548)和数据平面数据层750(例如，图5的数据平面数据层550)。数据平面DMZ层748可以包括可通信地耦合到数据平面app层746的(多个)可信app子网760和(多个)不可信app子网762以及数据平面VCN 718中包含的互联网网关734的(多个)LB子网722。(多个)可信app子网760可以通信地耦合到数据平面VCN 718中包含的服务网关736、数据平面VCN 718中包含的NAT网关738、以及数据平面数据层750中包含的(多个)DB子网730。(多个)不可信app子网762可以通信地耦合到数据平面数据层750中包含的数据平面VCN 718和(多个)DB子网730中包含的服务网关736。数据平面数据层750可以包括可以通信地耦合到数据平面VCN 718中包含的服务网关736的(多个)DB子网730。

[0094] (多个)不可信app子网762可以包括可通信地耦合到租户虚拟机(VM)766(1)-(N)的一个或多个主要VNIC 764(1)-(N)。每个租户VM 766(1)-(N)可以通信地耦合到可包含在各个容器出口VCN 768(1)-(N)中的各个app子网767(1)-(N)，容器出口VCN 768(1)-(N)可以包含在各个客户租赁770(1)-(N)中。各个次要VNIC 772(1)-(N)可以促进数据平面VCN 718中包含的(多个)不可信app子网762与容器出口VCN 768(1)-(N)中包含的app子网之间

的通信。每个容器出口VCN 768(1)-(N)可以包括NAT网关738,其可以通信地耦合到公共互联网754(例如,图5的公共互联网554)。

[0095] 包含在控制平面VCN 716中并且包含在数据平面VCN 718中的互联网网关734可以通信地耦合到元数据管理服务752(例如,图5的元数据管理系统552),元数据管理服务752可以通信地耦合到公共互联网754。公共互联网754可以通信地耦合到包含在控制平面VCN 716中和包含在数据平面VCN 718中的NAT网关738。包含在控制平面VCN 716中和包含在数据平面VCN 718中的服务网关736可以通信地耦合到云服务756。

[0096] 在一些实施例中,数据平面VCN 718可以与客户租赁770集成。在某些情况下,例如在执行代码时可能需要支持的情况下,这种集成对于IaaS提供程序的客户可能是有用或可取的。客户可能会提供要运行的代码,这些代码可能是破坏性的,可能会与其他客户资源通信,或者可能会导致不良影响。响应于此,IaaS提供商可以确定是否运行由客户提供给IaaS提供商的代码。

[0097] 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,并且请求将功能附连到数据平面app层746。运行该功能的代码可以在VM 766(1)-(N)中执行,并且该代码可以不被配置为在数据平面VCN 718上的任何其他地方运行。每个VM 766(1)-(N)可以连接到一个客户租赁770。包含在VM 766(1)-(N)中的各个容器771(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,运行代码的容器771(1)-(N),其中容器771(1)-(N)可以被包含在至少包含在(多个)不可信app子网762中的VM766(1)-(N)中),这可以帮助防止不正确或以其他方式不期望看到的代码损害IaaS提供商的网络或损害不同客户的网络。容器771(1)-(N)可以通信地耦合到客户租赁770,并且可以被配置为从客户租赁770发送数据或从客户租赁770接收数据。容器771(1)-(N)可以不被配置为向数据平面VCN 718中的任何其他实体发送数据或从数据平面VCN 718中的任何其他实体接收数据。在完成运行代码后,IaaS提供者可以杀死或以其他方式处置容器771(1)-(N)。

[0098] 在一些实施例中,(多个)可信app子网760可以运行可由IaaS提供商拥有或运营的代码。在该实施例中,(多个)可信app子网760可以通信地耦合到(多个)DB子网730,并且可以被配置为在(多个)DB子网730中执行CRUD操作。(多个)不可信app子网762可以通信地耦合到(多个)DB子网730,但是在该实施例中,(多个)不可信app子网可以被配置为在(多个)DB子网730中执行读操作。可以包含在每个客户的VM766(1)-(N)中并且可以运行来自客户的代码的容器771(1)-(N)可以不与(多个)DB子网730通信地耦合。

[0099] 在其他实施例中,控制平面VCN 716和数据平面VCN 718可以不直接通信地耦合。在该实施例中,在控制平面VCN 716和数据平面VCN 718之间可以不存在直接通信。然而,通信可以通过至少一种方法间接进行。LPG 710可以由IaaS提供商建立,其可以促进控制平面VCN 716和数据平面VCN 718之间的通信。在另一示例中,控制平面VCN 716或数据平面VCN 718可以经由服务网关736对云服务756进行调用。例如,从控制平面VCN 716对云服务756的调用可以包括对可以与数据平面VCN 718通信的服务的请求。

[0100] 图8是示出根据至少一个实施例的IaaS架构的另一示例模式的框图800。服务运营商802(例如,图5的服务运营商502)可以通信地耦合到安全主机租赁804(例如,图5的安全主机租赁504),该安全主机租赁804可以包括虚拟云网络(VCN)806(例如,图5的VCN 506)和安全主机子网808(例如,图5的安全主机子网508)。VCN 806可以包括LPG 810(例如,图5的

LPG 510),其可以经由包含在SSH VCN 812中的LPG 810通信地耦合到SSH VCN 812(例如,图5的SSH VCN 512)。SSH VCN 812可以包括SSH子网814(例如,图5的SSH子网514),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(例如,图5的控制平面VCN 516),并且可以经由包含在数据平面VCN 818中的LPG 810来通信地耦合到数据平面VCN 818(例如,图5的数据平面518)。控制平面VCN 816和数据平面VCN 818可以包含在服务租赁819中(例如,图5的服务租赁519)。

[0101] 控制平面VCN 816可以包括可包括(多个)LB子网822(例如,图5的(多个)LB子网522)的控制平面DMZ层820(例如,图5的控制平面DMZ层520)、可包括(多个)app子网826(例如,图5的(多个)app子网526)的控制平面应用层824(例如,图5的控制平面app层524)、可包括(多个)DB子网830(例如,图7的(多个)DB子网730)的控制平面数据层828(例如,图5的控制平面数据层528)。控制平面DMZ层820中包含的(多个)LB子网822可以通信地耦合到控制平面应用层824中包含的(多个)app子网826和可包含在控制平面VCN 816中的互联网网关834(例如,图5的互联网网关534),并且(多个)app子网826可以通信地耦合到控制平面数据层828中包含的(多个)DB子网830以及服务网关836(例如,图5的服务网关)和网络地址转换(NAT)网关838(例如,图5的NAT网关538)。控制平面VCN 816可以包括服务网关836和NAT网关838。

[0102] 数据平面VCN 818可以包括数据平面app层846(例如,图5的数据平面app层546)、数据平面DMZ层848(例如,图5的数据平面DMZ层548)和数据平面数据层850(例如,图5的数据平面数据层550)。数据平面DMZ层848可以包括可通信地耦合到数据平面app层846的(多个)可信app子网860(例如,图7的(多个)可信app子网760)和(多个)不可信app子网862(例如,图7的(多个)不可信app子网762)和包含在数据平面VCN 818中的互联网网关834的(多个)LB子网822。(多个)可信app子网860可以通信地耦合到数据平面VCN 818中包含的服务网关836、数据平面VCN 818中包含的NAT网关838以及数据平面数据层850中包含的(多个)DB子网830。(多个)不可信app子网862可以通信地耦合到数据平面数据层850中包含的数据平面VCN 818中的服务网关836和数据平面数据层850中包含的(多个)DB子网830。数据平面数据层850可以包括可通信地耦合到数据平面VCN 818中包含的服务网关836的(多个)DB子网830。

[0103] (多个)不可信app子网862可以包括主要VNIC 864(1)-(N),其可以通信地耦合到驻留在(多个)不可信app子网862内的租户虚拟机(VM)866(1)-(N)。每个租户VM 866(1)-(N)可以在各自的容器867(1)-(N)中运行代码,并且可以通信地耦合到可以包含在容器出口VCN 868中的数据平面app层846中的app子网826。各个次要VNIC 872(1)-(N)可以促进数据平面VCN 818中包含的(多个)不可信app子网862与容器出口VCN 868中包含的APP子网之间的通信。容器出口VCN可以包括NAT网关838,其可以通信地耦合到公共互联网854(例如,图5的公共互联网554)。

[0104] 包含在控制平面VCN 816中并包含在数据平面VCN 818中的互联网网关834可以通信地耦合到元数据管理服务852(例如,图5的元数据管理系统552),其可以通信地耦合到公共互联网854。公共互联网854可以通信地耦合到包含在控制平面VCN 816中和包含在数据平面VCN 818中的NAT网关838。包含在控制平面VCN 816中和包含在数据平面VCN 818中的服务网关836可以通信地耦合到云服务856。

[0105] 在一些示例中,图8的框图800的架构所示的模式可以被认为是图6的框图600的架构所示的模式的例外,并且如果IaaS提供商不能直接与客户(例如,断开的区域)通信,则IaaS提供商的客户可能期望该模式。客户可以实时访问每个客户的VM 866(1)-(N)中包含的各个容器867(1)-(N)。容器867(1)-(N)可以被配置为调用可包含在容器出口VCN 868中的数据平面app层846的(多个)app子网826中包含的各个次要VNIC 872(1)-(N)。次要VNIC 872(1)-(N)可以将调用发送到NAT网关838,NAT网关838可以将调用发送到公共互联网854。在该示例中,可以由客户实时访问的容器867(1)-(N)可以与控制平面VCN 816隔离,并且可以与数据平面VCN 818中包含的其他实体隔离。容器867(1)-(N)也可以与来自其他客户的资源隔离。

[0106] 在其他示例中,客户可以使用容器867(1)-(N)来调用云服务856。在该示例中,客户可以在容器867(1)-(N)中运行请求来自云服务856的服务的代码。容器867(1)-(N)可以将该请求发送到次要VNIC872(1)-(N),次要VNIC 872(1)-(N)可以将该请求发送到NAT网关,该NAT网关可以将该请求发送到公共互联网854。公共互联网854可以经由互联网网关834将该请求发送到控制平面VCN 816中包含的(多个)LB子网822。响应于确定请求有效,(多个)LB子网可以将请求发送到(多个)app子网826,其可以经由服务网关836将请求发送到云服务856。

[0107] 应当理解,图中所示的IaaS架构500、600、700、800可以具有不同于所示组件的其他组件。此外,图中所示的实施例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。在一些其他实施例中,IaaS系统可以具有比附图中所示更多或更少的组件,可以组合两个或更多组件,或者可以具有不同的组件配置或排列。

[0108] 在某些实施例中,本文描述的IaaS系统可以包括以自助、基于订阅、弹性可扩展、可靠、高度可用和安全的方式递送给客户的一套应用、中间件和数据库服务产品。这种IaaS系统的示例是由本受让人提供的Oracle Cloud Infrastructure(OCI)。

[0109] 图9示出了其中可以实现各种实施例的示例计算机系统900。系统900可用于实现上述任何计算机系统。如图所示,计算机系统900包括处理单元904,其经由总线子系统902与多个外围子系统通信。这些外围子系统可以包括处理加速单元906、I/O子系统908、存储子系统918和通信子系统924。存储子系统918包括有形计算机可读存储介质922和系统存储器910。

[0110] 总线子系统902提供用于让计算机系统900的各种组件和子系统按预期彼此通信的机制。虽然总线子系统902示意性地示出为单总线,但是总线子系统的可选实施例可以利用多个总线。总线子系统902可以是几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、外围设备总线、以及使用各种总线架构中的任何一种的本地总线。例如,这样的架构可以包括工业标准架构(ISA)总线、微通道架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围组件互连(PCI)总线,其可以被实现为按照IEEE P1386.1标准制造的夹层总线。

[0111] 可以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904控制计算机系统900的操作。处理单元904中可以包括一个或多个处理器。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904可以被实现为具有包括在每个处理单元中的单核或多核处理器的一个或多个独立处理单元932和/或934。在其他实施例中,

处理单元904还可以实现为通过将两个双核处理器集成到单个芯片中而形成的四核处理单元。

[0112] 在各种实施例中,处理单元904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。在任何给定时间,要执行的程序代码中的一些或全部可以驻留在(多个)处理器904中和/或存储子系统918中。通过适当的编程,(多个)处理器904可以提供上述各种功能。计算机系统900还可以包括处理加速单元906,其可以包括数字信号处理器(DSP)、专用处理器等。

[0113] I/O子系统908可以包括用户界面输入设备和用户界面输出设备。用户界面输入设备可以包括键盘、诸如鼠标或轨迹球之类的定点设备、集成到显示器中的触摸板或触摸屏、滚轮、点击轮、转盘、按钮、开关、小键盘、具有语音命令识别系统的音频输入设备、麦克风和其他类型的输入设备。用户界面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,其使用户能够通过使用手势和口头命令的自然用户界面来控制输入设备,并与诸如Microsoft Xbox®360游戏控制器的输入设备交互。用户界面输入设备还可以包括诸如Google Glass®眨眼检测器之类的眼势识别设备,其检测来自用户的眼部活动(例如,在拍照和/或进行菜单选择时眨眼),并将眼势转换为输入设备(例如,Google Glass®)。此外,用户界面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。

[0114] 用户界面输入设备还可以包括但不限于三维(3D)鼠标、操纵杆或指点杆、游戏手柄和图形输入板,以及诸如扬声器、数码相机、数码摄像机、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、激光测距仪和眼睛注视跟踪设备的音频/视频设备。此外,用户界面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、位置发射断层扫描、医学超声成像设备。用户界面输入设备还可以包括例如音频输入设备,诸如MIDI键盘、数字乐器等。

[0115] 用户界面输出设备可以包括显示子系统、指示灯或诸如音频输出设备等的非可视显示器等。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将信息从计算机系统900输出到用户或其他计算机的所有可能类型的设备和机构。例如,用户界面输出设备可以包括但不限于各种可视地传达文本、图形和音频/视频信息的显示设备,诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备和调制解调器。

[0116] 计算机系统900可以包括存储子系统918,其包括被示为当前位于系统存储器910内的软件元素。系统存储器910可以存储在处理单元904上可加载和可执行的程序指令,以及在这些程序的执行期间产生的数据。

[0117] 根据计算机系统900的配置和类型,系统存储器910可以是易失性的(例如,随机存取存储器(RAM))和/或非易失性的(例如只读存储器(ROM)、闪存等)。RAM通常包含可立即由处理单元904访问和/或当前由处理单元904操作和执行的数据和/或程序模块。在一些实现中,系统存储器910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)。在一些实现中,基本输入/输出系统(BIOS)通常可以存储在ROM中,该基本输入/输出系统包含诸如在启动期间帮助在计算机系统900内的元件之间传输信息的基本例程。作为示例而非限制,系统存储器910还示出应用程序912,其可以包括客户端

应用、网络浏览器、中间层应用、关系数据库管理系统(RDBMS)等、程序数据914和操作系统916。作为示例,操作系统916可以包括各种版本的Microsoft Windows®、Apple Macintosh®和/或Linux操作系统、各种市售的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/或移动操作系统,例如iOS、Windows®Phone、Android®OS、BlackBerry®10OS和Palm®OS操作系统。

[0118] 存储子系统918还可以提供有形的计算机可读存储介质,用于存储提供某些实施例的功能的基本编程和数据构造。当由提供上述功能的处理器执行时,可以将软件(程序、代码模块、指令)存储在存储子系统918中。这些软件模块或指令可以由处理单元904执行。存储子系统918还可以提供用于存储根据本公开使用的数据的储存库。

[0119] 存储子系统900还可以包括计算机可读存储介质读取器920,其还可以连接到计算机可读存储介质922。计算机可读存储介质922一起并且可选地与系统存储器910相结合,可以全面地表示远程的、本地的、固定的和/或可移动的存储设备以及用于临时和/或更永久地包含、存储、传输和检索计算机可读信息的存储介质。

[0120] 包含代码或代码部分的计算机可读存储介质922还可以包括本领域中已知或使用的任何适当介质,包括存储介质和通信介质,诸如但不限于以用于存储和/或传输信息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、电可擦除可编程只读存储器(EEPROM)、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光存储、盒式磁带、磁带、磁盘存储或其他磁存储设备、或其他有形的计算机可读介质。这还可以包括诸如数据信号、数据传输之类的非有形计算机可读介质,或可用于传输所需信息并可由计算系统900访问的任何其他介质。

[0121] 作为示例,计算机可读存储介质922可以包括对不可移除、非易失性磁介质进行读写的硬盘驱动器,对可移除、非易失性磁盘进行读写的磁盘驱动器,以及对可移除、非易失性光盘(例如CD ROM、DVD和Blu-Ray®盘)或其他光学介质进行读写的光盘驱动器。计算机可读存储介质922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、数字录像带等。计算机可读存储介质922还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,诸如固态RAM、动态RAM、静态RAM、基于DRAM的SSD、磁阻RAM(MRAM)SSD,以及使用DRAM和基于闪存的SSD的组合的混合SSD。盘驱动器及其相关联的计算机可读介质可以为计算机系统900提供计算机可读指令、数据结构、程序模块和其他数据的非易失性存储。

[0122] 通信子系统924提供到其他计算机系统和网络的接口。通信子系统924用作从其他系统接收数据和从计算机系统900向其他系统发送数据的接口。例如,通信子系统924可以使计算机系统1000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924可以包括用于访问无线语音和/或数据网络的射频(RF)收发机组件(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数据速率)的高层数据网络技术)、Wi-Fi(IEEE 802.11系列标准、或其他移动通信技术、或其任意组合)、全球定位系统接收器组件、和/或其他组件。在一些实施例中,除了无线接口之外或代替无线接口,通信子系统924可以提供有线网络连接(例如,以太网)。

[0123] 在一些实施例中,通信子系统924还可以代表可以使用计算机系统900的一个或多个用户接收结构化和/或非结构化数据馈送926、事件流928、事件更新930等形式的输入通信。

[0124] 作为示例,通信子系统924可以被配置为实时地从社交网络和/或其他通信服务的用户接收数据馈送926,其他通信服务诸如Twitter®馈送、Facebook®更新、诸如丰富站点摘要(RSS)馈送之类的网络馈送、和/或来自一个或多个第三方信息源的实时更新。

[0125] 此外,通信子系统924还可以被配置为接收连续数据流形式的数据,该连续数据流可以包括实时事件的事件流928和/或事件更新930,其本质上可以是连续的或没有明确结束的。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、金融自动收报机、网络性能测量工具(例如,网络监控和业务管理应用)、点击流分析工具、汽车业务监控等。

[0126] 通信子系统924还可以被配置为将结构化和/或非结构化数据馈送926、事件流928、事件更新930等输出到可以与耦合到计算机系统900的一个或多个流数据源计算机通信的一个或多个数据库。

[0127] 计算机系统900可以是各种类型中的一种,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、信息亭、服务器机架或任何其他数据处理系统。

[0128] 由于计算机和网络的不断变化的性质,附图中示出的对计算机系统900的描述仅旨在作为具体示例。具有比附图中描述的系统更多或更少的组件的许多其他配置也是可能的。例如,也可以使用定制的硬件和/或可以在硬件、固件、软件(包括小应用)或其组合中实现特定元素。此外,可以使用到诸如网络输入/输出设备的其他计算设备的连接。基于本文提供的公开和教导,本领域普通技术人员将理解实现各种实施例的其他方式和/或方法。

[0129] 虽然已经描述了具体实施例,但是各种修改、更改、备选构造和等同形式也包含在本公开的范围内。实施例不限于在某些特定数据处理环境中操作,而是自由地在多个数据处理环境中操作。另外,尽管已经使用特定的一系列交易和步骤描述了实施例,但是对于本领域的技术人员而言,显而易见的是,本公开的范围不限于所描述的一系列交易和步骤。上述实施例的各种特征和方面可以单独或联合使用。

[0130] 此外,虽然已经使用硬件和软件的特定组合来描述实施例,但是应当认识到,硬件和软件的其他组合也在本公开的范围内。实施例可以仅在硬件中、或仅在软件中、或使用其组合来实现。本文描述的各种过程可以以任意组合在同一处理器或不同处理器上实现。因此,在组件或模块被描述为被配置为执行某些操作的情况下,这种配置可以例如通过设计用于执行操作的电子电路、通过编程用于执行操作的可编程电子电路(诸如微处理器)或其任意组合来实现。进程可以使用各种技术进行通信,包括但不限于用于进程间通信的传统技术,并且不同的进程对可以使用不同的技术,或者同一对进程可以在不同的时间使用不同的技术。

[0131] 因此,说明书和附图应视为说明性的,而不是限制性的。然而,显而易见的是,可以在不背离权利要求中所阐述的更广泛的精神和范围的情况下对其进行添加、删减、删除以及其他修改和改变。因此,尽管已经描述了具体的公开实施例,但这些不旨在是限制性的。各种修改和等同形式在所附权利要求的范围内。

[0132] 在描述所公开的实施例的上下文中(特别是在以下权利要求的上下文中),除非本

文另有指示或与上下文明显相矛盾,否则使用术语“一”、“该”以及类似的指代将被解释为既包括单数又包括复数。除非另有说明,否则术语“包括”、“具有”、和“包含”应被解释为开放式术语(即,意思是“包括但不限于”)。“连接”一词应被解释为部分或全部包含在、依附或连接在一起,即使有什么东西介入。除非本文另有说明,并且每个单独的值被结合到说明书中,就好像它在本文被单独引用一样,否则,本文引用值范围仅仅是用作单独引用落在该范围内的每个值的速记方法。本文描述的所有方法都可以以任何适当的顺序执行,除非本文另有说明或与上下文明显矛盾。使用本文提供的任何和所有示例或示例性语言(例如,“诸如”)仅意在更好地说明实施例,并且除非另有声明,否则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对本公开的实践必不可少的任何非权利要求的要素。

[0133] 除非另有特别说明,否则,诸如短语“X、Y或Z中的至少一个”的析取语言旨在于一般用于表示项目、术语等可以是X、Y或Z、或其任意组合(例如,X、Y和/或Z)的上下文中理解。因此,这种析取语言通常不旨在也不应该暗示某些实施例要求X中的至少一个、Y中的至少一个或Z中的至少一个都存在。

[0134] 本文描述了本公开的优选实施例,包括用于实施本公开的已知最佳模式。本领域普通技术人员在阅读前述说明后,这些优选实施例的变型可能变得显而易见。本领域技术人员应当能够适当地采用这种变化,并且本公开可以不同于本文具体描述的方式来实施。因此,本公开包括在适用法律允许的情况下,在所附权利要求书中所记载的主题的所有修改和等同形式。此外,除非本文另有说明,否则上述元素在其所有可能的变体中的任何组合都包含在本公开中。

[0135] 本文引用的所有参考文献,包括出版物、专利申请和专利,本文以相同的程度通过引用并入,就像每个参考文献被单独和具体地指示通过引用并入并且本文整体陈述一样。

[0136] 在前述说明书中,参考其特定实施例描述了本公开的各方面,但是本领域技术人员将认识到,本公开不限于此。上述公开的各种特征和方面可以单独或联合使用。此外,在不背离本说明书更广泛的精神和范围的情况下,实施例可以在本文所描述的环境和应用之外的任何数量的环境和应用中使用。因此,说明书和附图应视为说明性的而不是限制性的。

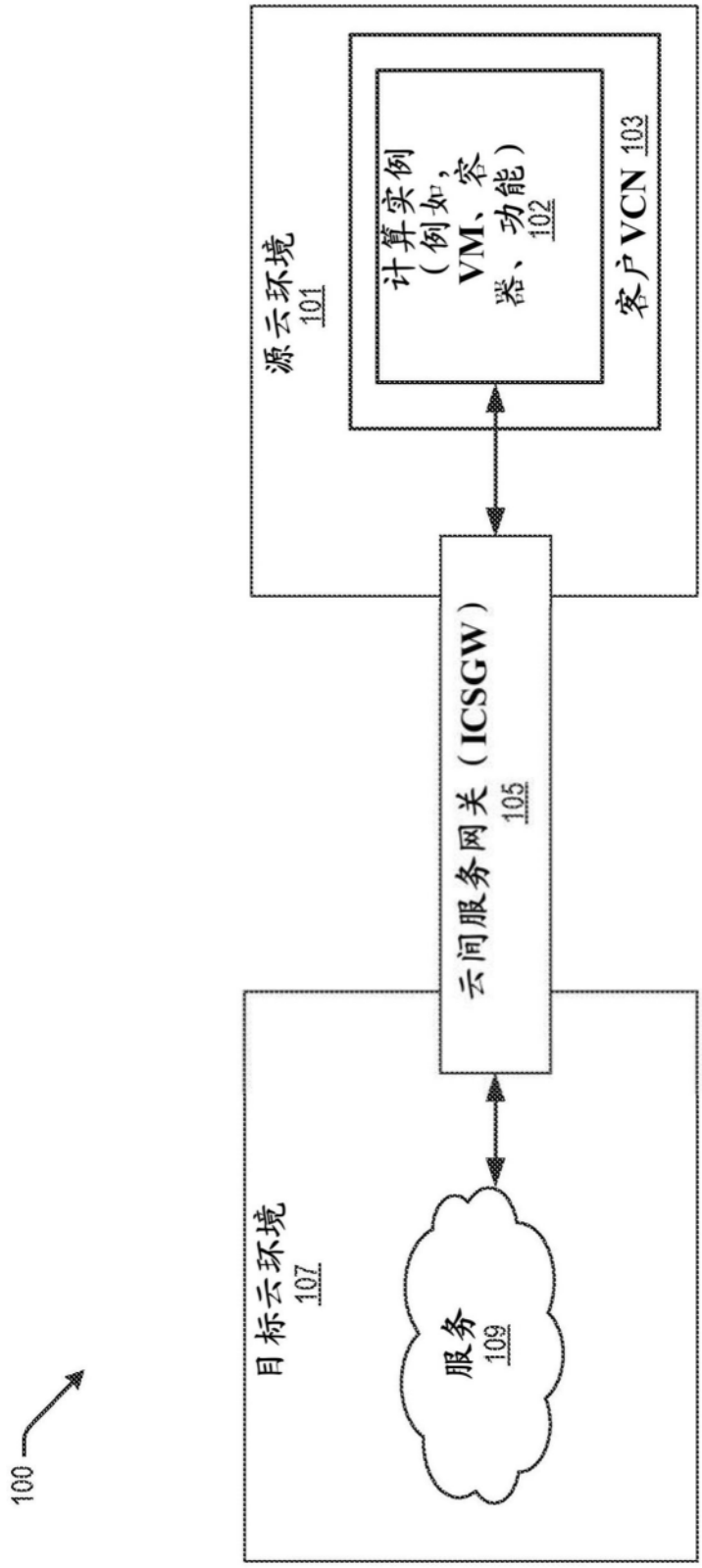

100
源云环境
101
计算实例
（例如，
VM、容
器、功能）
102
客户VCN 103
云间服务网关（ICSGW）
105
目标云环境
107
服务
109

图1

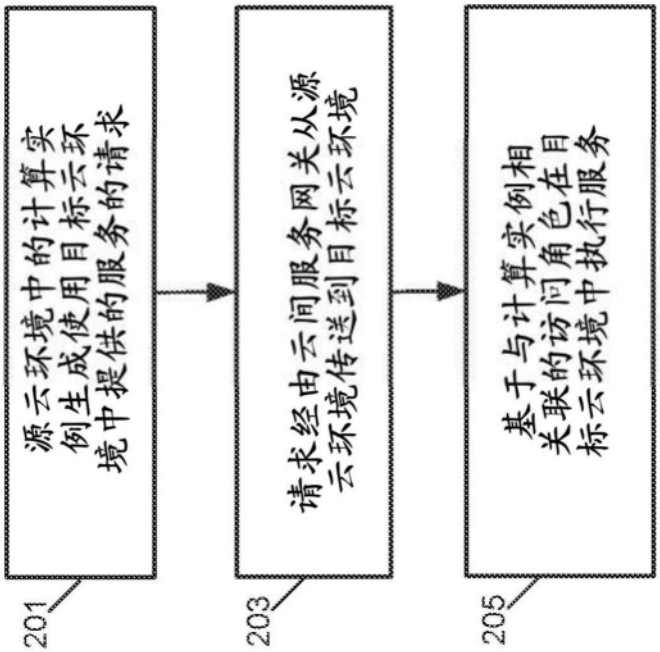

源云环境中的计算实例生成使用目标云环境中提供的服务的请求
201
请求经由云间服务网关从源云环境传送到目标云环境
203
基于与计算实例相关联的访问角色在目标云环境中执行服务
205

图2

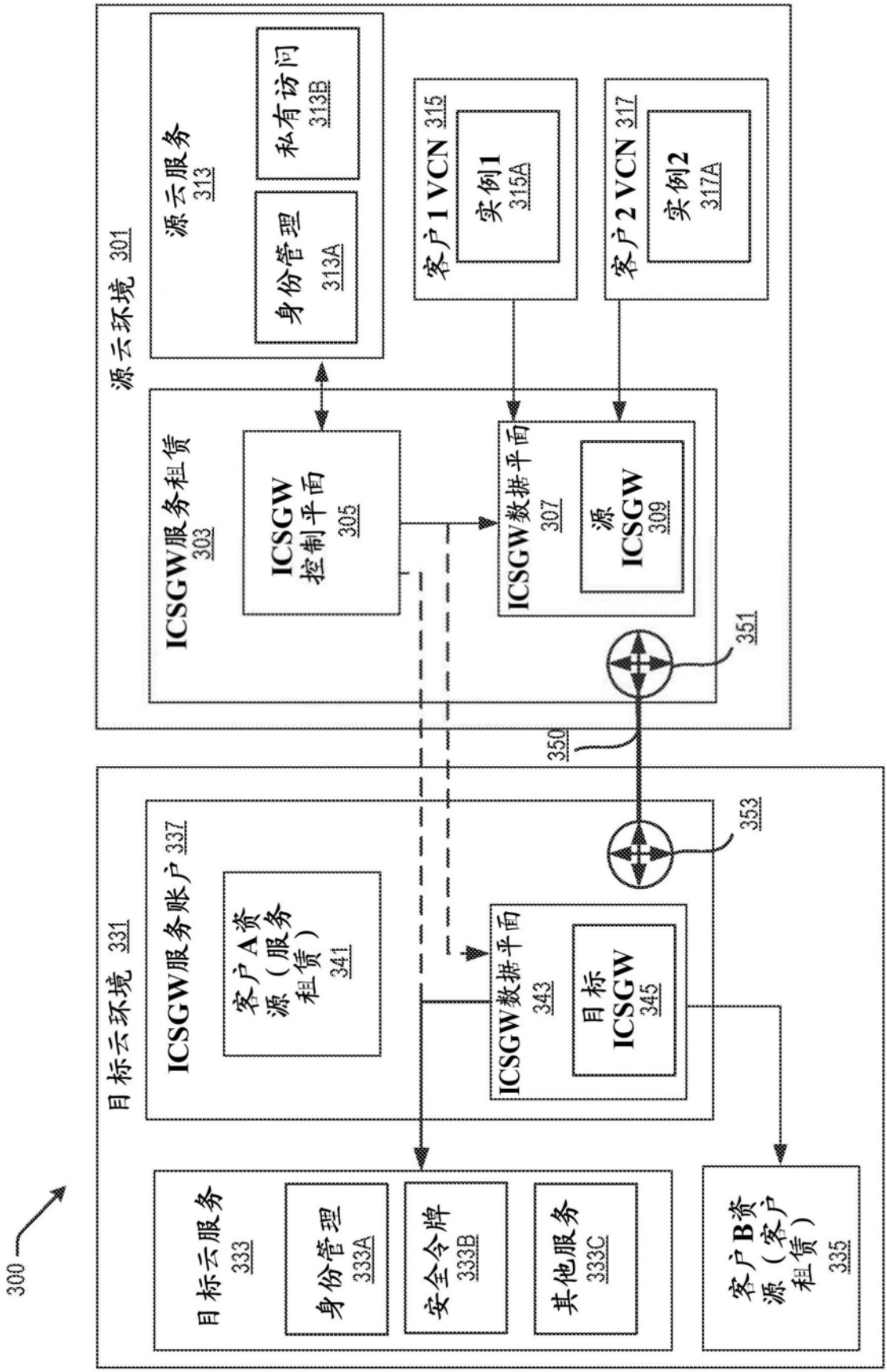

300
源云环境 301
源云服务 313
身份管理 313A
私有访问 313B
客户1 VCN 315
实例1 315A
客户2 VCN 317
实例2 317A
ICSGW服务租赁 303
ICSGW 控制平面 305
ICSGW数据平面 307
源 ICSGW 309
351
350
353
目标云环境 331
ICSGW服务账户 337
客户A资源（服务租赁） 341
ICSGW数据平面 343
目标 ICSGW 345
目标云服务 333
身份管理 333A
安全令牌 333B
其他服务 333C
客户B资源（客户租赁） 335

图3A

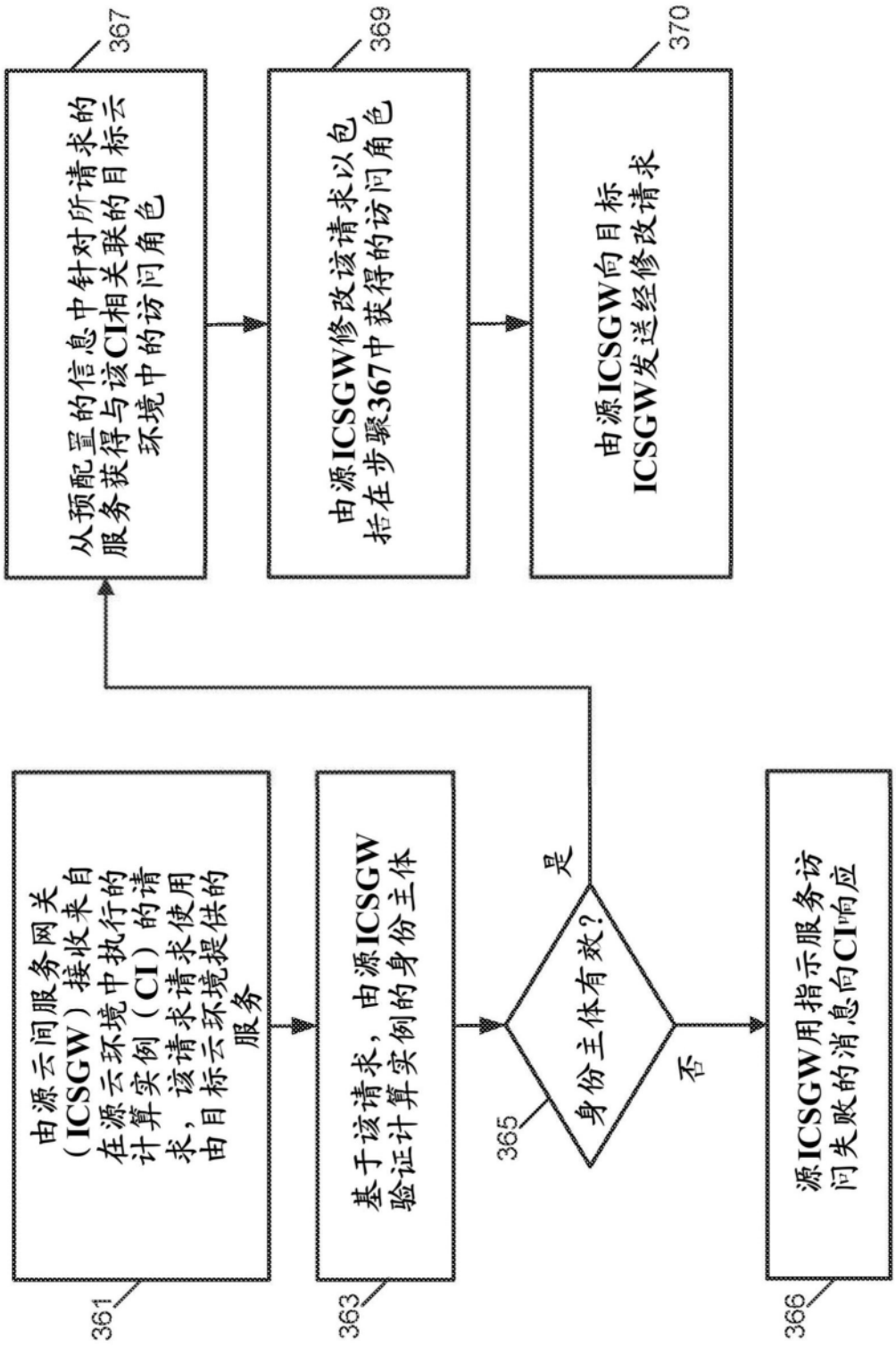

由源云间服务网关（ICSGW）接收来自在源云环境中执行的计算实例（CI）的请求，该请求请求使用由目标云环境提供的服务
361
基于该请求，由源ICSGW验证计算实例的身份主体
363
身份主体有效？
365
是
否
源ICSGW用指示服务访问失败的消息向CI响应
366
从预配置的信息中针对所请求的服务获得与该CI相关联的目标云环境中的访问角色
367
由源ICSGW修改该请求以包括在步骤367中获得的访问角色
369
由源ICSGW向目标ICSGW发送经修改请求
370

图3B

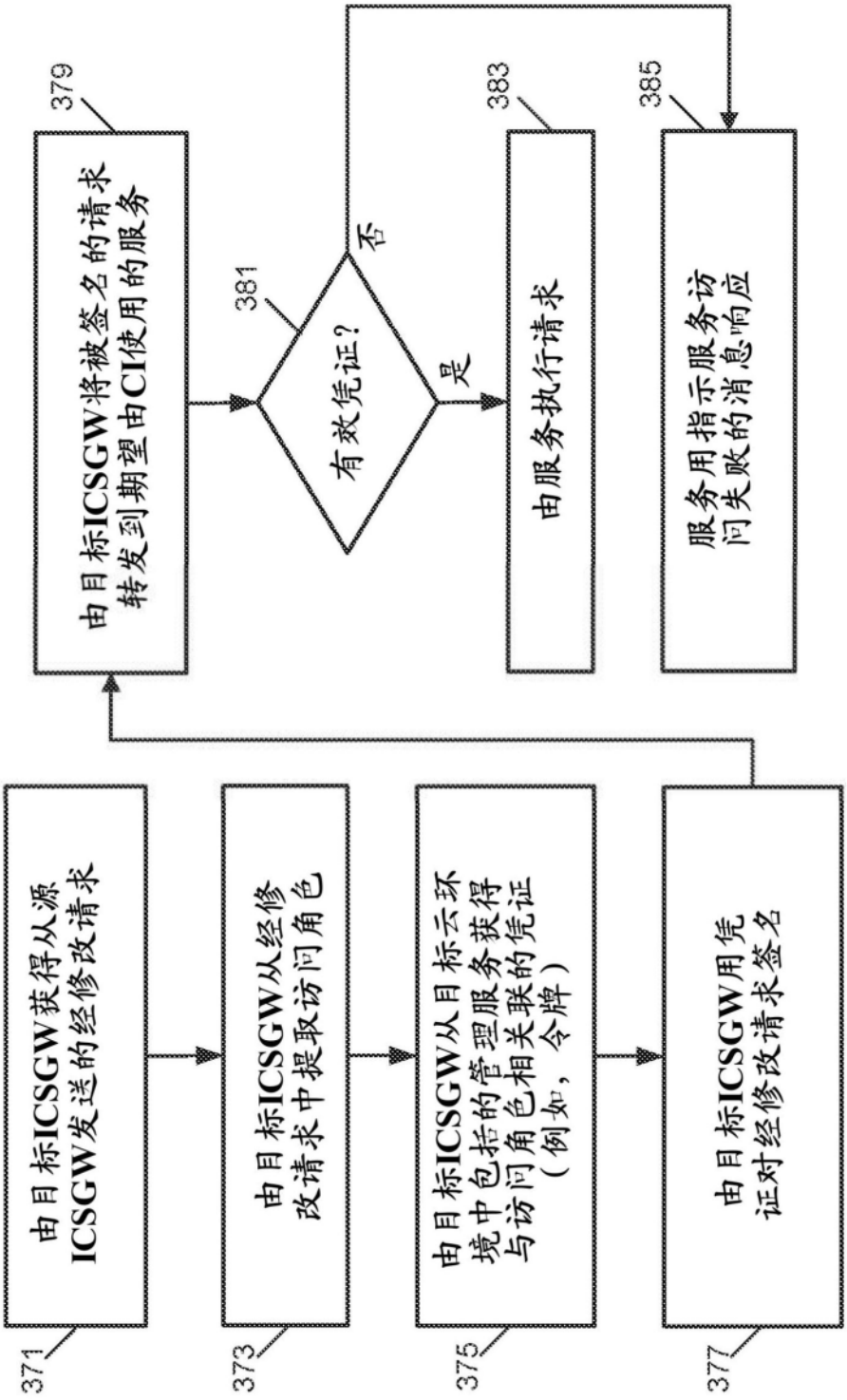

由目标ICSGW获得从源ICSGW发送的经修改请求
371
由目标ICSGW从经修改请求中提取访问角色
373
由目标ICSGW从目标云环境中包括的管理服务获得与访问角色相关联的凭证（例如，令牌）
375
由目标ICSGW用凭证对经修改请求签名
377
由目标ICSGW将被签名的请求转发到期望由CI使用的服务
379
有效凭证?
381
否
是
由服务执行请求
383
服务用指示服务访问失败的消息响应
385

图3C

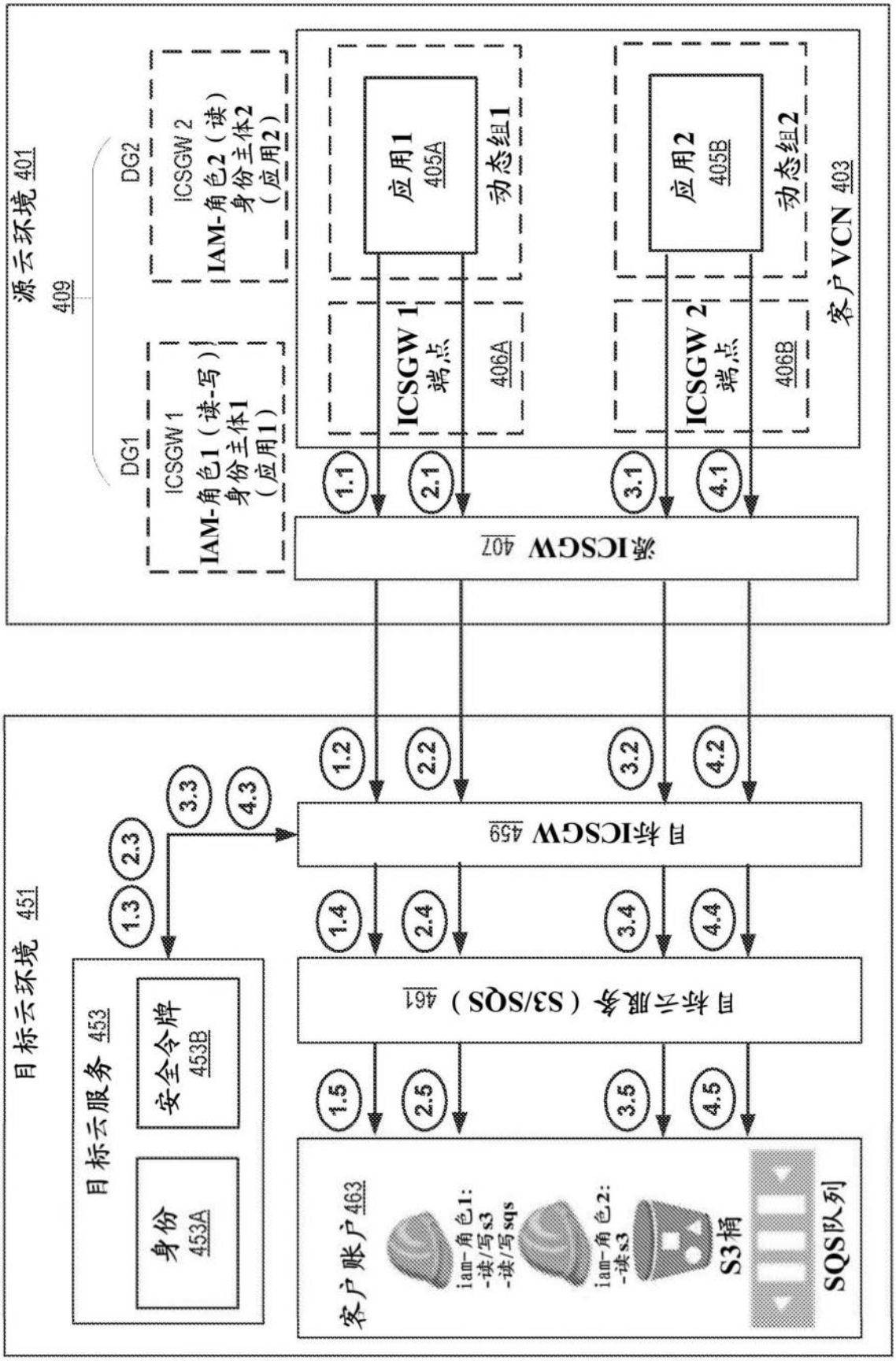

源云环境 401
409
DG1
ICSGW 1
IAM-角色1（读-写）
身份主体1
（应用1）
DG2
ICSGW 2
IAM-角色2（读）
身份主体2
（应用2）
客户 VCN 403
应用1
405A
动态组1
406A
ICSGW 1
端点
应用2
405B
动态组2
406B
ICSGW 2
端点
源ICSGW 407
1.1
2.1
3.1
4.1
目标云环境 451
目标ICSGW 459
1.2
2.2
3.2
4.2
目标云服务 453
身份
453A
安全令牌
453B
1.3
2.3
3.3
4.3
目标云服务（S3/SQS）461
1.4
2.4
3.4
4.4
客户账户463
iam-角色1:
-读/写s3
-读/写sqs
iam-角色2:
-读s3
S3桶
SQS队列
1.5
2.5
3.5
4.5

图4A

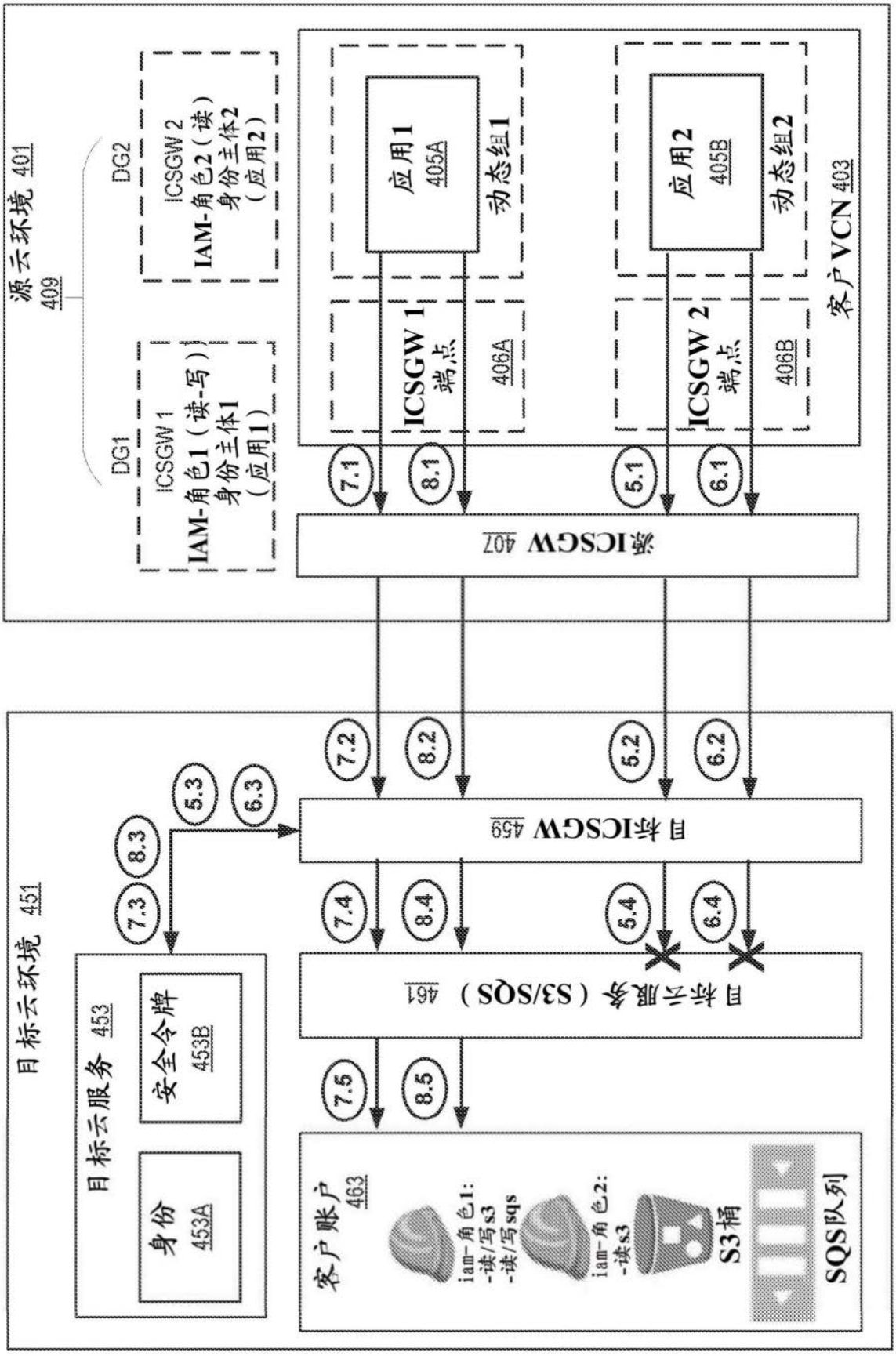

源云环境 401
409
DG1
ICSGW 1
IAM-角色1（读-写）
身份主体1
（应用1）
DG2
ICSGW 2
IAM-角色2（读）
身份主体2
（应用2）
客户VCN 403
应用1
405A
动态组1
406A
ICSGW 1
端点
应用2
405B
动态组2
406B
ICSGW 2
端点
源ICSGW 407
7.1
8.1
5.1
6.1
目标云环境 451
目标ICSGW 459
7.2
8.2
5.2
6.2
目标云服务（S3/SQS） 461
7.4
8.4
5.4
6.4
目标云服务 453
安全令牌
453B
身份
453A
5.3
6.3
7.3
8.3
客户账户
463
iam-角色1:
-读/写s3
-读/写sqs
iam-角色2:
-读s3
S3桶
SQS队列
7.5
8.5

图4B

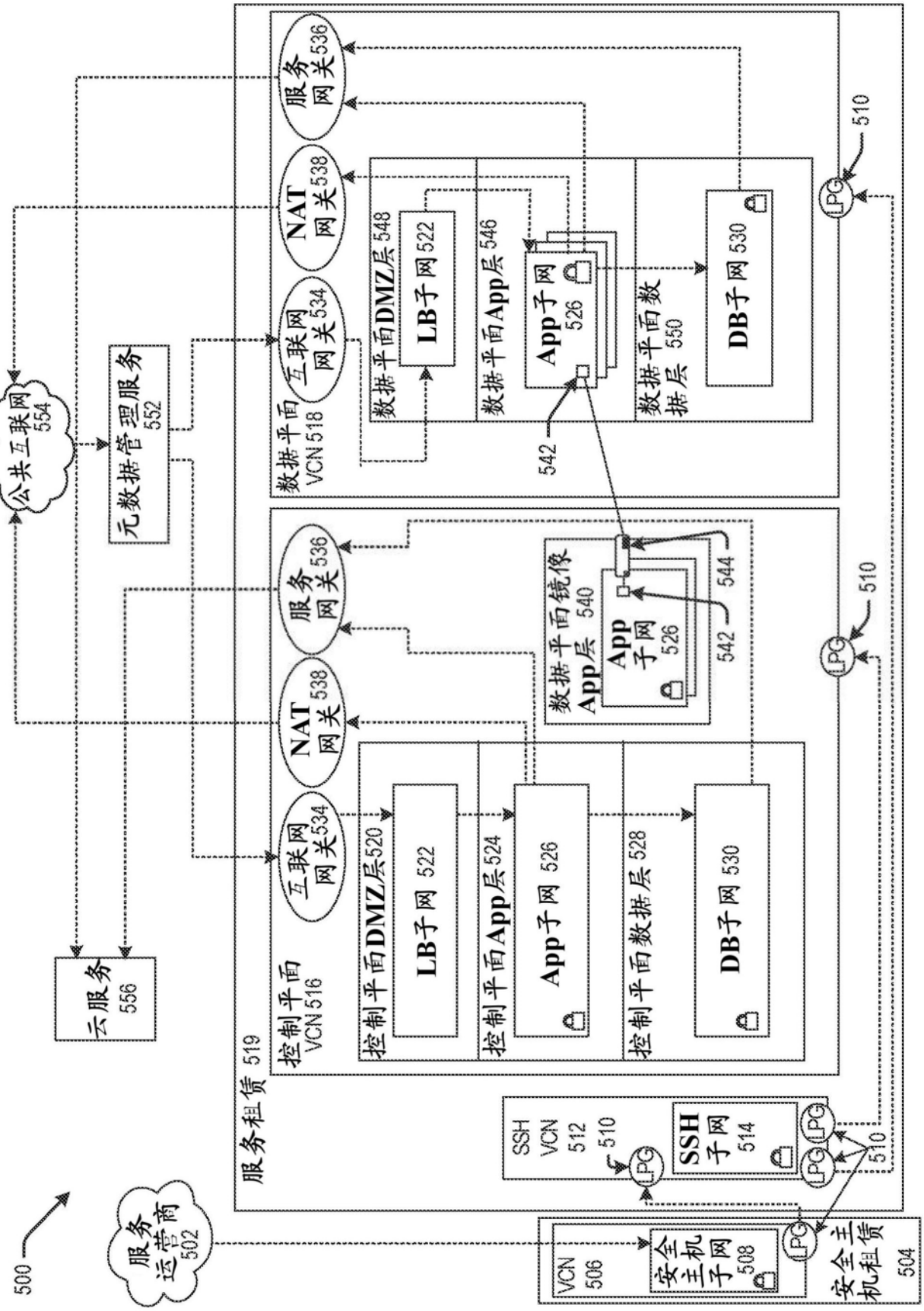

500
服务运营商 502
公共互联网 554
元数据管理服务 552
云服务 556
服务租赁 519
控制平面 VCN 516
互联网网关 534
NAT 网关 538
服务网关 536
控制平面DMZ层 520
LB子网 522
控制平面App层 524
App子网 526
控制平面数据层 528
DB子网 530
数据平面镜像 App层 540
542
544
数据平面 VCN 518
数据平面DMZ层 548
数据平面App层 546
数据平面数据层 550
SSH VCN 512
SSH 子网 514
510
LPG
VCN 506
安全主机子网 508
安全主机租赁 504

图5

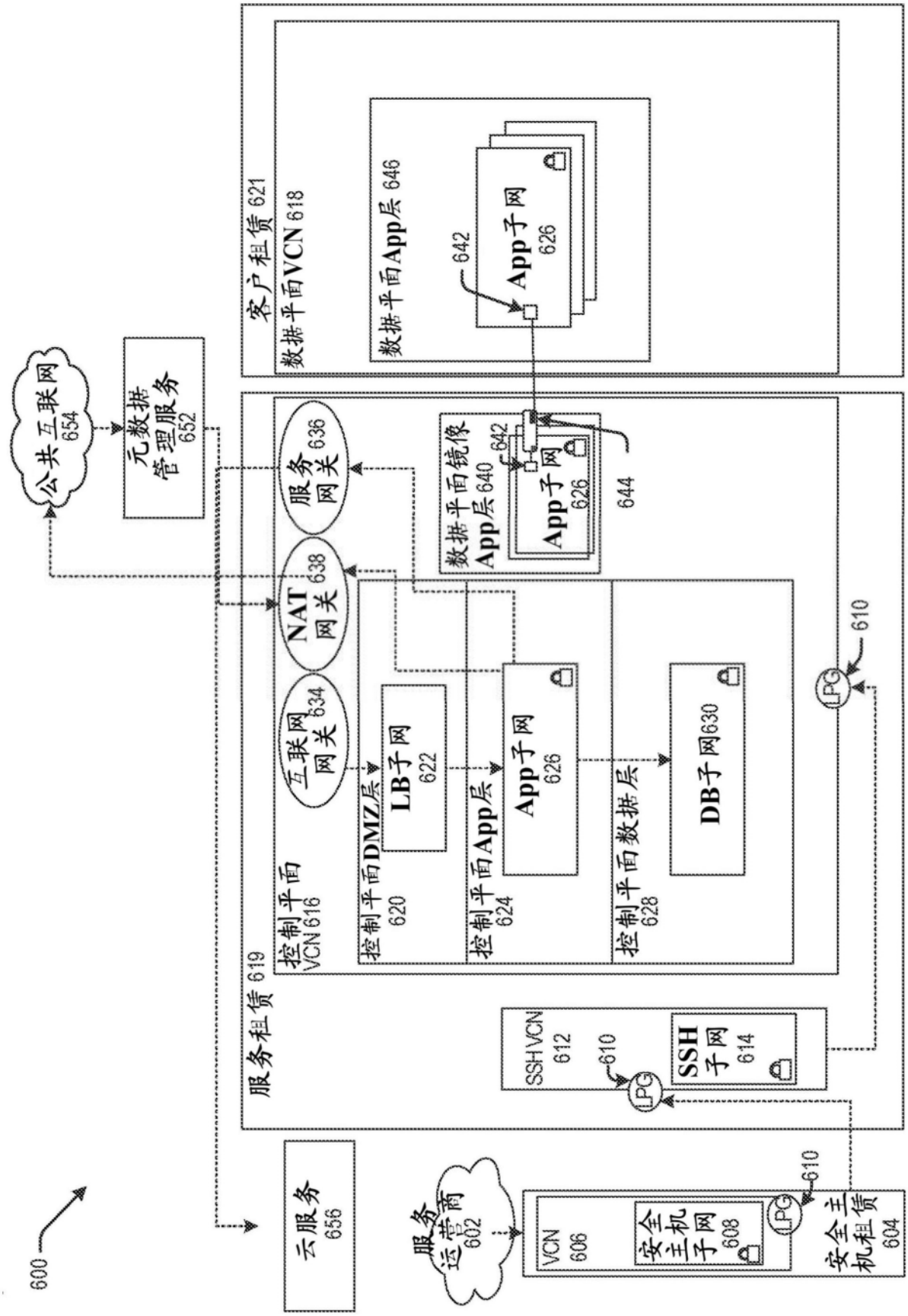

600
公共互联网 654
元数据管理服务 652
云服务 656
服务运营商 602
客户租赁 621
数据平面VCN 618
数据平面App层 646
642
App子网 626
644
服务租赁 619
控制平面VCN 616
服务网关 636
NAT网关 638
互联网网关 634
数据平面镜像App层 640
控制平面DMZ层 620
LB子网 622
控制平面App层 624
App子网 626
控制平面数据层 628
DB子网 630
610
LPG
SSH VCN 612
SSH子网 614
VCN 606
安全主机子网 608
安全主机租赁 604

图6

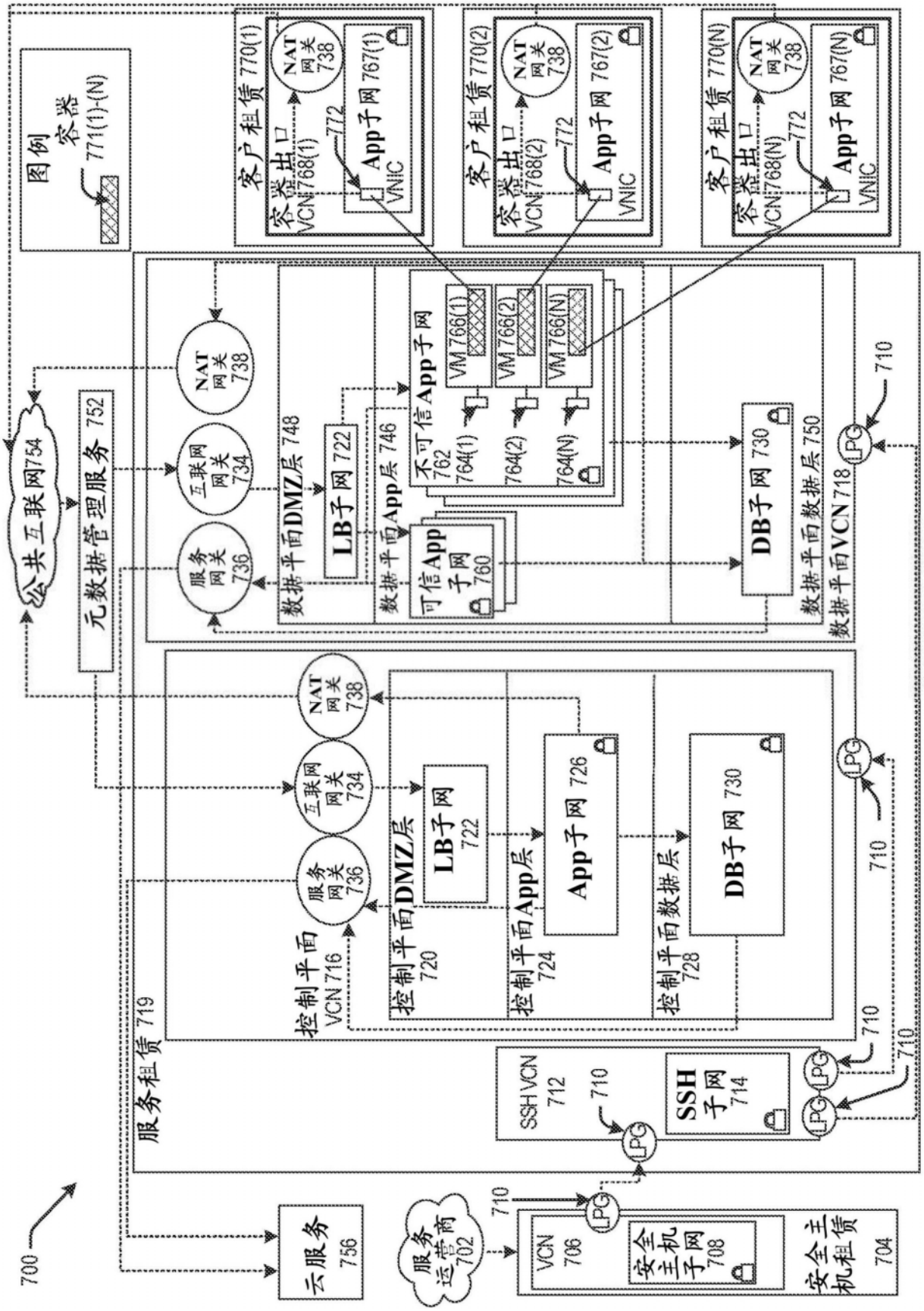

图例
容器
771(1)-(N)
客户租赁 770(1)
容器出口
VCN 768(1)
772
App子网 767(1)
VNIC
NAT网关 738
客户租赁 770(2)
容器出口
VCN 768(2)
772
App子网 767(2)
VNIC
NAT网关 738
客户租赁 770(N)
容器出口
VCN 768(N)
772
App子网 767(N)
VNIC
NAT网关 738
公共互联网754
元数据管理服务 752
互联网网关 734
服务网关 736
数据平面DMZ层 748
LB子网 722
数据平面App层 746
不可信App子网 762
VM 766(1)
VM 766(2)
VM 766(N)
764(1)
764(2)
764(N)
可信App子网 760
DB子网 730
数据平面数据层 750
数据平面VCN 718
710
LPG
服务租赁 719
控制平面VCN 716
控制平面DMZ层 720
LB子网 722
控制平面App层 724
App子网 726
控制平面数据层 728
DB子网 730
SSH VCN 712
SSH子网 714
云服务 756
服务运营商 702
VCN 706
安全主机子网 708
安全主机租赁 704
700

图7

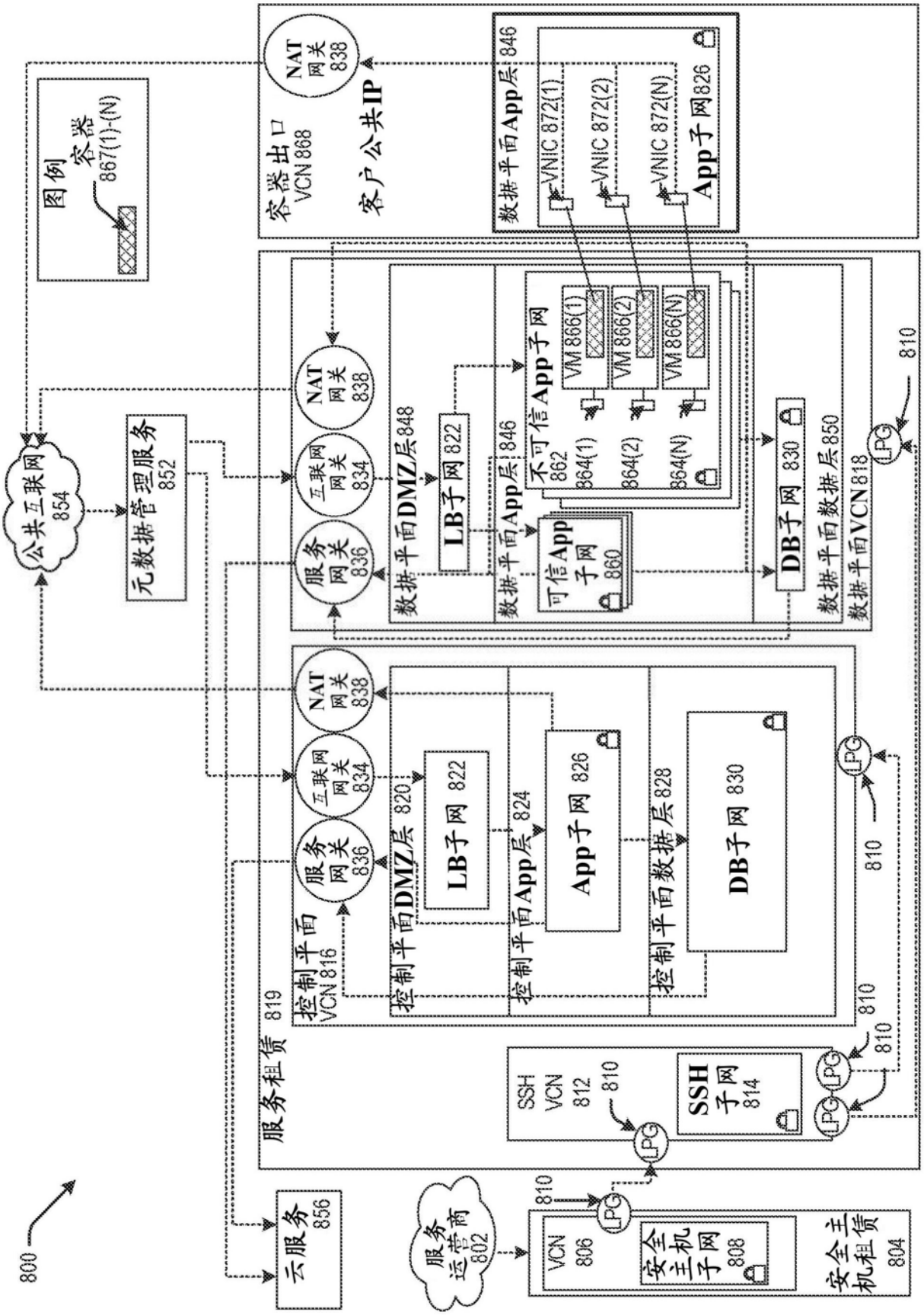

800
图例
容器
867(1)-(N)
公共互联网
854
元数据管理服务
852
云服务
856
服务运营商
802
服务租赁
819
控制平面
VCN 816
服务网关
836
互联网网关
834
NAT网关
838
控制平面DMZ层 820
LB子网 822
控制平面App层 824
App子网 826
控制平面数据层 828
DB子网 830
SSH
VCN
812
SSH
子网
814
VCN
806
安全主机子网
808
安全主机租赁
804
LPG
810
容器出口
VCN 868
客户公共IP
数据平面App层 846
VNIC 872(1)
VNIC 872(2)
VNIC 872(N)
App子网 826
数据平面DMZ层 848
LB子网 822
数据平面App层 846
不可信App子网
862
VM 866(1)
VM 866(2)
VM 866(N)
B64(1)
B64(2)
B64(N)
可信App子网
860
DB子网 830
数据平面数据层 850
数据平面VCN 818

图8

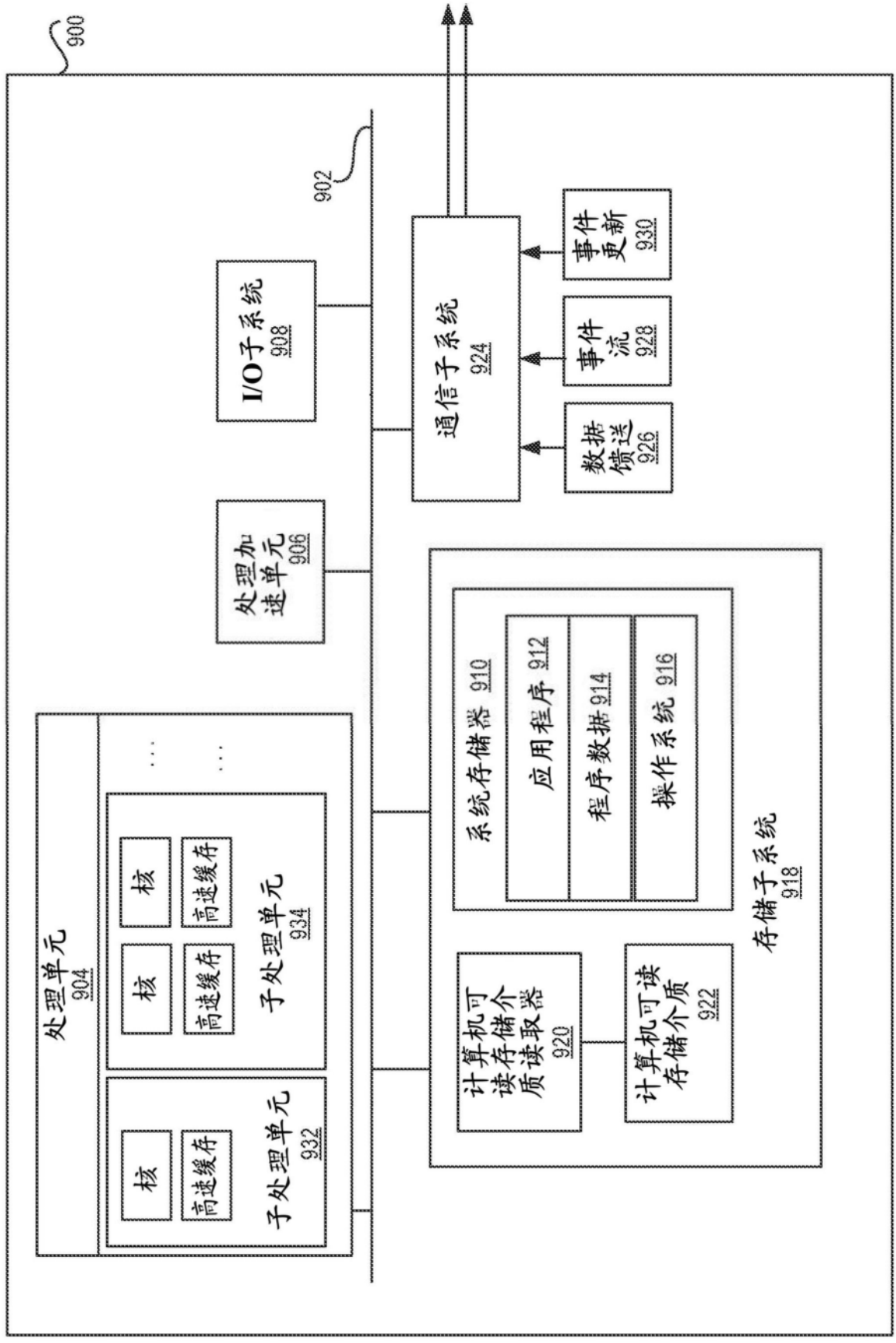

900
902
处理单元
904
核
高速缓存
核
高速缓存
子处理单元
932
核
高速缓存
核
高速缓存
子处理单元
934
I/O子系统
908
处理加速单元
906
通信子系统
924
数据馈送
926
事件流
928
事件更新
930
存储子系统
918
系统存储器 910
应用程序 912
程序数据 914
操作系统 916
计算机可读存储介质读取器
920
计算机可读存储介质
922

图9