(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 120035958 A
(43)申请公布日 2025.05.23

(21)申请号 202380072781.2

(22)申请日 2023.10.13

(30)优先权数据
63/416,042 2022.10.14 US
63/464,903 2023.05.08 US
63/467,241 2023.05.17 US
63/468,739 2023.05.24 US
63/469,763 2023.05.30 US
63/471,573 2023.06.07 US

(85)PCT国际申请进入国家阶段日
2025.04.14

(86)PCT国际申请的申请数据
PCT/US2023/076774 2023.10.13

(87)PCT国际申请的公布数据
WO2024/081838 EN 2024.04.18

(71)申请人 甲骨文国际公司
地址 美国

(72)发明人 M·G·M·伊德 D·施密特
S·科罗廖夫 S·莎玛
I·泽克瑟 N·B·露西娜莫戈隆
V·N·克拉尤什金
S·康德拉捷夫

(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 张鑫

(51)Int.Cl.
H04L 9/40(2006.01)
G06F 21/41(2006.01)
H04L 67/10(2006.01)

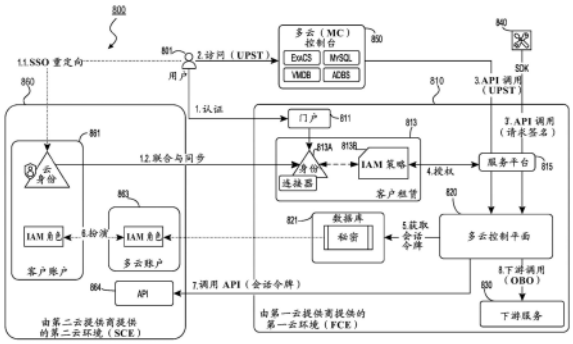
权利要求书3页 说明书53页 附图20页

(54)发明名称

多云基础设施中的身份管理

(57)摘要

描述了用于在第一云基础设施(包括在第一云服务提供商提供的第一云环境中)中提供多云控制平面(MCCP)的技术,该技术使得第一云基础设施中提供的服务和/或资源能够被第二云环境的用户使用,其中第二云环境与第一云环境不同。多云基础设施使得与第二云服务提供商的账户相关联的用户能够从第二云基础设施使用一组一个或多个云服务中的第一服务。多云基础设施在第二云服务提供商的账户与在第一云基础设施中创建的租赁之间创建链路,以使用户能够使用第一服务。



CN 120035958 A

1.一种方法,包括:

由多云基础设施的多云控制台接收来自用户的对服务的请求,所述请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;

由平台基于第一令牌对用户进行授权,所述授权包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;以及

响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

2.如权利要求1所述的方法,还包括:

在第一云环境的登录门户处接收用户的凭证,其中第一令牌由第一身份系统响应于成功认证凭证而生成,并且其中登录门户与多云基础设施的多云控制台不同。

3.如权利要求1或2所述的方法,其中所述请求是在多云控制台的GUI处接收的,所述GUI列出了由多云基础设施供应的多个服务。

4.如权利要求1、2或3所述的方法,其中多云控制平面托管云链路适配器、网络链路适配器和适配器池,云链路适配器、网络链路适配器和适配器池中的每一个与由多云基础设施提供的一组一个或多个云服务中的特定服务对应。

5.如前述权利要求中的任一项所述的方法,还包括:

由多云控制平面将第一令牌转换成第二令牌,第二令牌与服务相关联并用于访问服务。

6.如前述权利要求中的任一项所述的方法,还包括:

由多云控制平面实例化第二云环境中的服务账户,所述服务账户与第一云环境的云服务提供商相关联;以及

由多云控制平面经由服务账户获得对第二云环境中的用户账户的访问。

7.如权利要求6所述的方法,其中基于服务账户与第二云环境中的用户账户之间配置的信任,用户的身份信息从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统。

8.如前述权利要求中的任一项所述的方法,还包括:

使用多云基础设施创建第二云环境中用户的账户与第一云环境中与用户相关联的租赁之间的映射/链路。

9.如前述权利要求中的任一项所述的方法,还包括:

在第一云环境和第二云环境之间建立网络链路,所述网络链路促进从第二云环境访问在第一云环境中与用户相关联的租赁中部署的资源。

10.存储计算机可执行指令的一个或多个计算机可读非暂态介质,所述计算机可执行指令在由一个或多个处理器执行时,使得:

由多云基础设施的多云控制台接收来自用户的对服务的请求,所述请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;

由平台基于第一令牌对用户进行授权,所述授权包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;以及

响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

11.如权利要求10所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,还包括:

在第一云环境的登录门户处接收用户的凭证,其中第一令牌由第一身份系统响应于成功认证凭证而生成,并且其中登录门户与多云基础设施的多云控制台不同。

12.如权利要求10或11所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,其中所述请求是在多云控制台的GUI处接收的,所述GUI列出了由多云基础设施供应的多个服务。

13.如权利要求10、11或12所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,其中多云控制平面托管云链路适配器、网络链路适配器和适配器池,云链路适配器、网络链路适配器和适配器池中的每一个与由多云基础设施提供的一组一个或多个云服务中的特定服务对应。

14.如权利要求10至13中的任一项所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,还包括:

由多云控制平面将第一令牌转换成第二令牌,第二令牌与服务相关联并用于访问服务。

15.如权利要求10至14中的任一项所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,还包括:

由多云控制平面实例化第二云环境中的服务账户,所述服务账户与第一云环境的云服务提供商相关联;以及

由多云控制平面经由服务账户获得对第二云环境中的用户账户的访问。

16.如权利要求15所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,其中基于服务账户与第二云环境中的用户账户之间配置的信任,用户的身份信息从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统。

17.如权利要求10至16中的任一项所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,还包括:

使用多云基础设施创建第二云环境中用户的账户与第一云环境中与用户相关联的租赁之间的映射/链路。

18.如权利要求10至17中的任一项所述的存储计算机可执行指令的一个或多个计算机可读非暂态介质,还包括:

在第一云环境和第二云环境之间建立网络链路,所述网络链路促进从第二云环境访问在第一云环境中与用户相关联的租赁中部署的资源。

19.一种计算设备,包括:

一个或多个处理器;以及

包括指令的存储器,所述指令在用所述一个或多个处理器执行时,使得所述计算设备至少:

由多云基础设施的多云控制台接收来自用户的对服务的请求,所述请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;

由平台基于第一令牌对用户进行授权,包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;

响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

20.如权利要求19所述的计算设备,其中所述请求是在多云控制台的GUI处接收的,所述GUI列出了由多云基础设施供应的多个服务。

多云基础设施中的身份管理

[0001] 相关申请的交叉引用

[0002] 本申请是以下每个临时申请的非临时申请并要求其权益。以下每个临时申请的全部内容都通过引用并入本文用于所有目的：

[0003] (1)于2022年10月14日提交的美国临时申请No.63/416,042；

[0004] (2)于2023年5月8日提交的美国临时申请No.63/464,903；

[0005] (3)于2023年5月17日提交的美国临时申请No.63/467,241；

[0006] (4)于2023年5月24日提交的美国临时申请No.63/468,739；

[0007] (5)于2023年5月30日提交的美国临时申请No.63/469,763；

[0008] (6)于2023年6月7日提交的美国临时申请No.63/471,573；

技术领域

[0009] 本公开涉及云体系架构,并且更特别地涉及用于链接由不同云服务提供商提供的两个云环境的技术。由一个服务提供商提供的一个云环境的用户可以使用和管理由另一个云服务提供商提供的另一个云环境所提供的服务。

背景技术

[0010] 过去几年,云服务的采用率急剧上升,并且这个趋势只会增加。各种不同的云环境由不同的云服务提供商(CSP)提供,每个云环境提供一组一个或多个云服务。由云环境供应的该组云服务可以包括一种或多种不同类型的服务,包括但不限于软件即服务(SaaS)服务、基础设施即服务(IaaS)服务、平台即服务(PaaS)服务等。

[0011] 虽然目前有各种不同的云环境可用,但每个云环境都为其订阅客户提供封闭的生态系统。因此,云环境的客户被限于使用由该云环境供应的服务。对于订阅由一个CSP提供的云环境的客户来说,没有容易的方式来经由该云环境使用由不同CSP提供的不同云环境中供应的服务。本文讨论的实施例解决了这些问题和其他问题。

发明内容

[0012] 本公开涉及云体系架构,并且更特别地涉及用于链接由不同云服务提供商提供的两个云环境的技术。由一个服务提供商提供的一个云环境的用户可以管理由另一个云服务提供商提供的另一个云环境所提供的服务。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、代码或指令的非暂态计算机可读存储介质等。一些实施例可以通过使用计算机程序产品来实现,该计算机程序产品包括计算机程序/指令,该计算机程序/指令在由处理器执行时使处理器执行本公开中描述的任何方法。

[0013] 本公开的实施例提供了一种多云控制平面(MCCP)框架,该框架供给将特定云网络(例如,Oracle云基础设施(OCI))的服务交付给其他云(例如,AWS)上的用户的能力。MCCP框架允许((一个或多个)其他云环境的)用户访问云环境的服务(例如,PaaS服务、数据库服务,诸如自主数据库服务等),同时提供尽可能接近用户的(一个或多个)原生云环境的用户

体验。MCCP的关键价值主张是客户将能够体验外部云中的服务的完整数据平面能力。

[0014] 本公开的一个实施例涉及一种方法,包括:由多云基础设施的多云控制台接收来自用户的对服务的请求,该请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;由平台基于第一令牌对用户进行授权,该授权包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;以及响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

[0015] 根据本公开的一个方面,提供了存储计算机可执行指令的一个或多个计算机可读非暂态介质,该计算机可执行指令在由一个或多个处理器执行时,使得:由多云基础设施的多云控制台接收来自用户的对服务的请求,该请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;由平台基于第一令牌对用户进行授权,该授权包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;以及响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

[0016] 根据本公开的一个方面,提供了一种计算设备,包括:一个或多个处理器;以及包括指令的存储器,该指令在用一个或多个处理器执行时,使得计算设备至少:由多云基础设施的多云控制台接收来自用户的对服务的请求,该请求包括由与第一云环境相关联的第一身份系统生成的第一令牌;由平台基于第一令牌对用户进行授权,包括核实与用户相关联的身份信息,其中身份信息先前从与第二云环境相关联的第二身份系统迁移到第一云环境的第一身份系统;以及响应于用户被成功核实,由多云基础设施的多云控制平面在第一云环境中与用户相关联的租赁中部署与服务相关联的资源。

[0017] 本公开的一个方面提供了一种计算设备,包括一个或多个数据处理器,以及包含指令的非暂态计算机可读存储介质,该指令在一个或多个数据处理器上执行时,使得计算设备执行本文公开的一种或多种方法的部分或全部。

[0018] 本公开的另一方面提供了一种有形地实施在非暂态机器可读存储介质中的计算机程序产品,包括被配置为使一个或多个数据处理器执行本文公开的一种或多种方法的部分或全部的指令。

[0019] 当参考以下说明书、权利要求书和附图时,前述以及其他特征和实施例将变得更加明显。

附图说明

[0020] 当参考附图阅读以下具体实施方式时,可以更好地理解本公开的特征、实施例和优点。

[0021] 图1是分布式环境的高级图,示出了根据某些实施例的由云服务提供商基础设施托管的虚拟或覆盖云网络。

[0022] 图2描绘了根据某些实施例的CSPI内的物理网络中的物理组件的简化体系架构图。

[0023] 图3示出了根据某些实施例的CSPI内的示例布置,其中主机机器连接到多个网络虚拟化设备(NVD)。

[0024] 图4描绘了根据某些实施例的主机机器和NVD之间的连接性,用于提供I/O虚拟化以支持多租赁(tenancy)。

[0025] 图5描绘了根据某些实施例的由CSPI提供的物理网络的简化框图。

[0026] 图6描绘了根据某些实施例的分布式环境的简化高级图,该分布式环境包括由不同云服务提供商(CSP)提供的多个云环境,其中云环境包括提供专门基础设施的特定云环境,该基础设施使得由该特定云环境提供的一个或多个云服务能够被其他云环境的客户使用。

[0027] 图7描绘了根据一些实施例的互连两个不同云环境的多云基础设施的示例性高级体系架构。

[0028] 图8描绘了图示根据一些实施例的身份框架的多云体系架构。

[0029] 图9描绘了图示根据一些实施例的与用户登记处理对应的步骤的示例性流程图。

[0030] 图10描绘了图示根据一些实施例的第一云环境的身份连接器框架的框图。

[0031] 图11描绘了图示根据一些实施例的与执行身份联合的处理对应的步骤的示例性游泳图。

[0032] 图12描绘了图示根据一些实施例的与先决条件资源验证处理对应的步骤的示例性游泳图。

[0033] 图13描绘了图示根据一些实施例的为解决混淆代理问题而执行的步骤的示例性游泳图。

[0034] 图14描绘了图示根据一些实施例的云链路资源对象的示意图。

[0035] 图15描绘了图示根据一些实施例的由多云基础设施部署资源的示意图。

[0036] 图16是图示根据至少一个实施例的用于实现云基础设施即服务系统的一种模式的框图。

[0037] 图17是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0038] 图18是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0039] 图19是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0040] 图20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

[0041] 在以下描述中,出于解释的目的,阐述了具体细节以便提供对某些实施例的透彻理解。但是,显然可以在没有这些具体细节的情况下实践各种实施例。附图和描述并非旨在限制。词语“示例性”在本文用于表示“用作示例、实例或图示”。本文描述为“示例性”的任何实施例或设计不一定被解释为优选或优于其他实施例或设计。

[0042] 本公开一般而言涉及改进的云体系架构,并且更特别地涉及用于链接两个云环境(每个云环境由不同的云服务提供商(CSP)提供),使得一个云环境的用户可以使用由另一个不同的云环境提供的服务的技术。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、代码或指令的非暂态计算机可读存储介质等。一些实施例可

以通过使用计算机程序产品来实现,该计算机程序产品包括计算机程序/指令,该计算机程序/指令在由处理器执行时使处理器执行本公开中描述的任何方法。

[0043] 本公开的实施例提供了一种多云控制平面(MCCP)框架,该框架供给将特定云网络(例如,Oracle云基础设施(OCI))的服务交付给(例如,Amazons AWS中的)其他云上的用户的能力。MCCP框架允许((一个或多个)其他云环境的)用户访问云环境的服务(例如,PaaS服务),同时提供尽可能接近用户的(一个或多个)原生云环境的用户体验。MCCP的关键价值主张是客户将能够体验外部云中的服务的完整数据平面能力。

[0044] MCCP使第二云基础设施的用户(例如,AWS用户)能够以对用户透明的方式利用由第一云基础设施(例如,OCI)提供的资源(例如,数据库资源)。具体而言,由第一云基础设施提供的服务在第二云基础设施中显示为“原生”服务。这允许第二云基础设施的客户原生访问由第一云基础设施提供的服务。如下面将参考图6-11描述的,MCCP是在第一云基础设施中执行的微服务的集合,其暴露第一云基础设施的资源以供外部云用户(例如,第二云基础设施的用户)使用。每个微服务都充当提供与由第一云基础设施提供的资源的通信的代理。

[0045] 云网络的示例

[0046] 术语云服务一般用于指由云服务提供商(CSP)使用由CSP提供的系统和基础设施(云基础设施)按需(例如,经由订阅模型)向用户或客户提供的服务。通常,构成CSP的基础设施的服务器和系统与客户自己的内部部署服务器和系统是分离的。因此,客户可以利用由CSP提供的云服务,而无需为服务购买单独的硬件和软件资源。云服务被设计为为订阅客户提供对应用和计算资源的简单、可扩展的访问,而无需客户投资购买用于提供服务的基础设施。

[0047] 有几个云服务提供商提供各种类型的云服务。有各种不同类型或模型的云服务,包括软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)等。

[0048] 客户可以订阅由CSP提供的一个或多个云服务。客户可以是任何实体,诸如个人、组织、企业等。当客户订阅或注册由CSP提供的服务时,将为该客户创建租赁或账户。然后,客户可以经由这个账户访问与该账户相关联的所订阅的一个或多个云资源。

[0049] 如上所述,基础设施即服务(IaaS)是一种特定类型的云计算服务。在IaaS模型中,CSP提供基础设施(称为云服务提供商基础设施或CSPI),这些基础设施可以被客户使用来构建其自己的可定制网络并部署客户资源。因此,客户的资源和网络由CSP提供的基础设施托管在分布式环境中。这与传统计算不同,在传统计算中,客户的资源和网络由客户提供的基础设施托管。

[0050] CSPI可以包括形成物理网络的互连的高性能计算资源,包括各种主机机器、存储器资源和网络资源,该物理网络也被称为基底网络或底层网络。CSPI中的资源可以散布在一个或多个数据中心上,这些数据中心可以在地理上散布在一个或多个地理区域上。虚拟化软件可以由这些物理资源执行以提供虚拟化的分布式环境。虚拟化在物理网络上创建覆盖网络(也称为基于软件的网络、软件定义的网络或虚拟网络)。CSPI物理网络为在物理网络之上创建一个或多个覆盖或虚拟网络提供了底层基础。物理网络(或基底网络或底层网络)包括物理网络设备,诸如物理交换机、路由器、计算机和主机机器等。覆盖网络是运行在物理基底网络之上的逻辑(或虚拟)网络。给定的物理网络可以支持一个或多个覆盖网络。覆盖网络通常使用封装技术来区分属于不同覆盖网络的流量。虚拟或覆盖网络也称为虚拟

云网络(VCN)。虚拟网络是使用软件虚拟化技术实现的(例如,管理程序、由网络虚拟化设备(NVD)(例如,smartNIC)实现的虚拟化功能、架顶式(TOR)交换机、实现由NVD执行的一个或多个功能的智能TOR,以及其他机制)以创建可以在物理网络之上运行的网络抽象的层。虚拟网络可以采用多种形式,包括对等网络、IP网络等。虚拟网络通常是或者层3IP网络或者层2VLAN。这种虚拟或覆盖联网的方法常常被称为虚拟或覆盖层3联网。为虚拟网络开发的协议的示例包括IP-in-IP(或通用路由封装(GRE))虚拟可扩展LAN(VXLAN—IETF RFC 7348)、虚拟专用网络(VPN)(例如,MPLS层3虚拟专用网络(RFC 4364))、VMware的NSX、GENEVE(通用网络虚拟化封装)等。

[0051] 对于IaaS,由CSP提供的基础设施(CSPI)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,云计算服务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提供商还可以供应各种服务来伴随那些基础设施组件(例如,计费、监视、日志记录、安全性、负载平衡和聚类等)。因此,由于这些服务可以是策略驱动的,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可用性和性能。CSPI提供基础设施和一组互补的云服务,这些使客户能够在高度可用的被托管的分布式环境中构建和运行广泛的应用和服务。CSPI在可从各种联网位置(诸如从客户的内部部署网络)安全访问的灵活的虚拟网络中提供高性能计算资源和能力以及存储容量。当客户订阅或注册由CSP提供的IaaS服务时,为该客户创建的租赁是CSPI内的安全且隔离的分区,客户可以在其中创建、组织和管理他们的云资源。

[0052] 客户可以使用由CSPI提供的计算、存储器和联网资源构建他们自己的虚拟网络。可以在这些虚拟网络上部署一个或多个客户资源或工作负载,诸如计算实例。例如,客户可以使用由CSPI提供的资源来构建一个或多个可定制且私有的虚拟网络,称为虚拟云网络(VCN)。客户可以在客户VCN上部署一个或多个客户资源,诸如计算实例。计算实例可以采用虚拟机、裸机实例等形式。因此,CSPI提供基础设施和一组互补的云服务,这些使客户能够在高度可用的虚拟被托管环境中构建和运行广泛的应用和服务。客户不管理或控制由CSPI提供的底层物理资源,但可以控制操作系统、存储装置和已部署的应用;并且可能对所选择的联网组件(例如,防火墙)进行有限的控制。

[0053] CSP可以提供控制台,其使客户和网络管理员能够使用CSPI资源来配置、访问和管理部署在云中的资源。在某些实施例中,控制台提供可以用于访问和管理CSPI的基于web的用户界面。在某些实施方式中,控制台是由CSP提供的基于web的应用。

[0054] CSPI可以支持单租赁或多租赁体系架构。在单租赁体系架构中,软件(例如,应用、数据库)或硬件组件(例如,主机机器或服务器)服务于单个客户或租户。在多租赁体系架构中,软件或硬件组件服务于多个客户或租户。因此,在多租赁体系架构中,CSPI资源在多个客户或租户之间共享。在多租赁情况下,在CSPI中采取预防措施并实施保护措施,以确保每个租户的数据都是隔离的并且对其他租户保持不可见。

[0055] 在物理网络中,网络端点(“端点”)是指连接到物理网络并与其所连接的网络来回通信的计算设备或系统。物理网络中的网络端点可以连接到局域网(LAN)、广域网(WAN)或其他类型的物理网络。物理网络中传统端点的示例包括调制解调器、集线器、桥接器、交换机、路由器和其他联网设备、物理计算机(或主机机器)等。物理网络中的每个物理设备都有

可以用于与设备通信的固定网络地址。这个固定网络地址可以是层2地址(例如,MAC地址)、固定的层3地址(例如,IP地址)等。在虚拟化的环境或虚拟网络中,端点可以包括各种虚拟端点,诸如由物理网络的组件托管(例如,由物理主机机器托管)的虚拟机。虚拟网络中的这些端点由覆盖地址寻址,诸如覆盖层2地址(例如,覆盖MAC地址)和覆盖层3地址(例如,覆盖IP地址)。网络覆盖通过允许网络管理者使用软件管理(例如,经由实现用于虚拟网络的控制平面的软件)在与网络端点相关联的覆盖地址周围移动来实现灵活性。相应地,与物理网络不同,在虚拟网络中,可以使用网络管理软件将覆盖地址(例如,覆盖IP地址)从一个端点移动到另一个端点。由于虚拟网络建立在物理网络之上,因此虚拟网络中组件之间的通信涉及虚拟网络和底层物理网络二者。为了促进此类通信,CSPI的组件被配置为学习和存储将虚拟网络中的覆盖地址映射到基底网络中的实际物理地址的映射,反之亦然。然后使用这些映射来促进通信。客户流量被封装以促进在虚拟网络中的路由。

[0056] 相应地,物理地址(例如,物理IP地址)与物理网络中的组件相关联,并且覆盖地址(例如,覆盖IP地址)与虚拟或覆盖网络中的实体相关联。物理IP地址是与基底或物理网络中的物理设备(例如,网络设备)相关联的IP地址。例如,每个NVD都有相关联的物理IP地址。覆盖IP地址是与覆盖网络中的实体相关联的覆盖地址,诸如与客户的虚拟云网络(VCN)中的计算实例相关联的覆盖地址。两个不同的客户或租户(每个客户或租户都有其自己的私有VCN)可以潜在地在其VCN中使用相同的覆盖IP地址,而无需彼此了解。物理IP地址和覆盖IP地址都是真实IP地址的类型。这些地址与虚拟IP地址是分开的。虚拟IP地址通常是表示或映射到多个真实IP地址的单个IP地址。虚拟IP地址提供虚拟IP地址与多个真实IP地址之间的一对多映射。例如,负载平衡器可以使用VIP来映射或表示多个服务器,每个服务器都有其自己的真实IP地址。

[0057] 云基础设施或CSPI在物理上托管在世界上一个或多个区域的一个或多个数据中心中。CSPI可以包括物理或基底网络中的组件和位于建立在物理网络组件之上的虚拟网络中的虚拟化的组件(例如,虚拟网络、计算实例、虚拟机等)。在某些实施例中,CSPI在领域、区域和可用性域中被组织和托管。区域通常是包含一个或多个数据中心的局部地理地区。区域一般彼此独立并且可以相隔很远,例如,跨越国家甚至大陆。例如,第一个区域可以在澳大利亚,另一个在日本,另一个在印度,等等。CSPI资源在区域之间划分,使得每个区域都有自己独立的CSPI资源子集。每个区域可以提供一组核心基础设施服务和资源,诸如计算资源(例如,裸机服务器、虚拟机、容器和相关基础设施等);存储资源(例如,块卷存储装置、文件存储装置、对象存储装置、归档存储装置);联网资源(例如,虚拟云网络(VCN)、负载平衡资源、与内部部署网络的连接)、数据库资源;边缘联网资源(例如,DNS);以及访问管理和监视资源等。每个区域一般都有多条路径将其连接到领域中的其他区域。

[0058] 一般而言,应用被部署在它被最频繁使用的区域中(即,部署在与该区域相关联的基础设施上),因为使用附近的资源比使用远处的资源更快。应用也可以出于各种原因而部署在不同的区域,诸如冗余以减轻区域范围内事件(诸如大型天气系统或地震)的风险,以满足法律管辖区、税域和其他商业或社会标准等的不同要求。

[0059] 区域内的数据中心可以被进一步组织和细分为可用性域(AD)。可用性域可以与位于区域内的一个或多个数据中心对应。区域可以由一个或多个可用性域组成。在这种分布式环境中,CSPI资源或者是特定于区域的,诸如虚拟云网络(VCN),或者是特定于可用性域

的,诸如计算实例。

[0060] 区域内的AD彼此隔离,具有容错能力,并且被配置为使得它们极不可能同时发生故障。这是通过AD不共享关键基础设施资源(诸如联网、物理电缆、电缆路径、电缆入口点等)来实现的,使得区域内的一个AD处的故障不太可能影响同一区域内其他AD的可用性。同一区域内的AD可以通过低时延、高带宽网络彼此连接,这使得为其他网络(例如,互联网、客户的内部部署网络等)提供高可用性连接并且在多个AD中构建复制系统以实现高可用性和灾难恢复成为可能。云服务使用多个AD来确保高可用性并防止资源故障。随着由IaaS提供商提供的基础设施的增长,可以添加更多区域和AD以及附加的容量。可用性域之间的流量通常是加密的。

[0061] 在某些实施例中,区域被分组为领域。领域是区域的逻辑集合。领域彼此隔离并且不共享任何数据。同一领域中的区域可以彼此通信,但不同领域中的区域不能。客户与CSP的租赁或账户存在于单个领域中,并且可以散布在属于该领域的一个或多个区域中。通常,当客户订阅IaaS服务时,会在领域内客户指定的区域(称为“主”区域)中为该客户创建租赁或账户。客户可以将客户的租赁扩展到领域内的一个或多个其他区域。客户无法访问不在客户的租赁所在领域中的区域。

[0062] IaaS提供商可以提供多个领域,每个领域迎合特定的一组客户或用户。例如,可以为商业客户提供商业领域。作为另一个示例,可以为特定国家为那个国家内的客户提供领域。作为又一个示例,可以为政府等提供政府领域。例如,政府领域可以迎合特定政府并且可以具有比商业领域更高的安全性级别。例如,Oracle云基础设施(Oracle Cloud Infrastructure,OCI)目前为商业区域提供领域,并且为政府云区域提供两个领域(例如,FedRAMP授权的和IL5授权的)。

[0063] 在某些实施例中,AD可以被细分成一个或多个故障域。故障域是AD内的基础设施资源的分组,以提供反亲和性。故障域允许计算实例的分布,使得这些实例不位于单个AD内的相同物理硬件上。这被称为反亲和性。故障域是指共享单点故障的一组硬件组件(计算机、交换机等)。计算池在逻辑上被划分为故障域。因此,影响一个故障域的硬件故障或计算硬件维护事件不影响其他故障域中的实例。取决于实施例,用于每个AD的故障域的数量可以有所不同。例如,在某些实施例中,每个AD包含三个故障域。故障域充当AD内的逻辑数据中心。

[0064] 当客户订阅IaaS服务时,来自CSPI的资源被供应给客户并与客户的租赁相关联。客户可以使用这些供应的资源来构建私有网络并在这些网络上部署资源。由CSPI在云中托管的客户网络被称为虚拟云网络(VCN)。客户可以使用为客户分配的CSPI资源来设置一个或多个虚拟云网络(VCN)。VCN是虚拟或软件定义的私有网络。部署在客户的VCN中的客户资源可以包括计算实例(例如,虚拟机、裸机实例)和其他资源。这些计算实例可以表示各种客户工作负载,诸如应用、负载平衡器、数据库等。部署在VCN上的计算实例可以通过公共网络(诸如互联网)与公共可访问端点(“公共端点”)、与同一VCN或其他VCN(例如,客户的其他VCN或不属于该客户的VCN)中的其他实例、与客户的内部部署数据中心或网络以及与服务端点和其他类型的端点通信。

[0065] CSP可以使用CSPI来提供各种服务。在一些情况下,CSPI的客户本身可以像服务提供商一样起作用并使用CSPI资源提供服务。服务提供商可以暴露服务端点,该服务端点以

标识信息(例如,IP地址、DNS名称和端口)为特征。客户的资源(例如,计算实例)可以通过访问由服务为特定服务暴露的服务端点来使用该特定服务。这些服务端点一般是用户可经由公共通信网络(诸如互联网)使用与端点相关联的公共IP地址公开访问的端点。可公开访问的网络端点有时也称为公共端点。

[0066] 在某些实施例中,服务提供商可以经由用于服务的端点(有时称为服务端点)来暴露服务。服务的客户然后可以使用这个服务端点来访问服务。在某些实施方式中,为服务提供的服务端点可以由打算消费该服务的多个客户访问。在其他实施方式中,可以为客户提供专用服务端点,使得只有该客户可以使用该专用服务端点来访问服务。

[0067] 在某些实施例中,当创建VCN时,它与私有覆盖无类域间路由(CIDR)地址空间相关联,该地址空间是指派给VCN的一系列私有覆盖IP地址(例如,10.0/16)。VCN包括相关联的子网、路由表和网关。VCN驻留在单个区域内,但可以跨越该区域的可用性域中的一个或多个或所有。网关是为VCN配置的虚拟接口并且启用VCN与VCN外部的一个或多个端点之间的流量的通信。可以为VCN配置一种或多种不同类型的网关,以启用去往和来自不同类型端点的通信。

[0068] VCN可以被细分为一个或多个子网络,诸如一个或多个子网。因此,子网是可以在VCN内创建的配置的单元或细分。VCN可以有一个或多个子网。VCN内的每个子网都与连续范围的覆盖IP地址(例如,10.0.0.0/24和10.0.1.0/24)相关联,这些IP地址不与该VCN中的其他子网重叠并且表示VCN的地址空间内的地址空间子集。

[0069] 每个计算实例都与虚拟网络接口卡(VNIC)相关联,这使得计算实例能够参与VCN的子网。VNIC是物理网络接口卡(NIC)的逻辑表示。一般而言,VNIC是实体(例如,计算实例、服务)与虚拟网络之间的接口。VNIC存在于子网中,具有一个或多个相关联的IP地址,以及相关联的安全性规则或策略。VNIC相当于交换机上的层2端口。VNIC附接到计算实例和VCN内的子网。与计算实例相关联的VNIC使计算实例成为VCN的子网的一部分,并且使计算实例能够与和计算实例位于同一子网上的端点、与VCN中的不同子网中的端点或与VCN外部的端点通信(例如,发送和接收数据包)。因此,与计算实例相关联的VNIC确定计算实例如何与VCN内部和外部的端点连接。当创建计算实例并将其添加到VCN内的子网时,创建用于计算实例的VNIC并将其与该计算实例相关联。对于包括一组计算实例的子网,该子网包含与该组计算实例对应的VNIC,每个VNIC附接到该组计算机实例内的计算实例。

[0070] 经由与计算实例相关联的VNIC为每个计算实例指派私有覆盖IP地址。这个私有覆盖网络IP地址在创建计算实例时指派给与计算实例相关联的VNIC并用于路由去往和来自计算实例的流量。给定子网中的所有VNIC都使用相同的路由表、安全性列表和DHCP选项。如上所述,VCN内的每个子网都与连续范围的覆盖IP地址(例如,10.0.0.0/24和10.0.1.0/24)相关联,这些IP地址不与该VCN中的其他子网重叠并且表示VCN的地址空间内的地址空间子集。对于VCN的特定子网上的VNIC,指派给该VNIC的私有覆盖IP地址是来自为子网分配的连续范围的覆盖IP地址的地址。

[0071] 在某些实施例中,除了私有覆盖IP地址之外,计算实例还可以可选地被指派附加的覆盖IP地址,诸如例如如果在公共子网中,那么是一个或多个公共IP地址。这多个地址或者在同一个VNIC上或者在与计算实例相关联的多个VNIC上指派。但是,每个实例具有主VNIC,它是在实例启动期间创建的并且与指派给该实例的覆盖私有IP地址相关联—这个主

VNIC无法被删除。称为辅助VNIC的附加VNIC可以添加到与主VNIC相同的可用性域中的现有实例。所有VNIC都在与该实例相同的可用性域中。辅助VNIC可以位于与主VNIC相同的VCN中的子网中,或者位于同一VCN或不同VCN中的不同子网中。

[0072] 如果计算实例在公共子网中,那么可以可选地为其指派公共IP地址。在创建子网时,可以将子网指定为或者公共子网或者私有子网。私有子网意味着子网中的资源(例如,计算实例)和相关联的VNIC不能具有公共覆盖IP地址。公共子网意味着子网中的资源和相关联的VNIC可以具有公共IP地址。客户可以指定子网存在于单个可用性域中或跨区域或领域中的多个可用性域。

[0073] 如上所述,VCN可以被细分成一个或多个子网。在某些实施例中,为VCN配置的虚拟路由器(VR)(称为VCN VR或简称为VR)使得VCN的子网之间能够通信。对于VCN内的子网,VR表示用于该子网的逻辑网关,它使该子网(即,该子网上的计算实例)能够与VCN内其他子网上的端点以及VCN外的其他端点通信。VCN VR是逻辑实体,其被配置为在VCN中的VNIC和与VCN相关联的虚拟网关(“网关”)之间路由流量。下文关于图1进一步描述网关。VCN VR是层3/IP层概念。在一个实施例中,对于VCN存在一个VCN VR,其中VCN VR具有潜在不受限制数量的由IP地址寻址的端口,VCN的每个子网有一个端口。以这种方式,VCN VR对于VCN VR所附接到的VCN中的每个子网具有不同的IP地址。VR还连接到为VCN配置的各种网关。在某些实施例中,用于子网的覆盖IP地址范围中的特定覆盖IP地址被保留用于该子网的VCN VR的端口。例如,考虑VCN有两个子网,相关联的地址范围分别是10.0/16和10.1/16。对于地址范围为10.0/16的VCN中的第一个子网,这个范围内的地址被保留用于该子网的VCN VR的端口。在一些情况下,范围内的第一个IP地址可以被保留用于VCN VR。例如,对于覆盖IP地址范围为10.0/16的子网,可以为该子网的VCN VR的端口保留IP地址10.0.0.1。对于地址范围为10.1/16的同一VCN中的第二个子网,VCN VR可以具有用于IP地址为10.1.0.1的第二个子网的端口。VCN VR对于VCN中的每个子网具有不同的IP地址。

[0074] 在一些其他实施例中,VCN内的每个子网可以具有其自己的相关联的VR,该VR可由子网使用与VR相关联的保留或默认IP地址寻址。例如,保留或默认IP地址可以是与该子网相关联的IP地址范围中的第一个IP地址。子网中的VNIC可以使用这个默认或保留IP地址与与子网相关联的VR通信(例如,发送和接收数据包)。在这种实施例中,VR是该子网的入口/出口点。与VCN内的子网相关联的VR可以与和VCN内的其他子网相关联的其他VR通信。VR还可以与和VCN相关联的网关通信。子网的VR功能在为子网中的VNIC执行VNIC功能的一个或多个NVD上运行或由其执行。

[0075] 可以为VCN配置路由表、安全性规则和DHCP选项。路由表是用于VCN的虚拟路由表并且包括通过网关或特殊配置的实例将流量从VCN内的子网路由到VCN外的目的地的规则。可以定制VCN的路由表以控制数据包如何转发/路由到VCN和从VCN路由。DHCP选项是指在实例启动时自动提供给实例的配置信息。

[0076] 为VCN配置的安全性规则表示用于VCN的覆盖防火墙规则。安全性规则可以包括入口和出口规则,并指定允许进出VCN实例的流量的类型(例如,基于协议和端口)。客户可以选择给定规则是有状态的还是无状态的。例如,客户可以通过用源CIDR 0.0.0.0/0和目的地TCP端口22设置有状态入口规则来允许来自任何地方的传入SSH流量到一组实例。安全性规则可以使用网络安全性组或安全性列表来实现。网络安全性组由仅适用于该组中的资源

的一组安全性规则组成。另一方面,安全性列表包括适用于使用该安全性列表的任何子网中的所有资源的规则。可以为VCN提供带有默认安全性规则的默认安全性列表。为VCN配置的DHCP选项提供在实例启动时自动提供给VCN中的实例的配置信息。

[0077] 在某些实施例中,用于VCN的配置信息由VCN控制平面确定和存储。例如,用于VCN的配置信息可以包括关于以下的信息:与VCN相关联的地址范围、VCN内的子网和相关联的信息、与VCN相关联的一个或多个VR、VCN中的计算实例和相关联的VNIC、执行与VCN相关联的各种虚拟化网络功能的NVD(例如,VNIC、VR、网关)、用于VCN的状态信息以及其他VCN相关信息。在某些实施例中,VCN分发服务向NVD发布由VCN控制平面或其部分存储的配置信息。分发的信息可以用于更新由NVD存储和使用的信息(例如,转发表、路由表等),以将数据包转发到VCN中的计算实例或从计算实例转发数据包。

[0078] 在某些实施例中,VCN和子网的创建由VCN控制平面(CP)处置并且计算实例的启动由计算控制平面处置。计算控制平面负责为计算实例分配物理资源,然后调用VCN控制平面来创建VNIC并将其附接到计算实例。VCN CP还将VCN数据映射发送到被配置为执行数据包转发和路由功能的VCN数据平面。在某些实施例中,VCN CP提供负责向VCN数据平面提供更新的分发服务。VCN控制平面的示例也在图12、图13、图14和图15中描绘(参见参考标号1216、1316、1416和1516)并在下面进行描述。

[0079] 客户可以使用由CSPI托管的资源创建一个或多个VCN。部署在客户VCN上的计算实例可以与不同的端点通信。这些端点可以包括由CSPI托管的端点和CSPI外部的端点。

[0080] 图1、图2、图3、图4、图5和图12-16中描绘了用于使用CSPI实现基于云的服务的各种不同体系架构,并且在下文中进行描述。图1是分布式环境100的高级图,示出了根据某些实施例的由CSPI托管的覆盖或客户VCN。图1中描绘的分布式环境包括覆盖网络中的多个组件。图1中描绘的分布式环境100仅仅是个示例,并非旨在过度限制所要求保护的实施例的范围。许多变化、替代和修改是可能的。例如,在一些实施方式中,图1中描绘的分布式环境可以具有比图1中所示的更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。

[0081] 如图1中描绘的示例中所示,分布式环境100包括提供服务和资源的CSPI 101,客户可以订阅并使用这些服务和资源来构建他们的虚拟云网络(VCN)。在某些实施例中,CSPI 101向订阅客户提供IaaS服务。CSPI 101内的数据中心可以被组织到一个或多个区域。图1中示出了一个示例区域“区域US”102。客户已经为区域102配置了客户VCN c/o Oracle国际公司。客户可以在VCN 104上部署各种计算实例,其中计算实例可以包括虚拟机或裸机实例。实例的示例包括应用、数据库、负载平衡器等。

[0082] 在图1中描绘的实施例中,客户VCN 104包括两个子网,即,“子网-1”和“子网-2”,每个子网具有其自己的CIDR IP地址范围。在图1中,子网-1的覆盖IP地址范围是10.0/16,并且子网-2的地址范围是10.1/16。VCN虚拟路由器105表示用于VCN的逻辑网关,它启用VCN 104的子网之间以及与VCN外部的其他端点的通信。VCN VR 105被配置为在VCN 104中的VNIC和与VCN 104相关联的网关之间路由流量。VCN VR 105为VCN 104的每个子网提供端口。例如,VR 105可以为子网-1提供具有IP地址10.0.0.1的端口并为子网-2提供具有IP地址10.1.0.1的端口。

[0083] 可以在每个子网上部署多个计算实例,其中计算实例可以是虚拟机实例和/或裸

机实例。子网中的计算实例可以由CSPI 101内的一个或多个主机机器托管。计算实例经由与计算实例相关联的VNIC参与子网。例如,如图1中所示,计算实例C1经由与计算实例相关联的VNIC成为子网-1的一部分。同样,计算实例C2经由与C2相关联的VNIC成为子网-1的一部分。以类似的方式,多个计算实例(可以是虚拟机实例或裸机实例)可以是子网-1的一部分。经由其相关联的VNIC,每个计算实例都被指派私有覆盖IP地址和MAC地址。例如,在图1中,计算实例C1的覆盖IP地址为10.0.0.2,MAC地址为M1,而计算实例C2的私有覆盖IP地址为10.0.0.3,MAC地址为M2。子网-1中的每个计算实例(包括计算实例C1和C2)都有到使用IP地址10.0.0.1的VCN VR 105的默认路由,该地址是用于子网-1的VCN VR 105的端口的IP地址。

[0084] 子网-2上可以部署多个计算实例,包括虚拟机实例和/或裸机实例。例如,如图1中所示,计算实例D1和D2经由与相应计算实例相关联的VNIC成为子网-2的一部分。在图1中所示的实施例中,计算实例D1的覆盖IP地址为10.1.0.2,MAC地址为MM1,而计算实例D2的私有覆盖IP地址为10.1.0.3,MAC地址为MM2。子网-2中的每个计算实例(包括计算实例D1和D2)都有到使用IP地址10.1.0.1的VCN VR 105的默认路由,该地址是用于子网-2的VCN VR 105的端口的IP地址。

[0085] VCN A 104还可以包括一个或多个负载平衡器。例如,可以为子网提供负载平衡器,并且可以将负载平衡器配置为跨子网上的多个计算实例负载平衡流量。还可以提供负载平衡器以在VCN中跨子网负载平衡流量。

[0086] 部署在VCN 104上的特定计算实例可以与各种不同的端点通信。这些端点可以包括由CSPI 200托管的端点和CSPI 200外部的端点。由CSPI 101托管的端点可以包括:与特定计算实例位于同一子网上的端点(例如,子网-1中两个计算实例之间的通信);位于不同子网上但位于同一VCN内的端点(例如,子网-1中的计算实例与子网-2中的计算实例之间的通信);同一区域中不同VCN中的端点(例如,子网-1中的计算实例与同一区域106或110中的VCN中的端点之间的通信,子网-1中的计算实例与同一区域中服务网点110中的端点之间的通信);或不同区域中的VCN中的端点(例如,子网-1中的计算实例与不同区域108中的VCN中的端点之间的通信)。由CSPI 101托管的子网中的计算实例也可以与不由CSPI 101托管(即,在CSPI 101外部)的端点通信。这些外部端点包括客户的内部部署网络116中的端点、其他远程云托管网络118中的端点、可经由公共网络(诸如互联网)访问的公共端点114及其他端点。

[0087] 使用与源计算实例和目的地计算实例相关联的VNIC促进同一子网上的计算实例之间的通信。例如,子网-1中的计算实例C1可能想要将数据包发送到子网-1中的计算实例C2。对于源自源计算实例且其目的地是同一子网中的另一个计算实例的数据包,该数据包首先由与源计算实例相关联的VNIC处理。由与源计算实例相关联的VNIC执行的处理可以包括从数据包报头确定数据包的目的地信息、识别为与源计算实例相关联的VNIC配置的任何策略(例如,安全性列表)、确定用于数据包的下一跳、根据需要执行任何数据包封装/解封装功能,然后将数据包转发/路由到下一跳,目的是促进数据包到其预期目的地的通信。当目的地计算实例与源计算实例位于同一子网中时,与源计算实例相关联的VNIC被配置为识别与目的地计算实例相关联的VNIC并将数据包转发到该VNIC进行处理。然后执行与目的地计算实例相关联的VNIC并将数据包转发到目的地计算实例。

[0088] 对于要从子网中的计算实例传送到同一VCN中不同子网中的端点的数据包,通过与源和目的地计算实例相关联的VNIC以及VCN VR来促进通信。例如,如果图1中子网-1中的计算实例C1想要将数据包发送到子网-2中的计算实例D1,那么该数据包首先由与计算实例C1相关联的VNIC处理。与计算实例C1相关联的VNIC被配置为使用默认路由或VCN VR的端口10.0.0.1将数据包路由到VCN VR105。VCN VR 105被配置为使用端口10.1.0.1将数据包路由到子网-2。然后,与D1相关联的VNIC接收并处理数据包并且VNIC将数据包转发到计算实例D1。

[0089] 对于要从VCN 104中的计算实例传送到VCN 104外部的端点的数据包,通信由与源计算实例相关联的VNIC、VCN VR 105和与VCN 104相关联的网关促进。一种或多种类型的网关可以与VCN 104相关联。网关是VCN和另一个端点之间的接口,其中该另一个端点在VCN外部。网关是层3/IP层概念并且使VCN能够与VCN外部的端点通信。因此,网关促进VCN与其他VCN或网络之间的流量流动。可以为VCN配置各种不同类型的网关以促进与不同类型的端点的不同类型的通信。取决于网关,通信可以通过公共网络(例如,互联网)或通过私有网络进行。各种通信协议可以用于这些通信。

[0090] 例如,计算实例C1可能想要与VCN 104外部的端点通信。数据包可以首先由与源计算实例C1相关联的VNIC处理。VNIC处理确定数据包的目的地在C1的子网-1外部。与C1相关联的VNIC可以将数据包转发到用于VCN 104的VCN VR 105。VCN VR 105然后处理数据包,并且作为处理的一部分,基于数据包的目的地,确定与VCN 104相关联的特定网关作为用于数据包的下一跳。然后,VCN VR 105可以将数据包转发到特定的识别出的网关。例如,如果目的地是客户的内部部署网络内的端点,那么数据包可以由VCN VR 105转发到为VCN 104配置的动态路由网关(DRG)网关122。数据包然后可以从网关转发到下一跳,以促进数据包到其最终预期目的地的传送。

[0091] 可以为VCN配置各种不同类型的网关。可以为VCN配置的网关的示例在图1中描绘并且在下文进行描述。与VCN相关联的网关的示例也在图12、图13、图14和图15中描绘(例如,通过参考标号1234、1236、1238、1334、1336、1338、1434、1436、1438、1534、1536和1538引用的网关)并且如下所述。如图1中描绘的实施例中所示,动态路由网关(DRG)122可以添加到客户VCN 104或与客户VCN 104相关联,并为客户VCN 104与另一个端点之间的私有网络流量通信提供路径,其中该另一个端点可以是客户的内部部署网络116、CSPI 101的不同区域中的VCN 108,或者不是由CSPI 101托管的其他远程云网络118。客户内部部署网络116可以是使用客户的资源构建的客户网络或客户数据中心。对客户内部部署网络116的访问一般是非常受限的。对于同时具有客户内部部署网络116和由CSPI 101在云中部署或托管的一个或多个VCN 104的客户,客户可能想要他们的内部部署网络116和他们的基于云的VCN 104能够彼此沟通。这使客户能够构建扩展的混合环境,包括由CSPI 101托管的客户的VCN 104和他们的内部部署网络116。DRG 122启用这种此通信。为了启用此类通信,设置通信通道124,其中通道的一个端点位于客户内部部署网络116中,而另一个端点位于CSPI 101中并连接到客户VCN 104。通信通道124可以通过公共通信网络(诸如互联网)或私有通信网络。可以使用各种不同的通信协议,诸如公共通信网络(诸如互联网)上的IPsec VPN技术、使用私有网络而不是公共网络的Oracle的FastConnect技术等。客户内部部署网络116中形成通信通道124的一个端点的设备或装备被称为客户现场装备(CPE),诸如图1中描绘的CPE

126。在CSPI 101侧,端点可以是执行DRG 122的主机机器。

[0092] 在某些实施例中,可以将远程对等连接(RPC)添加到DRG,这允许客户将一个VCN与不同区域中的另一个VCN对等。使用这种RPC,客户VCN 104可以使用DRG 122与另一个区域中的VCN 108连接。DRG 122还可以用于与不由CSPI 101托管的其他远程云网络118(诸如Microsoft Azure云、亚马逊AWS云等)通信。

[0093] 如图1中所示,可以为客户VCN 104配置互联网网关(IGW)120,其使VCN 104上的计算实例能够与可通过公共网络(诸如互联网)访问的公共端点114通信。IGW 120是将VCN连接到诸如互联网之类的公共网络的网关。IGW 120使VCN(诸如VCN 104)内的公共子网(其中公共子网中的资源具有公共覆盖IP地址)能够直接访问公共网络114(诸如互联网)上的公共端点112。使用IGW 120,可以从VCN 104内的子网或从互联网发起连接。

[0094] 可以为客户的VCN 104配置网络地址转换(NAT)网关128,并使客户的VCN中没有专用公共覆盖IP地址的云资源能够访问互联网,并且在不暴露那些资源的情况下这样做以指引传入的互联网连接(例如,L4-L7连接)。这使VCN内的私有子网(诸如VCN 104中的私有子网-1)能够私有访问互联网上的公共端点。在NAT网关中,只能从私有子网发起到公共互联网的连接,而不能从互联网发起到私有子网的连接。

[0095] 在某些实施例中,可以为客户VCN 104配置服务网关(SGW)126,并为VCN 104和服务网络110中支持的服务端点之间的私有网络流量提供路径。在某些实施例中,服务网络110可以由CSP提供并且可以提供各种服务。这种服务网络的示例是Oracle的服务网络,它提供可供客户使用的各种服务。例如,客户VCN 104的私有子网中的计算实例(例如,数据库系统)可以将数据备份到服务端点(例如,对象存储装置,Object Storage),而无需公共IP地址或访问互联网。在某些实施例中,VCN可以只有一个SGW,并且连接只能从VCN内的子网发起,而不能从服务网络110发起。如果VCN与另一个对等,那么另一个VCN中的资源通常不能访问SGW。用FastConnect或VPN Connect连接到VCN的内部部署网络中的资源也可以使用为该VCN配置的服务网关。

[0096] 在某些实施方式中,SGW 126使用服务无类域间路由(CIDR)标签的概念,该标签是表示用于感兴趣的服务或服务组的所有区域性公共IP地址范围的字符串。客户在他们配置SGW和相关路由规则以控制到服务的流量时使用服务CIDR标签。如果服务的公共IP地址在未来发生改变,那么客户可以在配置安全性规则时可选地使用它,而无需调整它们。

[0097] 本地对等网关(LPG)132是可以添加到客户VCN 104并使VCN 104能够与同一区域中的另一个VCN对等的网关。对等是指VCN使用私有IP地址进行通信,流量无需穿过公共网络(诸如互联网)或无需通过客户的内部部署网络116路由流量。在优选实施例中,VCN对于它建立的每个对等体具有单独LPG。本地对等或VCN对等是用于在不同应用或基础设施管理功能之间建立网络连接性的常见做法。

[0098] 服务提供商(诸如服务网络110中的服务的提供商)可以使用不同的访问模型提供对服务的访问。根据公共访问模型,服务可以作为可由客户VCN中的计算实例经由公共网络(诸如互联网)公开访问的公共端点暴露,和/或可以经由SGW 126私有访问。根据特定的私有访问模型,服务可作为客户的VCN中的私有子网中的私有IP端点进行访问。这被称为私有端点(PE)访问并且使服务提供商能够将其服务作为客户的私有网络中的实例暴露。私有端点资源表示客户的VCN内的服务。每个PE在客户的VCN中由客户选择的子网中表现为VNIC

(称为PE-VNIC,具有一个或多个私有IP)。因此,PE提供了使用VNIC在私有客户VCN子网中呈现服务的方式。由于端点作为VNIC暴露,因此与VNIC相关联的所有特征(诸如路由规则、安全性列表等)现在都可以用于PE VNIC。

[0099] 服务提供商可以注册他们的服务以启用通过PE的访问。提供商可以将策略与服务相关联,这限制了服务对客户租赁的可见性。提供商可以在单个虚拟IP地址(VIP)下注册多个服务,尤其是对于多租户服务。可以有表示相同服务的多个这样的私有端点(在多个VCN中)。

[0100] 私有子网中的计算实例然后可以使用PE VNIC的私有IP地址或服务DNS名称来访问服务。客户VCN中的计算实例可以通过将流量发送到客户VCN中的PE的私有IP地址来访问该服务。私有访问网关(PAGW)130是可以附接到服务提供商VCN(例如,服务网络110中的VCN)的网关资源,该服务提供商VCN充当来自/去往客户子网私有端点的所有流量的入口/出口点。PAGW 130使提供商能够在不利用其内部IP地址资源的情况下扩展PE连接的数量。提供商只需要为在单个VCN中注册的任何数量的服务配置一个PAGW。提供商可以将服务表示为一个或多个客户的多个VCN中的私有端点。从客户的角度来看,PE VNIC不是附接到客户的实例,而是看起来附接到客户希望与之交互的服务。去往私有端点的流量经由PAGW 130路由到服务。这些被称为客户到服务私有连接(C2S连接)。

[0101] 通过允许流量流经FastConnect/IPsec链路和客户VCN中的私有端点,PE概念还可以用于将用于服务的私有访问扩展到客户的内部署网络和数据中心。通过允许流量在LPG 132和客户的VCN中的PE之间流动,还可以将服务的私有访问扩展到客户的对等VCN。

[0102] 客户可以在子网级别控制VCN中的路由,因此客户可以指定客户的VCN(诸如VCN 104)中的哪些子网使用每个网关。VCN的路由表用于决定是否允许流量通过特定网关离开VCN。例如,在特定实例中,用于客户VCN 104内的公共子网的路由表可以通过IGW 120发送非本地流量。用于同一客户VCN 104内的私有子网的路由表可以通过SGW 126发送以CSP服务为目的地的流量。所有剩余流量可以经由NAT网关128发送。路由表仅控制流出VCN的流量。

[0103] 与VCN相关联的安全性列表用于控制经由入站连接经由网关进入VCN的流量。子网中的所有资源都使用相同的路由表和安全性列表。安全性列表可以用于控制允许进出VCN的子网中的实例的特定类型的流量。安全性列表规则可以包括入口(入站)和出口(出站)规则。例如,入口规则可以指定允许的源地址范围,而出口规则可以指定允许的目的地地址范围。安全性规则可以指定特定的协议(例如,TCP、ICMP)、特定的端口(例如,用于SSH的22、用于Windows RDP的3389)等。在某些实施方式中,实例的操作系统可以强制执行自己的符合安全性列表规则的防火墙规则。规则可以是有状态的(例如,跟踪连接并自动允许响应,而没有针对响应流量的明确安全性列表规则)或无状态的。

[0104] 来自客户VCN的访问(即,通过部署在VCN 104上的资源或计算实例)可以被分类为公开访问、私有访问或专用访问。公开访问是指使用公共IP地址或NAT来访问公共端点的访问模型。私有访问使VCN 104中具有私有IP地址的客户工作负载(例如,私有子网中的资源)能够访问服务,而无需穿越诸如互联网之类的公共网络。在某些实施例中,CSPI 101使具有私有IP地址的客户VCN工作负载能够使用服务网关访问服务(的公共服务端点)。因此,服务网关通过在客户的VCN和驻留在客户的私有网络外部的服务的公共端点之间建立虚拟链路

来提供私有访问模型。

[0105] 此外,CSPI可以使用诸如FastConnect公开对等之类的技术提供专用公开访问,其中客户内部部署实例可以使用FastConnect连接访问客户VCN中的一个或多个服务,而无需遍历诸如互联网之类的公共网络。CSPI还可以使用FastConnect私有对等提供专用私有访问,其中具有私有IP地址的客户内部部署实例可以使用FastConnect连接访问客户的VCN工作负载。FastConnect是对使用公共互联网将客户的内部部署网络连接到CSPI及其服务的网络连接性替代方案。与基于互联网的连接相比,FastConnect提供了简单、灵活且经济的方式来创建具有更高带宽选项的专用和私有连接以及更可靠和一致的网络体验。

[0106] 图1和上面的伴随描述描述了示例虚拟网络中的各种虚拟化的组件。如上所述,虚拟网络建立在底层物理或基底网络上。图2描绘了根据某些实施例的为虚拟网络提供底层的CSPI 200内的物理网络中的物理组件的简化体系架构图。如图所示,CSPI 200提供分布式环境,包括由云服务提供商(CSP)提供的组件和资源(例如,计算、存储器和网络资源)。这些组件和资源用于向订阅客户(即,已订阅由CSP提供的一个或多个服务的客户)提供云服务(例如,IaaS服务)。基于客户订阅的服务,为客户供应CSPI 200的资源的子集(例如,计算、存储器和网络资源)。然后,客户可以使用由CSPI 200提供的物理计算、存储器和联网资源构建其自己的基于云的(即,CSPI托管的)可定制且私有虚拟网络。如前面所指示的,这些客户网络被称为虚拟云网络(VCN)。客户可以在这些客户VCN上部署一个或多个客户资源,诸如计算实例。计算实例可以是虚拟机、裸机实例等形式。CSPI 200提供基础设施和一组互补的云服务,这使客户能够在高度可用的托管环境中构建和运行广泛的应用和服务。

[0107] 在图2中描绘的示例实施例中,CSPI 200的物理组件包括一个或多个物理主机机器或物理服务器(例如,202、206、208)、网络虚拟化设备(NVD)(例如,210、212)、架顶式(TOR)交换机(例如,214、216)和物理网络(例如,218),以及物理网络218中的交换机。物理主机机器或服务器可以托管和执行参与VCN的一个或多个子网的各种计算实例。计算实例可以包括虚拟机实例和裸机实例。例如,图1中描绘的各种计算实例可以由图2中描绘的物理主机机器托管。VCN中的虚拟机计算实例可以由一个主机机器或多个不同的主机机器执行。物理主机机器也可以托管虚拟主机机器、基于容器的主机或功能等。图1中描绘的VNIC和VCN VR可以由图2中描绘的NVD执行。图1中描绘的网关可以由图2中描述的主机机器和/或NVD执行。

[0108] 主机机器或服务器可以执行在主机机器上创建和启用虚拟化的环境的管理程序(也称为虚拟机监视器或VMM)。虚拟化或虚拟化的环境促进了基于云的计算。一个或多个计算实例可以由主机机器上的管理程序在该主机机器上创建、执行和管理。主机机器上的管理程序使主机机器的物理计算资源(例如,计算、存储器和网络资源)能够在由主机机器执行的各种计算实例之间共享。

[0109] 例如,如图2中所描绘的,主机机器202和208分别执行管理程序260和266。这些管理程序可以使用软件、固件或硬件或其组合来实现。通常,管理程序是位于主机机器的操作系统(OS)之上的进程或软件层,OS进而在主机机器的硬件处理器上执行。管理程序通过使主机机器的物理计算资源(例如,诸如处理器/核心之类的处理资源、存储器资源、网络资源)能够在由主机机器执行的各种虚拟机计算实例之间共享来提供虚拟化的环境。例如,在图2中,管理程序260可以位于主机机器202的OS之上并使主机机器202的计算资源(例如,处

理、存储器和网络资源)能够在由主机机器202执行的计算实例(例如,虚拟机)之间共享。虚拟机可以具有其自己的操作系统(称为访客操作系统),其可以与主机机器的OS相同或不同。由主机机器执行的虚拟机的操作系统可以与由同一主机机器执行的另一个虚拟机的操作系统相同或不同。因此,管理程序使多个操作系统能够被同时执行,同时共享主机机器的相同计算资源。图2中描绘的主机机器可以具有相同或不同类型的管理程序。

[0110] 计算实例可以是虚拟机实例或裸机实例。在图2中,主机机器202上的计算实例268和主机机器208上的计算实例274是虚拟机实例的示例。主机机器206是提供给客户的裸机实例的示例。

[0111] 在某些情况下,可以向单个客户供应整个主机机器,并且由该主机机器托管的一个或多个计算实例(或者虚拟机或者裸机实例)所有都属于同一客户。在其他情况下,主机机器可以在多个客户(即,多个租户)之间共享。在这种多租赁场景中,主机机器可以托管属于不同客户的虚拟机计算实例。这些计算实例可以是不同客户的不同VCN的成员。在某些实施例中,裸机计算实例由没有管理程序的裸机服务器托管。当供应裸机计算实例时,单个客户或租户维护对托管该裸机实例的主机机器的物理CPU、存储器和网络接口的控制,并且主机机器不与其他客户或租户共享。

[0112] 如前所述,作为VCN的一部分的每个计算实例都与使该计算实例能够成为VCN的子网的成员的VNIC相关联。与计算实例相关联的VNIC促进去往和来自计算实例的数据包或帧的通信。VNIC在创建计算实例时与该计算实例相关联。在某些实施例中,对于由主机机器执行的计算实例,与该计算实例相关联的VNIC由连接到主机机器的NVD执行。例如,在图2中,主机机器202执行与VNIC 276相关联的虚拟机计算实例268,并且VNIC 276由连接到主机机器202的NVD 210执行。作为另一个示例,由主机机器206托管的裸机实例272与由连接到主机机器206的NVD 212执行的VNIC 280相关联。作为又一个示例,VNIC 284与由主机机器208执行的计算实例274相关联,并且VNIC 284由连接到主机机器208的NVD 212执行。

[0113] 对于由主机机器托管的计算实例,连接到该主机机器的NVD还执行与计算实例是其成员的VCN对应的VCN VR。例如,在图2中描绘的实施例中,NVD 210执行与计算实例268是其成员的VCN对应的VCN VR 277。NVD 212还可以执行与VCN对应的一个或多个VCN VR 283,该VCN与由主机机器206和208托管的计算实例对应。

[0114] 主机机器可以包括使主机机器能够连接到其他设备的一个或多个网络接口卡(NIC)。主机机器上的NIC可以提供使主机机器能够通信连接到另一个设备的一个或多个端口(或接口)。例如,主机机器可以使用在主机机器上和NVD上提供的一个或多个端口(或接口)连接到NVD。主机机器也可以连接到其他设备(诸如另一个主机机器)。

[0115] 例如,在图2中,主机机器202使用链路220连接到NVD 210,链路220在由主机机器202的NIC 232提供的端口234与NVD 210的端口236之间延伸。主机机器206使用链路224连接到NVD 212,链路224在由主机机器206的NIC 244提供的端口246与NVD 212的端口248之间延伸。主机机器208使用链路226连接到NVD 212,链路226在由主机机器208的NIC 250提供的端口252与NVD 212的端口254之间延伸。

[0116] NVD进而经由通信链路连接到架顶式(TOR)交换机,这些交换机连接到物理网络218(也称为交换机架构)。在某些实施例中,主机机器和NVD之间以及NVD和TOR交换机之间的链路是以太网链路。例如,在图2中,NVD 210和212分别使用链路228和230连接到TOR交换

机214和216。在某些实施例中,链路220、224、226、228和230是以太网链路。连接到TOR的主机机器和NVD的集合有时称为机架(rack)。

[0117] 物理网络218提供使TOR交换机能够彼此通信的通信架构。物理网络218可以是多层网络。在某些实施方式中,物理网络218是交换机的多层Clos网络,其中TOR交换机214和216表示多层和多节点物理交换网络218的叶级节点。不同的Clos网络配置是可能的,包括但不限于2层网络、3层网络、4层网络、5层网络和一般的“n”层网络。Clos网络的示例在图5中描绘并在下面进行描述。

[0118] 主机机器和NVD之间可能存在各种不同的连接配置,诸如一对一配置、多对一配置、一对多配置等。在一对一配置实施方式中,每个主机机器连接到自己单独的NVD。例如,在图2中,主机机器202经由主机机器202的NIC 232连接到NVD 210。在多对一配置中,多个主机机器连接到一个NVD。例如,在图2中,主机机器206和208分别经由NIC 244和250连接到同一个NVD 212。

[0119] 在一对多配置中,一个主机机器连接到多个NVD。图3示出了CSPI 300内的示例,其中主机机器连接到多个NVD。如图3中所示,主机机器302包括网络接口卡(NIC)304,其包括多个端口306和308。主机机器300经由端口306和链路320连接到第一NVD 310,并经由端口308和链路322连接到第二NVD 312。端口306和308可以是以太网端口并且主机机器302与NVD 310和312之间的链路320和322可以是以太网链路。NVD 310进而连接到第一TOR交换机314并且NVD 312连接到第二TOR交换机316。NVD 310和312与TOR交换机314和316之间的链路可以是以太网链路。TOR交换机314和316表示多层物理网络318中的层0交换设备。

[0120] 图3中描绘的布置提供了两条单独的物理网络路径,从物理交换机网络318到主机机器302:第一条路径穿过TOR交换机314到NVD 310再到主机机器302,第二条路径穿过TOR交换机316到NVD 312再到主机机器302。单独的路径提供了主机机器302的增强的可用性(称为高可用性)。如果路径(例如,路径之一中的链路断开)或设备(例如,特定NVD未运行)之一出现问题,那么另一条路径可以用于与主机机器302之间的通信。

[0121] 在图3中描绘的配置中,主机机器使用由主机机器的NIC提供的两个不同端口连接到两个不同的NVD。在其他实施例中,主机机器可以包括使主机机器能够连接到多个NVD的多个NIC。

[0122] 返回去参考图2,NVD是执行一个或多个网络和/或存储虚拟化功能的物理设备或组件。NVD可以是具有一个或多个处理单元(例如,CPU、网络处理单元(NPU)、FPGA、数据包处理管线等)、存储器(包括缓存)和端口的任何设备。各种虚拟化功能可以由NVD的一个或多个处理单元执行的软件/固件来执行。

[0123] NVD可以以各种不同的形式实现。例如,在某些实施例中,NVD被实现为称为smartNIC的接口卡或具有板载嵌入式处理器的智能NIC。smartNIC是独立于主机机器上的NIC的设备。在图2中,NVD 210和212可以被实现为分别连接到主机机器202以及主机机器206和208的smartNIC。

[0124] 但是,smartNIC只是NVD实施方式的一个示例。各种其他实施方式是可能的。例如,在一些其他实施方式中,NVD或由NVD执行的一个或多个功能可以结合到一个或多个主机机器、一个或多个TOR交换机以及CSPI 200的其他组件中或由其执行。例如,NVD可以在主机机器中实施,其中由NVD执行的功能由主机机器执行。作为另一个示例,NVD可以是TOR交换机

的一部分,或者TOR交换机可以被配置为执行由NVD执行的功能,这使TOR交换机能够执行用于公共云的各种复杂数据包转换。执行NVD的功能的TOR有时被称为智能TOR。在向客户提供虚拟机(VM)实例而非裸机(BM)实例的其他实施方式中,由NVD执行的功能可以在主机机器的管理程序内部实现。在一些其他实施方式中,NVD的功能中的一些可以卸载到在一组主机机器上运行的集中式服务。

[0125] 在某些实施例中,诸如当实现为如图2中所示的smartNIC时,NVD可以包括使其能够连接到一个或多个主机机器以及一个或多个TOR交换机的多个物理端口。NVD上的端口可以被分类为面向主机的端口(也称为“南端口”)或面向网络或面向TOR的端口(也称为“北端口”)。NVD的面向主机的端口是用于将NVD连接到主机机器的端口。图2中面向主机的端口的示例包括NVD 210上的端口236以及NVD 212上的端口248和254。NVD的面向网络的端口是用于将NVD连接到TOR交换机的端口。图2中面向网络的端口的示例包括NVD 210上的端口256和NVD 212上的端口258。如图2中所示,NVD 210使用从NVD 210的端口256延伸到TOR交换机214的链路228连接到TOR交换机214。类似地,NVD 212使用从NVD 212的端口258延伸到TOR交换机216的链路230连接到TOR交换机216。

[0126] NVD经由面向主机的端口从主机机器接收数据包和帧(例如,由主机机器托管的计算实例生成的数据包和帧),并且在执行必要的数据包处理之后,可以经由NVD的面向网络的端口将数据包和帧转发到TOR交换机。NVD可以经由NVD的面向网络的端口从TOR交换机接收数据包和帧,并且在执行必要的数据包处理之后,可以经由NVD的面向主机的端口将数据包和帧转发到主机机器。

[0127] 在某些实施例中,在NVD和TOR交换机之间可以有多个端口和相关联的链路。可以聚合这些端口和链路以形成多个端口或链路的链路聚合体组(称为LAG)。链路聚合允许将两个端点之间(例如,NVD和TOR交换机之间)的多条物理链路视为单条逻辑链路。给定LAG中的所有物理链路都可以以相同的速度在全双工模式下操作。LAG有助于增加两个端点之间的连接的带宽和可靠性。如果LAG中的物理链路之一发生故障,那么流量将动态且透明地重新指派到LAG中的其他物理链路之一。聚合的物理链路比每条单独的链路递送更高的带宽。与LAG相关联的多个端口被视为单个逻辑端口。流量可以在LAG的多条物理链路之间进行负载平衡。可以在两个端点之间配置一个或多个LAG。这两个端点可以位于NVD和TOR交换机之间、主机机器和NVD之间,等等。

[0128] NVD实现或执行网络虚拟化功能。这些功能由NVD执行的软件/固件执行。网络虚拟化功能的示例包括但不限于:数据包封装和解封装功能;用于创建VCN网络的功能;用于实现网络策略的功能,诸如VCN安全性列表(防火墙)功能性;促进数据包路由和转发到VCN中的计算实例和从该计算实例转发的功能;等等。在某些实施例中,在接收到数据包后,NVD被配置为执行数据包处理流水线以处理数据包并确定如何转发或路由数据包。作为这个数据包处理管线的一部分,NVD可以执行与覆盖网络相关联的一个或多个虚拟功能,诸如执行与VCN中的计算机实例相关联的VNIC、执行与VCN相关联的虚拟路由器(VR)、数据包的封装和解封装以促进虚拟网络中的转发或路由、某些网关(例如,本地对等网关)的执行、安全性列表的实施方式、网络安全组、网络地址转换(NAT)功能性(例如,逐个主机地将公共IP转换到私有IP)、节流功能和其他功能。

[0129] 在某些实施例中,NVD中的数据包处理数据路径可以包括多个数据包管线,每个管

线由一系列数据包变换级组成。在某些实施方式中,在接收到数据包后,数据包被解析并分类到单个管线。然后以线性方式处理数据包,一个级接一个级,直到数据包或者被丢弃或者通过NVD的接口发送出去。这些级提供基本的功能性数据包处理构建块(例如,验证报头、强制执行节流、插入新的层2报头、强制执行L4防火墙、VCN封装/解封装等),以便可以通过组合现有级来构建新的管线,并且可以通过创建新级并将它们插入现有管线来添加新的功能性。

[0130] NVD可以执行与VCN的控制平面和数据平面对应的控制平面和数据平面功能。VCN控制平面的示例也在图12、图13、图14和图15中描绘(参见参考标号1216、1316、1416和1516)并在下面进行描述。VCN数据平面的示例在图12、图13、图14和图15中描绘(参见参考标号1218、1318、1418和1518)并在下面进行描述。控制平面功能包括用于配置控制数据如何被转发的网络的功能(例如,设置路由和路由表、配置VNIC等)。在某些实施例中,提供了VCN控制平面,它集中计算所有覆盖到基底映射并将它们发布到NVD和虚拟网络边缘设备(诸如各种网关,诸如DRG、SGW、IGW等)。防火墙规则也可以使用相同的机制发布。在某些实施例中,NVD仅获得与该NVD相关的映射。数据平面功能包括基于使用控制平面设置的配置来实际路由/转发数据包的功能。VCN数据平面是通过在客户的网络数据包穿过基底网络之前对其进行封装来实现的。封装/解封装功能性在NVD上实现。在某些实施例中,NVD被配置为拦截进出主机机器的所有网络数据包并执行网络虚拟化功能。

[0131] 如上面所指示的,NVD执行各种虚拟化功能,包括VNIC和VCN VR。NVD可以执行与连接到VNIC的一个或多个主机机器托管的计算实例相关联的VNIC。例如,如图2中所描绘的,NVD 210执行与由连接到NVD 210的主机机器202托管的计算实例268相关联的VNIC 276的功能性。作为另一个示例,NVD 212执行与由主机机器206托管的裸机计算实例272相关联的VNIC 280,并执行与由主机机器208托管的计算实例274相关联的VNIC 284。主机机器可以托管属于不同VCN(属于不同客户)的计算实例,并且连接到主机机器的NVD可以执行与计算实例对应的VNIC(即,执行VNIC相关功能性)。

[0132] NVD还执行与计算实例的VCN对应的VCN虚拟路由器。例如,在图2中描绘的实施例中,NVD 210执行与计算实例268所属的VCN对应的VCN VR 277。NVD 212执行与由主机机器206和208托管的计算实例所属的一个或多个VCN对应的一个或多个VCN VR 283。在某些实施例中,与该VCN对应的VCN VR由连接到托管属于该VCN的至少一个计算实例的主机机器的所有NVD执行。如果主机机器托管属于不同VCN的计算实例,那么连接到该主机机器的NVD可以执行与那些不同VCN对应的VCN VR。

[0133] 除了VNIC和VCN VR之外,NVD还可以执行各种软件(例如,守护进程)并且包括一个或多个硬件组件,这些组件促进由NVD执行的各种网络虚拟化功能。为了简单起见,这些各种组件被分组在一起作为图2中所示的“数据包处理组件”。例如,NVD 210包括数据包处理组件286并且NVD 212包括数据包处理组件288。例如,用于NVD的数据包处理组件可以包括数据包处理器,该数据包处理器被配置为与NVD的端口和硬件接口交互以监视由NVD接收和使用NVD传送的所有数据包并存储网络信息。网络信息例如可以包括识别由NVD处置的不同网络流的网络流信息和每个流信息(例如,每个流统计信息)。在某些实施例中,网络流信息可以以每个VNIC为基础来存储。数据包处理器可以执行逐数据包的操纵以及实现有状态的NAT和L4防火墙(FW)。作为另一个示例,数据包处理组件可以包括被配置为将由NVD存储的

信息复制到一个或多个不同的复制目标存储库的复制代理。作为又一个示例,数据包处理组件可以包括被配置为执行NVD的日志记录功能的日志记录代理。数据包处理组件还可以包括用于监视NVD的性能和健康状况并且还可能监视连接到NVD的其他组件的状态和健康状况的软件。

[0134] 图1示出了示例虚拟或覆盖网络的组件,包括VCN、VCN内的子网、部署在子网上的计算实例、与计算实例相关联的VNIC、用于VCN的VR以及为VCN配置的一组网关。图1中描绘的覆盖组件可以由图2中描绘的物理组件中的一个或多个执行或托管。例如,VCN中的计算实例可以由图2中描绘的一个或多个主机机器执行或托管。对于由主机机器托管的计算实例,与该计算实例相关联的VNIC通常由连接到该主机机器的NVD执行(即,VNIC功能性由连接到该主机机器的NVD提供)。用于VCN的VCN VR功能由连接到托管或执行作为该VCN的一部分的计算实例的主机机器的所有NVD执行。与VCN相关联的网关可以由一种或多种不同类型的NVD执行。例如,某些网关可以由smartNIC执行,而其他网关可以由一个或多个主机机器或NVD的其他实施方式执行。

[0135] 如上所述,客户VCN中的计算实例可以与各种不同的端点通信,其中端点可以与源计算实例在同一子网内、在不同子网中但与源计算实例在同一VCN内,或者与位于源计算实例的VCN外部的端点通信。使用与计算实例相关联的VNIC、VCN VR以及与VCN相关联的网关来促进这些通信。

[0136] 对于VCN中同一子网上的两个计算实例之间的通信,使用与源和目的地计算实例相关联的VNIC促进通信。源和目的地计算实例可以由同一主机机器或不同的主机机器托管。源自源计算实例的数据包可以从托管源计算实例的主机机器转发到连接到该主机机器的NVD。在NVD上,使用数据包处理管线处理数据包,这可以包括与源计算实例相关联的VNIC的执行。由于用于数据包的目的地端点位于同一子网内,因此与源计算实例相关联的VNIC的执行导致数据包被转发到执行与目的地计算实例相关联的VNIC的NVD,然后NVD处理数据包并将其转发到目的地计算实例。与源和目的地计算实例相关联的VNIC可以在同一个NVD上执行(例如,当源和目的地计算实例由同一个主机机器托管时)或在不同的NVD上执行(例如,当源和目的地计算实例由连接到不同NVD的不同主机机器托管时)。VNIC可以使用由NVD存储的路由/转发表来确定用于数据包的下一跳。

[0137] 对于要从子网中的计算实例传送到同一VCN中不同子网中的端点的数据包,源自源计算实例的数据包从托管源计算实例的主机机器传送到连接到该主机机器的NVD。在NVD上,使用数据包处理管线处理数据包,这可以包括一个或多个VNIC以及与VCN相关联的VR的执行。例如,作为数据包处理管线的一部分,NVD执行或调用与和源计算实例相关联的VNIC对应的功能性(也称为执行VNIC)。由VNIC执行的功能性可以包括查看数据包上的VLAN标记。由于数据包的目的地在子网外部,因此接下来由NVD调用和执行VCN VR功能性。然后,VCN VR将数据包路由到执行与目的地计算实例相关联的VNIC的NVD。与目的地计算实例相关联的VNIC然后处理数据包并将数据包转发到目的地计算实例。与源和目的地计算实例相关联的VNIC可以在同一个NVD上执行(例如,当源和目的地计算实例由同一个主机机器托管时)或在不同的NVD上执行(例如,当源和目的地计算实例由连接到不同NVD的不同主机机器托管时)。

[0138] 如果用于数据包的目的地在源计算实例的VCN外部,那么源自源计算实例的数据

包从托管源计算实例的主机机器传送到连接到该主机机器的NVD。NVD执行与源计算实例相关联的VNIC。由于数据包的目的地端点在VCN外部,因此数据包随后由用于该VCN的VCN VR处理。NVD调用VCN VR功能性,这会导致数据包被转发到执行与VCN相关联的适当网关的NVD。例如,如果目的地是客户的内部部署网络内的端点,那么数据包可以由VCN VR转发到执行为VCN配置的DRG网关的NVD。VCN VR可以在与执行与源计算实例相关联的VNIC的NVD相同的NVD上执行,或者由不同的NVD执行。网关可以由NVD执行,NVD可以是smartNIC、主机机器或其他NVD实施方式。然后,数据包由网关处理并转发到下一跳,该下一跳促进将数据包传送到其预期的目的地端点。例如,在图2中描绘的实施例中,源自计算实例268的数据包可以通过链路220(使用NIC 232)从主机机器202传送到NVD 210。在NVD 210上,调用VNIC 276,因为它是与源计算实例268相关联的VNIC。VNIC 276被配置为检查数据包中封装的信息,并确定用于转发数据包的下一跳,目的是促进将数据包传送到其预期的目的地端点,然后将数据包转发到确定的下一跳。

[0139] 部署在VCN上的计算实例可以与各种不同端点通信。这些端点可以包括由CSPI 200托管的端点和CSPI 200外部的端点。由CSPI 200托管的端点可以包括同一VCN或其他VCN中的实例,这些VCN可以是客户的VCN,或者是不属于客户的VCN。由CSPI 200托管的端点之间的通信可以通过物理网络218执行。计算实例还可以与不由CSPI 200托管或在CSPI 200外部的端点通信。这些端点的示例包括客户的内部部署网络内的端点或数据中心,或可通过公共网络(诸如互联网)访问的公共端点。与CSPI 200外部的端点的通信可以使用各种通信协议通过公共网络(例如,互联网)(图2中未示出)或专用网络(图2中未示出)来执行。

[0140] 图2中描绘的CSPI 200的体系架构仅仅是示例,并非旨在限制。在替代实施例中,变化、替代和修改是可能的。例如,在一些实施方式中,CSPI 200可以具有比图2中所示的系统或组件更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。图2中描绘的系统、子系统和其他组件可以在由相应系统的一个或多个处理单元(例如,处理器、核心)执行的软件(例如,代码、指令、程序)中、使用硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。

[0141] 图4描绘了根据某些实施例的主机机器和NVD之间的连接,用于提供I/O虚拟化以支持多租赁。如图4中所描绘的,主机机器402执行提供虚拟化的环境的管理程序404。主机机器402执行两个虚拟机实例,属于客户/租户#1的VM1 406和属于客户/租户#2的VM2 408。主机机器402包括经由链路414连接到NVD 412的物理NIC 410。每个计算实例都附接到由NVD 412执行的VNIC。在图4中的实施例中,VM1 406附接到VNIC-VM1 420并且VM2 408附接到VNIC-VM2422。

[0142] 如图4中所示,NIC 410包括两个逻辑NIC,逻辑NIC A 416和逻辑NIC B 418。每个虚拟机附接到其自己的逻辑NIC并被配置为与其自己的逻辑NIC一起工作。例如,VM1 406附接到逻辑NIC A 416并且VM2 408附接到逻辑NIC B 418。虽然主机机器402仅包括由多个租户共享的一个物理NIC 410,但由于逻辑NIC,因此每个租户的虚拟机相信他们有自己的主机机器和NIC。

[0143] 在某些实施例中,每个逻辑NIC被指派有其自己的VLAN ID。因此,特定的VLAN ID被指派给用于租户#1的逻辑NIC A 416,并且分离的VLAN ID被指派给用于租户#2的逻辑NIC B 418。当数据包从VM1 406传送时,由管理程序将指派给租户#1的标签附加到数据包,

然后数据包通过链路414从主机机器402传送到NVD 412。以类似的方式,当数据包从VM2 408被传送时,指派给租户#2的标签由管理程序附加到数据包,然后数据包通过链路414从主机机器402传送到NVD 412。相应地,从主机机器402传送到NVD 412的数据包424具有识别特定租户和相关联的VM的相关联的标签426。在NVD上,对于从主机机器402接收到的数据包424,与该数据包相关联的标签426用于确定数据包是由VNIC-VM1 420还是由VNIC-VM2 422处理。数据包随后由对应的VNIC处理。图4中描述的配置使每个租户的计算实例能够相信他们拥有自己的主机机器和NIC。图4中描述的设置提供了I/O虚拟化以支持多租赁。

[0144] 图5描绘了根据某些实施例的物理网络500的简化框图。图5中描绘的实施例被结构化为Clos网络。Clos网络是特定类型的网络拓扑,被设计为提供连接冗余性,同时维持高对分带宽和最大资源利用率。Clos网络是一种无阻塞、多级或多层交换网络,其中级数或层数可以是二、三、四、五等。图5中描绘的实施例是3层网络,包括层1、层2和层3。TOR交换机504表示Clos网络中的层0交换机。一个或多个NVD连接到TOR交换机。层0交换机也被称为物理网络的边缘设备。层0交换机连接到也称为叶交换机的层1交换机。在图5中描绘的实施例中,一组“n”个层0TOR交换机连接到一组“n”个层1交换机并一起形成群聚(pod)。群聚中的每个层0交换机都互连到该群聚中的所有层1交换机,但群聚之间没有交换机的连接性。在某些实施方式中,两个群聚被称为块。每个块由一组“n”个层2交换机(有时称为主干交换机)提供服务或连接到这些交换机。物理网络拓扑中可以有几个块。层2交换机进而连接到“n”个层3交换机(有时称为超级主干交换机)。物理网络500之上的数据包的通信通常使用一种或多种层3通信协议来执行。通常,物理网络的所有层(TOR层除外)都是n向冗余的,因此允许高可用性。可以为群聚和块指定策略,以控制交换机在物理网络中彼此的可见性,从而启用物理网络的扩展(scale)。

[0145] Clos网络的特征是从一个层0交换机到另一个层0交换机(或从连接到层0交换机的NVD到连接到层0交换机的另一个NVD)达到的最大跳数是固定的。例如,在3层Clos网络中,数据包从一个NVD到达另一个NVD最多需要七跳,其中源和目标NVD连接到Clos网络的叶层。同样,在4层Clos网络中,数据包从一个NVD到达另一个NVD最多需要九跳,其中源和目标NVD连接到Clos网络的叶层。因此,Clos网络体系架构在整个网络中维持一致的时延,这对于数据中心内部和数据中心之间的通信是重要的。Clos拓扑可水平扩展且具有成本效益。通过在各个层添加更多交换机(例如,更多叶交换机和骨干交换机)以及通过增加相邻层的交换机之间的链路数量,可以轻松增加网络的带宽/吞吐量容量。

[0146] 在某些实施例中,CSPI内的每个资源都被指派称为云标识符(CID)的唯一标识符。这个标识符作为资源的信息的一部分包括在内并且可以用于管理资源,例如,经由控制台或通过API。用于CID的示例语法是:

[0147] ocid1.<RESOURCE TYPE>.<REALM>.[REGION][.FUTURE USE].<UNIQUE ID>

[0148] 其中,

[0149] ocid1:指示CID的版本的文字串;

[0150] resource type:资源的类型(例如,实例、卷、VCN、子网、用户、组等);

[0151] realm:资源所在的领域。示例值为用于商业领域的“c1”、用于政府云领域的“c2”或用于联邦政府云领域的“c3”等。每个领域可以有其自己的域名;

[0152] region:资源所在的区域。如果该区域不适用于该资源,那么这个部分可能为空;

[0153] future use:保留以备将来使用。

[0154] unique ID:ID的唯一部分。格式可以因资源或服务的类型而异。

[0155] 多云介绍

[0156] 图6描绘了根据某些实施例的分布式环境600的简化高级图,该分布式环境包括由不同云服务提供商(CSP)提供的多个云环境,其中云环境包括提供专门基础设施的特定云环境,该基础设施使得由该特定云环境提供的一个或多个云服务能够被其他云环境的客户使用。如图6中所描绘的,各种不同的云环境(也称为"云")可以由不同的云服务提供商(CSP)提供,每个云环境或云供应可以由该云环境的一个或多个客户订阅的一个或多个云服务。由CSP提供的云环境供应的一组云服务可以包括一个或多个不同类型的云服务,包括但不限于软件即服务(SaaS)服务、基础设施即服务(IaaS)服务、平台即服务(PaaS)服务、数据库即服务(DBaaS)服务等。由各种CSP提供的云环境的示例包括由Oracle Corporation提供的**Oracle®** Cloud Infrastructure(OCI)、由Microsoft Corporation提供的**Microsoft®**Azure、由Google LLC提供的Google Cloud™、由Amazon Corporation提供的Amazon Web Services(**AWS®**)等。由特定云环境供应的云服务可以与由另一个云环境供应的一组云服务不同。

[0157] 在典型的云环境中,CSP提供云服务提供商基础设施(CSPI),用于向其客户提供由该云环境供应的一个或多个云服务。由CSP提供的CSPI可以包括各种类型的硬件和软件资源,包括计算资源、存储器资源、联网资源、用于访问云服务的控制台等。由CSP提供的云环境的客户可以订阅由该云环境供应的云服务中的一个或多个。可以由CSP向其客户供应各种订阅模型。在客户订阅由云环境提供的云服务之后,一个或多个用户可以与订阅客户相关联,并且这些用户可以使用客户订阅的云服务。在某些实施方式中,当客户订阅由特定云环境提供的云服务时,将为该客户创建客户账户或客户租赁。然后可以将一个或多个用户与客户租赁相关联,然后这些用户可以在客户租赁下使用客户订阅的服务。有关客户订阅的服务、与客户租赁相关联的用户等的信息通常存储在云环境内并与客户租赁相关联。

[0158] 例如,图6中描绘了由三个不同的CSP提供的三个不同的云环境。这些包括由CSP A提供的云环境A(云A)610、由CSP B提供的云环境B(云B)640以及由CSP C提供的云环境C(云C)660。云A 610包括由CSP A提供的基础设施CSPI_A 612,并且这个基础设施可以用于提供由云A 610提供的一组服务"服务A"614。一个或多个客户(例如,Cust_A1 616-1、Cust_A2 616-2)可以订阅由云A 610提供的服务A 614中的一个或多个服务。一个或多个用户618-1可以与客户A1 616-1相关联,并且可以使用客户A1 616-1在云A 610中订阅的服务。以类似的方式,一个或多个用户618-2可以与客户A2616-2相关联,并且可以使用客户A2 616-2在云A 610中订阅的服务。在各种用例中,客户A1 616-1订阅的服务可以与客户A2 616-2订阅的服务不同。

[0159] 如图6中所描绘的,云B 640包括由CSP B提供的基础设施CSPI_B 642,并且这个基础设施可以用于提供由云B 640供应的一组服务"服务B"644。一个或多个客户(例如,Cust_B1 646-1)可以订阅服务B 644中的一个或多个服务。一个或多个用户648-1可以与客户B1 646-1相关联,并且可以在云B 640中使用客户B1 646-1订阅的服务。

[0160] 如图6中所描绘的,云C 660包括由CSP C提供的基础设施CSPI_C 662,并且这个基础设施可以用于提供由云C 660供应的一组服务"服务C"664。一个或多个客户(例如,Cust_

C1 666-1)可以订阅服务C 664中的一个或多个服务。一个或多个用户668-1可以与客户C1 666-1相关联,并且可以在云C 660中使用客户C1 666-1订阅的服务。要注意的是,服务A 614、服务B 644和服务C 664可以彼此不同。

[0161] 在现有的云实施方式中,每个云为其订阅客户和相关联的用户提供闭合的生态系统。因此,云环境的客户及其相关联的用户被限于使用由该客户订阅的云供应的服务。例如,客户B1 646-1及其用户648-1被限于使用由云B 640提供的服务B 644,并且不能使用他们在云B640中的账户访问来自不同云环境的服务,诸如由云A 610供应的服务A 614中的服务或由云C 660供应的服务C 664中的服务。本文描述的示教克服了这个限制。如本公开中所描述的,描述了使得能够在两个云环境之间创建链路的各种技术,该链路使得由第一CSP提供的第一云环境提供的服务能够由第二不同CSP提供的第二不同云环境的客户(和相关联的用户)使用客户在第二云环境中的账户来使用。

[0162] 例如,在图6中描绘的实施例中,除了其他基础设施620之外,由CSP A提供的基础设施CSPI_A 612还包括特殊基础设施622(称为启用多云的基础设施622或MEI 622或多云基础设施622),该特殊基础设施622使得由云A供应的一个或多个服务614能够由其他云(诸如云B 640和C 660)的客户和相关联的用户使用那些其他云中的客户账户来使用。在某些实施方式中,云B和C的客户不必在云A开设单独的账户即可使用由云A 610供应的服务614中的一个或多个服务。云B 640的客户B1 646-1和相关联的用户648-1可以使用他们在云B 640中的客户账户或租赁来使用由云A 610提供的一个或多个服务614。作为另一个示例,云C 660的客户C1 666-1和相关联的用户668-1可以使用他们在云C 660中的客户账户或租赁来使用由云A610提供的一个或多个服务614。

[0163] 在某些实施方式中,MEI 622使得能够在云A 610与其他云之间创建链路,其中这些链路可以由其他云的客户及其相关联的用户用来访问和使用由云A 610提供的服务。这在图6中以符号形式示为在云A 610和云B 640之间创建的链路670,以及在云A 610和云C 660之间创建的链路672。经由链路670,云B 640的客户可以访问或使用由云A 610提供的一个或多个服务614。同样,经由链路672,云C 660的客户可以访问或使用由云A 610提供的一个或多个服务614。

[0164] 有不同方式可以实现MEI 612。在某些实施例中,MEI 612可以包括使得能够与不同云建立链路的组件。例如,在图6中,MEI 622包括负责启用与云B 640的链路670的基础设施组件624,以及用于启用与云C 660的链路672的基础设施组件626。以类似的方式,MEI 622可以包括启用和促进与其他云的链路的其他组件。在一些实施例中,MEI 622的组件还可以促进与多个不同云的链路。

[0165] 一个云的客户可能想要或期望使用由不同云提供的云服务的原因有几个。以图6为例,云B 640的客户B1 646-1可能想要使用由云A610提供的云服务614的原因有多个。在一个用例场景中,这种情况可能发生,因为云A 610供应具有云B 640未提供的功能性的云服务。作为另一个用例场景,云A和B可以供应类似的服务,但由云A 610提供的服务可以比由云B 640供应的对应服务更好(例如,更多特征/功能性、更快等)。作为另一个用例场景,云B 640的客户B1 646-1可能想要使用由云A 610提供的云服务,因为该服务的价格比云B 640提供的更便宜。在一些情况下,可以存在云B 640的客户B1 646-1可能想要使用由云A 610提供的云服务地理限制或其他原因。例如,云A 610可以在云B 640未提供服务的地理地

区供应期望的服务,或者云B 640未在客户期望服务的地理地区提供特定服务。还可能存在为什么一个云的客户可能想要使用由不同云提供的服务的其他几个用例场景。

[0166] 在某些实施例中,MEI 622提供能力并执行功能以在云A 610和另一个云之间创建链路,并且经由该链路,使得与另一个云的客户相关联的用户能够以无缝的方式从另一个云本身访问和使用由云A 610提供的服务。例如,MEI 622使得与云640的客户B1 646-1相关联的用户648-1能够以无缝的方式访问由云A 610供应的服务A 614中的服务。在某些实施方式中,可以提供用户648-1可以从云B 640内访问的用户界面(例如,控制台),该用户界面使得用户能够看到由云A 610提供的服务614的列表并选择用户648-1希望访问的特定服务。响应于用户选择,MEI 622负责执行在云A和B之间建立链路670的处理,以使得能够访问所请求的服务。用于设置链路670的处理基本上由MEI 622自动执行。客户B1 646-1或相关联的用户648-1不必担心执行促进在云A 610和B 640之间创建、维护和使用链路670所需的任何系统、联网或其他配置改变。在创建云之间的链路时,用户或客户不会有任何负担。使用本公开中描述的技术,以快速高效的方式创建链路。

[0167] MEI 622可以使用各种技术使链路的创建和使用对用户和客户而言无缝衔接,从而提供增强的用户体验。在某些实施方式中,MEI 622使客户B1和相关联的用户648-1与之交互的用户界面(例如,图形用户界面GUI等)和处理流(诸如用于从云A 610请求服务和用于从云A 610访问所请求的服务)与客户/用户在云B 640中将体验到的界面和处理流基本相似。以这种方式,可能习惯于云B 640的界面和处理流的客户或用户不必学习新的界面和处理流来从云A 610访问服务614。MEI 622可以为不同云环境的用户呈现不同的界面和处理流。例如,可以向来自云B 640的用户呈现与云B的用户界面和流程基本相似的第一组用户界面和流程,而向从云C 660访问云A 610的用户呈现与云C的用户界面和流程基本相似的另一组用户界面和流程。这样做是为了简化并因此增强用户从其他云访问云A 610的服务614的体验。

[0168] 作为另一个示例,每个云环境通常包括被配置为提供云环境的安全性的身份管理系统。身份管理系统被配置为保护云环境中的资源,包括由CSP提供的资源和部署在云环境中的订阅云客户的资源。由身份管理系统执行的功能包括,例如,管理与云的订阅客户和相关联的用户相关联的身份凭证(例如,用户名、密码等),使用身份凭证基于为云环境配置的权限/访问策略来规范(regulate)用户对云资源和服务的访问,以及其他功能。不同的云可以使用不同的身份管理系统和相关联的技术。例如,云A 610中的身份管理系统和相关联的过程可以与云B 640中的身份管理系统和相关联的过程完全不同,而云B640中的身份管理系统和相关联的过程又可以与云C 660中的身份管理系统和相关联的过程完全不同。在某些实施方式中,虽然不同云环境之间的身份管理系统和相关联的过程存在差异,但本文描述的技术使得与第一云的客户相关联的用户能够使用与第一云中的客户和用户相关联的相同身份凭证来访问由不同云提供的云服务。

[0169] 例如,在图6中所描绘的实施例中,由CSP B提供的云B 640可以包括身份管理系统,该身份管理系统向其订阅客户和相关联的用户(诸如客户B1 646-1和相关联的用户648-1)指派或分配身份凭证。这些身份凭证与在云B 640中为客户B1 646-1创建的租赁相关联。在某些实施方式中,由云A 610提供的MEI 622使得与云B客户B1 646-1相关联的用户648-1能够使用与云B 640中的用户648-1和客户B1646-1相关联的身份凭证来访问来自云A

610中的服务A 614中的服务。这大大增强了用户648-1的用户体验,因为他们不必仅为了访问云A 610中的服务614而创建特定于云A 610的新身份凭证。MEI 622促进了这种访问。

[0170] 作为示例,云B 640的客户B1可以从由云A 610提供的一组服务614中选择使用服务,诸如数据库即服务(DBaaS)。响应于这种选择,MEI 622使得在云A 610和云B 640之间自动创建链路670,以使与客户B1 646-1相关联的用户648-1能够使用由云A 610提供的DBaaS服务。链路670的自动设置通过MEI 622来促进。在设置链路670之后,用户668-1可以经由云B 640使用云A 610中的DBaaS服务。作为使用这个服务的一部分,用户668-1可以经由云B 640向云A 610发送创建数据库资源的请求。作为响应,CSPI_A 612可以在云A 610中创建所请求的数据库。在某些实施方式中,所创建的数据库可以在云A 610中为客户B1创建的虚拟网络(例如,虚拟云网络或VCN)中供给,并且用户668-1可经由云B 640访问。然后,用户668-1可以从云B 640向云A 610发送请求以使用所供给的数据库。这些请求可以包括,例如,将数据写入数据库、更新存储在数据库中的数据、删除数据库中的数据、删除数据库、创建附加的数据库等的请求。在一些用例中,这些请求可以经由云B 640源自用户668-1或源自由云B 640提供的服务644。以这种方式,由云A 610提供的MEI 622使得与由不同CSP提供的不同云的客户相关联的用户能够无缝地访问由云A 610提供的服务。

[0171] 图6中描绘的分布式环境600仅仅是个示例,并非旨在过度限制所要求保护的实施例的范围。许多变化、替代和修改是可能的。例如,在替代实施例中,分布式环境600可以具有更多或更少的云环境。云环境还可以具有更多或更少的系统和组件,或者可以具有系统和组件的不同配置或布置。图6中描绘的系统和组件可以在由相应系统的一个或多个处理单元(例如,处理器、核心)执行的软件(例如,代码、指令、程序)中、使用硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,在存储器设备上)。

[0172] 多云控制平面(MCCP)

[0173] 图7描绘了根据一些实施例的将两个不同的云环境互连的多云基础设施的高级体系架构,每个云环境由云服务提供商提供。如图7中所示,高级体系架构700包括由第一云服务提供商(例如,OCI)710提供的第一云环境和由第二云服务提供商720(例如,AWS)提供的第二云环境。第一云环境710包括多云基础设施,该多云基础设施供给将第一云环境的服务交付给其他云环境(例如,第二云环境720)的用户的能力。具体而言,如下面将描述的,多云基础设施包括多云控制平面(MCCP)712和多云网络数据平面(MCNDP)716,其为用户供给从另一个云环境访问/管理第一云环境的服务(例如,PaaS服务)。

[0174] 多云基础设施提供尽可能接近用户的原生云环境(例如,第二云环境720)的用户体验,同时提供云环境之间的简单集成。注意的是,MCCP 712和MCNDP 716是多云基础设施的组件,它们由第一云服务提供商在第一云环境710中部署(和管理)。在一些实施例中,多云基础设施包括另一个组件(即,多云服务账户726A),该组件部署在第二云环境720中并由第一云服务提供商管理。

[0175] 根据一些实施例,第二云环境720包括客户账户721和第一云服务提供商的账户(本文称为多云账户或多云服务账户726A)。注意的是,第二云环境720也可以包括第二云门户(未示出),该第二云门户形成其中第二环境720的客户可以登录并管理其原生云部署和实例的集中式接入点。第二云门户可以提供用于监视和操作由第二云基础设施提供的服务的选项。根据一些实施例,第二云环境720包括供给模块722、监视模块724和身份系统723,

该身份系统包括身份模块723A和访问控制模块723B(即,本文也称为身份和访问管理(IAM)模块)。此外,客户账户721中包括的是客户的虚拟私有云(VPC)725A,其可以托管一个或多个计算实例725B。身份模块723A被配置为执行任务,诸如为第二云环境720的一个或多个用户创建一组一个或多个角色(以及与相应角色对应的相关联策略、权限等)。在一些实施方式中,访问控制模块723B充当第二云环境的用户目录。具体而言,访问控制模块723B可以被配置为创建用户池,并执行诸如添加用户登记、登录和对web和移动应用的访问控制之类的功能。

[0176] 供给模块722与第二云环境720提供的服务对应,该服务使用户能够以自动化且安全的方式建模和管理基础设施资源。例如,使用供给模块722,开发人员可以使用基础设施即代码模板定义和供给基础设施资源。换句话说,供给模块722使第二云环境720中客户账户中的资源的先决条件设置自动化。作为另一个示例,供给模块722还可以被配置为设置允许第一云环境的组件能够访问第二云环境中客户账户中的资源的先决条件资源。根据某些实施例,这通过允许多云服务账户726A访问客户账户721中的资源来实现,例如,允许多云服务账户与客户账户对等,允许多云基础设施的组件(例如,用于在第二云环境中发布度量的可观察性适配器等)。监视模块724使得能够监视整个堆栈(例如,应用、基础设施、网络和服务),并使用警报、日志和事件数据来执行自动化动作。监视模块724还可以利用仪表板(例如,在GUI中)可视化地描绘从第一云环境获得的一个或多个度量数据。

[0177] 多云服务账户726A包括虚拟私有云726B,其托管中转(transit)网关和直接连接组件。直接连接组件是联网组件,其提供使用互联网来利用第二云环境的云服务的替代方案。直接连接使客户能够与第二云环境建立低时延、安全且私密的连接,用于需要比互联网更高速度或更低时延的工作负载。中转网关是可以用于互连VPC和内部部署的网络的联网枢纽。在一些实施例中,多云服务账户726A中的中转网关用于与第二云环境720中的客户账户721对等(即,通信地耦合)。

[0178] 第一云环境710包括MCCP 712、客户租赁714和MCNDP 716。如前所述,MCCP 712和MCNDP 716是多云基础设施的部分,这些部分向其他云环境(例如,第二云环境720)的用户供给对第一云环境710提供的服务的访问,其中用户体验尽可能接近用户的原生云环境的用户体验,同时提供云环境之间的简单集成。

[0179] 第一云环境710还包括多云控制台750(不同于第二云门户),其允许在第二云基础设施720中经过认证的用户对经由多云基础设施暴露的第一云基础设施710的资源执行控制平面操作。换句话说,多云控制台750为第二云环境720的用户形成网关,以能够访问部署在第一云环境710中的资源。应该认识到的是,用户705可以直接从多云控制台750发出针对第一云基础设施提供的资源的请求(例如,CRUD请求)。

[0180] 第一云环境中包括的MCCP 712包括多个微服务,诸如代理模块712A、平台服务模块712B、以及适配器池712C。适配器池712C包括云链路适配器、数据库(DB)适配器、网络适配器、可观察性适配器和支持适配器。

[0181] 适配器池712C中包括的每个适配器负责向其他云环境(例如,第二云环境)的用户暴露一组唯一的底层资源(由第一云环境提供)。具体而言,适配器池712C中的每个适配器都映射到第一云基础设施供应的特定产品或资源。在一些实施方式中,注意的是,实际资源可以由第一云基础设施的原生控制平面(未示出)创建。第一云环境的原生控制平面提供跨

云环境的管理和编排。在这里可以设置配置基线、供给用户和角色访问、以及应用驻留,使得它们可以与相关服务一起执行。例如,关于数据库即服务(DBaaS),第一云环境的原生控制平面中包括的DBaaS控制平面被配置为实例化第一云环境的客户租赁714中的Exa数据库资源。

[0182] 用户705在多云控制台750处发出的请求被路由到MCCP的代理模块712A。注意的是,代理模块712A处理传入的请求以执行认证和访问控制。每个请求都包括与第二云基础设施中的用户账户相关联的令牌(token)(下面描述)。代理模块提取令牌并与访问控制模块723B(即,第二云环境的身份提供商系统)一起验证令牌。在验证成功后,代理模块712A可以检查与用户相关联的角色(即,特权集)。注意的是,角色可以与允许该角色执行的一个或多个任务/操作相关联。

[0183] 根据一个实施例,代理模块712A负责对MCCP的传入请求进行认证,并基于与令牌相关联的角色授权用户是否被允许执行所请求的操作。在一些实施方式中,代理模块712A可以通过利用与第一云基础设施相关联的服务平台(SPLAT)的自定义认证特征来执行上述认证处理。应该认识到的是,广义上讲,SPLAT是基础设施,它促进由云服务提供商提供的各种云服务的交付。SPLAT接受传入请求并将其转发到代理模块712A,代理模块712A进一步解析传入请求以确定授权决策,并向SPLAT返回成功或失败消息。当成功时,SPLAT可以将请求定向到路由模块,该路由模块将请求定向到适配器池中的适当适配器,而当失败时,SPLAT直接向调用者返回错误响应。

[0184] 根据一个实施例,代理模块712A接受来自第一云环境的服务平台(即,SPLAT)的预认证请求,并基于传入请求中包含的路径信息将请求路由到适当的适配器。在一些实施方式中,代理模块可以(从传入请求中)提取与服务的提供商对应的标识符,并将请求路由到适配器池712C中的适当适配器。

[0185] MCCP 712中包含的云链路适配器负责处置第一云环境提供的资源的生命周期操作。云链路适配器被配置为创建用户在第二云环境中的账户与第一云基础设施中的用户的对应租赁/账户之间的映射(或在登记处理时创建的关系)。换句话说,云链路适配器生成与用户在第一云环境中的租赁相关联的第一标识符与与用户在第二云环境中的账户相关联的第二标识符的映射。

[0186] 在一些实施例中,云链路适配器执行外部云标识符(例如,与用户在第二云环境中的账户相关联的第二标识符)和(与用户在第一云环境中的租赁相关联的)第一标识符之间的转换,以使通过MCCP的操作能够映射到第一云环境中的适当底层资源。在一些实施例中,云链路适配器生成数据对象以存储上述映射信息。此外,云链路适配器还生成与数据对象相关联的资源主体(resource-principal)。基于请求中包含的令牌(及其相关联角色)为资源主体指派一个或多个权限。用户基于资源主体从第二云基础设施实现对第一云环境提供的下游服务的访问。云链路适配器可以将数据对象和相关联的资源主体存储在第一云基础设施中用户的租赁的根隔间中。替代地或附加地,云链路适配器还可以将数据对象和资源主体本地持久化在多云基础设施的平台模块712B上,以便多云基础设施中包含的其他适配器无缝访问。

[0187] 网络适配器(也称为网络链路适配器)负责在客户账户721(在第二云环境中)与对应的客户租赁/账户(在第一云环境中)714之间创建网络链路(即,通信链路/通道)。根据一

些实施例,网络链路适配器获得令牌(来自平台模块712B)并创建(1)MCNDP 716与客户租赁714之间的第一对等关系(在第一云环境中),以及(2)客户账户721与第二云环境中包括的第一云服务提供商717的多云服务账户726A之间的第二对等关系(在第二云环境中)。

[0188] 第一云环境710中的MCNDP 716包括快速连接以及枢纽和辐射(hub and spoke)VCN,其供给要与第一云环境中的客户租赁714建立的网络连接(例如,从内部部署的位置、从外部云环境)。另一方面,多云服务账户中包含的中转网关与第二云环境中的客户账户对等。网络适配器可以配置互连719通信地耦合两个云环境。具体而言,在一端,互连与直接连接(位于多云服务账户726A中)耦合,而在另一端,互连与MCDP中的快速连接耦合。应该认识到的是,快速连接(包括在第一云环境中)和第二云环境中包括的直接连接可以共同位于同一区域中。此外,在两个云环境之间形成网络链路后,在客户账户中执行的应用(例如,在第二云环境的客户VPC中)能够访问资源,例如,部署在第一云环境的客户租赁714中的Exa数据库资源。应该认识到的是,网络链路将用户在第一云环境中的租赁与用户在第二云环境中的账户通信地耦合。

[0189] 如图7中所示,可观察性模块(包括在适配器池712C中)被配置为将与第一云环境中的客户租户中部署的资源相关的日志、度量和其他性能参数镜像或转发(例如,发布)到例如包括在第二云环境中包括的监视模块724中的仪表板以进行进一步处理。根据一些实施例,包括在多云基础设施中的平台服务模块712B被配置为存储与提供给第二云基础设施的用户的第一云环境的服务相关联的凭证。平台服务模块712B为包括在适配器池712C中的不同适配器提供例如令牌/资源主体,使得适配器可以与第一云基础设施的原生控制平面通信。根据一些实施例,平台服务模块712B暴露由不同适配器调用的API以执行诸如以下任务:

[0190] • 向适配器出售最小范围的访问令牌(由第二云基础设施颁发)。例如,网络适配器需要访问令牌来执行上述网络对等操作。

[0191] • 提供资源主体,适配器将使用该资源主体来调用下游服务以在第一云基础设施的客户租赁中创建资源。

[0192] • 触发从第一云基础设施到第二云基础设施的可观察性数据

[0193] (日志、度量、事件)的复制。

[0194] 如前所述,适配器池712C包括多个适配器,每个适配器负责向第二云基础设施的用户暴露第一云基础设施的一组唯一底层资源,即,每个适配器映射到由第一云环境供应的特定产品或资源。例如,Exa数据库适配器充当第二云基础设施用户创建和利用Exa数据库资源的代理。Exa数据库是硬件和软件的预配置组合,其提供用于执行数据库的基础设施。根据一些实施例,Exa数据库包括一组资源:(a)Exadata基础设施(即,硬件)、(b)VM云集群、(c)容器数据库和(d)可插拔数据库。根据一些实施例,多云基础设施提供了(对于第二云基础设施的用户)分析堆叠的基础设施的每个级别的能力。而且,MCCP为用户提供了灵活性,用户只需发出针对工作流的创建命令(经由多云控制台750),之后MCCP会在堆栈的每个级别自动创建各个资源。应该认识到的是,虽然图7中所描绘的适配器池712C包括五个不同的适配器,但这绝不限制MCCP体系架构700的范围。MCCP体系架构可以包括其他适配器,例如,基于云服务提供商的要求,专门供特定云服务提供商使用的专用适配器。

[0195] 在操作中,当用户705访问多云控制台750(例如,第一次)以执行登记操作(例如,

针对多云服务)时,用户705被重定向到供给模块722(包括在第二云环境720中)。用户可以针对第二云环境,即,使用与第二云环境相关联的凭证执行登录操作。在成功登录到第二云环境中后,供给模块722执行第二云环境中客户账户中资源的先决条件设置。注意的是,第二云环境中先决条件资源的供给可以包括创建角色(和相关联策略)以及针对身份系统723设置用户池。

[0196] 供给处理允许例如第二云环境中的多云服务账户访问第二云环境的客户账户中的资源。这样做时,第一云环境710中的资源可以针对第二云环境执行某些动作。例如,可观察性适配器/模块(包括在适配器池712C中)可以将与第一云环境中部署的资源相关联的度量传输到第二云环境的监视模块。作为供给处理的另一个示例,网络适配器(包括在适配器池712C中)可以将中转网关附接到第二云环境中的客户VPC,即,在第二云环境中形成对等。

[0197] 根据本公开的一些实施例,第二云环境720的身份系统723包括允许用户或服务临时承担不同角色的权限的特征(本文称为“承担角色”)。这样的特征使得能够在同一账户内或外进行跨账户访问或权限委托。当用户或服务承担角色时,他们会接收到一组临时安全凭证,其可以包括访问密钥、秘密访问密钥和会话令牌。然后,这些凭证可以用于基于授予承担角色的权限进行API调用或访问(第二云环境的)资源。因此,作为供给处理的一部分,多云服务账户可以被配置为承担某些角色,多云服务账户可以利用这些角色获得对第二云环境中的客户账户的访问。

[0198] 当用户成功登录到第二云环境720中并完成上述供给处理后,可以向用户发出访问令牌。然后将该令牌转发到多云控制台750,多云控制台750又将令牌转发到MCCP 712。MCCP 712中包含的代理模块712A执行如上所述的用户认证,并在用户成功获得授权(例如,检查用户是否具有足够的特权来发出特定类型的请求)后,将请求转发到适配器池712C中包含的适当适配器以执行用户的请求。

[0199] 在向其他云环境(例如,第二云环境720)的客户提供云环境(例如,第一云环境710)的服务时,需要使其他云环境(即,第二云环境)的用户能够以对(一个或多个)用户透明的方式从其各自的云环境访问/控制(部署在第一云环境中的)资源的框架(即,多云基础设施框架)。多云基础设施的一个重要方面是设计身份框架,该身份框架被配置为验证其他云环境的用户是否具有足够的特权/权限来向第一云环境发出访问/修改所部署的资源的请求。

[0200] 在多云设置中实现身份管理框架的一种简单途径是依赖外部云(例如,第二云环境)的身份管理工具来执行用户验证。例如,如果第二云环境是AWS,那么可以使用其身份管理工具(即,Cognito)进行身份管理。这种途径的缺点是,像Cognito这样的服务需要特殊设置并且耗时。而且,依赖特定服务提供商的身份管理系统(例如,AWS的Cognito)会带来兼容性问题,并且因此可能不会被广泛使用和接受。因此,本文描述了一种统一的身份管理框架,该框架使任何外部云环境的用户在经过验证后都能够访问(第一云环境的)资源。

[0201] 图8描绘了多云体系架构800,其图示了根据一些实施例的身份框架。图8描绘了两个云环境之间的交互,例如,(由第一云服务提供商提供的)第一云环境810和(由第二云服务提供商提供的)第二云环境860。第一云环境810包括几个组件,诸如门户811(例如,用于第一云环境的登录门户)、客户租赁813、服务平台815、多云控制平面820、数据库821和下游服务830。客户租赁813包括身份模块813A和(例如,与用户相关联的)一个或多个策略813B。

[0202] 第二云环境860包括客户账户861、多云账户(本文也称为多云服务账户)863和第二云环境的一个或多个API 864。如下面将描述的,图8的体系架构800为第二云环境860的用户供给部署和利用第一云环境810中的资源。在一些实施方式中,可以经由多云控制台850做出发布此类资源的部署的请求。例如,请求可以被定向到多云控制台的GUI,该GUI提供一个或多个服务(例如,exa数据库服务、MySQL服务、自主数据库服务、虚拟数据库服务等)的列表。下面描述了一种身份框架,该身份框架被实现为允许(第二云环境的)授权用户利用第一云环境的服务。该身份框架使用身份联合作为用户的多云认证的工具。

[0203] 根据一些实施例,在多云基础设施环境800中管理用户身份的步骤如下:(1)在步骤1中,用户801执行登录操作进入第一云环境中。注意的是,可以使用与第一云环境相关联的用户的凭证来执行登录操作。注意的是,登录操作可以经由门户811执行,例如,登录用户界面门户(SOUP),也称为第一云环境的登录门户。请求从SOUP转发到第一云环境813A的身份管理系统(即,身份模块),以对用户进行认证。身份管理系统的示例可以是身份云服务(IDCS)。

[0204] 在成功认证后,用户可以被重定向到第二云环境。具体而言,用户可以被定向到第二云环境的身份提供商。在步骤1.1中,用户可以使用与第二云环境相关联的用户凭证针对第二云环境执行登录操作。在成功登录后,在步骤1.2中,可以将来自第二云环境860的用户身份(例如,用户组、组的策略、角色等)联合,即,迁移到第一云环境。根据一些实施例,经由使用与第一云环境的身份系统相关联的连接器框架来促进联合处理。后面将参考图10和11描述联合处理和连接器框架的使用的细节。

[0205] 在用户801成功登录第一云环境810后,在步骤2中,向用户提供访问令牌,例如,用户主体会话令牌(UPST),并将其重定向到多云控制台850。注意的是,UPST是由身份模块813A响应于成功认证用户的凭证(例如,登录信息)而生成的。使用多云控制台850,用户801可以发出请求,诸如在第一云环境810中部署一个或多个资源(例如,exa数据库资源、自主数据库资源等)。多云控制台850触发对服务平台(SPLAT)的API调用(包括UPST),如步骤3中所示。SPLAT被配置为授权UPST(在步骤4中),即,确定用户是否有资格(即,具有足够的特权/权限)向多云控制台850发出调用、核实角色、与令牌相关联的权限等。根据一些实施例,可以针对从第二云环境860联合并存储在第一云环境810中的客户租赁(即,策略813B)中的用户角色、策略和其他信息来执行用户的授权。在成功核实UPST(即,用户被成功核实)后,请求被转发到多云控制平面820。

[0206] 根据一些实施例,并且如先前关于图7所述,多云控制平面820的一个方面是在第一云环境和第二云环境之间建立网络链路(例如,在两个云环境中的客户账户之间建立网络/通信链路)。为了这样做,多云控制平面820需要访问第二云环境中的(一个或多个)客户账户。在一些实施方式中,这经由多云账户863(即,部署在第二云环境中并属于第一云环境的云服务提供商的多云服务账户)来实现。

[0207] 应该认识到的是,多云控制平面820获得对第二云环境860中不同客户账户的访问的一种简单方式是各个客户可以向多云控制平面820提供API密钥。在这种设置中,多云控制平面820将承担存储多个密钥——每个密钥与第二云环境中的每个客户账户对应——的任务,以获得对第二云环境中相应客户账户的访问。显然,这样的框架不可扩展,并且会给多云控制平面820带来计算负担。因此,为了避免这种情况,根据本公开的一些实施例,多云

控制平面820经由先前部署在第二云环境860中的多云服务账户863获得对第二云环境860中不同客户账户的访问。可以经由存储在第一云环境810中的数据库821中的单个会话令牌获得对第二云环境860中的不同客户账户的这种访问。

[0208] 多云控制平面820从数据库获得会话令牌(例如,秘密密钥)以访问第二云环境860中的多云服务账户863(步骤5)。多云服务账户863又与第二云环境中的不同客户账户耦合以建立网络链路。注意的是,作为耦合的一部分,多云服务账户还获得对第二云环境的(一个或多个)客户账户中执行的计算实例的访问。而且,可以在多云服务账户863中提供用户角色的副本(步骤6)。注意的是,多云控制平面820也可以利用会话令牌访问第二云环境的一个或多个API,例如,访问第二云环境的一个或多个API以执行先决条件资源供给(后面参考图12进行描述)。此外,步骤8中的多云控制平面将UPST交换/转换成代表令牌(OBO),以向第一云环境的原生服务(即,下游服务)发出下游调用。

[0209] 应该认识到的是,为了使多云服务账户863能够获得对第二云环境中的各个客户账户的访问,必须在第二云环境中执行资源的先决条件供给。例如,如前面参考图7所述,使用供给模块722,开发人员可以使用基础设施即代码模板定义和供给基础设施资源。换句话说,供给模块722使第二云环境720中的客户账户中的资源的先决条件设置自动化。供给模块722还可以被配置为设置先决条件资源,允许第一云环境的组件(即,多云服务账户)获得对第二云环境中的客户账户中的资源的访问。后面将参考图12详细描述先决条件资源供给。而且,在上述图8的体系架构中,用户可以实现软件开发包(SDK)840来以编程方式执行上述功能。

[0210] 图9描绘了示例性流程图900,其图示了根据一些实施例的与用户登记处理对应的步骤。图9中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、核心)执行的软件(例如,代码、指令、程序)中、使用硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图9中呈现的和下面描述的方法旨在是说明性和非限制性的。虽然图9描绘了以特定顺序或次序发生的各种处理步骤,但这并不是旨在限制。在某些替代实施例中,处理可以按照某种不同的次序执行,或者一些步骤也可以并行执行。

[0211] 该处理开始于步骤901,其中用户(例如,经由浏览器)导航到多云控制台。例如,用户导航到多云控制台的登记API/GUI以登记由第一云环境提供的多云服务。多云控制台的这种界面在本文被称为登记GUI。在步骤903中,用户输入租赁名称(例如,第一云环境中的租赁的标识符)或选择登记第一云环境中的租赁。

[0212] 响应于用户选择登记第一云环境中的租赁,处理移动到步骤904,其中用户被定向到第一云环境的登记页面。此后,在登记第一云环境中的租赁后,处理循环回到步骤903。响应于用户在步骤903中输入租赁名称,处理移动到步骤905,其中用户输入其凭证(例如,登录用户名、密码等)以执行登录操作。步骤907中的处理执行查询以确定是否存在网络链路(即,第二云环境中的客户账户与第一云环境中的客户租赁之间的通信链路)。在一些实施方式中,可以通过查询链路资源对象来做出这样的确定,链路资源对象包括将用户在第一云环境中的租赁链接到用户在第二云环境中的账户的信息。这样的链路资源对象还可以包括指示相应云环境之间是否配置了网络链路的信息(例如,状况标志)。如果对查询的响应是肯定的,那么处理移动到步骤923,否则响应于查询是否定的,那么处理移动到步骤908。

[0213] 如果多云链路(即,网络链路)不存在,那么步骤908中的处理将用户重定向到第二

云环境(例如,将用户重定向到与第二云环境相关联的GUI)。具体而言,用户被重定向以使用与第二云环境相关联的凭证执行登录操作。这样的GUI可以与和第二云环境的门户相关联的登录GUI对应。在成功登录后,步骤909中的处理开始验证处理。具体而言,该处理尝试验证要在第二云环境中配置的一组先决条件资源。注意的是,该组先决条件资源是建立两个云环境之间的网络链路所必需的。

[0214] 根据一些实施例,包含在第二云环境的客户账户中的供给模块(图7中标记为722的框)可以触发先决条件资源的供给处理。例如,供给模块触发访问控制模块(图7中标记为723B的框)以开始为用户供给先决条件资源。供给包括为第二云环境的一个或多个用户创建一组一个或多个角色(以及与相应角色对应的相关联策略、权限等)。在一些实施方式中,访问控制模块充当第二云环境的用户目录。具体而言,访问控制模块可以被配置为创建用户池,并执行诸如添加用户登记、登录和对web和移动应用的访问控制之类的功能。

[0215] 在一些实施方式中,供给模块被配置为创建资源的层次结构(即,一组先决条件资源),每个资源与对应的角色相关联,例如,联网角色、可观察性角色和验证者角色。应该认识到的是,联网角色允许创建网络链路,即,将第一云环境和第二云环境的资源互连的通信路径,而可观察性角色供给可观察性模块(即,MCCP中包括的可观察性适配器)以发布与部署在第一云环境中的一个或多个资源相关联的、要传输到第二云环境的监视模块的度量。在一些实施例中,供给模块还可以被配置为设置先决条件资源,允许第一云环境的组件获得对第二云环境中的客户账户中的资源的访问。根据一些实施例,这通过允许多云服务账户(图7中标记为726A的框)访问客户账户中的资源来实现,例如,允许多云服务账户与客户账户对等、允许多云基础设施的组件(例如,可观察性适配器在第二云环境中发布度量等)。后面将参考图12描述关于先决条件资源供给的更多细节。

[0216] 步骤911中的处理执行查询以确定先决条件资源是否已正确配置和验证。如果对查询的响应是肯定的,那么处理移动到步骤917,否则处理移动到步骤913。在步骤913中,即,如果尚未配置先决条件资源,那么激活第二云环境的客户账户中的供给模块以开始如上所述的先决条件资源的供给处理。这样的处理包括用户在第二云环境中执行登录操作以执行先决条件资源供给处理(步骤915)。在成功执行先决条件资源供给处理后,处理循环回到步骤911。

[0217] 在验证先决条件资源后,步骤917中的处理检查哪些地理区域可用(对于第一云环境和第二云环境两者),使得可以建立网络链路。例如,可以执行检查以确定为第一云环境和第二云环境选择的区域是否位于同一位置(即,在地理位置上彼此靠近),使得可以在两个云环境之间建立网络链路。

[0218] 在步骤919中,(从步骤917中获得的可用区域中)为两个云环境选择主区域。例如,从第一云环境的可用区域中为第一云环境选择第一主区域,并且从第二云环境的可用区域中为第二云环境选择第二主区域。在为两个云环境选择主区域后,步骤921中的处理在两个云环境之间建立网络链路。

[0219] 在一些实施方式中,在步骤921中,可以发起执行几个功能的工作流。例如,工作流可以包括以下步骤:(i)触发网络适配器(包括在图7的MCCP中)来配置互连(图7中标记为719的链路)以通信地耦合两个云环境,以及(ii)在第一云环境中的用户租赁中创建隔间,使得所请求的资源可以部署在其中等。应该认识到的是,互连的配置可以包括将互连(在一

端)与第二云环境中的直接连接(位于多云服务账户726A中)耦合,并将互连(在另一端)与第一云环境中包括的快速连接耦合。

[0220] 步骤923中的处理确定多云链路的状况。例如,该处理确定网络链路是否已启动并正常运行。在步骤925中执行查询以确定网络链路是否准备就绪。如果对查询的响应是肯定的,那么处理移动到步骤927,其中用户被定向到多云控制台,例如,到多云控制台的API,该API描述可供用户在第一云环境中的租赁中部署的各种资源(即,提供这些资源的列表)。如果对步骤925中的查询的响应是否定的,那么处理循环回到步骤923,其中重新检查网络链路的状况。

[0221] 如前所述,在向其他云环境(例如,第二云环境)的客户提供第一云环境的服务时,需要使其他云环境的用户能够以对(一个或多个)用户透明的方式从其相应的云环境访问/控制(部署在第一云环境中的)资源的框架(即,多云基础设施框架)。图8描绘了这样的多云基础设施框架,其包括了统一身份管理框架,该框架使任何外部云环境的用户都能够在成功验证后都访问部署在第一云环境中的资源。验证处理的重要方面是联合一个云环境(例如,第二云环境)中的用户凭证,以在另一个云环境(例如,第一云环境)中自动复制/同步(参见图8中的步骤1.2)。

[0222] 下面描述的是处理,即,联合机制,该机制在第二云环境中实例化多云服务账户(例如,图7中标记为726A的框)以在两个云环境之间建立信任,此后使用户凭证能够从第二云环境同步到第一云环境。应该认识到的是,身份联合是将个人或实体的认证责任委托给可信外部方的处理。联合处理中的每一方都起到身份提供商(IdP)或服务提供商(SP)的角色。在身份联合中,IdP为用户的身份提供担保,并且SP为用户提供服务。当用户想要访问SP的服务时,SP将认证委托给IdP。注意的是,为了进行身份联合,SP必须信任IdP的认证能力。下面参考图10描述了多云基础设施在执行身份联合时采用的独特框架。

[0223] 现在转到图10,描绘了图示根据一些实施例的第一云环境的身份连接器框架的框图1000。具体而言,图10描绘了第一云环境的身份系统1010和第二云环境的身份系统1030,它们彼此通信地耦合。第一云环境的身份系统1010包括身份管理服务1011、身份连接器框架1013和连接器1015。

[0224] 根据本公开的一些实施例,通过使用身份连接器框架(ICF)来实现联合,该框架在调用应用(例如,身份管理服务1011)和访问目标资源(例如,第二云环境1030的身份系统中的用户凭证)的连接器模块/束之间提供一致的通用层。每个目标资源本身可以是系统或应用,但是连接器束使得任何调用应用能够管理目标资源上存在的对象。因此,连接器1015是第一云环境的身份系统中使用的集成工具。连接器建立在ICF框架1013上,并且在设计上是无状态的,即,连接器不存储任何信息。调用应用(例如,身份管理服务1011)向连接器1015供应用于其配置的一组值,包括连接到目标应用所需的信息。这是因为,身份连接器是无状态的,并且在这样做时,每个连接器束实现都与调用应用的实现解耦合。换句话说,连接器是使得从一个身份系统(例如,第二云环境)能够联合到另一个身份系统(例如,第一云环境)的组件。

[0225] 应该认识到的是,联合处理使得针对第二云环境中的用户身份执行的任何更改(例如,用户添加、从某些用户组中移除用户成员关系等)能够无缝地反映在第一云环境的身份系统中。本公开中的联合处理是经由连接器1015实现的,该连接器与多云服务账户中

的端点(即,由第一云环境的第一云服务提供商拥有并部署在第二云环境中的账户)通信以从第二云环境中检索信息(例如,用户身份信息)。

[0226] 图11描绘了图示了根据一些实施例的与执行身份联合的处理对应的步骤的示例性游泳图。具体而言,图11描绘了将第二云环境1130中的(一个或多个)用户的身份联合到第一云环境1110时执行的步骤。图11描绘了第一云环境1101的身份服务、第一云环境的多云平台1102、第一云环境的数据库(秘密存储库)1103、多云账户(即,第二云环境中包括的多云服务账户1105)、包括客户账户1106的客户VPC和第二云环境的身份服务1107之间的交互。

[0227] 根据一些实施例,第一云环境1101的身份服务(或替代地连接器模块)与第二云环境中的端点通信,以从第二云环境中的客户账户中检索客户凭证。应该认识到的是,由于信任和策略问题,第一云环境的身份服务将无法直接访问第二云环境中的客户账户。由此,连接器与之通信的端点是多云服务账户,该账户由第一云环境的提供商拥有并位于第二云环境中。注意的是,在用户登记时执行的先决条件资源供给处理(接下来参考图12描述)期间,多云服务账户被授予对第二云环境中的客户账户的访问。换句话说,在多云服务账户和第二云环境中的客户账户之间建立了信任。

[0228] 此外,根据本公开的一些实施例,第二云环境720的身份系统723包括允许用户或服务临时承担不同角色的权限的特征(本文称为“承担角色”)。这样的特征使得能够在同一账户内或外进行跨账户访问或权限委托。当用户或服务承担角色时,他们会接收到一组临时安全凭证,其中可以包括访问密钥、秘密访问密钥和会话令牌。然后,这些凭证可以用于基于授予承担角色的权限进行API调用或访问(第二云环境的)资源。因此,作为供给处理的一部分,多云服务账户可以被配置为承担某些角色,多云服务账户可以用这些角色获得对第二云环境中的客户账户的访问。

[0229] 所图11中描绘的处理开始于步骤1,其中第一云环境1101的身份服务向多云平台1102传输检索与部署在第二云环境中的多云账户1105相关联的凭证的请求。在步骤2中,多云平台1102尝试从第一云环境中包括的数据库1103中检索所述凭证。在步骤3中多云平台1102获得凭证。在检索到凭证后,在步骤4中,多云平台1102尝试承担与多云服务账户相关的角色,即,多云平台1102被指派允许其访问多云服务账户1105的角色。在用户登记时,如果正确执行了先决条件资源的配置,那么多云平台1102获得与多云服务账户相关联的凭证(例如,第一凭证)(步骤5)。

[0230] 在成功获取对多云服务账户的访问后,在步骤6中多云平台1102尝试承担与第二云环境1130中的客户账户1106相关的角色(基于在步骤5中获得的凭证)。注意的是,这是可能的,因为在设置期间,多云服务账户1105被授予访问第二云环境中的客户账户的权限。在步骤7中,多云平台1102获得与客户账户相关联的凭证(例如,第二凭证)。在步骤8中,执行角色更改处理,其中多云平台1102获得的与第二云环境中的客户账户1106相关联的凭证被传递/传输到第一云环境1101的身份服务模块。在获得第二凭证后,第一云环境的身份服务模块与第二云环境的身份服务1107通信地耦合(步骤9)。在步骤10中,在获得第二凭证后,第一云环境的身份服务1101可以向第二云环境的身份服务发出调用/请求,以便同步用户身份,即,用户组、权限、角色等。以这种方式,用户身份从第二云环境联合到第一云环境。注意的是,上述身份联合处理可以在固定时间实例上连续执行,使得在第二云环境中执行的

用户身份的任何更改都可以无缝迁移到第一云环境。

[0231] 现在转到图12,其中描绘了图示根据一些实施例的与先决条件资源验证处理对应的步骤的示例性游泳图。具体而言,图12描绘了确定第二云环境中是否已配置一组资源时执行的步骤,该组资源促进第二云环境的用户利用与第二云环境不同的第一云环境供应的多云服务。图12描绘了用户1201、第二云环境的供给模块1202、第二云环境的身份管理模块1203、第一云环境中包括的多云控制台(登记)1205、第一云环境中包括的多云基础设施的多云控制平面(MCCP)1206、多云数据库1207和多云服务账户1208之间的交互。应该认识到的是,多云控制台1205以及MCCP 1206可以被视为包含在第一云环境中的多云基础设施的组件。

[0232] 该处理开始于步骤S1,其中用户1201向多云注册控制台1205(例如,多云控制台的登记API)提供凭证(例如,与第二云环境相关联的账户ID)。多云控制台1205在接收到凭证后,向MCCP 1206传输确定是否已为该用户配置一组先决条件资源的请求(步骤S2)。

[0233] 响应于接收到开始验证一组先决条件资源的请求,在步骤S3A中,MCCP 1206从数据库1207中获得与服务账户(即,在第二云环境中实例化并属于第一云环境的多云服务账户)相关联的凭证。在步骤S3B中,MCCP 1206获得与服务账户相关联的凭证。此外,在步骤S4A中,基于在步骤S3B中获得的凭证,MCCP 1206访问服务账户1208。本质上,MCCP 1206承担代理角色,即,代表客户行事,并访问服务账户。在步骤S4B中,MCCP 1206获得服务账户的临时访问凭证。

[0234] 在步骤S5中,MCCP 1206继续承担验证者角色,即,允许MCCP 1206执行用户验证的角色。在一些实施方式中,与MCCP 1206相关联的API承担验证者角色来执行用户的验证。在一种情况下,如果这是用户1201第一次访问多云控制台1205(例如,为了登记由多云基础设施提供的服务),那么尚未执行一组先决条件资源的供给。因此,在步骤S6中,第二云环境的身份系统(其包括IAM模块1204)向MCCP 1206传输通知,指示验证者角色不存在。在步骤S7中,MCCP 1206可以存储元数据信息,包括用户在第一云环境中的租赁标识符和用户在第二云环境中的账户。

[0235] MCCP 1206向多云控制台1205传输通知(步骤S8),通知资源的先决条件设置不完整或无效。进而,在步骤S9中,多云控制台1205向用户提供通知(例如,经由与多云控制台相关联的API)以开始或启动先决条件资源的供给处理。在步骤S10中,用户1201与第二云环境的客户账户中包括的供给模块1202进行通信以触发供给处理。

[0236] 在步骤S11中,供给模块1202触发IAM模块1203以开始为用户供给先决条件资源。例如,如前面参考图7所述,供给包括为第二云环境的一个或多个用户创建一组一个或多个角色(以及与相应角色对应的相关联策略、权限等)。在一些实施方式中,访问控制模块(包括在第二云环境的身份系统中)充当第二云环境的用户目录。具体而言,访问控制模块可以被配置为创建用户池,并执行诸如添加用户登记、登录和对web和移动应用的访问控制之类的功能。在一些实施方式中,供给模块1202被配置为创建资源的层次结构,每个资源与对应的角色相关联,例如,联网角色、可观察性角色和验证者角色。

[0237] 应该认识到的是,当在第二云环境中执行供给先决条件资源的处理时,第一云环境的多云控制台1205可以同时与MCCP 1206通信以确定是否已配置资源的先决条件验证(步骤S2'、S5'、S6'和S8',各自分别与步骤S2、S5、S6和S8对应)。由于先决条件资源的供给

正在同时发生(即,尚未完成),因此在步骤S6'中,第二云环境的IAM模块1204向MCCP 1206传输通知,指示尚未创建角色。

[0238] 在步骤S12中,多云控制台1205向MCCP 1206传输另一个请求,以确定是否已为该用户配置了一组先决条件资源。MCCP 1206重新尝试承担验证者角色(步骤S13)。这一次,由于已创建角色(即,完成先决条件资源的供给),因此MCCP 1206从第二云环境的IAM模块1204接收通知,通知验证者角色存在。具体而言,在步骤S14中,IAM模块1204向MCCP 1206提供多云服务账户(例如,部署在第二云环境中并由第一云环境的第一CSP控制)的临时凭证。

[0239] 在步骤S15中,MCCP 1206验证角色的层次结构中的其他角色。例如,MCCP 1206核实是否已创建联网角色和可观察性角色。在步骤S16中,MCCP 1206接收到角色创建成功的确认。在步骤S17中,MCCP 1206向多云控制台1205传输通知,指示先决条件资源的配置完成。在步骤S18中,多云控制台1205进而可以向用户通知先决条件资源的成功配置。

[0240] 此外,在步骤S19中,在用户被成功定向到多云控制台1205后,可以激活MCCP中包含的云链路适配器,以向用户1201提供将第二云环境中的客户账户与第一云环境中的客户账户链接的选项。换句话说,云链路适配器执行链接客户在两个不同云环境中的两个账户的处理,如下面参考图14所述。注意的是,在链接不同云环境中的两个账户后,第二云环境的(一个或多个)用户可以利用由第一云环境中包括的多云基础设施提供的(一个或多个)服务。应该认识到的是,在用户向多云基础设施登记后,MCCP 1206还被配置为创建将第一云环境与第二云环境通信地耦合的网络链路。

[0241] 根据一些实施例,多云基础设施的一个方面是在第二云环境中实例化多云账户(也称为多云服务账户),该账户由第一云环境的服务提供商控制并且已预先配置有足够的特权以与第二云环境中的不同客户账户进行通信。在这样的设置中,可能存在一些安全考虑,其中多云服务账户可能被胁迫(例如,被恶意第三方)来不正当地获取对第二云环境中的特定客户账户的访问。这样的安全问题在本文被称为"混淆代理问题",即,多云服务账户与混淆代理对应。下面描述了由多云控制平面实现的解决混淆代理问题的安全解决方案。

[0242] 如前所述,在第二云环境中,提供了称为跨账户访问服务的服务,即,特定账户被允许承担第二云环境的另一个账户中的角色。在多云环境设置中,多云服务账户(部署在第二云环境中)可以利用这种跨账户服务。由于这种跨账户访问服务而产生的安全考虑是混淆代理问题,即,多云服务账户可能(在恶意第三方的胁迫下)试图承担特定客户账户中的角色以获取对客户信息的欺诈性访问。本文描述了防止多云服务账户进行此类欺诈性访问的技术。具体而言,本文提出的技术涉及:(a)利用可以由多云平台和/或多云控制台生成的外部ID(对于每个客户唯一),以及(b)生成和存储外部ID的机制。

[0243] 图13描绘了图示根据一些实施例的为解决混淆代理问题而执行的步骤的示例性游泳图。具体而言,图13描绘了图示多云登记控制台1301、供给模块1302(包括在第二云环境中)、MCCP登记API 1303、云链路适配器的API 1304、适配器1305(包含在适配器池中)、MCCP平台1306和第二云环境中的客户账户1307之间的交互的步骤。图13中描绘的游泳图包括由多云平台(MCP)为每个客户生成唯一ID(本文称为外部ID)。客户的外部ID最初存储在平台上(例如,在用户登记处理期间存储在第一云环境中包含的键值数据库中),并且是短暂的。当形成云链路(即,第一云环境中的客户账户与第二云环境中的客户账户之间的映射)后,外部ID最终存储在第二云环境中的相应客户账户(例如,客户保险库)中。应该认识

到的是,外部ID可以存储在客户保险库中或链路资源对象(即,云链路对象)中,此后出于安全考虑,可以从第一云环境中包含的键值数据库中删除外部ID。

[0244] 图13中的处理开始于步骤S1,其中多云控制台1301向MCP登记API 1303传输请求(即,验证先决条件请求)。这种请求可以包括客户(在第二云环境中)的账户ID。在步骤S2中,MCCP登记API 1303尝试从MCCP平台1306获得客户的凭证。由于尚未建立客户的账户,因此可以将"无权访问"消息传输回MCCP登记API 1303,然后可以将其中继到多云控制台1301(步骤S3)。

[0245] 在步骤S4中,多云控制台1301向MCCP平台1306传输获得客户的外部ID的请求。在步骤S5中,MCCP平台1306为客户生成外部ID,即,唯一ID,并将生成的ID存储在数据库(例如,键值数据库)中。在步骤S6中,MCCP平台1306将外部ID提供给多云控制台1301。在步骤S7中,多云控制台1301向供给模块1302发出请求以开始供给先决条件资源的处理。供给处理可以包括供给模块1302触发访问控制模块(例如,图8中标记为803的框)以开始为用户供给先决条件资源。例如,如前面参考图7所述,供给包括为第二云环境的一个或多个用户创建一组一个或多个角色(以及与相应角色对应的相关联策略、权限等)。

[0246] 访问控制模块可以被配置为创建用户池,并执行诸如添加用户登记、登录和对web和移动应用的访问控制之类的功能。在一些实施方式中,供给模块1303被配置为创建资源的层次结构(本文称为一组先决条件资源),每个资源都与对应的角色相关联,例如,联网角色、可观察性角色和验证者角色。应该认识到的是,联网角色允许创建网络链路,即,将第一云环境和第二云环境的资源互连的通信路径,而可观察性角色供给(MCCP的)可观察性模块以发布与部署在第一云环境中的一个或多个资源相关联的、要传输到第二云环境的监视模块的度量。验证者角色允许多云基础设施的控制平面执行用户验证。注意的是,步骤S7的资源先决条件供给与与图12的步骤S10对应的资源先决条件供给对应。但是,步骤S7的资源先决条件供给中的附加要求是利用生成的外部ID作为客户的先决条件验证处理中的参数。

[0247] 应该认识到的是,当在第二云环境中执行供给先决条件资源的处理时,第一云环境的多云控制台1301可以同时与MCCP登记API 1303通信以确定是否已配置资源的先决条件验证(步骤S8)。由于先决条件资源的供给正在同时发生(即,尚未完成),因此在步骤S9中,MCCP登记API 1303向多云控制台1301传输通知,指示尚未创建角色。

[0248] 此外,在步骤S10中,在第一云环境的多云控制台1301与MCCP登记API 1303通信以确定是否已配置资源的先决条件验证后。如果第二云环境的供给模块已完成先决条件验证,那么在步骤S11中,MCCP登记API 1303传输从MCCP平台1306获得凭证的请求。MCCP平台1306进而在步骤S12中提取在步骤S5中存储在键值数据库中的外部ID。基于提取的外部ID,在步骤S13中MCCP平台1306承担与第二云环境1307中的客户账户相关的角色,并在步骤S14中提取会话密钥。在步骤S15中,MCCP登记API 1303利用会话密钥获得角色、用户组和其他资源的列表(步骤S16),此后MCCP登记API 1303可以通知多云控制台1301验证处理完成(步骤S17)。

[0249] 直到这个步骤(即,步骤S17),注意的是,客户的外部ID存储在MCCP平台本地(例如,在键值数据库中)。此外,在发起云链接处理(即,将客户(在第一云环境中)的账户映射到客户在第二云环境中的账户的处理)后,可以从MCCP平台中删除外部ID并将其存储在客户的保险库中,即,在客户账户的隔间中(例如,在第二云环境中)。外部ID可以短期(例如,

一周)存储在平台上,此后可以长期存储在客户的保险库中。应该认识到的是,步骤S1-S17与验证处理对应,而步骤S19-S22与资源供给处理对应。

[0250] 在步骤S18中,多云控制台触发请求,该请求将被传输到云链路适配器1304的API以开始云链接处理。图14描绘了这种映射的图形表示。具体而言,转到图14,其中描绘了示出根据一些实施例的云链路资源对象的示意图。云链路资源对象将用户在第二云基础设施中的账户的信息映射到用户在第一云基础设施中的租赁。如图14中所示,第二云环境1410包括客户的账户1401,包括一些账户元数据1402。账户元数据可以包括诸如用户组的标识符等信息。第一云环境1405包括客户租赁1411,该客户租赁1411包括云链路资源对象1430。云链路资源对象1430包括几个参数,诸如客户在第一云环境中的租赁ID 1430A、镜像账户元数据1402信息的用户池ID 1430B、与第二云环境的身份管理系统的标识符对应的客户端ID 1430C、包括指向为客户实例化的隔间1440的指针的基隔间ID、以及包括客户在第二云环境中的账户的标识符并包括指向第一云环境中为客户实例化的隔间1440A的指针的账户ID 1430D。应该认识到的是,客户的资源被部署在第一云环境中为客户实例化的隔间中。

[0251] 返回图13,在完成云链接处理后,在资源供给阶段,适配器1305(例如,来自MCCP中包括的适配器池)传输从MCCP平台1306获得(例如,第二云环境中的多云服务账户的)凭证的请求。MCCP平台1306进而可以从第二云环境中的客户账户中提取外部ID,并进一步承担允许MCCP平台代表客户执行操作的角色(步骤S20)。例如,在从第二云环境1307中的客户账户获得会话密钥(步骤S21)后,适配器1305可以利用会话密钥在第一云环境中的客户账户中部署资源(例如,自主数据库)。

[0252] 以这种方式,本公开的多云基础设施通过禁止欺诈性第三方实体获取对客户账户的访问(即,因为他们将无法访问存储在客户保险库中且需要获取对客户账户的访问的外部ID)来解决混淆代理问题。注意的是,上面关于图13描述的特征绝不限制本公开的范围。例如,在替代途径中,为客户生成外部ID(和将生成的外部ID存储在客户保险库中)可以由多云登记控制台执行。

[0253] 图15描绘了图示根据一些实施例的由多云基础设施部署资源的示意图。如图15中所示,第一云环境包括多云控制台1551、服务平台(SPLAT)1552、代理1553、云链路适配器1554、数据库适配器1555和平台1556。当用户访问多云控制台1551时,在一些实施例中,用户可以被定向到第二云环境的身份管理系统1560,以便针对第二云环境执行登录操作。注意的是,在成功登录后,用户连同令牌(例如,访问令牌)一起被重定向回多云控制台1551。应该认识到的是,用户可以利用多云控制台1551发出命令以访问、创建或更新第一云基础设施中用户的租赁中的资源。为了便于说明,下面描述了用户利用多云控制台1551发出创建数据库资源(例如,Exa数据库资源)的请求的场景。

[0254] 多云控制台1551提供多个选项,例如,创建资源、访问资源、更新资源等。这些选项可以以多云控制台1551中的可选图标(例如,按钮)的形式提供给用户。当用户执行选择(例如,以创建资源)时,将触发对服务平台1552的API调用。应该认识到的是,在一些实施方式中,对服务平台1551做出的请求可以是诸如REST类型调用(或POST调用)之类的调用,其包括授权报头,该授权报头包括与第二云基础设施中的用户相关联的令牌。请求中还包括的是元数据信息,包括(第二云环境的)账户ID、资源名称、提供商名称和由用户请求的资源的类型。

[0255] 包括令牌的调用被进一步转发到执行认证和访问控制操作的代理模块1553。根据一些实施例,代理模块1553通过提取调用中包含的令牌来执行认证操作。在一些实施方式中,代理模块1553通过将签名(用于对请求进行签名)与第二云基础设施的公开可用签名进行比较来验证令牌,以确保请求源自与第二云基础设施相关联的有效客户。此外,代理模块1553还可以检查与令牌相关联的角色(即,特权),例如,角色是否与DB管理员对应等。基于角色,代理模块1553可以将请求路由到MCCP框架中包含的适当适配器,即,适配器池712C中包含的适配器之一,如图7中所示。

[0256] 根据一个实施例,代理模块1553将角色(与令牌相关联)与为每个适配器发布和指派(作为API规范的一部分)的预先配置的角色列表进行比较。例如,如果与令牌相关联的角色与“Exadata DB管理员”对应,那么请求可以被理解为创建Exa数据库的请求,并且因此该请求被转发到数据库适配器1555。此外,根据一些实施例,代理模块1553可以分析REST调用中包含的信息,诸如提供商ID、所请求的资源类型等,并且基于所分析的信息,代理模块1553可以将请求转发到适当的适配器。

[0257] 在一些实施方式中,由代理模块1553获得的请求可能不包含识别用户在将要部署资源的第一云基础设施中的租赁的信息。因此,代理模块1553与云链路适配器1554通信以获得第二云基础设施中的用户账户到第一云基础设施中的用户租赁的映射信息。如果映射信息存在,那么代理模块1553获得与第一云基础设施中的用户租赁相关的信息,并将该信息传递给数据库适配器1555。以这种方式,数据库适配器1555知道用户在将要创建/部署资源的第一云基础设施中的租赁。但是,如果云链路适配器1554确定不存在映射信息,那么代理模块1553可以简单地发出传回用户的“未经授权的访问”消息作为对创建数据库资源的请求的响应。

[0258] 注意的是,在一些实施方式中,云链路适配器1554创建数据对象(本文称为云链路资源对象或链路资源对象),用于存储识别所链接的两个账户的元数据信息。例如,数据对象存储元数据信息,包括与第一云基础设施中的租赁(即,账户)相关联的第一标识符和与第二云服务提供商的用户账户相关联的第二标识符的映射。这样的映射在本文称为资源上下文。此外,云链路适配器1554还可以创建与资源上下文相关联的资源主体(本文称为云链路资源主体)。云链路适配器1554可以在第一云基础设施中的用户租赁的根隔间内维护数据对象以及资源主体。在一些实施例中,云链路适配器1554还可以在平台1156中本地持久化数据对象和/或资源主体。

[0259] 在一些实施方式中,数据库适配器1555可以获得在平台1556中本地持久化的资源主体。数据库适配器1555可以向第一云基础设施中包含的一个或多个下游服务传输请求(包括资源主体),以在第一云基础设施中的用户租赁中创建资源。换句话说,第一云基础设施中包含的下游服务利用从平台1556获得的身份(即,资源主体)在第一云基础设施中的用户租赁中创建/部署所需资源,例如,Exa数据库。当用户发出创建Exa数据库的请求时,用户可以间歇性地轮询MCCP以获得请求的状况。当第一云基础设施的下游服务在第一云基础设施中的用户租赁中创建资源时,MCCP可以向用户通知请求成功完成。

[0260] 云基础设施的示例

[0261] 如以上所指出的,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提供商还可以供应各种服务来伴随这些基础设施组件(例如,计费、监视、记载、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。

[0262] 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那个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。

[0263] 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。

[0264] 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,位于管理程序层之下(例如,服务器、存储装置、网络硬件和虚拟化)。因此,客户可以负责处理(OS)、中间件和/或应用部署(例如,在(例如,可以按需启动的)自助服务虚拟机等上)。

[0265] 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。

[0266] 在一些情况下,IaaS供给存在两个不同的挑战。首先,在任何东西运行之前供给一组初始基础设施存在最初的挑战。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。

[0267] 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)。也可以供给其他基础设施元素,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。

[0268] 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,可以利用供给工具供给资源,和/或一旦供给基础设施就可以利用部署工具部署代码。

[0269] 图16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1600。服务运

营商1602可以通信地耦合到可以包括虚拟云网络(VCN)1606和安全主机子网1608的安全主机租赁1604。在一些示例中,服务运营商1602可以使用一个或多个客户端计算设备,其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®或其他通信协议。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)中的任何一种的工作站计算机。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/或能够通过可以访问VCN 1606和/或互联网的网络进行通信的个人消息传递设备。

[0270] VCN 1606可以包括本地对等网关(LPG)1610,其可以经由包含在SSH VCN 1612中的LPG 1610通信地耦合到安全壳(SSH)VCN 1612。SSH VCN 1612可以包括SSH子网1614,并且SSH VCN 1612可以经由包含在控制平面VCN 1616中的LPG 1610通信地耦合到控制平面VCN 1616。此外,SSH VCN 1612可以经由LPG 1610通信地耦合到数据平面VCN 1618。控制平面VCN 1616和数据平面VCN 1618可以包含在可以由IaaS提供商拥有和/或操作的服务租赁1619中。

[0271] 控制平面VCN 1616可以包括充当外围网络(例如,公司内部网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1620。基于DMZ的服务器可以承担有限责任并有助于控制安全性漏洞。此外,DMZ层1620可以包括一个或多个负载平衡器(LB)子网1622、可以包括(一个或多个)应用子网1626的控制平面应用层1624、可以包括(一个或多个)数据库(DB)子网1630(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1628。包含在控制平面DMZ层1620中的(一个或多个)LB子网1622可以通信地耦合到包含在控制平面应用层1624中的(一个或多个)应用子网1626和可以包含在控制平面VCN 1616中的互联网网关1634,并且(一个或多个)应用子网1626可以通信地耦合到包含在控制平面数据层1628中的(一个或多个)DB子网1630以及服务网关1636和网络地址转换(NAT)网关1638。控制平面VCN 1616可以包括服务网关1636和NAT网关1638。

[0272] 控制平面VCN 1616可以包括数据平面镜像应用层1640,其可以包括(一个或多个)应用子网1626。包含在数据平面镜像应用层1640中的(一个或多个)应用子网1626可以包括可以执行计算实例1644的虚拟网络接口控制器(VNIC)1642。计算实例1644可以将数据平面镜像应用层1640的(一个或多个)应用子网1626通信地耦合到可以包含在数据平面应用层1646中的(一个或多个)应用子网1626。

[0273] 数据平面VCN 1618可以包括数据平面应用层1646、数据平面DMZ层1648和数据平面数据层1650。数据平面DMZ层1648可以包括(一个或多个)LB子网1622,其可以通信地耦合到数据平面应用层1646的(一个或多个)应用子网1626和数据平面VCN 1618的互联网网关

1634。(一个或多个)应用子网1626可以通信地耦合到数据平面VCN 1618的服务网关1636和数据平面VCN 1618的NAT网关1638。数据平面数据层1650还可以包括可以通信地耦合到数据平面应用层1646的(一个或多个)应用子网1626的(一个或多个)DB子网1630。

[0274] 控制平面VCN 1616和数据平面VCN 1618的互联网网关1634可以通信地耦合到元数据管理服务1652,元数据管理服务1652可以通信地耦合到公共互联网1654。公共互联网1654可以通信地耦合到控制平面VCN 1616和数据平面VCN 1618的NAT网关1638。控制平面VCN 1616和数据平面VCN 1618的服务网关1636可以通信地耦合到云服务1656。

[0275] 在一些示例中,控制平面VCN 1616或数据平面VCN 1618的服务网关1636可以对云服务1656进行应用编程接口(API)调用,而无需通过公共互联网1654。从服务网关1636到云服务1656的API调用可以是单向的:服务网关1636可以对云服务1656进行API调用,并且云服务1656可以将请求的数据发送到服务网关1636。但是,云服务1656可以不发起对服务网关1636的API调用。

[0276] 在一些示例中,安全主机租赁1604可以直接连接到服务租赁1619,服务租赁1619否则可以被隔离。安全主机子网1608可以通过LPG 1610与SSH子网1614通信,LPG 1610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1608连接到SSH子网1614可以使安全主机子网1608访问服务租赁1619内的其他实体。

[0277] 控制平面VCN 1616可以允许服务租赁1619的用户设置或以其他方式供给期望的资源。在控制平面VCN 1616中供给的期望资源可以在数据平面VCN 1618中部署或以其他方式使用。在一些示例中,控制平面VCN 1616可以与数据平面VCN 1618隔离,并且控制平面VCN 1616的数据平面镜像应用层1640可以经由VNIC 1642与数据平面VCN 1618的数据平面应用层1646通信,VNIC 1642可以包含在数据平面镜像应用层1640和数据平面应用层1646中。

[0278] 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1652的公共互联网1654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1652可以通过互联网网关1634将请求传送到控制平面VCN 1616。请求可以被包含在控制平面DMZ层1620中的(一个或多个)LB子网1622接收。(一个或多个)LB子网1622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1622可以将请求传输到包含在控制平面应用层1624中的(一个或多个)应用子网1626。如果请求被验证并且需要对公共互联网1654的调用,那么对公共互联网1654的调用可以被传输到可以对公共互联网1654进行调用的NAT网关1638。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1630中。

[0279] 在一些示例中,数据平面镜像应用层1640可以促进控制平面VCN 1616和数据平面VCN 1618之间的直接通信。例如,可能期望对包含在数据平面VCN 1618中的资源应用对配置的更改、更新或其他适当的修改。经由VNIC 1642,控制平面VCN 1616可以直接与包含在数据平面VCN 1618中的资源通信,并且从而可以执行对配置的更改、更新或其他适当的修改。

[0280] 在一些实施例中,控制平面VCN 1616和数据平面VCN 1618可以包含在服务租赁1619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 1616或数据平面VCN 1618。替代地,IaaS提供商可以拥有或操作控制平面VCN 1616和数据平面VCN 1618,这两者平面都可以包含在服务租赁1619中。该实施例可以使得能够隔离可能阻止用户或客

户与其他用户或其他客户的资源交互的网络。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威胁预防级别的公共互联网1654进行存储。

[0281] 在其他实施例中,包含在控制平面VCN 1616中的(一个或多个)LB子网1622可以被配置为从服务网关1636接收信号。在这个实施例中,控制平面VCN 1616和数据平面VCN 1618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1654。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1619上,服务租赁1619可能与公共互联网1654隔离。

[0282] 图17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1700。服务运营商1702(例如,图16的服务运营商1602)可以通信地耦合到安全主机租赁1704(例如,图16的安全主机租赁1604),该安全主机租赁1704可以包括虚拟云网络(VCN)1706(例如,图16的VCN 1606)和安全主机子网1708(例如,图16的安全主机子网1608)。VCN 1706可以包括本地对等网关(LPG)1710(例如,图16的LPG 1610),其可以经由包含在SSH VCN 1712中的LPG 1710通信地耦合到安全壳(SSH)VCN 1712(例如,图16的SSH VCN 1612)。SSH VCN 1712可以包括SSH子网1714(例如,图16的SSH子网1614),并且SSH VCN 1712可以经由包含在控制平面VCN 1716中的LPG 1710通信地耦合到控制平面VCN 1716(例如,图16的控制平面VCN 1616)。控制平面VCN 1716可以包含在服务租赁1719(例如,图16的服务租赁1619)中,并且数据平面VCN 1718(例如,图16的数据平面VCN 1618)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1721中。

[0283] 控制平面VCN 1716可以包括可以包含(一个或多个)LB子网1722(例如,图16的(一个或多个)LB子网1622)的控制平面DMZ层1720(例如,图16的控制平面DMZ层1620)、可以包含(一个或多个)应用子网1726(例如,图16的(一个或多个)应用子网1626)的控制平面应用层1724(例如,图16的控制平面应用层1624)、可以包含(一个或多个)数据库(DB)子网1730(例如,类似于图16的(一个或多个)DB子网1630)的控制平面数据层1728(例如,图16的控制平面数据层1628)。包含在控制平面DMZ层1720中的(一个或多个)LB子网1722可以通信地耦合到包含在控制平面应用层1724中的(一个或多个)应用子网1726和可以包含在控制平面VCN 1716中的互联网网关1734(例如,图16的互联网网关1634),并且(一个或多个)应用子网1726可以通信地耦合到包含在控制平面数据层1728中的(一个或多个)DB子网1730以及服务网关1736(例如,图16的服务网关)和网络地址转换(NAT)网关1738(例如,图16的NAT网关1638)。控制平面VCN 1716可以包括服务网关1736和NAT网关1738。

[0284] 控制平面VCN 1716可以包括可以包含(一个或多个)应用子网1726的数据平面镜像应用层1740(例如,图16的数据平面镜像应用层1640)。包含在数据平面镜像应用层1740中的(一个或多个)应用子网1726可以包括可以执行计算实例1744(例如,类似于图16的计算实例1644)的虚拟网络接口控制器(VNIC)1742(例如,1642的VNIC)。计算实例1744可以促进数据平面镜像应用层1740的(一个或多个)应用子网1726和可以包含在数据平面应用层1746(例如,图16的数据平面应用层1646)中的(一个或多个)应用子网1726之间经由包含在数据平面镜像应用层1740中的VNIC 1742和包含在数据平面应用层1746中的VNIC 1742的通信。

[0285] 包含在控制平面VCN 1716中的互联网网关1734可以通信地耦合到元数据管理服务1752(例如,图16的元数据管理服务1652),该元数据管理服务1752可以通信地耦合到公

共互联网1754(例如,图16的公共互联网1654)。公共互联网1754可以通信地耦合到包含在控制平面VCN 1716中的NAT网关1738。包含在控制平面VCN 1716中的服务网关1736可以通信地耦合到云服务1756(例如,图16的云服务1656)。

[0286] 在一些示例中,数据平面VCN 1718可以包含在客户租赁1721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 1716,并且IaaS提供商可以为每个客户设置包含在服务租赁1719中的唯一计算实例1744。每个计算实例1744可以允许包含在服务租赁1719中的控制平面VCN 1716和包含在客户租赁1721中的数据平面VCN 1718之间的通信。计算实例1744可以允许在包含在服务租赁1719中的控制平面VCN 1716中供给的资源被部署或以其他方式在包含在客户租赁1721中的数据平面VCN 1718中使用。

[0287] 在其他示例中,IaaS提供商的客户可以具有存在于客户租赁1721中的数据库。在这个示例中,控制平面VCN 1716可以包括数据平面镜像应用层1740,其可以包括(一个或多个)应用子网1726。数据平面镜像应用层1740可以驻留在数据平面VCN 1718中,但数据平面镜像应用层1740可能不在数据平面VCN 1718中。即,数据平面镜像应用层1740可以访问客户租赁1721,但是数据平面镜像应用层1740可能不存在于数据平面VCN 1718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1740可以被配置为对数据平面VCN 1718进行调用,但可以不被配置为对包含在控制平面VCN 1716中的任何实体进行调用。客户可能期望在数据平面VCN 1718中部署或以其他方式使用在控制平面VCN 1716中供给的资源,并且数据平面镜像应用层1740可以促进客户的期望部署或资源的其他使用。

[0288] 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 1718。在这个实施例中,客户可以确定数据平面VCN 1718可以访问什么,并且客户可以限制从数据平面VCN 1718对公共互联网1754的访问。IaaS提供商可能无法应用过滤器或以其他方式控制数据平面VCN 1718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1721中的数据平面VCN 1718上可以帮助将数据平面VCN 1718与其他客户和公共互联网1754隔离开。

[0289] 在一些实施例中,云服务1756可以由服务网关1736调用以访问公共互联网1754、控制平面VCN 1716或数据平面VCN 1718上可能不存在的服务。云服务1756与控制平面VCN 1716或数据平面VCN 1718之间的连接可以不是实时的或连续的。云服务1756可以存在于由IaaS提供商拥有或操作的不同网络上。云服务1756可以被配置为接收来自服务网关1736的调用并且可以被配置为不接收来自公共互联网1754的调用。一些云服务1756可以与其他云服务1756隔离,并且控制平面VCN 1716可以与可能与控制平面VCN 1716不在同一区域的云服务1756隔离。例如,控制平面VCN 1716可能位于“区域1”,并且云服务“部署16”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 1716中的服务网关1736对部署16进行调用,那么该调用可以被传输到区域1中的部署16。在这个示例中,控制平面VCN 1716或区域1中的部署16可能不与区域2中的部署16通信地耦合或以其他方式通信。

[0290] 图18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1800。服务运营商1802(例如,图16的服务运营商1602)可以通信地耦合到安全主机租赁1804(例如,图16的安全主机租赁1604),该安全主机租赁1804可以包括虚拟云网络(VCN)1806(例如,图16的VCN 1606)和安全主机子网1808(例如,图16的安全主机子网1608)。VCN 1806可以包括LPG 1810(例如,图16的LPG 1610),其可以经由包含在SSH VCN 1812中的LPG 1810

通信地耦合到SSH VCN 1812(例如,图16的SSH VCN 1612)。SSH VCN 1812可以包括SSH子网1814(例如,图16的SSH子网1614),并且SSH VCN 1812可以经由包含在控制平面VCN 1816中的LPG 1810通信地耦合到控制平面VCN 1816(例如,图16的控制平面VCN 1616)并且经由包含在数据平面VCN 1818中的LPG 1810耦合到数据平面VCN 1818(例如,图16的数据平面1618)。控制平面VCN 1816和数据平面VCN 1818可以包含在服务租赁1819(例如,图16的服务租赁1619)中。

[0291] 控制平面VCN 1816可以包括可以包含(一个或多个)负载平衡器(LB)子网1822(例如,图16的(一个或多个)LB子网1622)的控制平面DMZ层1820(例如,图16的控制平面DMZ层1620)、可以包括(一个或多个)应用子网1826(例如,类似于图16的(一个或多个)应用子网1626)的控制平面应用层1824(例如,图16的控制平面应用层1624)、可以包括(一个或多个)DB子网1830的控制平面数据层1828(例如,图16的控制平面数据层1628)。包含在控制平面DMZ层1820中的(一个或多个)LB子网1822可以通信地耦合到包含在控制平面应用层1824中的(一个或多个)应用子网1826和可以包含在控制平面VCN 1816中的互联网网关1834(例如,图16的互联网网关1634),并且(一个或多个)应用子网1826可以通信地耦合到包含在控制平面数据层1828中的(一个或多个)DB子网1830以及服务网关1836(例如,图16的服务网关)和网络地址转换(NAT)网关1838(例如,图16的NAT网关1638)。控制平面VCN 1816可以包括服务网关1836和NAT网关1838。

[0292] 数据平面VCN 1818可以包括数据平面应用层1846(例如,图16的数据平面应用层1646)、数据平面DMZ层1848(例如,图16的数据平面DMZ层1648),以及数据平面数据层1850(例如,图16的数据平面数据层1650)。数据平面DMZ层1848可以包括可以通信地耦合到数据平面应用层1846的(一个或多个)可信应用子网1860和(一个或多个)不可信应用子网1862以及包含在数据平面VCN 1818中的互联网网关1834的(一个或多个)LB子网1822。(一个或多个)可信应用子网1860可以通信地耦合到包含在数据平面VCN 1818中的服务网关1836、包含在数据平面VCN 1818中的NAT网关1838以及包含在数据平面数据层1850中的(一个或多个)DB子网1830。(一个或多个)不可信应用子网1862可以通信地耦合到包含在数据平面VCN 1818中的服务网关1836和包含在数据平面数据层1850中的(一个或多个)DB子网1830。数据平面数据层1850可以包括可以通信地耦合到包含在数据平面VCN 1818中的服务网关1836的(一个或多个)DB子网1830。

[0293] (一个或多个)不可信应用子网1862可以包括可以通信地耦合到租户虚拟机(VM)1866(1)-(N)的一个或多个主VNIC 1864(1)-(N)。每个租户VM 1866(1)-(N)可以通信地耦合到可以包含在相应容器出口VCN 1868(1)-(N)中的相应应用子网1867(1)-(N),相应容器出口VCN 1868(1)-(N)可以包含在相应客户租赁1870(1)-(N)中。相应的辅助VNIC 1872(1)-(N)可以促进数据平面VCN 1818中包含的(一个或多个)不可信应用子网1862与容器出口VCN 1868(1)-(N)中包含的应用子网之间的通信。每个容器出口VCN 1868(1)-(N)可以包括NAT网关1838,该NAT网关1838可以通信地耦合到公共互联网1854(例如,图16的公共互联网1654)。

[0294] 包含在控制平面VCN 1816中并且包含在数据平面VCN 1818中的互联网网关1834可以通信地耦合到元数据管理服务1852(例如,图16的元数据管理系统1652),该元数据管理服务1852可以通信地耦合到公共互联网1854。公共互联网1854可以通信地耦合到包含在

控制平面VCN 1816中并且包含在数据平面VCN 1818中的NAT网关1838。包含在控制平面VCN 1816中和包含在数据平面VCN 1818中的服务网关1836可以通信地耦合到云服务1856。

[0295] 在一些实施例中,数据平面VCN 1818可以与客户租赁1870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、可能与其他客户资源通信或可能以其他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与IaaS提供商的代码。

[0296] 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1846的功能。运行该功能的代码可以在VM 1866(1)-(N)中执行,并且该代码可以不被配置为在数据平面VCN 1818上的其他任何地方运行。每个VM 1866(1)-(N)可以连接到一个客户租赁1870。包含在VM 1866(1)-(N)中的相应容器1871(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1871(1)-(N)运行代码,其中容器1871(1)-(N)可能至少包含在(一个或多个)不可信应用子网1862中包含的VM 1866(1)-(N)中),这可以帮助防止不正确的或以其他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1871(1)-(N)可以通信地耦合到客户租赁1870并且可以被配置为传输或接收来自客户租赁1870的数据。容器1871(1)-(N)可以不被配置为从数据平面VCN 1818中的任何其他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他方式处置容器1871(1)-(N)。

[0297] 在一些实施例中,(一个或多个)可信应用子网1860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1860可以通信地耦合到(一个或多个)DB子网1830并且被配置为在(一个或多个)DB子网1830中执行CRUD操作。(一个或多个)不可信应用子网1862可以通信地耦合到(一个或多个)DB子网1830,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1830中执行读取操作。可以包含在每个客户的VM 1866(1)-(N)中并且可以运行来自客户的代码的容器1871(1)-(N)可以不与(一个或多个)DB子网1830通信地耦合。

[0298] 在其他实施例中,控制平面VCN 1816和数据平面VCN 1818可以不直接通信地耦合。在这个实施例中,控制平面VCN 1816和数据平面VCN 1818之间可能没有直接通信。但是,通信可以通过至少一种方法间接发生。LPG 1810可以由IaaS提供商建立,其可以促进控制平面VCN 1816和数据平面VCN 1818之间的通信。在另一个示例中,控制平面VCN 1816或数据平面VCN 1818可以经由服务网关1836调用云服务1856。例如,从控制平面VCN 1816对云服务1856的调用可以包括对可以与数据平面VCN 1818通信的服务的请求。

[0299] 图19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1900。服务运营商1902(例如,图16的服务运营商1602)可以通信地耦合到安全主机租赁1904(例如,图16的安全主机租赁1604),该安全主机租赁1904可以包括虚拟云网络(VCN)1906(例如,图16的VCN 1606)和安全主机子网1908(例如,图16的安全主机子网1608)。VCN 1906可以包括LPG 1910(例如,图16的LPG 1610),该LPG 1910可以经由包含在SSH VCN 1912(例如,图16的SSH VCN 1612)中的LPG 1910通信地耦合到SSH VCN 1912。SSH VCN 1912可以包括SSH子网1914(例如,图16的SSH子网1614),并且SSH VCN 1912可以经由包含在控制平面VCN 1916中的LPG 1910通信地耦合到控制平面VCN 1916(例如,图16的控制平面VCN 1616)

并且经由包含在数据平面VCN 1918中的LPG 1910耦合到数据平面VCN 1918(例如,图16的数据平面1618)。控制平面VCN 1916和数据平面VCN 1918可以包含在服务租赁1919(例如,图16的服务租赁1619)中。

[0300] 控制平面VCN 1916可以包括可以包含(一个或多个)LB子网1922(例如,图16的(一个或多个)LB子网1622)的控制平面DMZ层1920(例如,图16的控制平面DMZ层1620)、可以包括(一个或多个)应用子网1926(例如,图16的(一个或多个)应用子网1626)的控制平面应用层1924(例如,图16的控制平面应用层1624)、可以包括(一个或多个)DB子网1930(例如,图18的(一个或多个)DB子网1830)的控制平面数据层1928(例如,图16的控制平面数据层1628)。包含在控制平面DMZ层1920中的(一个或多个)LB子网1922可以通信地耦合到包含在控制平面应用层1924中的(一个或多个)应用子网1926和可以包含在控制平面VCN 1916中的互联网网关1934(例如,图16的互联网网关1634),并且(一个或多个)应用子网1926可以通信地耦合到包含在控制平面数据层1928中的(一个或多个)DB子网1930以及服务网关1936(例如,图16的服务网关)和网络地址转换(NAT)网关1938(例如,图16的NAT网关1638)。控制平面VCN 1916可以包括服务网关1936和NAT网关1938。

[0301] 数据平面VCN 1918可以包括数据平面应用层1946(例如,图16的数据平面应用层1646)、数据平面DMZ层1948(例如,图16的数据平面DMZ层1648)),以及数据平面数据层1950(例如,图16的数据平面数据层1650)。数据平面DMZ层1948可以包括可以通信地耦合到数据平面应用层1946的(一个或多个)可信应用子网1960(例如,图18的(一个或多个)可信应用子网1860)和(一个或多个)不可信应用子网1962(例如,图18的(一个或多个)不可信应用子网1862)以及包含在数据平面VCN 1918中的互联网网关1934的(一个或多个)LB子网1922。(一个或多个)可信应用子网1960可以通信地耦合到包含在数据平面VCN 1918中的服务网关1936、包含在数据平面VCN 1918中的NAT网关1938以及包含在数据平面数据层1950中的(一个或多个)DB子网1930。(一个或多个)不可信应用子网1962可以通信地耦合到包含在数据平面VCN 1918中的服务网关1936和包含在数据平面数据层1950中的(一个或多个)DB子网1930。数据平面数据层1950可以包括可以通信地耦合到包含在数据平面VCN 1918中的服务网关1936的(一个或多个)DB子网1930。

[0302] (一个或多个)不可信应用子网1962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1962内的租户虚拟机(VM)1966(1)-(N)的主VNIC 1964(1)-(N)。每个租户VM 1966(1)-(N)可以在相应的容器1967(1)-(N)中运行代码,并且可通信地耦合到可以包含在容器出口VCN 1968中包含的数据平面应用层1946中的应用子网1926。相应的辅助VNIC 1972(1)-(N)可以促进包含在数据平面VCN 1918中的(一个或多个)不可信应用子网1962和包含在容器出口VCN 1968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1954(例如,图16的公共互联网1654)的NAT网关1938。

[0303] 包含在控制平面VCN 1916中和包含在数据平面VCN 1918中的互联网网关1934可以通信地耦合到元数据管理服务1952(例如,图16的元数据管理系统1652),该元数据管理服务1952可以通信地耦合到公共互联网1954。公共互联网1954可以通信地耦合到包含在控制平面VCN 1916中并且包含在数据平面VCN 1918中的NAT网关1938。包含在控制平面VCN 1916中并且包含在数据平面VCN 1918中的服务网关1936可以通信地耦合到云服务1956。

[0304] 在一些示例中,图19的框图1900的体系架构所示的模式可以被认为是图18的框图

1800的体系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通信(例如,断开连接的区域),那么这种模式可能是IaaS提供商的客户所期望的。客户可以实时访问每个客户的VM 1966(1)-(N)中包含的相应容器1967(1)-(N)。容器1967(1)-(N)可以被配置为对包含在数据平面应用层1946的(一个或多个)应用子网1926中的相应辅助VNIC 1972(1)-(N)进行调用,该数据平面应用层1946可以包含在容器出口VCN 1968中。辅助VNIC 1972(1)-(N)可以将调用传输到NAT网关1938,NAT网关1938可以将调用传输到公共互联网1954。在这个示例中,可以由客户实时访问的容器1967(1)-(N)可以与控制平面VCN 1916隔离,并且可以与数据平面VCN 1918中包含的其他实体隔离。容器1967(1)-(N)也可以与来自其他客户的资源隔离。

[0305] 在其他示例中,客户可以使用容器1967(1)-(N)来调用云服务1956。在这个示例中,客户可以运行容器1967(1)-(N)中从云服务1956请求服务的代码。容器1967(1)-(N)可以将该请求传输到辅助VNIC 1972(1)-(N),辅助VNIC 1972(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1954。公共互联网1954可以经由互联网网关1934将请求传输到包含在控制平面VCN 1916中的(一个或多个)LB子网1922。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1926,该(一个或多个)应用子网1926可以经由服务网关1936将请求传输到云服务1956。

[0306] 应当认识到的是,各图中描绘的IaaS体系架构1600、1700、1800、1900可以具有除所描绘的那些之外的其他组件。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。在一些其他实施例中,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配置或组件布置。

[0307] 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、弹性可扩展、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人提供的Oracle云基础设施(OCI)。

[0308] 图20图示了其中可以实现各种实施例的示例计算机系统2000。系统2000可以用于实现上述任何计算机系统。如图所示,计算机系统2000包括经由总线子系统2002与多个外围子系统通信的处理单元2004。这些外围子系统可以包括处理加速单元2006、I/O子系统2008、存储子系统2018和通信子系统2024。存储子系统2018包括有形计算机可读存储介质2022和系统存储器2010。

[0309] 总线子系统2002提供用于让计算机系统2000的各种组件和子系统按意图彼此通信的机制。虽然总线子系统2002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2002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)局部总线和外围组件互连(PCI)总线,其可以被实现为按IEEE P1386.1标准制造的Mezzanine总线。

[0310] 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2004控制计算机系统2000的操作。一个或多个处理器可以被包括在处理单元2004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2004可以被实现为一个或多个独立的处理单元2032和/或2034,其中在每个处理单元中包括单核或多核处理器。在其

他实施例中,处理单元2004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。

[0311] 在各种实施例中,处理单元2004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2004中和/或存储子系统2018中。通过适当的编程,(一个或多个)处理器2004可以提供上述各种功能。计算机系统2000可以附加地包括处理加速单元2006,其可以包括数字信号处理器(DSP)、专用处理器,等等。

[0312] I/O子系统2008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、麦克风以及其他类型的输入设备。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,诸如的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的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到输入设备(例如,Google**Glass®**)中的输入的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。

[0313] 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,诸如MIDI键盘、数字乐器等的音频输入设备。

[0314] 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2000向用户或其他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。

[0315] 计算机系统2000可以包括包含软件元素、被示为当前位于系统存储器2010中的存储子系统2018。系统存储器2010可以存储可加载并且可在处理单元2004上执行的程序指令,以及在这些程序的执行期间所产生的数据。

[0316] 取决于计算机系统2000的配置和类型,系统存储器2010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,等等)。RAM通常包含可被处理单元2004立即访问和/或目前正被处理单元2004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2010可以包括多种不同类型的存储器,例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,诸如包含有助于在启动

期间在计算机系统2000的元素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,但不是限制,系统存储器2010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2012,程序数据2014,以及操作系统2016。作为示例,操作系统2016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®** 160S和**Palm®** OS操作系统的移动操作系统。

[0317] 存储子系统2018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结构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2018中。这些软件模块或指令可以被处理单元2004执行。存储子系统2018也可以提供用于存储根据本公开被使用的数据的储存库。

[0318] 存储子系统2000也可以包括可被进一步连接到计算机可读存储介质2022的计算机可读存储介质读取器2020。与系统存储器2010一起并且,可选地,与其相结合,计算机可读存储介质2022可以全面地表示用于临时和/或更持久地包含、存储、发送和检索计算机可读信息的远程、本地、固定和/或可移除存储设备加存储介质。

[0319] 包含代码或代码的部分的计算机可读存储介质2022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)、闪存存储器或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光学储存器、磁带盒、磁带、磁盘储存器或其他磁存储设备,或者其他有形的计算机可读介质。这还可以包括非有形的计算机可读介质,诸如数据信号、数据传输或可以用于传输期望信息并可以由计算系统2000访问的任何其他介质。

[0320] 举例来说,计算机可读存储介质2022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®**盘或其他光学介质)读取或写到其的光盘驱动器。计算机可读存储介质2022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、数字音频带,等等。计算机可读存储介质2022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(诸如固态RAM、动态RAM、静态RAM)、基于DRAM的SSD,磁阻RAM(MRAM)SSD,以及使用基于DRAM和闪存存储器的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2000提供计算机可读指令、数据结构、程序模块及其他数据的非易失性存储。

[0321] 通信子系统2024提供到其他计算机系统和网络的接口。通信子系统2024用作用于从其他系统接收数据和从计算机系统2000向其他系统发送数据的接口。例如,通信子系统2024可以使计算机系统2000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2024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型数据速率)的先进数据网络技术,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(GPS)接收器组件和/或其他组件。在一些实施例中,作为无线接口的附加或者替代,通信子系统2024可以提供有线网络连接(例如,以太网)。

[0322] 在一些实施例中,通信子系统2024也可以代表可以使用计算机系统2000的一个或多个用户接收结构化和/或非结构化数据馈送2026、事件流2028、事件更新2030等形式的输入通信。

[0323] 举例来说,通信子系统2024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2026,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。

[0324] 此外,通信子系统2024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2028和/或事件更新2030。产生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,等等。

[0325] 通信子系统2024也可以被配置为向一个或多个数据库输出结构化和/或非结构化数据馈送2026、事件流2028、事件更新2030,等等,这一个或多个数据库可以与耦合到计算机系统2000的一个或多个流式数据源计算机通信。

[0326] 计算机系统2000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、或任何其他数据处理系统。

[0327] 由于计算机和网络的不断变化的本质,图中绘出的计算机系统2000的描述仅仅要作为具体的示例。具有比图中绘出的系统更多或更少组件的许多其他配置是可能的。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applets)或其组合来实现。另外,也可以采用到诸如网络输入/输出设备之类的其他计算设备的连接。基于本文提供的公开内容和示教,本领域普通技术人员将认识到实现各种实施例的其他方式和/或方法。

[0328] 虽然已经描述了具体实施例,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。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。

[0329] 另外,虽然已经使用硬件和软件的特定组合描述了实施例,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。相应地,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,包括但不限于用于处理间通信的常规技术,并且不同的处理对可以使用不同的技术,或者同一对处理可以在不同时间

使用不同的技术。

[0330] 相应地,说明书和附图被认为是说明性的而不是限制性的。但是,显然可以对其进行添加、减少、删除和其他修改和改变而不背离权利要求中阐述的更广泛的精神和范围。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。

[0331] 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”以及类似的指称要被解释为涵盖单数和复数,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(including)”和“包含(containing)”要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、附加到或连接在一起,即使中间存在一些东西。除非本文另有指示,否则本文中值范围的列举仅旨在用作个别引用落入该范围内的每个单独值的速记方法,并且每个单独值被并入说明书中,就好像它在本文中个别列举一样。除非本文另有指示或与上下文明显矛盾,否则本文所述的所有方法都可以以任何合适的顺序执行。本文提供的任何和所有示例或示例性语言(例如,“诸如”)的使用仅旨在更好地阐明实施例并且不对本公开的范围构成限制,除非另有声明。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。

[0332] 析取语言,诸如短语“X、Y或Z中的至少一个”,除非另有明确说明,否则旨在在一般用于表示项目、术语等的上下文中理解,可以是X、Y或Z,或它们的任何组合(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。

[0333] 本文描述了本公开的优选实施例,包括已知用于实施本公开的最佳模式。那些优选实施例的变型对于本领域普通技术人员在阅读上述描述后会变得显而易见。普通技术人员应该能够适当地采用这样的变型并且可以以不同于本文具体描述的方式来实践本公开。相应地,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,否则本公开包括在其所有可能的变化中的上述元素的任何组合。

[0334] 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,就好像每个参考文献个别且具体地指示通过引用并入并在本文中全文阐述一样。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那些之外的任何数量的环境和应用中被使用。相应地,本说明书和附图应当被认为是说明性而不是限制性的。

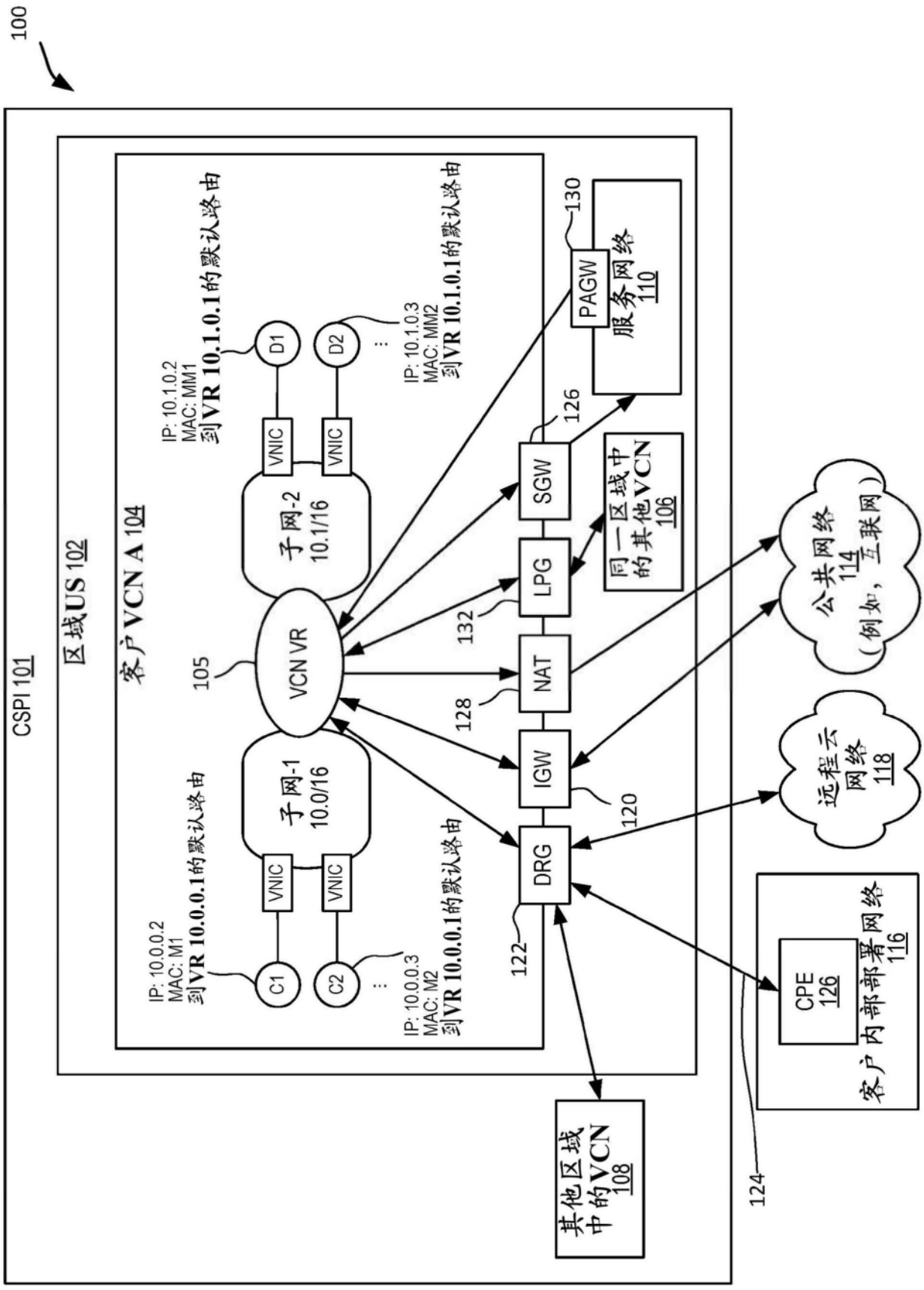

100
CSPI 101
区域US 102
客户VCN A 104
105
VCN VR
子网-1
10.0/16
子网-2
10.1/16
VNIC
C1
C2
D1
D2
IP: 10.0.0.2
MAC: M1
到VR 10.0.0.1的默认路由
IP: 10.0.0.3
MAC: M2
到VR 10.0.0.1的默认路由
IP: 10.1.0.2
MAC: MM1
到VR 10.1.0.1的默认路由
IP: 10.1.0.3
MAC: MM2
到VR 10.1.0.1的默认路由
DRG
122
IGW
120
NAT
128
LPG
132
SGW
126
PAGW
130
服务网络
110
同一区域中
的其他VCN
106
公共网络
114
(例如，互联网)
远程云
网络
118
其他区域
中的VCN
108
CPE
126
客户内部部署网络
116
124

图1

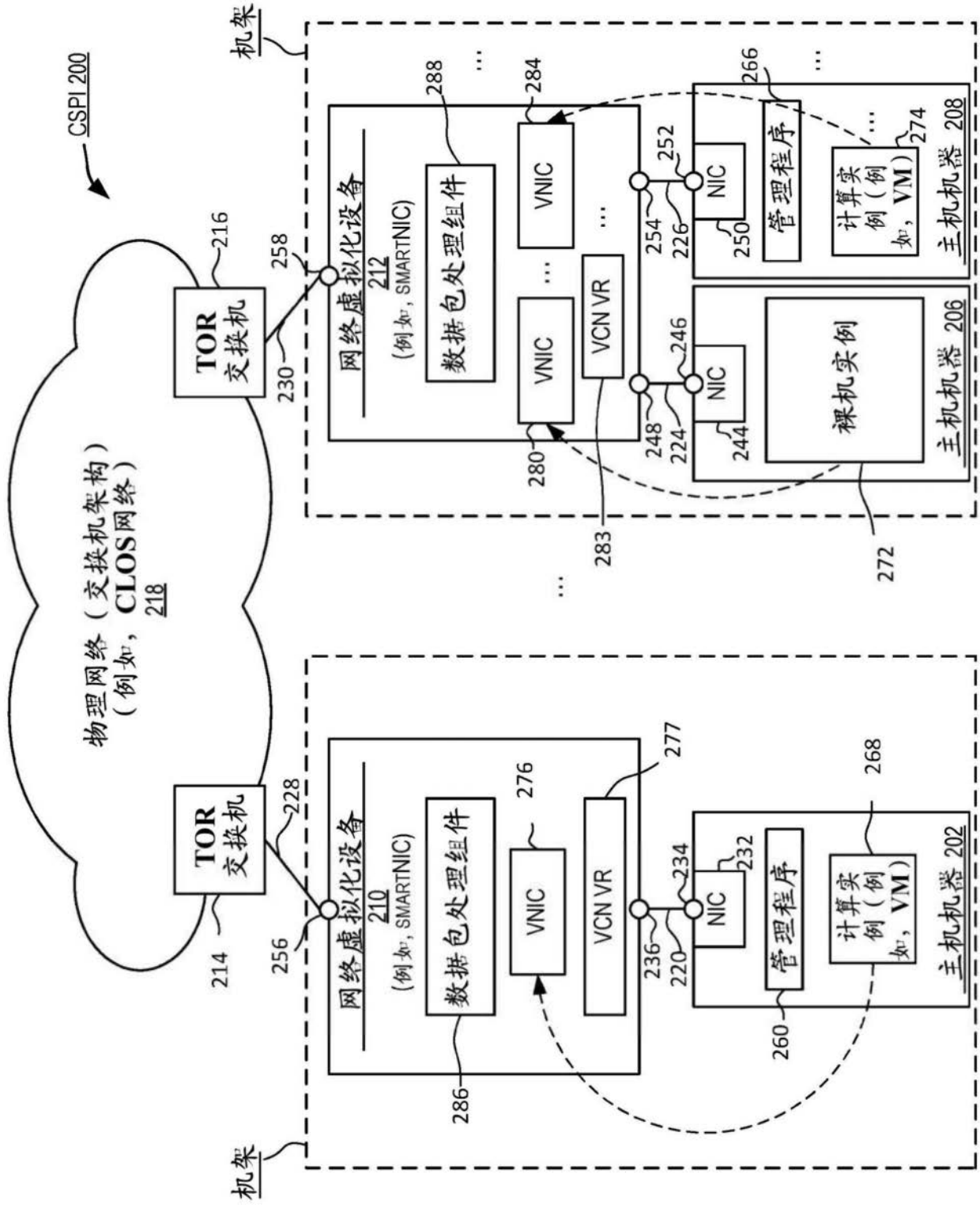

CSPI 200
物理网络（交换机架构）
（例如，CLOS网络）
218
TOR
交换机
216
TOR
交换机
214
机架
机架
网络虚拟化设备
212
（例如，SMARTNIC）
网络虚拟化设备
210
（例如，SMARTNIC）
数据包处理组件
288
数据包处理组件
286
VNIC
284
VNIC
280
VNIC
276
VCN VR
283
VCN VR
277
NIC
252
NIC
250
NIC
246
NIC
244
NIC
234
NIC
232
管理程序
266
管理程序
260
裸机实例
272
计算实例（例如，VM）
274
计算实例（例如，VM）
268
主机机器 208
主机机器 206
主机机器 202
254
226
248
224
236
220
258
230
256
228

图2

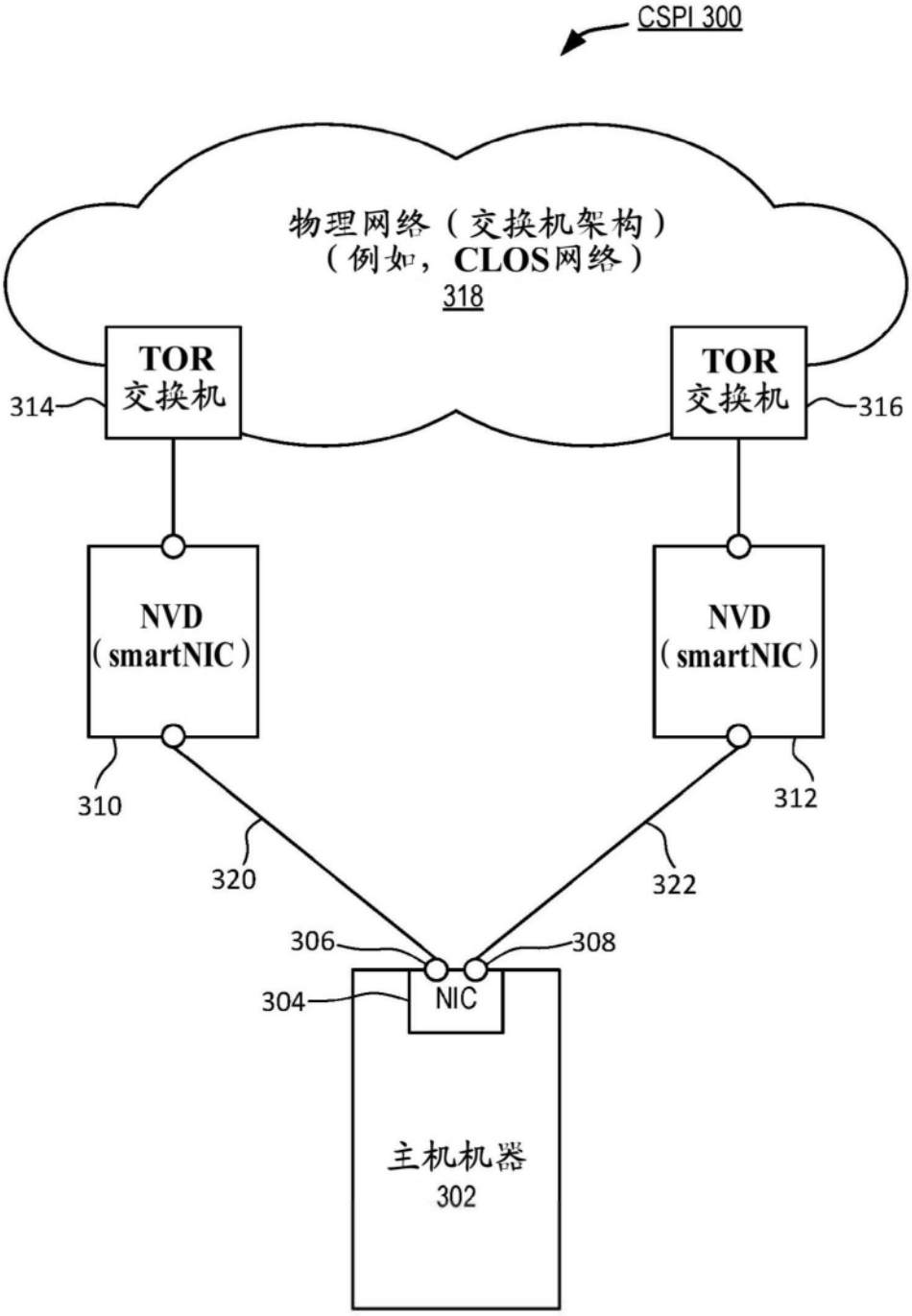

CSPI 300
物理网络（交换机架构）
（例如，CLOS网络）
318
TOR
交换机
314
TOR
交换机
316
NVD
(smartNIC)
NVD
(smartNIC)
310
312
320
322
306
308
304
NIC
主机机器
302

图3

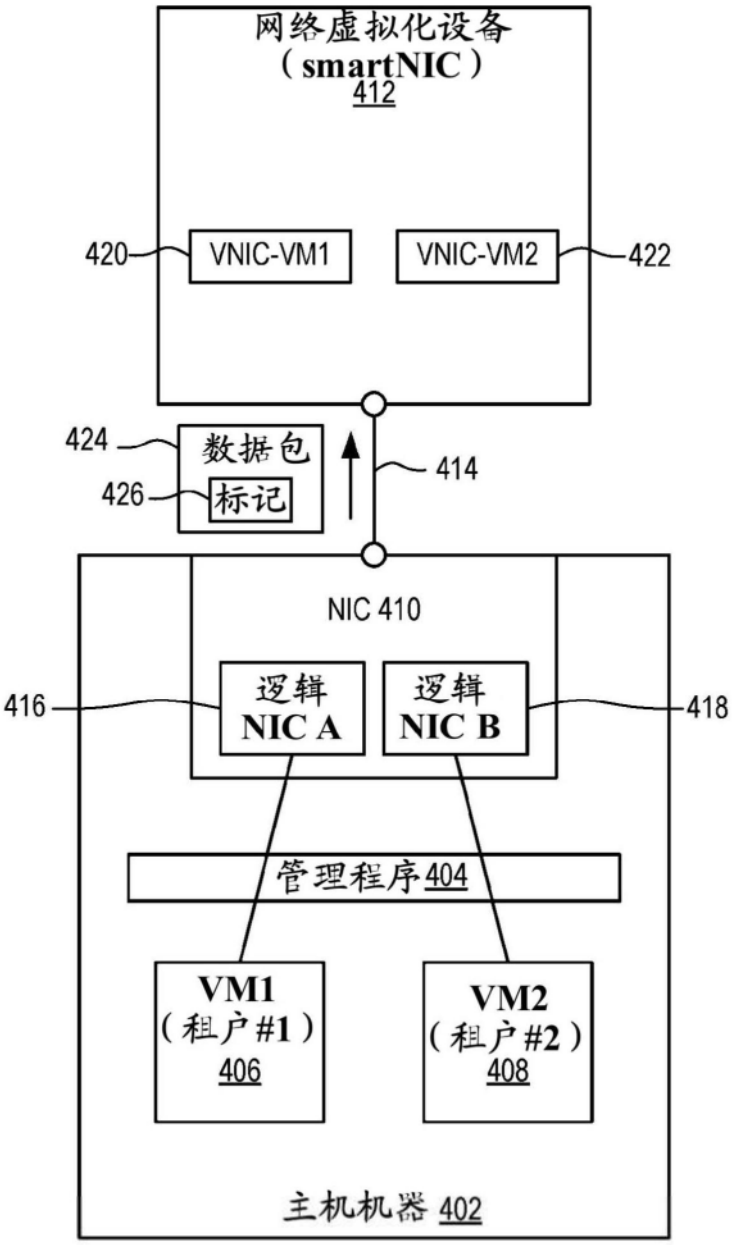

网络虚拟化设备
（smartNIC）
412
420
VNIC-VM1
VNIC-VM2
422
424
数据包
426
标记
414
NIC 410
416
逻辑
NIC A
逻辑
NIC B
418
管理程序404
VM1
（租户#1）
406
VM2
（租户#2）
408
主机机器 402

图4

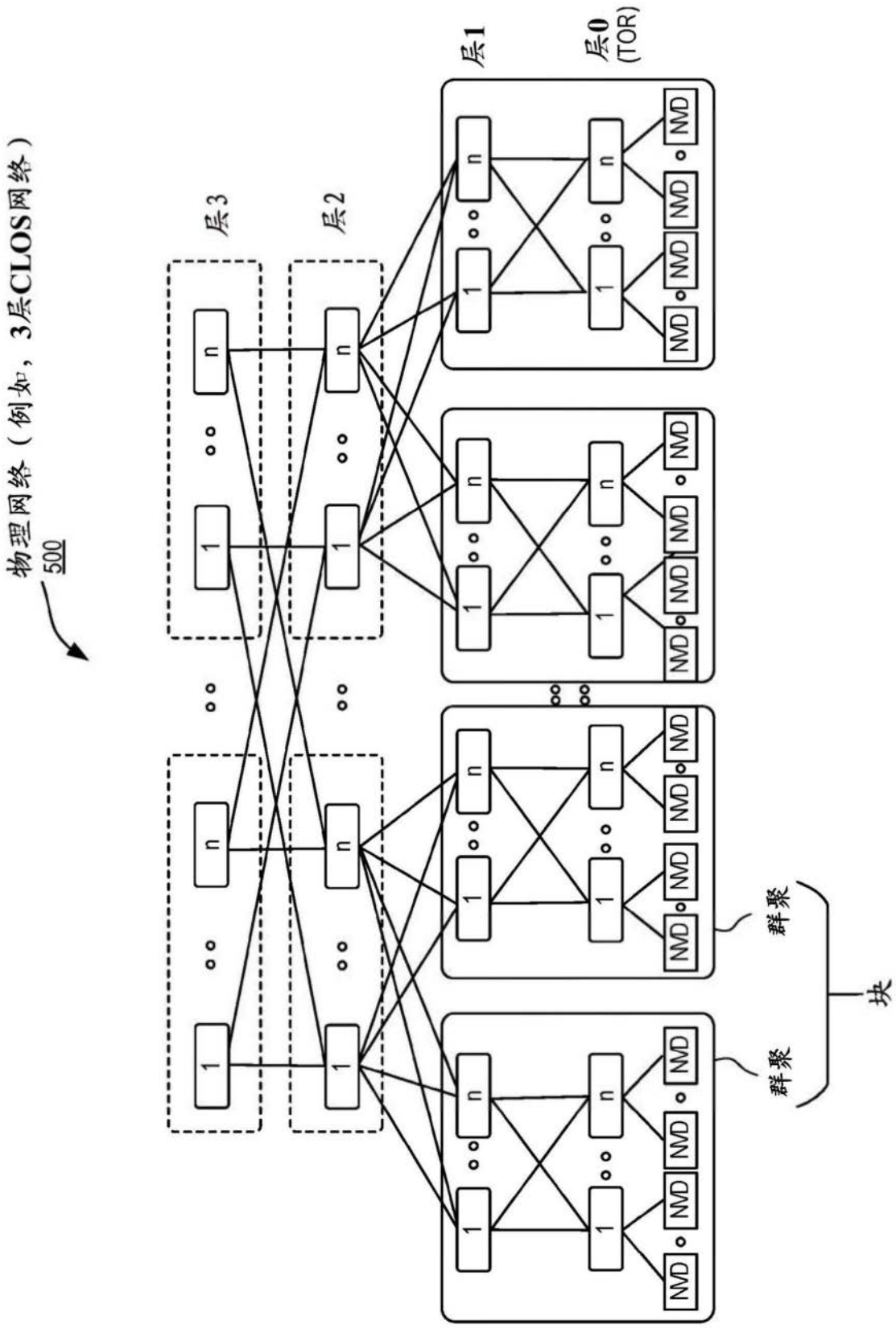


图5

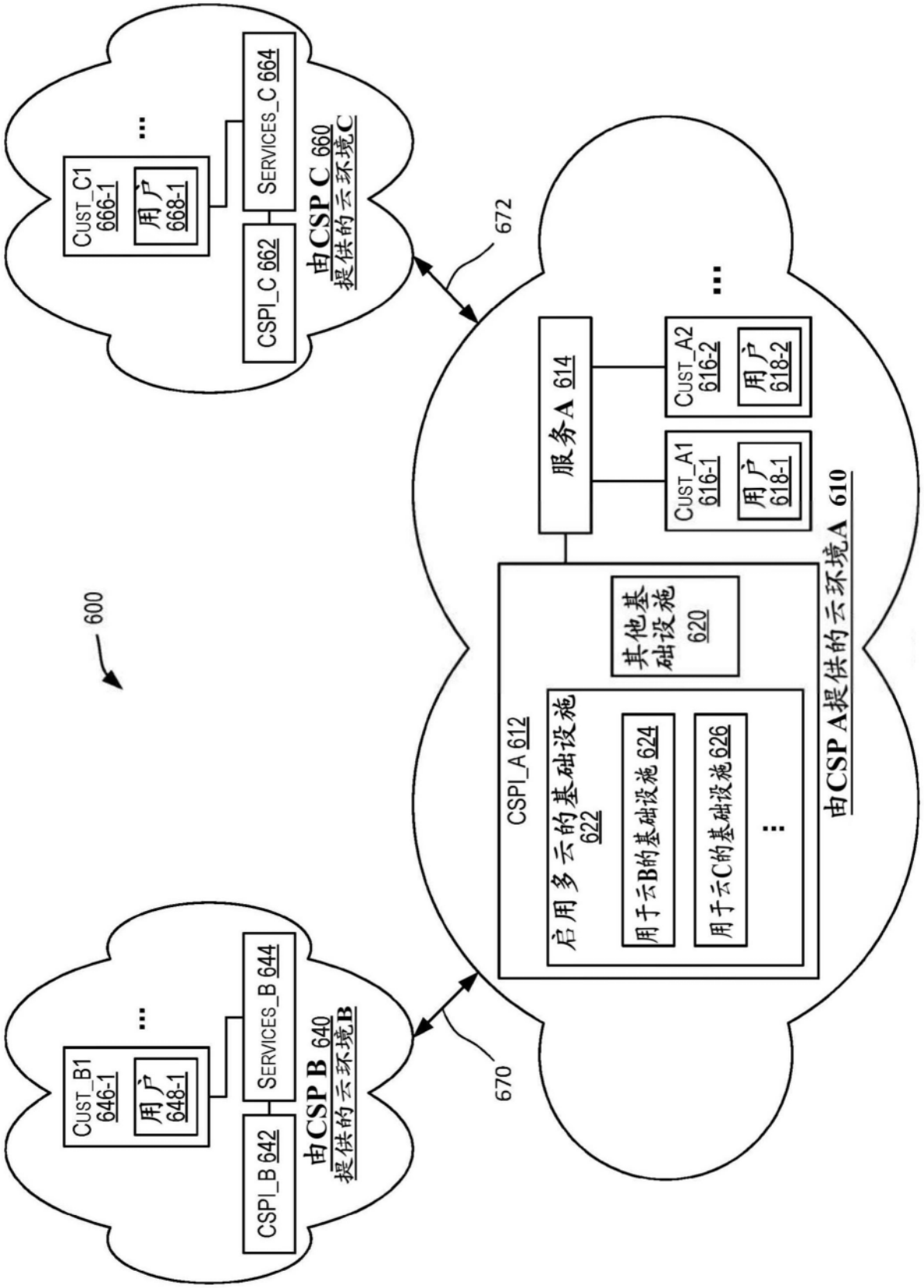

600
由CSP A提供的云环境A 610
CSPI_A 612
启用多云的基础设施 622
用于云B的基础设施 624
用于云C的基础设施 626
其他基础设施 620
服务A 614
CUST_A1 616-1
用户 618-1
CUST_A2 616-2
用户 618-2
672
670
由CSP C 660 提供的云环境C
CUST_C1 666-1
用户 668-1
SERVICES_C 664
CSPI_C 662
由CSP B 640 提供的云环境B
CUST_B1 646-1
用户 648-1
SERVICES_B 644
CSPI_B 642

图6

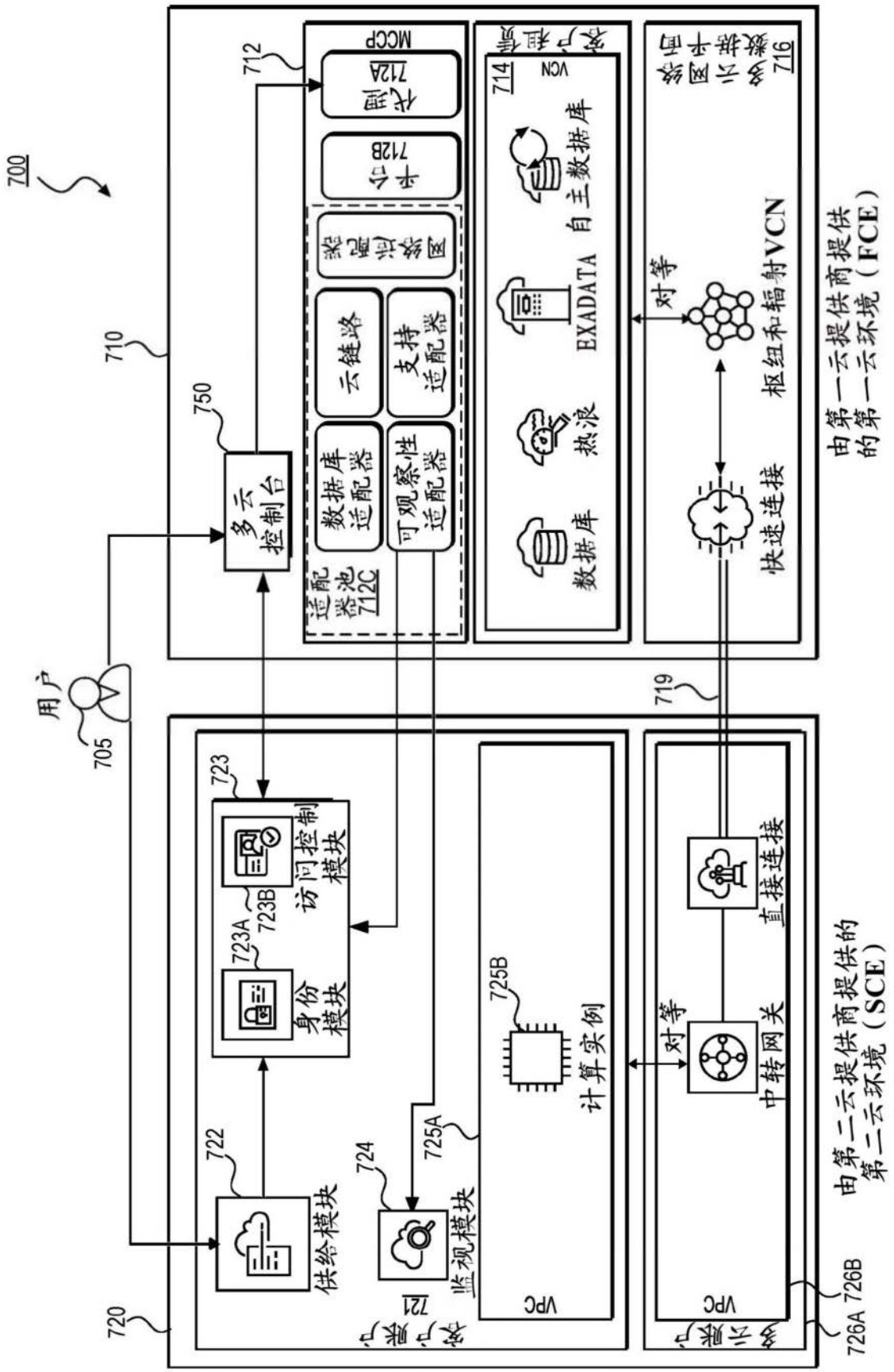

700
710
712
MCCP
代理
712A
平台
712B
云链路
支持适配器
数据库适配器
可观察性适配器
适配器池
712C
多云控制台
750
714
VCN
自主数据库
EXADATA
热浪
数据库
716
多云数据平面
枢纽和辐射VCN
快速连接
对等
由第一云提供商提供的第一云环境（FCE）
用户
705
719
720
723
访问控制模块
723A
723B
身份模块
722
供给模块
724
监视模块
721
725A
725B
计算实例
VPC
对等
中转网关
直接连接
726A
726B
由第二云提供商提供的第二云环境（SCE）

图7

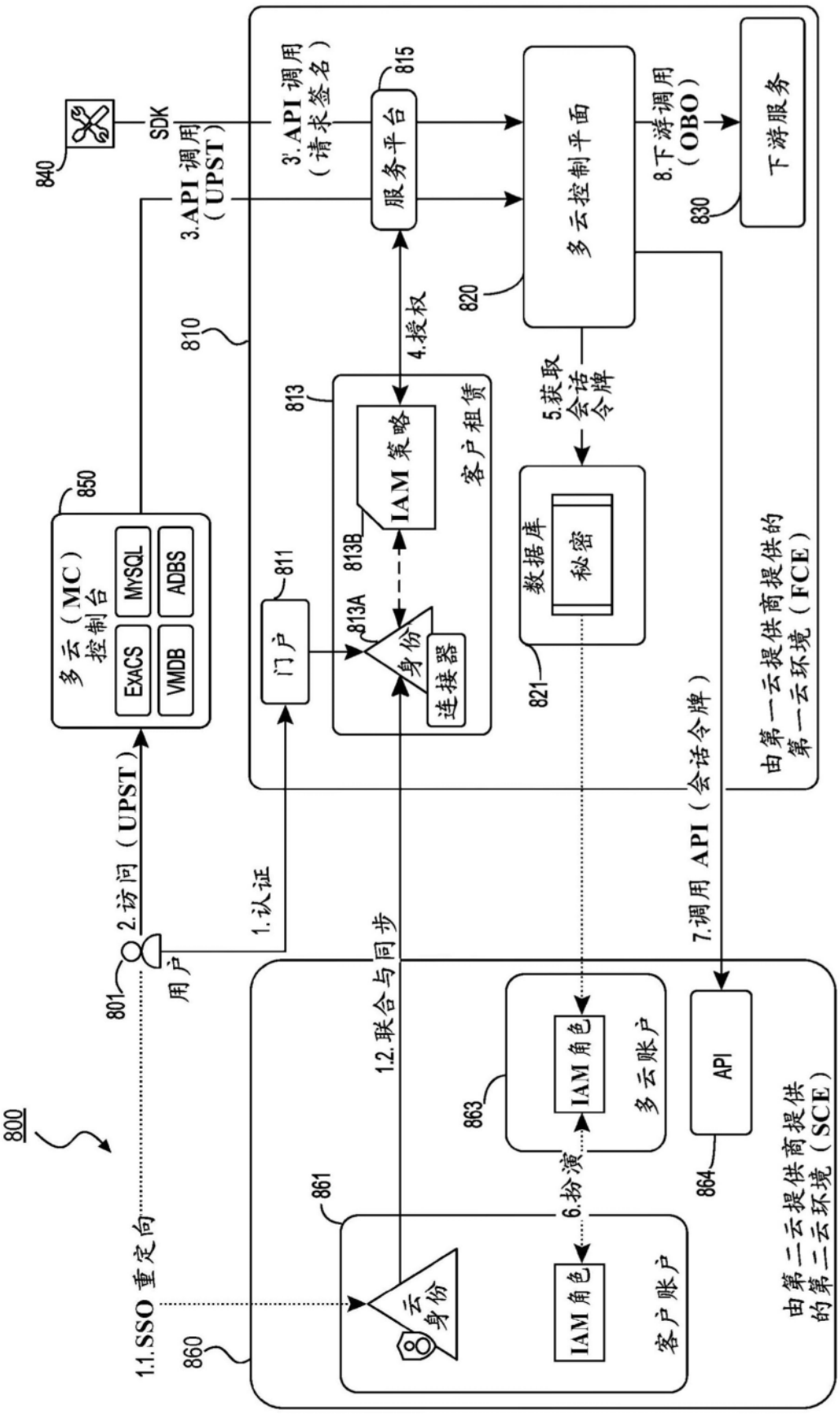

800
801
用户
1.认证
2.访问（UPST）
1.1.SSO 重定向
1.2.联合与同步
3.API 调用（UPST）
3'.API 调用（请求签名）
4.授权
5.获取会话令牌
6.扮演
7.调用 API（会话令牌）
8.下游调用（OBO）
SDK
840
多云（MC）控制台
ExaCS
MySQL
VMDB
ADBS
850
810
门户
811
身份
813A
IAM 策略
813B
连接器
客户租赁
813
服务平台
815
多云控制平面
820
数据库
秘密
821
下游服务
830
由第一云提供商提供的第一云环境（FCE）
云身份
861
客户账户
IAM 角色
860
IAM 角色
863
多云账户
API
864
由第二云提供商提供的第二云环境（SCE）

图8

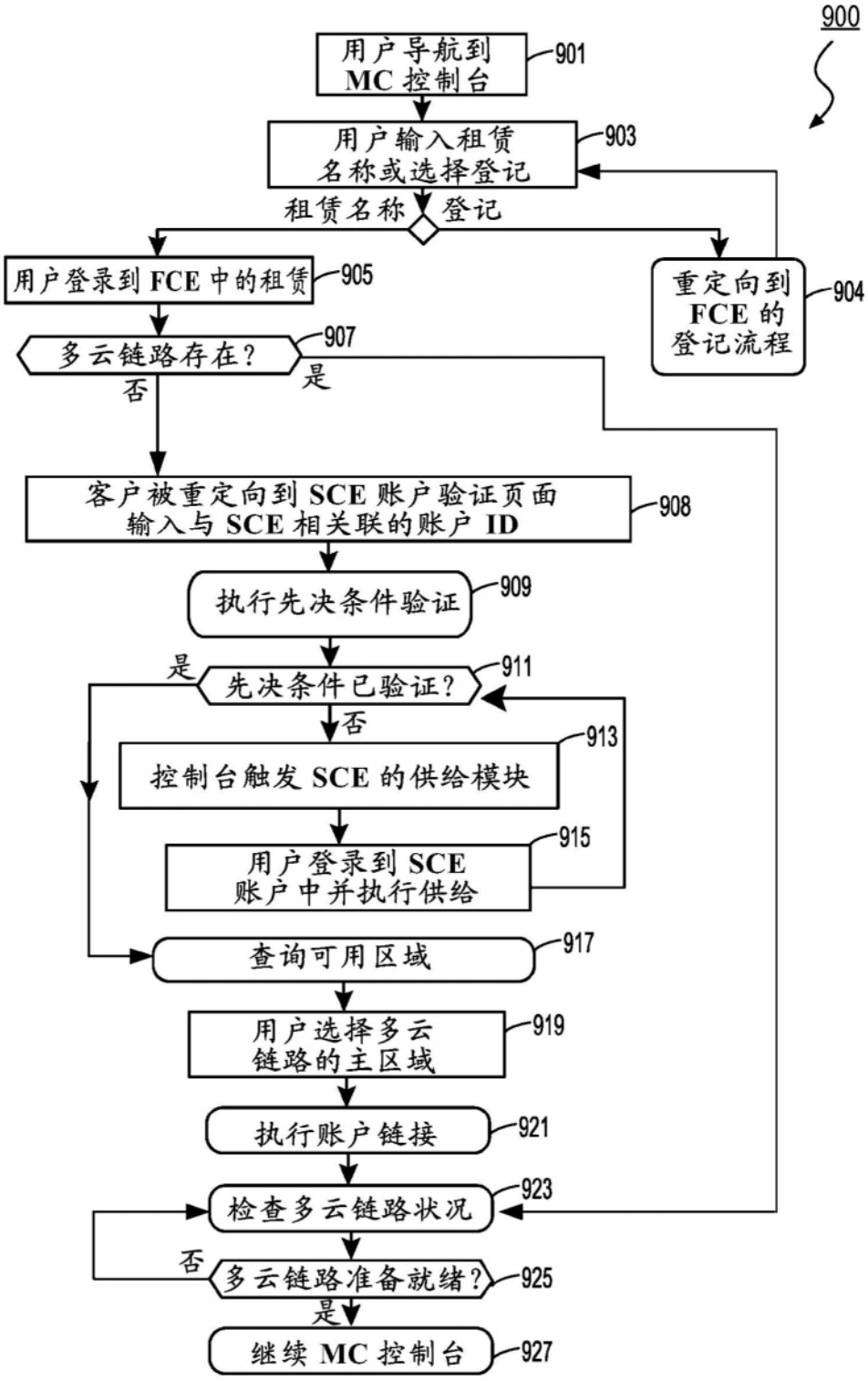

900
用户导航到 MC 控制台
901
用户输入租赁名称或选择登记
903
租赁名称
登记
用户登录到 FCE 中的租赁
905
重定向到 FCE 的登记流程
904
多云链路存在？
907
否
是
客户被重定向到 SCE 账户验证页面输入与 SCE 相关联的账户 ID
908
执行先决条件验证
909
是
先决条件已验证？
911
否
控制台触发 SCE 的供给模块
913
用户登录到 SCE 账户中并执行供给
915
查询可用区域
917
用户选择多云链路的主区域
919
执行账户链接
921
检查多云链路状况
923
否
多云链路准备就绪？
925
是
继续 MC 控制台
927

图9

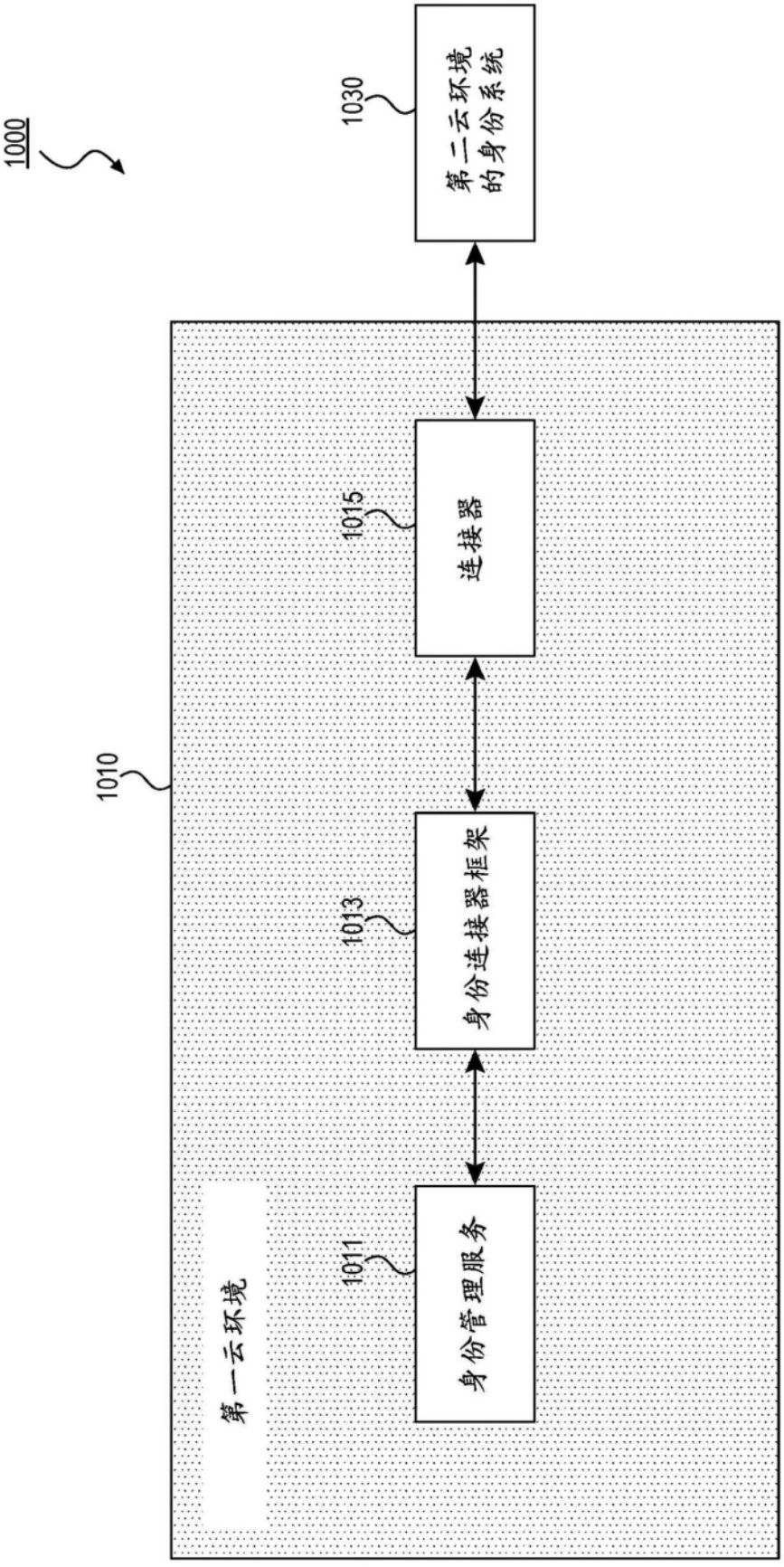

1000
1030
第二云环境的身份系统
1010
1015
连接器
1013
身份连接器框架
1011
身份管理服务
第一云环境

图10

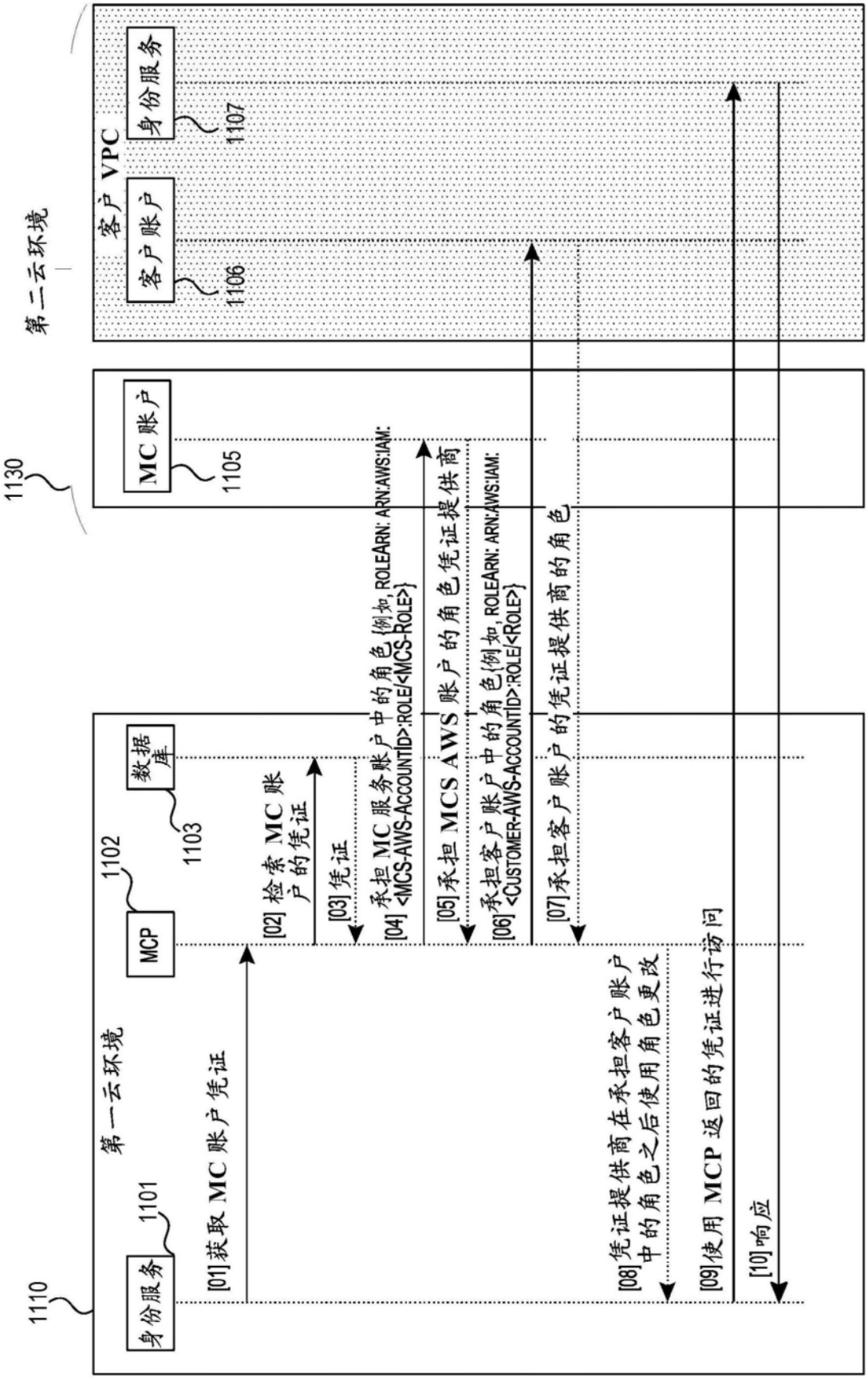

第一云环境
1110
身份服务
1101
MCP
1102
数据库
1103
第二云环境
1130
MC 账户
1105
客户 VPC
客户账户
1106
身份服务
1107
[01]获取 MC 账户凭证
[02] 检索 MC 账户的凭证
[03] 凭证
[04] 承担 MC 服务账户中的角色 {例如, ROLEARN: ARN:AWS:IAM: <MCS-AWS-ACCOUNTID>:ROLE/<MCS-ROLE>}
[05]承担 MCS AWS 账户的角色凭证提供商
[06] 承担客户账户中的角色{例如, ROLEARN: ARN:AWS:IAM: <CUSTOMER-AWS-ACCOUNTID>:ROLE/<ROLE>}
[07]承担客户账户的凭证提供商的角色
[08]凭证提供商在承担客户账户中的角色之后使用角色更改
[09]使用 MCP 返回的凭证进行访问
[10] 响应

图11

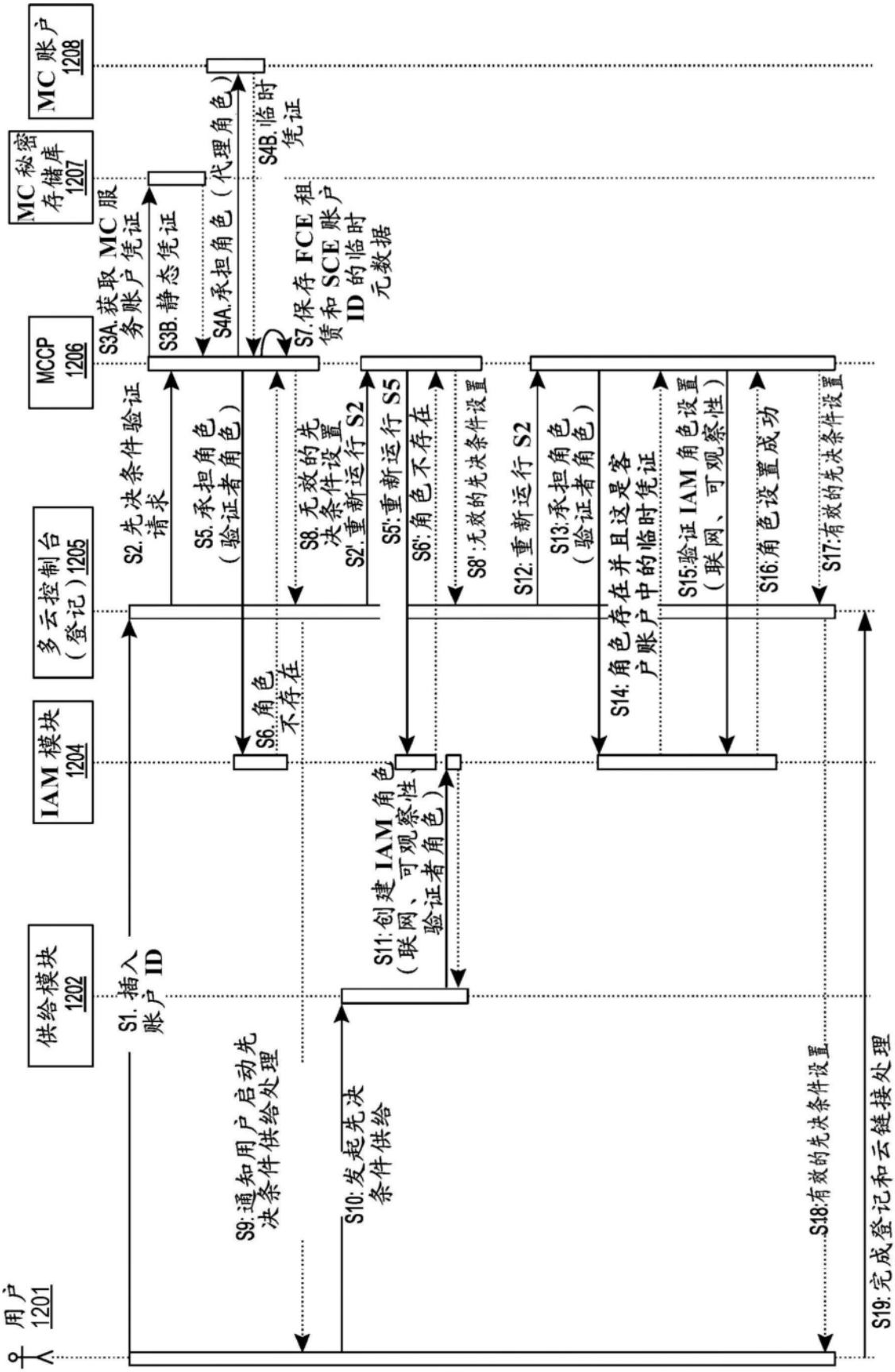

用户 1201
供给模块 1202
IAM 模块 1204
多云控制台（登记）1205
MCCP 1206
MC 秘密存储库 1207
MC 账户 1208
S1. 插入账户 ID
S2. 先决条件验证请求
S3A. 获取 MC 服务账户凭证
S3B. 静态凭证
S4A. 承担角色（代理角色）
S4B. 临时凭证
S5. 承担角色（验证者角色）
S6. 角色不存在
S7. 保存 FCE 租赁和 SCE 账户 ID 的临时元数据
S8. 无效的先决条件设置
S2'. 重新运行 S2
S5'. 重新运行 S5
S6'. 角色不存在
S8'. 无效的先决条件设置
S9. 通知用户启动先决条件供给处理
S10. 发起先决条件供给
S11. 创建 IAM 角色（联网、可观察性、验证者角色）
S12. 重新运行 S2
S13. 承担角色（验证者角色）
S14. 角色存在并且这是客户账户中的临时凭证
S15. 验证 IAM 角色设置（联网、可观察性）
S16. 角色设置成功
S17. 有效的先决条件设置
S18. 有效的先决条件设置
S19. 完成登记和云链接处理

图12

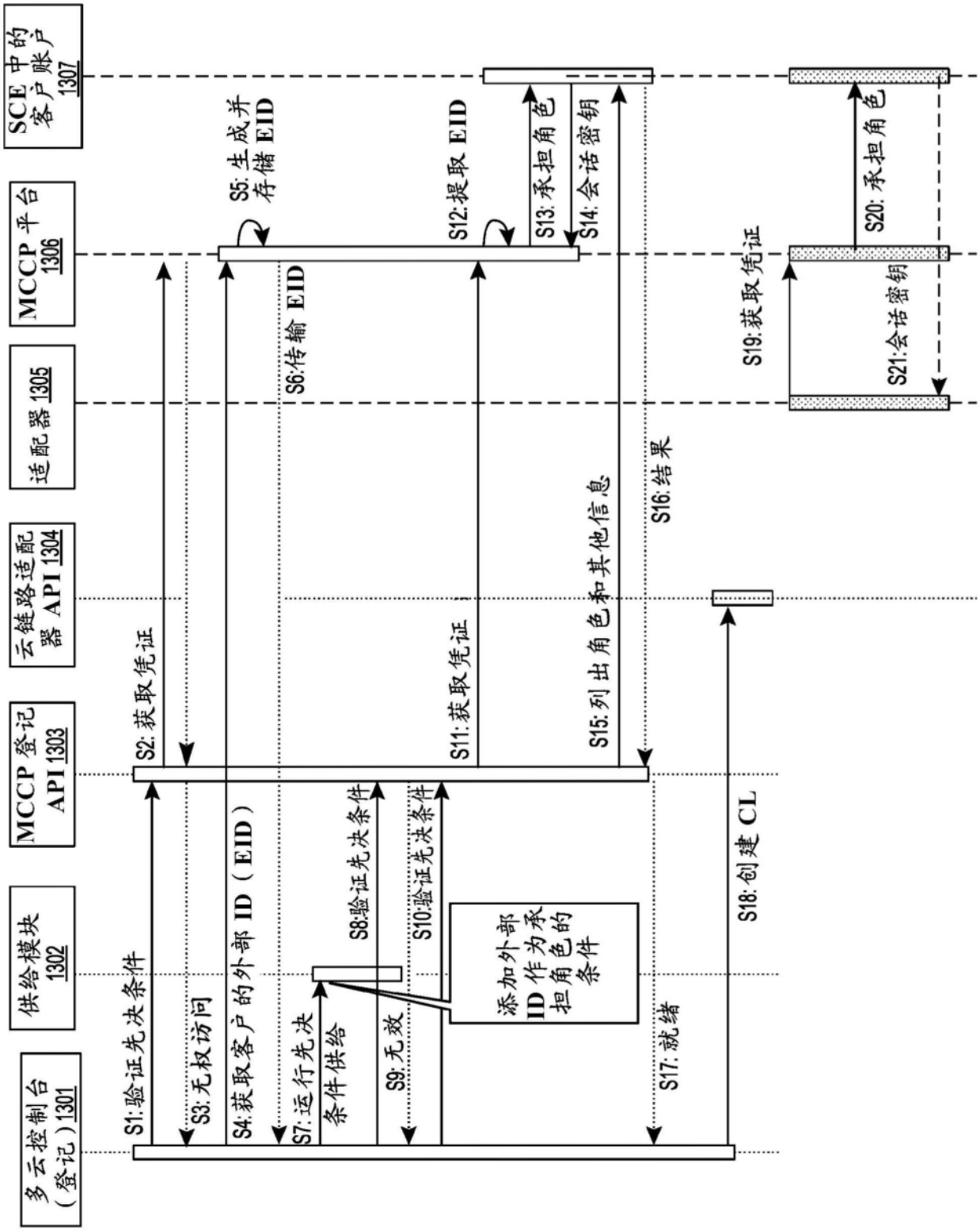

多云控制台（登记）1301
供给模块 1302
MCCP 登记 API 1303
云链路适配器 API 1304
适配器 1305
MCCP 平台 1306
SCE 中的客户账户 1307
S1:验证先决条件
S2:获取凭证
S3:无权访问
S4:获取客户的外部 ID（EID）
S5:生成并存储 EID
S6:传输 EID
S7:运行先决条件供给
S8:验证先决条件
S9:无效
S10:验证先决条件
S11:获取凭证
S12:提取 EID
S13:承担角色
S14:会话密钥
S15:列出角色和其他信息
S16:结果
S17:就绪
S18:创建 CL
S19:获取凭证
S20:承担角色
S21:会话密钥
添加外部 ID 作为承担角色的条件

图13

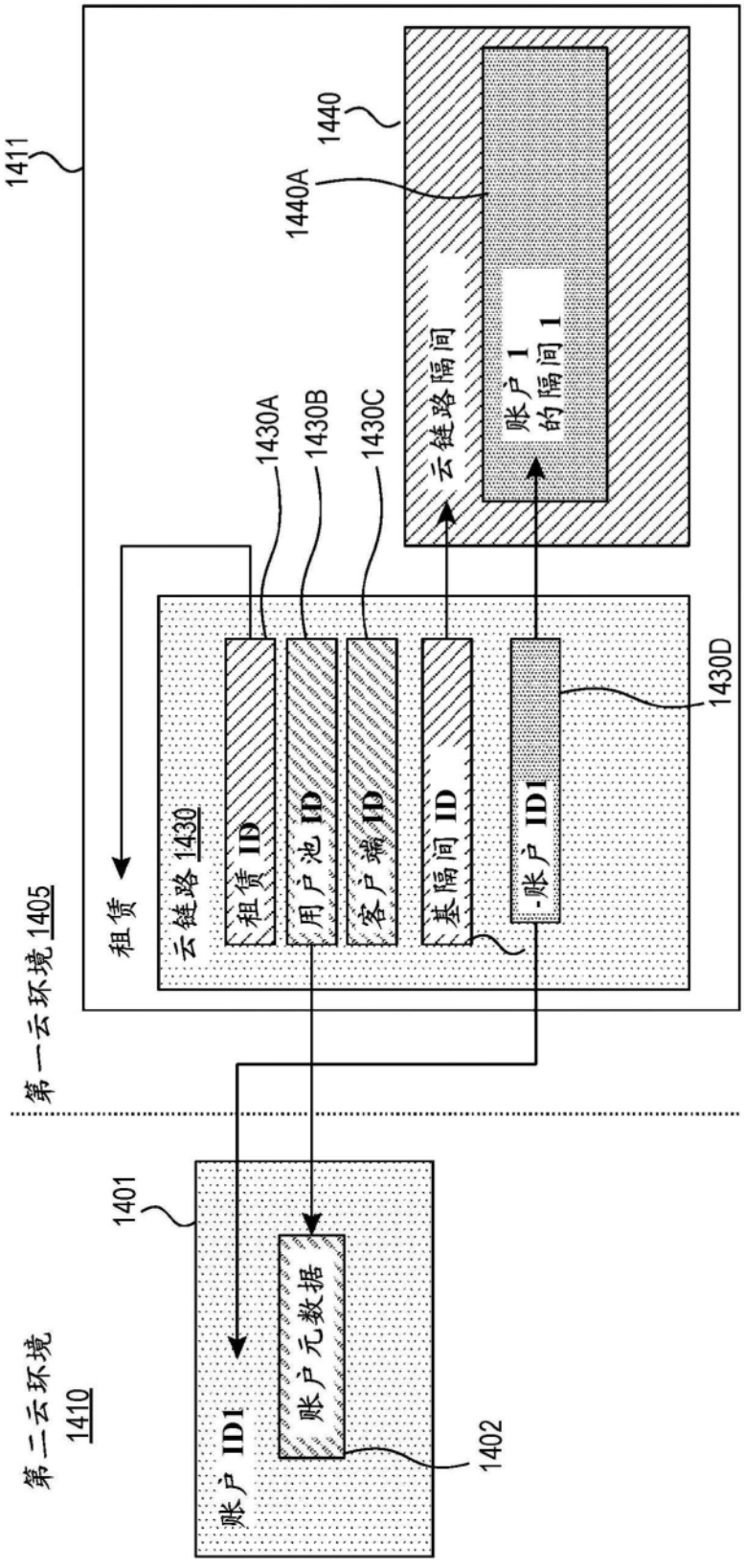

第一云环境 1405
第二云环境 1410
1411
1440
1440A
云链路隔间
账户 1 的隔间 1
1430A
1430B
1430C
1430D
云链路 1430
租赁 ID
用户池 ID
客户端 ID
基隔间 ID
-账户 ID1
租赁
1401
账户 ID1
账户元数据
1402

图14

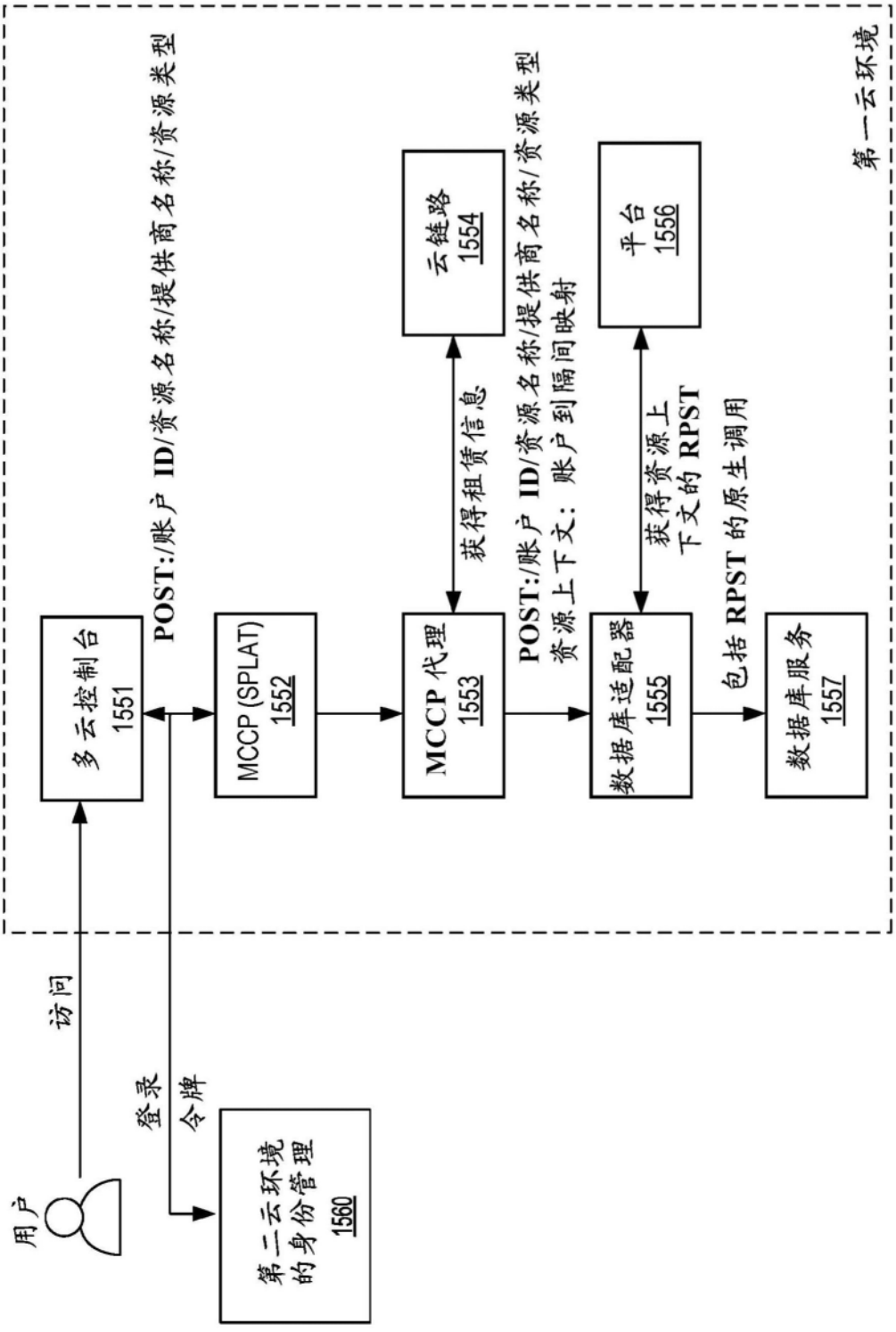

第一云环境
多云控制台
1551
POST:/账户 ID/资源名称/提供商名称/资源类型
MCCP (SPLAT)
1552
MCCP 代理
1553
获得租赁信息
云链路
1554
POST:/账户 ID/资源名称/提供商名称/资源类型
资源上下文：账户到隔间映射
数据库适配器
1555
获得资源上
下文的 RPST
平台
1556
包括 RPST 的原生调用
数据库服务
1557
访问
登录
令牌
用户
第二云环境
的身份管理
1560

图15

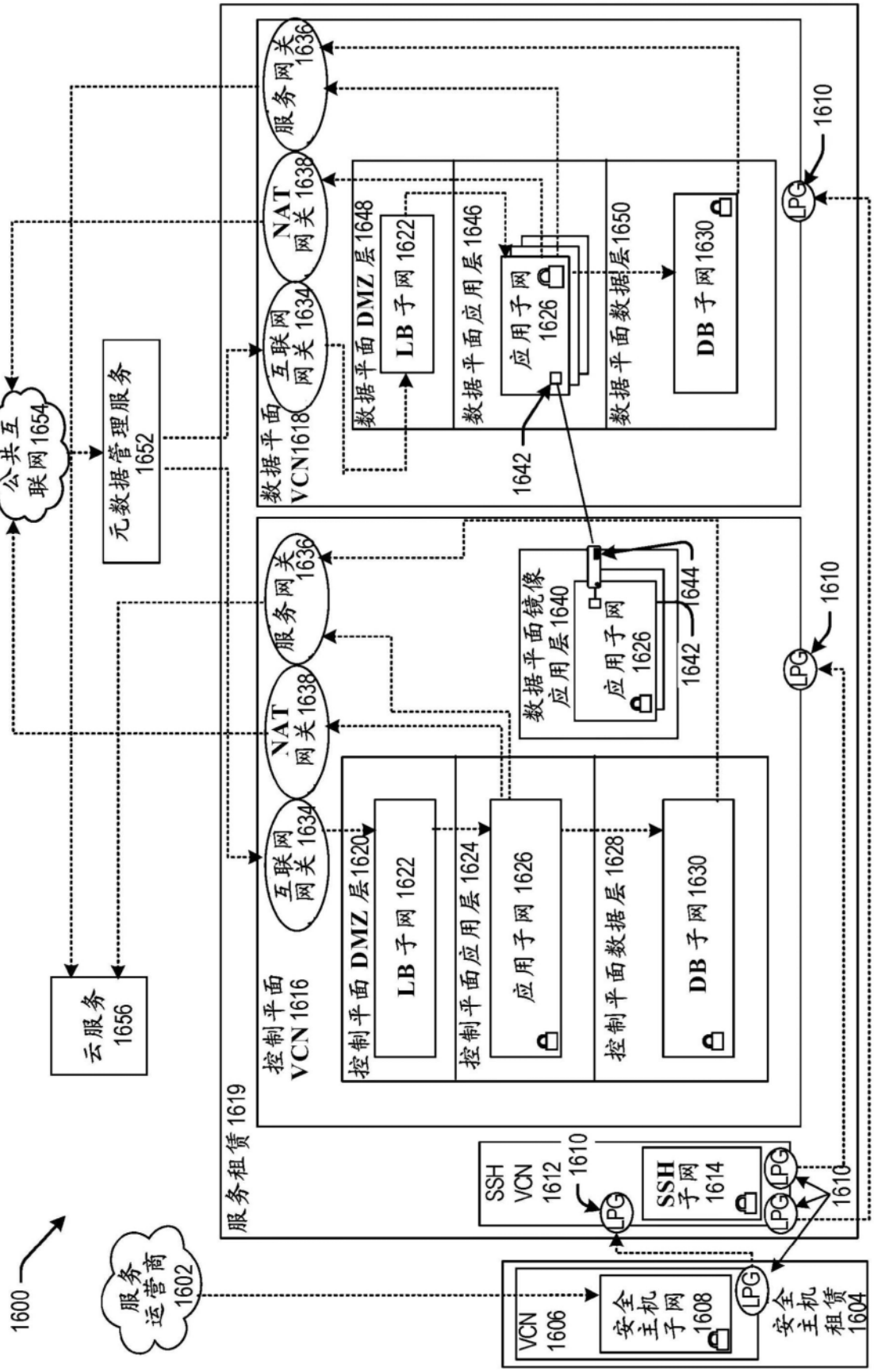

1600
服务运营商 1602
公共互联网 1654
元数据管理服务 1652
云服务 1656
服务租赁 1619
控制平面 VCN 1616
互联网网关 1634
NAT 网关 1638
服务网关 1636
控制平面 DMZ 层 1620
LB 子网 1622
控制平面应用层 1624
应用子网 1626
控制平面数据层 1628
DB 子网 1630
数据平面镜像应用层 1640
1642
1644
数据平面 VCN 1618
数据平面 DMZ 层 1648
数据平面应用层 1646
数据平面数据层 1650
SSH VCN 1612
SSH 子网 1614
1610
LPG
VCN 1606
安全主机子网 1608
安全主机租赁 1604

图16

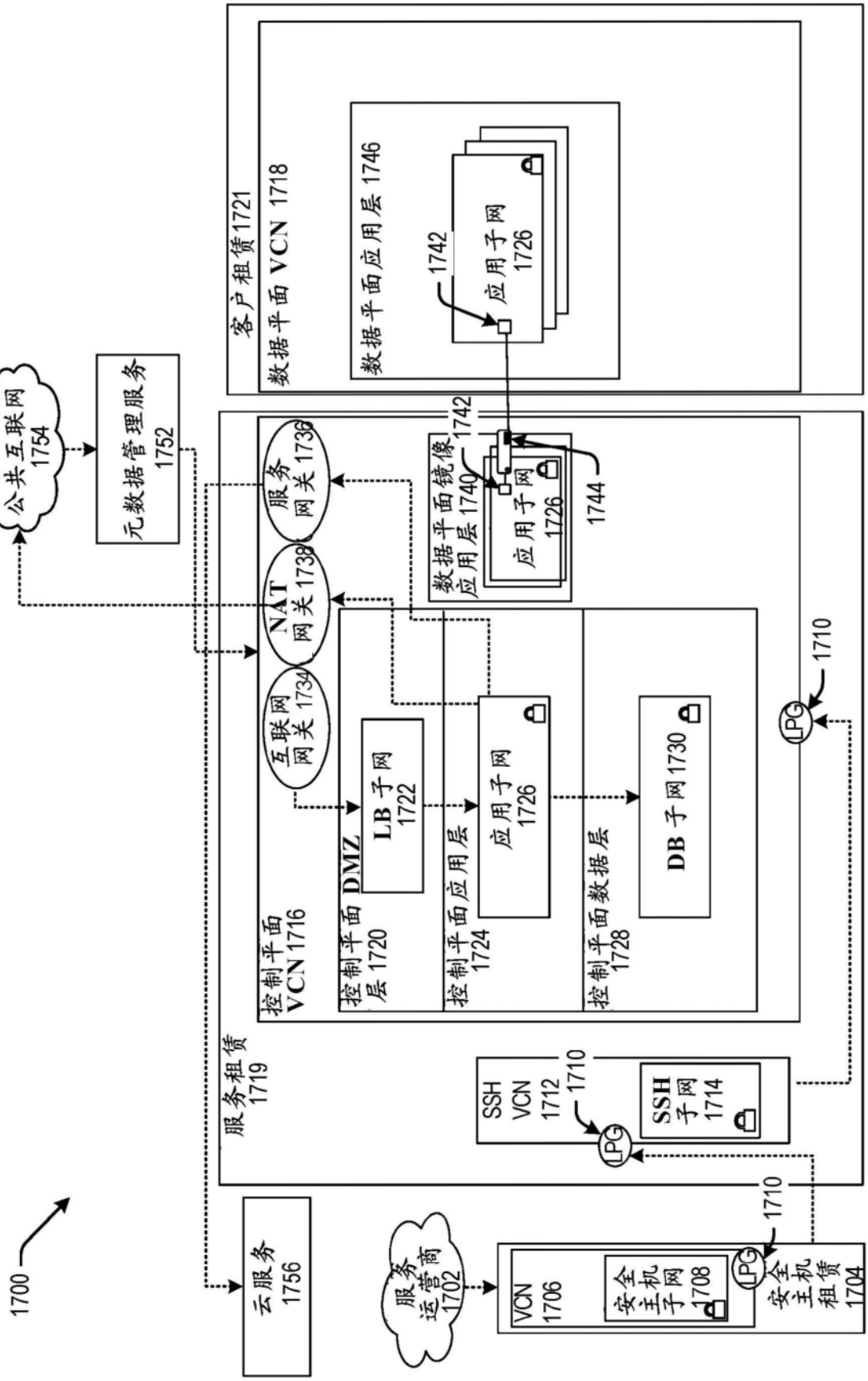

1700
公共互联网 1754
元数据管理服务 1752
云服务 1756
服务运营商 1702
客户租赁1721
数据平面 VCN 1718
数据平面应用层 1746
1742
应用子网 1726
数据平面镜像 应用层 1740
1744
服务租赁 1719
控制平面 VCN 1716
服务网关 1736
NAT 网关 1738
互联网网关 1734
DMZ
LB 子网 1722
控制平面 层 1720
控制平面应用层 1724
控制平面数据层 1728
DB 子网 1730
SSH VCN 1712
SSH 子网 1714
VCN 1706
安全主机子网 1708
安全主机租赁 1704
LPG
1710

图17

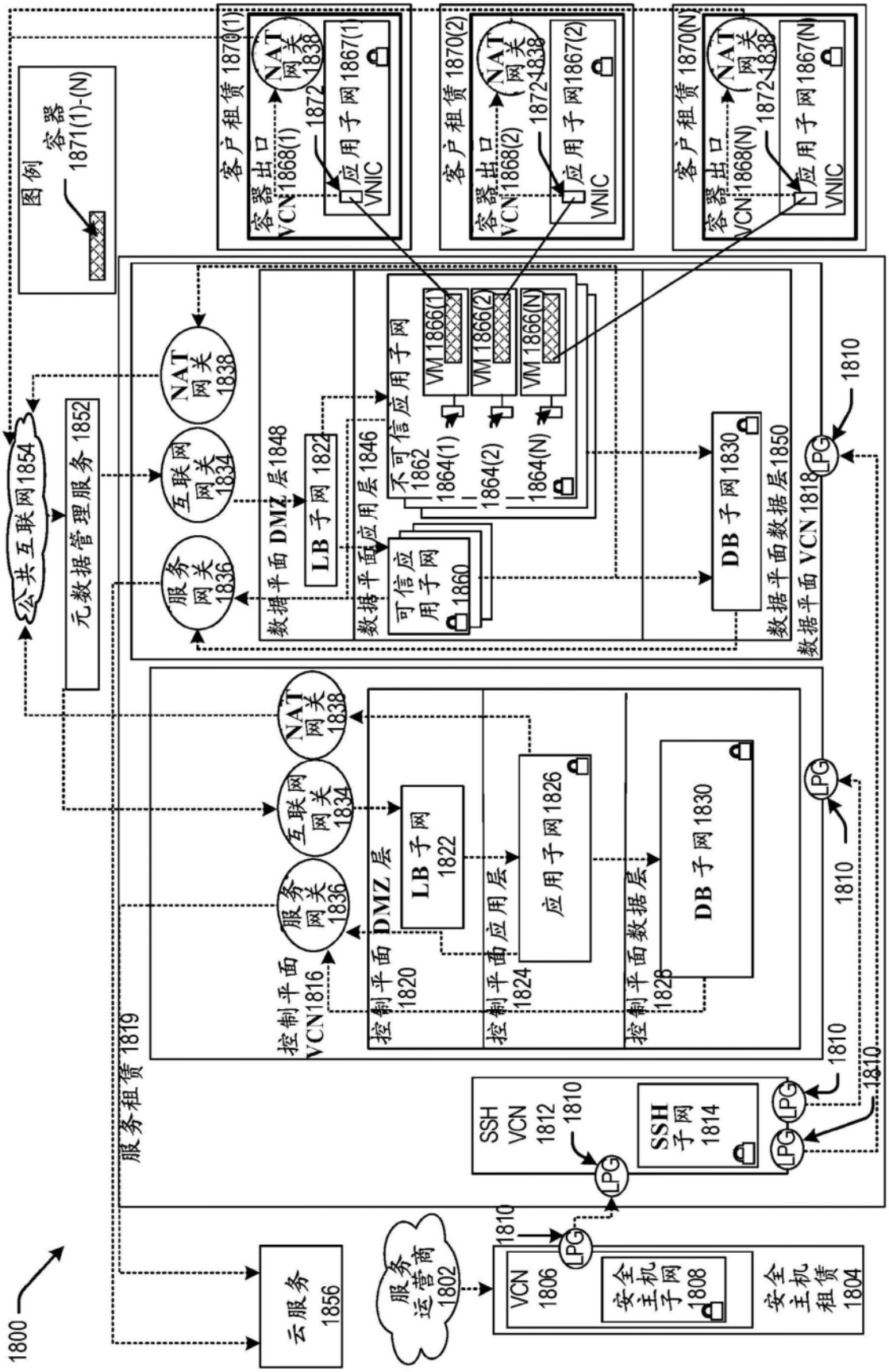

1800
云服务 1856
服务运营商 1802
VCN 1806
安全主机子网 1808
安全主机租赁 1804
SSH VCN 1812
SSH 子网 1814
服务租赁 1819
控制平面 VCN1816
控制平面 DMZ 层 1820
LB 子网 1822
控制平面应用层 1824
应用子网 1826
控制平面数据层 1828
DB 子网 1830
数据平面 DMZ 层 1848
数据平面应用层 1846
数据平面数据层 1850
数据平面 VCN 1818
可信应用子网 1860
不可信应用子网 1862
VM 1866(1)
VM 1866(2)
VM 1866(N)
1864(1)
1864(2)
1864(N)
客户租赁 1870(1)
客户租赁 1870(2)
客户租赁 1870(N)
容器出口 VCN 1868(1)
容器出口 VCN 1868(2)
容器出口 VCN 1868(N)
应用子网 1867(1)
应用子网 1867(2)
应用子网 1867(N)
VNIC
NAT 网关 1838
互联网网关 1834
服务网关 1836
公共互联网 1854
元数据管理服务 1852
图例
容器 1871(1)-(N)
LPG
1810

图18

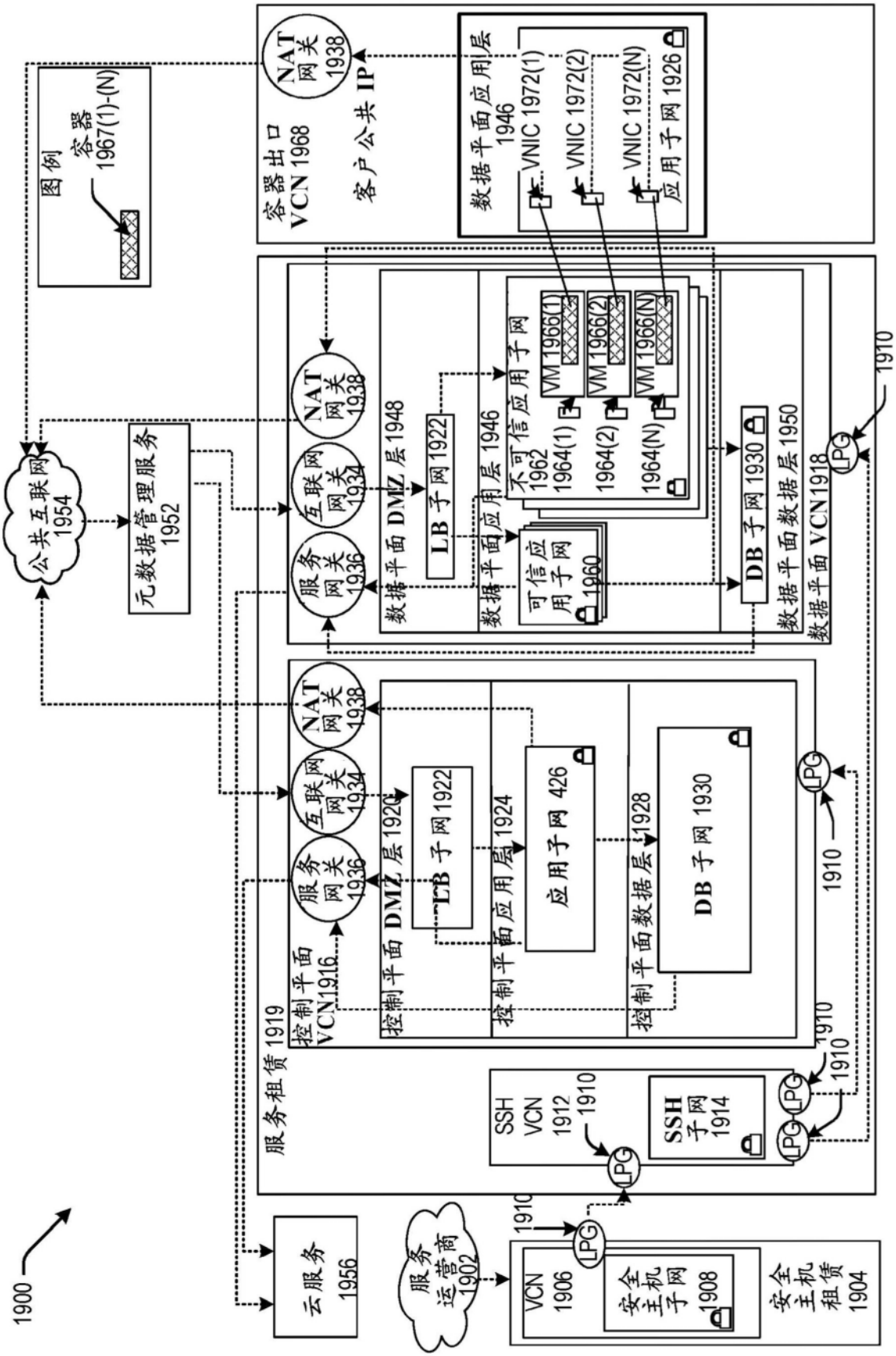

1900
图例
容器
1967(1)-(N)
容器出口
VCN 1968
客户公共 IP
NAT
网关
1938
数据平面应用层
1946
VNIC 1972(1)
VNIC 1972(2)
VNIC 1972(N)
应用子网 1926
公共互联网
1954
元数据管理服务
1952
互联网
网关
1934
服务
网关
1936
数据平面 DMZ 层 1948
LB 子网 1922
数据平面应用层 1946
可信应用子网
1960
不可信应用子网
1962
VM 1966(1)
VM 1966(2)
VM 1966(N)
1964(1)
1964(2)
1964(N)
DB 子网 1930
数据平面数据层 1950
数据平面 VCN 1918
LPG
1910
服务租赁 1919
控制平面
VCN 1916
控制平面 DMZ 层 1920
LB 子网 1922
控制平面应用层 1924
应用子网 426
控制平面数据层 1928
DB 子网 1930
SSH
VCN
1912
SSH
子网
1914
云服务
1956
服务
运营商
1902
VCN
1906
安全
主机
子网
1908
安全
主机
租赁
1904

图19

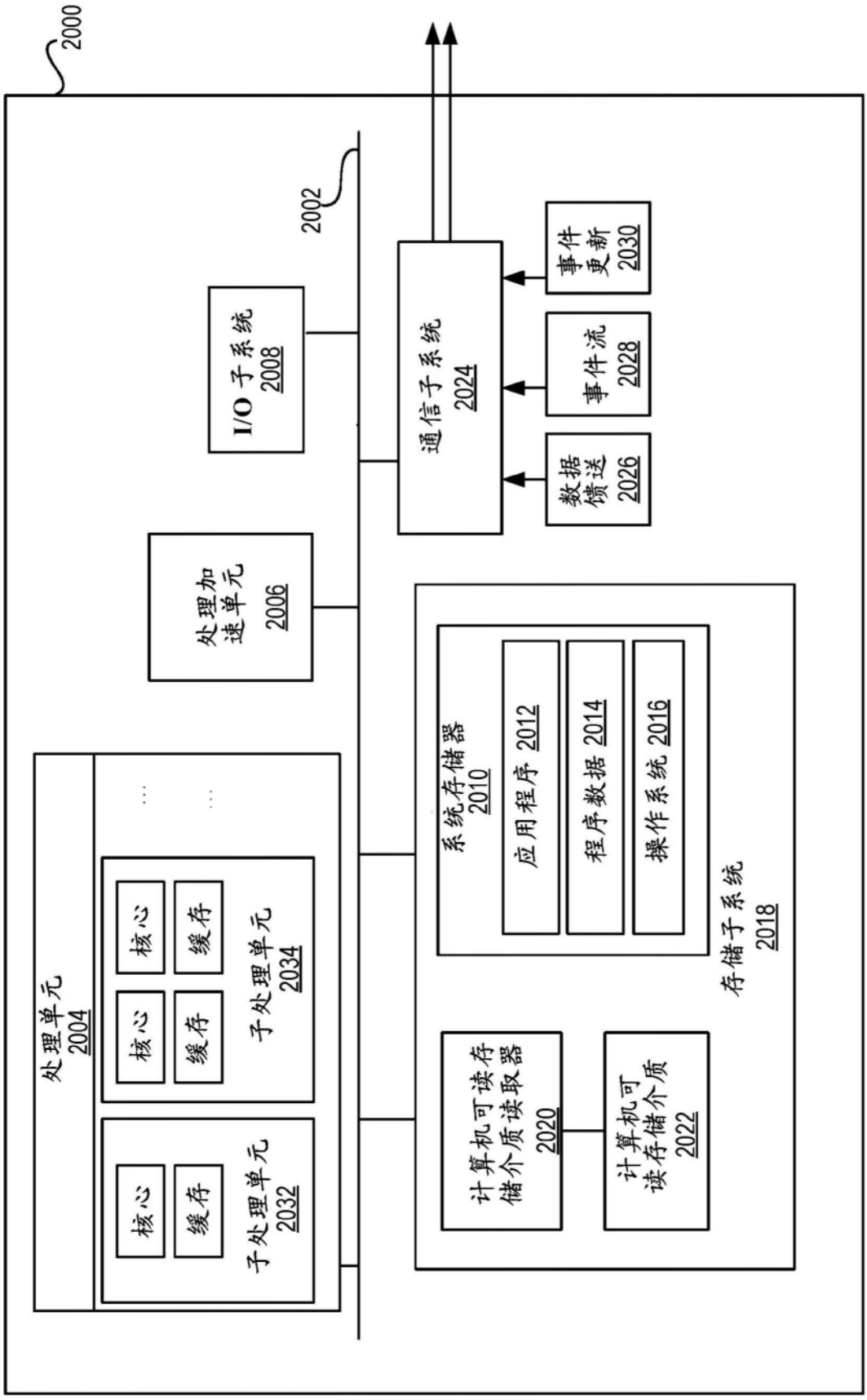

2000
2002
I/O 子系统 2008
通信子系统 2024
事件更新 2030
事件流 2028
数据馈送 2026
处理加速单元 2006
处理单元 2004
核心
缓存
子处理单元 2032
子处理单元 2034
系统存储器 2010
应用程序 2012
程序数据 2014
操作系统 2016
存储子系统 2018
计算机可读存储介质读取器 2020
计算机可读存储介质 2022

图20