



(12) 发明专利

(10) 授权公告号 CN 110830357 B

(45) 授权公告日 2022. 01. 21

(21) 申请号 201910739288.7

(51) Int.Cl.

(22) 申请日 2019.08.12

H04L 12/46 (2006.01)

G06F 9/455 (2006.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 110830357 A

审查员 巫吟荷

(43) 申请公布日 2020.02.21

(30) 优先权数据

62/718,869 2018.08.14 US

16/132,209 2018.09.14 US

(73) 专利权人 瞻博网络公司

地址 美国加利福尼亚

(72) 发明人 圣胡·C·亚伯拉罕

(74) 专利代理机构 北京康信知识产权代理有限

责任公司 11240

代理人 王红艳

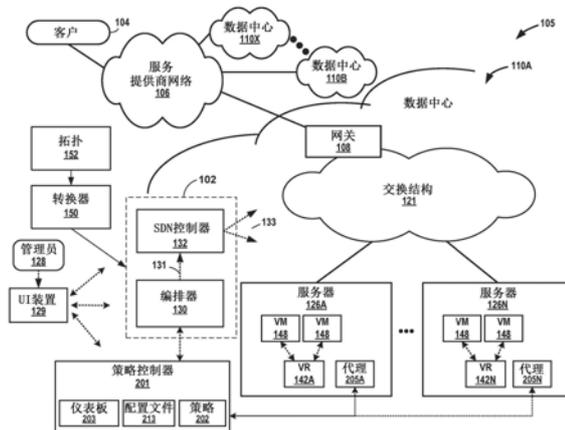
权利要求书3页 说明书40页 附图12页

(54) 发明名称

使用高级拓扑描述的多云虚拟计算环境供应

(57) 摘要

本公开涉及使用高级拓扑描述的多云虚拟计算环境供应。在一个示例中，一种方法可以包括由计算装置获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述。每个计算基础设施可以使用不同的计算架构来实现，并且由不同的提供商来部署。该示例方法还可以包括：通过在计算装置上执行的规则引擎，将高级拓扑描述转换为计算基础设施的相应模板，每个模板以符合模式的格式描述虚拟计算环境的拓扑，该模式可以由相应的一个计算基础设施处理，以在相应的一个计算基础设施中实现虚拟计算环境，并且输出用于配置计算基础设施的模板。



1. 一种供应虚拟计算环境的方法,所述方法包括:

由计算装置获得要在多个计算基础设施中供应的所述虚拟计算环境的高级拓扑描述,其中,所述高级拓扑描述包括多个对象,其中,所述多个计算基础设施中的每个计算基础设施使用多个计算架构中不同的计算架构来实现,并且其中,所述多个计算基础设施中的每个计算基础设施由不同的提供商来部署;

通过在所述计算装置上执行的规则引擎,将所述高级拓扑描述转换为针对所述多个计算基础设施的相应模板,其中,所述多个模板中的每个模板以符合模式的格式描述所述虚拟计算环境的拓扑,所述模式能够由所述多个计算基础设施中的相应的一个计算基础设施处理,以在所述多个计算基础设施中的所述相应的一个计算基础设施中实现所述虚拟计算环境;并且

其中,转换所述高级拓扑描述包括确定所述多个对象中的对象是用于所述多个计算基础设施中的计算基础设施的对象,并且响应于所述确定,生成所述多个模板中的用于所述多个计算基础设施中的所述计算基础设施的模板以包括所述对象以用于在所述计算基础设施中供应;并且

使用所述多个模板的相应模板供应所述多个计算基础设施中的每个计算基础设施,以实现所述虚拟计算环境。

2. 根据权利要求1所述的方法,

其中,所述虚拟计算环境的所述高级拓扑描述包括用人类可读数据串行化语言编码的文本文件,并且

其中,所述虚拟计算环境的所述高级拓扑描述包括虚拟网络、存储器和由虚拟计算环境提供的服务中的至少一个。

3. 根据权利要求2所述的方法,其中,所述人类可读数据串行化语言包括YAML非标记语言(YAML)。

4. 根据权利要求1所述的方法,其中,所述方法还包括将一个或多个虚拟执行元件部署到所述虚拟计算环境。

5. 根据权利要求1所述的方法,

其中,所述拓扑为每个所述计算基础设施定义一个或多个项目,并且

其中,针对计算基础设施的所述一个或多个项目中的每个项目定义了要在所述计算基础设施中供应的相应虚拟私有云。

6. 根据权利要求1所述的方法,其中,获得所述高级拓扑描述包括获得包括多个字段的所述高级拓扑描述,所述多个字段包括提供商、组织、项目和至少一个实例中的至少一个。

7. 根据权利要求6所述的方法,其中,所述至少一个实例包括名称、角色、供应、用户名、接口、协议、可用性区域、机器ID、实例类型、子网、安全组和体积大小中的至少一个。

8. 根据权利要求1所述的方法,其中,将所述高级拓扑描述转换为所述模板,包括基于所述高级拓扑描述创建相应模板,其中,基础设施即代码(IaC)软件被配置为使用所述模板在所选择的一个计算基础设施中实现所述虚拟计算环境。

9. 根据权利要求8所述的方法,其中,IaC软件包括Terraform。

10. 根据权利要求1所述的方法,其中,所述提供商包括亚马逊网络服务(AWS)、谷歌云平台(GCP)和微软Azure中的至少一个。

11. 根据权利要求1至10中任一项所述的方法,其中,将所述高级拓扑描述转换为所述模板包括基于所述规则引擎的一组规则将所述高级拓扑描述转换为所述模板。

12. 根据权利要求11所述的方法,其中,基于所述一组规则将所述高级拓扑描述转换为所述模板包括:

对于所述一组规则中的规则,将一组条件应用于所述高级拓扑描述,

对于所述一组条件中的每个应用条件,确定相应条件是否表示成功;并且

响应于确定所述一组条件中的至少一个条件表示成功,使用所述计算装置执行对应于所述一组规则中的规则的事件。

13. 根据权利要求12所述的方法,其中,所述对象是第一对象,并且其中,执行所述事件包括:

在所述高级拓扑描述中识别所述多个对象中对应于提供商的第二对象;并且

根据对应于所述第二对象的所述提供商,将所述第二对象放置在所述相应模板的模板中。

14. 一种计算系统,包括:

一个或多个处理器,耦接到存储器,其中,所述一个或多个处理器被配置为:

获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述,其中,所述高级拓扑描述包括多个对象,其中,所述多个计算基础设施中的每个计算基础设施使用多个计算架构中不同的计算架构来实现,并且其中,所述多个计算基础设施中的每个计算基础设施由多个提供商中不同的提供商来部署;

将所述高级拓扑描述转换为所述多个计算基础设施的相应模板,其中,所述多个模板中的每个模板以符合模式的格式描述虚拟计算环境的拓扑,所述模式能够由所述多个计算基础设施中的相应的一个计算基础设施处理,以在所述多个计算基础设施中的所述相应的一个计算基础设施中实现所述虚拟计算环境;并且

其中,转换所述高级拓扑描述,所述一个或多个处理器被配置为确定所述多个对象中的对象是用于所述多个计算基础设施中的计算基础设施的对象,并且响应于所述确定,生成所述多个模板中的用于所述多个计算基础设施中的所述计算基础设施的模板以包括所述对象以用于在第一计算基础设施中供应;并且

使用所述多个模板的相应模板供应所述多个计算基础设施中的每个计算基础设施,以实现所述虚拟计算环境。

15. 根据权利要求14所述的计算系统,

其中,所述虚拟计算环境的所述高级拓扑描述包括用人类可读数据串行化语言编码的文本文件,并且

其中,所述虚拟计算环境的所述高级拓扑描述包括虚拟网络、存储器和由所述虚拟计算环境提供的服务中的至少一个。

16. 根据权利要求14所述的计算系统,其中,所述一个或多个处理器还被配置为将一个或多个虚拟执行元件部署到所述虚拟计算环境。

17. 根据权利要求14至16中任一项所述的计算系统,其中,为了将所述高级拓扑描述转换为所述相应模板,所述一个或多个处理器被配置为基于规则引擎的一组规则将所述高级拓扑描述转换为所述模板。

18. 根据权利要求17所述的计算系统,其中,为了基于所述一组规则将所述高级拓扑描述转换为所述相应模板,所述一个或多个处理器被配置为:

对于所述一组规则的规则,将一组条件应用于所述高级拓扑描述,

对于所述一组条件中的每个应用条件,确定相应条件是否表示成功;并且

响应于确定所述一组条件中的至少一个条件表示成功,执行对应于所述一组规则中的规则的事件。

19. 根据权利要求18所述的计算系统,其中,所述对象是第一对象,并且其中,为了执行所述事件,所述一个或多个处理器被配置为

在所述高级拓扑描述中识别所述多个对象中对应于提供商的第二对象;并且

根据对应于所述第二对象的所述提供商,将所述第二对象放置在所述相应模板的模板中。

20. 一种非暂时性计算机介质,包括用于使一个或多个处理器执行以下操作的指令:

获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述,其中,所述高级拓扑描述包括多个对象,其中,所述多个计算基础设施中的每个计算基础设施使用多个计算架构中不同的计算架构来实现,并且其中,所述多个计算基础设施中的每个计算基础设施由多个提供商中不同的提供商来部署;

将所述高级拓扑描述转换为所述多个计算基础设施的相应模板,其中,所述多个模板中的每个模板以符合模式的格式描述虚拟计算环境的拓扑,所述模式能够由所述多个计算基础设施中的相应的一个计算基础设施处理,以在所述多个计算基础设施中的所述相应的一个计算基础设施中实现所述虚拟计算环境;并且

其中,转换所述高级拓扑描述,所述指令使得所述一个或多个处理器确定所述多个对象中的对象是用于所述多个计算基础设施中的计算基础设施的对象,并且响应于所述确定,生成所述多个模板中的用于所述多个计算基础设施中的所述计算基础设施的模板以包括所述对象以用于在第一计算基础设施中供应;并且

使用所述多个模板的相应模板供应所述多个计算基础设施中的每个计算基础设施,以实现所述虚拟计算环境。

## 使用高级拓扑描述的多云虚拟计算环境供应

### 技术领域

[0001] 本公开涉及计算基础设施虚拟化,并且更具体地,涉及在计算基础设施中供应虚拟计算环境。

### 背景技术

[0002] 在典型的云数据中心环境中,大量互连的服务器提供计算和/或存储能力来运行各种应用程序。例如,数据中心可以包括为订户(即,数据中心的客户)托管应用程序和服务的设施。例如,数据中心可以托管所有基础设施设备,例如,网络和存储系统、冗余电源和环境控制。在典型的数据中心中,存储系统和应用服务器集群经由一层或多层物理网络交换机和路由器提供的高速交换结构互连。更复杂的数据中心为遍布全球的基础设施提供位于各种物理托管设施中的用户支持设备。

[0003] 虚拟机是基于机器级虚拟化的虚拟化方案。虚拟机包括在主机计算装置的管理程序上运行的客户操作系统,以模拟计算机的硬件,从而为执行应用程序提供新的计算机环境。

[0004] 集装箱化是一种基于操作系统级虚拟化的虚拟化方案。集装箱是轻型且便携式执行环境,用于相互隔离以及与主机隔离的应用程序。因为集装箱没有与主机硬件计算环境紧密耦接,所以应用程序可以绑定到集装箱图像,并作为单个轻型包在支持底层集装箱架构的任何主机或虚拟主机上执行。因此,集装箱解决了如何使软件在不同的计算环境中工作的问题。集装箱提供了从一个计算环境持续运行到另一虚拟或物理计算环境的承诺。

[0005] 由于集装箱固有的轻型特性,单个主机可以支持比传统虚拟机(VM)更多的集装箱实例。集装箱通常是短暂的,可以比VM更有效地创建和移动,并且也可以作为逻辑相关元件的组来管理(对于某些编排平台,例如,Kubernetes,有时称为“舱”)。这些集装箱特征影响了对集装箱网络解决方案的需求:网络应该是敏捷的和可扩展的。VM、集装箱和裸机服务器可能需要在同一个计算环境中共存,能够在不同部署的应用程序之间通信。集装箱网络还应该不能确知如何使用用于部署集装箱化应用程序的多种编排平台。

[0006] 管理应用程序执行的部署和基础设施的计算基础设施可能涉及两个主要角色:(1)编排——用于跨主机集群自动化应用程序的部署、扩展和操作,并提供计算基础设施,其可以包括以集装箱为中心的计算机基础设施;以及(2)网络管理——用于在网络基础设施中创建虚拟网络,以实现在虚拟环境(例如,集装箱或虚拟机)上运行的应用程序之间以及在传统(例如,物理)环境上运行的应用程序之间的分组通信。软件定义的网络有助于网络管理。

### 发明内容

[0007] 本公开描述了使用分布在多个不同计算基础设施上的多云虚拟计算环境的高级拓扑描述来实现多云虚拟计算环境的供应的技术。例如,拓扑文件使用对由网络实例和计算装置组成的项目进行编码的高级语义和语法来定义所需的多云虚拟计算环境,并定义实

例之间的连通性和关系。多云虚拟计算环境可以跨越多个不同的计算基础设施,这些计算基础设施对应于均托管多云虚拟计算环境的一个或多个项目的不同计算基础设施。该一个或多个项目可以包括应用程序、租户、组织等的任意组合。计算基础设施可以是例如公共云或私有云形式的虚拟化计算基础设施或者裸机服务器系统基础设施。多云虚拟计算环境的每个项目本身是单个计算基础设施内的虚拟计算环境,并且构成要在多个不同计算基础设施中供应的整个多云虚拟计算环境的一部分。

[0008] 转换器可以解析拓扑文件,以从包括网络、一个或多个存储装置和包括实例的计算资源的运营商获得虚拟计算基础设施细节,并且然后应用规则数据库,来为多云拓扑创建一组模板。该组模板中的每个模板可以定义要在一组多个计算基础设施中的不同一个计算基础设施内提供的期望虚拟计算环境。控制器可以将这组模板中的每个模板应用于相应的计算基础设施,以供应符合相应计算基础设施的计算基础设施拓扑模式的模板中定义的一个或多个项目。在控制器实现了期望的虚拟计算环境之后,控制器可以分发虚拟机或其他虚拟执行元件,用于使用多云虚拟计算环境执行应用程序。

[0009] 在一些示例中,除了将期望的计算基础设施应用于数据中心之外,控制器可以被配置为观察数据中心的计算基础设施的当前状态。例如,控制器可以观察示例数据中心中的第一基础设施。此外,控制器可以将第一基础设施与表示示例数据中心的期望计算基础设施的第二基础设施进行比较。转换器可以创建指令(即,至少一个模板),当由控制器导出时,这些指令将把第一基础设施转换为第二基础设施。这样,控制器可以被配置为在多个计算基础设施上指示期望的基础设施。

[0010] 这些技术可以提供一个或多个技术优势。一般来说,计算基础设施可以因平台而异。更具体地,构建和维护计算基础设施的指令可以因公共云和私有云而异。这些技术可以使应用开发者能够使用具有符合高级描述模式的定义的拓扑文件来为一个或多个应用程序定义完整的多云虚拟计算环境。具有如本文所述的转换器的控制器可以将拓扑文件转换为用于供应相应计算基础设施的相应模板,从而使得开发者能够表达预期的多云拓扑,而不必为不同计算基础设施内的每个项目单独创建模板。例如,控制器可以使用第一模板在由第一提供商运营的第一数据中心中构建和维护计算基础设施。此外,控制器可以使用第二模板在由第二提供商运营的第二数据中心中构建和维护计算基础设施。基于使用高级语言(例如,YAML非标记语言(YAML))表达的预期多云拓扑,自动创建每个计算基础设施所需的每个模板,可以减少供应拓扑的时间,并且至少在某些情况下允许零接触供应。

[0011] 在一个示例中,一种方法包括:由计算装置获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述,其中,每个计算基础设施使用不同的计算架构来实现,并且由不同的提供商来部署;由在计算装置上执行的规则引擎,将高级拓扑描述转换为计算基础设施的相应模板,每个模板以符合模式的格式描述虚拟计算环境的拓扑,该模式可以由相应的一个计算基础设施处理,以在相应的一个计算基础设施中实现虚拟计算环境;并且输出用于配置计算基础设施的模板。

[0012] 作为另一示例,一种计算系统包括:一个或多个处理器,其耦接到存储器,其中,该一个或多个处理器被配置为:获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述,其中,每个计算基础设施使用不同的计算架构来实现,并且由不同的提供商来部署;将高级拓扑描述转换为计算基础设施的相应模板,每个模板以符合模式的格式描述虚

拟计算环境的拓扑,该模式可以由相应的一个计算基础设施处理,以在相应的一个计算基础设施中实现虚拟计算环境;并且输出用于配置计算基础设施的模板。

[0013] 作为另一示例,一种非暂时性计算机介质包括指令,用于使一个或多个处理器:获得要在多个计算基础设施中供应的虚拟计算环境的高级拓扑描述,其中,每个计算基础设施使用不同的计算架构来实现,并且由不同的提供商来部署;将高级拓扑描述转换为计算基础设施的相应模板,每个模板以符合模式的格式描述虚拟计算环境的拓扑,该模式可以由相应的一个计算基础设施处理,以在相应的一个计算基础设施中实现虚拟计算环境;并且输出用于配置计算基础设施的模板。

[0014] 本公开的一个或多个示例的细节在附图和以下描述中阐述。从说明书和附图以及权利要求书中,本公开的其他特征、目的和优点将变得显而易见。

### 附图说明

[0015] 图1是示出根据本公开的一个或多个方面的示例网络的概念图,该示例网络包括示例数据中心,在该示例数据中心中,监控基于云的计算环境的基础设施元件的性能和使用度量,并且可选地包括与多个进程共享的资源相关的内部处理器度量。

[0016] 图2是示出根据本公开中描述的技术的示例网络的框图,该示例网络包括用于在网络内引导信息的控制器。

[0017] 图3是示出根据本公开中描述的技术的包括控制器、公共云、私有云和裸机服务器系统的另一示例网络的框图。

[0018] 图4是示出根据本公开中描述的技术的使用控制器管理的另一示例多云计算基础设施的概念图。

[0019] 图5是示出根据本公开中描述的技术的构建和监控多云计算基础设施的示例操作的流程图。

[0020] 图6是示出根据本公开中描述的技术的被配置为将拓扑转换为用于在一个或多个虚拟私有云(VPC)中安装和修改对象的一个或多个模板的示例转换器的框图。

[0021] 图7是示出根据本公开中描述的技术的示例计算装置的框图。

[0022] 图8是示出根据本公开中描述的技术的用于在网络内引导集装箱的另一示例控制器的框图。

[0023] 图9是示出根据本公开中描述的技术的包括至少一个区域和至少一个可用性区域的示例私有云的框图。

[0024] 图10A至图10C是示出根据本公开中描述的技术的包括至少一个网关单元的示例系统的框图。

[0025] 在所有附图和文本中,相同的附图标记表示相同的元件。

### 具体实施方式

[0026] 图1是示出根据本公开的一个或多个方面的示例网络105的概念图,该示例网络105包括示例数据中心110A,在示例数据中心110A中监控基于云的计算环境的基础设施元件的性能和使用度量,并且可选地包括与多个进程共享的资源相关的内部处理器度量。图1示出了网络105和数据中心110A的一个示例实现,其托管一个或多个基于云的计算机网络、计

算域或项目,在本文通常被称为云计算集群。基于云的计算集群可以共同位于共同的整体计算环境中(例如,单个数据中心),或者分布在不同的环境中(例如,不同的数据中心)。基于云的计算集群可以是例如不同的云环境,例如,OpenStack云环境、Kubernetes云环境或其他计算集群、域、网络等的各种组合。网络105和数据中心110A的其他实现在其他情况下可以是合适的。这种实现可以包括图1的示例中包括的组件的子集和/或可以包括图1中未示出的额外组件。数据中心110A可以是数据中心110A-110X(统称为“数据中心110”)的示例数据中心。

[0027] 每个数据中心110可以表示不同的计算基础设施,例如,公共、私有或混合云、或者裸机服务器系统基础设施。不同的计算基础设施可以使用不同的计算平台和技术来实现,使得一个数据中心110A的配置不适用于不同的数据中心110B。示例公共云基础设施包括微软Azure、谷歌计算平台和亚马逊网络服务。任何一个或多个数据中心110也可以表示企业或其他实体的内部计算基础设施。

[0028] 数据中心110可以经由服务提供商网络106彼此互连,并且与和客户104相关联的客户网络互连。通常,每个数据中心110为通过服务提供商网络106耦接到数据中心的客户104的应用程序和服务提供操作环境。数据中心110可以例如是主机基础设施设备,例如,网络和存储系统、冗余电源和环境控制。服务提供商网络106可以耦接到由其他提供商管理的一个或多个网络,并且因此可以形成大规模公共网络基础设施(例如,互联网)的一部分。

[0029] 在一些示例中,每个数据中心110可以表示许多地理上分布的网络数据中心中的一个。如图1的示例所示,每个数据中心110可以表示为客户104提供网络服务的设施。客户104可以是集体类别,例如,企业和政府或个人。例如,网络数据中心可以为几个企业和最终用户提供网络服务。其他示例性服务可以包括数据存储、虚拟专用网络、流量工程、文件服务、数据挖掘、科学或超级计算等。在一些实施例中,每个数据中心110可以是单独的网络服务器、网络对等体等。

[0030] 在这个示例中,每个数据中心110包括通过由一层或多层物理网络交换机和路由器提供的高速交换结构121互连的一组存储系统和应用服务器126A-126N(在本文中称为“服务器126”)。交换结构121由一组互连的架顶(TOR)交换机(未示出)提供,这些交换机耦接到机箱交换机的分布层(未示出)。虽然未示出,但是每个数据中心110还可以包括例如一个或多个非边缘交换机、路由器、集线器、网关、诸如防火墙的安全装置、入侵检测和/或入侵防御装置、服务器、计算机终端、膝上型计算机、打印机、数据库、诸如蜂窝电话或个人数字助理的无线移动装置、无线接入点、网桥、电缆调制解调器、应用加速器或其他网络装置。

[0031] 在图1的示例中,数据中心110A为通过服务提供商网络106耦接到数据中心110A的客户104的应用程序和服务提供操作环境。尽管结合图1的网络105描述的功能和操作可以被示为分布在图1中的多个装置上,但是在其他示例中,归因于图1中的一个或多个装置的特征和技术可以由一个或多个这样的装置的本地组件在内部执行。类似地,一个或多个这样的装置可以包括某些组件并执行各种技术,这些技术可以在本文的描述中归因于一个或多个其他装置。此外,某些操作、技术、特征和/或功能可以结合图1来描述,或者由特定组件、装置和/或模块来执行。在其他示例中,这样的操作、技术、特征和/或功能可以由其他组件、装置或模块来执行。因此,归于一个或多个组件、装置或模块的一些操作、技术、特征和/或功能可以归于其他组件、装置和/或模块,即使本文没有以这种方式具体描述。

[0032] 数据中心110A托管基础设施设备,例如,网络和存储系统、冗余电源和环境控制。服务提供商网络106可以耦接到由一个或多个提供商管理的一个或多个网络,并且因此可以形成大规模公共网络基础设施(例如,互联网)的一部分。

[0033] 在一些示例中,数据中心110A可以表示许多地理上分布的网络数据中心中的一个。如图1的示例所示,数据中心110A是为客户104提供网络服务的设施。客户104可以是集体实体,例如,企业和政府或个人。例如,一个网络数据中心可以为几个企业和最终用户提供网络服务。其他示例性服务可以包括数据存储、虚拟专用网络、流量工程、文件服务、数据挖掘、科学或超级计算等。在一些示例中,数据中心110A是单独的网络服务器、网络对等体等。

[0034] 在图1的示例中,数据中心110A包括一组存储系统和应用服务器,包括通过由一层或多层物理网络交换机和路由器提供的高速交换结构121互连的服务器126。服务器126充当数据中心的物理计算节点。例如,每个服务器126可以为一个或多个特定于客户的虚拟机148(图1中的“VM”)或其他虚拟化实例(例如,集装箱)的执行提供操作环境。每个服务器126可替换地称为主机计算装置,或者更简单地称为主机。服务器126可以执行一个或多个虚拟化实例,例如,虚拟机、集装箱或用于运行一个或多个服务的其他虚拟执行环境/元件,例如,虚拟化网络功能(VNF)。服务器126可以另外或替代地使用集装箱来托管集装箱化应用程序。

[0035] 尽管未示出,交换结构121可以包括耦接到机箱交换机的分布层的架顶(TOR)交换机,并且数据中心110A可以包括一个或多个非边缘交换机、路由器、集线器、网关、诸如防火墙的安全装置、入侵检测和/或入侵防御装置、服务器、计算机终端、膝上型计算机、打印机、数据库、诸如蜂窝电话或个人数字助理的无线移动装置、无线接入点、网桥、电缆调制解调器、应用加速器或其他网络装置。交换结构121可以执行层3路由,以通过服务提供商网络106在数据中心110A和客户104之间路由网络流量。网关108用于在交换结构121和服务提供商网络106之间转发和接收分组。

[0036] 根据本公开的一个或多个示例,软件定义的网络(“SDN”)控制器132提供逻辑上并且在某些情况下物理上集中的控制器,用于促进数据中心110A内的一个或多个虚拟网络的操作。术语SDN控制器和虚拟网络控制器(“VNC”)在整个本公开中可以互换使用。在一些示例中,SDN控制器132响应于经由北行API 131从编排器130接收到的配置输入而操作,而北行API 131又响应于从与用户界面装置129交互和/或操作用户界面装置129的管理员128接收到的配置输入而操作。在2013年6月5日提交的题为“PHYSICAL PATH DETERMINATION FOR VIRTUAL NETWORK PACKET FLOWS”的国际申请号PCT/US 2013/044378中,找到了关于与数据中心110A或其他软件定义的网络的其他装置一起操作的SDN控制器132的额外信息,该申请通过引用结合于此,如同在本文完全阐述的一样。

[0037] 用户界面装置129可以被实现为用于交互呈现输出和/或接受用户输入的任何合适的装置。例如,用户界面装置129可以包括显示器。用户界面装置129可以是计算系统,例如,由用户和/或管理员128操作的移动或非移动计算装置。根据本公开的一个或多个方面,用户界面装置129可以例如表示工作站、膝上型或笔记本计算机、台式计算机、平板计算机或可以由用户操作和/或呈现用户界面的任何其他计算装置。在一些示例中,用户界面装置129可以与策略控制器201物理分离和/或位于不同的位置。在这样的示例中,用户界面装置

129可以通过网络或其他通信手段与策略控制器201通信。在其他示例中,用户界面装置129可以是策略控制器201的本地外围装置,或者可以集成到策略控制器201中。

[0038] 在一些示例中,编排器130管理数据中心110A的功能,例如,计算、存储、联网和应用资源。例如,编排器130可以为数据中心110A内或数据中心上的租户创建虚拟网络。编排器130可以将虚拟机 (VM) 连接到租户的虚拟网络。编排器130可以将租户的虚拟网络连接到外部网络,例如,互联网或VPN。编排器130可以在一组VM上或向租户网络的边界实现安全策略。编排器130可以在租户的虚拟网络中部署网络服务(例如,负载均衡器)。

[0039] 在一些示例中,SDN控制器132管理网络和联网服务,例如,负载均衡、安全性,并且经由南行API 133将资源从服务器126分配给各种应用程序。即,南行API 133表示由SDN控制器132使用的一组通信协议,以使网络的实际状态等于由编排器130指定的期望状态。例如,SDN控制器132通过配置以下内容来实现来自编排器130的高级请求:物理交换机,例如,TOR交换机、机箱交换机和交换结构121;物理路由器;物理服务节点,例如,防火墙和负载均衡器;以及虚拟服务,例如,VM中的虚拟防火墙。SDN控制器132在状态数据库中维护路由、联网和配置信息。

[0040] 通常,任何两个网络装置之间(例如,交换结构121内的网络装置(未示出)之间或服务器126和客户104之间或服务器126之间)的流量可以使用许多不同的路径遍历物理网络。例如,两个网络装置之间可能有几种不同的等价路径。在某些情况下,属于从一个网络装置到另一网络装置的网络流量的分组可以在每个网络交换节点处使用称为多路径路由的路由策略在各种可能的路径中分布。例如,互联网工程任务组(IETF) RFC 2992“等价多路径算法的分析(Analysis of an Equal-Cost Multi-Path Algorithm)”描述了一种沿等价多路径路由分组的组路由技术。RFC 2992的技术分析了一种特定的多路径路由策略,该策略涉及通过散列分组报头字段将流分配到箱,这些分组报头字段通过单个确定性路径发送来自特定网络流的所有分组。

[0041] 例如,“流”可以由分组报头中使用的五个值或“五元组”来定义,即,用于通过物理网络路由分组的协议、源IP地址、目的地IP地址、源端口和目的地端口。例如,协议指定了通信协议,例如,TCP或UDP,并且源端口和目的地端口是指连接的源端口和目的地端口。匹配特定流条目的一组一个或多个分组数据单元(PDU)表示一个流。可以使用PDU的任何参数对流进行广义分类,例如,源和目的地数据链路(例如,MAC)和网络(例如,IP)地址、虚拟局域网(VLAN)标签、传输层信息、多协议标签交换(MPLS)或通用MPLS(GMPLS)标签以及接收流的网络装置的入口端口。例如,流可以是在传输控制协议(TCP)连接中传输的所有PDU、由特定的MAC地址或IP地址提供的所有PDU、具有相同VLAN标签的所有PDU或在相同交换端口接收的所有PDU。

[0042] 虚拟路由器142(虚拟路由器142A到虚拟路由器142N,在图1中统称为“虚拟路由器142”)为数据中心110A内的相应虚拟网络执行多个路由实例,并将分组路由到在服务器126提供的操作环境内执行的适当虚拟机。每个服务器126可以包括虚拟路由器。例如,由服务器126A的虚拟路由器142A从底层物理网络结构接收的分组可以包括外部报头,以允许物理网络结构将有效载荷或“内部分组”隧道传输到服务器126A的网络接口的物理网络地址。外部报头不仅可以包括服务器的网络接口的物理网络地址,还可以包括虚拟网络标识符,例如,识别一个虚拟网络的VxLAN标签或多协议标签交换(MPLS)标签以及由虚拟路由器执行

的相应路由实例。内部分组包括具有目的地网络地址的内部报头,该目的地网络地址符合由虚拟网络标识符识别的虚拟网络的虚拟网络寻址空间。

[0043] 在一些方面,虚拟路由器在将从底层物理网络结构接收的多个隧道分组传送到分组的适当路由实例之前缓冲并聚合这些分组。即,在服务器126中的一个服务器上执行的虚拟路由器可以从交换结构121内的一个或多个TOR交换机接收分组流的进站隧道分组,并且在将隧道分组路由到本地执行的虚拟机之前,处理隧道分组,以构建单个聚合隧道分组,用于转发到虚拟机。即,虚拟路由器可以缓冲多个进站隧道分组,并构建单个隧道分组,其中,多个隧道分组的有效载荷组合成单个有效载荷,并且移除隧道分组上的外部/覆盖报头,并用单个报头虚拟网络标识符替换。以这种方式,虚拟路由器可以将聚合隧道分组转发到虚拟机,就好像从虚拟网络接收到单个进站隧道分组一样。此外,为了执行聚合操作,虚拟路由器可以利用基于内核的卸载引擎,该卸载引擎无缝且自动地指导隧道分组的聚合。在题为“PACKET SEGMENTATION OFFLOAD FOR VIRTUAL NETWORKS”的美国专利申请14/228,844中描述了虚拟路由器将流量转发到在服务器126上执行的客户特定虚拟机的进一步示例技术,该申请通过引用结合于此。

[0044] 在一些示例实现中,在服务器126上执行的虚拟路由器142在多个处理器核心之间操纵接收到的进站隧道分组,以便在处理分组以路由到一个或多个虚拟机和/或物理机时,促进核心之间的分组处理负载均衡。作为一个示例,服务器126A包括多个网络接口卡和多个处理器核心,以执行虚拟路由器142A,并在多个处理器核心之间引导接收的分组,以促进核心之间的分组处理负载均衡。例如,服务器126A的特定网络接口卡可以与指定的处理器核心相关联,网络接口卡将所有接收到的分组引导到该处理器核心。不同的处理器核心不是处理每个接收到的分组,而是根据应用于内部和外部分组报头中的至少一个的散列函数,将流卸载到一个或多个其他处理器核心,以便利用其他处理器核心的可用工作周期进行处理。

[0045] 拓扑152表示用于虚拟计算环境的拓扑(例如,节点、虚拟网络等的设置)的高级基于意图的描述。在一些示例中,用人类可读的数据串行化语言编写拓扑152,例如,YAML非标记语言(YAML)或JavaScript对象符号(JSON)。拓扑152可以包括多个项目,每个项目具有一个或多个装置实例,并且当应用于数据中心110时,可以用该项目配置数据中心110的计算基础设施,以供应可以跨越数据中心110中包括的多个不同计算基础设施的多云虚拟计算环境。如本文所述,计算基础设施包括网络基础设施。

[0046] 转换器150可以将拓扑152转换为一组指令,一旦由控制器102执行,这些指令将在数据中心110中构建和修改多个虚拟化基础设施。在一些示例中,拓扑152可以基于来自GUI(未示出)的输入来创建。在其他示例中,拓扑152可以由在数据中心110A中执行或在任何数据中心110外部执行的控制器102自动生成。拓扑152可以包括基于定义的提供商而不同的列表。根据定义的提供商,可以包括不同的数据结构和参数。拓扑152可以包括识别期望的虚拟计算环境中的节点的IP地址。这样,拓扑152可以通过指定对应于网络内节点的IP地址来确定虚拟计算环境。转换器150可以包括一个或多个应用编程接口(API)。API可以定义一个接口,转换器150通过该接口与拓扑152交互。转换器150可以被配置为使用API从拓扑152“拉取”数据。

[0047] 此外,转换器150可以解析拓扑152的人类可读语言,并确定由拓扑152指示的基础

设施元件的组织层级。在解析拓扑152中,转换器150可以采用语言解析技术。转换器150可以使用多个规则来管理拓扑152到指令的转换,用于指导控制器102构建和监控数据中心110的基础设施。在一些示例中,转换器150可以使用多个规则来确定数据中心110的身份,使得转换器150可以创建包括对应于每个数据中心110的对象的模板。通过识别与每个对象相关联的数据中心110,转换器150可以将拓扑152的每个对象应用于数据中心110的正确数据中心。

[0048] 网络105可以使控制器102能够创建可扩展的多云架构,该架构提供了一个框架,该框架允许在计算资源位于任何地方时消耗计算资源——编排网络和端到端安全。此外,网络105可以在全球范围内实现一致的策略实施。例如,对于物理、虚拟、集装箱和云基础设施,策略实施可以是一致的,并且是集中管理的。网络105执行的过程可以是可用的和自动化的。在某些情况下,可用性和冗余性可以经由自动化来保持或增强,以减少创建和维护计算基础设施时的人为错误。此外,使用网络105的转换器150构建和维护计算基础设施可以允许创建具有宏和微段的多租户环境。例如,网络105可以创建或摄取区域/标签/名称空间来限制环境之间的移动。这些技术可以提高粒度和可见性。例如,网络105可能提供粒度和完全可见性以及物理和虚拟(底层和上层)之间的交互。

[0049] 多云联网和结构技术(例如,在本文描述的技术)可以跨混合云环境提供一组联网和安全特征。例如,网络105的拓扑152和转换器150可以使用自动供应、管理、监控和分析来实现计算、联网和策略服务在私有、公共和裸机系统上的无缝扩展。可以使用多云网关来提供和编排公共云的安全网络扩展。

[0050] 在图1的示例中,数据中心110A还包括为数据中心110A提供监控、调度和性能管理的策略控制器201。策略控制器201与部署在至少一些相应物理服务器216内的监控代理205交互,用于监控物理计算节点以及在物理主机上执行的任何虚拟化主机(例如,VM 148)的资源使用。以这种方式,监控代理205提供分布式机制,用于收集各种各样的使用度量以及用于策略控制器201安装的策略的本地实施。在示例实现中,监控代理205运行在数据中心110A的基础设施的最低级别“计算节点”上,这些计算节点提供计算资源来执行应用工作负载。计算节点例如可以是服务器126、虚拟机148、集装箱等的裸机主机。

[0051] 在一些示例中,策略控制器201可以被配置为确定和/或识别在每个服务器126上执行的虚拟机、集装箱、服务和/或应用程序的形式的元件。如本文所使用的,资源通常指虚拟化基础设施的可消耗组件,即,基础设施所使用的组件,例如,CPU、存储器、磁盘、磁盘I/O、网络I/O、虚拟CPU和轨迹虚拟路由器。资源可以具有一个或多个特征,每个特征与由策略代理205(和/或策略控制器201)分析并可选地报告的度量相关联。下面参考图2描述资源的示例原始度量的列表。

[0052] 通常,基础设施元件(在本文也称为元件)是基础设施的组件,其包括或消耗消耗性资源,以便操作。示例元件包括主机、物理或虚拟网络装置、实例(例如,虚拟机、集装箱或其他虚拟操作环境实例)、聚合、项目和服务。在某些情况下,一个元件可以是另一元件的资源。虚拟网络装置可以包括例如虚拟路由器和交换机、vRouter、vSwitch、开放式虚拟交换机和虚拟隧道转发器(VTF)。度量是一个值,其衡量一个元件消耗的资源量,作为资源的特征。

[0053] 策略控制器201可以被实现为任何合适的计算装置或在任何合适的计算装置内或者在多个计算装置上实现。策略控制器201或策略控制器201的组件可以实现为计算装置的

一个或多个模块。在一些示例中，策略控制器201可以包括在数据中心110A内包括的一类计算节点(例如，“基础设施节点”)上执行的多个模块。这样的节点可以是OpenStack基础设施服务节点或Kubernetes主节点，和/或可以实现为虚拟机。在一些示例中，策略控制器201可以与数据中心110A内的一些或所有其他计算节点具有网络连接，并且还可以与管理数据中心110A的其他基础设施服务具有网络连接。

[0054] 一个或多个策略202可以包括使一个或多个策略代理205监控与服务器126相关联的一个或多个度量的指令。一个或多个策略202可以包括使一个或多个策略代理205分析与服务器126相关联的一个或多个度量以确定是否满足规则的条件指令。一个或多个策略202可以替代地或另外包括使策略代理205向策略控制器201报告一个或多个度量的指令，包括这些度量是否满足与一个或多个策略202相关联的规则的条件。所报告的信息可以包括一个或多个策略202指定或要求的原始数据、汇总数据和采样数据。

[0055] 图1中示出的和/或本公开其他地方示出或描述的各种组件、功能单元和/或模块(例如，用户界面装置129、编排器130、SDN控制器132和策略控制器201、策略代理205)可以使用驻留在一个或多个计算装置中和/或在一个或多个计算装置上执行的软件、硬件、固件或硬件、软件和固件的混合来执行所描述的操作。例如，计算装置可以用多个处理器或多个装置来执行一个或多个这样的模块。计算装置可以作为在底层硬件上执行的虚拟机执行一个或多个这样的模块。一个或多个这样的模块可以作为操作系统或计算平台的一个或多个服务来执行。一个或多个这样的模块可以作为一个或多个可执行程序在计算平台的应用层执行。在其他示例中，模块提供的功能可以由专用硬件装置实现。尽管一个或多个存储装置中包括的某些模块、数据存储、组件、程序、可执行文件、数据项、功能单元和/或其他项可以单独示出，但是一个或多个这样的项可以组合并作为单个模块、组件、程序、可执行文件、数据项或功能单元来操作。例如，一个或多个模块或数据存储可以组合或部分组合，使得作为单个模块操作或提供功能。此外，一个或多个模块可以彼此结合操作，使得例如一个模块充当另一模块的服务或扩展。此外，存储装置内示出的每个模块、数据存储、组件、程序、可执行文件、数据项、功能单元或其他项可以包括多个组件、子组件、模块、子模块、数据存储和/或未示出的其他组件或模块或数据存储。此外，存储装置中示出的每个模块、数据存储、组件、程序、可执行文件、数据项、功能单元或其他项可以以各种方式实现。例如，存储装置内示出的每个模块、数据存储、组件、程序、可执行文件、数据项、功能单元或其他项可以被实现为在计算装置上执行的操作系统的一部分。

[0056] 图2是示出根据本公开中描述的技术的示例网络200的框图，该示例网络200包括用于在网络200内引导信息的控制器214。服务提供商网络206可以是图1的服务提供商网络106的示例。云210可以是图1的数据中心110A的示例。编排器212可以是图1的编排器130的示例。控制器214可以是图1的控制器132的示例。控制器132和编排器212可以实现整体控制器，例如，图1的控制器102。云220可以是图1的数据中心110B-110X中任何一个的示例。

[0057] 根据本公开的一个或多个实施例，控制器212提供逻辑上并且在一些情况下物理上集中的控制器，用于促进云210和云220中的每一个内的一个或多个虚拟网络的操作，例如，云220的VPC 1。在一些示例中，控制器212可以响应于从转换器(例如，图1的转换器150)接收的配置输入而操作。

[0058] 在一些示例中，编排器212管理云210的功能，例如，计算、存储、联网和应用资源。

例如,编排器212可以为云210内或跨数据中心的租户创建虚拟网络。编排器212可以将虚拟机 (VM) 连接到租户的虚拟网络。编排器212可以将租户的虚拟网络连接到外部网络,例如,服务提供商网络206或云220。编排器212可以在一组VM上或向租户网络的边界实现安全策略。编排器212可以在租户的虚拟网络中部署网络服务(例如,负载均衡器)。在一些示例中,控制器214在状态数据库中维护路由、联网和配置信息。在一些示例中,编排器212使用Kubernetes来自动化集装箱化应用程序的部署、扩展和管理。例如,编排器212可以使用Kubernetes来经由控制器214将集装箱部署到服务器226A-226E(统称为“服务器226”)中的任何一个。在一些示例中,集装箱可以包括Docker集装箱。编排器212可以向控制器214输出指令,以经由网关230将集装箱部署到服务器226。

[0059] 服务器组226(例如,服务器226B和226C)可以通过由一层或多层物理网络交换机和路由器提供的高速交换结构(未示出)互连。交换机结构由一组互连的架顶(TOR)交换机(未示出)提供,这些交换机耦接到机箱交换机的分布层(未示出)。尽管未示出,云210和云220中的每一个还可以包括例如一个或多个非边缘交换机、路由器、集线器、网关、诸如防火墙的安全装置、入侵检测和/或入侵防御装置、服务器、计算机终端、膝上型计算机、打印机、数据库、诸如蜂窝电话或个人数字助理的无线移动装置、无线接入点、网桥、电缆调制解调器、应用加速器或其他网络装置。服务器226的每个服务器可以包括至少一个虚拟路由器和至少一个集装箱或虚拟机。

[0060] 网关230A-230C(统称为“网关230”)可以提供虚拟专用网络(VPN)服务,用于通过广域网(WAN)提供连接。可以使用基于标准的VPN对租户应用程序工作量执行租户隔离。网关230可以使用安全策略框架为每个数据中心110A提供相同的安全姿态。此外,网关230可以在公共云和私有云环境中跨可用性区域提供弹性。网关230可以被配置用于基于角色的访问控制(RBAC)和与活动目录/轻量级目录访问协议(AD/LDAP)的集成。在一些示例中,网关230可以使控制器202能够在一个或多个数据中心之间传输分组,包括集装箱。网关230可以使用加密连接(例如,具有Nat-t或SSL的IPSec)来在网关门户230A、230B和230C之间交换信息。

[0061] 图3是示出根据本公开中描述的技术的示例性多云计算基础设施300的框图,包括控制器302、公共云304、私有云306和裸机服务器系统308。在一些示例中,控制器302可以通过将软件映射到相应节点来提供公共云304、私有云306和裸机服务器系统308。供应包括准备和装备网络的过程,从而允许网络提供新的服务。例如,供应可以包括使用控制器302将集装箱部署到公共云304、私有云306和裸机服务器系统308中的任一个的节点。此外,供应可以包括使用控制器302来启用公共云304、私有云306和裸机服务器系统308中的任一个上的安全性(例如,激活或编程防火墙)。另外,控制器302可以监控和管理公共云304、私有云306和裸机服务器系统308中的每一个。例如,如果网络300接收到执行新任务的指令,则控制器302可以通过在公共云304、私有云306和裸机服务器系统308中的至少一个中部署新软件和创建新的基础设施配置来供应网络300,以执行新任务。控制器302可以表示图1的控制器102的示例实例。

[0062] 图4是示出根据本公开中描述的技术的使用控制器管理的另一示例多云计算基础设施400的概念图。网络400的控制器402可以将软件部署到数据中心,包括服务器410、VPC 420、VPC 430和裸机服务器系统440。服务器410可以包括一个或多个虚拟机和一个或多个集装箱。此外,VPC 420、VPC 430和裸机服务器系统440可以包括一个或多个虚拟机和一个

或多个集装箱。在一些示例中,控制器402可以部署集装箱来构建数据中心中的计算基础设施。控制器402可以从转换器(未示出)接收指令。指令可以指示要部署到每个相应数据中心以实现期望的虚拟计算环境的数据(例如,集装箱、对象、应用程序等)。另外,数据中心可以向控制器402输出指示网络结构的当前状态的信息。转换器可以被配置为使用由数据中心输出的虚拟计算环境的当前状态和虚拟计算环境的期望状态来产生模板。控制器400可以应用模板来构建数据中心的多个计算基础设施。控制器402可以表示图1的控制器102的示例实例。

[0063] 图5是示出根据本公开中描述的技术的构建和监控多云计算基础设施的示例操作500的流程图。参考图1的网络105描述示例操作500。

[0064] 根据示例操作500,拓扑文件包括用于定义一个或多个服务器的基础设施的意图的声明性模型(510)。声明性模型可以是多云对象的通用YAML模式,其允许支持多个提供商(例如,公共云、私有云、裸机服务器系统等)。在一些示例中,拓扑152可以包括声明性模型。声明性模型可以是一个或多个服务器的期望拓扑(例如,一个或多个服务器的元件之间的期望交互,例如,节点、链接等)。YAML或其他人类可读语言对于编码声明性模型可能是有益的,使得声明性模型可以有效地解析并应用于具有许多不同提供商(例如,云服务提供商)的许多数据中心。在一些示例中,图形用户界面(GUI)可以显示声明性模型,使得用户可以用YAML语言编写和编辑声明性模型。在其他示例中,GUI可以显示声明性模型的视觉表示,使得用户能够向GUI提供指示节点、链接等的输入。

[0065] 控制器102可以映射由声明性模型指示的网络拓扑,并提供网络拓扑的图形(例如,视觉表示)(520)。例如,转换器150的解析器可以解析声明性模型的人类可读语言,并确定声明性模型所指示的网络元件的组织层级。解析器可以使用语言解析技术。换言之,解析器可以获取输入数据(例如,声明性模型的文本),并构建给出网络拓扑图的数据结构。在一些示例中,解析器可以由用户编程。在其他示例中,可以使用编译器生成器来创建解析器。该图可以包括解析树、抽象语法树、流程图、示出网络连接的图或另一视觉表示中的至少一个。

[0066] 此外,根据示例操作500,控制器102被配置为给不同提供商构建基础设施并配置所需对象(530)。示例对象可以包括变量、数据结构、功能、方法和被配置为管理计算机程序的其他值。例如,在计算机网络中,对象可以定义一个或多个转发路径元件之间的连接,确定如何通过转发路径路由分组。转发路径元件可以是执行简单活动(例如,计数器或丢弃)、条件或复杂构造(例如,表、树或查找)的类型。例如,路由器的分组处理器可以将转发路径元件设置为下一跳数据,该下一跳数据可以作为沿着分组处理器的内部分组转发路径的一系列“下一跳”链接在一起。分组处理的结果决定了分组处理器将分组从入口转发单元上的分组输入接口转发或处理到出口转发单元上的输出接口的方式。因此,对象可以定义如何通过转发路径路由分组。

[0067] 对象可以很像转发路径之间的连接,继续网络的一个或多个元件之间的连接,以创建由高级拓扑描述(例如,拓扑152)定义的虚拟计算环境。在一些示例中,高级拓扑描述包括指示虚拟计算环境提供的虚拟网络、存储和服务中的至少一个的数据。例如,控制器102可以使用对象来连接云、一组安全组规则、虚拟机(VM)、负载均衡器、域名系统(DNS)、内容传送网络(CDN)等中的至少一个。在控制器102使用对象来确定计算基础设施内的一组安全组规则的示例中,控制器102可以有效地定制计算基础设施内的防火墙。换言之,数据中

心110A可以使用对象来监控输入和输出的网络流量。控制器102可以使用声明性模型指定对应于网络中多个服务器中的每个服务器的不同组的安全组规则。例如,声明性模型可以包括服务器和相应的一组安全组规则之间的连接。因此,配置对象可以是构建和维护计算基础设施的一个组成部分。

[0068] 控制器102可以将构建的基础设施映射到控制器的角色,以将控制器软件供应到网络内的节点上(540)。例如,OpenShift和K8s处理器可以部署在网络节点上,并且可以启用网络安全。控制器软件的供应可以在GUI上可视化。此外,数据中心110A可以根据声明性模型来管理和监控计算基础设施(550)。例如,如果更新声明性模型,则控制器102进而可以根据声明性模型中反映的变化来更新计算基础设施。控制器102可以被配置为确定计算基础设施的当前状态,并在GUI上显示当前状态的视觉表示。GUI可以接受指示对计算基础设施的期望改变的输入,并且声明性模型可以相应地更新。

[0069] 图6是示出被配置为将拓扑602转换为用于在一个或多个公共云606A-606C(统称为(云606))中安装和修改对象的一个或多个模板618的示例转换器604的框图。转换器604可以包括API 610、解析器612、规则数据库614、模板生成器616、模板618和模板应用单元619。转换器604可以是图1的转换器150的示例。另外,拓扑602可以是图1的拓扑152的示例。

[0070] 通常,转换器604可以将拓扑602转换为多个模板,一旦由控制器132执行,这些模板将在一个或多个数据中心上构建和修改虚拟计算环境。拓扑602可以表示要在多个计算基础设施中的一个中供应的虚拟计算环境的高级拓扑描述。在一些示例中,拓扑602可以基于来自GUI(未示出)的输入来创建。在其他示例中,拓扑602可以由数据中心110A的控制器102自动生成。拓扑602可以包括基于定义的提供商而不同的列表。拓扑602可以包括将被实例化为相应云606内的虚拟计算环境的一个或多个项目,以供应整体多云虚拟计算环境。根据项目的指定提供商,可以包括不同的数据结构和参数。拓扑602可以包括识别期望的虚拟计算环境中的节点的IP地址。这样,拓扑602可以通过指定对应于网络内节点的IP地址来确定虚拟计算环境。拓扑602可以如下创建:

[0071] 创建拓扑

[0072] 本节提供创建拓扑所需的所有信息。拓扑是包含已定义的提供商的列表。根据提供商,需要不同的数据结构和参数。

[0073] 1.0nPrem

[0074] OnPrem是提供商。可能有已经在运行的实例或需要创建的新实例。需要设置经由ssh到主机的连接,并且这是先决条件。

[0075] 注意:轨迹多云部署的所有实例都假设操作系统为centos7.4

[0076] 1.1字段规范OnPrem提供商:

[0077] 提供商(provider):[字符串](必需)

[0078] 组织(organization):[字符串](可选)

[0079] 项目(project):[字符串](可选)

[0080] 实例(instances):[列表][实例](必需)

[0081] OnPrem实例:

[0082] 名称(name):[字符串][唯一](必需)

[0083] public\_IP:[字符串][ip](必需)

- [0084] private\_IP:[字符串][ip] (必需)
- [0085] private\_subnet:[字符串][cidr] (必需)
- [0086] vip:[字符串][ip] (必需)
- [0087] 角色(roles):[列表][角色] (必需)
- [0088] 供应(provision):[bool] (必需)
- [0089] 用户名(username):[字符串] (必需)
- [0090] 接口(interface):[字符串][接口]
- [0091] 协议(protocols):[列表][协议] (可选)
- [0092] 角色:
- [0093] • 网关(gateway):多云网关
- [0094] • compute\_node:轨迹计算节点和k8s节点
- [0095] • 控制器(controller):轨迹控制器和k8s-主
- [0096] 协议:
- [0097] • ipsec\_client:允许实例充当ipsec客户端
- [0098] • ipsec\_server:允许实例充当ipsec服务器
- [0099] • ssl\_client:允许实例充当ssl客户端
- [0100] • ssl\_server:允许实例充当ssl服务器
- [0101] 1.2定义OnPrem提供商字段provider应该具有值OnPrem。
- [0102] 提供商:OnPrem
- [0103] 字段organization和project是可选的,该字段可以指定项目和组织。
- [0104] 组织:Juniper
- [0105] 项目:多云
- [0106] 1.3定义OnPrem实例字段instances应该具有带有实例对象的列表。
- [0107] 实例:
- [0108] • 名称:实例名称
- [0109] • public\_ip:外部ip,将由ansible使用
- [0110] • private\_ip:内部ip
- [0111] • private\_subnet:Bird将通告的子网
- [0112] • vip:虚拟ip,将由vrrp使用
- [0113] • 角色:该主机的列表角色
- [0114] • 供应:轨迹供应
- [0115] • 用户名:ansible将使用的主机用户名
- [0116] • 接口:vrouter将使用的接口
- [0117] • 协议:允许该主机使用的列表协议,如果该主机是网关o
- [0118] o默认为OnPrem[ssl\_clinet],该设置不要求可通过互联网访问的public\_ip
- [0119] 示例:
- [0120] 名称:OnPrem1
- [0121] 角色:
- [0122] -网关

[0123] 供应:真  
[0124] 用户名:root  
[0125] public\_ip:10.10.10.10  
[0126] private\_ip:192.168.100.17  
[0127] private\_subnet:192.168.100.0/24  
[0128] 接口:eth1  
[0129] vip:192.168.100.254  
[0130] 协议:  
[0131] -ipsec\_client  
[0132] 1.4示例  
[0133] 具有两个主机、一个网关和混合(控制器和计算机主机)的OnPrem  
[0134] -提供商:onprem  
[0135] 组织:juniper  
[0136] 项目:多云  
[0137] 实例:  
[0138] -名称:GW\_1\_OnPrem  
[0139] 角色:  
[0140] -网关  
[0141] 供应:真用户名:root  
[0142] public\_ip:10.10.10.10  
[0143] private\_ip:192.168.100.17  
[0144] private\_subnet:192.168.100.0/24  
[0145] 接口:eth1  
[0146] vip:192.168.100.254  
[0147] 协议:  
[0148] -ssl\_client  
[0149] -ssl\_server  
[0150] -名称:控制器  
[0151] 角色:  
[0152] -控制器  
[0153] -compute\_node  
[0154] 供应:真  
[0155] 用户名:root  
[0156] public\_ip:11.11.11.11  
[0157] private\_ip:192.168.100.77  
[0158] private\_subnet:192.168.100.0/24  
[0159] 接口:eth1  
[0160] vip:192.168.100.254  
[0161] 具有四个主机、两个网关、控制器和计算主机的OnPrem

[0162] -提供商:onprem  
[0163] 组织:juniper  
[0164] 项目:多云  
[0165] 实例:  
[0166] -名称:GW\_1\_OnPrem  
[0167] 角色:  
[0168] -网关  
[0169] 供应:真  
[0170] 用户名:root  
[0171] public\_ip:10.10.10.10  
[0172] private\_ip:192.168.100.17  
[0173] private\_subnet:192.168.100.0/24  
[0174] 接口:eth1  
[0175] vip:192.168.100.254  
[0176] 协议:  
[0177] -ssl\_client  
[0178] -ssl\_server  
[0179] -名称:GW\_2\_OnPrem  
[0180] 角色:  
[0181] -网关  
[0182] 供应:真  
[0183] 用户名:root  
[0184] public\_ip:77.77.77.77  
[0185] private\_ip:192.168.100.57  
[0186] private\_subnet:192.168.100.0/24  
[0187] 接口:eth1  
[0188] vip:192.168.100.254  
[0189] 协议:  
[0190] -ssl\_client  
[0191] -ssl\_server  
[0192] -名称:控制器  
[0193] 角色:  
[0194] -控制器  
[0195] 供应:真  
[0196] 用户名:root  
[0197] public\_ip:11.11.11.11  
[0198] private\_ip:192.168.100.187  
[0199] private\_subnet:192.168.100.0/24  
[0200] 接口:eth1

- [0201] - 名称:计算节点 (Compute\_node)
- [0202] 角色:
- [0203] -计算节点 (compute\_node)
- [0204] 供应:真
- [0205] 用户名:root
- [0206] public\_ip:13.13.13.13
- [0207] private\_ip:192.168.100.67
- [0208] private\_subnet:192.168.100.0/24
- [0209] 接口:eth1
- [0210] 2AWS
- [0211] AWS是亚马逊网络服务的提供商。这意味着任何定义的实例和资源都将由 terraform创建。
- [0212] 1.1字段规范AWS提供商:
- [0213] 提供商:[字符串] (必需)
- [0214] 组织:[字符串] (可选)
- [0215] 项目:[字符串] (可选)
- [0216] 地区:[列表][地区] (必需)
- [0217] AWS地区:
- [0218] 名称:[字符串][唯一] (必需)
- [0219] 云:[列表][云] (必需)
- [0220] AWS云:
- [0221] 名称:[字符串][唯一] (必需)
- [0222] cidr\_block:[字符串][cidr] (必需)
- [0223] 子网:[列表][子网] (必需)
- [0224] 安全组 (security\_groups) : [列表][security\_group] (必需)
- [0225] 实例:[列表][实例] (必需)
- [0226] AWS子网:
- [0227] 名称:[字符串][唯一] (必需)
- [0228] cidr\_block:[字符串][cidr] (必需)
- [0229] availability\_zone:[字符串][availability\_zone] (必需)
- [0230] AWS security\_group:
- [0231] 名称:[字符串][唯一] (必需)
- [0232] 入口:[字符串][规则] (可选)
- [0233] 出口:[字符串][规则] (可选)
- [0234] AWS实例:
- [0235] 名称:[字符串][唯一] (必需)
- [0236] 角色:[列表][角色] (必需)
- [0237] 供应:[bool] (必需)
- [0238] 用户名:[字符串] (必需)

- [0239] 接口:[字符串][接口] (必需)
- [0240] 协议:[列表][协议] (可选)
- [0241] availability\_zone:[字符串][availability\_zone] (必需)
- [0242] machine\_id:[字符串][ami] (必需)
- [0243] instance\_type:[字符串][instance\_type] (必需)
- [0244] security\_groups:[列表][security\_group.name] (必需)
- [0245] 子网:[子网.名称] (必需)
- [0246] volume\_size:[字符串] (可选)
- [0247] 接口:
- [0248]
  - vrouter (用于aws)
- [0249] \*或物理接口
- [0250] machine\_id:\*instance\_type取决于区域
- [0251] 注:如需了解每个地区的centos AWS AMI的列表,请点击此处-[centos-ami](#)
- [0252] 实例类型:\*ami取决于推荐的ami:优化计算
- [0253] 体积大小:最小值:-网关:#TODO填充-控制器:#TODO填充-compute\_node:#TODO填充
- [0254] 推荐:-网关:#TODO填充-控制器:#TODO填充-compute\_node:#TODO填充
- [0255] 可用性区域:
- [0256]
  - a
- [0257]
  - b
- [0258]
  - c\*取决于地区是否支持
- [0259] 1.3定义区域中的AWS区域是对象区域列表。
- [0260] 区域:
- [0261]
  - 名称:aws区域的名称
- [0262]
  - 云:列出将在此区域通过terraform创建的云对象
- [0263] 示例:
- [0264] 名称:eu-west-1
- [0265] 云:
- [0266] -名称:vpc\_1
- [0267] ...
- [0268] 云 (vpc) :
- [0269]
  - 名称:虚拟私有云的名称
- [0270]
  - cidr\_block:虚拟私有云的cidr\_block
- [0271]
  - 子网:将在此vpc中由terraform创建的子网对象列表
- [0272]
  - security\_group:将在此vpc中由terraform创建的security\_group
- [0273] 对象列表
- [0274]
  - 实例:将在此vpc中由terraform创建的实例对象列表
- [0275] 示例:
- [0276] 名称:vpc\_1
- [0277] cidr\_block:172.16.0.0/23

- [0278] 子网:
- [0279] -名称:subnet\_1
- [0280] ...
- [0281] security\_groups:
- [0282] -名称:all\_in
- [0283] ...
- [0284] 实例:
- [0285] -名称:GW\_1
- [0286] ...
- [0287] 子网:
- [0288] • 名称:子网名称
- [0289] • cidr\_block:此子网的cidr必须是唯一的,并且属于vpc cidr\_block
- [0290] • availability\_zone:该子网的availability\_zone
- [0291] 示例:
- [0292] 名称:subnet\_1
- [0293] cidr\_block:172.16.0.0/24
- [0294] availability\_zone:a
- [0295] 安全组:
- [0296] • 名称:安全组的名称
- [0297] • 入口:入口规则(terraform from)
- [0298] • 出口:出口规则(Terraform from)
- [0299] 示例:
- [0300] 名称:名称:all\_in\_all\_out
- [0301] 入口:
- [0302] from\_port:0
- [0303] to\_port:0
- [0304] 协议:"-1"
- [0305] cidr\_blocks:
- [0306] -"0.0.0.0/0"
- [0307] 出口:
- [0308] from\_port:0
- [0309] to\_port:0
- [0310] 协议:"-1"
- [0311] cidr\_blocks:
- [0312] -"0.0.0.0/0"
- [0313] 实例:
- [0314] • 名称:实例的名称
- [0315] • 角色:此主机的列表角色
- [0316] • 供应:轨迹供应

- [0317] • 用户名:ansible将使用的主机用户名取决于ami
- [0318] • 接口:vrouter将使用的接口必须是vrouter
- [0319] • 协议:允许该主机使用的列表协议,如果该主机是网关
- [0320] o默认aws[ssl\_clinet、ssl\_server、ipsec\_client、ipsec\_server]
- [0321] • availability\_zone:该子网的availability\_zone
- [0322] • machine\_id:ami id
- [0323] • instance\_type:实例类型取决于ami
- [0324] • security\_groups:将连接到此实例的安全组名称的列表
- [0325] • 子网:将作为专用子网连接到此实例的子网名称
- [0326] • volume\_size:此实例的可选额外存储
- [0327] 示例:
- [0328] 名称:GW\_1\_grazyna
- [0329] availability\_zone:a
- [0330] 角色:
- [0331] -网关
- [0332] 供应:真
- [0333] 用户名:centos
- [0334] machine\_id:ami-ee6a718a
- [0335] instance\_type:c4.大
- [0336] volume\_size:10
- [0337] security\_groups:
- [0338] -all\_in\_all\_out
- [0339] 子网:subnet\_1
- [0340] 接口:eth1
- [0341] 3GCP
- [0342] 谷歌是谷歌云平台的提供商。这意味着定义的任何实例和资源都将由terraform创建。
- [0343] 1.1字段规范谷歌提供商:
- [0344] 提供商:[字符串](必需)
- [0345] 组织:[字符串](可选)
- [0346] 项目:[字符串](必需)
- [0347] 地区:[列表][地区](必需)
- [0348] 谷歌区域:
- [0349] 名称:[字符串][唯一](必需)
- [0350] 云:[列表][云](必需)
- [0351] 谷歌云:
- [0352] 名称:[字符串][唯一](必需)
- [0353] 子网:[列表][子网](必需)
- [0354] firewalls\_external:[列表][firewall\_rule](必需)

- [0355] firewalls\_internal:[列表][firewall\_rule] (必需)
- [0356] 实例:[列表][实例] (必需)
- [0357] 谷歌子网:
- [0358] 名称:[字符串][唯一] (必需)
- [0359] cidr\_block:[字符串][cidr] (必需)
- [0360] 谷歌firewalls\_external:
- [0361] 名称:[字符串][唯一] (必需)
- [0362] 允许:[字符串][规则] (可选)
- [0363] 拒绝:[字符串][规则] (可选)
- [0364] 谷歌firewalls\_internal:
- [0365] [列表][规则]
- [0366] 谷歌规则:
- [0367] 名称:[字符串][唯一] (必需)
- [0368] 允许:[字符串][规则] (可选)
- [0369] 拒绝:[字符串][规则] (可选)
- [0370] 谷歌允许/拒绝:
- [0371] 协议:tcp、udp、icmp、esp、ah、sctp
- [0372] 端口:端口和/或端口范围列表
- [0373] 谷歌实例:
- [0374] 名称:[字符串][唯一] (必需)
- [0375] 角色:[列表][角色] (必需)
- [0376] 供应:[bool] (必需)
- [0377] 用户名:[字符串] (必需)
- [0378] 接口:[字符串][接口] (必需)
- [0379] 协议:[列表][协议] (可选)
- [0380] availability\_zone:[字符串][availability\_zone] (必需)
- [0381] machine\_id:[字符串][ami] (必需)
- [0382] instance\_type:[字符串][instance\_type] (必需)
- [0383] 子网:[子网名称] (必需)
- [0384] volume\_size:[字符串] (可选)
- [0385] Machine Id:\*instance\_type取决于区域
- [0386] 体积大小:最小值:-网关:#TODO填充-控制器:#TODO填充-compute\_node:#TODO填充
- [0387] 推荐:-网关:#TODO填充-控制器:#TODO填充-compute\_node:#TODO填充
- [0388] 可用性区域:
- [0389] • a
- [0390] • b
- [0391] • c\*取决于地区是否支持
- [0392] 示例:

- [0393] 名称:europa-west3
- [0394] 云:
- [0395] -名称:vpc\_1
- [0396] ...
- [0397] 云(vpc):
- [0398] • 名称:虚拟私有云的名称
- [0399] • cidr\_block:虚拟私有云的cidr\_block
- [0400] • 子网:将在此vpc中由terraform创建的子网对象列表
- [0401] • firewalls\_external:将在此vpc中由terraform创建的防火墙对象列表
- [0402] • firewalls\_internal:将在此vpc中由terraform创建的防火墙对象列表
- [0403] • 实例:将在此vpc中由terraform创建的实例对象列表
- [0404] 示例:
- [0405] 名称:vpc\_1
- [0406] cidr\_block:172.16.0.0/23
- [0407] 子网:
- [0408] -名称:subnet\_1
- [0409] ...
- [0410] firewalls\_internal:
- [0411] -名称:全部
- [0412] ...
- [0413] firewalls\_external:
- [0414] -名称:全部
- [0415] ...
- [0416] 实例:
- [0417] -名称:GW\_1
- [0418] ...
- [0419] 子网:
- [0420] • 名称:子网名称
- [0421] • cidr\_block:此子网的cidr必须是唯一的,并且属于vpc cidr\_block
- [0422] 示例:
- [0423] 名称:subnet\_1
- [0424] cidr\_block:172.16.0.0/24
- [0425] firewalls external:[列表规则]
- [0426] firewalls internal:[列表规则]
- [0427] 示例:
- [0428] firewalls\_external:
- [0429] -名称:all-icmp
- [0430] 允许:
- [0431] 协议:icmp

[0432] firewalls\_internal:

[0433] -名称:all-tcp

[0434] 允许:

[0435] 协议:tcp

[0436] 实例:

[0437] • 名称:实例的名称

[0438] • 角色:此主机的列表角色

[0439] • 供应:轨迹供应

[0440] • 用户名:ansible将使用的主机用户名取决于ami

[0441] • 接口:vrouter将使用的接口

[0442] • 协议:允许该主机使用的列表协议,如果该主机是网关o

[0443] o默认aws[ssl\_clinet,ssl\_server,ipsec\_client,ipsec\_server]

[0444] • availability\_zone:该子网的availability\_zone

[0445] • machine\_id:图像id

[0446] • instance\_type:machine\_type

[0447] • firewalls\_external:防火墙规则列表

[0448] • firewalls\_internal:防火墙规则列表

[0449] • 子网:将作为专用子网连接到此实例的子网名称

[0450] • volume\_size:此实例的可选额外存储

[0451] 示例:

[0452] 名称:GW\_1\_grazyna

[0453] availability\_zone:a

[0454] 角色:

[0455] -网关

[0456] 供应:真

[0457] 用户名:ubuntu

[0458] machine\_id:ubuntu-1604-xenial-v20170307

[0459] instance\_type:n1-standard-1

[0460] volume\_size:10

[0461] 子网:subnet\_1

[0462] 接口:eth1

[0463] 修改

[0464] 本章将为VPC添加新的计算机主机,同时也将添加新的VPC。当前部署能力太低时,这很有用。

[0465] 修改拓扑

[0466] 改变topology.yml,这样会显示以下内容。注意,文件的标题没有改变,只是附加了一些数据。

[0467] -提供商:aws

[0468] 组织:juniper

[0469] 项目:轨迹-多云  
[0470] 地区:  
[0471] -名称:eu-central-1  
[0472] 云:  
[0473] -名称:scaling-vpc-1  
[0474] cidr\_block:172.16.0.0/23  
[0475] 子网:  
[0476] -名称:subnet\_1\_scaling-vpc-1  
[0477] cidr\_block:172.16.0.0/24  
[0478] availability\_zone:a  
[0479] 安全组:  
[0480] -名称:all\_in\_scaling-vpc-1  
[0481] 入口:  
[0482] from\_port:0  
[0483] to\_port:0  
[0484] 协议:"-1"  
[0485] cidr\_blocks:  
[0486] -"0.0.0.0/0"  
[0487] -名称:all\_out\_scaling-vpc-1  
[0488] 出口:  
[0489] from\_port:0  
[0490] to\_port:0  
[0491] 协议:"-1"  
[0492] cidr\_blocks:  
[0493] -"0.0.0.0/0"  
[0494] 实例:  
[0495] -名称:Contril\_GW\_scaling-VPC-1  
[0496] availability\_zone:a  
[0497] 角色:  
[0498] -网关  
[0499] 供应:真  
[0500] 用户名:centos  
[0501] machine\_id:ami-337be65c  
[0502] instance\_type:t2.xlarge  
[0503] volume\_size:10  
[0504] security\_groups:  
[0505] -all\_out\_scaling-vpc-1  
[0506] -all\_in\_scaling-vpc-1  
[0507] 子网:subnet\_1\_scaling-vpc-1

[0508] 接口:vrouter  
[0509] -名称:Contril\_controller\_scaling-VPC-1  
[0510] availability\_zone:a  
[0511] 供应:真  
[0512] 用户名:centos  
[0513] 角色:  
[0514] -控制器  
[0515] -k8s\_master  
[0516] machine\_id:ami-337be65c  
[0517] instance\_type:t2.xlarge  
[0518] volume\_size:24  
[0519] security\_groups:  
[0520] -all\_out\_scaling-vpc-1  
[0521] -all\_in\_scaling-vpc-1  
[0522] 子网:subnet\_1\_scaling-vpc-1  
[0523] 接口:eth0  
[0524] -名称:Compute\_scaling-vpc-1  
[0525] availability\_zone:a  
[0526] 供应:真  
[0527] 用户名:centos  
[0528] 角色:  
[0529] -compute\_node  
[0530] machine\_id:ami-337be65c  
[0531] instance\_type:t2.xlarge  
[0532] volume\_size:24  
[0533] security\_groups:  
[0534] -all\_out\_scaling-vpc-1  
[0535] -all\_in\_scaling-vpc-1  
[0536] 子网:subnet\_1\_scaling-vpc-1  
[0537] 接口:eth0  
[0538] -名称:Another\_compute\_scaling-vpc-1  
[0539] availability\_zone:a  
[0540] 供应:真  
[0541] 用户名:centos  
[0542] 角色:  
[0543] -compute\_node  
[0544] machine\_id:ami-337be65c  
[0545] instance\_type:t2.xlarge  
[0546] volume\_size:24

[0547] security\_groups:  
[0548] -all\_out\_scaling-vpc-1  
[0549] -all\_in\_scaling-vpc-1  
[0550] 子网:subnet\_1\_scaling-vpc-1  
[0551] 接口:eth0  
[0552] -名称:scaling-vpc-2  
[0553] cidr\_block:172.18.0.0/23  
[0554] 子网:  
[0555] -名称:subnet\_1\_scaling-vpc-2  
[0556] cidr\_block:172.18.0.0/24  
[0557] availability\_zone:a  
[0558] security\_groups:  
[0559] -名称:all\_in\_scaling-vpc-2  
[0560] 入口:  
[0561] from\_port:0  
[0562] to\_port:0  
[0563] 协议:"-1"  
[0564] cidr\_blocks:  
[0565] -"0.0.0.0/0"  
[0566] -名称:all\_out\_scaling-vpc-2  
[0567] 出口:  
[0568] from\_port:0  
[0569] to\_port:0  
[0570] 协议:"-1"  
[0571] cidr\_blocks:  
[0572] -"0.0.0.0/0"  
[0573] 实例:  
[0574] -名称:Contril\_GW\_scaling-VPC-2  
[0575] availability\_zone:a  
[0576] 角色:  
[0577] -网关  
[0578] 供应:真  
[0579] 用户名:centos  
[0580] machine\_id:ami-337be65c  
[0581] instance\_type:t2.xlarge  
[0582] volume\_size:10  
[0583] security\_groups:  
[0584] -all\_out\_scaling-vpc-2  
[0585] -all\_in\_scaling-vpc-2

- [0586] 子网:subnet\_1\_scaling-vpc-2
- [0587] 接口:vrouter
- [0588] -名称:Compute\_scaling-vpc-2
- [0589] availability\_zone:a
- [0590] 供应:真
- [0591] -用户名:centos
- [0592] 角色:
- [0593] -compute\_node
- [0594] machine\_id:ami-337be65c
- [0595] instance\_type:t2.xlarge
- [0596] volume\_size:24
- [0597] security\_groups:
- [0598] -all\_out\_scaling-vpc-2
- [0599] -all\_in\_scaling-vpc-2
- [0600] 子网:subnet\_1\_scaling-vpc-2
- [0601] 接口:eth0
- [0602] 另一VPC可以使用不同的IP地址池。
- [0603] 将修改应用于拓扑文件
- [0604] 使用以下命令更新关于变化的terraform
- [0605] ./transform/generate\_topology.py-t topology.yml-s secret.yml
- [0606] 创造必要的资源
- [0607] 使用此命令在AWS上创建资源
- [0608] terraform应用-自动-批准
- [0609] 重新生成库存
- [0610] 键入以下内容,以创建库存和轨迹配置:
- [0611] transform/generate\_inventories.py-t topology.yml-s secret.yml-ts  
terraform.tfstate
- [0612] 这将创建库存、轨迹配置以及state.yml。
- [0613] 更新网关
- [0614] 使用Ansible更新网关并提供新网关
- [0615] ansible-playbook-i inventories/inventory.yml
- [0616] ansible/gateway/playbooks/deploy\_and\_run\_all.yml
- [0617] 配置新的集装箱主机
- [0618] 使用该命令为轨迹部署准备新主机:
- [0619] ansible-playbook-i inventories/inventory.yml ansible/contrail/  
playbooks/configure.yml
- [0620] 拓扑602可以是网络的计算节点、网络节点和虚拟网络等的设置。这些被称为实例。此外或替代地,拓扑602可以包括多个项目,多个项目中的每个项目与云606相关联。换言之,拓扑602可以表示网络的优选基础设施,包括与至少一个VPC 606相关联的对象网络。

在一些示例中,拓扑602以人类可读的数据串行化语言编写,例如,YAML。YAML可以被配置为编码标量、列表、关联数组等。作为示例,拓扑602可以包括以下语言,来定义用于内部虚拟计算环境的项目和用于基于公共云的虚拟计算环境的三个其他项目,以供应整体多云虚拟计算环境(或“多云拓扑”):

```
[0621] -提供商:onprem
[0622] 组织:juniper-contrail
[0623] 项目:juniper-contrail
[0624] 实例:
[0625] -名称:OnPremGW-1
[0626] 角色:
[0627] -网关
[0628] 供应:真
[0629] 用户名:root
[0630] 密码:c0ntrail123
[0631] public_ip:10.87.65.157
[0632] private_ip:172.16.75.157
[0633] private_subnet:172.16.64.0/23
[0634] 接口:p514p1
[0635] vip:172.16.75.253
[0636] 协议:
[0637] -ssl_client
[0638] -提供商:谷歌
[0639] 组织:juniper-contrail
[0640] 项目:轨迹-codilime-多云
[0641] 地区:
[0642] -名称:us-west1
[0643] 云:
[0644] -名称:gcn-contrail-PVT
[0645] 子网:
[0646] -名称:子网-1
[0647] cidr_block:192.168.2.0/24
[0648] firewalls_external:
[0649] -名称:all-wan
[0650] 允许:
[0651] 协议:全部
[0652] firewalls_internal:
[0653] -名称:all-lan
[0654] 允许:
[0655] 协议:全部
```

[0656] 实例:  
[0657] -名称:gcloud-contrail-gw  
[0658] 角色:  
[0659] -网关  
[0660] 供应:真  
[0661] 用户名:ubuntu  
[0662] os:ubuntu16  
[0663] instance\_type:n1-standard-1  
[0664] 子网:子网-1  
[0665] 接口:ens5  
[0666] -名称:gcloud-contrail-k8s-node-1  
[0667] 供应:真  
[0668] 用户名:ubuntu  
[0669] 角色:  
[0670] -compute\_node  
[0671] os:ubuntu16  
[0672] instance\_type:n1-standard-1  
[0673] 子网:子网-1  
[0674] 接口:ens4  
[0675] -名称:gcloud-contrail-k8s-node-2  
[0676] 供应:真  
[0677] 用户名:ubuntu  
[0678] 角色:  
[0679] -compute\_node  
[0680] os:ubuntu16  
[0681] instance\_type:n1-standard-1  
[0682] 子网:子网-1  
[0683] 接口:ens4  
[0684] -提供商:aws  
[0685] 组织:juniper-contrail  
[0686] 项目:轨迹-多云  
[0687] 地区:  
[0688] -名称:us-east-1  
[0689] 云:  
[0690] -名称:AWS-contrail  
[0691] cidr\_block:192.168.0.0/23  
[0692] 子网:  
[0693] -名称:subnet\_1\_AWS-contrail  
[0694] cidr\_block:192.168.0.0/24

[0695] availability\_zone:a  
[0696] security\_groups:  
[0697] -名称:all\_in\_AWS-contrail  
[0698] 入口:  
[0699] from\_port:0  
[0700] to\_port:0  
[0701] 协议:"-1"  
[0702] cidr\_blocks:  
[0703] -"0.0.0.0/0"  
[0704] -名称:all\_out\_AWS-contrail  
[0705] 出口:  
[0706] from\_port:0  
[0707] to\_port:0  
[0708] 协议:"-1"  
[0709] cidr\_blocks:  
[0710] -"0.0.0.0/0"  
[0711] 实例:  
[0712] -名称:aws-contrail-gw  
[0713] availability\_zone:a  
[0714] 角色:  
[0715] -网关  
[0716] 供应:真  
[0717] 用户名:ubuntu  
[0718] machine\_id:ami-5c66ea23  
[0719] instance\_type:c4.large  
[0720] volume\_size:24  
[0721] security\_groups:  
[0722] -all\_out\_aws-contrail  
[0723] -all\_in\_aws-contrail  
[0724] 子网:subnet\_1\_AWS-contrail  
[0725] 接口:eth1  
[0726] protocols\_mode:  
[0727] -ssl\_server  
[0728] -名称:aws-contrail-k8s-node  
[0729] availability\_zone:a  
[0730] 供应:真  
[0731] 用户名:ubuntu  
[0732] 角色:  
[0733] -compute\_node

[0734] machine\_id:ami-5c66ea23  
[0735] instance\_type:c4.large  
[0736] volume\_size:24  
[0737] security\_groups:  
[0738] -all\_out\_aws-contrail  
[0739] -all\_in\_aws-contrail  
[0740] 子网:subnet\_1\_AWS-contrail  
[0741] 接口:eth0  
[0742] -提供商:azure  
[0743] 组织:Juniper  
[0744] 项目:contrail-codilime-multicloud  
[0745] 地区:  
[0746] -名称:WestUS2  
[0747] resource\_group:轨迹-多云  
[0748] 云:  
[0749] -名称:contrail-az-1  
[0750] cidr\_block:192.168.0.0/16  
[0751] 子网:  
[0752] -名称:subnet\_contrail\_az\_1  
[0753] cidr\_block:192.168.1.0/24  
[0754] security\_group:allow\_all\_protocols  
[0755] security\_groups:  
[0756] -名称:allow\_all\_protocol-contrail-az-1  
[0757] 规则:  
[0758] -名称:all\_in-contrail-az-1  
[0759] 方向:进站  
[0760] -名称:all\_out-contrail-az-1  
[0761] 方向:出站  
[0762] 实例:  
[0763] -名称:az-contril-gw-1  
[0764] 角色:  
[0765] -网关  
[0766] 供应:真  
[0767] 用户名:ubuntu  
[0768] os:ubuntu16  
[0769] instance\_type:Standard\_F16s\_v2  
[0770] 子网:subnet\_contrail\_az\_1  
[0771] 接口:eth1  
[0772] 名称:controller-contrail-az-1

[0773] 供应:真  
[0774] 用户名:ubuntu  
[0775] 角色:  
[0776] -控制器  
[0777] -k8s\_master  
[0778] os:ubuntu16  
[0779] instance\_type:Standard\_F32s\_v2  
[0780] 子网:subnet\_contrail\_az\_1  
[0781] 接口:eth0  
[0782] 名称:compute-contrail-az-1  
[0783] 供应:真  
[0784] 用户名:ubuntu  
[0785] 角色:  
[0786] -compute\_node  
[0787] os:ubuntu16  
[0788] instance\_type:Standard\_F16s\_v2  
[0789] 子网:subnet\_contrail\_az\_1  
[0790] 接口:eth0  
[0791] -名称:contrail-az-2  
[0792] cidr\_block:10.0.0.0/16  
[0793] 子网:  
[0794] -名称:subnet\_contrail\_az\_2  
[0795] cidr\_block:10.0.1.0/24  
[0796] security\_group:allow\_all\_protocols-contrail-az-2  
[0797] security\_groups:  
[0798] -名称:allow\_all\_protocol-contrail-az-2  
[0799] 规则:  
[0800] -名称:all\_in-contrail-az-2  
[0801] 方向:进站  
[0802] -名称:all\_out-contrail-az-2  
[0803] 方向:出站  
[0804] 实例:  
[0805] -名称:az-contril-gw-2  
[0806] 角色:  
[0807] -网关  
[0808] 供应:真  
[0809] 用户名:ubuntu  
[0810] os:ubuntu16  
[0811] instance\_type:Standard\_F16s\_v2

[0812] 子网:subnet\_contrail\_az\_2  
[0813] 接口:eth1  
[0814] -名称:compute-contrail-az-2  
[0815] 供应:真  
[0816] 用户名:ubuntu  
[0817] 角色:  
[0818] -compute\_node  
[0819] os:ubuntu16  
[0820] instance\_type:Standard\_F16s\_v2  
[0821] 子网:subnet\_contrail\_az\_2  
[0822] 接口:eth0

[0823] 应用程序接口 (API) 可以促进应用程序的创建和应用程序之间的通信。例如, (API) 610包括定义的接口,转换器604通过该接口与其他计算装置交互,以接收拓扑602。API 602可以被配置为从拓扑602“拉取”数据。尽管在图2中示出为包括单个API 610,但是在其他示例中,转换器604可以包括多个API,以从多个后端系统中拉取上下文数据。

[0824] 解析器612可以解析拓扑602的人类可读语言,并确定由拓扑602指示的网络元件的组织层级。解析器可以使用语言解析技术。换言之,解析器612可以获取输入数据(例如,拓扑602的文本),并构建给出拓扑602的图形的数据结构。更具体地,解析器612可以绘制拓扑602内的对象网络,使得对象网络的连接变得明显。在一些示例中,解析器612可以由用户编程。在其他示例中,解析器612可以使用编译器生成器来创建。该图可以包括解析树、抽象语法树、流程图、示出网络连接的图或另一视觉表示中的至少一个。

[0825] 规则数据库614可以包括使用模板生成器616管理拓扑602到模板618的转换的多个规则。规则数据库614的每个规则可以包括确定规则是成功还是失败的至少一个条件。每个条件可以包括至少一个事实、至少一个运算符和至少一个值。此外,每个规则可以包括一个事件。如果规则被认为是成功的,则触发事件。当评估规则数据库614的规则时,转换器604使用至少一个运算符来比较至少一个事实和至少一个值。规则可以实现全运算符或任意运算符中的至少一个。所有运算符都要求规则的多个条件中的每个条件必须是真实的,以便规则被认为是成功的。任何运算符都要求规则的多个条件中的至少一个条件必须是真实的,以便规则被认为是成功的。在一些示例中,可以嵌套所有运算符和任何运算符来创建复杂的布尔表达式。

[0826] 基于多个规则将拓扑602转换为模板618可以包括对于这组规则的规则,将一组条件应用于拓扑602。对于这组条件中的每个应用条件,转换器604可以确定相应的条件是否表示成功。响应于确定这组条件中的至少一个条件表示成功,转换器604可以执行对应于这组规则中的规则的事件。为了执行该事件,转换器604可以在拓扑602中识别对应于提供商的对象,并且根据对应于该对象的提供商将该对象放置在相应模板618的模板中。

[0827] 在一些示例中,模板生成器616可以使用规则数据库614的至少一个规则来确定云的身份,使得转换器604可以创建包括对应于每个云的对象模板。通过识别与每个对象相关联的云,模板生成器616使得转换器604能够将拓扑602的每个对象应用到云606的正确云。规则数据库614中可以包括以下示例规则:

```
假设 GoogleCloudRule = {  
[0828]   conditions: {  
           all: [{  
             fact: 'account-information',  
             operator: 'equal',  
             value: 'GCP',  
             path: '.tenant' // access the tenant property of  
             "account-information"  
           }, {  
             fact: 'VPC',  
             operator: 'in',  
             value: ['active'],  
             path: '.status'  
           }, {  
             fact: 'subnet',  
             operator: 'contains',  
             value: "",  
             path: '.prefix'  
[0829]   }, {  
             fact: 'security-group',  
             operator: 'contains',  
             value: "",  
             path: '.sgid'  
           }]  
         },  
         event: {  
           type: 'Google-Cloud-Event',  
           params: {  
             message: 'current Google cloud object'  
           }  
         }  
       }  
     }  
   engine.addRule(GoogleCloudRule)
```

[0830] 示例规则包含四个条件,包括:[{事实:‘帐户信息’、运算符:‘相等’、值:‘GCP’,路径:‘.tenant’ //访问“帐户信息”的租户属性}、{事实:‘VPC’、运算符:“in”、值:[‘活动’]、路径:‘.status’}、{事实:‘子网’、运算符:‘包含’、值:”、路径:‘.prefix’}、{fact:‘安全组’、运算符:‘包含’、值:”、路径:‘.sgid’}].示例规则包括单个事件,如下所示:事件:{键入:“谷歌-云-事件”,参数:{消息:‘当前谷歌云对象’}}。示例规则采用全运算符,这意味着四个条件中的每一个都必须成功,转换器604才能认为示例规则成功并触发事件。这样,为了触发将拓扑602的对象识别为谷歌云对象的事件,‘帐户信息’必须等于‘GCP’,‘VPC’必须是‘活动的’,‘子网’必须包含值”,并且‘安全组’必须包含值”。响应于确定拓扑602的对象是谷歌云对象,转换器604可以将该对象应用于VPC 606B。除了上述示例规则之外,规则数据库614还可以包括以下示例规则:

从 ‘json-rules-engine’ 导入{引擎}

引擎=['aws', 'google', 'azure']

/\*\*

\*设置新引擎

\*/

假设引擎=新引擎 ()

/\*\*

[0831] \*识别 AWS、谷歌和 Azure 的规则,

\*

\*/

假设 AzureRule={

conditions: {

all: [{

fact: 'account-information',

operator: 'equal',

value: 'azure',

```
        path: '.tenant' // access the tenant property of
        "account-information"
    }, {
        fact: 'Virtual Networks',
        operator: 'in',
        value: ['active'],
        path: '.status'
    }, {
        fact: 'subnet',
        operator: 'contains',
        value: '',
        path: '.prefix'
    }, {
        fact: 'security-group',
        operator: 'contains',
        value: '',
        path: '.sgid'
    }
    ]
},
event: {
    type: 'Azure-Cloud-Event',
    params: {
        message: 'current Azure cloud object'
    }
}
}
engine.addRule(AzureRule)
假设 AWSRule={
    conditions: {
        all: [{
            fact: 'account-information',
```

```

        operator: 'equal',
        value: 'AWS',
        path: '.tenant' // access the tenant property of
        "account-information"
    }, {
        fact: 'VPC',
        operator: 'in',
        value: ['active'],
        path: '.status'
    }, {
        fact: 'subnet',
        operator: 'contains',
        value: "",
        path: '.prefix'
    }, {
[0833]     fact: 'security-group',
        operator: 'contains',
        value: "",
        path: '.sgid'
    }
    ]
},
event: {
    type: 'AWS-Event',
    params: {
        message: 'current AWS cloud object'
    }
}
}

engine.addRule(AWSRule)

```

[0834] 模板生成器616可以使用Ansible来操作,Ansible是自动供应、配置管理和应用部署的软件。这样,模板生成器616可以使用ansible来执行规则数据库614的规则,以将解析器612解析的拓扑602转换为一个或多个模板618。模板618可以包括对应于每个云606的至少一个模板。在一些示例中,模板应用单元619可以使用控制器,例如,图1的控制器104,将模板618应用到云606。更具体地,模板应用单元619可以在云606内安装和修改对象,以定制

云606的多个计算基础设施。尽管图6的转换器604是针对公共云描述的,但是模板应用单元619也可以应用对应于公共云、内部云、裸机服务器系统或其他类型的数据中心的模板618。此外,对云606的修改或供应可以仅涉及在其中创建/修改/供应VPC。模板应用单元619可以使用terraform(基础设施即代码(IaC)的软件)将模板618应用到云606。

[0835] Terraform是一种软件,能够使用机器可读的定义文件而不是使用物理硬件配置或交互式配置工具来管理和配置数据中心。首先,terraform可以基于期望的基础设施配置来供应计算基础设施。其次,在创建计算基础设施之后,terraform被配置为根据期望的基础设施修改来修改计算基础设施。在一些示例中,terraform可以使用三个基本操作:刷新、计划和应用。Terraform刷新使得模板应用单元619能够观察计算基础设施的当前状态。Terraform计划允许模板应用单元619将期望的虚拟计算基础设施与计算基础设施的当前状态进行比较。另外,terraform应用使得模板应用单元619能够将对象应用到网络,使得网络实现期望的计算基础设施。模板618表示云606的多个期望的计算基础设施。模板应用单元619可以观察每个云606中计算基础设施的当前状态,并且使用模板618,模板应用单元619可以计划对云606的多个计算基础设施的改变。随后,模板应用单元619可以将模板618应用于云606,从而在云606内实现多个期望的虚拟化基础设施。

[0836] 图7是根据本公开中描述的技术的示例计算装置700的框图。计算装置700可以是云计算基础设施的图1的控制器102的示例实例。图7的计算装置700可以表示被配置为对SDN控制器132和编排器130中的至少一个执行操作的一个或多个真实或虚拟服务器。这样,计算装置700在某些情况下可以为迷你节点的相应集群实现一个或多个主节点。

[0837] 尽管API 720、解析器722、规则724、自动生成器726、模板728和terraform 729被示出和描述为由单个计算装置700执行,但是可以分布在多个计算装置700中。换言之,多个计算装置700中的每一个可以为任何一个或多个应用编程接口720、解析器722、规则724、自动生成器726、模板728和terraform 729的一个或多个实例提供硬件操作环境。

[0838] 在该示例中,计算装置700包括耦接计算装置700硬件环境的硬件组件的总线742。总线742耦接网络接口卡(NIC)730、存储盘746和一个或多个微处理器710(以下称为“微处理器310”)。在某些情况下,前端总线可以耦接微处理器710和存储装置744。在一些示例中,总线742可以耦接存储器装置744、微处理器710和NIC 730。总线742可以表示外围组件接口(PCI)快速(PCIe)总线。在一些示例中,直接存储器访问(DMA)控制器可以控制耦接到总线742的组件之间的DMA传输。在一些示例中,耦接到总线742的组件控制耦接到总线742的组件之间的DMA传输。

[0839] 微处理器710可以包括一个或多个处理器,每个处理器包括独立的执行单元,以执行符合指令集架构的指令,这些指令存储到存储介质。执行单元可以被实现为单独的集成电路(IC),或者可以组合在一个或多个多核处理器(或“多个核”处理器)内,每个多核处理器使用单个IC(即,芯片多处理器)来实现。

[0840] 磁盘746表示计算机可读存储介质,其包括以用于存储诸如处理器可读指令、数据结构、程序模块或其他数据的信息的任何方法或技术实现的易失性和/或非易失性、可移动和/或不可移动介质。计算机可读存储介质包括但不限于随机存取存储器(RAM)、只读存储器(ROM)、EEPROM、闪存、CD-ROM、数字多功能盘(DVD)或其他光存储装置、盒式磁带、磁带、磁盘存储装置或其他磁存储装置或可用于存储所需信息并可由微处理器710访问的任何其他

介质。

[0841] 主存储器744包括一个或多个计算机可读存储介质,其可以包括随机存取存储器(RAM),例如,各种形式的动态RAM(DRAM)(例如,DDR2/DDR3SDRAM)或静态RAM(SRAM)、闪存、或任何其他形式的固定或可移动存储介质,其可以用于以指令或数据结构的形式携带或存储期望的程序代码和程序数据,并且可以被计算机访问。主存储器744提供由可寻址存储位置组成的物理地址空间。

[0842] 网络接口卡(NIC)730包括一个或多个接口732,其被配置为使用底层物理网络的链路交换分组。接口732可以包括具有一个或多个网络端口的端口接口卡。NIC 730还可以包括卡上存储器,以例如存储分组数据。NIC 730和耦接到总线742的其他装置之间的直接存储器访问传输可以从NIC存储器读取/写入NIC存储器。

[0843] 存储器744、NIC 730、存储盘746和微处理器710可以为软件堆栈提供操作环境,该软件堆栈包括在内核空间中执行的操作系统内核714。内核714可以表示例如微软公司提供的Linux、伯克利软件分发(BSD)、另一Unix变体内核或视窗服务器操作系统内核。在一些情况下,操作系统可以执行管理程序和由管理程序管理的一个或多个虚拟机。示例虚拟机管理程序包括用于Linux内核的基于内核的虚拟机(KVM)、Xen、VMware提供的ESXi、微软提供的视窗Hyper-V以及其他开源和专有虚拟机管理程序。术语管理程序可以包括虚拟机管理器(VMM)。包括内核714的操作系统为用户空间745中的一个或多个进程提供执行环境。

[0844] 计算装置700可以耦接到物理网络交换结构,该物理网络交换结构包括覆盖网络,该覆盖网络将交换结构从物理交换机扩展到耦接到交换结构的物理服务器的软件或“虚拟”路由器,例如,图2的虚拟路由器220。计算装置700可以使用一个或多个专用虚拟网络来配置集群的迷你节点。

[0845] 包括API 720、规则724、自动生成器726、模板728和terraform 729的转换器750可以将拓扑152转换为一个或多个模板,这些模板定义了用于在一个或多个数据中心中配置多个计算基础设施的指令。这些组件可以表示转换器604的相应组件的示例。

[0846] 图8是示出根据本公开中描述的技术的用于在多云基础设施800内引导集装箱的另一示例控制器的框图。图8的基础设施800包括内部云810和私有云820。控制器812可以经由网关门户830A-830C(统称为网关830)分发数据(例如,分组、对象、集装箱、应用程序等)。网关830可以是图2的网关230的示例。在一些示例中,网关830的各种网关门户可以使用一组路径连接。例如,网关门户830A和网关门户830B可以通过边界网关协议(BGP)840A和互联网协议安全(IPSec)加密覆盖信道850A连接。BGP是一种标准化的外部网关协议,用于在服务器之间交换路由和可达性信息。例如,BGP可以发送通过一个或多个路由器(例如,基础设施800的vRouter)路由分组所需的信息。BGP会话可以加密,也可以不加密。因此,网关830包括用于在网关门户之间传输路由信息的安全信道可能是有益的。IPSec加密覆盖信道850可以连接网关门户,使得路由信息可以以安全的方式传输。

[0847] 图9是示出根据本公开中描述的技术的包括至少一个区域和至少一个可用性区域的示例私有云900的框图。该至少一个区域的每个区域包括具有映射到相应区域中的物理数据中心的可用性区域集合的地理区域。至少一个区域的每个区域在位置、电力、供水等方面与至少一个区域的每个其他区域物理隔离并且独立。可用性区域是私有云900的客户可用的区域中的逻辑数据中心。一个区域中的每个可用性区域都有冗余和独立的电源、网络

和连接,以降低两个可用性区域同时出现故障的可能性。

[0848] 图10A至图10C是示出根据本公开中描述的技术的包括至少一个网关门户的示例网络1000的框图。网关门户可以位于网络1000的每个可用性区域内。此外,控制器被配置为在可用性区域(包括网关门户)内构建和监控计算基础设施。如图10A所示,可用性区域的网关门户可以被配置为经由加密信道(IPSec、安全套接字层(SSL)或网络地址转换器遍历(Nat-t))与控制器的网关门户通信。如图10B所示,当每个可用性区域(例如,AZ-1和AZ-2)正常运行时,可用性区域(例如,AZ-1)内的租户装置被配置为与另一可用性区域(例如,AZ-2)内的控制器和租户装置一起发送和接收信息(例如,分组、集装箱等)。如果可用性区域(例如,AZ-1)离线(图10C),则另一可用性区域(例如,AZ-2)可以保持在线,并且网关门户可以使AZ-2内的租户装置能够与DC-1和DC-2的控制器交换信息。

[0849] 在一些示例中,可用性区域的故障可以由网关处理。例如,在实例故障期间,网关门户部署在每个可用性区域以及DC-1和DC-2内的活动-备用对中。网关实例故障将会通告隧道路由和下一跳,以指向当前活动的网关门户。如果两个网关实例都在可用性区域(例如,AZ-1)中发生故障,则将经由VPC内的AZ-2引导通往网关实例的路由。

[0850] 对于包括在任何流程图或流程图中的在本文描述的过程、设备和其他示例或图示,在本文描述的任何技术中包括的某些操作、动作、步骤或事件可以以不同的顺序执行,可以添加、合并或完全省略(例如,并非所有描述的动作或事件对于技术的实践都是必要的)。此外,在某些示例中,操作、动作、步骤或事件可以同时执行,例如,通过多线程处理、中断处理或多个处理器,而不是依次执行。此外,某些操作、动作、步骤或事件可以自动执行,即使没有被特别标识为自动执行。此外,被描述为自动执行的某些操作、动作、步骤或事件也可以不自动执行,但是在一些示例中,这些操作、动作、步骤或事件可以响应于输入或另一事件来执行。

[0851] 在一个或多个示例中,所描述的功能可以用硬件、软件、固件或其任意组合来实现。如果以软件实现,这些功能可以作为一个或多个指令或代码存储在计算机可读介质上和/或通过计算机可读介质传输,并由基于硬件的处理单元执行。计算机可读介质可以包括计算机可读存储介质,其对应于有形介质(例如,数据存储介质)或者包括有助于计算机程序从一个地方传输到另一地方的任何介质的通信介质(例如,根据通信协议)。以这种方式,计算机可读介质通常可以对应于(1)有形计算机可读存储介质(其是非暂时性的)或者(2)通信介质,例如,信号或载波。数据存储介质可以是可由一个或多个计算机或一个或多个处理器访问的任何可用介质,以检索指令、代码和/或数据结构来实现本公开中描述的技术。计算机程序产品可以包括计算机可读介质。

[0852] 通过示例而非限制的方式,这种计算机可读存储介质可以包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储器、磁盘存储器或其他磁存储装置、闪存或任何其他介质,其可以用于以指令或数据结构的形式存储期望的程序代码并且可以由计算机访问。此外,任何连接都适当地称为计算机可读介质。例如,如果使用同轴电缆、光纤电缆、双绞线、数字用户线路(DSL)或诸如红外、无线电和微波的无线技术从网站、服务器或其他远程源传输指令,则同轴电缆、光纤电缆、双绞线、DSL或诸如红外、无线电和微波的无线技术包括在介质的定义中。然而,应当理解,计算机可读存储介质和数据存储介质不包括连接、载波、信号或其他瞬态介质,而是指向非瞬态有形存储介质。使用的磁盘和光盘包括光盘(CD)、激光光盘、光盘、

数字多功能光盘 (DVD)、软盘和蓝光光盘,其中,磁盘通常磁性地再现数据,而光盘用激光光学地再现数据。上述的组合也应该包括在计算机可读介质的范围内。

[0853] 指令可以由一个或多个处理器执行,例如,一个或多个数字信号处理器 (DSP)、通用微处理器、专用集成电路 (ASIC)、现场可编程逻辑阵列 (FPGA) 或其他等效的集成或分立逻辑电路。因此,本文使用的术语“处理器”或“处理电路”可以均指任何前述结构或任何其他适于实现所描述的技术的结构。此外,在一些示例中,所描述的功能可以在专用硬件和/或软件模块内提供。此外,这些技术可以在一个或多个电路或逻辑元件中完全实现。

[0854] 本公开的技术可以在多种装置或设备中实现,包括无线手机、移动或非移动计算装置、穿戴式或非穿戴式计算装置、集成电路 (IC) 或一组 IC (例如,芯片组)。在本公开中描述了各种组件、模块或单元,以强调被配置为执行所公开的技术的装置的功能方面,但是不一定需要由不同的硬件单元来实现。相反,如上所述,各种单元可以组合在硬件单元中,或者由互操作硬件单元的集合提供,包括如上所述的一个或多个处理器,结合合适的软件和/或固件。

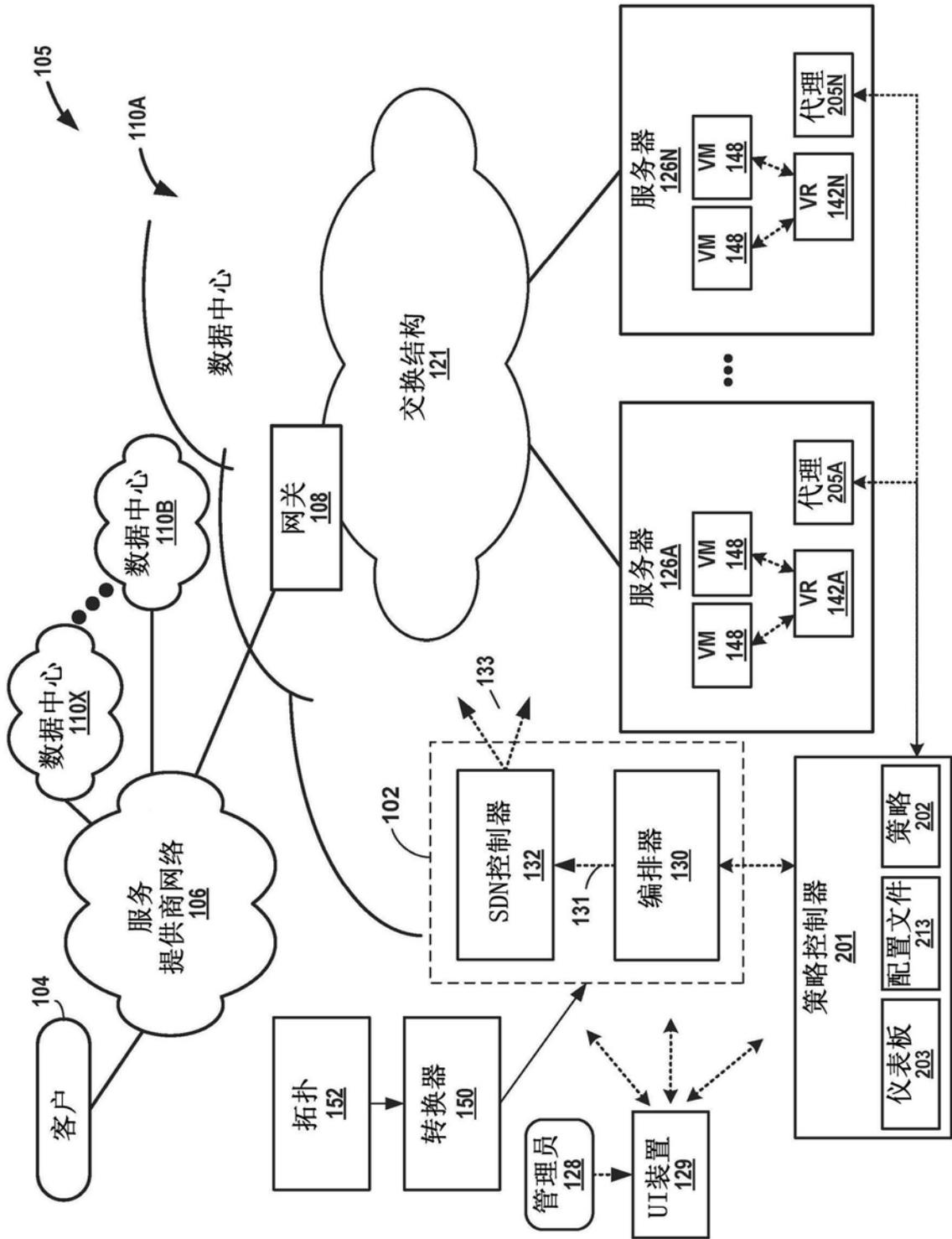


图1

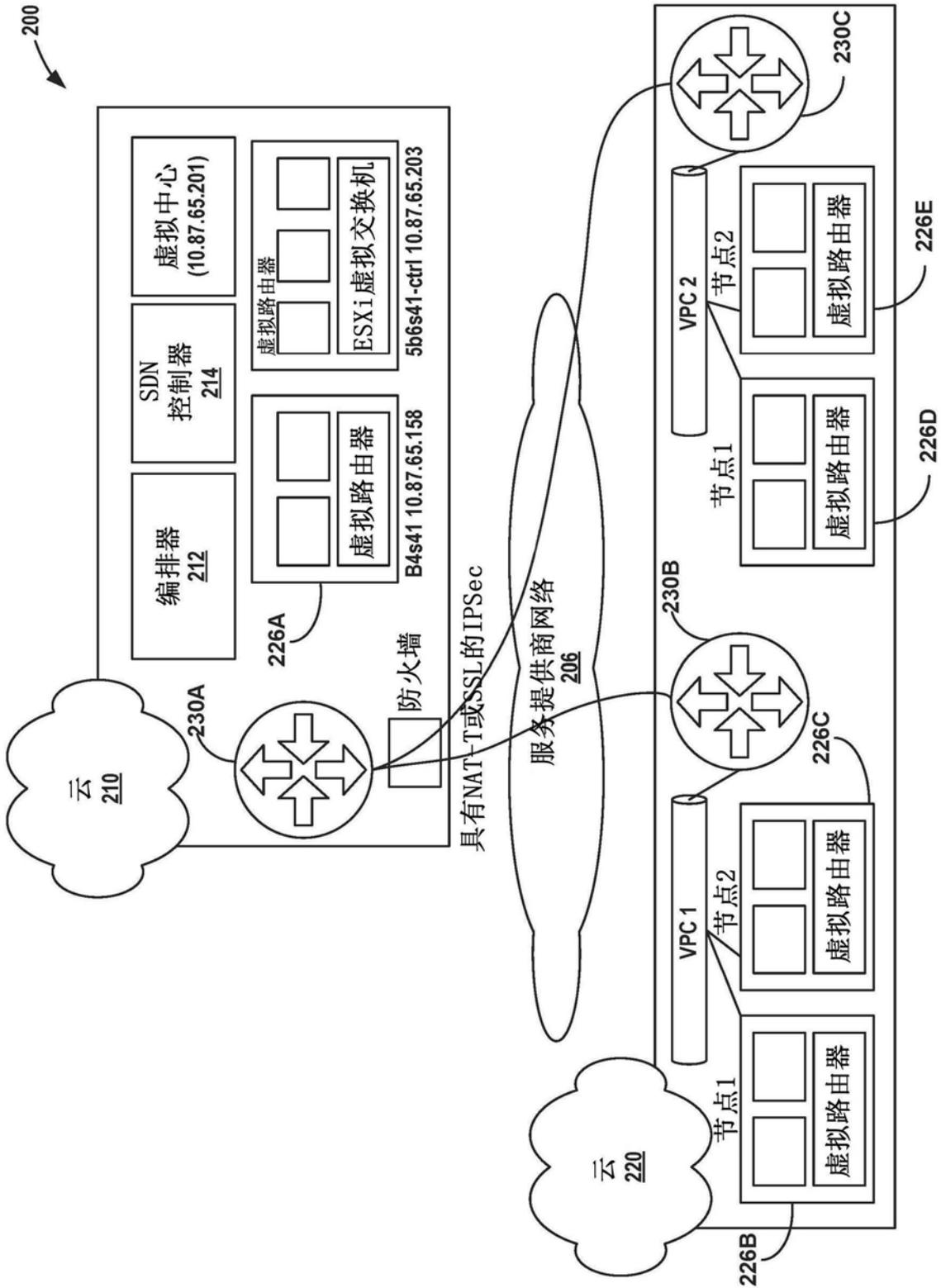


图2

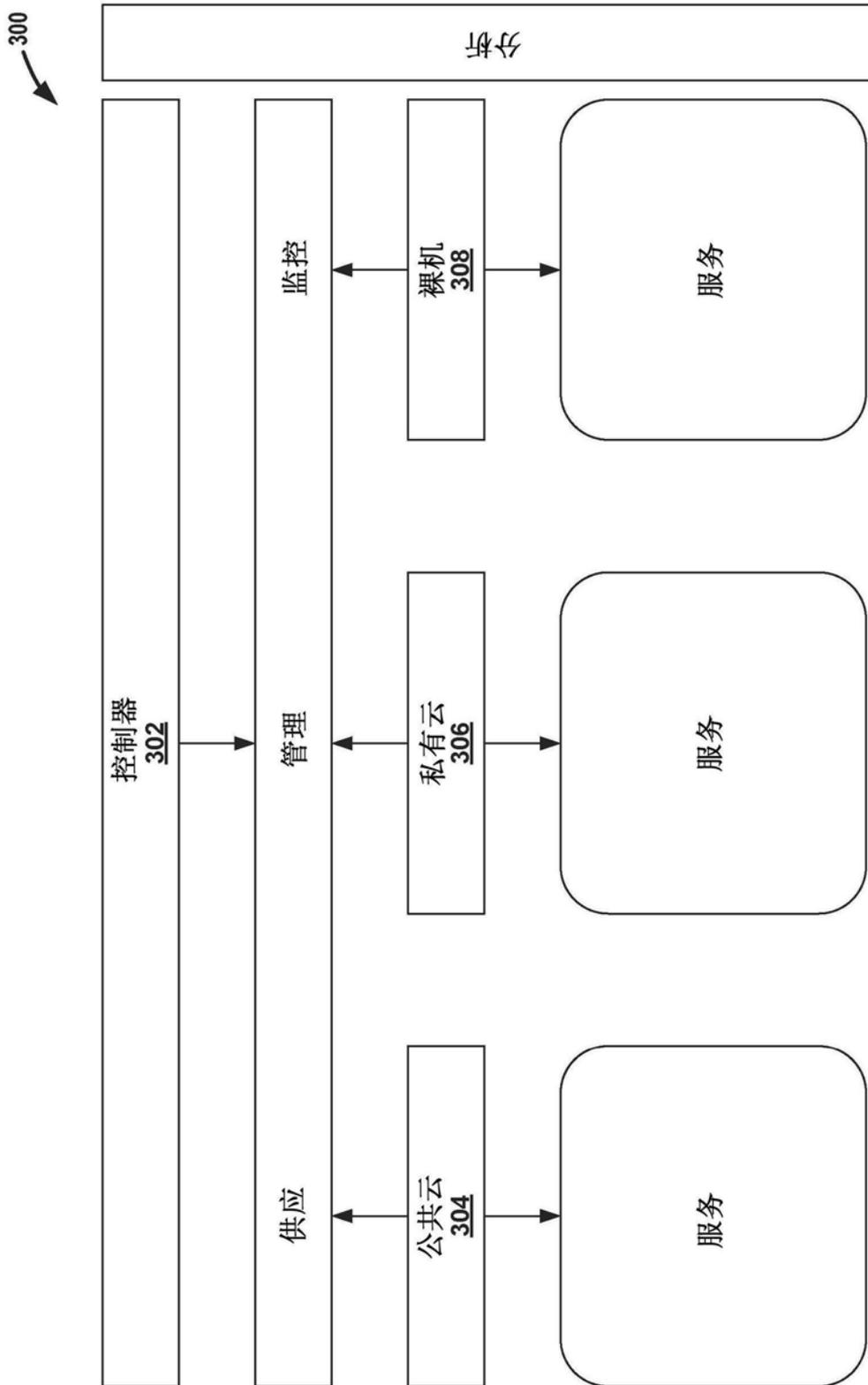


图3

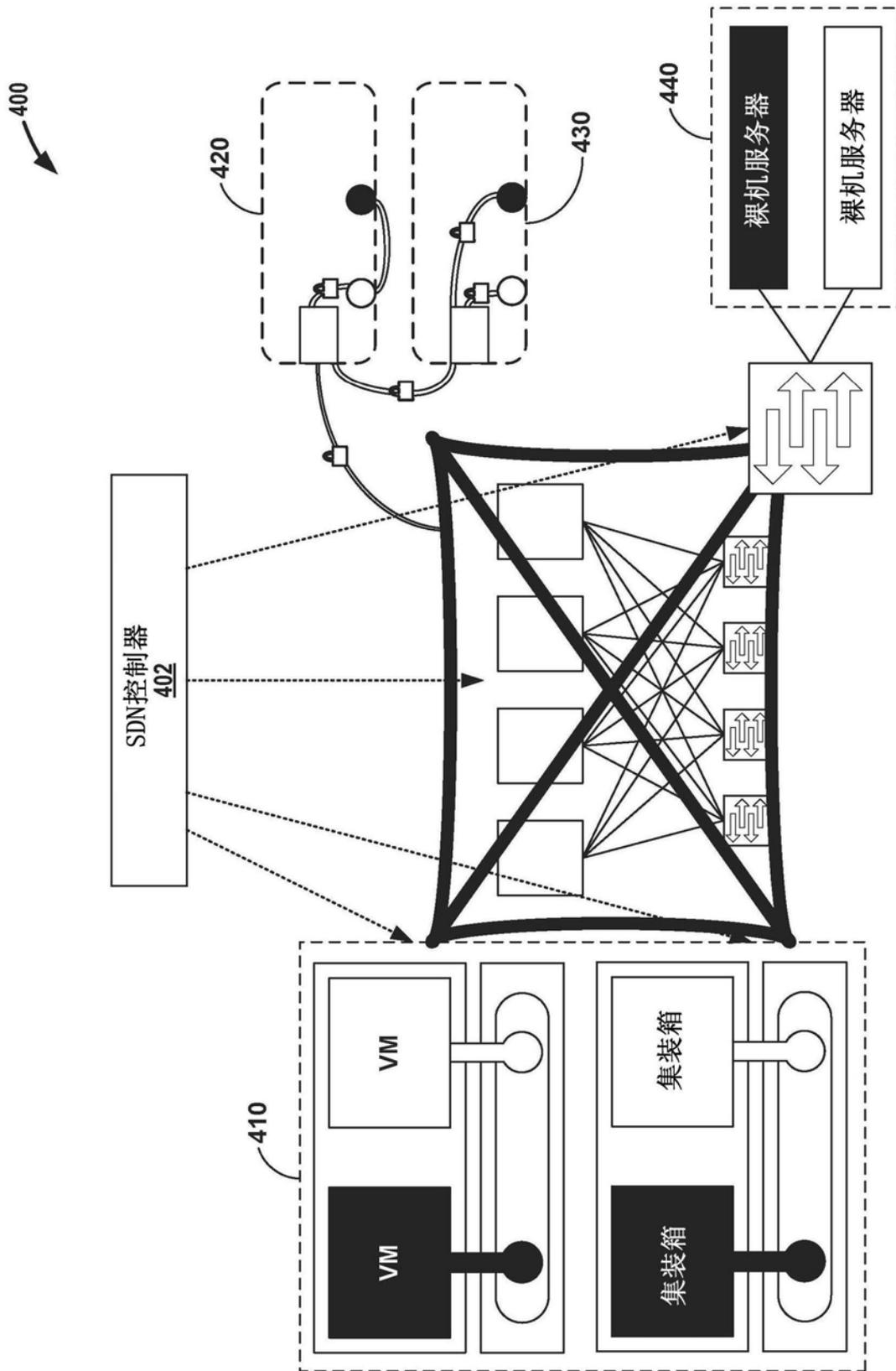


图4

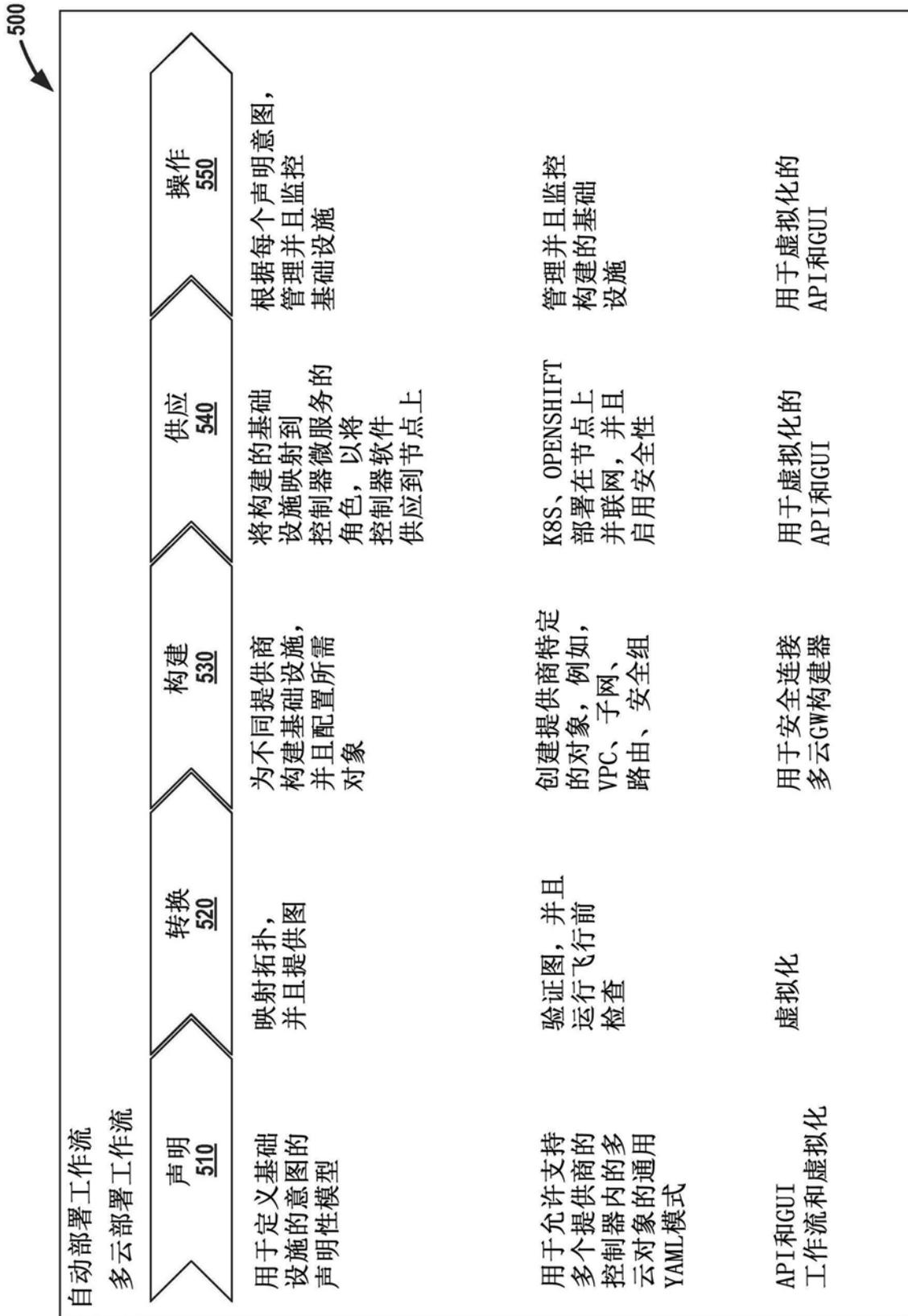


图5

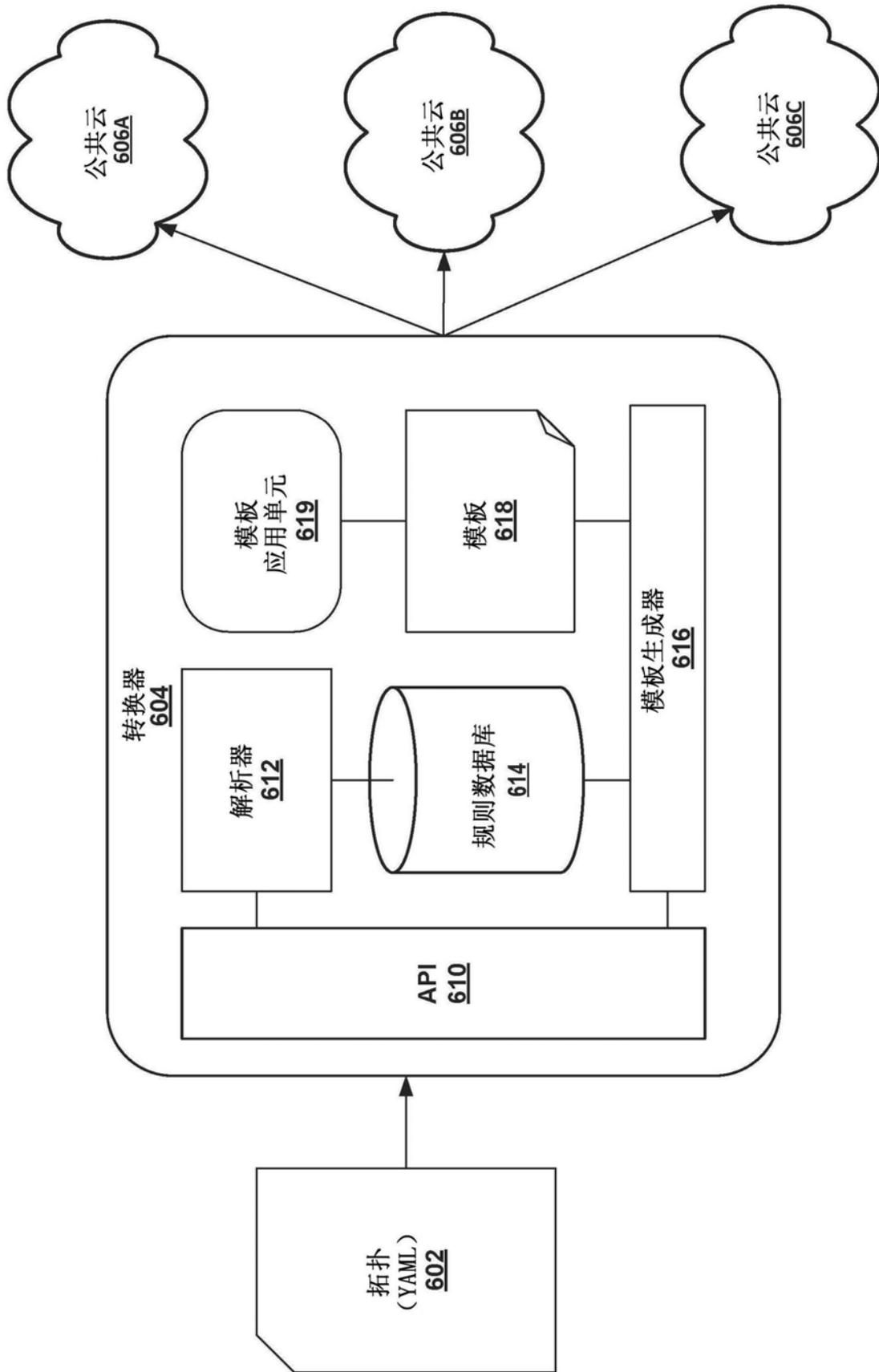


图6

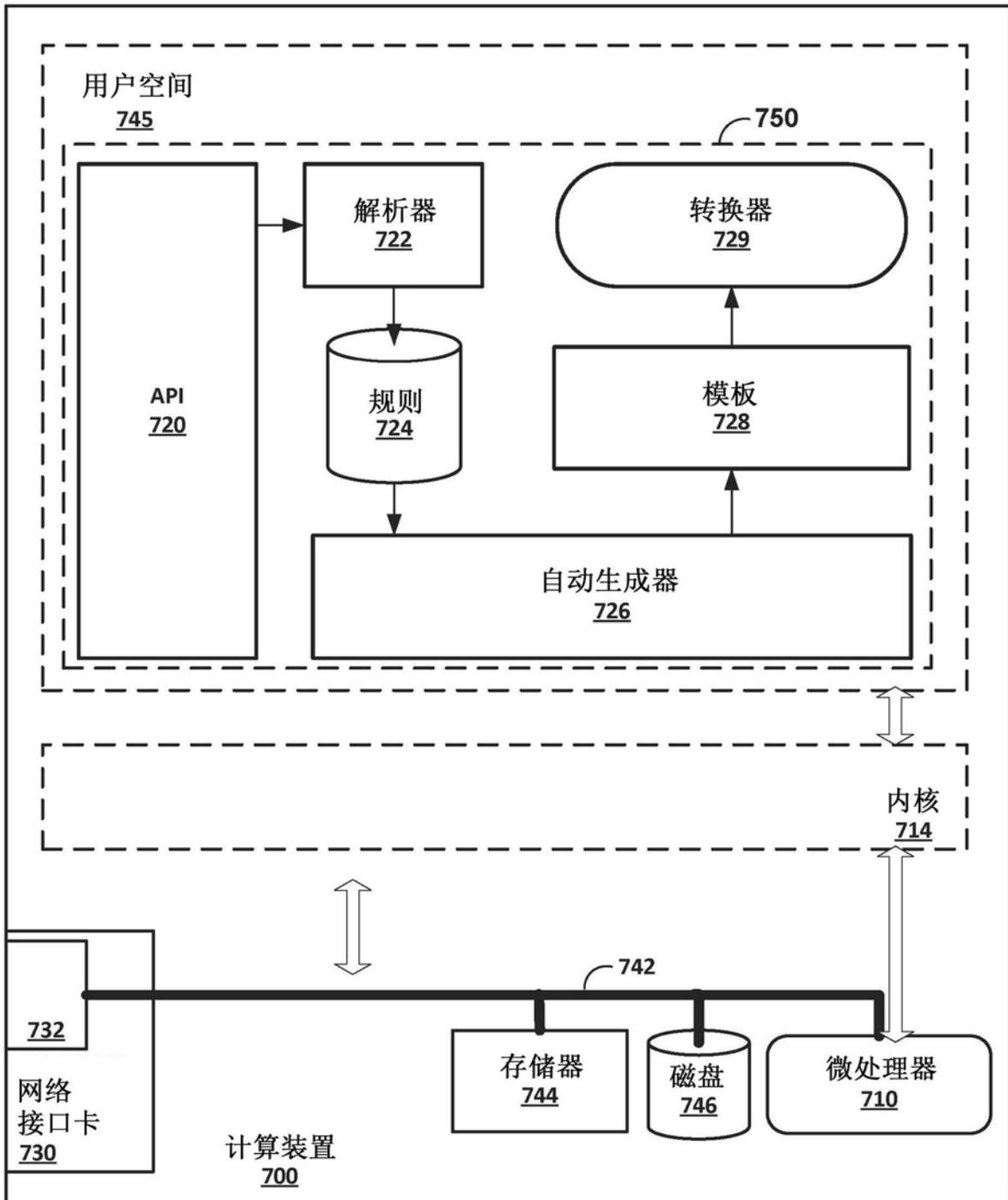


图7

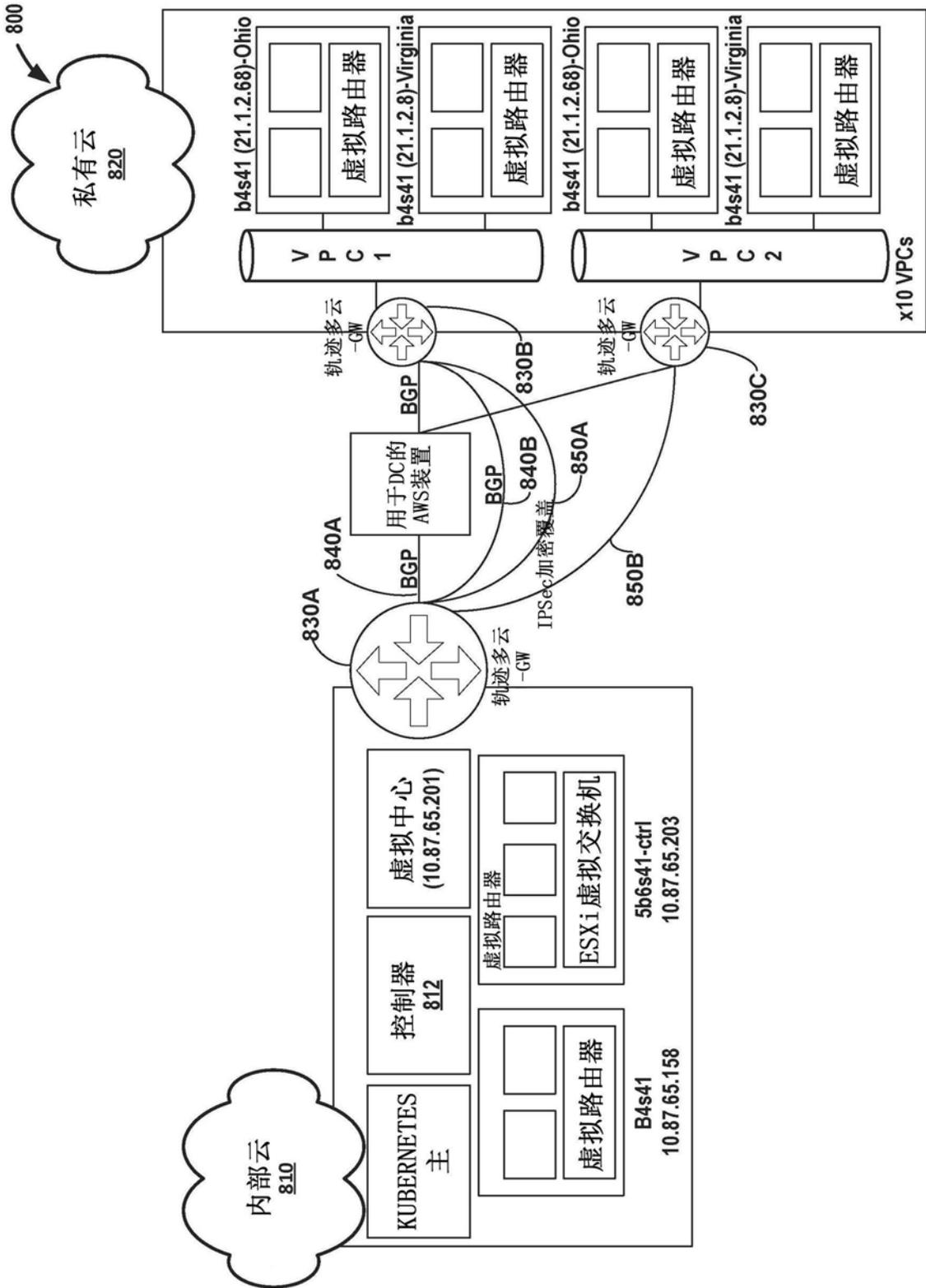


图8

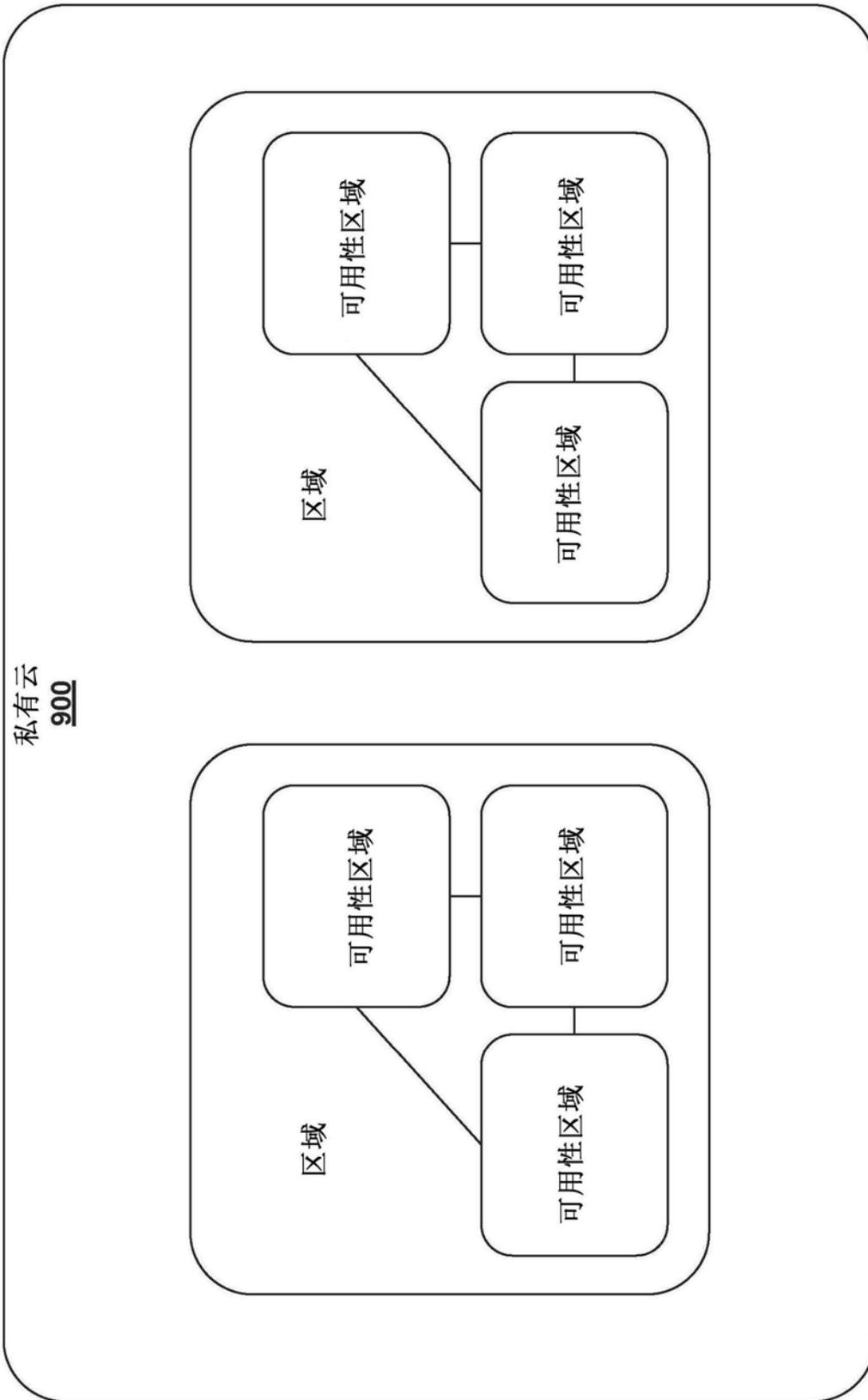


图9

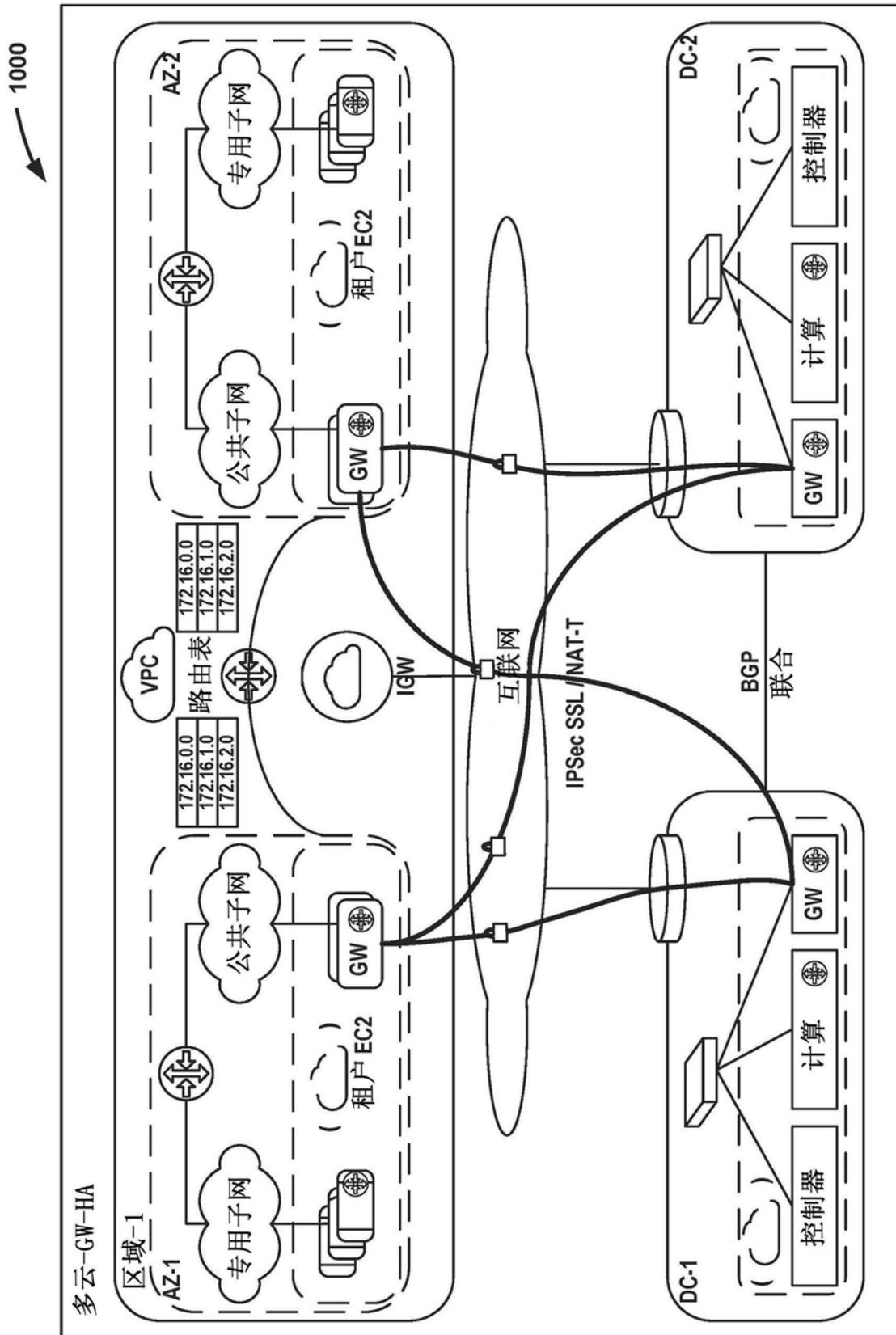


图10A

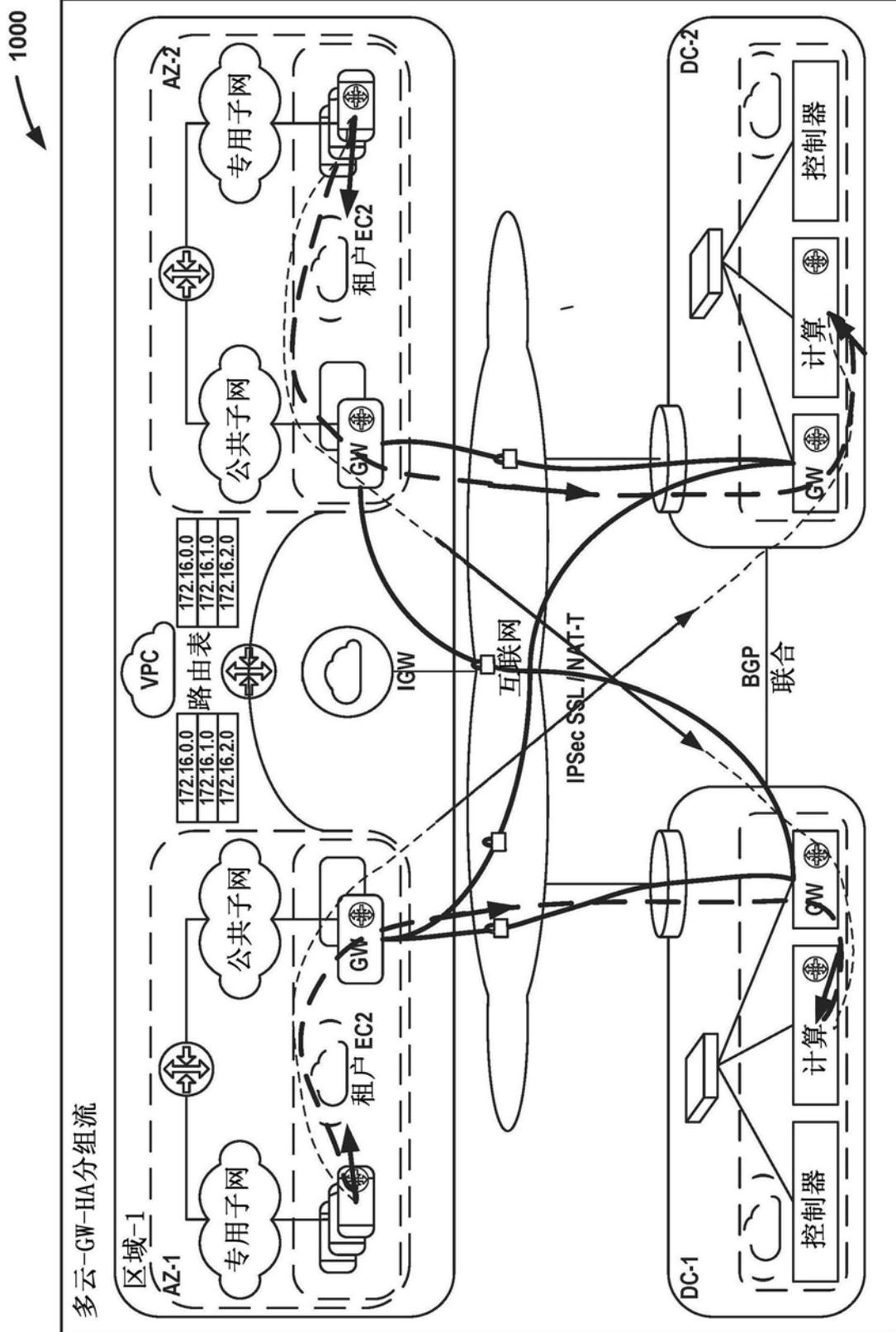


图10B

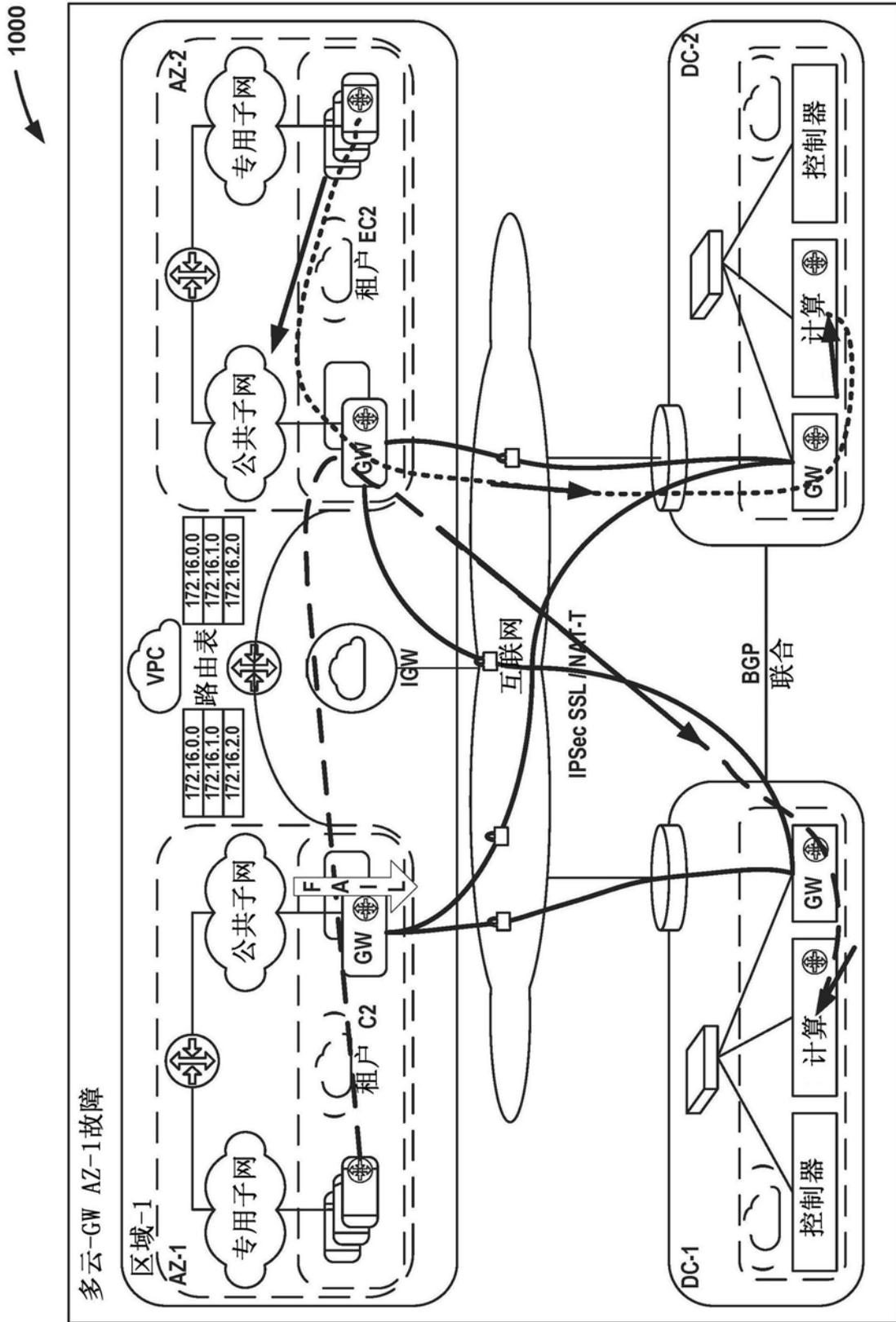


图10C