虚拟私有网络

产品文档

文档目录

虚拟私有网络
产品简介
产品概述

最近更新时间: 2023-03-20 16:36:39

什么是云虚拟私有网络

虚拟私有网络（Virtual Private Cloud，VPC）为您提供隔离的云上网络空间，帮您轻松创建建行云上数据中心。您可以创建虚拟私有网络VPC，并自定义VPC内IP地址、子网、路由、网络ACL等。您定义的虚拟私有网络VPC可以通过NAT网关访问Internet，也可以通过VPN连接或专线接入连接您本地的数据中心，构建混合云。

功能优势

功能优势

最近更新时间: 2023-03-20 16:56:39

稳定

建行云采用成熟的网络虚拟化技术，通过链路冗余，网关主备，保证网络高可用，提供高速低延时的稳定网络。

隔离

建行云通过 Overlay 技术，帮助您在建行云上构建一个完全隔离的虚拟私有网络环境，不同虚拟网络VPC间不能通信，满足您业务的安全隔离需要。

安全

建行云提供安全组和网络ACL服务，帮助您实现针对虚拟私有网络进行灵活的安全管控， 实现端口维度和实例维度的资源访问控制。

Internet互访

建行提供NAT服务帮助您的虚拟私有网络VPC进行Internet 访问；并可搭配弹性负载均衡等产品满足您部署Internet服务的需求。

多样化接入

建行云虚拟私有网络为您提供专线接入、VPN 连接等方式，帮助您连接本地数据中心与建行云上的资源。

应用场景

最近更新时间: 2023-03-20 16:56:39

主要的应用场景为互联网金融相关业务

云上数据中心

基于建行云创建不同的VPC承载不同业务模块，创建100%隔离的云上网络环境。

混合云架构

基于建行云部署云上数据中心，与云下本地数据中心通过VPN或专线连接，实现混合云架构。

提供Internet服务

基于建行云部署面向Internet的服务，配合弹性负载均衡服务，实现云上服务灵活部署。

访问Internet

基于建行云部署虚拟私有网络VPC支持多台CVM同时访问Internet，为公网应用提供支撑。

概念解释

最近更新时间: 2023-03-20 16:56:39

• 私有网络

虚拟私有网络（Virtual Private Cloud）能帮助您在建行云上构建出独立的网络空间，可以配合云主机、负载均衡等云服务一起使用。建行云虚拟私有网络为您提供以下功能：

1) 通过控制台自定义网段划分、IP地址、路由策略等

2) 通过弹性 IP 、NAT 网关等灵活访问 Internet

3) 通过 VPN 和专线接入将私有网络与您的数据中心连通

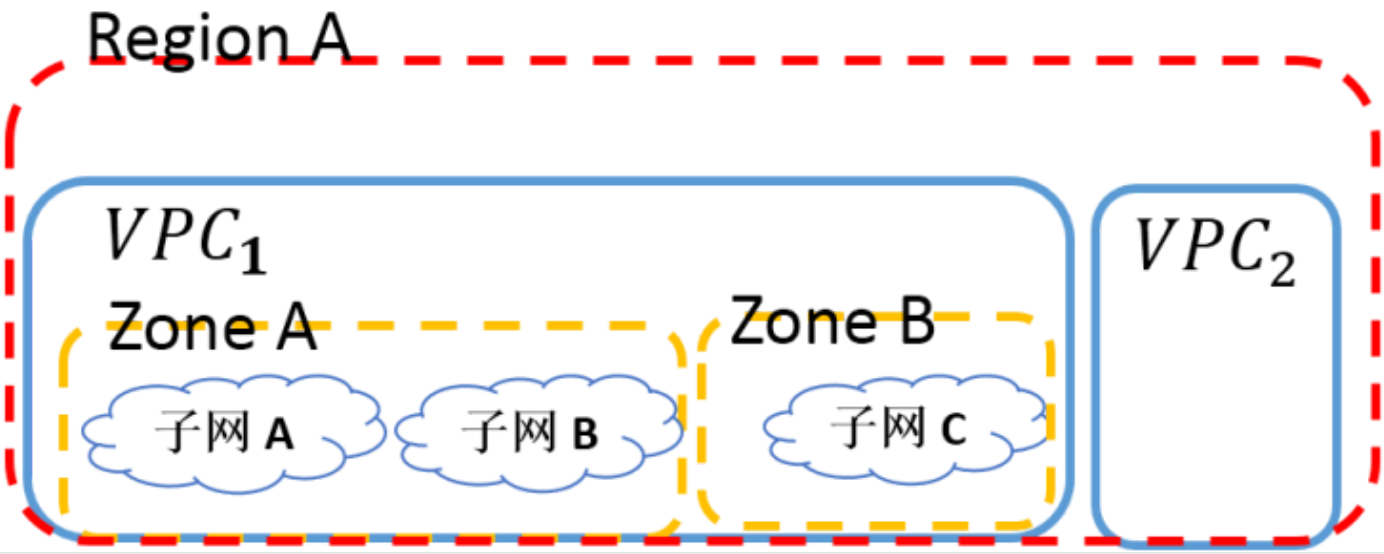
4) 通过对等连接服务可实现云上资源互通

通过安全组和网络ACL可以多维度、全方位的满足您的网络安全需求。

用户在创建 VPC 时，需要以无类域间路由（CIDR）块（例如 10.0.0.0/16）的形式为 VPC 指定 IP 地址组。私有网络有地域属性，比如VPC A 处于武汉，用户无法跨地域创建 VPC 。建行云暂时仅提供“武汉”地域，后续将持续增加地域。

• 子网

子网是 VPC 内的 IP 地址块，私有网络中的所有云资源都必须部署在子网内。子网具有可用区属性，如下图所示，在创建 VPC后，您可以在私有网络所属地域下的每个可用区中添加子网。可用区设计目的是隔离其他可用区的故障，通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。建行云暂时仅提供一个可用区，后续将持续增加可用区。



• 私有网络的IP地址

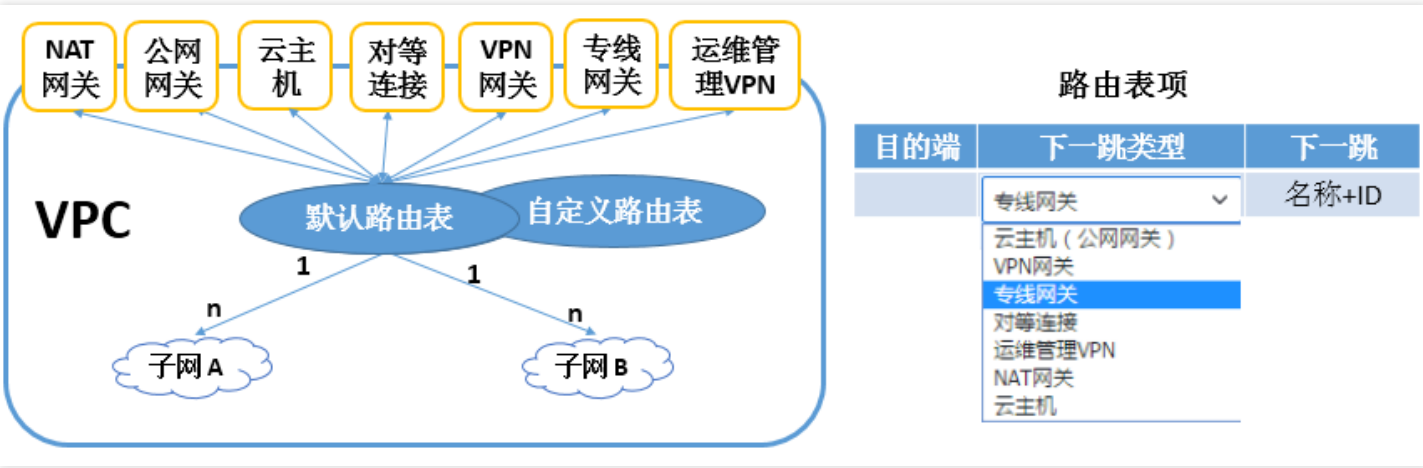
您可以通过指定CIDR（无类别域间路由）实现对私有网络和子网整体 IP 划分，建行云虚拟私有网络中使用的IP地址分为三类：

内网IP地址，是 VPC 内的实例必须指配的IP地址，用于 VPC 中实例之间的通信，无法用于 Internet 通信。

公网IP地址，是用于 Internet 访问的 IP 地址，并可用于实例与 Internet 之间的通信。
弹性IP（EIP），是可以独立申请的公网 IP 地址，支持与 NAT 网关实例的动态绑定和解绑。
• CIDR
CIDR（无类别域间路由，Classless Inter-Domain Routing）是由用户指定的独立网络空间地址块，通过IP和掩码结合，实现对网络的整体划分。以 10.1.0.0/16 为例，斜杠左边为网络块的IP，斜杠右边为网络块的掩码。通过设定掩码的大小就可以调整网络块的大小。网络块包括的IP数 = 2^(32-掩码)，因而 10.1.0.0/16 网络块最多包含65536个IP地址。目前私有网络支持三个网段内网IP：
10.0.0.0 – 10.255.255.255 (10/8 前缀)
172.16.0.0 – 172.31.255.255 (172.16/12 前缀)
192.168.0.0 – 192.168.255.255 (192.168/16 前缀)
掩码范围：允许最小为/16掩码，最大为/28掩码
在规划CIDR时需要注意：
1) 私有网络在创建时候必须指定 CIDR，创建后不可修改。
2) 子网的 CIDR 必须是所在私有网络 CIDR 的一部分。
3) 建立对等连接的私有网络之间的CIDR不能重叠。
4) VPN连接中每条SPD策略对应一个本端网段（私有网络网段）和对端网段（您的IDC网段），本段网段和对端网段不能重叠。
• 广播和组播
仅支持子网内组播和广播。
• 地域（Region）
建行云机房分布在北京武汉，这些节点都由地域（region）和可用区（zone）构成。创建私有网络时需要选择地域，创建子网时需要选择可用区，且子网必须选择在私有网络所在地域内的可用区；
申请云服务时建议选择最靠近您客户的地域，可降低访问时延。
1) 处在同一地域的云服务产品之间通过内网互通（不同用户间的云资源默认隔离）。
2) 处在不同地域的云服务产品之间内网默认不能互通。
3) 负载均衡服务绑定服务器时，只能选择绑定本地域的云服务器。
• 可用区（Zone）
可用区是同一地域下电力和网络互相独立的物理区域（一般是一个物理机房），命名采用【城市+编号】的结构。可用区的设计目标是保证不同可用区间故障相互隔离（大型灾害或者大型电力故障除外），不出现故障扩散，使得用户的业务持续在线服务。对于大型应用而言容灾是业务可用性的重要保障，多机房部署是容灾的通用做法；对于普通用户而言，多机房部署本是奢侈的投资，但建行云的多可用区设计让每个客户在不增加额外成本、运维复杂度的同时实现业务多机房容灾部署。
• 容灾型架构：当您的业务需要更高可用性时，跨可用区的多机房部署在保证低延时的同时为用户提供了高容灾保障。例如：可以分别在自用北京一区和自用北京二区申请云服务器，单可用区故障不会影响其他可用区云服务的正常运行。
• 低延时架构：若应用内部更注重低网络时延，则可以将业务部署在同一个可用区中。
关于可用区您需要注意的是：

在同一地域内可用区与可用区之间内网互通，同一可用区内网络延时更小。
已申请的云服务资源和网络不支持可用区的更换。

• 路由表
路由表由一系列路由规则组成，用于控制私有网络（VPC）内子网的出流量走向。如下图所示，云上的路由表有两种类型：默认路由表和自定义路由表。每个子网都必须关联一个路由表，每个路由表可以关联多个子网。
路由表由一系列路由策略组成，路由策略包括路由目的端、下一跳类型和下一跳组成，下一跳的类型可以是下图中的所有组件。



• 默认路由表
用户创建私有网络时，系统会自动为其生成一个默认路由表。在之后创建子网的过程中，如果用户没有选择自定义路由表则子网会自动关联该默认路由表。可以在默认路由表中添加、删除和修改路由规则，但无法删除该默认路由表。
• 自定义路由表
除了默认路由表之外，还可以在 VPC 中创建其他自定义路由表，自定义路由表可以被删除。用户可以为具有相同路由策略的子网建立一个自定义路由表，并将路由表和需要遵循其中路由策略的所有子网关联。您可以在 创建子网时绑定路由表或子网创建后更换路由表。
• 关联路由表
每个路由表可以关联同一个私有网络中的多个子网，但每个子网有且只能关联一个路由表。您可以在子网中更改关联路由表，但不能在路由表中更改或删除关联子网。
• 路由规则
路由规则用来控制数据包的路由途径。有默认路由规则和自定义路由规则两种类型，其中每条路由规则包含了三个参数：
目的端：目的网段描述（仅支持网段格式，如果希望目的端为单个 IP，可设置掩码为32（如： 172.16.1.1/32），目的端 不可以是路由表所在私有网络内的IP段。
下一跳类型：私有网络的数据包出口。私有网络下一跳类型支持“VPN网关”、“专线网关”等类型。
下一跳：指定具体跳转至哪个下一跳实例（使用下一跳 ID 标识）。
注意：

所有路由表均包含一条默认 local 路由规则，含义为私有网络内网互通。其路由规则为 [Local，Local，Local]，该路由规则不能被删除和修改。

• 路由规则优先级

当路由表中存在多条路由规则时，路由优先级由高至低分别为：

1) 私有网络内流量：私有网络内流量最优先匹配。

2) 最精确路由：非私有网络内流量根据最精确路由规则匹配。

内网 IPv4 地址

内网 IPv4 地址是建行云 IPv4 内网服务的实现形式，无法通过内网 IPv4 访问 Internet。每个云服务器实例一经创建即被分配一个内网 IPv4 地址，内网 IPv4 地址可由系统自动分配，在私有网络环境下，内网 IPv4 地址也可由用户自定义。

内网 IPv6 地址

内网 IPv6 地址是建行云 IPv6 内网服务的实现形式，无法通过内网 IPv6 访问 Internet。在创建云服务器实例时，可选择免费分配 IPv6 地址，系统将自动分配，亦可在创建后再进行获取，在虚拟私有网络环境下，内网 IPv6 地址也可由用户自定义。

使用指引

最近更新时间: 2023-03-20 16:56:39

子网：

• 私有网络有地域属性，支持在同地域内多个可用区之间部署。

• 私有网络创建后无法更改大小，如果需要您可以删除当前 VPC 并重新创建一个私有网络。

• 私有网络仅支持子网内组播和广播。

• 私有网络可以包含多个子网，每个子网的网络块均为私有网络CIDR的子集，多个子网的CIDR网络块不可以重叠。

• 子网有可用区属性，不支持跨可用区部署，且子网的可用区只能是其私有网络地域下的可用区，子网中的云主机需与子网在同一个可用区。

• 新建私有网络和子网时候需指定 CIDR 且创建后无法更改，我们建议您创建时为私有网络和子网留出足够的IP资源以防业务扩容导致网络资源不足。

• 建行云保留了各个子网的前面两个IP地址和最后一个 IP 地址，以作IP联网之用。

例如：子网 CIDR 为 172.16.0.0/24，则建行云保留的 IP 地址为：172.16.0.0、172.16.0.1、和 172.16.0.255。

• 用户需要先创建好私有网络并划分子网后才可以在私有网络部署云服务资源，比如云主机和数据库等。

• 私有网络中添加云主机时，系统会在指定子网内为该实例默认随机分配一个内网 IP，用户可以在子机创建后重新指定每台云主机的内网 IP。

• 云服务器一旦选择了私有网络便不可变更，但支持在私有网络内更换子网。

• 云服务器更改私有网络的内网 IP 地址会导致主机重启，耗时会有一定差异，一般在两分钟左右。

• 私有网络内一台云服务器只能绑定一个内网 IP 和一个公网 IP

• 每个子网必须关联一个路由表，通过设定路由表可以指定子网的网络路由。

路由表

• 每个子网必须关联一个路由表，每个路由表可以关联多个子网。

• 默认路由表及已经关联了子网的自定义路由表不能删除。

• 默认 local 路由规则不能删除。

• 不支持 BGP 和 OSPF 等动态路由协议。

• 如下表所示，每个 VPC 上创建的路由表和在每个路由表中添加的路由规则均存在数量限制：

资源	限制（个）
每个私有网络内的路由表数	10
每个子网关联路由表个数	1
每个路由表的路由策略数	50

安全组

关于网络 ACL 您需要了解：

• 一个网络 ACL 可以绑定多个子网，但一个子网同一时间只能绑定一个网络 ACL。

- 网络 ACL 有单独的入站和出站规则，每条规则包括协议类型、端口、源/目的 IP，策略（拒绝/允许）和备注。
- 每个新建网络 ACL 最初都为关闭状态（不允许任何数据流），直至您添加规则为止。
- 网络 ACL 没有任何状态，对允许入站数据流的响应会随着出站数据流规则的变化而改变（反之亦然），亦即您需要分别对请求和响应数据流设置规则。
- 网络 ACL 对所关联子网内的 CVM 实例之间的互访不产生影响。

资源	限制（个）
每个私有网络内网络ACL数	50
每个网络ACL中规则数	入站方向：20条，出站方向：20条
每个子网关联的网络ACL个数	1
每个网络ACL关联的子网个数	无限制

实例	配额
IP地址对象（ipm）	每个租户上限1000
IP地址组对象（）	每个租户上限1000
协议端口对象（）	每个租户上限1000
协议端口组对象（）	每个租户上限1000
IP地址对象（ipm）内的IP地址成员	每个租户上限20
IP地址组对象（ipmg）内的IP地址对象成员（ipm）	每个租户上限20
协议端组对象（ppm）内的协议端口成员	每个租户上限20
协议端口组对象（ppmg）内的协议端口对象成员（ppm）	每个租户上限20
IP地址对象（ipm）可被多少个IP地址组对象（ipmg）引用	每个租户上限50
协议端口对象（ppm）可被多少个协议端口组对象（ppmg）引用	每个租户上限50

操作指南
私有网络

最近更新时间: 2023-03-20 17:18:59

私有网络

如何规划私有网络数量

如果您的业务量较小，且部署在同一地域，业务间无须通过私有网络进行隔离，推荐您规划一个私有网络。

您可以在一个私有网络中创建多个子网和路由表来实现流量的精细化管理，另外，建议您将多个子网分散到不同的可用区，实现不同可用区之间的相互容灾

创建私有网络

私有网络是使用云服务的基础，当一个地域未创建任何私有网络，在该地域创建云服务器、负载均衡或数据库时，您可以选择建行云为您自动创建默认私有网络和子网，而无需自行创建。

1）登录 私有网络控制台。

2）在【私有网络】页面顶部，选择 VPC 所属地域，单击【新建】。

3）在弹出的【新建 VPC】对话框中，填写 VPC 信息和初始子网信息。

4）参数设置完成后，单击【确定】完成 VPC 的创建，创建成功的 VPC 展示在列表中，如下图所示，新建 VPC 包含一个初始子网和一个默认路由表。

删除私有网络

当 VPC 不再使用，且 VPC 中的 IP 没有被占用、VPC 内没有云资源（如子网、云服务器、云数据库、网关等）时，可删除 VPC。

1）登录私有网络控制台。

2）在【私有网络】页面顶部，选择 VPC 所属地域。

3）在 VPC 列表中待删除的 VPC 右侧操作列单击【删除】，并确认操作。

子网

最近更新时间: 2023-03-20 17:18:59

子网

创建私有网络、初始化子网和路由表

私有网络至少包含一个子网，只有在子网中才可以添加云服务资源。

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台。
2. 选择一个列表上方下拉框中的地域，单击【新建】在此地域下创建私有网络。
3. 填写私有网络和子网的名称和CIDR（单击查看CIDR规划的约束），并选择子网的可用区。
4. 单击【创建】即可完成私有网络及子网的创建。

新增子网

用户可以同时创建一个或多个子网。

1. 单击私有网络控制台左导航栏中的【子网】。
2. 选择需要创建子网的地域和私有网络。
3. 单击【新建】，填写子网络名称、CIDR、可用区和关联路由表。
4. （可选）单击【新增一行】，可以同时创建多个子网。
5. 单击【创建】按钮完成子网创建。

关联子网和路由表

每个子网都必须关联一个路由表，用来指定子网的出站路由，您可以实时更改子网关联的路由表。如果需要新建路由表则可以参考创建路由表。

1. 进入私有网络控制台选择左导航栏中的【子网】。
2. 鼠标移动到需要修改的【子网】一行，选择操作中的【更换路由表】。
3. 单击【保存】按钮即可完成子网与路由表的关联。

向子网中添加云主机

1. 进入私有网络控制台选择左导航栏中的【子网】。
2. 在需要添加云主机的子网所在行，单击增加云主机图标。
   或者您可以：
3. 在CVM介绍页，单击立即创建按钮。
4. 在第三步，选择存储与网络，选择需要对应的私有网络和子网。
   查看私有网络内的所有资源

5. 单击私有网络控制台左导航栏中的【私有网络】。
6. 在列表上方，选择需要查看的私有网络所在地域。
7. 单击私有网络ID，进入详情页，即可查看私有网络内的所有资源。

修改云主机内网IP

云主机主网卡的主内网IP支持修改，辅助网卡的主内网IP不支持修改，操作步骤如下：

1. 进入云服务器控制台，单击左导航栏的云主机，进入云主机列表页。
2. 单击云主机ID，进入云主机详情页，单击上方tab：弹性网卡。
3. 单击修改主IP。
4. 填入新的IP，并保存即可。

删除私有网络

删除私有网络的前提条件是：私有网络内的IP没有被占用，同时私有网络内没有资源（例如：子网、NAT网关等）。

1. 单击私有网络控制台左导航栏中的【私有网络】。
2. 在列表上方，选择需要删除的私有网络所在地域。
3. 选择需要删除的私有网络所在列，单击操作列的【删除】。

删除子网

删除子网的前提条件是：子网内的IP没有被占用，同时子网内没有资源（例如：云主机等）。

1. 单击私有网络控制台左导航栏中的【子网】。
2. 选择需要删除的子网的所在地域和私有网络。
3. 选择需要删除的子网所在列，单击【删除】。

路由表

最近更新时间: 2023-03-20 17:18:59

修改默认路由表

在创建私有网络时系统会自动创建一个默认路由表，新建子网默认与默认路由表相关联。

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台。
2. 单击左导航栏中【路由表】，在路由表列表中单击路由表 ID 进入路由表详情页。
3. 【新增路由策略】即可新增路由规则。输入目的端网段，选择下一跳类型（公网网关、VPN网关、专线网关等），再选择下一跳 ID。
4. 单击【确定】按钮，此编辑立即生效。
5. （可选）单击路由规则右侧的【编辑】按钮，即可开始修改路由规则。
6. （可选）单击路由规则右侧的【删除】按钮，可删除该路由策略。

创建自定义路由表

除了系统自动生成的默认路由表，用户还可以自定义新的路由表。

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台。
2. 单击左导航栏中【路由表】，单击列表上方【新建】按钮，在创建路由表弹出框中输入路由表名称、所属私有网络及新建路由策略。
3. 单击【创建】按钮，即可在路由表列表中看到您新建的路由表。

删除自定义路由表

系统自动生成的默认路由表无法删除，但自定义路由表可以任意创建、修改和删除。

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台。
2. 单击左导航栏中【路由表】，单击要删除的路由表所在行的【删除】按钮。
3. 单击确认弹窗中的【删除】按钮即可删除所选的自定义路由表。

更改子网关联路由表

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台。
2. 单击左导航栏中【子网】选项卡，鼠标移动到需要修改的子网路由表编辑按钮即会出现在【关联路由表】列中。
3. 单击【编辑】按钮，在下拉框中选择关联路由表。
4. 单击【保存】即完成子网与路由表的关联。

安全组

最近更新时间: 2023-03-20 17:18:59

创建安全组

1. 登录虚拟私有网络服务器控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择【地域】，单击【+新建】。
4. 在弹出的“新建安全组”窗口中，完成配置。

添加安全组规则

登录虚拟私有网络控制台。

1. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
2. 在安全组管理页面，选择【地域】，找到需要设置规则的安全组。 3) 在需要设置规则的安全组行中，单击操作列的【修改规则】。
3. 在安全组规则页面，单击“入站规则”，并根据实际需求选择以下任意一种方式完成操作。

关联实例至安全组

1. 登录虚拟私有网络控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择实例所在地域，找到需要设置规则的安全组。
4. 在需要设置规则的安全组行中，单击操作列的【管理实例】，进入关联实例页面。
5. 在关联实例页面，单击【新增关联】。
6. 在弹出的“新增实例关联”窗口中，勾选安全组需要绑定的实例，单击【确定】。

移除安全组

1. 登录虚拟私有网络控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择【地域】，找到需要将实例移出的安全组。
4. 在需要将实例移出的安全组行中，单击操作列的【管理实例】，进入关联实例页面。
5. 在关联实例页面，选择需要移出的实例，单击【移出安全组】。
6. 在弹出的提示框中，单击【确定】。

调整安全组优先级

1. 登录虚拟私有网络控制台。
2. 在实例管理页面，单击云服务器实例 ID，进入详情页面。

3. 选择【安全组】选项卡，进入安全组管理页面。
4. 在右侧“已绑定安全组”模块中，单击【排序】，选中安全组右侧的并上下拖动，调整安全组的优先级，位置越靠上，安全组的优先级越高。
5. 完成调整后，单击【保存】即可。

修改安全组规则

1. 登录虚拟私有网络控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择【地域】，找到需要修改规则的安全组。
4. 在需要修改规则的安全组行中，单击操作列的【修改规则】，进入安全组规则页面。
5. 在安全组规则页面，根据需要修改安全组规则所属的方向（入站/出站），单击【入站/出站规则】页签。
6. 找到需要修改的安全组规则，单击操作列的【编辑】，即可对已有规则进行修改。

删除安全组规则

1. 登录虚拟私有网络控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择【地域】，找到需要删除规则的安全组。
4. 在需要删除规则的安全组行中，单击操作列的【修改规则】，进入安全组规则页面。
5. 在安全组规则页面，根据需要删除安全组规则所属的方向（入站/出站），单击【入站/出站规则】页签。
6. 找到需要删除的安全组规则，单击操作列的【删除】。
7. 在弹出的提示框中，单击【确定】。

删除安全组

1. 登录虚拟私有网络控制台。
2. 在左侧导航栏，单击【安全组】，进入安全组管理页面。
3. 在安全组管理页面，选择【地域】，找到需要删除的安全组。
4. 在需要删除的安全组行中，单击操作列的【更多】>【删除】。
5. 在弹出的提示框中，单击【确定】。

参数模板

最近更新时间: 2023-03-20 17:18:59

参数模板是一组 IP 地址或协议端口参数的集合，将一组有相同诉求的IP 地址或协议端口保存为模板，在添加安全组规则时，作为来源/目的 IP、协议端口可直接引用。合理使用参数模板，可以提高您使用安全组的效率。
支持如下四种类型的参数模板：
1) IP 地址：也称为 IP 地址对象，是一组 IP 地址的集合，支持单个 IP、CIDR、IP 范围。
2) IP 地址组：也称为 IP 地址组对象，是多个 IP 地址对象的集合。
3) 协议端口：也称为协议端口对象，是一组协议端口的集合，支持单个端口、多个端口、连续端口及所有端口，协议支持 TCP、UDP、 ICMP、GRE 协议。
4) 协议端口组：也称为协议端口组对象，是一组协议端口对象的集合。
•IP 地址模板支持格式
1) 单个 IP，如10.0.0.1。
2) 连续 IP，如10.0.0.1 – 10.0.0.100。
3) 网段，如10.0.1.0/24。
•端口模板支持格式
1) 单个端口，如TCP:80。
2) 多个离散端口，如TCP:80,443。
3) 连续端口，如TCP:3306–20000。
4) 所有端口，如TCP:ALL。

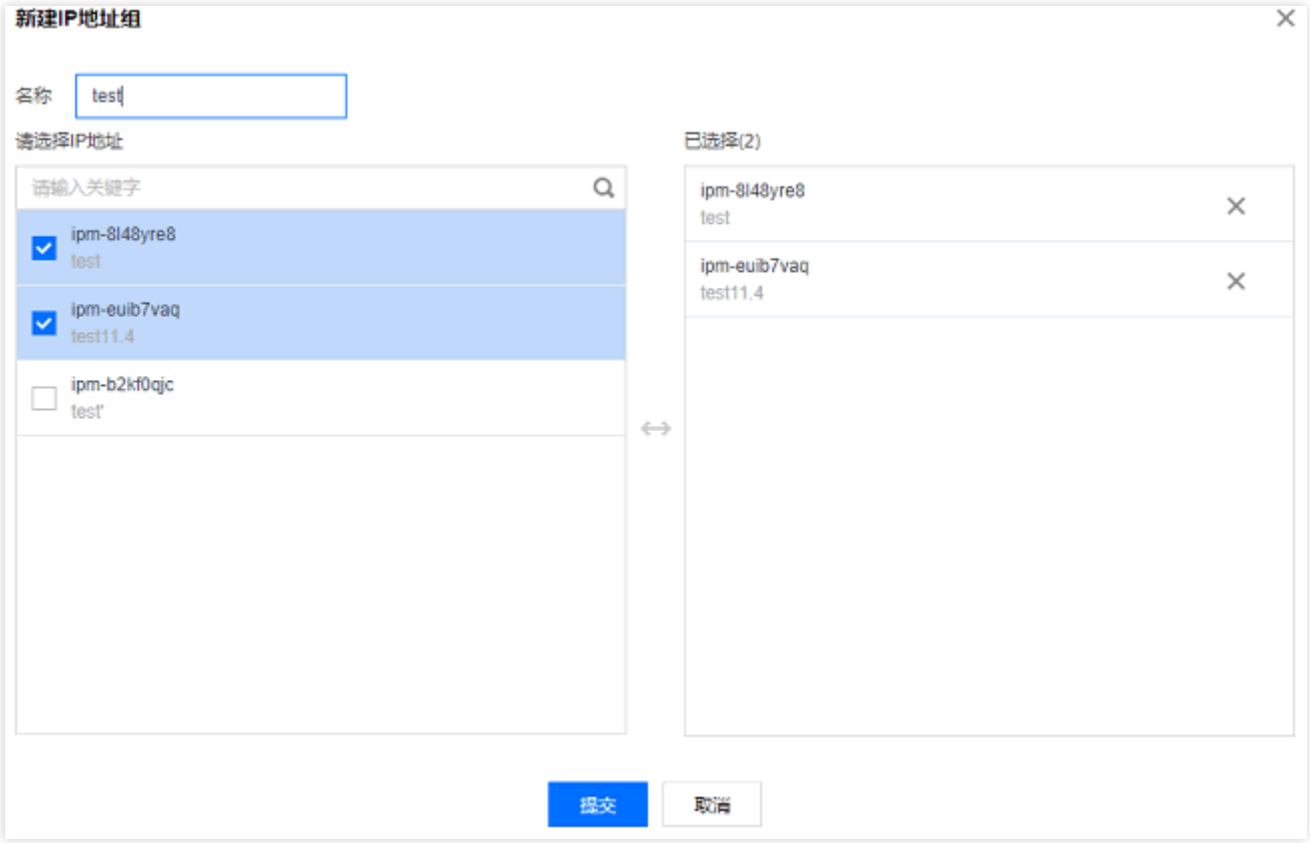
创建 IP 地址参数模板

1. 登录 私有网络控制台。
2. 单击左侧目录中的安全 > 参数模板，进入管理页面。
3. 在“IP 地址”标签页，单击+新建。
4. 在弹出框中，填写名称和 IP 地址，单击提交即可。
   IP 地址支持按照如下范围添加多个 IP 地址，请换行分隔，格式如下：
   单个 IP：如10.0.0.1或 FF05::B5。
   CIDR 网段：如10.0.1.0/24或 FF05:B5::/60。
   连续地址段：如10.0.0.1 – 10.0.0.100。

创建IP地址组参数模板

选择IP 地址组标签页，进入管理页面，单击+新建。

在弹出框中，填写名称，并选择需要添加的 IP 地址对象，单击提交即可。



创建协议端口参数模板

将具有相同诉求或频繁编辑诉求的协议端口加入到该协议端口对象中。

操作步骤

登录 私有网络控制台。

1) 单击左侧目录中的安全 > 参数模板，进入管理页面。

2) 单击协议端口选项卡，进入“协议端口”标签页，单击+新建。

3) 在弹出框中，填写名称和协议端口，单击提交即可。

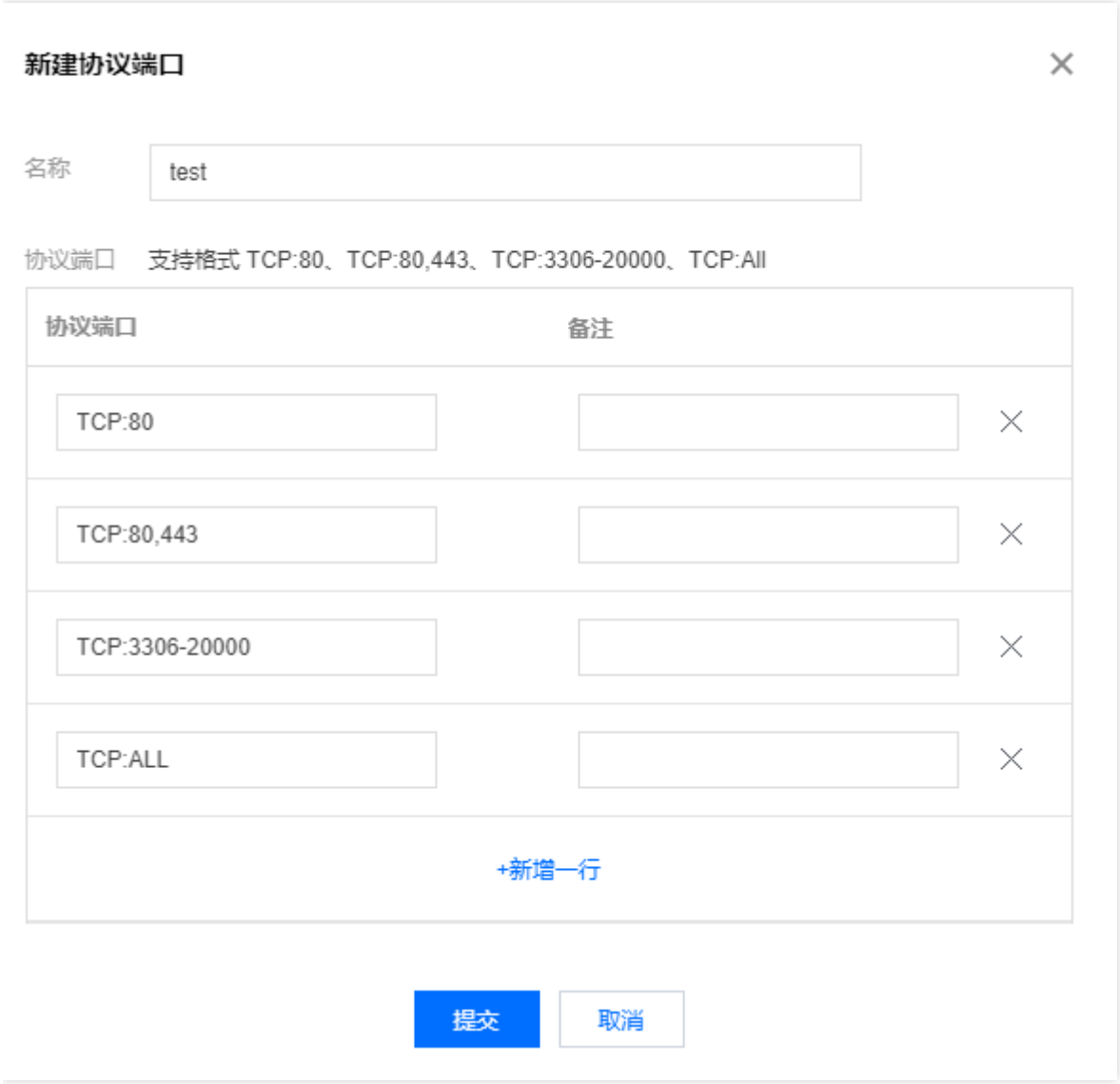
协议端口支持按照入下范围添加多个协议端口，请换行分隔，格式如下：

1) 单个端口，如TCP:80。

2) 多个离散端口，如TCP:80,443。

3) 连续端口，如TCP:3306–20000。

4) 所有端口，如TCP:ALL。



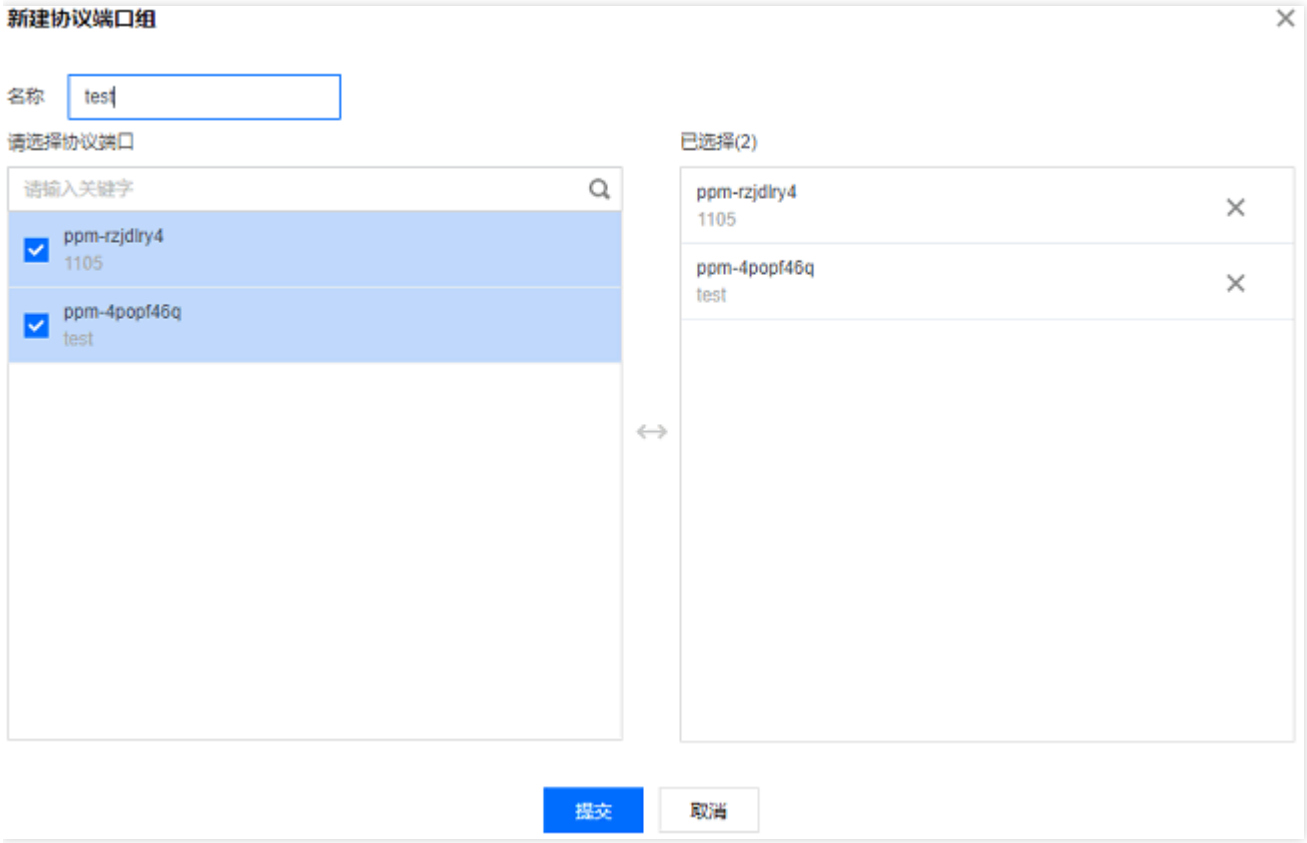
创建协议端口组参数模板

您可将创建的多个协议端口对象同时添加到一个协议端口组中，统一管理。

操作步骤

1. 选择协议端口组标签页，进入管理页面，单击+新建。

2. 在弹出框中，填写名称和选择需要添加的协议端口对象，单击提交即可。



修改参数模板

如需对创建的参数模板进行修改，例如，增加/删除 IP 地址、增加/删除协议端口，可按照如下步骤操作。

操作步骤

单击已创建的 IP 地址、IP 地址组、协议端口，或协议端口组参数模板，右侧的“编辑”，例如，下图为修改IP地址对象。

在弹出的编辑对话框中，修改相应参数，并单击提交即可。

删除参数模板

如不需要使用参数模板，可将其删除，删除后，所有包含此参数模板的安全组中的策略配置将一同删除，请评估后谨慎操作。

操作步骤

单击已创建的参数模板右侧的删除。

删除后，所有包含此 IP 地址、或协议端口的策略将一同删除，确认无误后，在弹出的删除确认框中继续单击删除。

在安全组中引用参数模板

参数模板创建后，可直接在安全组添加规则时引用参数模板来快速添加 IP 来源或协议端口，提高安全组规则的添加效率。

操作步骤

1) 登录 私有网络控制台。

2) 单击左侧目录中的安全 > 安全组，进入管理页面。

3) 在列表中，找到需要引用参数模板的安全组，单击其 ID，进入详情页。

4) 在入站 / 出站规则标签页中，单击添加规则。

5) 在弹出框中，选择“自定义”类型，在“来源”、“协议端口”中选择已创建的参数模板，并单击“完成”。添加入站 / 出站规则的详细步骤，请参见 添加安全组规则。

6) 后续如需增加新的 IP 地址或协议端口，仅需在对应 IP 地址组或协议端口组中增加即可，无须修改安全组规则或新建安全组。

ACL

最近更新时间: 2023-03-20 17:18:59

创建网络ACL

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2. 单击【新建】按钮，在新建网络 ACL 弹出框中输入名称、选择所属的私有网络，单击确定完成。

查看网络 ACL 列表

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2. 在顶部选择地域及私有网络，即可查看属于此私有网络的网络 ACL 列表。

增加网络 ACL 规则

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2. 在列表中单击要修改的网络 ACL 的 ID，进入网络 ACL 详情页。
3. 单击【入站规则】或【出站规则】选项卡，在规则列表旁单击【编辑】按钮，在编辑状态下单击【新增一行】按钮。
4. 新增的规则会默认加入规则列表的 首行，选择协议类型并输入端口、源 IP/目的 IP和策略，单击【保存】按钮。
   新增的规则即会显示在 ACL 规则列表中。

删除网络 ACL 规则

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2. 在列表中单击要修改的网络 ACL 的 ID，进入网络 ACL 详情页。
3. 单击【入站规则】或【出站规则】选项卡，在规则列表旁单击【编辑】按钮，在编辑状态下单击 ACL 规则后方的【删除】按钮。
4. 此时本条 ACL 规则置灰。若本次删除属于误操作，则可通过单击【恢复删除】按钮将其恢复。
5. 单击【保存】按钮，保存上述操作。
   注：ACL规则的删除必须保存后才会生效。

子网关联网络 ACL

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络ACL】选项卡。

2. 单击需要关联的网络 ACL 的 ID，进入网络 ACL 详情页。
3. 单击【基本信息】选项卡，在关联子网部分单击【新增关联】按钮。
4. 在关联子网弹出框中，选择需要关联的本私有网络下的子网，单击【确定】按钮，即可成功关联网络 ACL 与子网。

子网解关联网络 ACL

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】–【网络 ACL】选项卡。
2. 单击需要解关联的网络 ACL 的 ID，进入网络 ACL 详情页。
3. 单击【基本信息】选项卡，在关联子网列表中需要解关联的子网项后单击【解绑】按钮；或勾选所有需要解绑的
   子网，单击【批量解绑】按钮，即可解绑该子网与网络 ACL。

删除网络 ACL

1. 登录建行云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】–【网络ACL】选项卡。
2. 单击需要删除的网络 ACL 的【删除】按钮，在确认删除弹出框中单击【确定】，即可删除本网络 ACL 及本网络ACL 的所有规则。
3. 若【删除】按钮置灰，则表示本网络 ACL 正与子网相关联，您需要先解除这些关联后才能进行删除操作。

弹性网卡

最近更新时间: 2023-03-20 17:18:59

创建弹性网卡

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 选择地区和私有网络，单击【+新建】。
4. 在弹窗中，输入名称，选择弹性网卡的所属私有网络、子网后，选择分配的内网 IP （可自动分配也可手动填写），如需添加标签可展开【高级选项】进行添加。

绑定云服务器

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】。
3. 在弹性网卡列表页，找到需要绑定和配置的弹性网卡所在行，单击操作栏中的【绑定云服务器】。
4. 登录云服务器配置弹性网卡。

解绑云服务器

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 找到需要解绑的弹性网卡所在行，单击操作栏中的【解绑云服务器】。

申请辅助内网IP

1. 登录私有网络控制台。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 单击需要申请辅助内网 IP 的实例 ID，进入详情页。
4. 单击选项卡中的【IPv4 地址管理】，查看内网 IP 信息。
5. 单击【分配内网 IP】，在弹出框中选择自动分配，或手动填写要分配的内网 IP 地址，单击【确定】即可。
6. 在云服务器配置辅助内网IP使其生效。

释放辅助内网IP

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 单击需要查看的实例 ID，进入详情页。
4. 单击选项卡中的【IPv4 地址管理】，查看已绑定的内网 IP 和弹性公网 IP。
5. 找到需要释放的内网 IP 所在行，单击操作栏中的【释放】。
6. 在弹框中单击【确定】完成操作。

修改主内网IP

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 单击需要修改的实例 ID，进入详情页。
4. 单击选项卡中的【IPv4 地址管理】，查看已绑定的主内网 IP。
5. 单击需要修改的主内网 IP 所在行的【修改主 IP】。
6. 在弹窗内输入新的主内网 IP，单击【确定】即可。

修改所属子网

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 单击需要修改的实例 ID，进入详情页。
4. 单击所属子网后的【更换子网】。
5. 在弹出框中选择需要更换的子网，并指定新的主 IP。

删除弹性网卡

1. 登录私有网络控制台 。
2. 单击左侧目录中的【IP 与网卡】>【弹性网卡】，进入弹性网卡列表页。
3. 找到需要删除的弹性网卡所在行，单击操作栏中的【删除】。
4. 在弹框中单击【确定】即可。

常见问题
使用相关
子网无法删除

最近更新时间: 2023-03-20 16:32:14

当租户需要删除该子网，显示删除失败，还有未删除的资源时，如何定位问题是帮助租户解决排查问题的关键。
定位工具介绍
租户端私有网络界面。
问题定位及处理
登录租户端私有网络界面，确定是否还有资源未删除。
租户点击删除子网，提示删除子网失败或提示删除失败或4000子网内还有设备，无法删除。通常情况内，是由于该子网内还存在租户可见的、不可见的资源。

序号	原因&处理办法
1	该子网内还存在CLB实例，请租户查看是否还有CLB实例未删除
2	该子网关联ACL，请先将ACL解绑
3	该子网内还存在物理服务映射IP，请租户查看自建服务或数据库服务或CFS服务等是否皆已删除

排查思路：
登录console端，选择私有网络–子网，点击要删除的子网实例名称，进入子网详情页面，查看资源数量是否均为0。查看要删除的子网可用IP数，确认当前可用IP数是否与子网可用IP数相同。若当前可用IP数＜子网总共可用IP数，则是存在IP被占用情况，请检查是否存在表中1、3的情况。若无法解决，请联系建行云处理。

VPC无法删除

最近更新时间: 2023-03-20 16:32:14

当租户删除VPC失败时，用F12查看DeleteVpc接口返回结果提示VPC内仍有资源或仍有ip在使用，需要联系建行云处理。

定位工具介绍

开发者工具：Windows自带的查看部分源码的工具。

问题定位及处理

当租户删除VPC失败时，用F12查看DeleteVpc接口返回结果提示VPC内仍有资源，或指定资源 SubnetId 已经在使用中。 请先自查该VPC内是否还有未删除的资源，包括并不限于负载均衡、ACL、数据库等。

序号	原因&处理办法
1	VPC内用户可见资源未清空
2	VPC内有作为遗留探测用途的IP被占用

排查思路：

1) 点击私有网络，点击要删除的VPC实例名称，进入VPC详情页面，确认资源数量是否为除路由表数量为1，其他资源数量均为0。如果除路由表外的某项资源数量不为0，则请户自行评估删除。

2) 私有网络-安全-网络ACL，检查是否存在和VPC绑定的网络ACL实例，若存在，请租户自行删除。

步骤（1）、（2）确认不存在资源后，若该VPC内长时间未曾新建、变更资源，请先在该VPC内新建一台CVM，然后删除该CVM，再依次删除子网、VPC。若仍然删除不成功，请联系建行云。

安全问题

如何确保在 VPC 中运行的云主机的安全

最近更新时间: 2023-03-20 16:32:14

VPC本身是一个逻辑隔离的网络环境，另外安全组和网络 ACL 可以用来进行流量控制： 安全组可用于指定允许进出各个云主机的进站和出站网络流量。没有显式允许进出实例的流量将自动被拒绝。
网络访问控制列表(ACL)也可允许或拒绝进出各个子网的网络流量。

安全组与网络ACL的区别

最近更新时间: 2023-03-20 16:32:14

安全组	网络ACL
cvm实例级别的流量控制（第一防御层）	子网级别的流量控制（第二防御层）
支持允许规则和拒绝规则	支持允许规则和拒绝规则
有状态：返回数据流会被自动允许，不受任何规则的影响	无状态：返回数据流必须被规则明确允许
只有在启动CVM实例的同时指定安全组，或稍后将安全组与实例关联的情况下，操作才会被应用到实例	自动应用关联子网内的所有CVM实例（备份防御层，若CVM实例为绑定安全组，这里可以做备份防御）

IP和路由表问题

VPC 和子网中可以使用哪些 IP 地址范围

最近更新时间: 2023-03-20 16:32:14

私有网络支持三个网段的内网IP：10.a.0.0/8（a属于0至255）、172.b.0.0/16（b属于0至31）、192.168.0.0/16。私有网络的 CIDR 可以为以上三个网段，或者是网段中的一部分。

网络块包括的 IP 数 =2^(32-掩码)，因而 10.1.0.0/16 网络块最多包含 65536 个 IP 地址。