(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115989660 B
(45)授权公告日 2024.04.12

(21)申请号 202180051521.8
(22)申请日 2021.08.04
(65)同一申请的已公布的文献号
申请公布号 CN 115989660 A
(43)申请公布日 2023.04.18
(30)优先权数据
63/068,943 2020.08.21 US
63/068,945 2020.08.21 US
17/393,347 2021.08.03 US
(85)PCT国际申请进入国家阶段日
2023.02.21
(86)PCT国际申请的申请数据
PCT/US2021/044456 2021.08.04
(87)PCT国际申请的公布数据
WO2022/039925 EN 2022.02.24
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 I·多左瑞茨 T·阿尔瑞赫姆
J·童 L·库珀曼
N·R·波特兰普里 B·G·钱德朗
B·普拉蒂 N·格拉斯
G·纳嘎拉加 J·J·纳达尔
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 刘前红
(51)Int.Cl.
H04L 9/40(2022.01)
(56)对比文件
CN 103118053 A,2013.05.22
CN 109196505 A,2019.01.11
CN 110192198 A,2019.08.30
EP 2880837 B1,2019.10.30
US 2016028737 A1,2016.01.28
US 2019384645 A1,2019.12.19
审查员 刘锐

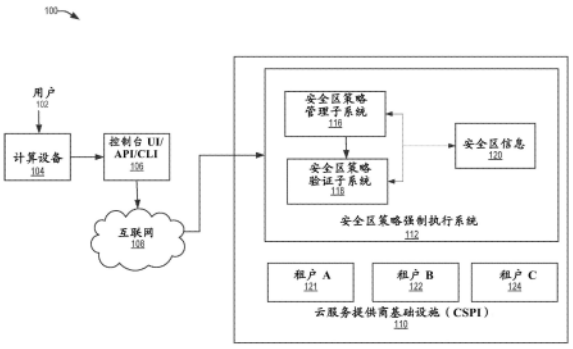
权利要求书3页 说明书32页 附图17页

(54)发明名称

云基础设施系统中的安全区策略强制执行

(57)摘要

公开了一种基于云的安全解决方案,该解决方案提供用于管理和强制执行与云中被管理的各种资源相关的安全策略的稳健且安全的框架。基于云的安全解决方案由云服务提供商基础设施中的安全区策略强制执行系统实现。系统接收对资源执行操作的请求并确定与该资源相关联的隔间。系统确定隔间与安全区相关联并确定适用于该资源的一组一个或多个安全区策略。系统然后基于所述一组一个或多个安全区策略确定对资源的操作不被准许,并且响应于确定对资源的操作不被准许,允许对资源执行操作。



CN 115989660 B

1.一种安全区策略强制执行方法,包括:

由云服务提供商基础设施中的安全区策略强制执行系统接收对资源执行操作的请求;

由安全区策略强制执行系统确定与所述资源相关联的隔间,所述隔间与一组一个或多个隔间策略相关联;

由安全区策略强制执行系统基于所述一组一个或多个隔间策略确定对所述资源的所述操作被准许;

响应于基于所述一组一个或多个隔间策略确定对所述资源的所述操作被准许,由安全区策略强制执行系统确定所述隔间与安全区相关联,所述安全区与一组一个或多个安全区策略相关联;

由安全区策略强制执行系统基于所述一组一个或多个安全区策略确定对所述资源的所述操作是否被准许;

在基于所述一组一个或多个安全区策略确定对所述资源的所述操作不被准许时,由安全区策略强制执行系统不允许对所述资源执行所述操作。

2.如权利要求1所述的安全区策略强制执行方法,其中确定与所述资源相关联的隔间还包括确定与所述资源相关联的隔间的隔间标识符。

3.如权利要求1所述的安全区策略强制执行方法,其中适用于所述资源的所述一组一个或多个隔间策略包括与所述隔间相关联的一个或多个隔间策略和与在层次上与该隔间相关的一个或多个父隔间相关联的一个或多个隔间策略的联合。

4.如权利要求1所述的安全区策略强制执行方法,还包括:

在基于所述一组一个或多个安全区策略确定对所述资源的所述操作被准许时,允许对所述资源执行所述操作。

5.如权利要求1所述的安全区策略强制执行方法,其中适用于所述资源的所述一组一个或多个安全区策略包括与安全区相关联的一个或多个安全区策略和与在层次上与所述安全区相关的一个或多个父安全区相关联的一个或多个安全区策略的联合。

6.如权利要求1所述的安全区策略强制执行方法,其中所述一组一个或多个安全区策略中的安全区策略被表示为一组一个或多个表达式,其中所述一组表达式中的每个表达式包括一组一个或多个条件,并且其中所述一组一个或多个条件中的每个条件指定关于要对所述资源执行的所述操作的限制。

7.如权利要求6所述的安全区策略强制执行方法,其中所述限制指定要求对所述资源进行加密的准则、限制所述资源从所述资源所在的隔间移动的准则或禁止从公共互联网访问所述资源的准则。

8.如权利要求7所述的安全区策略强制执行方法,其中所述限制指定与和所述资源相关联的一个或多个次要资源相关的准则,其中所述一个或多个次要资源影响所述资源的操作。

9.如权利要求1所述的安全区策略强制执行方法,其中所述一组一个或多个安全区策略禁止要对所述资源执行的所述操作的特定配置。

10.如权利要求1所述的安全区策略强制执行方法,还包括由安全区策略强制执行系统向用户传输结果,所述结果指示对所述资源成功执行了所述操作。

11.如权利要求1所述的安全区策略强制执行方法,还包括由安全区策略强制执行系统

向用户传输结果,所述结果指示未成功地对所述资源执行所述操作。

12.如权利要求1所述的安全区策略强制执行方法,其中基于所述一组一个或多个安全区策略确定对所述资源的所述操作是否被准许包括基于所述一组一个或多个安全区策略确定对所述资源的所述操作不被准许。

13.如权利要求1所述的安全区策略强制执行方法,其中所述云服务提供商基础设施至少包括第一租户和第二租户,并且其中第一租户的第一隔间和第二租户的第一隔间与安全区策略强制执行系统所实现的多个安全区中的第一安全区相关联。

14.一种云服务提供商基础设施中的安全区策略强制执行系统,包括:

处理器;以及

存储指令的存储器,指令当被处理器执行时将系统配置为:

接收对资源执行操作的请求;

确定与所述资源相关联的隔间,所述隔间与一组一个或多个隔间策略相关联;

基于所述一组一个或多个隔间策略确定对所述资源的所述操作被准许;

响应于基于所述一组一个或多个隔间策略确定对所述资源的所述操作被准许,确定所述隔间与安全区相关联,所述安全区与一组一个或多个安全区策略相关联;

基于所述一组一个或多个安全区策略确定对所述资源的所述操作是否被准许;以及

在基于所述一组一个或多个安全区策略确定对所述资源的所述操作不被准许时,不允许对所述资源执行所述操作。

15.如权利要求14所述的安全区策略强制执行系统,还包括用于确定与所述资源相关联的隔间的隔间标识符的指令。

16.如权利要求14所述的安全区策略强制执行系统,其中所述一组一个或多个安全区策略中的安全区策略被表示为一组一个或多个表达式,其中所述一组表达式中的每个表达式包括一组一个或多个条件,并且其中所述一组一个或多个条件中的每个条件指定关于要对所述资源执行的所述操作的限制。

17.一种具有存储在其上的程序代码的非暂态计算机可读介质,所述程序代码可由一个或多个处理设备执行以执行操作,所述操作包括:

由提供对云服务提供商基础设施中的资源的安全访问的安全区策略强制执行系统接收将隔间与安全区相关联的第一请求,所述隔间与一组一个或多个隔间策略相关联;

响应于第一请求,由安全区策略强制执行系统将所述隔间与所述安全区相关联,所述安全区与一组一个或多个安全区策略相关联;并且其中

作为将所述隔间与所述安全区相关联的结果,所述隔间与所述一组一个或多个安全区策略以及所述一组一个或多个隔间策略相关联;并且其中

如果基于所述一组一个或多个隔间策略和所述一组一个或多个安全区策略中的至少一者确定对所述资源的所述操作不被准许时,不允许在所述隔间内对所述资源执行所述操作。

18.如权利要求17所述的非暂态计算机可读介质,其中所述操作还包括:

由安全区策略强制执行系统接收向所述隔间添加另一资源的第二请求;以及

响应于第二请求,由安全区策略强制执行系统至少部分地基于所述一组一个或多个隔间策略和所述一组一个或多个安全区策略来确定对所述另一资源的访问。

19.如权利要求17所述的非暂态计算机可读介质,其中所述一组一个或多个安全区策略禁止要对所述资源执行的一组操作或禁止要对所述资源执行的操作的特定版本。

20.如权利要求17所述的非暂态计算机可读介质,其中所述一组一个或多个安全区策略中的安全区策略被表示为一组一个或多个表达式,其中所述一组表达式中的每个表达式包括一组一个或多个条件,并且其中所述一组一个或多个条件中的每个条件指定关于要对所述资源执行的操作的限制。

21.如权利要求17所述的非暂态计算机可读介质,其中如果对所述资源的所述操作基于所述一组一个或多个隔间策略被准许并且基于所述一组一个或多个安全区策略不被准许,则不允许在所述隔间内对所述资源执行所述操作。

云基础设施系统中的安全区策略强制执行

[0001] 相关申请的交叉引用

[0002] 本申请要求2021年8月3日提交的标题为“Security Zone Policy Enforcement in a cloud infrastructure system”的美国非临时申请No.17/393,347的优先权。美国非临时申请No.17/393,347的内容出于所有目的通过引用整体并入本文。

[0003] 本申请根据35U.S.C.119(e)要求2020年8月21日提交的标题为“Secure Resource Provisioning in a virtual computing environment”的美国临时申请No.63/068,943和2020年8月21日提交的标题为“Secure Resource Provisioning in a virtual computing environment using intention based security policies”的美国临时申请No.63/068,945的权益和优先权,其全部内容出于所有目的通过引用并入本文。

背景技术

[0004] 一般而言,基于云的应用(例如,企业公共云应用、第三方云应用等)的使用正在飙升,访问来自于各种设备(例如,桌面和移动设备)以及各种用户(例如,员工、合作伙伴、客户等)。对于向云过渡的公司和企业,云服务提供商必须能够为其用户提供稳健的安全解决方案。基于云的安全服务提供了允许公司和企业利用云计算的众多优势、同时保持安全并确保满足数据隐私和合规性要求的安全解决方案。由于基于云的服务和基于云的应用具有丰富的多样性和可访问性,因此需要由云提供商安全地管理的云资源的量持续快速增长。需要改进现有的用于安全地配置和管理云中资源的基于云的安全服务,以提供对云中资源的更加稳健、安全且可靠的访问。

发明内容

[0005] 本公开一般而言涉及基于云的安全解决方案。更具体而言,但不作为限制,本公开描述了一种基于云的安全解决方案,其提供用于管理和强制执行与在云中管理的各种资源相关的安全策略的稳健且安全的框架。

[0006] 在某些实施例中,公开了云服务提供商基础设施中的安全区(security zone)策略强制执行系统。安全区策略强制执行系统接收对资源执行操作的请求,并确定与该资源相关联的隔间(compartment)。系统确定隔间与安全区相关联并确定适用于该资源的一组一个或多个安全区策略。系统然后基于该组一个或多个安全区策略确定对资源的操作被准许,并且响应于确定对资源的操作被准许而允许对资源执行操作。

[0007] 在某些示例中,系统确定与资源相关联的隔间的隔间标识符和适用于资源的一组一个或多个隔间策略。适用于资源的该组一个或多个隔间策略包括与隔间相关联的一个或多个隔间策略和与在层次上与隔间相关的一个或多个父隔间相关联的一个或多个隔间策略的联合(union)。

[0008] 在某些示例中,系统基于所述一组一个或多个隔间策略确定对资源的操作被准许,并且响应于基于所述一组一个或多个隔间策略确定对资源的操作被准许,确定隔间与安全区相关联。

[0009] 在某些示例中,系统包括基于所述一组一个或多个隔间策略确定对资源的操作不被准许,并且响应于该确定,不允许对资源执行操作。在某些示例中,系统包括基于所述一组安全区策略确定对资源的操作不被准许,并且响应于该确定,不允许对资源执行该操作。

[0010] 在某些示例中,适用于资源的所述一组一个或多个安全区策略包括与安全区相关联的一个或多个安全区策略和与在层次上与安全区相关的一个或多个父安全区相关联的一个或多个安全区策略的联合。

[0011] 在某些示例中,所述一组一个或多个安全区策略中的安全区策略被表示为一组一个或多个表达式。该组表达式中的每个表达式包括一组一个或多个条件,并且该组一个或多个条件中的每个条件指定关于要对资源执行的操作的限制。在某些示例中,限制指定要求对资源进行加密的准则、限制资源从资源所在的隔间移动的准则或禁止从公共互联网访问该资源的准则。在某些示例中,限制指定与和资源相关联的一个或多个次要资源相关的准则,其中该一个或多个次要资源影响资源的操作。在某些示例中,所述一组一个或多个安全区策略禁止要对资源执行的操作的特定配置。

[0012] 在某些示例中,系统向用户发送指示已成功地对资源执行操作的结果。在某些示例中,结果指示没有成功地对资源执行操作。

[0013] 在某些示例中,系统接收将隔间与安全区相关联的请求。隔间与一组一个或多个隔间策略相关联。响应于该请求,系统将隔间与安全区相关联。安全区与一组一个或多个安全区策略相关联。作为关联的结果,隔间与一组一个或多个安全区策略以及一组一个或多个隔间策略相关联。在某些示例中,系统接收将资源添加到隔间的请求,并且响应于该请求,至少部分地基于所述一组一个或多个隔间策略和所述一组一个或多个安全区策略来确定对资源的访问。在某些示例中,所述一组一个或多个安全区策略禁止要对资源执行的一组操作或禁止要对资源执行的操作的特定版本。

[0014] 在某些实施例中,公开了云服务提供商基础设施(CSPI)中的集中式应用编程接口(API)请求处理系统。API请求处理系统接收标识要对CSPI中的资源执行的操作的API请求。系统根据API请求确定与资源相关联的隔间信息和上下文信息。响应于确定与资源相关联的隔间信息和上下文信息,系统确定资源驻留在与安全区相关联的隔间中。系统然后处理API请求并将API请求的处理结果发送到集中式API处理系统的用户。

[0015] 在某些示例中,系统根据API请求确定主要资源。在某些示例中,主要资源是API请求中标识的资源。系统确定受API请求影响的次要资源。次要资源是与主要资源相关联的资源。在某些示例中,次要资源没有作为API请求的一部分被标识。

[0016] 在某些示例中,隔间信息包括隔间标识符和与API请求中标识的主要资源相关联的一组一个或多个隔间策略。在某些示例中,上下文信息与受API请求影响的次要资源相关联。上下文信息可以包括与次要资源相关联的资源标识符、与次要资源相关联的隔间标识符或与次要资源相关联的资源状态。在某些示例中,上下文信息标识CSPI中被配置为执行API请求的下游服务。

[0017] 在某些示例中,系统基于与资源相关联的隔间信息和上下文信息确定准许对API请求中标识的资源执行操作,并且响应于该确定,确定资源驻留在与安全区相关联的隔间中。在某些示例中,集中式API处理系统对API请求的处理包括将API请求和与资源相关联的隔间信息发送到安全区策略强制执行系统以供处理。该处理还包括由集中式API处理系统

从安全区策略强制执行系统接收对API请求的处理结果。在某些示例中,结果指示准许对资源执行该操作。在某些示例中,结果指示不准许对资源执行该操作。在某些示例中,集中式API处理系统将结果发送给用户。在某些示例中,处理API请求包括由安全区策略强制执行系统评估与隔间的安全区相关联的一组一个或多个安全区策略。

[0018] 在某些示例中,在确定与资源相关联的隔间信息和上下文信息之前,系统确定用户被授权对API请求中标识的资源执行操作。在某些示例中,与资源相关联的隔间信息和上下文信息被存储在与API请求相关联的安全区规范中。

[0019] 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、代码或指令等的非暂态计算机可读存储介质。提及这些说明性实施例不是为了限制或定义本公开,而是为了提供示例以帮助理解本公开。在详细描述中讨论了附加的实施例,并且在那里提供了进一步的描述。

附图说明

[0020] 当参考附图阅读以下详细描述时,将更好地理解本公开的特征、实施例和优点。

[0021] 图1描绘了根据某些实施例的包括云服务提供商基础设施(CSPI)的计算环境的高级图示,该CSPI包括用于提供用于管理和强制执行与由CSPI管理的各种资源相关的安全策略的安全框架的能力。

[0022] 图2是根据某些实施例的计算环境200的示例性图示,计算环境200包括由图1中所示的安全区策略管理子系统116提供的安全框架。

[0023] 图3描绘了根据某些实施例的由图1中所示的CSPI中的安全区策略管理子系统116执行的过程300的示例。

[0024] 图4描绘了根据某些实施例的由图1中所示的CSPI中的安全区策略验证子系统执行的过程400的示例。

[0025] 图5A是根据某些实施例的由图1中所示的CSPI的租户的用户创建的隔间继承隔间策略的示例性图示。

[0026] 图5B是根据某些实施例的由图1中所示的CSPI的租户创建的隔间继承与安全区相关联的安全区策略的示例性图示。

[0027] 图6描绘了根据某些实施例的包括云服务提供商基础设施(CSPI)110的计算环境600的高级图示,CSPI 110包括集中式API请求处理系统和安全区策略强制执行系统,用于提供安全框架以启用对由CSPI管理的各种资源的安全访问。

[0028] 图7描绘了根据某些实施例的由集中式API请求处理系统执行的用于向用户提供对由CSPI管理的各种资源的安全访问的过程700的示例。

[0029] 图8描绘了根据某些实施例的由安全区策略强制执行系统112执行的处理的过程800的示例,以基于评估与资源相关联的一组安全区策略来确定是否允许对资源执行操作。

[0030] 图9是例示了根据某些实施例的集中式API请求处理系统与图6中所示的一个或多个其它系统之间为了向用户提供对由CSPI管理的各种资源的安全访问而进行的交互的顺序图。

[0031] 图10是根据某些实施例的与标识用于使用图6中所示的CSPI中的计算服务来启动计算实例资源的操作的API请求对应的安全区规范的示例。

[0032] 图11是根据某些实施例的与标识用于将卷(volume)附连到实例、将引导卷(boot volume)附连到实例以及使用CSPI中的计算服务改变用于实例的隔间标识符的操作的API请求对应的安全区规范的示例。

[0033] 图12是根据某些实施例的与标识用于创建子网、创建互联网网关、改变用于子网的隔间标识符和以及使用CSPI中的计算服务来改变用于互联网网关的隔间标识符的操作的API请求对应的安全区规范的示例。

[0034] 图13是例示了根据至少一个实施例的IaaS体系架构的示例模式的框图1300。

[0035] 图14是例示了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1400。

[0036] 图15是例示了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1500。

[0037] 图16是例示了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1600。

[0038] 图17图示了其中可以实现各种实施例的示例计算机系统1700。

具体实施方式

[0039] 在下面的描述中,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性的。“示例性”一词在本文中的意思是“用作示例、实例或说明”。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于其它实施例或设计,或比其有优势。

[0040] 本公开一般而言涉及基于云的安全解决方案。更具体而言,但不作为限制,本公开描述了一种基于云的安全解决方案,该解决方案提供用于管理和强制执行与在云中管理的各种资源相关的安全策略的稳健且安全的框架。

[0041] 随着每天越来越多的企业将他们的数据中心和应用迁移到云端,云数据安全变得越来越重要。基于云的安全解决方案通过全面的数据安全策略确保为其用户实现高质量的云数据安全。例如,身份和访问管理(IAM)是云中提供的常见类型的安全解决方案。IAM技术通过定义策略来确保云数据安全性,通过这些策略可以管理用户身份以规范用户对云中资源的访问。IAM策略可以被配置为定义限制用户访问他们无权访问的资源的能力和/或限制用户在云中执行某些动作/操作的能力的用户角色。

[0042] 现有的基于云的安全解决方案在为用户提供用于配置、访问和管理云中的资源(例如,网络、服务器、存储、应用和服务)的稳健和安全框架的能力方面受到限制。例如,采用IAM策略的基于云的安全解决方案通常是特定于用户/组的,并且绑定到请求访问的用户的身份。例如,企业或云提供商的管理员可以定制某组用户(例如,属于企业内的特定部门的用户)的访问特权,使得特定的一组用户始终可以基于他们在企业中的角色/身份被提供对某些资源的访问。这会损害企业的整体安全性需求,尤其是在企业需要确保访问受到严格监管以便为企业提供稳健的数据安全性控制时。此外,IAM技术的使用要求企业或云的管理员维护其所有用户的更新和同步的信息。这需要管理敏感的身份信息并引起企业的隐私担忧。

[0043] 在本公开中描述的基于云的安全解决方案提供了优于常规的基于云的安全服务

的若干技术进步和/或改进。基于云的安全解决方案提供了稳健且安全的框架,用于管理和强制执行与由云服务提供商(CSP)管理的各种资源相关的安全策略。所公开的安全框架包括一组安全区和安全区策略,这些安全区策略可以在被企业的用户访问的云中的一组资源上强制执行。对该组资源的访问由一组安全区策略支配并且不绑定到访问资源的用户的身份。因此,如果违反了与资源相关联的一组安全区策略,那么可能被IAM策略准许访问某个资源(和/或对资源执行操作)的用户可能会被所公开的安全解决方案拒绝访问。安全区策略基于“拒绝语义”,其旨在不允许企业的任何用户对一组资源执行某些动作或操作。这与现有IAM授权策略采用的传统“允许语义”形成对比,后者允许特定用户基于用户在企业内的角色/身份对资源执行特定动作。

[0044] 在某些示例中,所公开的基于云的安全解决方案由云服务提供商基础设施(CSPI)内的安全区策略强制执行系统实现,CSPI使用由CSP提供的系统和基础设施(云基础设施)按需将安全区策略强制执行系统提供给用户或客户(例如,经由订阅模式)。所公开的安全区策略强制执行系统为企业的用户提供了用于安全地配置、访问和管理他们在云中的资源的稳健和安全的框架。资源可以包括但不限于由CSPI在分布式环境中托管的计算、联网、对象存储或数据库资源。在下面的附图及其随附描述中描述了与由安全区策略强制执行系统执行的实施方式和处理相关的细节。

[0045] 云服务提供商基础设施(CSPI)中的安全区策略强制执行系统

[0046] 现在参考附图,图1描绘了根据某些实施例的包括云服务提供商基础设施(CSPI)110的计算环境100的高级图示,CSPI 110包括用于提供用于管理和强制执行与由CSPI管理的各种资源相关的安全策略的安全框架的能力。在某些实施例中,安全框架由CSPI 110内的安全区策略强制执行系统112提供。由CSPI管理的资源可以包括但不限于由CSPI 110托管在分布式环境中的计算、联网、对象存储或数据库资源。CSPI 110的用户102可以使用这些资源构建他们自己的网络。例如,用户可以使用由CSPI 110提供的资源来构建一个或多个可定制且私有的网络,称为虚拟云网络(VCN)(在本文也称为“虚拟客户网络”)。用户可以在这些VCN上部署一个或多个资源,诸如计算实例。计算实例可以采用虚拟机、裸机实例等形式。

[0047] 安全区策略强制执行系统112可以由一个或多个计算系统来实现,该一个或多个计算系统执行计算机可读指令(例如,代码、程序)以实现安全区策略强制执行系统112。如图1中所描绘的,安全区策略强制执行系统112包括各种子系统,包括安全区策略管理子系统116和安全区策略验证子系统118。由安全区策略强制执行系统112作为其处理的一部分使用或生成的数据或信息的部分可以包括安全区信息120,该安全区信息120可以由安全区策略强制执行系统112存储在一个或多个数据库或文件中。图1中描绘的系统和子系统可以使用由计算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)、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)。

[0048] 安全区策略强制执行系统112可以以各种不同的配置来实现。在图1中所描绘的实施例中,安全区策略强制执行系统112在CSPI 110中的一个或多个服务器上实现,并且其安全的资源访问和管理服务可以在订阅的基础上提供给云服务的订户。图1中描绘的计算环境100仅仅是示例,并且非意在不当地限制要求保护的实施例的范围。本领域普通技术人员

将认识到许多可能的变化、替代和修改。例如,在一些实施方式中,安全区策略强制执行系统112可以使用比图1中所示的子系统更多或更少的子系统来实现,可以组合两个或更多个子系统,或者可以具有子系统的不同配置或布置。

[0049] 在图1中所描绘的实施例中,安全区策略强制执行系统112包括安全区策略管理系统116和安全区策略验证子系统118。安全区策略管理系统116包括提供用于管理与CSPI中的各种资源(例如,计算、联网、对象存储或数据库资源)相关的安全策略的安全框架的能力。在某些示例中,由安全区策略管理子系统116提供的安全框架包括安全区信息120,该安全区信息120可以由一组安全区和与该组安全区相关联的一组安全区策略组成。“安全区”可以指由安全区策略管理子系统116管理的安全框架中被设计为对驻留在CSPI 100中的隔间中的一组资源强制执行隐式和显式的安全区策略的专门区域。安全区策略防止要对驻留在隔间中的一组资源执行的违反由安全区定义的安全性要求的某些操作。“隔间”可以指用于组织和控制对由CSPI 110管理的资源的访问的逻辑容器。隔间可以与限制对驻留在隔间中的资源的使用的一组隔间策略相关联。该组隔离策略中的每个策略可以影响CSPI中的一个或多个资源,诸如计算、联网、对象存储和数据库资源。隔间内的资源可以根据各种准则被逻辑组织。例如,隔间内的资源可以基于由CSPI提供的特定服务(例如,计算、存储器和联网服务)、基于用户的企业内的部门(工程、人力资源、IT等)等被逻辑组织。准则可以由与CSPI 110的客户/租户(例如,120、122或124)相关联的用户(例如,管理员)102指定。由安全区策略管理子系统116实现的包括安全区和安全区策略的安全框架的示例在图2中详细描述。

[0050] 在某些实施例中,安全区策略管理系统116包括将隔间与安全区相关联、将资源添加到与安全区相关联的隔间、查看与安全区相关联的安全区策略、指定安全区作为“最大安全区”等的能力。“最大安全区”可以表示被配置为包括由安全区策略强制执行系统定义的所有可用安全区策略的安全区。与安全区相关联的隔间自动继承与该安全区相关联的一组安全区策略。在某些示例中,安全区策略表示附加层的安全策略,除了与隔间相关联的隔间策略之外,该附加层的安全策略也可以对驻留在隔间中的一组资源强制执行。安全区策略可以禁止对驻留在隔间中的一组资源执行整组操作、禁止对一组资源执行操作的子集,或禁止对一组资源执行操作的特定版本/配置。举例来说,基于与隔间相关联的隔间策略,用户可能被准许利用公共互联网协议(IP)地址在隔间中创建资源(例如,计算实例),但是基于与隔间相关联的安全区策略,可能不被准许利用公共IP地址创建资源。图2中描述了安全区策略管理系统116实现安全区策略的附加细节。

[0051] 安全区策略验证子系统118包括用于评估是否可以对驻留在与安全区相关联的隔间中的资源执行操作的能力。基于评估,安全区策略验证子系统118可以准许或拒绝CSPI 110的用户对资源执行操作的能力。例如,安全区策略验证子系统118可以禁止用户尝试从公共互联网访问资源、确保用户创建的资源使用客户管理的密钥被加密,等等。

[0052] 在某些示例中,CSPI 110的用户102可以使用可能经由一个或多个通信网络可通信地耦合到CSPI 110的计算设备104与安全区策略强制执行系统112交互。计算设备可以是各种类型,包括但不限于移动电话、平板电脑、台式计算机等。用户102可以与希望利用由安全区策略强制执行系统112提供的服务来安全地管理和访问CSPI内的资源的CSPI 110的客户或租户(例如,120、122或124)相关联。用户可以使用控制台用户接口(UI)、经由应用编程

接口(API)或经由连接到用户的计算设备(例如,104)的命令行接口(CLI)106与安全区策略强制执行系统112交互以安全性地管理和访问部署在CSPI 110中的资源。例如,控制台UI可以是由安全区策略强制执行系统112提供的基于web的用户接口(UI)(或基于web的应用),以使得用户能够与安全区策略强制执行系统112交互以安全地访问和管理他们在CSPI中的资源。举例来说,用户可以与安全区策略强制执行系统112交互以创建隔间、将隔间与安全区关联、将资源添加到隔间、查看与安全区相关联的安全区策略、删除隔间、在隔间内创建子隔间、将隔间移动到同一租户内的不同父隔间、将安全区指定为"最大安全区"等。

[0053] 在某些示例中,安全区策略强制执行系统112可以被配置为从用户接收对资源执行操作的请求。例如,用户可以经由连接到用户的设备的UI发送在用户的VCN中创建或启动虚拟机实例的请求。安全区策略强制执行系统112可以处理该请求并将处理的结果发送给用户。结果可以包括已成功地能够对资源执行操作的信息、由于策略违反而无法执行操作的消息以及结果中可能包括的其它信息。结果可以例如经由连接到用户的设备104的UI输出给用户。

[0054] 图2是根据某些实施例的计算环境200的示例性图示,该计算环境200包括由图1中所示的安全区策略管理子系统116提供的安全框架。在某些示例中,安全框架包括由一组安全区202、204和206以及与该组安全区相关联的一组安全区策略208、210和212组成的安全区信息120。如前所述,"安全区"可以指被设计为强制执行隐式和显式的安全区策略的专用区,这些安全区策略防止对驻留在隔间中的一组资源执行违反由安全区定义的安全性要求的操作。在某些实施方式中,与安全区(例如,202、204或206)相关联的安全区策略(例如,208、210或212)可以被表示为一组一个或多个表达式,其中每个表达式包括一组一个或多个条件。每个表达式可以评估为真或假,并对它们包含的条件执行逻辑"与"。在某些示例中,每个条件可以指定关于可以对CSPI内的资源执行的特定操作的限制。安全区策略对其包含的所有表达式执行逻辑"或",因此如果任何表达式为真,那么安全区策略返回真值。对于安全区策略的真评估指示导致阻止在资源上准许用户的操作/所请求的操作的违反。

[0055] 举例来说,要求对安全区内的对象存储资源(例如,对象存储桶)进行加密的安全区策略可以如下表达为:

[0056] 安全区策略(对象存储资源)=expr1(context.part1)|expr2(context.part2),其中:

[0057] expr1(context.part1)=condition 1(Bucket.Encryption.Type=Symmetric)& condition 2(Bucket.Encryption.Key.Size<512)and expr2(context.part2)=condition 1(Bucket.Encryption.Key.Type=customer-managed)

[0058] 在上述示例中,安全区策略所表达的第一个表达式expr1(context.part1)包括第一条件condition 1(Bucket.Encryption.Type=Symmetric)和第二条件condition 2(Bucket.Encryption.Key.Size<512)。第一条件限制用户使用非对称的加密类型创建对象存储资源(桶)的能力。第二条件限制用户利用小于512字节的密钥创建对象存储资源的能力。由安全区策略表示的第二个表达式expr2(context.part2)包括一个条件,该条件强制执行以下要求:对象存储资源应当使用客户管理的主加密密钥而不是由对象存储服务管理的默认加密密钥来创建。

[0059] 每个表达式,expr1(context.part1)和expr2(context.part2),通过对它们包含

的条件执行逻辑“与”来评估为真或假。例如,第一个表达式expr1(context.part1)拒绝用户使用密钥尺寸小于512位密钥的对称加密创建对象存储资源的能力。第二个表达式expr2(context.part2)拒绝用户创建包括默认加密密钥的对象存储资源的能力。用于对象存储资源的安全区策略对所有表达式运行逻辑“或”,因此如果任何表达式为真,那么该策略返回真值。针对安全区策略的真评估指示导致阻止用户的动作(即,它阻止用户使用密钥尺寸小于512位密钥的对称加密创建对象存储资源或使用默认加密密钥创建对象存储资源)的违反。

[0060] 在替代实施方式中,基于资源的元数据的结构,用于对象存储资源的安全区策略的表达式也可以使用通配符来表示,如下所示:

[0061] Expr 1:*.Encryption.Type＝Symmetric&&*.Encrypti°n.Key.Size<512

[0062] 在又一种实施方式中,用于资源(例如,对象存储资源)的安全区策略的表达式可以表示为如下所示:

[0063] Expr 1:Encryption.Type＝Symmetric&&Encryption.Key.Size<512

[0064] 在某些示例中,安全区策略(例如,208、210或212)可以属于特定的安全区策略类别。每个安全区策略类别包括禁止对一组资源执行某组操作的策略。不同的安全区策略类别可以包括例如访问限制安全区策略类别、数据安全性/数据加密安全区策略类别、资源关联限制安全区策略类别、资源移动限制安全区策略类别或数据持久性安全区策略类别。下面描述各种安全区策略类别。

[0065] 访问限制安全区策略

[0066] 属于这个类别的策略的示例包括禁止在安全区中创建的资源可从公共互联网访问的策略。例如,这个类别中的策略确保安全区中的子网不能公开,互联网网关不能添加到安全区内的虚拟云网络(VCN),在安全区中创建的对象存储桶不能公开,安全区中的数据库不能指派给公共子网等。

[0067] 数据安全/数据加密安全区策略

[0068] 这个类别中的策略的示例包括要求使用客户管理的密钥对安全区中的资源进行加密的策略和要求在传输中和静止时对数据进行加密的策略。例如,这个类别中的策略确保在安全区中创建的诸如块卷、引导卷、对象存储桶和数据库之类的资源使用客户管理的主加密密钥,而不是由服务管理的默认加密密钥。此外,这个类别中的策略确保在安全区中创建的块卷、引导卷、对象存储桶和数据库使用具有特定位数的密钥进行加密。

[0069] 资源关联限制安全区策略

[0070] 这个类别中的策略的示例包括要求影响主要资源的安全态势的资源(例如,主要资源)的组成部分(例如,次要资源)也必须位于安全区中的策略。例如,这个类别中的策略确保附连到安全区中的计算实例的所有块存储卷/引导卷本身必须在安全区中,不在安全区中的计算实例不能附连到位于安全区中的块存储卷/引导卷,如果块卷/引导卷附连到不在安全区中的计算实例则不能将其移动到安全区,安全区中的计算实例必须使用也在安全区中的子网,安全区中的数据库必须使用也在安全区中的子网等等。

[0071] 资源移动限制安全区策略

[0072] 这个类别中的策略的示例包括通过不允许将某些资源从安全区移动到标准隔间(因为它可能不太安全)、不允许将现有资源从标准隔间移动到安全区(除非满足所有安全

区策略)等来确保数据完整性的策略。例如,这个类别中的策略可以确保块卷/引导卷、计算实例、子网、桶或数据库不能从安全区移动到标准隔间。

[0073] 数据持久性安全区策略

[0074] 这个类别中的策略的示例包括确保必须定期对在安全区中创建的资源执行自动备份的策略。例如,这个类别中的策略确保安全区中的数据库备份不能用于创建不在安全区中的数据库、不能克隆安全区中的数据库以创建不在安全区中的数据库等。

[0075] 返回到图2的讨论,并且如前所述,安全区策略管理系统116可以配置有管理安全框架的能力,该安全框架包括由一组安全区(202、204和206)及其相关的安全区策略(208、210和212)组成的安全区信息120。安全区策略管理系统116还可以包括用于将隔间与安全区相关联、向隔间添加资源、查看与安全区相关联的安全区策略、删除隔间、在隔间内创建子隔间、将隔间移动到同一租赁内的不同父隔间、将安全区指定为最大安全区等的能力。例如,在图2中所描绘的实施例中,隔间A1 216可以由CSPI 110的第一租户A 121的用户创建并且与一组隔间策略218相关联。类似地,隔间B1 220可以由第二租户B 122的用户创建并与一组隔间策略相关联。此外,在这个实施例中,隔间A1 216和隔间B1 220都与安全区-1 202相关联。

[0076] 如前所述,隔间的创建以及隔间与安全区的关联可以由CSPI 110的客户或租户的用户通过经由控制台UI、经由API或经由连接到用户的计算设备的CLI 106将请求发送到安全区策略管理子系统116来执行。在接收到用户的请求后,安全区策略管理子系统116创建隔间并将隔间与安全区相关联。在将隔间(216或220)与安全区(例如,安全区-1 202)相关联后,隔间自动继承与安全区相关联的一组安全区策略(例如,208)。在某些实施例中,与安全区相关联的隔间在本文中可以被称为“安全区隔间”。然后用户可以将资源添加到安全区隔间。除了与隔间相关联的一组隔间策略之外,添加到安全区隔间的任何资源还自动与和安全区相关联的安全区策略相关联(即,自动继承)。

[0077] 在图2中所描绘的实施例中,租户A 121的隔间A1 216和租户B122的隔间B1都与同一个安全区-1 202相关联。在某些实施方式中,租户A 121的隔间A1 216和租户B 122的隔间B1 220可以与不同的安全区相关联。例如,隔间A1 216可以与安全区-1 202相关联,而隔间B1 220可以与不同的安全区-2 204相关联。此外,包括图2中描绘的安全区信息120的安全框架被描述为可由CSPI 110的各个租户访问和共享的通用框架。在替代实施例中,安全区信息120可以是特定于租户的并且在每个租户的基础上定义。图2中描绘的安全框架仅仅是示例并且非意在不当地限制要求保护的实施例的范围。本领域普通技术人员将认识到许多可能的变化、替代和修改。例如,其它实施方式是可能的,其中多个隔间可以与租户相关联、多个隔间可以与相同/或不同的安全区相关联、隔间可以与多于一个安全区相关联等等。在某些实施方式中,包括安全区和安全区策略的安全区信息120可以由CSPI 110的管理员或者由CSPI 110的租户的用户定义。

[0078] 在某些实施方式中,图2中描绘的安全区可以在层次上彼此相关。例如,在一个示例中,安全区-1 202和安全区-2 204可以在层次上相关,其中安全区-1 202是子安全区-2 204的父安全区。在这个示例中,如果隔间A1 216与安全区-2 204相关联,那么它变得自动与安全区-1202相关联并且因此继承与安全区-2 204相关联的安全区策略210。继续这个示例,在某个实施方式中,如果与安全区-1 202相关联的一组安全区策略208属于“访问限制”

类别并且与安全区-2 204相关联的一组安全区策略210属于“数据加密”类别,那么当将资源R1或R2添加到隔间A1 216,除了与资源所在的隔间A1 216相关联的隔间策略之外,资源还自动与“数据加密”安全区策略和“访问限制”安全区策略相关联。隔间中的资源与一个或多个安全区及其相关联的安全区策略的关联禁止用户能够对驻留在隔间中的资源执行某些操作,如果这些操作违反了由安全区策略定义的安全要求的话。

[0079] 在某些示例中,由安全区策略定义的安全要求可以禁止能对驻留在隔间中的资源执行的整组操作、禁止能对资源执行的操作的子集或者禁止能对资源执行的操作的特定版本/配置。例如,基于与资源相关联的IAM策略,可以准许对资源R1执行的一组操作(O1…On)。当资源R1被添加到隔间A1 216时,可被准许对R1执行的一组操作可以缩减为与隔间关联的隔间策略所允许的操作的子集(O1,O2,O5)。因此,与隔间相关联的隔间策略可以表示可被准许对驻留在隔间中的资源执行的一组操作上的第一过滤器。

[0080] 当隔间A1 216变得与安全区(例如,安全区-1 202)相关联时,它附加地继承安全区的安全区策略以及与在层次上与安全区相关的任何安全区相关联的安全区策略。基于上述示例,现在可以基于安全区策略将被准许对R1执行的一组操作进一步缩减为更小的操作子集(例如,O1)。因此,安全区策略可以表示可被准许对驻留在隔间中的资源执行的一组操作的第二或附加过滤器。图5B中描绘了安全区及其相关联的安全策略与隔间的关联的示例性图示。

[0081] 在某些示例中,安全区策略可以禁止可对驻留在隔间中的资源执行的操作(例如,O1)的特定配置。举例来说,用于驻留在隔间A1216中的R1的隔间策略可以准许用户创建资源R1,以便可以从公共网络(即,互联网)公开访问它,即,准许使用公共互联网协议(IP)地址创建R1。当隔间A1 216变得与安全区-1 202相关联时,与安全区-1 202相关联的安全区策略208可以禁止用户能够使用公共IP地址创建R1。作为另一个示例,如果资源引用/附连到公共子网资源,那么安全区策略可以不允许用户创建/启动“虚拟机”资源实例,因为子网资源可以与禁止用户从使用公共IP地址的子网资源启动“虚拟机”实例的安全区策略相关联。

[0082] 在某些实施方式中,隔间(例如,隔间A1 216)也可以在层次上与在租赁内创建的其它隔间相关。例如,在图2中所描绘的实施例中,隔间A1 216可以与租赁内创建的一个或多个隔间(即,父隔间)在层次上相关(即,作为其子隔间)。当资源(例如,R1)被添加到隔间A1 216时,除了与隔间相关联的一个或多个父隔间的隔间策略之外,该资源还自动继承与该隔间相关联的隔间策略。图5A中描绘了隔间继承隔间策略的示例性图示。

[0083] 图3描绘了根据某些实施例的由图1中所示的CSPI中的安全区策略管理子系统116执行的过程300的示例。图3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)、硬件或其组合中实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图3中呈现并在下面描述的过程300旨在是说明性而非限制性的。虽然图3描绘了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些替代实施例中,这些步骤可以以某个不同的次序执行,或者一些步骤也可以并行执行。

[0084] 图3中描绘的处理始于方框302,安全区策略管理子系统116接收将隔间与安全区相关联的请求。隔间可以与一组隔间策略相关联并且包括零个或更多个资源。在方框304

处,安全区策略管理子系统116将隔间与安全区相关联。作为关联的结果,隔间变得与和安全区相关联的一组安全区策略和一组隔间策略相关联。

[0085] 在方框306处,安全区策略管理子系统116基于隔间策略和安全区策略确定对隔间中的现有资源(如果存在的话)的访问。在某些示例中,在方框308处,安全区策略管理子系统116可以接收将新资源添加到隔间的请求。在方框310处,安全区策略管理子系统116基于隔间策略和安全区策略确定对新资源的访问。

[0086] 图4描绘了根据某些实施例的由图1中所示的CSPI中的安全区策略验证子系统执行的过程400的示例。图4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)、硬件或其组合中实现。软件可以存储在非暂态存储介质上(例如,在存储器设备上)。图4中呈现并在下面描述的过程400旨在是说明性而非限制性的。虽然图4描绘了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些替代实施例中,这些步骤可以以某个不同的次序执行,或者一些步骤也可以并行执行。

[0087] 图4中描绘的处理始于方框402,安全区策略验证子系统118接收对资源执行操作的请求。例如,该请求可以标识要对“实例”(即,虚拟机实例)执行的操作(例如,“启动实例”操作),以使用公共IP地址在用户的租赁中创建虚拟机实例。在方框404处,安全区策略验证子系统118确定与资源相关联的隔间。在方框406处,安全区策略验证子系统118基于在方框404中识别的隔间来确定适用于资源的一组隔间策略。除了在层次上与隔间相关的一个或多个父隔间的隔间策略之外,适用于资源的隔间策略还可以包括与该隔间相关联的隔间策略。在方框408处,安全区策略验证子系统118基于在方框406中确定的隔间策略来确定是否准许对资源的操作。例如,适用于资源的隔间策略可以准许用户创建虚拟机实例以便可以从公共网络(即,互联网)公开访问它,即,准许使用公共IP地址创建虚拟机实例。

[0088] 如果基于在方框406中确定的隔间策略不能执行对资源的操作,那么在方框410处,安全区策略验证子系统118不允许对资源执行操作。如果基于在方框406中确定的隔间策略可以执行对资源的操作,那么在方框412处,安全区策略验证子系统118确定在方框404中确定的隔间是否与安全区相关联。如果隔间不与安全区相关联,那么在方框414处,安全区策略验证子系统118允许对资源执行操作。如果隔间与安全区相关联,那么在方框416处,安全区策略验证子系统118确定与隔间相关联的安全区。在方框418处,安全区策略验证子系统118基于在方框416中确定的安全区来确定适用于资源的一组安全区策略。除了在层次上与安全区相关的一个或多个父安全区的安全区策略之外,适用于资源的安全区策略还可以包括与该安全区关联的安全区策略。在方框420处,安全区策略验证子系统118基于在418中确定的安全区策略来确定是否准许对资源的操作。例如,适用于资源的安全区策略可能不准许使用公共IP地址来创建虚拟实例资源。

[0089] 如果基于在418中确定的安全区策略不允许对资源的操作,那么在方框410处,安全区策略验证子系统118不允许对资源执行操作。如果基于在418中确定的策略允许对资源的操作,那么在方框414处,安全区策略验证子系统118允许对资源执行操作。在某些示例中,在方框414处执行的处理可以包括由安全区策略验证子系统118向CSPI中的下游服务发送请求以进一步处理该请求。作为下游服务执行的处理的结果,安全区策略验证子系统118可以向用户发送指示能够成功地对资源执行操作的结果。

[0090] 图5A是根据某些实施例的由图1中所示的CSPI的租户的用户创建的隔间继承隔间策略的示例性图示。在图5A中描绘的示例中,隔间C1 502、隔间C2 504和隔间C3 506在层次上彼此相关,其中隔间C1 502是隔间C2 504的父隔间,而隔间C2 504是隔间C3 506的父隔间。隔间C1 502与允许对驻留在隔间中的一组资源执行操作01的一组隔间策略508相关联。隔间C2 504与允许对驻留在隔间中的一组资源执行操作02的一组隔间策略510相关联。因为隔间C2 504是隔间C1 502的子隔间,所以它自动继承隔间C1 502的隔间策略508。隔间C3 506与允许对驻留在隔间中的一组资源执行操作03的一组隔间策略512相关联。因为隔间C3 506是隔间C2 504和隔间C1502的子隔间,所以它自动继承隔间C2 504的隔间策略510以及隔间C1 502的隔间策略。

[0091] 图5B是根据某些实施例的由图1中所示的CSPI的租户创建的隔间继承与安全区相关联的安全区策略的示例性图示。图5B中描绘的示例说明了图5A中描绘的隔间C1 502、隔间C2 504和隔间C3 506以及它们相关联的隔间策略508、510和512。在某些示例中,当隔间(例如,隔间C3 506)变得与安全区(安全区-1 514)相关联时,与安全区-1 514相关联的安全区策略516被应用于该隔间。由于隔间C3506与安全区策略516的关联,最初被允许对驻留在该隔间中的资源R1执行的一组操作(01,02,03)现在缩减为操作的子集(01)。因此,安全区策略表示附加层的安全策略,除了与隔间关联的隔间策略之外,该附加层的安全策略也可以对驻留在隔间中的一组资源强制执行。安全区策略可以禁止可对驻留在隔间中的一组资源执行的整组操作、禁止操作的子集或禁止可以对一组资源执行的操作的特定配置/版本。

[0092] 在某些实施方式中,上面的图1-4、图5A和图5B中描述的安全区策略强制执行系统可以与集中式请求处理系统协作,该集中式请求处理系统被配置为提供用于向CSPI的用户提供安全的资源访问的集中点。集中式请求处理系统可以与安全区策略强制执行系统一起操作,以提供集中式稳健和安全的框架,用于管理和强制执行与由CSPI管理的各种资源相关的安全策略。在某些示例中,由集中式请求处理系统执行的处理可以涉及评估与资源所在的一个或多个隔间相关联的隔间策略和安全区策略,以确定是否可以对请求中标识的资源执行某些操作。作为处理的结果,如果违反了策略(即,隔间策略或安全区策略),那么不允许用户执行请求中标识的操作,并且集中式请求处理系统向用户发送不允许用户执行该操作的信息。在某些实施例中,集中式请求处理系统可以由CSPI 110中的集中式应用编程接口(API)请求处理系统实现,如下面的图6中所示。下面参考图6-12及其随附描述来描述与由集中式应用编程接口(API)请求处理系统执行的实施方式和处理相关的细节。

[0093] 云服务提供商基础设施(CSPI)中的集中式应用编程接口(API)请求处理系统

[0094] 图6描绘了根据某些实施例的包括云服务提供商基础设施(CSPI)110的计算环境600的高级图示,该CSPI 110包括集中式API请求处理系统和安全区策略强制执行系统,用于提供安全框架以使得能够对由CSPI管理的各种资源进行安全访问。如前所述,资源可以包括但不限于由CSPI 110托管在分布式环境中的计算、联网、对象存储和数据库资源。CSPI 110的租户或客户的用户102可以使用由CSPI 110提供的资源来构建他们自己的网络(例如,VCN 620)并在VCN 620上部署一个或多个资源622A-622N,诸如计算实例(例如,虚拟机、裸机实例)。

[0095] CSPI基础设施110可以由一个或多个计算系统实现,这些计算系统执行计算机可

读指令(例如,代码、程序)以实现用于管理和强制执行与由CSPI管理的各种资源相关的安全策略的安全框架。如图6中所描绘的,CSPI 110包括各种系统和子系统,包括集中式API请求处理系统604、身份管理系统606、隔间标识符系统608和安全区策略强制执行系统112。由集中式API请求处理系统604作为其处理的一部分使用或生成的数据或信息的部分可以由安全区策略强制执行系统112存储在持久存储器数据存储库610中和安全区信息(例如,图1中所示的120)中。CSPI 110附加地包括一组一个或多个下游服务618A-618N,其可以经由一个或多个通信网络可通信地耦合到集中式API请求处理系统604。CSPI 110的客户的用户102可以利用下游服务来供应或部署客户的VCN 620中的基础设施资源。图6中描绘的系统和子系统可以使用由计算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)、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)。

[0096] 集中式API请求处理系统604可以以各种不同的配置来实现。在图6中描绘的实施例中,集中式API请求处理系统604在CSPI 110中的一个或多个服务器上实现,并且可以在订阅的基础上向云服务的订户提供其集中式安全资源访问服务。图6中描绘的计算环境600仅仅是示例,并且非意在不当地限制要求保护的实施例的范围。本领域普通技术人员将认识到许多可能的变化、替代和修改。例如,在一些实施方式中,CSPI 110可以使用比图1中所示的子系统更多或更少的子系统来实现,可以组合两个或更多个子系统,或者可以具有子系统的不同配置或布置。

[0097] 如图6中所描绘的,CSPI 110的用户102可以使用可能经由一个或多个通信网络可通信地耦合到CSPI 110的计算设备104与集中式API请求处理系统604交互。计算设备可以是各种类型的,包括但不限于移动电话、平板电脑、台式计算机等。用户102可以表示希望利用由集中式API请求处理系统604和安全区策略强制执行系统112提供的服务以安全地管理和访问他们在CSPI内的资源的CSPI 110的客户或租户。例如,用户102可以使用控制台用户接口(UI)、经由应用编程接口(API)或经由连接到用户的计算设备(例如,104)的命令行接口(CLI)106与集中式API请求处理系统604交互以安全地管理和访问他们在CSPI 110中的资源。例如,控制台UI可以是由集中式API请求处理系统604提供的基于web的用户接口(UI)(或基于web的应用),以使得用户能够与集中式API请求处理系统604交互。

[0098] 在某些实施例中,用户可以经由控制台UI、经由API或经由连接到用户的计算设备104的CLI 106向集中式API请求处理系统604发送API请求602。API请求602可以标识要对由CSPI 110管理的资源执行的操作。举例来说,API请求可以标识要对由CSPI管理的“实例”资源(例如,虚拟机实例)执行的“启动实例”操作。API请求的其它示例可以包括例如用于创建“子网”资源的“创建子网”操作、用于创建“块存储卷”资源的“创建块存储卷”操作等。在接收到请求后,集中式API请求处理系统604执行处理以确定是否可以对API请求中标识的资源安全地执行操作而不违反与请求中标识的资源相关的任何策略(例如,隔间策略以及安全区策略)。基于该处理,集中式API请求处理系统604将(一个或多个)结果624返回给发出请求的计算机设备104。(一个或多个)结果134可以包括能够对资源成功地执行操作的信息、由于策略违反而无法执行操作的消息以及结果中可能包括的其它信息。(一个或多个)结果624可以例如经由连接到用户的设备104的UI 106输出给用户。

[0099] 由集中式API请求处理系统602作为其处理的一部分使用或生成的数据或信息的

部分可以存储在持久存储器数据存储库610中。在某些示例中,存储在持久存储器数据存储库中的信息可以包括安全区规范612、API到下游服务映射信息614以及API规范616。安全区规范612可以存储与API请求中标识的资源相关的信息、API请求中为了对资源执行标识的操作而标识的(一个或多个)下游服务、评估API请求所需的上下文信息等。API到下游服务映射信息614可以存储与API请求如何映射到CSPI中的下游服务相关的信息,并且API规范616包括与一组下游服务使用的API相关的信息。

[0100] 安全区规范612、API到下游服务映射信息614和API规范616可以被集中式API请求处理系统602作为其处理的一部分使用,以评估对API请求中标识的资源的操作是否被准许由用户执行。在某些示例中,信息612、614和616可以由集中式API请求处理系统604的用户(例如,管理员)上传到持久存储器数据存储库610,作为由集中式API请求处理系统604提供给CSPI 110的集中式安全资源访问服务的一部分。

[0101] 在某些方法中,除了利用存储在持久存储器数据存储库610中的信息612、614或616之外,集中式API请求处理系统602还可以与诸如身份管理系统606、隔间标识符系统608和安全区策略强制执行系统112的一个或多个系统交互以获得用于评估是否允许用户执行API请求中标识的操作所需的信息。下面针对图7中描绘的流程图和附带描述来描述由集中式API请求处理系统604执行的处理及其与各种系统606、608和112的交互以提供对CSPI 110内的资源的安全访问的附加细节。

[0102] 图7描绘了根据某些实施例的由集中式API请求处理系统执行的用于向用户提供对由CSPI管理的各种资源的安全访问的过程700的示例。图7中描绘的处理可以在由相应系统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)、硬件或其组合的中实现。软件可以存储在非暂态存储介质上(例如,在存储器设备上)。图7中呈现并在下面描述的过程700旨在是说明性而非限制性的。虽然图7描绘了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些替代实施例中,这些步骤可以以某个不同的次序执行,或者一些步骤也可以并行执行。在某些实施例中,诸如在图6中描绘的实施例中,图7中描绘的处理可以由集中式API请求处理系统604执行。

[0103] 在图7中描绘的实施例中,处理开始于方框702,集中式API请求处理系统604从用户接收API请求(例如,602)。API请求可以标识要对由CSPI管理的资源执行的操作。举例来说,API请求可以标识要对“实例”资源(例如,虚拟机实例)执行的“启动实例”操作以在CSPI中的用户的VCN 620中创建/启动虚拟机实例110。

[0104] 在方框704处,集中式API请求处理系统604向身份管理系统606发送指令(例如,API授权请求)以确定用户是否被授权实行/执行在方框702中接收到的API请求。由身份管理系统704执行的处理可以包括对用户(例如,基于用户的用户名和密码)进行认证并且在成功认证用户后,确定用户是否被授权执行API请求中标识的操作。例如,身份管理系统704可以利用系统定义的IAM策略来确定用户是否被授权执行API请求中标识的操作。

[0105] 在方框706处,集中式API请求处理系统604基于由身份管理系统606执行的处理从身份管理系统606接收响应。

[0106] 在方框708处,集中式API请求处理系统604确定身份管理系统606是否已授权用户执行API请求中标识的操作。如果用户未被授权执行该操作,那么在方框710处,集中式API请求处理系统604向用户发送指示API请求的处理结束的错误消息。

[0107] 如果身份管理系统606已授权用户执行API请求中标识的操作,那么在方框712处,集中式API请求处理系统604从API请求中确定(a)“主要资源”,其包括API请求本身中命名的资源。在方框714处,集中式API请求处理系统604根据API请求确定零个或更多个“次要”资源或“关联”资源,其包括与主要资源相关联的资源。关联资源可能不会在请求本身中被标识,但包括受API请求影响的资源。举例来说,执行“启动实例”操作的API请求中的主要资源可以表示“计算”资源实例并且关联资源可以是用于启动主要资源(即,计算实例)的“引导卷”、“映像”或“子网”资源。在替代方法中,主要资源和次要资源都可以被包括在API请求中。

[0108] 在某些示例中,集中式API请求处理系统604可以根据存储在持久存储器数据存储库610中的API规范信息616来确定受方框714中的API请求影响的次要资源。例如,根据API规范信息616,集中式API请求处理系统604可以获得与在方框702中接收到的API请求对应的API规范。API规范可以识别主要资源以及受API请求影响的次要资源,连同要对主要资源执行的(一个或多个)操作。在其它方法中,集中式API请求处理系统604可以基于从存储在数据存储库610中的安全区规范612访问与API请求对应的安全区规范来确定受方框712中的API请求影响的关联资源和主要资源。下面在图10-12中详细描述与API请求对应的安全区规范的示例。

[0109] 在方框716处,集中式API请求处理系统604确定用于在方框712中确定的主要资源的隔间信息。隔间信息可以包括资源所在的隔间的隔间标识符和适用于该资源的隔间策略。除了在层次上与隔间相关的一个或多个父隔间的隔间策略之外,适用于资源的隔间策略还可以包括与隔间相关联的隔间策略。在某些情况下,集中式API请求处理系统604可以向隔间标识符系统608发送获得隔间信息的指令。在其它情况下,集中式API请求处理系统604可以从与API请求相关联的安全区规范中获得隔间信息。

[0110] 在方框718处,集中式API请求处理系统604确定与在方框714中确定的次要资源相关的上下文信息。上下文信息可以包括与次要资源相关联的隔间信息、与次要资源相关联的资源标识符、负责执行API请求的下游服务等。例如,对于标识“启动实例”操作的API请求,可以将主要资源确定为“实例”资源并且可以将次要资源确定为用于启动主要资源的“引导卷”资源。上下文信息可以包括引导卷资源标识符和用于执行API请求中标识的“启动实例”操作的下游服务(例如,块存储服务)。

[0111] 集中式API请求处理系统604可以使用各种方法来确定/获得用于次要资源的上下文信息。例如,在一种方法中,集中式API请求处理系统604可以利用存储在持久存储器数据存储库610中的安全区规范信息612来确定适用于次要资源的上下文信息。在另一种方法中,集中式API请求处理系统604可以直接从API到下游服务映射信息614或从负责执行API请求的下游服务确定或获得适用于资源的上下文信息。

[0112] 在方框720处,集中式API请求处理系统604将与主要资源相关联的隔间信息和与次要资源相关的上下文信息发送到身份管理系统606以供处理。由身份管理系统606执行的处理可以包括例如使用上下文信息来基于与主要资源所在的隔间相关联的隔间策略来确定是否允许对主要资源的操作。在方框722处,集中式API请求处理系统604从身份管理系统接收是否允许对资源执行API请求中标识的操作的指示。

[0113] 在方框724处,集中式API请求处理系统604确定是否允许对资源执行操作。如果不

允许该操作,那么在方框710处,集中式API请求处理系统604向用户发送指示API请求的处理结束的错误消息。

[0114] 如果API请求被允许,那么处理前进到方框726,其中集中式API请求处理系统604确定主要资源是否驻留在与安全区相关联的隔间中。在图2及其随附描述中详细描述了关于隔间与安全区的关联的细节。如果主要资源不驻留在与安全区相关联的隔间中,那么处理前进到方框734以准许用户执行API请求。

[0115] 如果主要资源驻留在与安全区相关联的隔间中,那么在方框728处,集中式API请求处理系统604调用安全区策略强制执行系统112以确定是否允许对资源执行操作。

[0116] 在方框730处,基于由安全区策略强制执行系统112执行的处理,集中式API请求处理系统604从安全区策略强制执行系统112接收是否允许对资源的操作的指示。例如,安全区策略强制执行系统112可以基于评估与在方框726中确定的安全区相关联的安全区策略来确定准许对资源的操作。在图8及其随附描述中描述了由安全区策略强制执行系统112执行以确定是否允许对资源的操作的处理的附加细节。

[0117] 在方框732处,如果确定不允许该操作,那么在方框710处,集中式API请求处理系统604向用户发送指示API请求的处理结束的错误消息。在方框732处,如果确定允许该操作,那么在方框734处,集中式API请求处理系统604允许执行API请求。

[0118] 图8描绘了根据某些实施例的由安全区策略强制执行系统112执行以基于评估与资源相关联的一组安全区策略来确定是否允许对资源执行操作的处理的过程800的示例。图8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)、硬件或其组合中实现。软件可以存储在非暂态存储介质上(例如,在存储器设备上)。图8中呈现并在下面描述的过程800旨在是说明性而非限制性的。虽然图8描绘了以特定顺序或次序发生的各种处理步骤,但这并非意在限制。在某些替代实施例中,这些步骤可以以某个不同的次序执行,或者一些步骤也可以并行执行。在某些实施例中,图8中描绘的处理描述了由图7的方框730中的安全区策略强制执行系统112执行的处理的附加细节。

[0119] 在某些实施例中,图8中描绘的处理始于方框802,安全区策略强制执行系统112接收到要对资源执行的操作和与该资源相关联的隔间(即,隔间id)。在方框804处,安全区策略强制执行系统112确定适用于资源的安全区策略。除了在层次上与安全区相关的一个或多个父安全区的安全区策略之外,适用于资源的安全区策略还可以包括与安全区相关联的安全区策略。例如,安全区策略强制执行系统112可以从由安全区策略强制执行系统112管理的安全区信息(例如,图1中所示的120)中获得关于安全区策略的信息。

[0120] 在方框806处,安全区策略强制执行系统112执行评估以基于在方框804中确定的策略确定是否准许对资源进行操作。如果允许操作,那么在方框808处,安全区策略强制执行系统112向集中式API请求处理系统发送“操作被允许”响应。如果不允许该操作,那么在方框810处,安全区策略强制执行系统112向集中式API请求处理系统发送“操作不被允许”响应。

[0121] 图9是图示了根据某些实施例的集中式API请求处理系统与图6中所示的一个或多个其它系统之间的交互以向用户提供对由CSPI管理的各种资源的安全访问的顺序图。图9中描绘的处理始于用户向集中式API请求处理系统604发送API请求902。举例来说,API请求

可以标识要对API请求中标识的“虚拟机”资源实例执行的操作(例如,“启动实例”)。在接收到请求后,集中式API请求处理系统604向身份管理系统606发送授权请求(AuthZ请求)904以确定用户是否被授权执行API请求。在操作906处,身份管理系统606向集中式API请求处理系统604返回指示用户是否被授权执行API请求的响应(AuthZ响应)。

[0122] 如果用户被授权执行API请求,那么在操作908处,集中式API请求处理系统604向隔间标识符系统608发送获得/获取API请求中标识的主要资源的隔间信息的指令。“主要资源”可以包括在API请求本身中标识的资源。例如,“计算”资源实例可以被确定为执行“启动实例”操作的API请求中的主要资源。如前所述,隔间信息可以包括隔间标识符和适用于资源的隔间策略。在操作910处,集中式API请求处理系统604从隔间标识符系统608接收隔间信息。

[0123] 在操作912处,集中式API请求处理系统604向负责执行API请求的下游服务发送获得与受API请求影响的次要资源相关的上下文信息的请求。“次要”资源或“关联”资源可以包括与主要资源相关联的资源。关联资源可能不会被标识在请求本身中,但包括受API请求影响的资源。举例来说,执行“启动实例”操作的API请求中的主要资源可以表示“计算”资源实例,而关联/次要资源可以是用于启动主要资源(即,计算实例)的“引导卷”、“映像”或“子网”资源。例如,基于“启动实例”API请求的示例,引导卷标识符(bootVolumeId)可以是从次要(关联)“引导卷”资源启动“实例”主要资源所需的相关输入(上下文信息)。在某些示例中,集中式API请求处理系统604可以从被配置为执行API请求中标识的操作的下游服务(例如,计算服务618A)获取上下文信息。在其它示例中,集中式API请求处理系统604可以从安全区规范612中获取与存储在持久存储器数据存储库610中的API请求相关的上下文信息。描述可以指定和/或获得与API请求相关的上下文信息的方式的附加细节与图10-12中描述的安全区规范相关地进行描述。

[0124] 在操作914处,集中式API请求处理系统604接收处理API请求所需的上下文信息。在某些示例中,在方框916处,集中式API请求处理系统604可以可选地基于API请求中标识的主要资源和关联资源来准备附加的上下文变量。附加的上下文变量可以包括例如获得API请求中标识的资源的当前状态等。例如,对于将引导卷附连到计算实例的示例,附加的上下文变量可以包括获得和要与块卷一起使用的加密密钥相关的信息。

[0125] 在操作918处,集中式API请求处理系统604将隔间信息和上下文信息发送到身份管理系统606以供处理。在操作920处,身份管理系统606处理/评估隔间信息和上下文信息以确定是否允许对资源的操作并且向集中式API请求处理系统604发送是否允许对资源执行在API请求中标识的操作的指示。如果不允许API请求,那么在某些实施例中,集中式API请求处理系统604可以在操作922处向用户发送指示API请求的处理结束的错误消息。

[0126] 在924处,集中式API请求处理系统604确定主要资源是否驻留在与安全区相关联的隔间中,并且如果是,那么将安全区信息(例如,安全区id)发送到安全区策略强制执行系统112。在操作926处,安全区策略强制执行系统112基于评估与安全区相关联的安全区策略(以及在层次上与安全区相关的安全区相关联的任何安全区策略)执行确定是否准许对资源的操作的处理。基于该处理,在操作928处,安全区策略强制执行系统122向集中式API请求处理系统604发送响应。

[0127] 如果响应指示操作被允许,那么在操作932处,集中式API请求处理系统将API请求

转发(路由)到标识的下游服务618A(例如,计算服务)以供进一步处理。作为API请求的成功处理的结果,在操作934处,下游服务618向集中式API请求处理系统604发送成功执行了操作的下游响应。在操作936处,集中式API请求处理系统604向用户发送成功执行了API请求的指示。如果响应指示不允许API请求,那么在操作930处,集中式API请求处理系统604向用户发送指示策略违反错误的消息并结束对用户的API请求的处理。

[0128] 图10是根据某些实施例的与标识用于使用图6中所示的CSPI中的计算服务来启动计算实例资源的操作的API请求对应的安全区规范的示例。在所描绘的示例中,用于“启动实例”API请求的安全区规范标识要对计算实例资源执行的操作(即,“LaunchInstance”)、执行该操作的下游服务(“computer service”)、API请求中标识的主要资源(“instance”)以及与主要资源相关联的一组关联资源(“boot volume”、“image”和“subnet”)。如图10中所描绘的,在一个示例中,安全区规范中的“associationPredicate”参数可以被用于标识资源是关联资源。例如,当从次要“boot volume”资源启动主要“instance”资源时,引导卷资源被视为关联资源,当从“image”启动“instance”资源时,映像资源被视为关联资源,当从“subnet”启动“instance”资源时,子网资源被视为关联资源,等等。

[0129] 安全区规范还包括被配置为获取与主要资源相关联的关联资源的上下文信息的“contextFetchExpression”参数。例如,引导卷标识符(bootVolumeId)可以是从“引导卷”启动实例所需的相关输入(上下文),映像标识符(imageId)可以是从“映像”启动实例所需的相关输入(上下文),并且子网标识符(subnetId)可以是从“子网”启动实例所需的相关输入(上下文)。在某些示例中,安全区规范还包括可以被用于获得与API请求中标识的主要资源和关联资源相关联的隔间标识符的“compartmentIdExpression”参数。

[0130] 图11是根据某些实施例的与标识用于将卷附连到实例、将引导卷附连到实例以及使用CSPI中的计算服务改变用于实例的隔间标识符的操作的API请求对应的安全区规范的示例。在所描绘的示例中,用于“附连卷”API请求的安全区规范识别要对计算实例资源执行的操作(即,“AttachVolume”)、执行该操作的下游服务(“computer service”)、API请求中标识的主要资源(“instance”)以及与主要资源相关联的关联资源(“volume”)。用于“附连卷”API请求的安全区规范还识别将卷附连到实例所需的上下文信息(卷id)以及与API请求中标识的主要资源和关联资源相关联的隔间标识符。

[0131] 类似地,用于“附连引导卷”API请求的安全区规范识别要对实例资源执行的操作(“AttachBootVolume”)、执行该操作的下游服务(“computer service”)、API请求中标识的主要资源(“instance”)以及与主要资源相关联的关联资源(“bootvolume”)。用于“附连引导卷”API请求的安全区规范还识别将卷附连到实例所需的上下文信息(引导卷id)以及与API请求中标识的主要资源和关联资源相关联的隔间标识符。用于“改变实例隔间”API请求的安全区规范识别要对实例资源执行的操作(“ChangeInstanceCompartment”)、执行该操作的下游服务(“computer service”)以及API请求中标识的主要资源(“instance”)。用于“改变实例隔间”API请求的安全区规范还识别改变实例的隔间所需的上下文信息(资源id)以及与主要资源相关联并在API请求中标识的隔间标识符。

[0132] 图12是根据某些实施例的与识别用于创建子网、创建互联网网关、改变用于子网的隔间标识符以及使用CSPI中的服务来改变用于互联网网关的隔间标识符的操作的API请求对应的安全区规范的示例。在所描绘的示例中,用于“创建子网”API请求的安全区规范识

别要对子网资源执行的操作(“CreateSubnet”)、执行该操作的下游服务(“virtual network service”)以及API请求中标识的主要资源(“subnet”)。用于“创建子网”API请求的安全区规范还识别创建子网所需的上下文信息以及与主要资源相关联的隔间标识符。对于这个示例,上下文信息包括关于子网的IP地址的信息以确定API请求中的创建子网操作是否使用公共IP来创建子网。

[0133] 类似地,用于“创建互联网网关”API请求的安全区规范识别要对互联网网关资源执行的操作(“CreateInternetGateway”)、执行该操作的下游服务(“virtual network service”)以及API请求中标识的主要资源(“internet gateway”)。用于“创建互联网网关”API请求的安全区规范还识别与API请求中标识的主要资源相关联的隔间标识符。用于“改变子网隔间”API请求的安全区规范识别要对子网资源执行的操作(“ChangeSubnetCompartment”)、执行该操作的下游服务(“virtual network service”)、API请求中标识的主要资源(“subnet””)以及与主要资源相关联的隔间标识符。用于“改变互联网网关隔间”API请求的安全区规范识别要对互联网网关资源执行的操作(“ChangeInternetGatewayCompartment”)、执行该操作的下游服务(“virtual network service”)、API请求中标识的主要资源(“internet gateway”)以及与主要资源相关联的隔间标识符。

[0134] 由所公开的安全区策略强制执行系统实现的基于云的安全解决方案为企业的用户提供了用于安全地配置、访问和管理他们在云中的资源的稳健的安全框架。如上所述,在某些实施例中,安全区策略强制执行系统与用于管理和强制执行与由CSPI管理的各种资源相关的安全策略的集中式请求处理系统一起操作。本公开中描述的基于云的安全解决方案提供了优于常规的基于云的安全服务的若干技术进步和/或改进。所公开的安全框架包括一组安全区和安全区策略,这些安全区策略可以在企业的用户访问的云中的一组资源上强制执行。对一组资源的访问由一组安全区策略支配,并且不绑定到访问资源的用户的身份。因此,如果违反了与资源相关联的一组安全区策略,那么被IAM策略允许访问特定资源(和/或对资源执行操作)的用户可以被所公开的安全解决方案拒绝访问。安全区策略基于“拒绝语义”,其旨在不允许企业的任何用户对一组资源执行某些动作或操作。这与基于用户在企业内的角色/身份而允许特定用户对资源执行特定动作的现有IAM授权策略采用的传统“允许语义”形成对比。

[0135] 示例体系架构

[0136] 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的服务器和系统是分开的。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。云服务被设计为向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。

[0137] 存在提供各种类型的云服务的若干云服务提供商。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。

[0138] 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,为那个客户创建租赁或账户。然后,客户可以经由该账户访问与该账户相关联的经订阅的一个或多个云资源。

[0139] 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提供商还可以提供各种服务来伴随这些基础设施组件(例如,计费、监视、日志记录、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。

[0140] 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。

[0141] 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。

[0142] 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、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)。

[0143] 在一些示例中,IaaS供给(provisioning)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。

[0144] 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初始基础设施集存在最初的挑战。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,可以通过使得基础设施的配置能够以声明的方式定义来解决这两个挑战。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。

[0145] 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,可配置的和/或共享的计算资源的潜在按需池),也称为核心网络。在一些示例中,还可以供给定义如何设置网络的入站/出站流量的一个或多个入站/出站流量组规则以及一个或多个虚拟机(VM)。也可以供给其它基础设施元素,诸如负载平衡器、数据库等。随着期望和/或添加越来越多的基础设施元素,基础设施可以逐步演进。

[0146] 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/或一旦基础设施被供给就可以利用部署工具部署代码。

[0147] 图13是图示了根据至少一个实施例的IaaS体系架构的示例模式的框图1300。服务运营商1302可以可通信地耦合到可以包括虚拟云网络(VCN)1306和安全主机子网1308的安全主机租赁1304。在一些示例中,服务运营商1302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®**或其它通信协议。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它电子设备,诸如瘦客户端计算机、支持互联网的游戏系统(例如,具有或不具有**Kinect®**手势输入设备的Microsoft Xbox游戏控制台),和/或能够通过可以访问VCN 1306和/或互联网的网络进行通信的个人消息传递设备。

[0148] VCN 1306可以包括本地对等网关(LPG)1310,其可以经由包含在SSH VCN 1312中的LPG 1310可通信地耦合到安全壳(SSH)VCN 1312。SSH VCN 1312可以包括SSH子网1314,并且SSH VCN 1312可以经由包含在控制平面VCN 1316中的LPG 1310可通信地耦合到控制平面VCN 1316。此外,SSH VCN 1312可以经由LPG 1310可通信地耦合到数据平面VCN 1318。控制平面VCN 1316和数据平面VCN 1318可以包含在可以由IaaS提供商拥有和/或操作的服务租赁1319中。

[0149] 控制平面VCN 1316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1320。基于DMZ的服务器可以具有有限责任并有助于保持包含缺口。此外,DMZ层1320可以包括一个或多个负载平衡器(LB)子网1322、可以包括(一个或多个)应用子网1326的控制平面应用层1324、可以包括(一个或多个)数据库(DB)子网1330(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1328。控制平面DMZ层1320中包含的(一个或多个)LB子网1322可以可通信地耦合到包含在控制平面应用层1324中的(一个或多个)应用子网1326和可以包含在控制平面VCN 1316中的互联网网关1334,并且(一个或多个)应用子网1326可以可通信地耦合到包含在控制平面数据层1328中的(一个或多个)DB子网1330以及服务网关1336和网络地址转换(NAT)网关1338。控制平面VCN 1316可以包括服务网关1336和NAT网关1338。

[0150] 控制平面VCN 1316可以包括数据平面镜像应用层1340,其可以包括(一个或多个)应用子网1326。数据平面镜像应用层1340中包含的(一个或多个)应用子网1326可以包括可执行计算实例1344的虚拟网络接口控制器(VNIC)1342。计算实例1344可以将数据平面镜像应用层1340的(一个或多个)应用子网1326可通信地耦合到可以包含在数据平面应用层1346中的(一个或多个)应用子网1326。

[0151] 数据平面VCN 1318可以包括数据平面应用层1346、数据平面DMZ层1348和数据平面数据层1350。数据平面DMZ层1348可以包括(一个或多个)LB子网1322,其可以可通信地耦合到数据平面应用层1346的(一个或多个)应用子网1326和数据平面VCN 1318的互联网网关1334。(一个或多个)应用子网1326可以可通信地耦合到数据平面VCN 1318的服务网关1336和数据平面VCN 1318的NAT网关1338。数据平面数据层1350还可以包括可以可通信地耦合到数据平面应用层1346的(一个或多个)应用子网1326的(一个或多个)DB子网1330。

[0152] 控制平面VCN 1316和数据平面VCN 1318的互联网网关1334可以可通信地耦合到元数据管理服务1352,元数据管理服务1352可以可通信地耦合到公共互联网1354。公共互联网1354可以可通信地耦合到控制平面VCN 1316和数据平面VCN 1318的NAT网关1338。控制平面VCN 1316和数据平面VCN 1318的服务网关1336可以可通信地耦合到云服务1356。

[0153] 在一些示例中,控制平面VCN 1316或数据平面VCN 1318的服务网关1336可以对云服务1356进行应用编程接口(API)调用,而无需通过公共互联网1354。从服务网关1336到云服务1356的API调用可以是单向的:服务网关1336可以对云服务1356进行API调用,并且云服务1356可以将请求的数据发送到服务网关1336。但是,云服务1356可以不发起对服务网关1336的API调用。

[0154] 在一些示例中,安全主机租赁1304可以直接连接到服务租赁1319,服务租赁1319否则可以被隔离。安全主机子网1308可以通过LPG 1310与SSH子网1314通信,LPG 1310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1308连接到SSH子网1314可以使安全主机子网1308可访问服务租赁1319内的其它实体。

[0155] 控制平面VCN 1316可以允许服务租赁1319的用户设置或以其它方式供给期望的资源。在控制平面VCN 1316中供给的期望资源可以在数据平面VCN 1318中部署或以其它方式使用。在一些示例中,控制平面VCN 1316可以与数据平面VCN 1318隔离,并且控制平面VCN 1316的数据平面镜像应用层1340可以经由VNIC 1342与数据平面VCN 1318的数据平面应用层1346通信,VNIC 1342可以包含在数据平面镜像应用层1340和数据平面应用层1346中。

[0156] 在一些示例中,系统的用户或客户可以通过公共互联网1354来做出请求,例如创建、读取、更新或删除(CRUD)操作,公共互联网1354可以将请求传送到元数据管理服务1352。元数据管理服务1352可以通过互联网网关1334将请求传送到控制平面VCN 1316。请求可以被控制平面DMZ层1320中包含的(一个或多个)LB子网1322接收。(一个或多个)LB子网1322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1322可以将请求传输到控制平面应用层1324中包含的(一个或多个)应用子网1326。如果请求被验证并且需要对公共互联网1354的调用,那么对公共互联网1354的调用可以被传输到可以对公共互联网1354进行调用的NAT网关1338。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1330中。

[0157] 在一些示例中,数据平面镜像应用层1340可以促进控制平面VCN 1316和数据平面VCN 1318之间的直接通信。例如,可能期望向数据平面VCN 1318中包含的资源应用对配置的更改、更新或其它适当的修改。经由VNIC 1342,控制平面VCN 1316可以直接与数据平面VCN 1318中包含的资源通信,并且从而可以执行对配置的更改、更新或其它适当的修改。

[0158] 在一些实施例中,控制平面VCN 1316和数据平面VCN 1318可以包含在服务租赁

1319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 1316或数据平面VCN 1318。替代地,IaaS提供商可以拥有或操作控制平面VCN 1316和数据平面VCN 1318,这两者都可以包含在服务租赁1319中。该实施例可以使得能够隔离可能阻止用户或客户与其它用户或其它客户的资源交互的网络。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的威胁防护级别的公共互联网1354进行存储。

[0159] 在其它实施例中,控制平面VCN 1316中包含的(一个或多个)LB子网1322可以被配置为从服务网关1336接收信号。在这个实施例中,控制平面VCN 1316和数据平面VCN 1318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1354。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可与公共互联网1354隔离的服务租赁1319上。

[0160] 图14是图示了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1400。服务运营商1402(例如,图13的服务运营商1302)可以可通信地耦合到安全主机租赁1404(例如,图13的安全主机租赁1304),该安全主机租赁1404可以包括虚拟云网络(VCN)1406(例如,图13的VCN 1306)和安全主机子网1408(例如,图13的安全主机子网1308)。VCN 1406可以包括本地对等网关(LPG)1410(例如,图13的LPG 1310),其可以经由包含在SSH VCN 1412中的LPG 1310可通信地耦合到安全壳(SSH)VCN 1412(例如,图13的SSH VCN 1312)。SSH VCN 1412可以包括SSH子网1414(例如,图13的SSH子网1314),并且SSH VCN 1412可以经由包含在控制平面VCN 1416中的LPG 1410可通信地耦合到控制平面VCN 1416(例如,图13的控制平面VCN 1316)。控制平面VCN 1416可以包含在服务租赁1419(例如,图13的服务租赁1319)中,并且数据平面VCN 1418(例如,图13的数据平面VCN 1318)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1421中。

[0161] 控制平面VCN 1416可以包括可包括(一个或多个)LB子网1422(例如,图13的(一个或多个)LB子网1322)的控制平面DMZ层1420(例如,图13的控制平面DMZ层1320)、可包括(一个或多个)应用子网1426(例如,图13的(一个或多个)应用子网1326)的控制平面应用层1424(例如,图13的控制平面应用层1324)、可包括(一个或多个)数据库(DB)子网1430(例如,类似于图13的(一个或多个)DB子网1330)的控制平面数据层1428(例如,图13的控制平面数据层1328)。包含在控制平面DMZ层1420中的(一个或多个)LB子网1422可以可通信地耦合到包含在控制平面应用层1424中的(一个或多个)应用子网1426和可以包含在控制平面VCN 1416中的互联网网关1434(例如,图13的互联网网关1334),并且(一个或多个)应用子网1426可以可通信地耦合到包含在控制平面数据层1428中的(一个或多个)DB子网1430以及服务网关1436(例如,图13的服务网关)和网络地址转换(NAT)网关1438(例如,图13的NAT网关1338)。控制平面VCN 1416可以包括服务网关1436和NAT网关1438。

[0162] 控制平面VCN 1416可以包括可包括(一个或多个)应用子网1426的数据平面镜像应用层1440(例如,图13的数据平面镜像应用层1340)。包含在数据平面镜像应用层1440中的(一个或多个)应用子网1426可以包括可以执行计算实例1444(例如,类似于图13的计算实例1344)的虚拟网络接口控制器(VNIC)1442(例如,1342的VNIC)。计算实例1444可以促进数据平面镜像应用层1440的(一个或多个)应用子网1426和可以包含在数据平面应用层1446(例如,图13的数据平面应用层1346)中的(一个或多个)应用子网1426之间经由包含在数据平面镜像应用层1440中的VNIC 1442和包含在数据平面应用层1446中的VNIC 1442的

通信。

[0163] 包含在控制平面VCN 1416中的互联网网关1434可以可通信地耦合到元数据管理服务1452(例如,图13的元数据管理服务1352),该元数据管理服务1452可以可通信地耦合到公共互联网1454(例如,图13的公共互联网1354)。公共互联网1454可以可通信地耦合到包含在控制平面VCN 1416中的NAT网关1438。包含在控制平面VCN 1416中的服务网关1436可以可通信地耦合到云服务1456(例如,图13的云服务1356)。

[0164] 在一些示例中,数据平面VCN 1418可以包含在客户租赁1421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 1416,并且IaaS提供商可以为每个客户设置包含在服务租赁1419中的唯一计算实例1444。每个计算实例1444可以允许包含在服务租赁1419中的控制平面VCN 1416和包含在客户租赁1421中的数据平面VCN 1418之间的通信。计算实例1444可以允许在包含在服务租赁1419中的控制平面VCN 1416中供给的资源被部署或以其它方式在包含在客户租赁1421中的数据平面VCN 1418中使用。

[0165] 在其它示例中,IaaS提供商的客户可以具有存在于客户租赁1421中的数据库。在这个示例中,控制平面VCN 1416可以包括数据平面镜像应用层1440,其可以包括(一个或多个)应用子网1426。数据平面镜像应用层1440可以驻留在数据平面VCN 1418中,但数据平面镜像应用层1440可能不在数据平面VCN 1418中。即,数据平面镜像应用层1440可以访问客户租赁1421,但是数据平面镜像应用层1440可能不存在于数据平面VCN 1418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1440可以被配置为对数据平面VCN 1418进行调用,但可以不被配置为对包含在控制平面VCN 1416中的任何实体进行调用。客户可能期望在数据平面VCN 1418中部署或以其它方式使用在控制平面VCN 1416中供给的资源,并且数据平面镜像应用层1440可以促进客户的期望部署或资源的其它使用。

[0166] 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 1418。在这个实施例中,客户可以确定数据平面VCN 1418可以访问什么,并且客户可以限制从数据平面VCN 1418对公共互联网1454的访问。IaaS提供商可能无法应用过滤器或以其它方式控制数据平面VCN 1418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1421中的数据平面VCN 1418上可以帮助将数据平面VCN 1418与其它客户和公共互联网1454隔离开。

[0167] 在一些实施例中,云服务1456可以由服务网关1436调用以访问公共互联网1454、控制平面VCN 1416或数据平面VCN 1418上可能不存在的服务。云服务1456与控制平面VCN 1416或数据平面VCN 1418之间的连接可以不是实时的或连续的。云服务1456可以存在于由IaaS提供商拥有或操作的不同网络上。云服务1456可以被配置为接收来自服务网关1436的调用并且可以被配置为不接收来自公共互联网1454的调用。一些云服务1456可以与其它云服务1456隔离,并且控制平面VCN 1416可以与可能与控制平面VCN 1416不在同一区域的云服务1456隔离。例如,控制平面VCN 1416可能位于“区域1”,并且云服务“部署13”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 1416中的服务网关1436对部署13进行调用,那么该调用可以被传输到区域1中的部署13。在这个示例中,控制平面VCN 1416或区域1中的部署13可能不与区域2中的部署13可通信地耦合或以其它方式通信。

[0168] 图15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1500。服务运营商1502(例如,图13的服务运营商1302)可以可通信地耦合到安全主机租赁1504

(例如,图13的安全主机租赁1304),该安全主机租赁1504可以包括虚拟云网络(VCN)1506(例如,图13的VCN 1306)和安全主机子网1508(例如,图13的安全主机子网1308)。VCN 1506可以包括LPG 1510(例如,图13的LPG 1310),其可以经由包含在SSH VCN 1512中的LPG 1510可通信地耦合到SSH VCN 1512(例如,图13的SSH VCN 1312)。SSH VCN 1512可以包括SSH子网1514(例如,图13的SSH子网1314),并且SSH VCN 1512可以经由包含在控制平面VCN 1516中的LPG 1510可通信地耦合到控制平面VCN 1516(例如,图13的控制平面VCN 1316)并且经由包含在数据平面VCN 1518中的LPG 1510耦合到数据平面VCN 1518(例如,图13的数据平面1318)。控制平面VCN 1516和数据平面VCN 1518可以包含在服务租赁1519(例如,图13的服务租赁1319)中。

[0169] 控制平面VCN 1516可以包括可包括(一个或多个)负载平衡器(LB)子网1522(例如,图13的(一个或多个)LB子网1322)的控制平面DMZ层1520(例如,图13的控制平面DMZ层1320)、可包括(一个或多个)应用子网1526(例如,类似于图13的(一个或多个)应用子网1326)的控制平面应用层1524(例如,图13的控制平面应用层1324)、可包括(一个或多个)DB子网1530的控制平面数据层1528(例如,图13的控制平面数据层1328)。包含在控制平面DMZ层1520中的(一个或多个)LB子网1522可以可通信地耦合到包含在控制平面应用层1524中的(一个或多个)应用子网1526和可包含在控制平面VCN 1516中的互联网网关1534(例如,图13的互联网网关1334),并且(一个或多个)应用子网1526可以可通信地耦合到包含在控制平面数据层1528中的(一个或多个)DB子网1530以及服务网关1536(例如,图13的服务网关)和网络地址转换(NAT)网关1538(例如,图13的NAT网关1338)。控制平面VCN 1516可以包括服务网关1536和NAT网关1538。

[0170] 数据平面VCN 1518可以包括数据平面应用层1546(例如,图13的数据平面应用层1346)、数据平面DMZ层1548(例如,图13的数据平面DMZ层1348),以及数据平面数据层1550(例如,图13的数据平面数据层1350)。数据平面DMZ层1548可以包括可以可通信地耦合到数据平面应用层1546的(一个或多个)可信应用子网1560和(一个或多个)不可信应用子网1562以及包含在数据平面VCN 1518中的互联网网关1534的(一个或多个)LB子网1522。

[0171] (一个或多个)可信应用子网1560可以可通信地耦合到包含在数据平面VCN 1518中的服务网关1536、包含在数据平面VCN 1518中的NAT网关1538以及包含在数据平面数据层1550中的(一个或多个)DB子网1530。(一个或多个)不可信应用子网1562可以可通信地耦合到包含在数据平面VCN 1518中的服务网关1536和包含在数据平面数据层1550中的(一个或多个)DB子网1530。数据平面数据层1550可以包括可以可通信地耦合到包含在数据平面VCN 1518中的服务网关1536的(一个或多个)DB子网1530。

[0172] (一个或多个)不可信应用子网1562可以包括可以可通信地耦合到租户虚拟机(VM)1566(1)-(N)的一个或多个主VNIC 1564(1)-(N)。每个租户VM 1566(1)-(N)可以可通信地耦合到可以包含在相应容器出口VCN 1568(1)-(N)中的相应应用子网1567(1)-(N),相应容器出口VCN 1568(1)-(N)可以包含在相应客户租赁1570(1)-(N)中。相应的辅助VNIC 1572(1)-(N)可以促进数据平面VCN 1518中包含的(一个或多个)不可信应用子网1562与容器出口VCN 1568(1)-(N)中包含的应用子网之间的通信。每个容器出口VCN 1568(1)-(N)可以包括NAT网关1538,该NAT网关1538可以可通信地耦合到公共互联网1554(例如,图13的公共互联网1354)。

[0173] 包含在控制平面VCN 1516中并且包含在数据平面VCN 1518中的互联网网关1534可以可通信地耦合到元数据管理服务1552(例如,图13的元数据管理系统1352),该元数据管理服务1552可以可通信地耦合到公共互联网1554。公共互联网1554可以可通信地耦合到包含在控制平面VCN 1516中并且包含在数据平面VCN 1518中的NAT网关1538。包含在控制平面VCN 1516中和包含在数据平面VCN 1518中的服务网关1536可以可通信地耦合到云服务1556。

[0174] 在一些实施例中,数据平面VCN 1518可以与客户租赁1570集成。在一些情况下,诸如在执行代码时可能期望支持的情况下,这种集成对于IaaS提供商的客户可能是有用的或期望的。客户可能提供可能具有破坏性、可能与其它客户资源通信或可能以其它方式导致非期望效果的代码来运行。作为对此的响应,IaaS提供商可以确定是否运行由客户给与IaaS提供商的代码。

[0175] 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,并请求附连到数据平面层应用1546的功能。运行该功能的代码可以在VM 1566(1)-(N)中执行,并且该代码可以不被配置为在数据平面VCN 1518上的其它任何地方运行。每个VM 1566(1)-(N)可以连接到一个客户租赁1570。包含在VM 1566(1)-(N)中的相应容器1571(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1571(1)-(N)运行代码,其中容器1571(1)-(N)可能至少包含在(一个或多个)不可信应用子网1562中包含的VM 1566(1)-(N)中),这可以帮助防止不正确的或以其它方式非期望的代码损坏IaaS提供商的网络或损坏不同客户的网络。容器1571(1)-(N)可以可通信地耦合到客户租赁1570并且可以被配置为传输或接收来自客户租赁1570的数据。容器1571(1)-(N)可以不被配置为从数据平面VCN 1518中的任何其它实体传输或接收数据。在运行代码完成后,IaaS提供商可以终止或以其它方式处置容器1571(1)-(N)。

[0176] 在一些实施例中,(一个或多个)可信应用子网1560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1560可以可通信地耦合到(一个或多个)DB子网1530并且被配置为在(一个或多个)DB子网1530中执行CRUD操作。(一个或多个)不可信应用子网1562可以可通信地耦合到(一个或多个)DB子网1530,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1530中执行读取操作。可以包含在每个客户的VM 1566(1)-(N)中并且可以运行来自客户的代码的容器1571(1)-(N)可以不与(一个或多个)DB子网1530可通信地耦合。

[0177] 在其它实施例中,控制平面VCN 1516和数据平面VCN 1518可以不直接可通信地耦合。在这个实施例中,控制平面VCN 1516和数据平面VCN 1518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 1510可以由IaaS提供商建立,其可以促进控制平面VCN 1516和数据平面VCN 1518之间的通信。在另一个示例中,控制平面VCN 1516或数据平面VCN 1518可以经由服务网关1536调用云服务1556。例如,从控制平面VCN 1516对云服务1556的调用可以包括对可以与数据平面VCN 1518通信的服务的请求。

[0178] 图16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1600。服务运营商1602(例如,图13的服务运营商1302)可以可通信地耦合到安全主机租赁1604(例如,图13的安全主机租赁1304),该安全主机租赁1604可以包括虚拟云网络(VCN)1606(例如,图13的VCN 1306)和安全主机子网1608(例如,图13的安全主机子网1308)。VCN 1606

可以包括LPG 1610(例如,图13的LPG 1310),该LPG 1610可以经由包含在SSH VCN 1612(例如,图13的SSH VCN 1312)中的LPG 1610可通信地耦合到SSH VCN 1612。SSH VCN 1612可以包括SSH子网1614(例如,图13的SSH子网1314),并且SSH VCN 1612可以经由包含在控制平面VCN 1616中的LPG 1610可通信地耦合到控制平面VCN 1616(例如,图13的控制平面VCN 1316)并且经由包含在数据平面VCN 1618中的LPG 1610耦合到数据平面VCN 1618(例如,图13的数据平面1318)。控制平面VCN 1616和数据平面VCN 1618可以包含在服务租赁1619(例如,图13的服务租赁1319)中。

[0179] 控制平面VCN 1616可以包括可包括(一个或多个)LB子网1622(例如,图13的(一个或多个)LB子网1322)的控制平面DMZ层1620(例如,图13的控制平面DMZ层1320)、可包括(一个或多个)应用子网1626(例如,图13的(一个或多个)应用子网1326)的控制平面应用层1624(例如,图13的控制平面应用层1324)、可包括(一个或多个)DB子网1630(例如,图15的(一个或多个)DB子网1530)的控制平面数据层1628(例如,图13的控制平面数据层1328)。包含在控制平面DMZ层1620中的(一个或多个)LB子网1622可以可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(例如,图13的互联网网关1334),并且(一个或多个)应用子网1626可以可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(例如,图13的服务网关)和网络地址转换(NAT)网关1638(例如,图13的NAT网关1338)。控制平面VCN 1616可以包括服务网关1636和NAT网关1638。

[0180] 数据平面VCN 1618可以包括数据平面应用层1646(例如,图13的数据平面应用层1346)、数据平面DMZ层1648(例如,图13的数据平面DMZ层1348))、以及数据平面数据层1650(例如,图13的数据平面数据层1350)。数据平面DMZ层1648可以包括可以可通信地耦合到数据平面应用层1646的(一个或多个)可信应用子网1660(例如,图15的(一个或多个)可信应用子网1560)和(一个或多个)不可信应用子网1662(例如,图15的(一个或多个)不可信应用子网1562)以及包含在数据平面VCN 1618中的互联网网关1634的(一个或多个)LB子网1622。(一个或多个)可信应用子网1660可以可通信地耦合到包含在数据平面VCN 1618中的服务网关1636、包含在数据平面VCN 1618中的NAT网关1638以及包含在数据平面数据层1650中的(一个或多个)DB子网1630。(一个或多个)不可信应用子网1662可以可通信地耦合到包含在数据平面VCN 1618中的服务网关1636和包含在数据平面数据层1650中的(一个或多个)DB子网1630。数据平面数据层1650可以包括可以可通信地耦合到包含在数据平面VCN 1618中的服务网关1636的(一个或多个)DB子网1630。

[0181] (一个或多个)不可信应用子网1662可以包括可以可通信地耦合到驻留在(一个或多个)不可信应用子网1662内的租户虚拟机(VM)1666(1)-(N)的主VNIC 1664(1)-(N)。每个租户VM 1666(1)-(N)可以在相应的容器1667(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 1668中包含的数据平面应用层1646中的应用子网1626。相应的辅助VNIC 1672(1)-(N)可以促进包含在数据平面VCN 1618中的(一个或多个)不可信应用子网1662和包含在容器出口VCN 1668中的应用子网之间的通信。容器出口VCN可以包括可以可通信地耦合到公共互联网1654(例如,图13的公共互联网1354)的NAT网关1638。

[0182] 包含在控制平面VCN 1616中和包含在数据平面VCN 1618中的互联网网关1634可以可通信地耦合到元数据管理服务1652(例如,图13的元数据管理系统1352),该元数据管

理服务1652可以可通信地耦合到公共互联网1654。公共互联网1654可以可通信地耦合到包含在控制平面VCN 1616中并且包含在数据平面VCN 1618中的NAT网关1638。包含在控制平面VCN 1616中并且包含在数据平面VCN 1618中的服务网关1636可以可通信地耦合到云服务1656。

[0183] 在一些示例中,图16的框图1600的体系架构所示的模式可以被认为是图15的框图1500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 1666(1)-(N)中包含的相应容器1667(1)-(N)。容器1667(1)-(N)可以被配置为对包含在数据平面应用层1646的(一个或多个)应用子网1626中的相应辅助VNIC 1672(1)-(N)进行调用,该数据平面应用层1646可以包含在容器出口VCN 1668中。辅助VNIC 1672(1)-(N)可以将调用传输到NAT网关1638,NAT网关1638可以将调用传输到公共互联网1654。在这个示例中,可以由客户实时访问的容器1667(1)-(N)可以与控制平面VCN 1616隔离,并且可以与数据平面VCN 1618中包含的其它实体隔离。容器1667(1)-(N)也可以与来自其它客户的资源隔离。

[0184] 在其它示例中,客户可以使用容器1667(1)-(N)来调用云服务1656。在这个示例中,客户可以运行容器1667(1)-(N)中从云服务1656请求服务的代码。容器1667(1)-(N)可以将该请求传输到辅助VNIC 1672(1)-(N),辅助VNIC 1672(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1654。公共互联网1654可以经由互联网网关1634将请求传输到包含在控制平面VCN 1616中的(一个或多个)LB子网1622。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1626,该(一个或多个)应用子网1626可以经由服务网关1636将请求传输到云服务1656。

[0185] 应当认识到的是,各图中描绘的IaaS体系架构1300、1400、1500、1600可以具有除所描绘的那些之外的其它组件。另外,各图中所示的实施例仅仅是可以结合本公开的实施例的云基础设施系统的一些示例。在一些其它实施例中,IaaS系统可以具有比各图中所示更多或更少的组件、可以组合两个或更多个组件,或者可以具有不同的配置或组件布置。

[0186] 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)。

[0187] 图17图示了其中可以实现各种实施例的示例计算机系统1700。系统1700可以用于实现上述任何计算机系统。如图所示,计算机系统1700包括经由总线子系统1702与多个外围子系统通信的处理单元1704。这些外围子系统可以包括处理加速单元1706、I/O子系统1708、存储子系统1718和通信子系统1724。存储子系统1718包括有形计算机可读存储介质1722和系统存储器1710。

[0188] 总线子系统1702提供用于让计算机系统1700的各种部件和子系统按意图彼此通信的机制。虽然总线子系统1702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1702可以是若干种类型的总线结构中的任何一种,包括存储器总线或存储器控制器、外围总线、以及使用任何各种总线体系架构的局部总线。例如,这种体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线,其可以

被实现为按IEEE P1386.1标准制造的Mezzanine总线。

[0189] 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1704控制计算机系统1700的操作。一个或多个处理器可以被包括在处理单元1704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1704可以被实现为一个或多个独立的处理单元1732和/或1734,其中在每个处理单元中包括单核或多核处理器。在其它实施例中,处理单元1704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。

[0190] 在各种实施例中,处理单元1704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1704中和/或存储子系统1718中。通过适当的编程,(一个或多个)处理器1704可以提供上述各种功能。计算机系统1700可以附加地包括处理加速单元1706,其可以包括数字信号处理器(DSP)、专用处理器,等等。

[0191] I/O子系统1708可以包括用户接口输入设备和用户接口输出设备。用户接口输入设备可以包括键盘、诸如鼠标或轨迹球的定点设备、结合到显示器中的触摸板或触摸屏、滚动轮、点击轮、拨盘、按钮、开关、键盘、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备可以包括,例如,运动感测和/或手势识别设备,诸如的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。

[0192] 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。

[0193] 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1700向用户或其它计算机输出信息的所有可能类型的设备和机制。例如,用户接口输出设备可以包括,但不限于,可视地传达文本、图形和音频/视频信息的各种显示设备,诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备,以及调制解调器。

[0194] 计算机系统1700可以包括包含软件元件、被示为当前位于系统存储器1710中的存储子系统1718。系统存储器1710可以存储可加载并且可在处理单元1704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。

[0195] 取决于计算机系统1700的配置和类型,系统存储器1710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1704立即访问和/或目前正被处理单元1704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1710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1700的元件之间传送信息的基本例程的基本输入/输出系统(BIOS),通常可以被存储在ROM中。作为示例,但不是限制,系统存储器1710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1712,程序数据1714,以及操作系统1716。作为示例,操作系统1716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®**操作系统等)和/或诸如iOS、**Windows®** Phone、**Android®** OS、**BlackBerry®** 10OS和**Palm®** OS操作系统的移动操作系统。

[0196] 存储子系统1718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1718中。这些软件模块或指令可以被处理单元1704执行。存储子系统1718也可以提供用于存储根据本公开被使用的数据的储存库。

[0197] 存储子系统1700也可以包括可被进一步连接到计算机可读存储介质1722的计算机可读存储介质读取器1720。与系统存储器1710一起并且,可选地,与其相结合,计算机可读存储介质1722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。

[0198] 包含代码或代码的部分的计算机可读存储介质1722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)、闪存存储器或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光学储存器、磁带盒、磁带、磁盘储存器或其它磁存储设备,或者其它有形的计算机可读介质。这也可以包括非有形的计算机可读介质,诸如数据信号、数据传输,或者可以被用来发送期望信息并且可以被计算系统1700访问的任何其它介质。

[0199] 作为示例,计算机可读存储介质1722可以包括从不可移除的非易失性磁介质读取或写到其的硬盘驱动器、从可移除的非易失性磁盘读取或写到其的磁盘驱动器、以及从可移除的非易失性光盘(诸如CD ROM、DVD和**Blu-Ray®**盘或其它光学介质)读取或写到其的光盘驱动器。计算机可读存储介质1722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1722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1700提供计算机可读指令、数

据结构、程序模块及其它数据的非易失性存储。

[0200] 通信子系统1724提供到其它计算机系统和网络的接口。通信子系统1724用作用于从其它系统接收数据和从计算机系统1700向其它系统发送数据的接口。例如,通信子系统1724可以使计算机系统1700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1724可以包括用于访问无线语音和/或数据网络的射频(RF)收发器部件(例如,使用蜂窝电话技术,诸如3G、4G或EDGE(用于全球演进的增强型数据速率)的先进数据网络技术,WiFi(IEEE 802.11系列标准),或其它移动通信技术,或其任意组合)、全球定位系统(GPS)接收器部件和/或其它部件。在一些实施例中,作为无线接口的附加或者替代,通信子系统1724可以提供有线网络连接(例如,以太网)。

[0201] 在一些实施例中,通信子系统1724也可以代表可以使用计算机系统1700的一个或多个用户接收结构化和/或非结构化数据馈送1726、事件流1728、事件更新1730等形式的输入通信。

[0202] 举例来说,通信子系统1724可以被配置为实时地从社交网络和/或其它通信服务的用户接收数据馈送1726,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。

[0203] 此外,通信子系统1724也可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1728和/或事件更新1730。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。

[0204] 通信子系统1724也可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1726、事件流1728、事件更新1730,等等,这一个或多个数据库可以与耦合到计算机系统1700的一个或多个流式数据源计算机通信。

[0205] 计算机系统1700可以是各种类型之一,包括手持便携式设备(例如,**iPhone®**蜂窝电话、**iPad®**计算平板电脑、PDA)、可穿戴设备(例如,**Google®**Glass头戴式显示器)、PC、工作站、大型机、信息站、服务器机架、或任何其它数据处理系统。

[0206] 由于计算机和网络的不断变化的本质,在图中绘出的计算机系统1700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部件的许多其它配置是可能的。例如,定制的硬件也可以被使用和/或特定的元素可以用硬件、固件、软件(包括applets)或其组合来实现。另外,也可以采用到诸如网络输入/输出设备之类的其它计算设备的连接。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它方式和/或方法。

[0207] 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。

[0208] 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它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。

[0209] 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、删除和其它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。

[0210] 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。

[0211] 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。

[0212] 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。

[0213] 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。

[0214] 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。

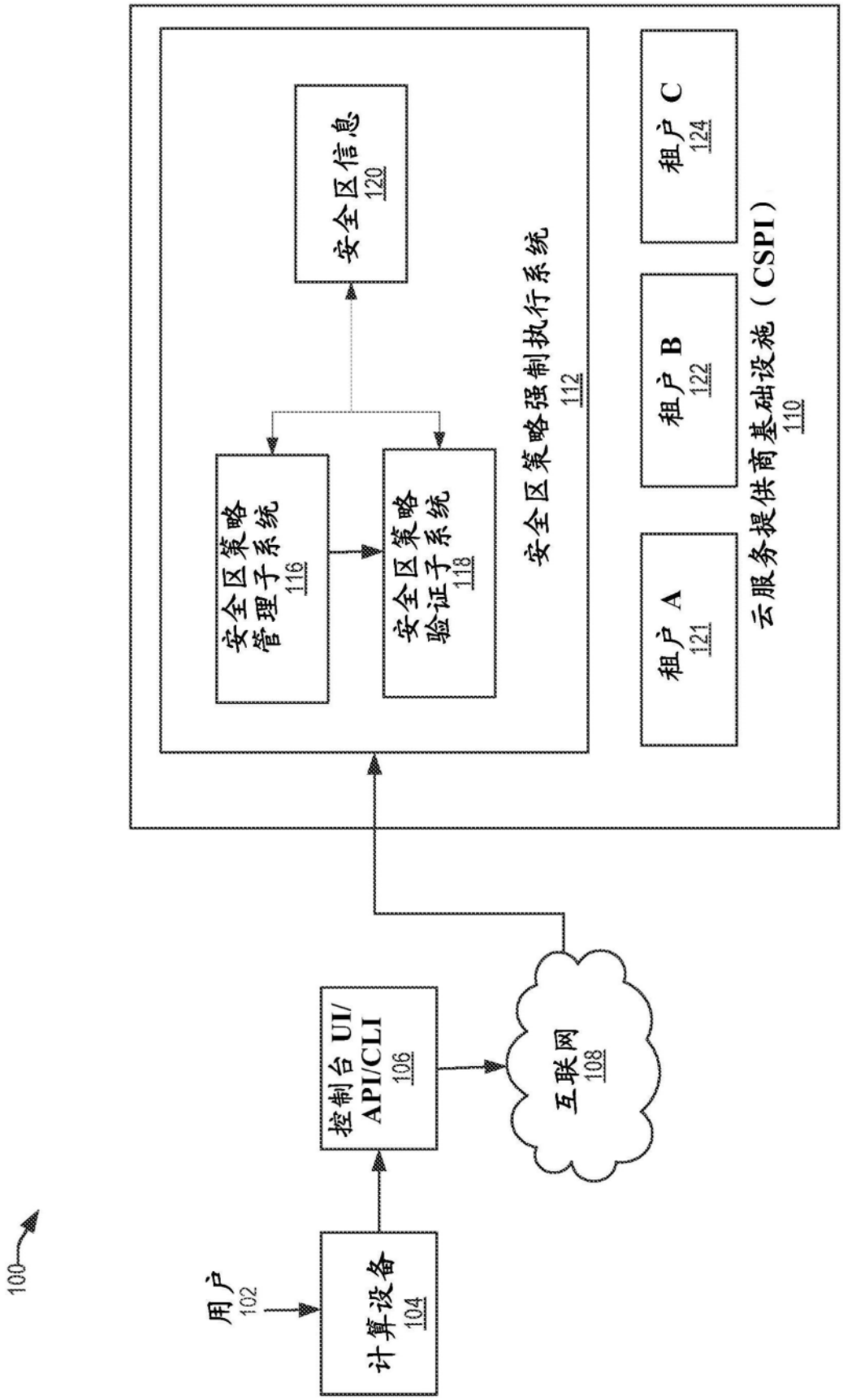

100
用户
102
计算设备
104
控制台 UI/
API/CLI
106
互联网
108
云服务提供商基础设施（CSPI）
110
安全区策略强制执行系统
112
安全区策略
管理子系统
116
安全区策略
验证子系统
118
安全区信息
120
租户 A
121
租户 B
122
租户 C
124

图1

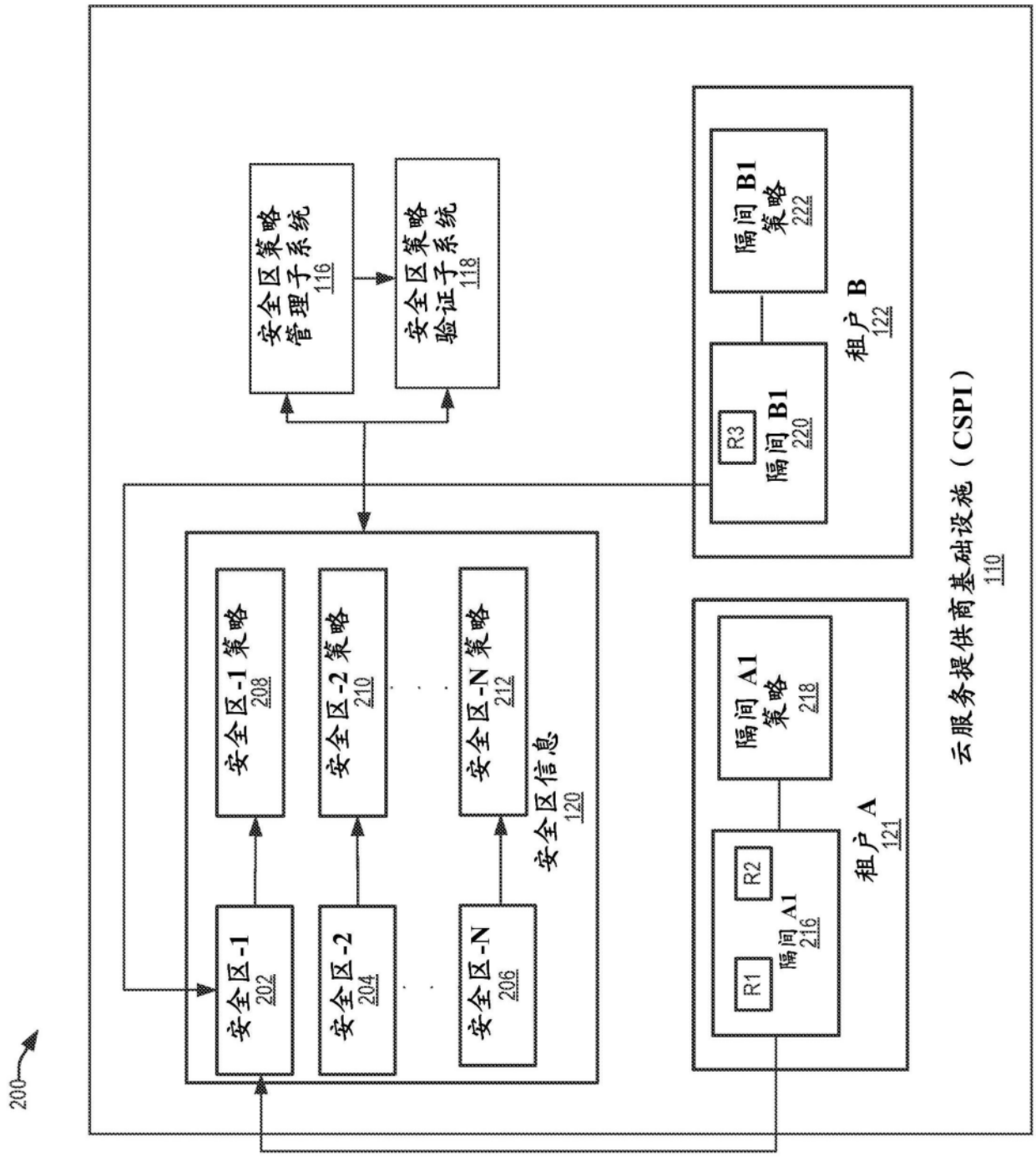

200
云服务提供商基础设施（CSPI）
110
安全区策略管理子系统
116
安全区策略验证子系统
118
安全区信息
120
安全区-1
202
安全区-2
204
安全区-N
206
安全区-1策略
208
安全区-2策略
210
安全区-N策略
212
租户 A
121
隔间 A1
216
R1
R2
隔间 A1策略
218
租户 B
122
隔间 B1
220
R3
隔间 B1策略
222

图2

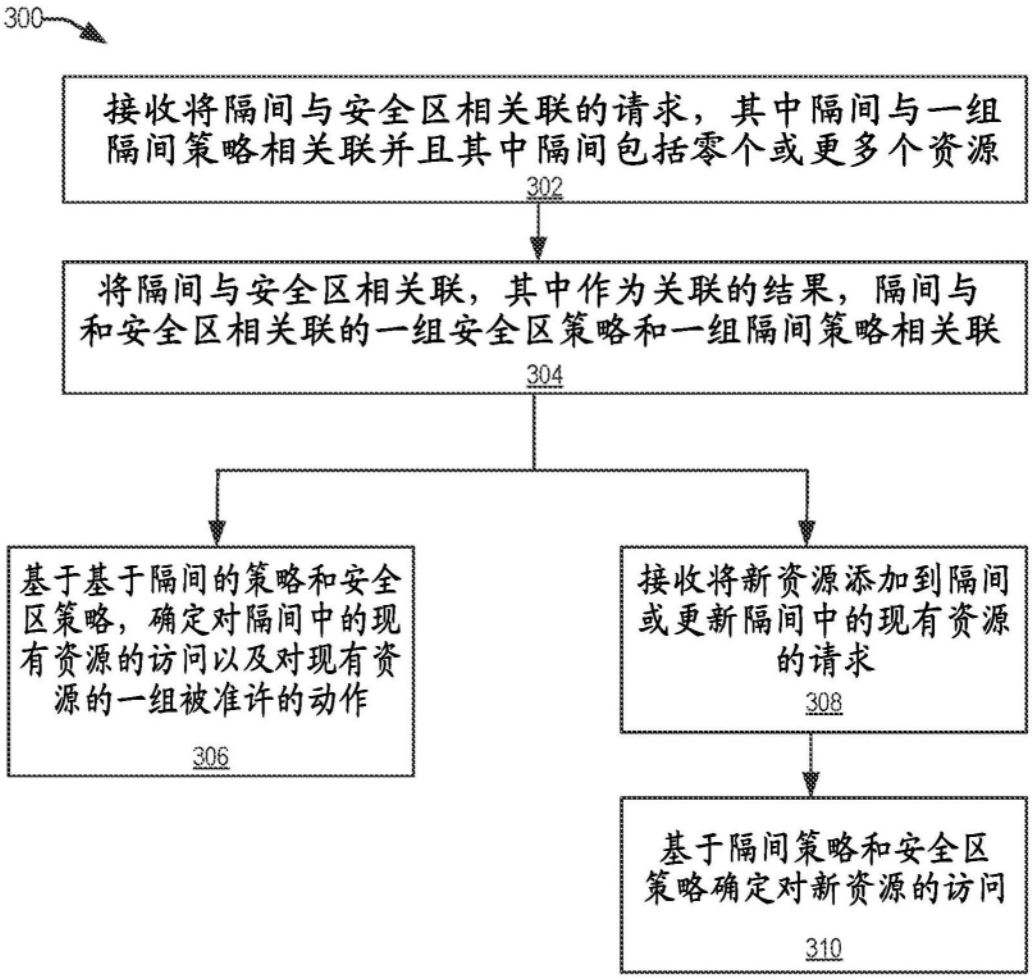

300
接收将隔间与安全区相关联的请求，其中隔间与一组隔间策略相关联并且其中隔间包括零个或更多个资源
302
将隔间与安全区相关联，其中作为关联的结果，隔间与和安全区相关联的一组安全区策略和一组隔间策略相关联
304
基于基于隔间的策略和安全区策略，确定对隔间中的现有资源的访问以及对现有资源的一组被准许的动作
306
接收将新资源添加到隔间或更新隔间中的现有资源的请求
308
基于隔间策略和安全区策略确定对新资源的访问
310

图3

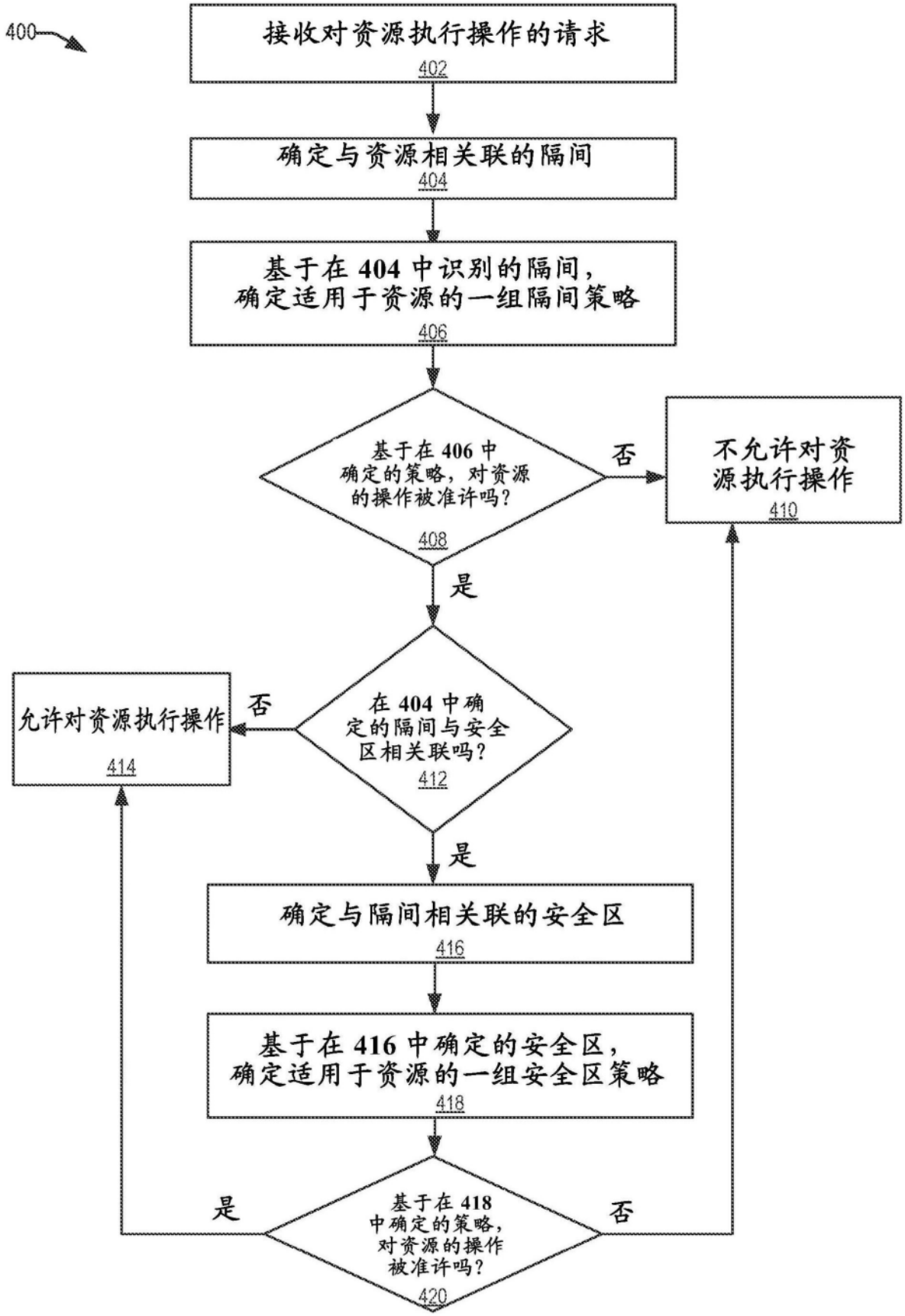

400
接收对资源执行操作的请求
402
确定与资源相关联的隔间
404
基于在 404 中识别的隔间，确定适用于资源的一组隔间策略
406
基于在 406 中确定的策略，对资源的操作被准许吗？
408
否
不允许对资源执行操作
410
是
在 404 中确定的隔间与安全区相关联吗？
412
否
允许对资源执行操作
414
是
确定与隔间相关联的安全区
416
基于在 416 中确定的安全区，确定适用于资源的一组安全区策略
418
基于在 418 中确定的策略，对资源的操作被准许吗？
420
是
否

图4

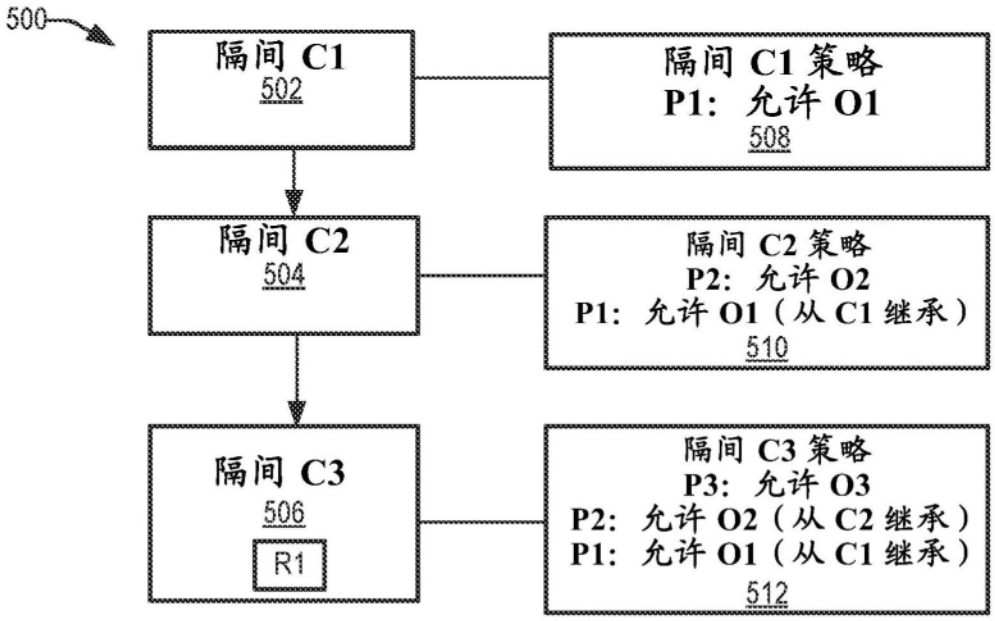

500
隔间 C1
502
隔间 C1 策略
P1: 允许 O1
508
隔间 C2
504
隔间 C2 策略
P2: 允许 O2
P1: 允许 O1（从 C1 继承）
510
隔间 C3
506
R1
隔间 C3 策略
P3: 允许 O3
P2: 允许 O2（从 C2 继承）
P1: 允许 O1（从 C1 继承）
512

图5A

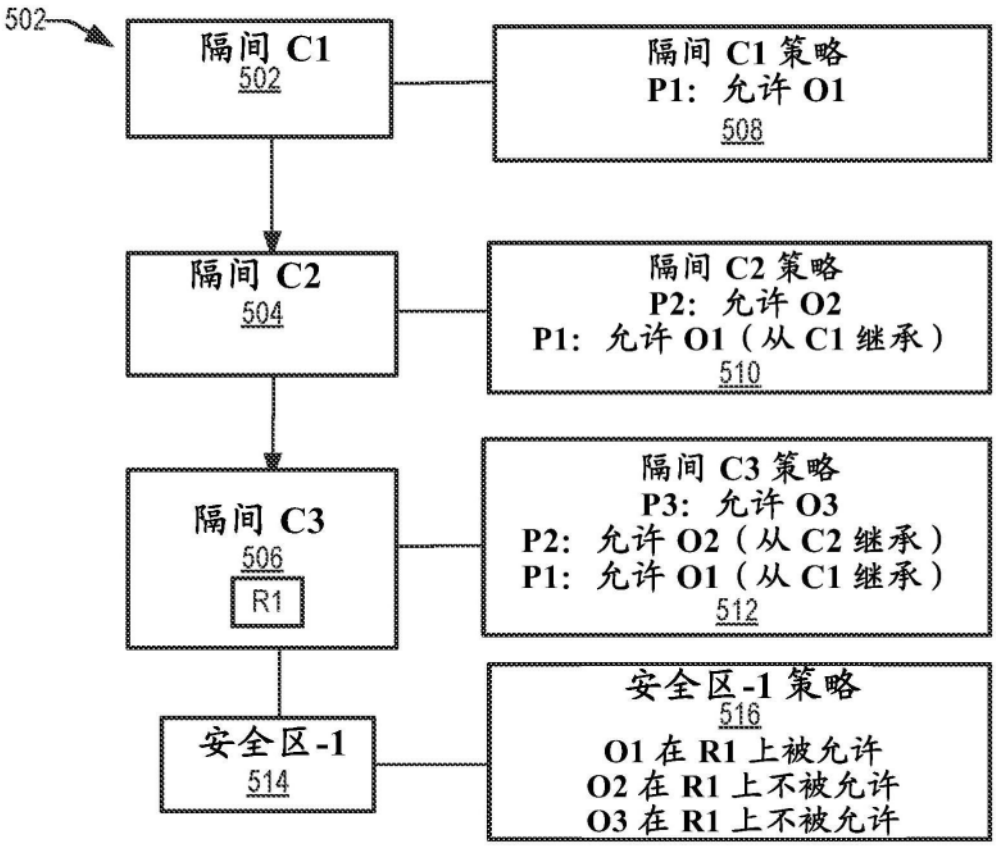

502
隔间 C1
502
隔间 C1 策略
P1: 允许 O1
508
隔间 C2
504
隔间 C2 策略
P2: 允许 O2
P1: 允许 O1（从 C1 继承）
510
隔间 C3
506
R1
隔间 C3 策略
P3: 允许 O3
P2: 允许 O2（从 C2 继承）
P1: 允许 O1（从 C1 继承）
512
安全区-1
514
安全区-1 策略
516
O1 在 R1 上被允许
O2 在 R1 上不被允许
O3 在 R1 上不被允许

图5B

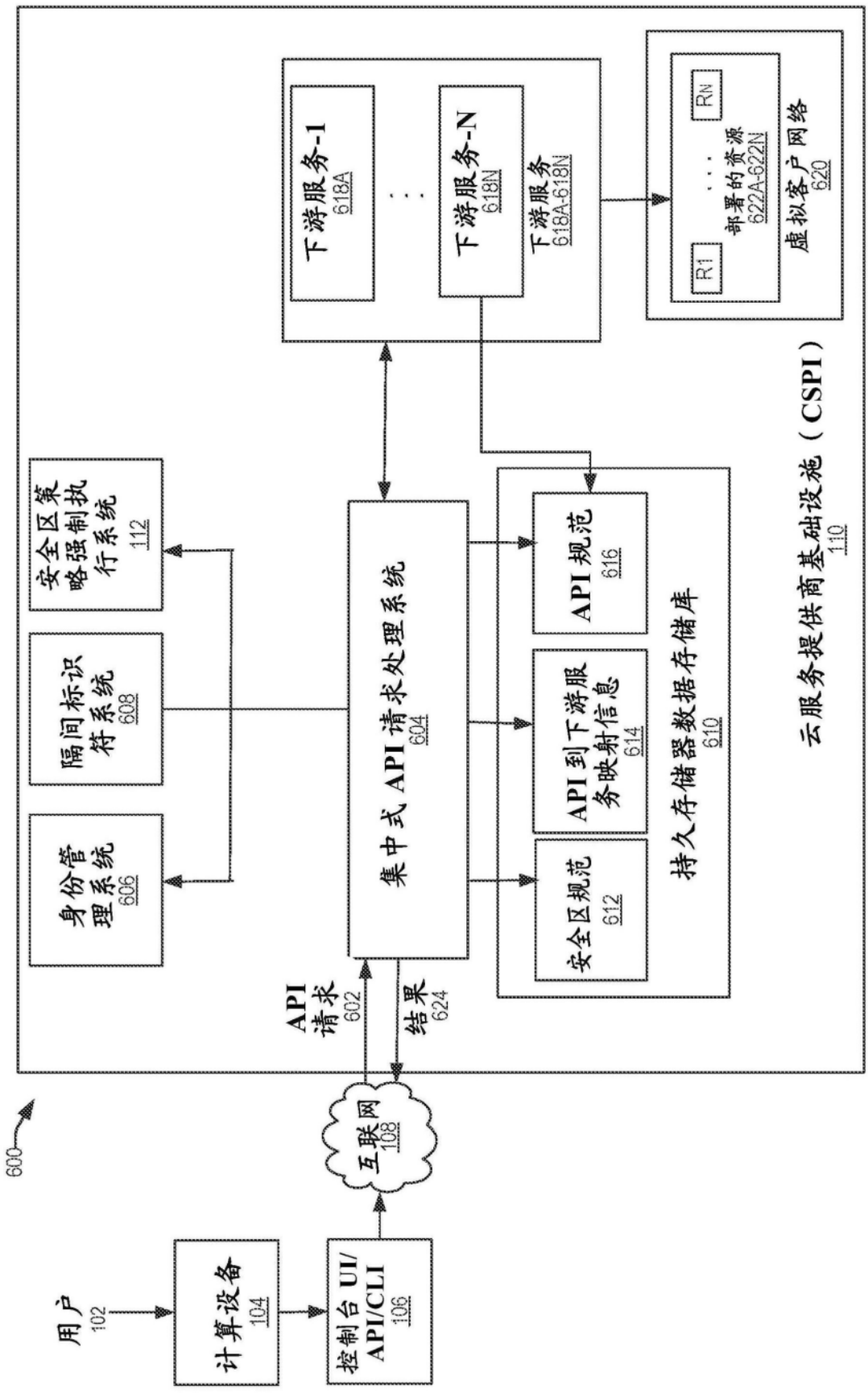

600
用户
102
计算设备
104
控制台 UI/
API/CLI
106
互联网
108
API
请求
602
结果
624
云服务提供商基础设施（CSPI）
110
集中式 API 请求处理系统
604
身份管理系统
606
隔间标识符系统
608
安全区策略强制执行系统
112
持久存储器数据存储库
610
API 规范
616
API 到下游服务映射信息
614
安全区规范
612
下游服务-1
618A
下游服务-N
618N
下游服务
618A-618N
虚拟客户网络
620
R1
RN
部署的资源
622A-622N

图6

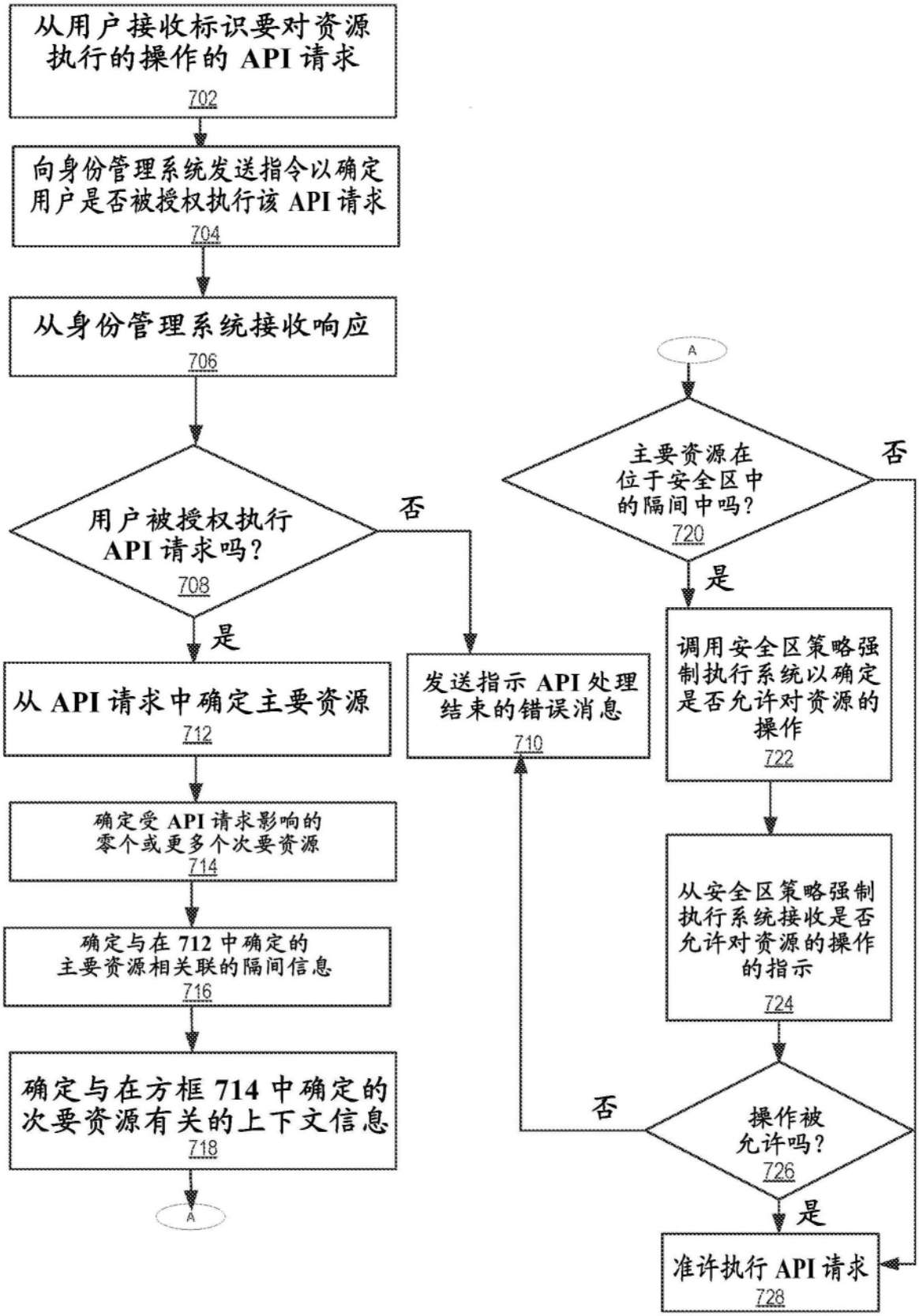

从用户接收标识要对资源执行的操作的 API 请求
702
向身份管理系统发送指令以确定用户是否被授权执行该 API 请求
704
从身份管理系统接收响应
706
用户被授权执行 API 请求吗?
708
否
是
发送指示 API 处理结束的错误消息
710
从 API 请求中确定主要资源
712
确定受 API 请求影响的零个或更多个次要资源
714
确定与在 712 中确定的主要资源相关联的隔间信息
716
确定与在方框 714 中确定的次要资源有关的上下文信息
718
A
A
主要资源在位于安全区中的隔间中吗?
720
否
是
调用安全区策略强制执行系统以确定是否允许对资源的操作
722
从安全区策略强制执行系统接收是否允许对资源的操作的指示
724
操作被允许吗?
726
否
是
准许执行 API 请求
728

图7

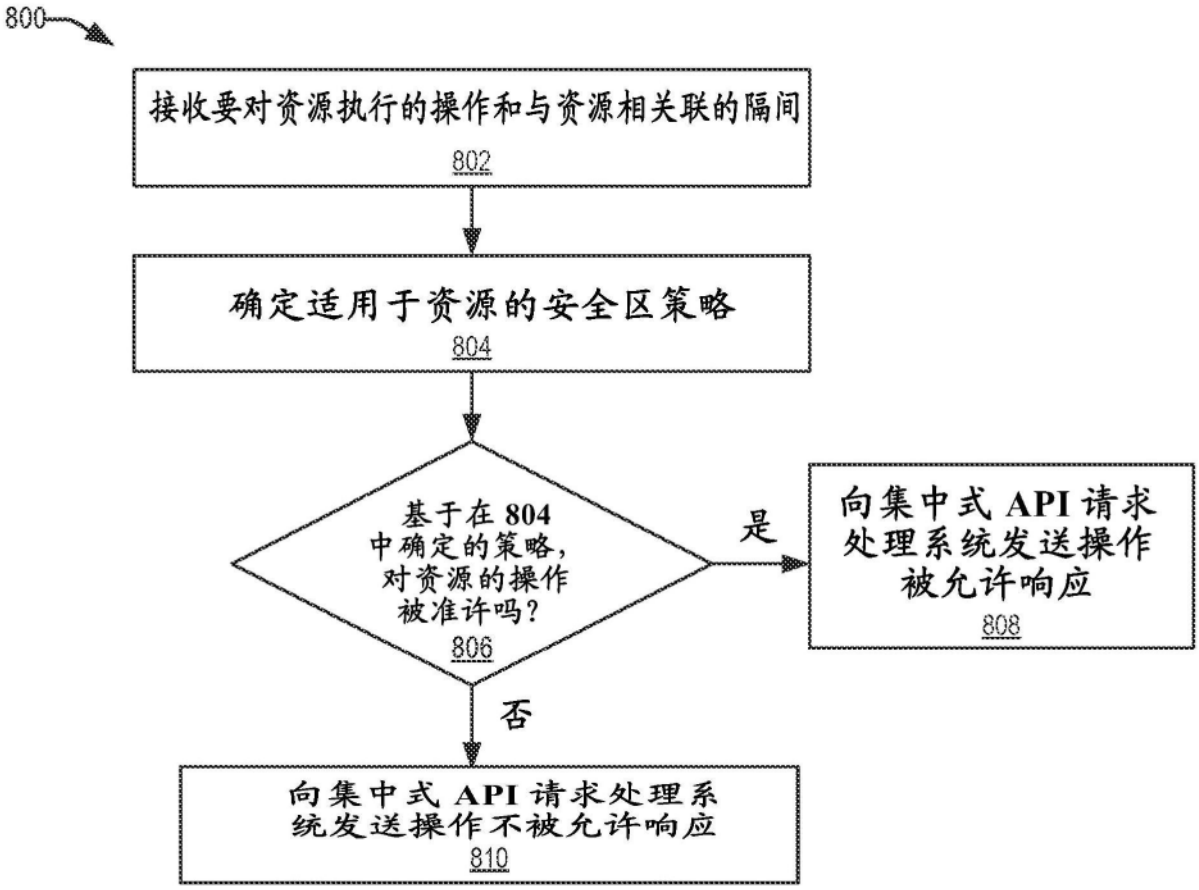

800
接收要对资源执行的操作和与资源相关联的隔间
802
确定适用于资源的安全区策略
804
基于在804中确定的策略，对资源的操作被准许吗？
806
是
向集中式API请求处理系统发送操作被允许响应
808
否
向集中式API请求处理系统发送操作不被允许响应
810

图8

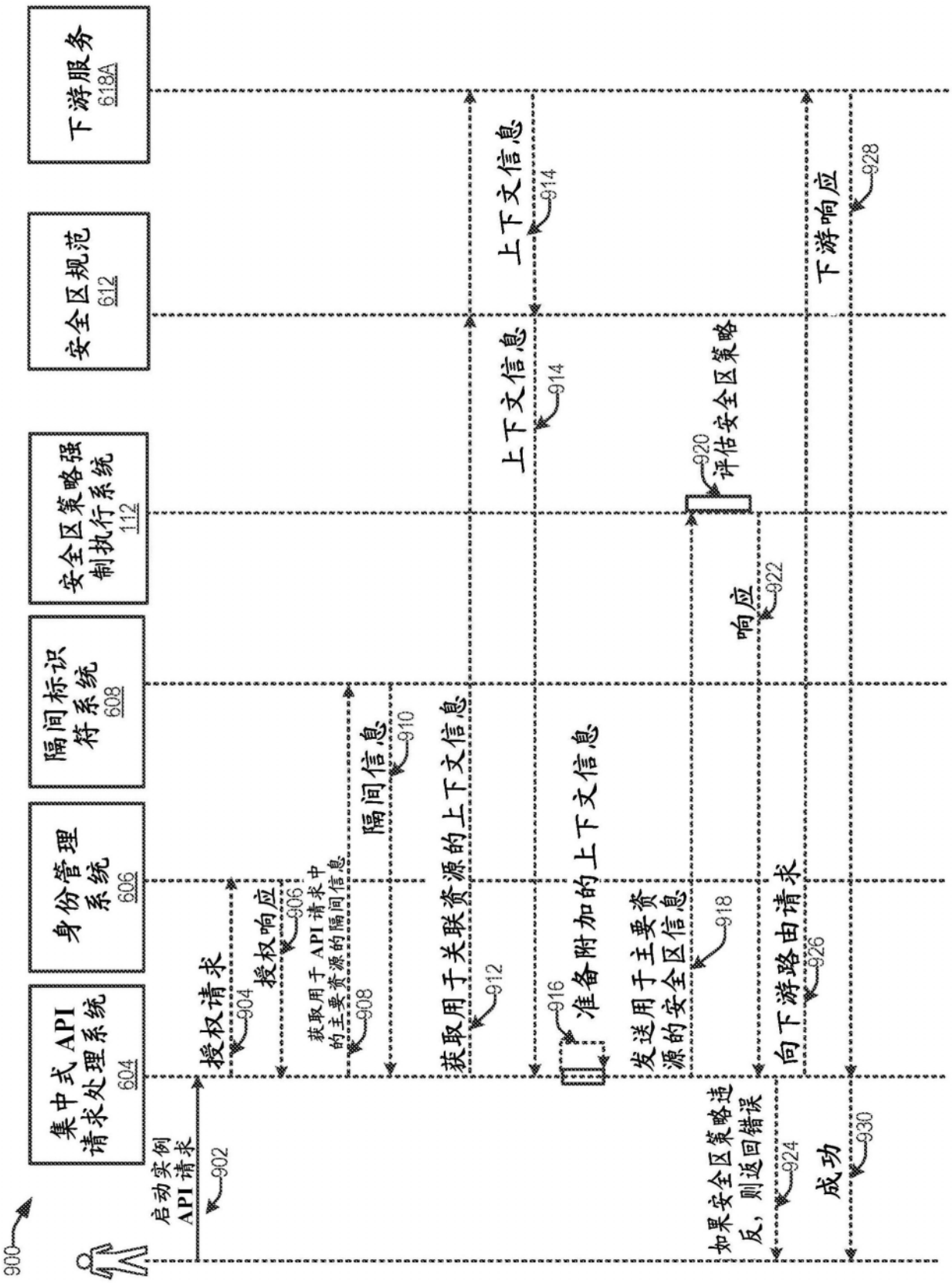

900
集中式API请求处理系统 604
身份管理系统 606
隔间标识符系统 608
安全区策略强制执行系统 112
安全区规范 612
下游服务 618A
启动实例API请求
902
授权请求
904
授权响应
906
获取用于API请求中的主要资源的隔间信息
908
隔间信息
910
获取用于关联资源的上下文信息
912
上下文信息
914
准备附加的上下文信息
916
上下文信息
914
发送用于主要资源的安全区信息
918
评估安全区策略
920
响应
922
如果安全区策略违反，则返回错误
924
向下游路由请求
926
下游响应
928
成功
930

图9

1000

```
service: compute
  operations: [
    # LAUNCH_INSTANCE
    {
      id: LaunchInstance
      associatedResources: [
        {
          name: instance
          compartmentIdExpression: "request.body.compartmentId"
          isPrimary: true
        }
        {
          name: boot volume
          associationPredicate: "request.body.sourceDetails?.sourceType == 'bootVolume'"
          contextFetchExpression:
          "downstream.getOr404('blockstorage','GetBootVolume',request.body.sourceDetails.bootVolumeId)"
          compartmentIdExpression: "context['bootvolume'].compartmentId"
        }
        {
          name: image
          associationPredicate: "request.body.sourceDetails?.sourceType == 'image'"
          contextFetchExpression: "downstream.getOr404('compute-
imaging','GetImage',request.body.sourceDetails.imageId)"
        }
        {
          name: subnet
          associationPredicate: "request.body.createVnicDetails?.subnetId != null"
          contextFetchExpression:
          "downstream.getOr404('virtualNetwork','GetSubnet',request.body.createVnicDetails.subnetId)"
          compartmentIdExpression: "context['subnet'].compartmentId"
        }
      ]
      context: {
        image: [
          {
            contextName: compartmentId
            contextValueExpression: "context['image']?.compartmentId"
          }
          {
            contextName: kmsKeyId
            contextValueExpression: "request.body.sourceDetails?.kmsKeyId"
          }
        ]
      }
  }
```

图10

1100

```
service: compute
operations: [
 # ATTACH_VOLUME
  {
   id: AttachVolume
   associatedResources: [
    {
     name: instance
     contextFetchExpression:
     "downstream.getOr404('compute','GetInstance',splat.getOrThrow(request.body.instanceId,
'MissingParameter'))"
     compartmentIdExpression: "context['instance'].compartmentId"
     isPrimary: true
    }
    {
     name: volume
     contextFetchExpression: """
        downstream.getOr404(
        'blockstorage',
        splat.getEntityType(request.body.volumeId) == 'bootvolume' ? 'GetBootVolume' : 'GetVolume',
        splat.getOrThrow(request.body.volumeId, 'MissingParameter'))"""
     compartmentIdExpression: "context['volume'].compartmentId"
    }
   ]
   context: {
   }
  }
  # ATTACH_BOOT_VOLUME
  {
   id: AttachBootVolume
   associatedResources: [
    {
     name: instance
     contextFetchExpression:
     "downstream.getOr404('compute','GetInstance',splat.getOrThrow(request.body.instanceId,
'MissingParameter'))"
     compartmentIdExpression: "context['instance'].compartmentId"
     isPrimary: true
    }
    {
     name: bootvolume
     contextFetchExpression:
"downstream.getOr404('blockstorage','GetBootVolume',splat.getOrThrow(request.body.bootVolumeId,
'MissingParameter'))"
     compartmentIdExpression: "context['bootvolume'].compartmentId"
    }
   ]
   context: {
   }
  }
  # CHANGE_INSTANCE_COMPARTMENT
  {
   id: ChangeInstanceCompartment
   associatedResources: [
    {
     name: instance
     contextFetchExpression: "downstream.getOr404('compute','GetInstance',request.resourceId)"
     compartmentIdExpression: "context['instance'].compartmentId"
     destinationCompartmentIdExpression: "request.body.compartmentId"
     isPrimary: true
    }
   ]
   context: {
   }
  }
 ]
}
```

图11


1200
service: virtual network
operations: [
{
id: CreateSubnet
associatedResources: [
{
name: subnet
compartmentIdExpression: "request.body.compartmentId"
isPrimary: true
}
]
context: {
subnet: [
{
contextName: prohibitPublicIpOnVnic
contextValueExpression: "request.body.prohibitPublicIpOnVnic ?: false"
}
]
}
}
{
id: CreateInternetGateway
associatedResources: [
{
name: internetgateway
compartmentIdExpression: "request.body.compartmentId"
isPrimary: true
}
]
context: {
}
}
{
id: ChangeSubnetCompartment
associatedResources: [
{
name: subnet
contextFetchExpression:
"downstream.getOr404('virtualNetwork','GetSubnet',request.resourceId)"
compartmentIdExpression: "context['subnet'].compartmentId"
destinationCompartmentIdExpression: "request.body.compartmentId"
isPrimary: true
}
]
context: {
subnet: [
{
contextName: prohibitPublicIpOnVnic
contextValueExpression: "context['subnet'].prohibitPublicIpOnVnic"
}
]
}
}
{
id: ChangeInternetGatewayCompartment
associatedResources: [
{
name: internetgateway
destinationCompartmentIdExpression: "request.body.compartmentId"
isPrimary: true
}
]
context: {
}
}
]
}

图12

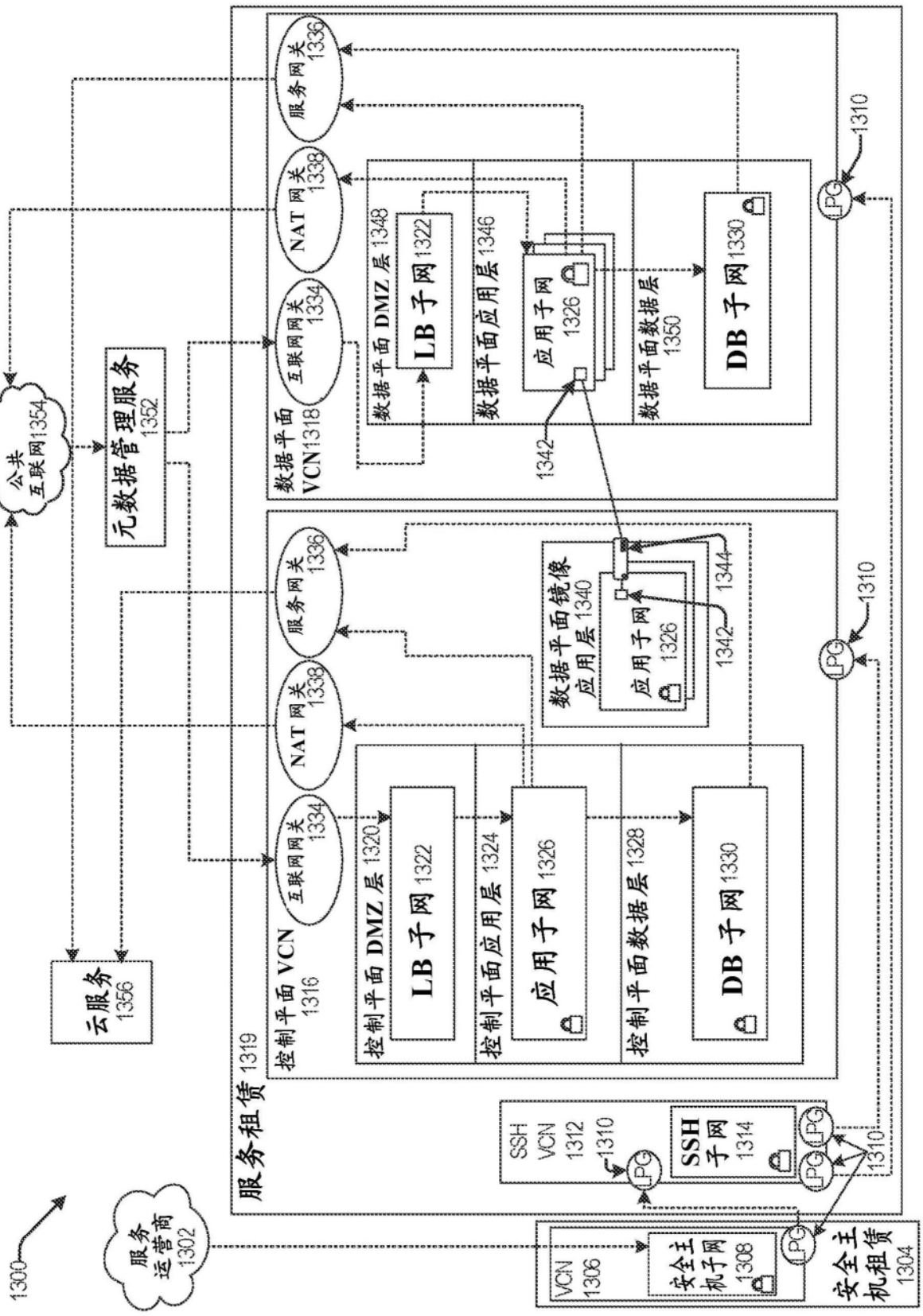

1300
服务运营商 1302
公共互联网 1354
元数据管理服务 1352
云服务 1356
服务租赁 1319
控制平面 VCN 1316
互联网网关 1334
NAT 网关 1338
服务网关 1336
控制平面 DMZ 层 1320
LB 子网 1322
控制平面应用层 1324
应用子网 1326
控制平面数据层 1328
DB 子网 1330
数据平面镜像应用层 1340
1342
1344
数据平面 VCN 1318
数据平面 DMZ 层 1348
数据平面应用层 1346
数据平面数据层 1350
SSH VCN 1312
SSH 子网 1314
VCN 1306
安全主机子网 1308
安全主机租赁 1304
PG
1310

图13

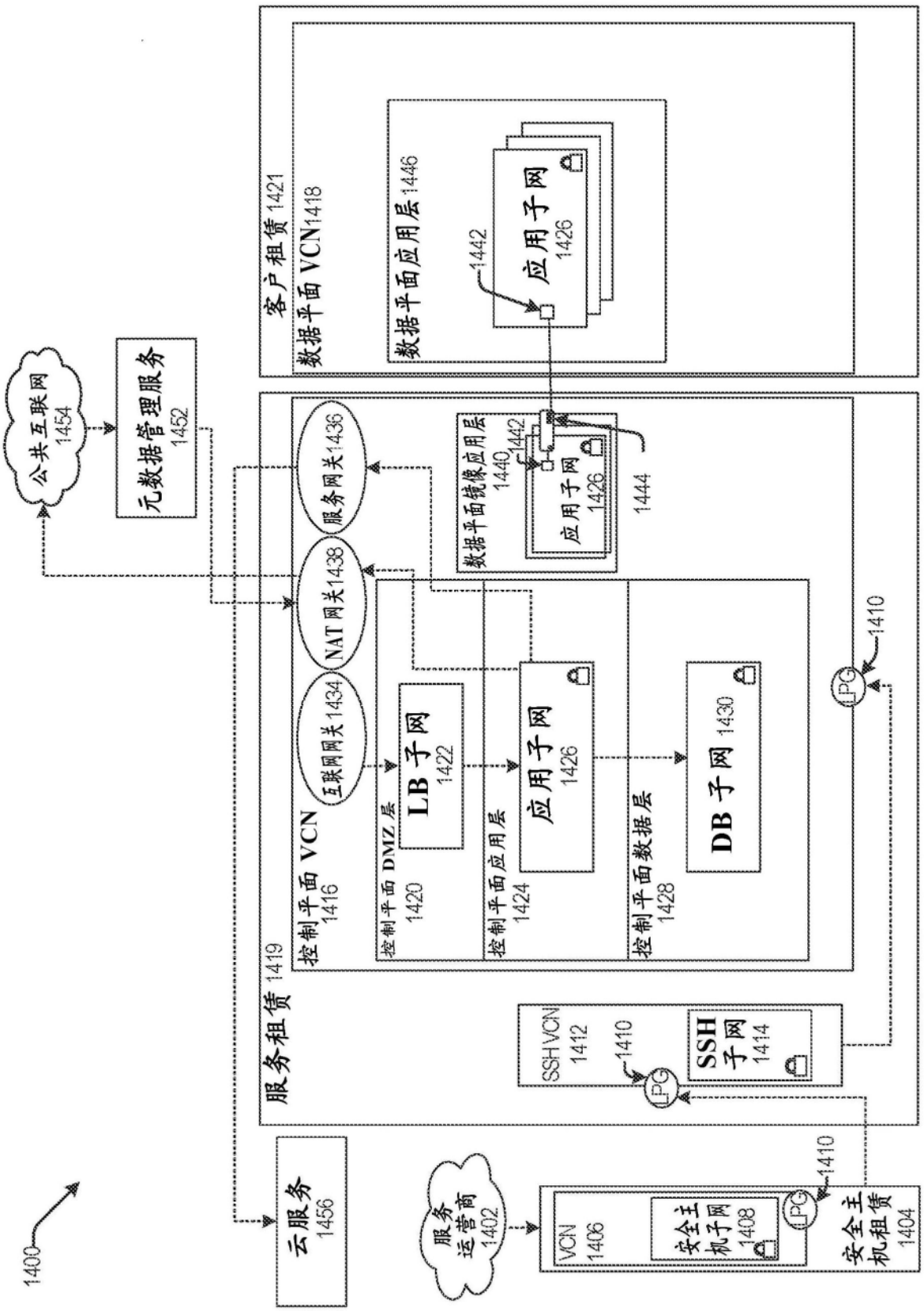

1400
公共互联网 1454
元数据管理服务 1452
云服务 1456
服务运营商 1402
客户租赁 1421
数据平面 VCN1418
数据平面应用层 1446
1442
应用子网 1426
服务租赁 1419
控制平面 VCN 1416
互联网网关 1434
NAT 网关1438
服务网关1436
数据平面镜像应用层 1440
1444
控制平面 DMZ 层 1420
LB 子网 1422
控制平面应用层 1424
控制平面数据层 1428
DB 子网 1430
1410
SSH VCN 1412
SSH 子网 1414
VCN 1406
安全主机子网 1408
安全主机租赁 1404

图14

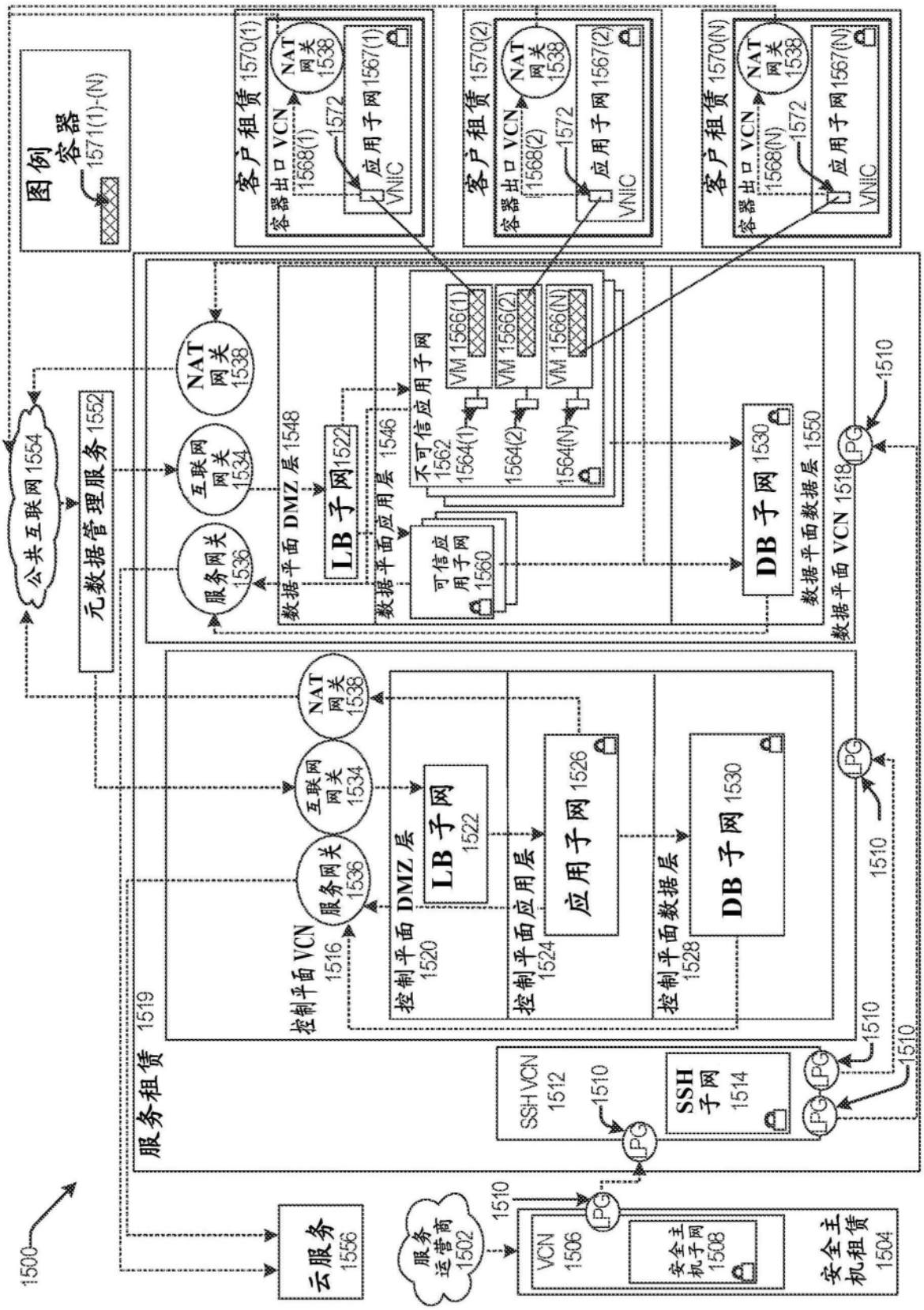

图例
容器 1571(1)-(N)
客户租赁 1570(1)
容器出口 VCN 1568(1)
NAT 网关 1538
1572
应用子网 1567(1)
VNIC
客户租赁 1570(2)
容器出口 VCN 1568(2)
应用子网 1567(2)
客户租赁 1570(N)
容器出口 VCN 1568(N)
应用子网 1567(N)
公共互联网 1554
元数据管理服务 1552
互联网网关 1534
服务网关 1536
数据平面 DMZ 层 1548
LB 子网 1522
数据平面应用层 1546
不可信应用子网 1562
VM 1566(1)
VM 1566(2)
VM 1566(N)
1564(1)
1564(2)
1564(N)
可信应用子网 1560
DB 子网 1530
数据平面数据层 1550
数据平面 VCN 1518
1510
服务租赁 1519
控制平面 VCN 1516
控制平面 DMZ 层 1520
控制平面应用层 1524
应用子网 1526
控制平面数据层 1528
SSH VCN 1512
SSH 子网 1514
LPG
1500
云服务 1556
服务运营商 1502
VCN 1506
安全主机子网 1508
安全主机租赁 1504

图15

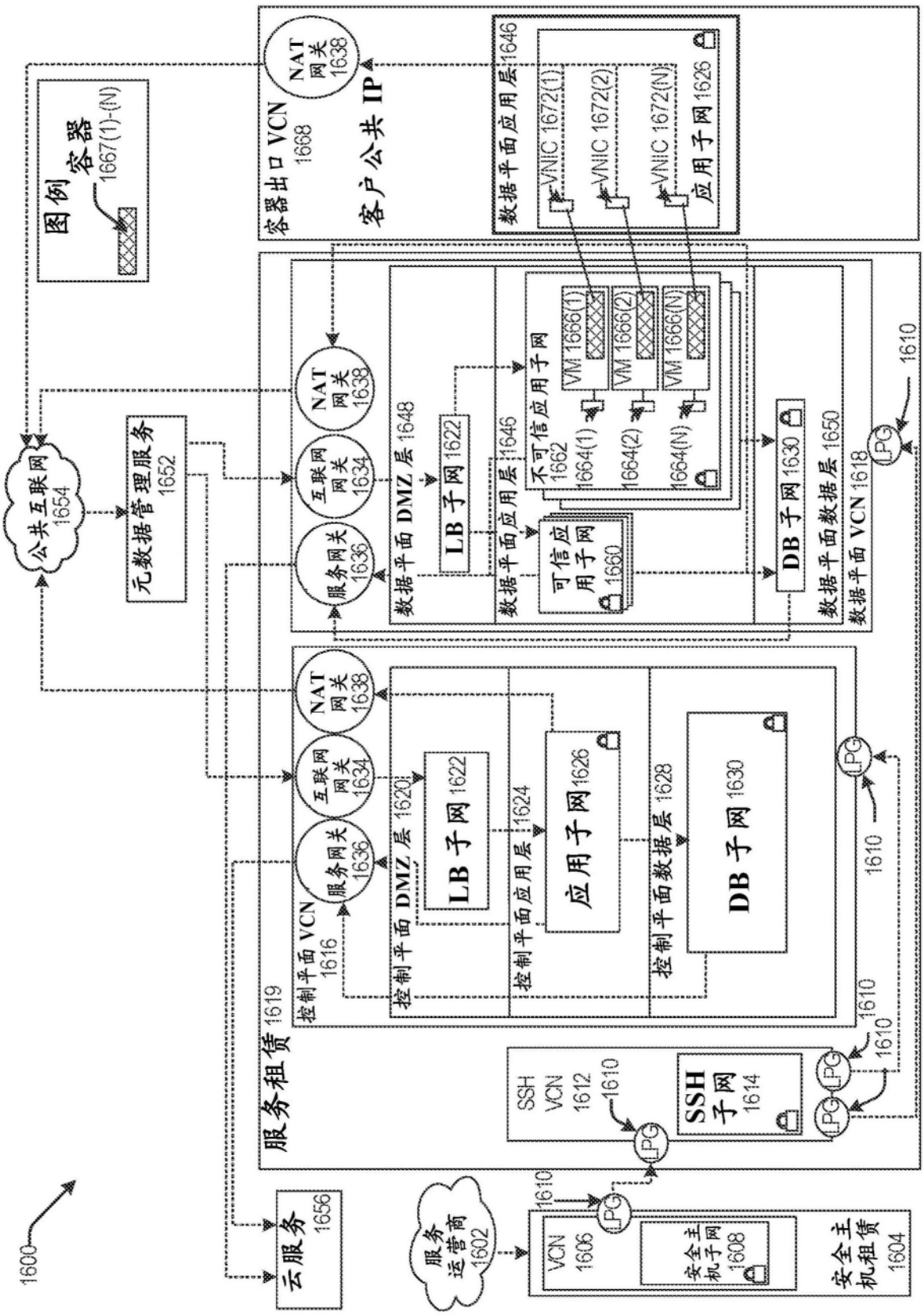

1600
图例
容器 1667(1)-(N)
容器出口 VCN 1668
客户公共 IP
NAT 网关 1638
数据平面应用层 1646
VNIC 1672(1)
VNIC 1672(2)
VNIC 1672(N)
应用子网 1625
公共互联网 1654
元数据管理服务 1652
互联网网关 1634
服务网关 1636
数据平面 DMZ 层 1648
LB 子网 1622
数据平面应用层 1645
不可信应用子网 1662
VM 1666(1)
VM 1666(2)
VM 1666(N)
1664(1)
1664(2)
1664(N)
可信应用子网 1660
DB 子网 1630
数据平面数据层 1650
数据平面 VCN 1618
1610
服务租赁 1619
控制平面 VCN 1616
控制平面 DMZ 层 1620
控制平面应用层 1624
控制平面数据层 1628
SSH VCN 1612
SSH 子网 1614
LPG
云服务 1656
服务运营商 1602
VCN 1606
安全主机子网 1608
安全主机租赁 1604

图16

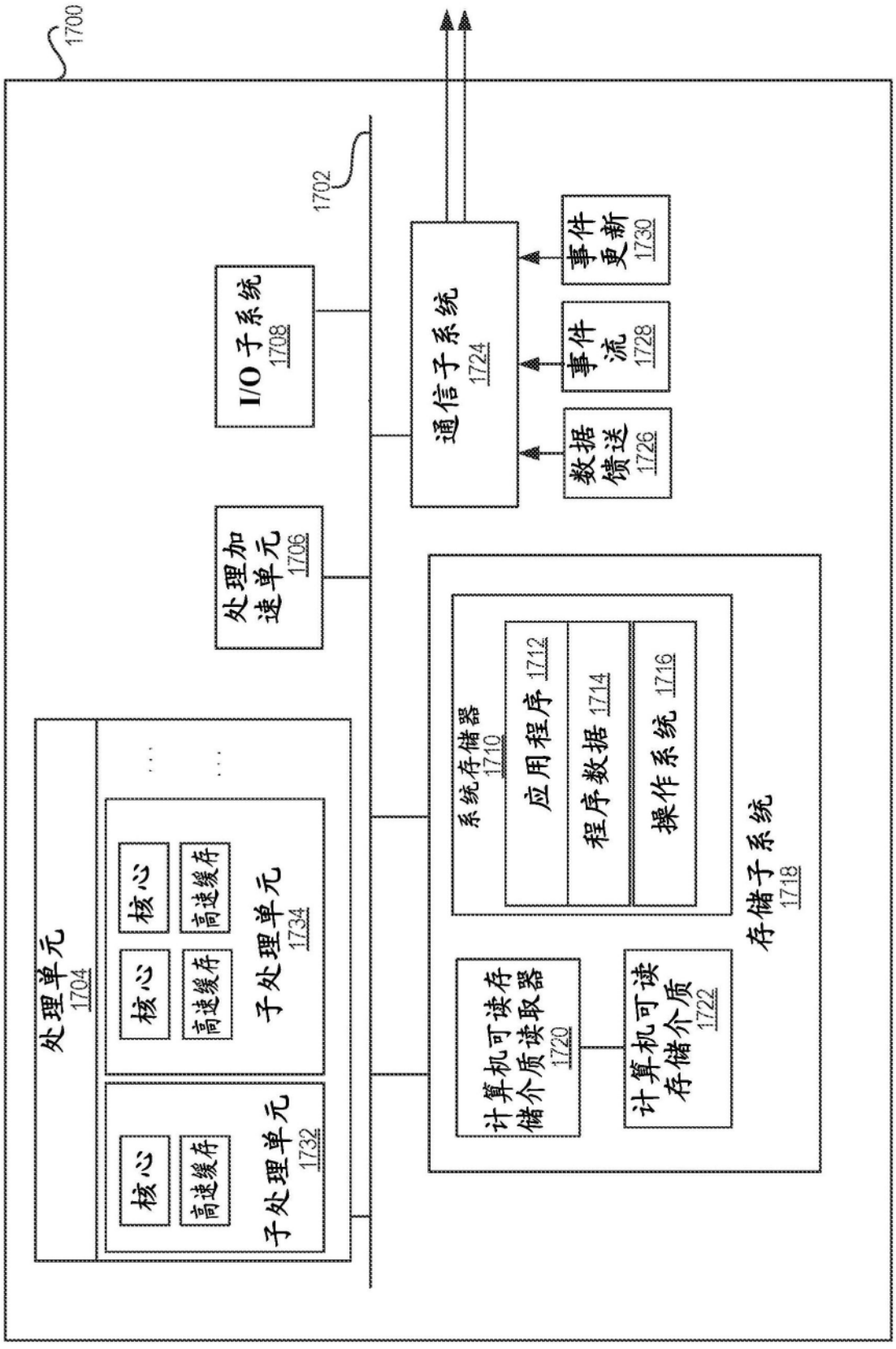

1700
1702
处理单元
1704
核心
高速缓存
核心
高速缓存
子处理单元
1732
核心
高速缓存
核心
高速缓存
子处理单元
1734
I/O子系统
1708
处理加速单元
1706
通信子系统
1724
事件更新
1730
事件流
1728
数据馈送
1726
存储子系统
1718
系统存储器
1710
应用程序 1712
程序数据 1714
操作系统 1716
计算机可读存储介质读取器
1720
计算机可读存储介质
1722

图17