目录

虚拟私有网络与子网

虚拟私有网络

虚拟私有网络（Virtual Private Cloud）能帮助您在金山云构建出独立的网络空间，与您在数据中心运行的传统网络极其相似，但是托管在金山云私有网络内的是您在金山云上的服务资源，包括：云主机、负载均衡、云数据库等云服务资源。金山云私有网络为您提供以下功能：

- 通过控制台和 API 自定义网段划分、IP地址、路由策略等
- 通过弹性 IP 、NAT 网关灵活访问 Internet
- 通过 VPN 和高速通道将私有网络与您的数据中心连通
- 通过对等连接服务可实现两地三中心容灾
- 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，金山云可以创建位于华北1（北京）、华东1（上海）或香港的虚拟私有网络。

子网

子网是 VPC 内的 IP 地址块，虚拟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，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。

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，金山云私有网络中使用的IP地址分为三类：

- **内网 IP 地址**： VPC 内的实例必须指配内网IP地址，用于 VPC 中实例之间的通信，无法用于 Internet 通信。
- **弹性公网IP（EIP）**：可以独立申请的公网 IP 地址，支持与 KEC/SLB 等实例动态绑定和解绑。

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 10.2.0.0/16 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 10.2.0.0/16 网络块最多包含65536个IP地址。

在规划CIDR时需要注意：

- 虚拟私有网络在创建时候必须指定 CIDR，且创建后不可修改。
- 子网的 CIDR 必须是所在私有网络 CIDR 的一部分。
- 目前，私有网络 CIDR 的掩码支持/21至/8之间，亦即私有网络空间最少包含2048个、最大包含16,777,216个 IP 地址。
- 建立对等连接的私有网络之间的CIDR不能重叠。

使用约束

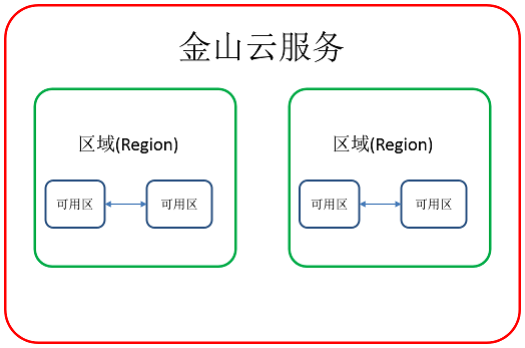
关于虚拟私有网络、子网您需要注意的是：

- 虚拟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。
- 虚拟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。
- 虚拟私有网络不支持多播或广播。
- 虚拟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。
- 新建虚拟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虚拟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。
- 用户需要先创建好虚拟私有网络并划分子网后才可以在虚拟私有网络部署云服务资源，比如云主机和数据库等。
- 每个子网会保留4个IP ：网络IP 、广播IP 、网关IP、保留IP。
- 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，用户可以在主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。
- 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。

地域和可用区

金山云数据中心分布在多个位置，这些位置由地域（Region）和可用区（Availability Zone）构成。

每个地域（Region）是一个独立的地理区域。每个地域内由一个或者多个相互隔离的位置，称为可用区（Zone）。每个地域（Region)是完全独立的，地域和地域通常距离较远，比如北京和上海是两个不同的地域。每个可用区都是独立的，但同一地域下的可用区距离较近，通过低时延高带宽的内网链路相连。下图阐明了区域和可用区之间的关系。



金山云支持用户在不同地域，可用区分配云资源，并且建议用户在设计系统时考虑将资源放置在不同可用区以屏蔽单点故障导致的服务不可用状态。金山云目前有以下地域和可用区：

- 中国地区

地域	可用区
华北1（北京）	可用区A，可用区B，可用区C
华北金融1（北京）	可用区A
华北政务1（北京）	可用区A
华东1（上海）	可用区A，可用区B
华东金融1（上海）	可用区A
华南1（广州）	可用区A
香港	可用区A

- 海外地区

地域	可用区
新加坡	可用区A
俄罗斯（莫斯科）	可用区A，可用区B

地域

金山云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。当前国内覆盖华北、华东、华南、香港等地区，海外覆盖新加坡、俄罗斯等地区。金山云会逐步增加区域和可用区供应以满足更多节点的覆盖。建议选择靠近终端用户的地域，可降低访问时延、提高下载速度。

用户启动实例、查看实例等动作都是区分地域属性的。

- 即使处于不同可用区，同区域下的云资源之间均通过内网互通，可以直接使用 VPC 内网IP访问。
- 不同地域之间的云产品默认不能通过内网通信。
  - 云服务器默认不可跨地域内网互访，默认不可跨地域访问云数据库，云缓存Redis；
  - 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；
- 不同地域之间云资源可以通过_弹性公网IP(EIP) 进行 Internet 访问；处于私有网络中的云服务也可以通过金山云提供的**对等连接**经由金山云高速互联网络通信，比 Internet 访问更稳定更快速。
- 上述内网互通是均指同一账户下的资源互通，不同账户的资源内网完全隔离；如需跨账号互相访问，可使用金山云**对等连接**服务，打通两个账号下的私有网络。

可用区

可用区（Availability Zone）是指金山云在同一地域内电力，网络，机房互相独立的物理数据中心。目标是能够保证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。通过在多个可用区启动不同实例，用户可以保护应用程序不受单一位置故障的影响，实现同地域下高可用服务。

用户启动实例时，可以选择指定地域下的任意可用区。当用户需要设计应用系统的高可靠性保持某个实例发生故障，服务仍然可用时，可以使用跨可用区的部署方案（如负载均衡，弹性IP等），以达到单可用区故障情况下，服务仍然可用。

公网NAT

简介

金山云 NAT （Network Address Translation）网络地址转换是一款能够让VPC内的云服务器或物理机访问互联网的产品，多机热备，故障自动切换，单 IP 最大支持 15Gbps 带宽，最大可支持 20 个 IP ，1亿以上并发连接数。

NAT是一种将虚拟私有网络中内网 IP 地址和公网 IP 地址进行转换的服务，能够让虚拟私有网络内无公网 IP 的云服务器或云物理主机访问 Internet（但不支持 Internet 主动访问虚拟私有网络内的云服务器或云物理主机）。金山云虚拟私有网络 NAT 的典型应用场景如下：

大出口、高可用 Internet 访问：针对用户需要超大带宽、公网 IP 使用量大、部署服务较多的公网访问应用场景，金山云 NAT 均可以满足需求。

安全的 Internet 访问：金山云虚拟私有网络的 NAT 提供 IP 的安全转换。如果用户希望隐藏虚拟私有网络内主机的公网 IP 以避免暴露其网络部署，同时又希望访问公网，那么使用金山云 NAT 可以满足这类需求。

产品特性

SNAT：源网络地址转换，用于 VPC 内的云服务器或云物理主机访问互联网。 DNAT：将NAT网关上的公网IP映射给云服务器使用，使云服务器能够提供互联网服务。DNAT支持端口映射和IP映射。 高性能：单IP可支撑最大 **15Gbps** 级别的转发能力； 高可用：多机热备，单机出故障自动切换业务无感知。

网络拓扑图

NAT 网关是一个处于 Internet 和 VPC 边界的网关，并接在 VPC 的路由器上。VPC 内云主机等资源通过 NAT 网关向外发送数据包时，数据会先经过路由器，按照路由策略进行路由选择。然后 NAT 网关通过 NAT IP 地址作为源 IP 地址，将流量发送到 Internet

NAT限速策略

购买带宽小于50Mbps，入机房最大放开到50Mbps，购买带宽大于等于50Mbps，出机房和入机房仍 1:1 限速。

弹性IP

简介

弹性公网IP（Elastic IP，简称EIP）是与用户账户相关联的IP地址，可以绑定到用户的任何一台云服务器、云物理主机或负载均衡上，让绑定的云资源具有和Internet通信的能力;拥有多种灵活的计费方式，可以满足各种业务场景的需求。

产品特性

- 资源关联：可以随时和云服务器、云物理机、负载均衡进行关联。
- 带宽灵活调整：带宽灵活调整，应对业务变化，实现网络的弹性。
- 精准计费：计费方式提供包年包月和按量计费，精准计量，将您的成本降到最低。
- 资源解耦：无论是否绑定云资源，弹性IP都属于您的账号，直到主动释放。
- 线路丰富：支持动态BGP，电信，联通，移动等多种线路。
- 灵活扩展：支持弹性 IP 共享带宽，增加带宽使用的灵活性。

使用范围

弹性IP可以随时和云服务器、云物理机、负载均衡进行关联。弹性IP只能与在同一地域内的资源进行绑定，支持动态的绑定和解绑。

- 1个弹性 IP 同一时间只能绑定到1个资源上
- 1个资源同一时间只能绑定1个弹性IP

EIP限速策略

原则上金山云会分配给用户与购买出流量带宽1：1的公网入带宽。但由于入流量带宽普遍比出流量带宽小，所以金山云在当前可用区整体入流量带宽低于出流量带宽时，会放开用户入流量带宽的限制，允许一定量的超出，增强用户体验。购买带宽小于50Mbps，入机房最大放开到50Mbps，购买带宽大于等于50Mbps，出机房和入机房仍 1:1 限速。

当金山云当前可用区整体入流量带宽大于出流量带宽时，会重新限制用户的入流量带宽，且优先限制入流量带宽与出流量带宽有极端差异的用户。

弹性IP不通原因排查方法

弹性IP不通一般有如下原因：

1）弹性IP没有绑定到资源上，具体绑定方法见 弹性IP产品使用文档

2）查看弹性IP绑定的资源内部是否有安全策略，如果有安全组策略，例如：禁止8080端口访问，那么弹性IP的8080端口也是无法访问的。

新建IPv4/IPv6双栈VPC

新建IPv4/IPv6双栈VPC

您可以在创建的VPC时,选择是否给VPC分配IPv6网段，默认不分配IPv6网段。如果您选择分配IPv6网段，金山云将为您的VPC自动分配掩码为/56的IPv6网段(如2401:1d40:f1a:b800::/56)，并且自动为您创建一条目标网段为::/0下一跳为互联网网关的路由

注意：

- 目前仅华北1（北京）、华南1（广州）、华东1（上海）地区支持IPv6。
- VPC创建后，不能再修改和删除IPv6网段。
- 需要您手动在安全组配置一条目标IP为::/0的出向规则。

操作步骤

1. 在控制台依次点击【网络】---【虚拟私有网络】进入虚拟私有网络页面，点击“新建VPC”按钮，
2. 在新的窗口内填写虚拟私有网络信息（名称、网段），子网信息（名称、网段）、NAT信息（名称），**需要勾选支持IPv6**，默认无IPv6网段。
3. 其他配置操作步骤和IPv4操作相同。

为已有VPC开启IPv6网段

为已有VPC开启IPv6网段

您可以为已创建的VPC配置IPv6网段。若您对存量的VPC开启IPv6网段后，不会影响已有的子网属性，存量的子网依然是IPv4的，您可以在新建子网时选择子网是否分配IPv6网段，默认不分配。

注意：

- 目前仅华北1（北京）、华东1（上海）、华南1（广州）支持IPv6。
- VPC创建后，不能再修改和删除IPv6网段。
- 需要您手动在安全组配置一条目标IP为::/0的出向规则。

操作步骤

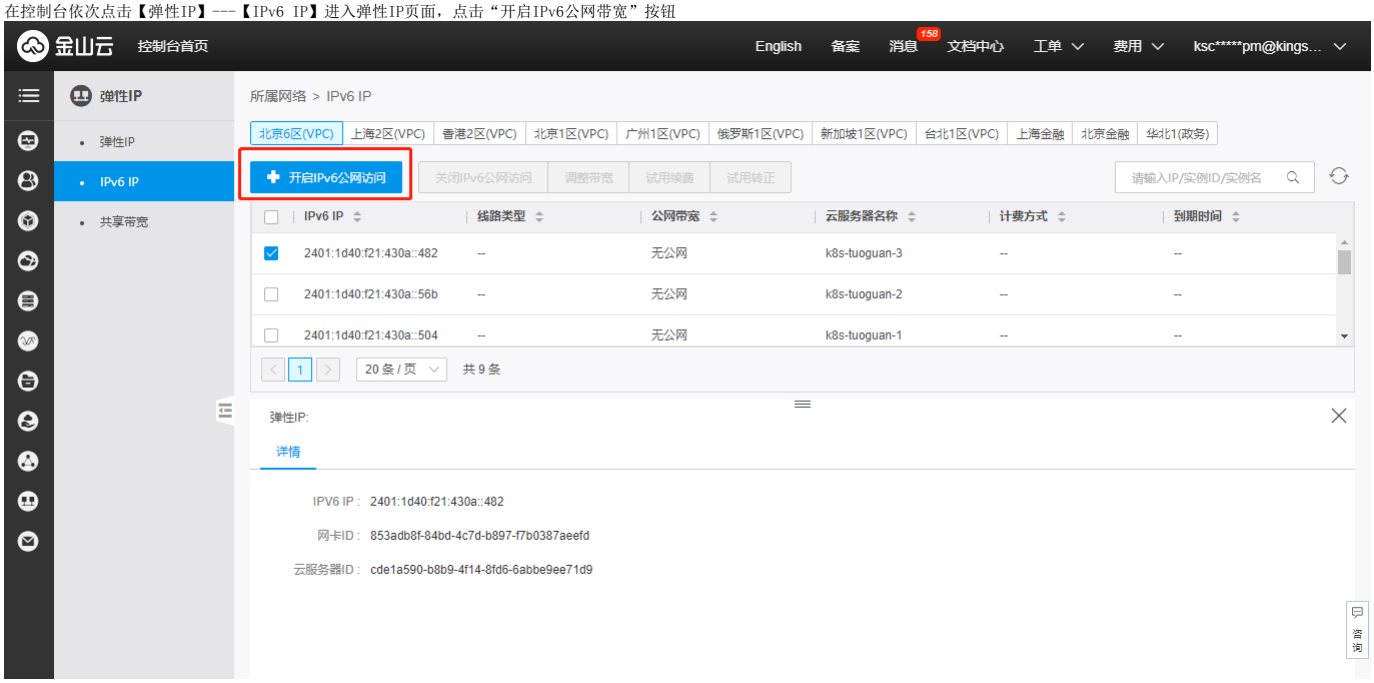
1. 在控制台依次点击【网络】---【虚拟私有网络】进入虚拟私有网络页面，为已有VPC点击“添加IPv6网段”按钮
2. 点击“确定”按钮。分配成功后会在VPC列表自动显示为该VPC分配的IPv6网段。

IPv6公网带宽

若您的云服务器支持IPv6，并且加入到IPv6的子网中，系统会为您的云服务器分配一个IPv6 IP地址，默认只具备VPC内IPv6内网通信权限。您需要为IPv6地址开通IPv6公网带宽，使IPv6地址可以进行公网通信。

操作步骤

1. 在控制台依次点击【弹性IP】---【IPv6 IP】进入弹性IP页面，点击“开启IPv6公网带宽”按钮



2. 选择计费方式和带宽值，然后单击立即购买完成支付。
3. 当某个IPv6地址不需要公网通信能力时，您可以“关闭IPv6公网访问”

VPN连接

产品简介

VPN 连接（VPN connections）是一种通过公网加密通道连接您的IDC和虚拟私有网络的方式

组成部分

VPN连接由三个部分组成：VPN网关、客户网关、VPN通道

VPN网关

VPN网关是虚拟私有网络建立VPN连接的出口网关，与客户网关（客户IDC侧的IPsecVPN服务网关）配合使用，主要用于金山云虚拟私有网络和金山云外IDC之间建立安全可靠的加密网络通信。金山云VPN网关采用双机热备策略，单台故障时自动切换，不影响业务正常运行。

VPN网关根据带宽上限分为5种设置，分别为：5M、10M、20M、50M、100M。您可以随时调整 VPN 网关带宽设置，即时生效。

客户网关

客户网关是指客户IDC机房的IPsecVPN服务网关，客户网关需与金山云VPN网关配合使用，一个VPN网关可与多个客户网关建立带有加密的VPN网络通道。

VPN通道

VPN网关和客户网关建立后，即可建立VPN通道，用于虚拟私有网络和金山云外IDC之间的加密通信。当前VPN通道支持 IPsec和GreOverIPsec加密协议，可满足绝大多数 VPN 连接的需求。

VPN 通道在运营商公网中运行，公网的网络阻塞、抖动会对VPN网络质量有影响，因此也无法提供 SLA 服务协议保障。如果业务对延时、抖动敏感，建议通过高速通道接入私有网络。

金山云上的 VPN 通道在实现 IPsec 中使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立会话。IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPSec 会话。

VPN通道的建立包括以下配置信息：

- 基本信息
- IKE配置（选填）
- IPsec配置（选填）

下面详细介绍基本信息、IKE 配置（选填）和 IPsec 配置（选填）。

基本信息

协议类型：Ipsec/GreOverIPsec 预共享秘钥：预共享密钥是用于验证IPSec连接的Unicode 字符串，金山云侧和客户侧必须使用相同的预共享密钥。

IKE配置

配置项	说明
版本	IKE V1
加密算法	身份加密算法，支持aes、3des、des共3种
认证算法	身份认证算法，支持md5和sha
DH分组	指定IKE交换密钥时使用的DH组，支持DHGroup1、DHGroup2、DHGroup5，密钥交换的安全性随着DH组的扩大而增加，但交换的时间也增加了

IPsec配置

配置项	说明
加密算法	身份加密算法，支持esp-3des、esp-aes、esp-des、esp-null、esp-seal共5种
认证算法	身份认证算法，支持esp-sha-hmac和esp-sha-hmac
生存周期(s)	单位：秒
生存周期(KB)	单位：KB

计费方式

VPN连接价格详情请联系金山云客服。

对等连接

产品简介

VPC 对等连接是一种用于跨VPC网络数据同步的互联服务，打通对等连接的两个VPC之间就像同一个VPC网络一样。您可以实现同地域或跨地域的相同/不同账号的VPC互联，通过在两端配置路由策略，可以实现不同VPC的流量互通。对等连接不依赖某个独立硬件，因而不存在单点故障或带宽瓶颈。

什么样的VPC之间可以创建对等连接

1. 对等连接的两个VPC网段不能重叠
2. 对等连接的隧道网关的对端网段不能和对端VPC的网段重叠

   例如有2个VPC，分别为A和B

   A中隧道网关的对端网段为A1和A2，B中隧道网关的对端网段为B1和B2

   - A与B的网段不能重叠
   - A与B1和B2的网段不能重叠
   - B与A1和A2的网段不能重叠

注：

- 对等连接的互通性不能传递，如有3个VPC分别为A、B和C，如果A与B，A与C分别建立对等连接，但是B与C的流量并不互通。
- 要使对等连接两端实现真正的通信，您必须在发起端和接收端的相关路由表上配置指向对端的路由规则。

同地域对等连接与跨地域对等连接

虚拟私有网络支持同地域和跨地域对等连接（即：虚拟私有网络跨地域互联），由于对等连接两端的物理距离不同，底层实现架构不一样，因此两者功能和计费上存在一些差异，对比如下：

比较项	同地域对等连接	跨地域对等连接
带宽	无带宽上限	支持1-200Mbps，以1Mbps为步长调整
计费规则	免费	支持包年包月的计费规则，阶梯收费
跨账号连接	支持	支持
访问权限	对等连接双方云服务器均可访问对端云服务器、数据库、负载均衡等全部资源	对等连接双方云服务器均可访问对端云服务器、数据库、负载均衡等全部资源
功能权限	对等连接两端 VPC 网段不可重复；一个 VPC 连接多个 VPC 时多个对端 VPC 网段也不可重复	对等连接两端 VPC 网段不可重复；一个 VPC 连接多个 VPC 时多个对端 VPC 网段也不可重复

- 同地域对等连接主要用于打通同地域处于不同虚拟私有网络中的应用。
- 跨地域的对等连接的典型应用场景是：跨地域容灾，跨地域互通连接不同地域的虚拟私有网络，快速部署两地三中心容灾方案，大带宽高可靠，满足金融级网络容灾需求。

对等连接计费方式

金山云同地域对等连接不收费，跨地域对等连接包年包月实行阶梯计费模式，以北京-上海为例，目前跨地域对等连接价格如下表所示：

地区	带宽	价格	单位
	1-10Mbps	480	元/月/Mbps
	10-20Mbps	240	元/月/Mbps
	20-50Mbps	180	元/月/Mbps
北京-上海	50-100Mbps	132	元/月/Mbps
	100-200Mbps	99	元/月/Mbps
	200-500Mbps	72	元/月/Mbps
	500-1000Mbps	52.2	元/月/Mbps

如上图所示，如购买北京到上海地区的对等连接，带宽为45Mbps，则一个月的费用为10*480+10*240+(45-10-10)*180=11,700元

注：如需购买其他地域对等连接，请联系金山云客服。

VPC安全性

金山云 VPC 提供两种安全功能，提高您 VPC 的安全性：

- 安全组是用作关联主机的防火墙，可在实例级别控制入站和出站的数据流。
- 网络访问控制列表 (ACL) 是关联子网的防火墙，在子网级别控制入站和出站数据流。

当您在 VPC 中启动主机时，可以指定关联一个安全组，如果您在启动实例时未指定安全组，实例会自动归属到 VPC 的默认安全组。在您的 VPC 中的每项实例都可能属于不同的安全组集合。

除了使用安全组之外，您还可以添加网络 ACL 以作为第二防御层。

您还可以在您的实例中配置额外的防火墙解决方案，进一步的提高主机安全性。

您还可以使用金山云IAM功能来管理您组织内部人员 创建，编辑安全组和网络ACL的权限。例如只有网络管理员可以有权限创建编辑安全策略，而其它人员只能使用主机。

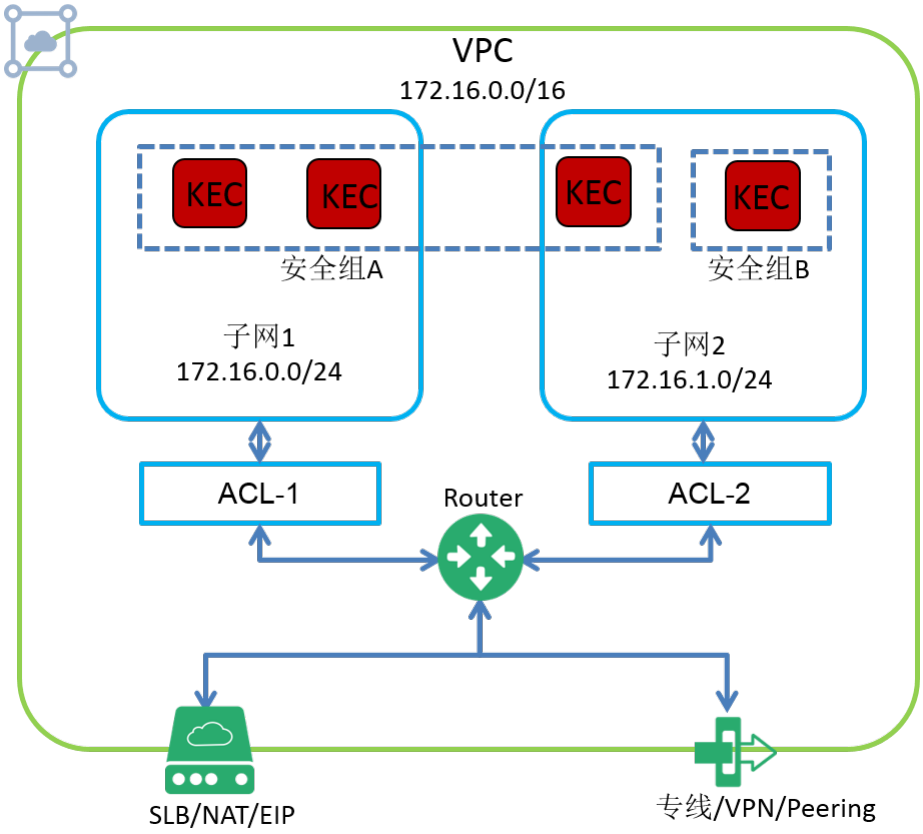
安全组与网络 ACL 的比较：

下表概述了安全组和网络 ACL 之间的基本差异。

安全组	网络ACL
在实例级别操作（第一防御层）	在子网级别操作（第二防御层）
仅支持允许规则	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

在决定是否允许数据流前评估所有规则 在决定是否允许数据流时按照数字顺序处理所有规则
只有在启动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 自动应用到关联子网内的所有实例（备份防御层，因此您便不需要依靠别人为您指定安全组）

下图展示了由安全组和网络 ACL 提供的安全层。例如，来自 Internet 网关的数据流会通过路由表中的路径被路由到合适的子网。与子网相关联的网络 ACL 规则控制允许进入子网的数据流。与实例相关的安全组规则控制允许进入实例的数据流。



安全组（防火墙）

安全组是什么？

安全组是一种有状态的服务器虚拟防火墙，它用于设置单台或多台云服务器的网络访问控制，是金山云提供的重要的网络安全隔离手段。

安全组是一个逻辑上的分组，可以将同一地域内具有相同网络安全隔离需求的云服务器实例加到同一个安全组内。您可以通过安全组策略对云服务器的出入流量进行安全过滤。

在您创建 KEC 实例时，可以将一个或多个安全组与该实例相关联。为安全组添加规则，规定流入或流出其关联的 KEC 实例的流量。

您可以随时修改安全组的规则；新规则立即生效，应用于与该安全组相关联的所有 KEC实例。

金山云在每个 VPC 地域均添加了一个默认安全组，默认安全组放行所有出 VPC 的流量，入流量默认拒绝。您可以根据需要修改安全组规则或创建新的安全组。

什么是多安全组？

多安全组是指一台云服务器的网卡在 VPC 环境下最多可以同时加入5个安全组，一台云物理主机的网卡在 VPC 环境下最多可以同时加入3个安全组，同时可以匹配加入的安全组规则，因为安全组规则都是放行（允许）规则，所以只要有一条规则匹配就会放行（允许通过）。

安全组的特性

安全组特性	云服务器	裸金属服务器
出站流量	默认允许所有流量	默认允许所有流量
入站流量(TCP/ICMP)	默认拒绝所有流量	默认拒绝所有流量
入站流量(IP/UDP)	默认拒绝所有流量	默认允许所有流量
配置白名单（允许流量）	是	是
配置黑名单（拒绝流量）	否	否
同安全组下的服务器	直接互通	直接互通
不同安全组下的服务器	默认不互通	默认不互通
同子网、不同安全组下的服务器	默认互通	裸金属服务器之间直接互通
服务器可关联安全组数量	5个	3个
服务器至少关联安全组数量	1个	1个
安全组规则是否是有状态的	是	是
安全组支持协议	IP（全部协议）、TCP、UDP、ICMP	IP（全部协议）、TCP、UDP、ICMP

裸金属服务器的安全组特殊限制

- 只对对南北向（裸金属服务器到其他服务）流量生效
- 东西向（裸金属服务器到裸金属服务器）同VPC且可用区内安全组不生效

注意：出站放行ip的时候，入站会放行udp。出站放行udp的时候，入站会放行udp。为了提高裸金属服务器的安全性，在创建关联云物理主机的安全组时，对于UDP协议建议用户配置访问外部的固定端口，对于IP协议，也不建议配置0.0.0.0/0出网规则。

入站：从服务器外到服务器内。出站：从服务器内到服务器外

有状态的安全规则，有状态是一种记忆功能，即一个包允许入站就允许出站，允许出站就允许入站

例如：云服务器A在安全组2里，规则（没入站规则，出站全部允许），云服务器B在安全组1里，规则（入站全部允许，出站全部允许）

结果：

- 云服务器A可以PING通云服务器B，因为A出站允许，所以可以出，因为安全组是有状态的，虽然没有入站规则，作为A出站的响应数据依然可以入
- 云服务器B无法PING通云服务器A

安全组规则

安全组规则可控制允许到达与安全组相关联的 KEC 实例的入站流量以及允许离开 KEC 实例的出站流量（从上到下依次筛选规则）。系统默认安全组放行所有出 VPC 流量，拒绝所有入 VPC 流量。 对于安全组的每条规则，您可以指定以下几项内容：

- 协议类型：例如 TCP、UDP 或 ICMP 等。
- 行为：默认为允许
- 端口：来源或目标的端口范围。
- 源IP（入站规则）或目标IP（出站规则）：单个 IP 地址或地址范围（用 CIDR 表示法）

常见的安全组规则类型

- 云服务器不受任何限制，可以被任意地址访问，配置如下入站规则和出站规则即可，但有一定的安全风险，建议按需配置安全组规则
- 云服务器指定端口可以被访问，配置指定端口和协议即可。例如：Linux服务器需要SSH，配置（TCP协议，22端口，0.0.0.0/0），建议普通用户使用此类规则
- 仅指定IP可以访问云服务器指定端口，配置指定端口和协议及源IP。例如：下图代表只有120.1.2.3这个IP可以访问云服务器的22端口，仅建议高级用户使用此类规则

云服务器和云物理主机在安全组有什么不同？

云物理主机的安全组和云服务器的安全组功能基本一致

- 在同一个子网的多台云物理主机之间不受安全组限制
- 在同一个子网的多台云服务器之间受安全组限制

操作指南

1、创建安全组

1）登录 金山云控制台，依次点击【网络】—【虚拟私有网络】—【安全组(防火墙)】，进入安全组信息页面

2）点击【新建安全组】，输入安全组名称，选择虚拟私有网络信息，默认情况选中【入站规则】，点击下方的【新增一行】

3）在新增的规则上，选择【协议】，填写【起始端口】【结束端口】【源IP】【备注】信息

4）重复步骤3）可以创建多条入站规则或出站规则，创建完成后，点击【确定】

5）提示“创建成功”的提示框，代表安全组创建成功

2、编辑（增加、修改、删除）入站规则/出站规则

1）登录 金山云控制台，依次点击【网络】—【虚拟私有网络】—【安全组(防火墙)】

2）选中需要编辑的安全组，点击上方的【编辑入站规则】 或者在下方选项卡选择【入站规则】—【编辑入站规则】，进入入站规则编辑页面

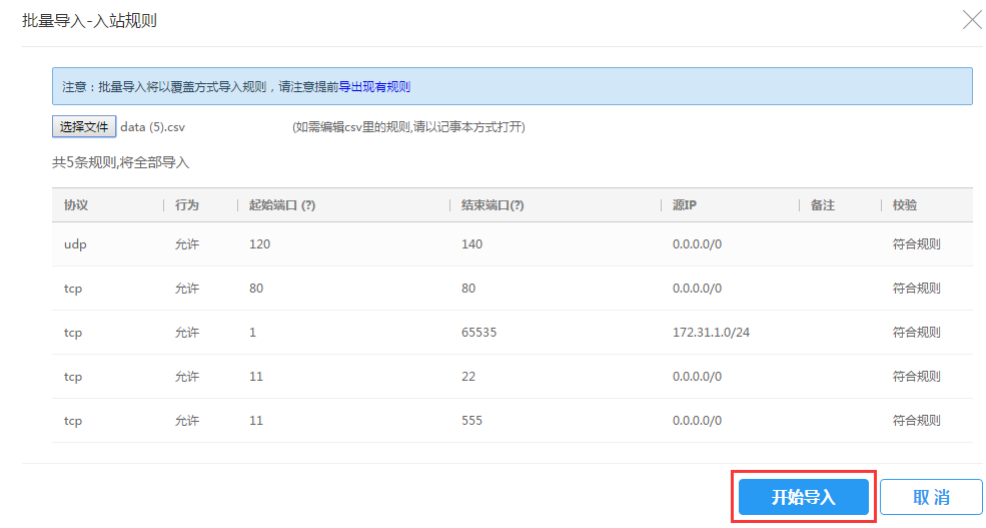
3）在入站规则编辑页面，可以对已有入站规则修改和删除，也可以新增入站规则。入站规则页面支持【批量导入】和【导出规则】

4）点击【批量导入】，跳转到批量导入页面，点击【选择文件】按钮，导入入站规则

导入文件格式如下所示：

```
协议,行为,起始端口,结束端口,源IP,备注
udp,允许,120,140,0.0.0.0/0,
tcp,允许,80,80,0.0.0.0/0,
tcp,允许,1,65535,172.31.1.0/24,
tcp,允许,11,22,0.0.0.0/0,
tcp,允许,11,555,0.0.0.0/0,
```

5) 批量导入入站规则后，在页面下方查看全部入站规则，点击【开始导入】，然后可以在入站规则页面查看批量导入的入站规则信息。



注： 1、批量导入将以覆盖方式导入规则，请注意提前导出现有规则； 2、支持CSV格式的导入，为了保证导入文件格式符合要求，目前建议先导出规则，然后用记事本打开编辑所需的规则信息，若采用其他方式打开或编辑文件会导致文件格式不符合要求。

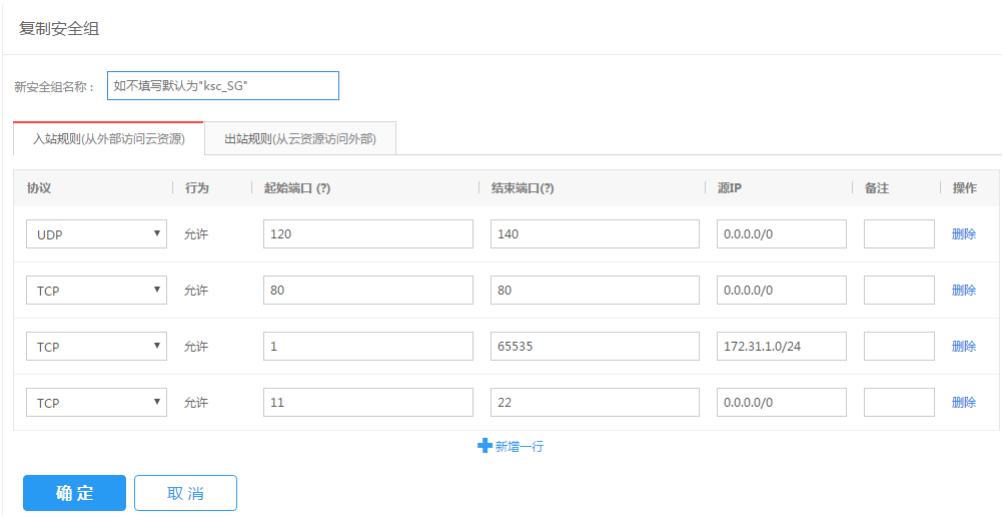
6) 点击【导出规则】，将批量导出现有的所有入站规则信息，导出格式为CSV，如需编辑，请用记事本方式打开编辑并保存。 **注：** 编辑出站规则与入站规则操作类似，不再赘述

3、复制安全组

1) 登录 金山云控制台，依次点击【网络】--【虚拟私有网络】--【安全组(防火墙)】

2) 选中需要复制的安全组，点击【复制安全组】按钮

3) 在弹出的复制安全组页面，输入新的安全组名称，下方默认展示复制安全组的入站/出站规则信息，可以编辑（增加、修改、删除）现有的规则信息，编辑完成后，点击【确定】



4) 跳出“复制成功”的提示框，代表安全组复制成功，可以在安全组页面查看复制的安全组信息

4、删除安全组

1) 登录 金山云控制台，依次点击【网络】--【虚拟私有网络】--【安全组(防火墙)】

2) 选中需要删除的安全组，并点击【删除】按钮

3) 在删除确认页面，点击【删除】

4)跳出“删除成功”的提示框，代表安全组成功删除

注：VPC中默认安全组不能删除，安全组中还有关联云服务器或者裸金属服务器时不能删除。

5、管理云服务器

1)登录 金山云控制台，依次点击【网络】--【虚拟私有网络】--【安全组(防火墙)】

2)选择需管理云服务器的安全组,点击上方的【管理云服务器】，或点击下方【云服务器信息】--【管理云服务器】，进入管理云服务器页面。

3)在管理云服务器页面，左下方展示未加入此安全组的网卡，右下方展示已加入此安全组的网卡，点击【添加】或【移动】来管理此安全组下的云服务器，然后点击【确定】

4)跳出“操作成功”的提示框，代表操作成功

6、管理裸金属服务器

1)登录 金山云控制台，依次点击【网络】--【虚拟私有网络】--【安全组(防火墙)】

2)选择需管理云物理主机的安全组,点击上方的【管理云物理主机】，或点击下方【裸金属服务器信息】--【管理裸金属服务器】，进入管理裸金属服务器页面。

3)在管理裸金属服务器页面，左下方展示未加入此安全组的网卡，右下方展示已加入此安全组的网卡，点击【添加】或【移动】来管理此安全组下的云物理主机，然后点击【确定】

4)跳出“操作成功”的提示框，代表操作成功

网络ACL

1. 网络 ACL 概述
2. 网络 ACL 基本信息
3. 网络 ACL 规则
4. 使用场景
5. 自定义网络 ACL 示例
6. 临时端口
7. 安全组与网络ACL的区别
8. 操作指南

网络 ACL 概述

网络访问控制列表 (Access Control List，ACL)是一个子网级别无状态的可选安全层，可以精确到协议和端口粒度，可作为防火墙，以控制进出子网的数据流。您可以设置网络 ACL，使其规则与您的安全组相似，以便为您的 VPC 添加额外安全层。 ACL 无状态的特性，即使设置入站规则允许某些访问，如果没有设置相应的出站规则也会导致无法响应访问。

网络 ACL 基本信息

以下是您需要了解的有关网络 ACL 的基本信息:

- 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 是规则的编号列表，以供我们按顺序评估（从编号最小的规则开始，编号越小优先级越高）以判断数据流是否被允许进入或离开任何与网络 ACL 关联的子网。您可以使用的最高规则编号为 32766。我们建议您从创建规则编号为 100 的倍数的规则开始，以使您可以在稍后需要时插入新的规则。
- 同一个方向的ACL规则编号不允许重复。
- 网络 ACL 有单独的入站和出站规则，每项规则是允许或是拒绝数据流。
- 您可以创建自定义网络 ACL；每个自定义网络 ACL默认出入都放行，直至您添加规则为止。
- 网络 ACL 没有任何状态即您需要分别对请求和响应数据流设置规则。
- 同一个子网内的主机不受关联的ACL策略控制。
- 金山云公共服务网段需要放行，否则将无法正常使用SLB、yum源、NTP、DNS、服务器安全客户端等服务。公共服务网段如下：
  198.18.0.0/15，100.64.0.0/10，11.0.0.0/8，33.0.0.0/8，120.92.212.184。

网络 ACL 规则

您可以创建新的网络ACL规则，并绑定到指定子网。当您在网络 ACL 中添加或删除规则时，更改也会自动应用到与其绑定的子网。

网络 ACL 规则有如下部分组成：

- 优先级：即规则编号，规则评估从编号最低的规则开始。优先级数值越小，优先级越高，只要有一条规则与流量匹配，即应用该规则，并忽略与之冲突的任意更高编号的规则。
- 支持的协议：IP、UDP、TCP、ICMP
- 行为：允许或者拒绝
- 源数据（入站）或目标数据（出站）：对于TCP，UDP，为源数据或目标数据的IP或者IP范围（用CIDR表示），对于ICMP协议为 icmp_type 和 icmp_code。

使用场景

用户可以为具有相同网络流量控制的子网绑定同一个网络 ACL，通过设置出站和入站允许/拒绝规则，对进出子网的流量进行精确控制。例如，您在金山云私有网关内托管多层 Web 应用，创建了不同子网分别部署 Web 层、逻辑层和数据层服务，通过网络 ACL 您可以控制这三个子网之间的访问：Web 层子网和数据库层子网无法相互访问，只有逻辑层可以访问 Web 层和数据层子网。

自定义网络 ACL 示例

下表展示了一个自定义网络 ACL 示例。其中包括允许 HTTP 和 HTTPS 数据流进入的规则（入站规则 100 和 110）。相应的出站规则，以允许响应入站数据流（出站规则 120，适用于临时端口 49152-65535），网络 ACL 还包括允许 SSH 和 RDP 数据流进入子网的入站规则。出站规则 120 允许离开子网的响应。 网络 ACL 出站规则（100 和 110）允许离开子网的 HTTP 和 HTTPS 数据流。存在相应的入站规则，以允许响应出站数据流（入站规则 140，适用于临时端口 49152-65535）。

入站规则

优先级	源IP	协议	端口范围	允许/拒绝	备注
100	0.0.0.0/0	TCP	80	允许	允许来自任何地方的入站 HTTP 数据流
110	0.0.0.0/0	TCP	443	允许	允许来自任何地方的入站 HTTP 数据流
120	192.0.2.0/24	TCP	49152-65535	允许	允许来自您的办公网络的公有 IP 地址范围内的入站 SSH 数据流（通过 Internet 网关）。
140	0.0.0.0/0	TCP	49152-65535	允许	允许从源于子网的请求返回的入站数据流
150	0.0.0.0/0	UDP	49152-65535	允许	允许从源于子网的请求返回的入站数据流
32766	0.0.0.0/0	IP	IP	拒绝	拒绝所有尚未经前置规则（不可修改）处理的入站数据流。

出站规则

优先级	目标IP	协议	端口范围	允许/拒绝	备注
100	0.0.0.0/0	TCP	80	允许	允许从子网到 Internet 的出站 HTTP 数据流。
110	0.0.0.0/0	TCP	443	允许	允许从子网到 Internet 的出站 HTTPS 数据流。
120	192.0.2.0/24	TCP	1024-65535	允许	允许对 Internet 客户端进行出站响应（例如，向访问子网中 Web 服务器的人员开放网页）。
32766	0.0.0.0/0	IP	IP	拒绝	拒绝所有尚未经前置规则（不可修改）处理的出站数据流。

随着数据包流向子网，我们会根据与子网关联的 ACL 的进入规则评估数据包（从规则列表的顶端开始向下移动）。 信息包被指定发往 SSL 端口 (443)。数据包不匹配第一项评估规则（规则 100）。它匹配第二条规则 (110)，即允许数据包进入子网。如果数据包的目的地已经指定为端口 139 (NetBIOS)，则最初两项规则可能无法匹配，但是“*”规则最终可能会拒绝这个数据包。 在您需要开放一系列端口、同时在此部分端口内您想拒绝部分数据，您需要添加一项拒绝规则，并确保将拒绝规则的优先级设置为大于放开一系列端口规则的优先级，即拒绝规则的优先级数值小于放开一系列端口的数值。

临时端口

临时端口是客户端发起请求时配置的端口，设置网络 ACL 出站规则时需注意这点。由于网络 ACL 无状态的特性，即使设置入站规则允许某些访问，如果没有设置相应的出站规则会导致无法响应访问。

某客户端向 VPC 内某子网中主机发起请求，该子网关联了网络 ACL。客户端默认配置的端口属于临时端口范围。如果网络 ACL 出站规则中没有设置允许对应临时端口的流量，那么客户端的请求将无法返回。根据客户端的操作系统不同，临时端口范围也随之不同。

- 许多 Linux 内核（包括 KSC Linux 内核）使用端口 32768-61000，生成自 Sever Load Balancing 的请求使用端口 1024-65535
- Windows Server 2003 使用端口 1025-5000
- Windows Server 2008 使用端口 49152-65535

实际上，为涵盖不同客户端类型可能进入到您 VPC 中的公有实例的数据流，您需要开放临时端口 1024-65535。但是，您也可以在 ACL 中添加规则以拒绝任何在此范围内的来自恶意端口的数据流。您只需确保拒绝规则的优先级大于允许一系列临时端口数据流的规则。

安全组与网络ACL的区别

安全组	网络ACL
云服务器实例级别的流量控制（第一层防御）	子网级别的流量控制（第二层防御）
只支持允许规则	支持允许与拒绝规则
对VPC内的云服务器， 出站流量默认允许，入站流量拒绝，直至添加规则为止	每个自定义网络 ACL 默认出入都放行，直至添加规则为止。
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
在决定是否允许数据流前评估所有规则	在决定是否允许数据流时按照数字顺序处理所有规则
只有在启动 KEC 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	自动应用到关联子网内的所有 KEC 实例（备份防御层，因此您便不需要依靠别人为您指定安全组）

操作指南

创建网络 ACL

1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入 ACL 页面。

2）点击【新建】按钮，在新建 ACL 页面中输入名称、选择所属的私有网络，点击确定完成。

查看网络 ACL 列表

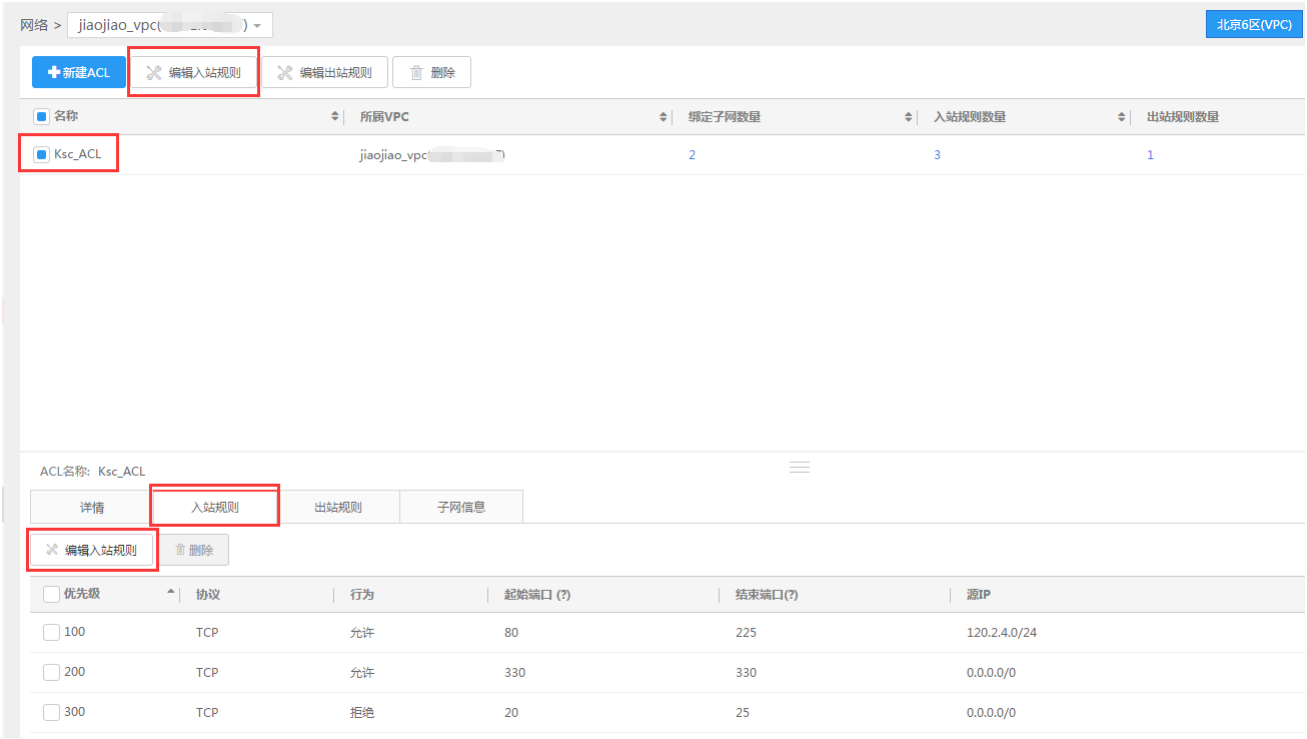
1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2）在顶部选择地域及虚拟私有网络，即可查看属于此私有网络的网络 ACL 列表。

编辑网络 ACL 入站规则

1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2）在列表中选中要编辑的网络 ACL 的 名称，点击上方的【编辑入站规则】按钮或者点击下方【入站规则】选项卡，然后点击【编辑入站规则】按钮，进入入站规则页面。

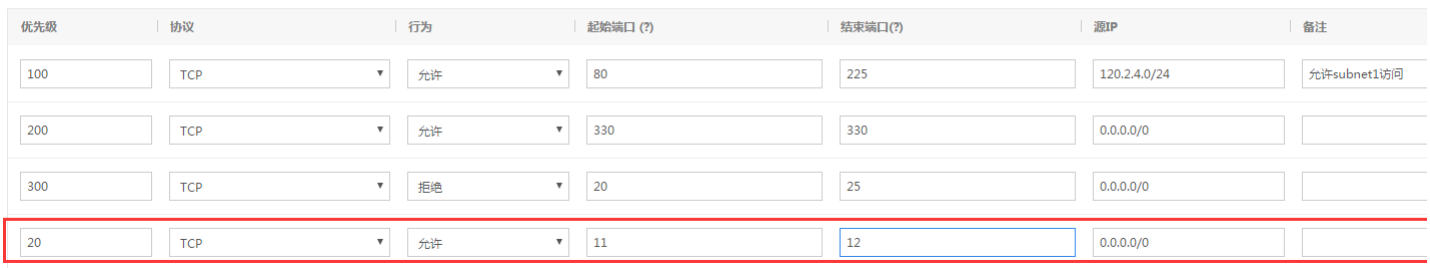


3) 可以编辑已有的入站规则，也可以点击下方的【新增一行】按钮添加新的入站规则。

编辑ACL入站规则(Ksc_ACL)

4) 输入新增入站协议的优先级、协议、行为、端口范围、源IP，点击【确定】按钮，提示“编辑ACL入站规则成功”，跳回 ACL 页面。

编辑ACL入站规则(Ksc_ACL)



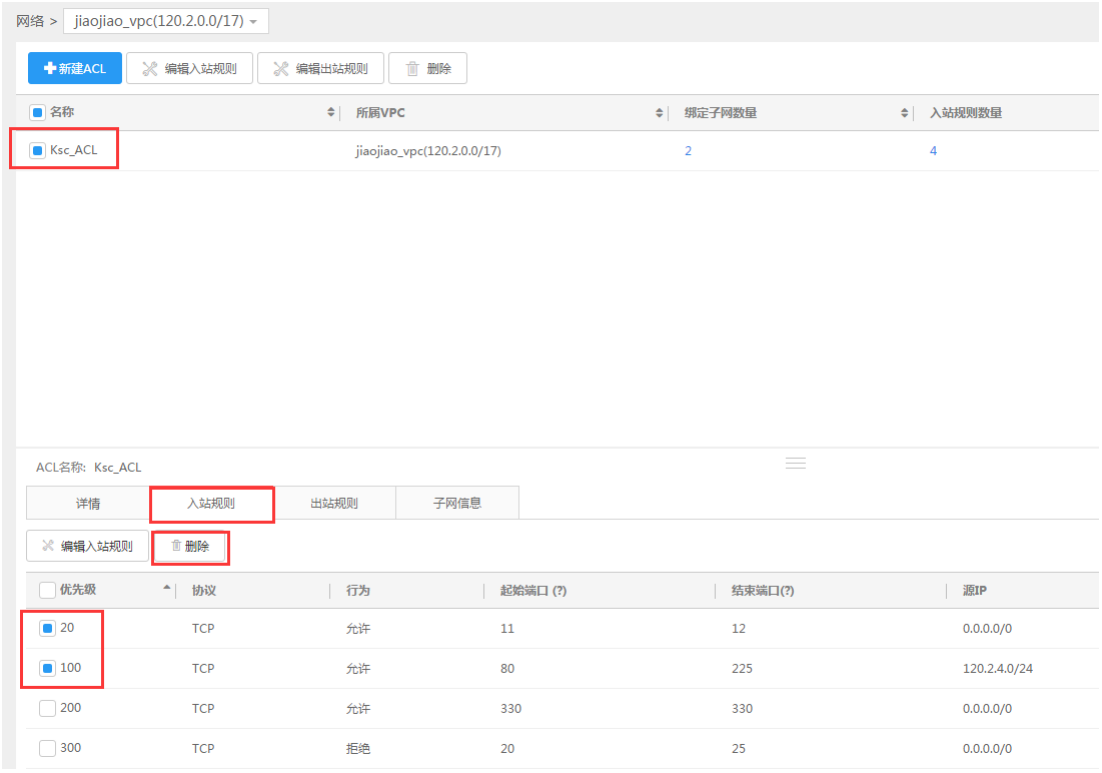
5) 新增的规则根据设置的优先级进行排序，优先级越高（数值越小）越靠前，如下图所示

注：出站规则的编辑方式与入站规则类似，只是在编辑出站协议时，源IP改变为目的IP。

删除网络 ACL 入站规则

1) 登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2) 在列表中选中要删除入站规则的网络 ACL 的 名称，点击下方【入站规则】选项卡，在下方显示的入站规则列表中，选中需要删除的入站规则，点击上方的【删除】按钮



3）在跳出的删除确认页面，点击【删除】 。

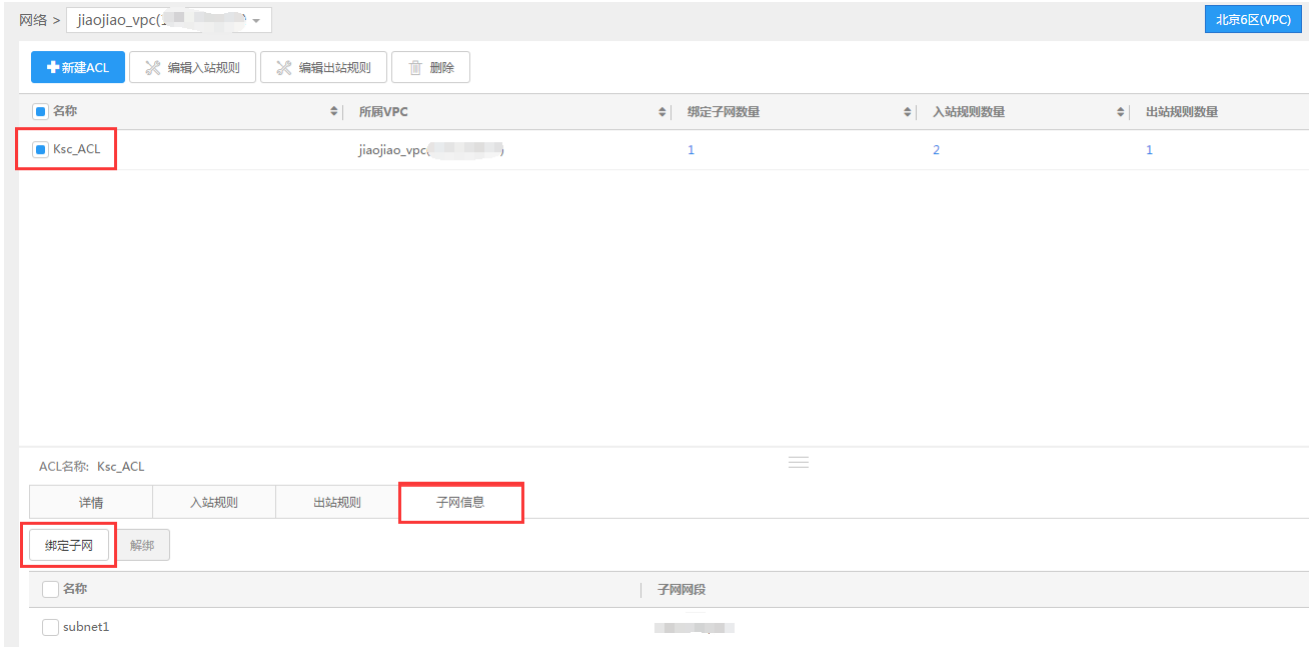
4）看到删除成功的提示，表示删除成功

注：删除出站规则与删除入站规则操作类似，只需在步骤2）改为选择 【出站规则】 选项卡即可。

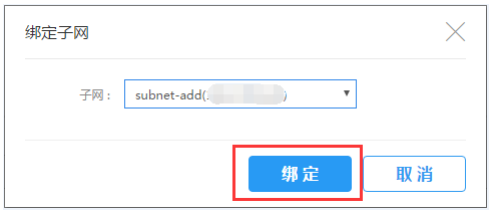
子网绑定网络 ACL

1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2）选中需要绑定子网的 ACL 的 名称，在下方的页面选择【子网信息】选项，下方展示该 ACL 已绑定的子网信息，点击【绑定子网】按钮，进入绑定子网页面。



3）在跳出的绑定子网页面，选择需要绑定的子网（名称和网段），点击【绑定】按钮。



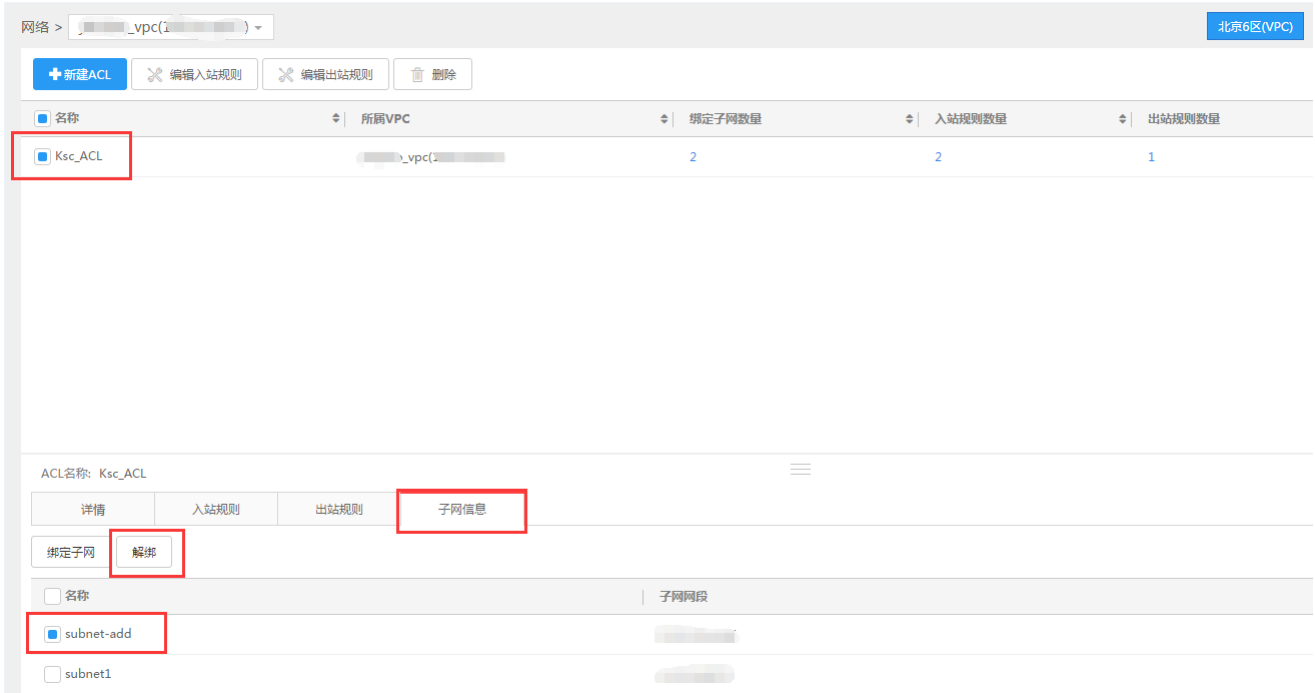
4）跳出“绑定成功”的提示框，代表绑定子网成功

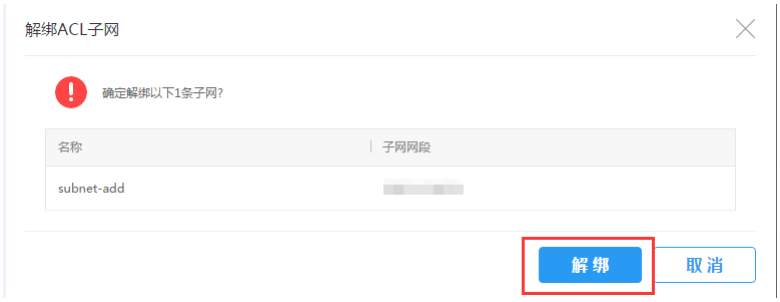
注：一个子网只能绑定一个 ACL ，一个 ACL 可以绑定多个子网。

子网解绑网络 ACL

1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2）选中需要解绑子网的 ACL 的 名称，在下方的页面选择【子网信息】选项，下方展示该 ACL 已绑定的子网信息，选中需要解绑的子网，点击【解绑】按钮





3）在跳出的解绑子网确认页面，点击【解绑】按钮。

4）跳出“绑定成功”的提示框，代表解绑子网成功

删除网络 ACL

1）登录 金山云控制台 依次点击【网络】--【虚拟私有网络】--【ACL】，进入ACL页面。

2）选中需要删除的 ACL 的 名称，点击上方的【删除】按钮

3）在跳出的删除确认页面，点击【删除】按钮。

4）跳出“删除成功”的提示框，代表删除成功

注：在删除网络 ACL 前，需要先解绑与 ACL 绑定的子网，否则系统会提示“请先解绑ACL关联的子网，再删除ACL”的信息。

路由

简介

路由是由一系列路由规则组成，用于控制虚拟私有网络（VPC）内子网的出流量走向。金山云上的路由有两种类型：默认路由规则和自定义路由规则。

路由是由一系列路由规则组成，路由规则包括路由目标网段、下一跳类型和下一跳组成，下一跳的类型可以是互联网网关、主机路由、VPN通道和对等连接等。

默认路由规则

用户创建虚拟私有网络时，默认需要创建一个普通子网和一个终端子网，系统会自动为其生成默认路由规则。在路由页面，选中对应的虚拟私有网络，可以添加或删除路由规则，但无法删除系统默认路由规则。在子网选项下创建新子网，系统也会自动将新子网路由信息添加到对应的路由中。

自定义路由规则

除了默认路由规则之外，还可以在 VPC 中创建自定义路由规则，自定义路由规则可以被删除。

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四个参数：

- 目标网段：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：192.168.115.91/32）。
- 所属 VPC：指示该路由规则所在的 VPC 的名称和网段信息。
- 类型：私有网络的数据包出口。私有网络下一跳类型支持“互联网网关”、“本地子网”、“对等连接”等类型。
- 下一跳：指定具体跳转至哪个下一跳实例，使用下一跳名称标识。

路由规则优先级

当路由中存在多条路由规则时，路由优先级由高至低分别为：

- 虚拟私有网络内流量：虚拟私有网络内流量最优先匹配
- 最精确路由：虚拟私有网络外流量根据最精确路由规则匹配
- 公网IP：路由规则均匹配失效时，通过公网 IP 对 Internet 进行外访

操作指南

创建自定义路由规则

除了系统自动生成的默认路由规则，用户还可以自定义新的路由规则。

1）登录 金山云控制台 依次点击【网络】-【虚拟私有网络】-【路由】，进入路由列表页面。 2）点击列表上方【新建】按钮，在新建路由弹出框中选择所属虚拟私有网络，目标网段、下一跳的类型以及对应的实例 3）点击【新建】按钮，即可在路由列表中看到您新建的路由规则。

删除自定义路由规则

系统自动生成的默认路由规则无法删除，自定义路由规则可以任意创建和删除。

1）登录 金山云控制台 依次点击【网络】-【虚拟私有网络】-【路由】，进入路由列表页面。 2）选中要删除的路由规则，点击上方的【删除】。 3）在删除路由的确认弹窗中的点击【删除】即可删除所选的自定义路由规则。