

专有网络 VPC

用户指南

用户指南

产品简介

产品简介

专有网络VPC (Virtual Private Cloud)，帮助用户基于阿里云构建出一个隔离的网络环境。您可以完全掌控自己的虚拟网络，包括选择自有IP地址范围、划分网段、配置路由表和网关等。此外您也可以通过专线/VPN等连接方式将VPC与传统数据中心组成一个按需定制的网络环境，实现应用的平滑迁移上云。

专有网络与经典网络的区别

- 经典网络类型的云产品，统一部署在阿里云的公共基础网络内，网络的规划和管理由阿里云负责，更适合对网络易用性要求比较高的客户。
- 专有网络，是指用户在阿里云的基础网络内建立一个可以自定义的专有隔离网络，用户可以自定义这个专有网络的网络拓扑和IP地址，与经典网络相比，专有网络比较适合有网络管理能力和需求的客户。

专有网络开放使用的地域

亚太 (新加坡)、华南 1 (深圳)、华北 2 (北京)、华东 2 (上海)、美东 (弗吉尼亚)、香港、华东 1 (杭州)、美西 (硅谷)

具体有哪些地域以实际的控制台为准。

产品对比

功能点	经典网络	专有网络
二层逻辑隔离	不支持	支持
自定义私网网段	不支持用户自定义	用户自定义
私网IP规划	经典网络内唯一	专有网络内唯一，专有网络间可重复
自建VPN	不支持	支持
私网互通	账号内相同地域内互通	专有网络内互通，专有网络间隔离

自建Nat网关	不支持	支持
---------	-----	----

产品名词解释

名词	英文	说明
专有网络	VPC	专有网络是用户基于阿里云创建的自定义私有网络, 不同的专有网络之间彻底逻辑隔离, 用户可以在自己创建的专有网络内创建和管理云产品实例, 比如ECS, Intranet SLB, RDS等。
路由器	VRouter	路由器, 是VPC网络的枢纽, 它可以连接VPC内的各个交换机, 同时也是连接VPC与其他网络的网关设备。它会根据具体的路由条目的设置来转发网络流量。
交换机	VSwitch	交换机, 是组成VPC网络的基础网络设备。它可以连接不同的云产品实例。在VPC网络内创建云产品实例的时候, 必须指定云产品实例所在的交换机。
路由表	Route Table	路由表, 是指路由器上管理路由条目的列表。
路由条目	Route Entry	路由表中的每一项成为一条路由条目, 路由条目定义了通向指定目标网段的网络流量的下一跳地址, 路由条目包括系统路由和自定义路由两种类型。

专有网络

专有网络是用户基于阿里云创建的自定义私有网络, 不同的专有网络之间彻底逻辑隔离, 用户可以在自己创建的专有网络内创建和管理云产品实例, 比如ECS, Intranet SLB, RDS等。

专有网络管理：

- 在创建专有网络时, 用户需要以CIDRBlock的形式指定专有网络内使用的私网网段
- 专有网络创建之后, 用户需要继续创建交换机(VSwitch), 然后才能够在专有网络内创建云产品实例(ECS, SLB, RDS)
- 创建专有网络时, 需要指定CIDRBlock。当新建VPC实例的状态变成Available之后, 表示VPC创建成功, 可以进行下一步的管理操作
- 删除指定的专有网络, 必须首先删除专有网络内所有的云产品实例(包含安全组, 交换机, 云产品实例, 路由条目等)

专有网络网段：

- 关于CIDRBlock的相关信息，请参见维基百科上的Classless Inter-Domain Routing条目说明
- 专有网络创建成功之后，CIDRBlock无法修改，建议使用比较大的网段作为VPC的CIDRBlock(比如直接使用192.168.0.0/16和172.16.0.0/12以及10.0.0.0/8 3个网段)，尽量避免后续扩容。系统不会根据VPC的CIDRBlock来创建系统路由，所以使用比较大的地址范围来创建VPC，不会影响业务的正常使用

路由器

路由器，是VPC网络的枢纽，它可以连接VPC内的各个交换机，同时也是连接VPC与其他网络的网关设备。它会根据具体的路由条目的设置来转发网络流量。

产品约束：

- 每个VPC有且只有一个路由器
- 路由器不支持BGP和OSPF等动态路由协议

路由器管理：

- 创建VPC时，系统会自动为每个VPC创建1个路由器
- 删除VPC时，也会自动删除对应的路由器
- 不支持直接创建和删除路由器

交换机

交换机，是组成VPC网络的基础网络设备。它可以连接不同的云产品实例。在VPC网络内创建云产品实例的时候，必须指定云产品实例所在的交换机。

产品约束：

- 具体的产品约束，请参见VPC产品约束
- VPC的交换机，是一个3层交换机，不支持2层广播和组播

交换机管理：

- 只有当VPC的状态为Available时，才能创建新的交换机
- 交换机不支持并行创建，一个交换机创建成功之后，才能够创建下一个
- 交换机创建完成之后，无法修改CIDRBlock
- 删除交换机之前，必须先删除目标交换机所连接的云产品实例

交换机网段：

- 创建交换机时，需要指定一个CIDRBlock
- 新建交换机所使用的CIDRBlock必须从属于交换机所在的VPC的CIDRBlock
- 新建交换机所使用的CIDRBlock不能与已经存在的交换机的CIDRBlock冲突
- 新建交换机所使用的CIDRBlock不能包含已经存在的自定义路由的目标网段

路由表

路由表，是指路由器上管理路由条目的列表。

产品约束：

- 每个路由器有且只有1个路由表
- 路由表的路由条目会影响VPC中的所有云产品实例。目前不支持指定交换机和云产品实例的源地址策略路由。

路由表管理：

- 新建VPC时，系统会自动创建1个路由表
- 删除VPC时，系统会自动删除对应的路由表
- 不支持直接创建和删除路由表

路由条目

路由表中的每一项成为一条路由条目，路由条目定义了通向指定目标网段的网络流量的下一跳地址，路由条目包括系统路由和自定义路由两种类型。

- 路由器只支持静态路由，不支持ECMP等价路由

路由条目管理：

- 专有网络创建时，会自动创建1条系统路由，用于专有网络内的云产品实例访问专有网络外的云服务。
- 创建交换机，系统也会创建1条对应的系统路由
- 用户可以创建和删除自定义路由条目
- 系统路由条目由系统自动管理，用户无法创建和删除

产品优势

安全隔离

- 使用隧道技术,达到与传统VLAN方式相同的隔离效果
- 广播域隔离在网卡级别

访问控制

- 灵活的访问控制规则
- 满足政务，金融的安全隔离规范

软件定义网络

- 按需配置网络设置，软件定义网络
- 管理操作实时生效

丰富的网络连接方式

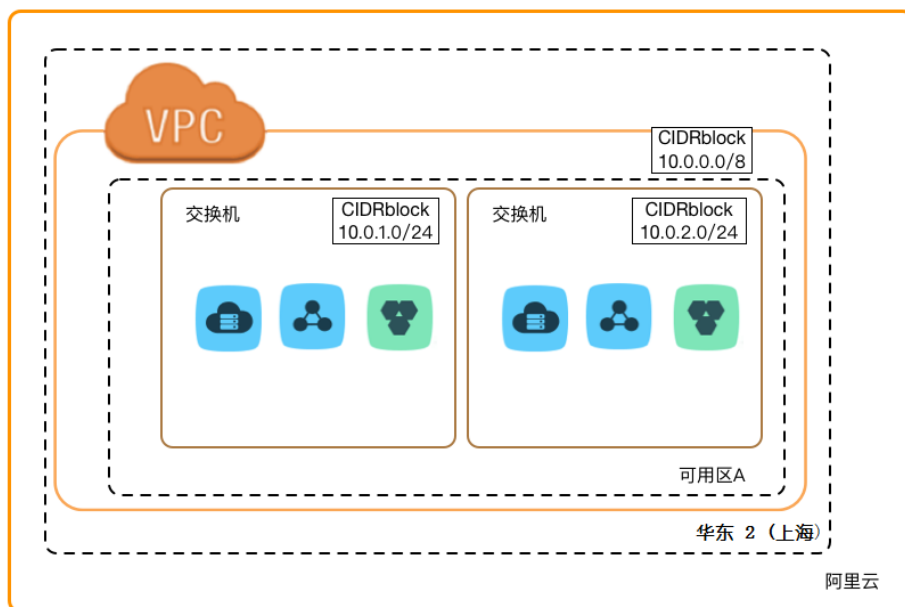
- 支持软件VPN
- 支持专线连接

使用场景

专有网络可以构建出一个隔离的网络环境。在这个网络中可以完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。此外您也可以通过专线/VPN等连接方式将VPC与传统数据中心组成一个按需定制的网络环境，实现应用的平滑迁移上云。

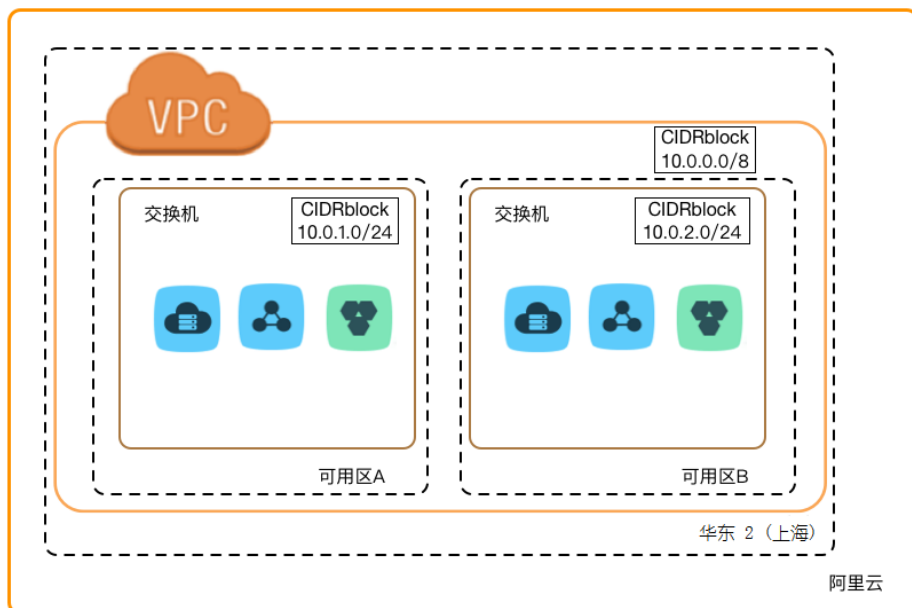
场景一：在阿里云上管理用户专属的网络

首先按照网络规划创建专有网络、交换机，并在该专有网络中创建云产品实例（如ECS、RDS、SLB、OCS等）并使用。



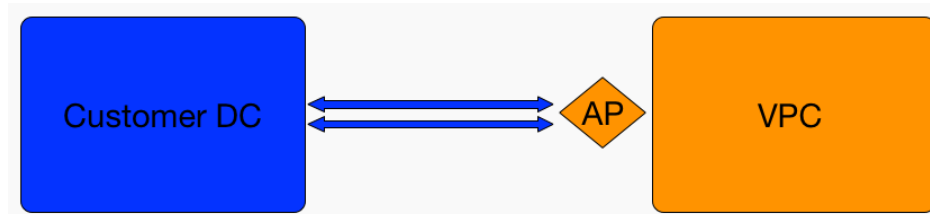
场景二：VPC中跨可用区部署资源

用户可以通过将资源部署在处于不同可用区的交换机中，从而实现利用阿里云可用区进行容灾。



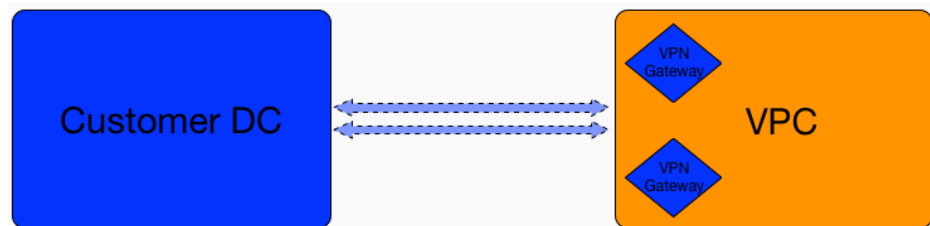
场景三：物理专线接入

通过物理专线将自有数据中心和阿里云VPC连接起来，实现用户网络与阿里云专有网络之间的内网互通，支持2条线路通过链路汇聚方式实现主备或双活。



场景四：VPN接入

在VPC内使用ECS自建VPN网关，实现用户网络与阿里云专有网络之间的内网互通，具体内容可以参考《VPN》。



技术原理

背景信息

随着云计算的不断发展，对虚拟化网络的要求越来越高，弹性(scalability)、安全(security)、可靠(resilience)、私密(privacy)，并且还要求极高的互联性能(performance)，因此催生了多种多样的网络虚拟化技术。

比较早的解决方案，是将虚拟机的网络和物理网络融合在一起，形成一个扁平的网络架构，例如大二层网络。这种类似的方案，随着虚拟化网络规模的增大，ARP欺骗、广播风暴、主机扫描等问题会越来越严重。为了解决这些问题，出现了各种网络隔离技术，把物理网络和虚拟网络彻底隔开。其中一种技术是用户之间用VLAN进行隔离，但是VLAN的数量最大只能支持到4096个，无法支撑公有云的巨大用户量。

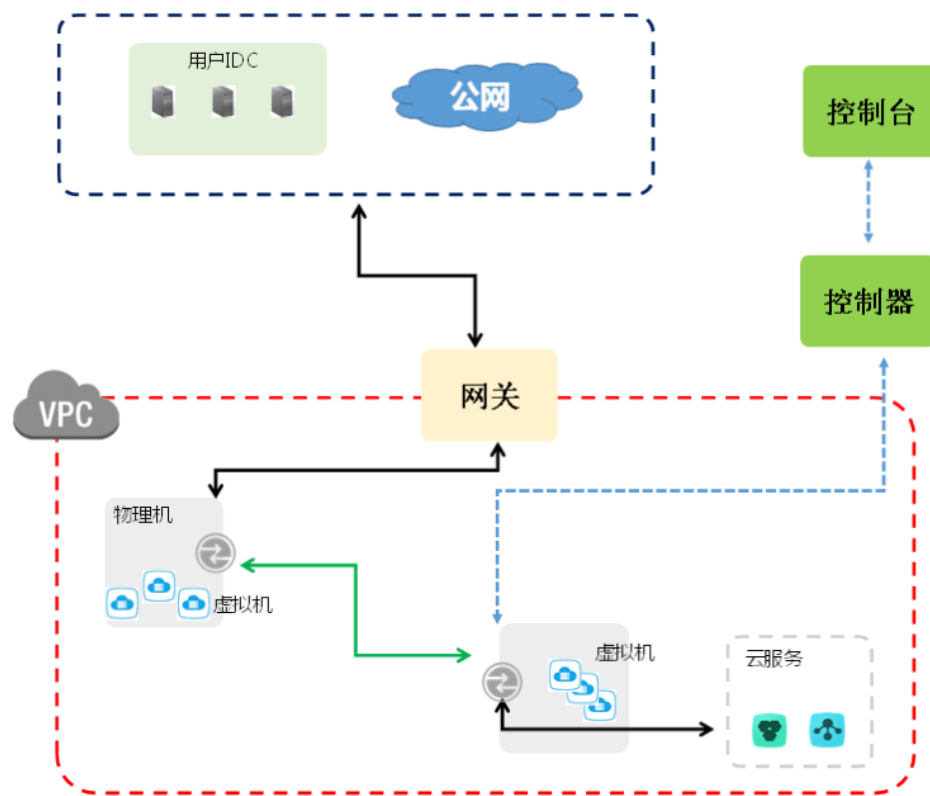
原理描述

基于目前主流的隧道技术，专有网络（Virtual Private Cloud，简称VPC）隔离了虚拟网络。每个VPC都有一个独立的隧道号，一个隧道号对应着一张虚拟化网络。一个VPC内的ECS之间的传输数据包都会加上隧道封装，带有唯一的隧道ID标识，然后送到物理网络上进行传输。不同VPC内的ECS因为所在的隧道ID不同，本身处于两个不同的路由平面，从而使得两个不同的隧道无法进行通信，天然的进行了隔离。

基于隧道技术，阿里云的研发团队自研了交换机，软件自定义网络（Software Defined Network，简称SDN）技术和硬件网关，在此基础上实现了VPC产品。

逻辑架构

图 1 VPC整体架构



如上图所示，在VPC架构里面包含交换机、网关和控制器三个重要的组件。

- 交换机和网关组成了数据通路的关键路径，控制器使用自研的协议下发转发表到网关和交换机，完成了配置通路的关键路径，整体架构里面，配置通路和数据通路互相分离。
- 交换机是分布式的结点，网关和控制器都有集群部署并且是多机房互备的，所有链路上都有冗余容灾，提升了VPC产品的整体可用性。
- 交换机和网关性能在业界都是领先的，自研的SDN协议和控制器，能轻松管控公有云成千上万张虚拟网络。

在产品上，除了给用户一张独立的虚拟化网络，阿里云还为每个VPC提供了独立的路由器、交换机组件，让用户可以更加丰富的进行组网。针对有内网安全需求的用户，还可以使用安全组技术在一个VPC进行更加细粒度的访问控制和隔离。缺省情况下，VPC内的ECS只能和本VPC内其他ECS通信，或者和VPC内的其他云服务之间进行通信。用户可以使用阿里云提供的VPC相关的EIP功能、高速通道功能，使得VPC可以和Internet、其他VPC、用户自有的网络（如用户办公网络、用户数据中心）之间进行通信。

弹性公网IP产品简介

产品简介

产品概述

弹性公网IP（Elastic IP Address，简称EIP），是可以独立购买和持有的公网IP地址资源，能动态绑定到不同的ECS实例上，绑定和解绑时无需停机。

- 独立的购买与持有

您可以单独购买一个弹性公网IP，而不是与其他计算资源或存储资源绑定购买。

您可以单独持有一个公网IP（需要付出一定的费用）。它作为您账户下一个独立的资源存在。

- 与计算资源的弹性绑定

您可以在需要时将该弹性公网IP绑定到ECS实例上，使该ECS实例具备使用该IP地址进行公网通信的能力。在不需要时，可以将之解绑。

- 可配置的网络能力

您可以根据您的需要来调整弹性公网IP的带宽值。带宽的修改即时生效。

- 弹性公网IP可绑定的资源范围

目前支持绑定弹性公网IP的资源，有且只有ECS实例；更多支持绑定弹性公网IP的资源，敬请期待。

- 弹性公网IP与ECS实例网卡

弹性公网IP是一种NAT IP。它实际位于阿里云的公网网关上，通过NAT方式映射到了被绑定ECS实例的私网网卡上。因此，绑定了弹性公网IP的ECS实例可以直接使用这个IP进行公网通信，但是在网卡上并不能看到这个IP地址。

EIP与ECS Public IP的比较

比较点	Elastic IP Address	ECS Public IP
支持的网络环境	VPC	Classic
是否能够单独持有	支持	不支持
是否支持在ECS上的弹性插拔	支持	不支持
ECS实例网卡上是否能看到该IP	不能	能

NAT网关产品简介

产品简介

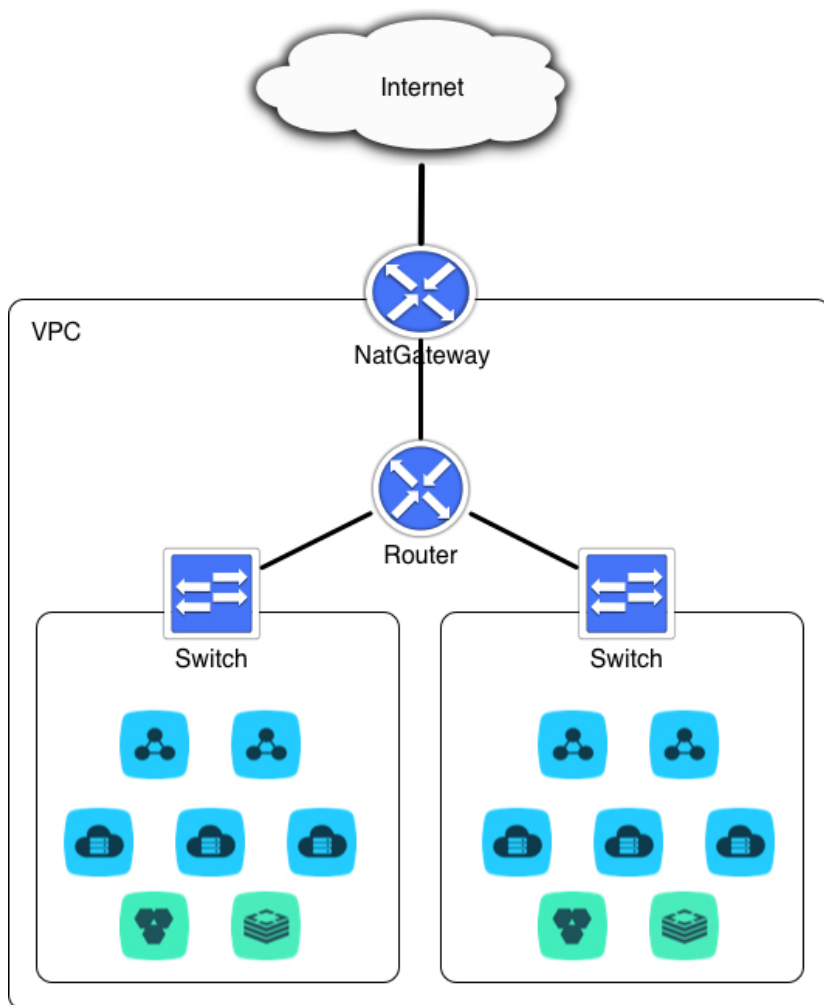
NAT网关（NAT Gateway）是一款企业级的VPC公网网关,提供NAT代理（SNAT、DNAT）、10Gbps级别的转发能力、Region级别的高可用性（跨可用区的容灾能力）。

共享带宽包（Bandwidth Package）是对NAT网关上的公网IP与公网带宽的封装；一个共享带宽包由一份公网带宽和一组公网IP组成，这些公网IP共享带宽。

NAT网关与共享带宽包需要配合使用，组合成为高性能、配置灵活的企业级网关。

网络拓扑

NAT网关在VPC中的网络拓扑位置，如图所示。



关键特性：

- **DNAT**：目的网络地址转换（入方向代理），用于VPC内的ECS面向互联网提供服务；支持端口映射、IP映射；
- **SNAT**：源网络地址转换（出方向代理），用于VPC内的ECS访问互联网内容；
- **多IP共享带宽**：NAT网关上购买公网IP和公网带宽时以"共享带宽包"形式购买，一个带宽包内的所有IP共享带宽；
- **高性能**：NAT网关可以支撑单实例10Gbps级别的转发能力；
- **高可用**：NAT网关基于SDN技术，采用跨可用区分布式架构，每个实例均具备应对可用区级别故障；
- **按需购买**：所有费用均为先使用后结算，实例规格、带宽大小、公网IP个数均可随时调整、即时生效；

NAT网关与弹性公网IP（EIP）的对比介绍

比较点	NAT网关上 BandwidthPackage	Elastic IP Address
-----	----------------------------	--------------------

支持的网络环境	VPC	VPC
是否支持多IP共享带宽	支持	不支持
公网IP与ECS的配合方式	SNAT ; DNAT (port mapping / IP mapping)	IP与ECS一对一绑定 (相当于IP mapping)
是否能方便实现IP与ECS绑定关系的灵活修改	支持	支持
是否支持单IP服务于多台ECS	支持	不支持
ECS实例网卡上是否能看到该IP	不能	不能
典型客户	企业客户 (ECS实例量大、公网IP使用量大、部署服务较多)	中小用户 (ECS/公网IP数量不大, 一对一映射管理更方便)

相关链接

典型使用场景

最佳实践-多IP共享带宽

最佳实践-高可用的SNAT网关

价格总览

API手册

产品名词解释

名词	英文	说明
NAT网关	NAT Gateway	一款企业级的VPC公网网关,提供NAT代理 (SNAT、DNAT)、10Gbps级别的转发能力、Region级别的高可用性 (跨可用区的容灾能力)。
共享带宽包	Bandwidth Package	对NAT网关上的公网IP与公网带宽的抽象封装。一个公网带宽包由一份公网带宽和一组公网IP组成, 这些公网IP共享带宽。共享带宽包中的公网IP可以通过NAT网关上的DNAT/SNAT功能分配给ECS使用
端口转发表	ForwardTable	端口转发表是NAT网关上的一张配置表,用于NAT网关上的DNAT功能配置。可以实现端口映射 (port mapping) 和IP映射 (IP mapping), 将NAT网关上的共享带宽包里的公网IP映射给ECS实例。

SNAT表	SnatTable	SNAT表是NAT网关上的一张配置表，用于NAT网关上的SNAT功能配置。可以以VSwitch为精度进行SNAT规则配置，使指定的VSwitch下的ECS使用指定的公网IP访问互联网。
-------	-----------	--

NAT网关

一款企业级的VPC公网网关,提供NAT代理（SNAT、DNAT）、10Gbps级别的转发能力、Region级别的高可用性（跨可用区的容灾能力）。

NAT网关管理：

- 当需要时，用户可以在指定VPC中创建一个NAT网关。NAT网关是一台虚拟网络设备，在VPC中起到公网网关的作用，是VPC中ECS访问公网的出入口。
- 用户需要在NAT网关上购买公网带宽和公网IP；NAT网关上的公网带宽和公网IP，抽象封装成了"共享带宽包"；一个共享带宽包包含一份公网带宽和一组公网IP；有关共享带宽包的详细介绍详见下文。
- 购买了公网带宽和公网IP之后，用户需要通过DNAT/SNAT配置（即对端口转发表和SNAT表进行修改操作），使NAT网关能按照您的预期将流量正确的转发到ECS上。有关端口转发表和SNAT表的介绍详见下文。
- 目前，NAT网关仅支持向ECS进行流量转发，不支持SLB、RDS、OCS等其他云产品。
- 当不再需要NAT网关和共享带宽包时，用户可以将他们删除。

以上所有管理动作，既可以通过控制台进行，也可以通过API/SDK/CLI工具进行。当前API已经上线，控制台稍后上线，敬请期待。

共享带宽包

对NAT网关上的公网IP与公网带宽的抽象封装。一个公网带宽包由一份公网带宽和一组公网IP组成，这些公网IP共享带宽。共享带宽包中的公网IP可以通过NAT网关上的DNAT/SNAT功能映射给ECS使用，NAT网关会按照您配置的映射关系进行流量转发。

带宽包管理：

- 在NAT网关上创建带宽包时，用户需要指定公网带宽大小和公网IP个数。创建成功后，这个带宽包会附着在NAT网关上，这些IP可以被NAT网关的SNAT/DNAT功能所使用。
- 带宽包中的所有IP共享带宽限速值。
- 当用户需要时，可以随时对带宽大小和公网IP个数进行增减。即时生效。
- 当用户不再需要NAT网关时，应先删除共享带宽包，再删除NAT网关。当NAT网关上还有共享带宽包存在时，直接删除NAT网关会被拒绝。

产品约束：

- 当前，每个NAT网关上最多只能存在一个带宽包。未来会支持一个NAT网关上放置多个带宽包。

- 带宽包的带宽可选范围为5Mbps-5000Mbps；如果您需要更大的带宽值，可以通过工单申请扩大带宽可选范围。
- 带宽包中的IP个数可选范围为1-50个；如果您需要更多的公网IP，可以通过工单申请扩大带宽包中公网IP个数的可选范围。

端口转发表

端口转发表是NAT网关上的一张配置表，用于NAT网关上的DNAT功能配置。可以实现端口映射（port mapping）和IP映射（IP mapping），将NAT网关上的共享带宽包里的公网IP映射给ECS实例

端口转发表管理：

- 每个NAT网关在创建时都会自带一张端口转发表。用户无法对端口转发表进行删除或新建。
- 用户可以对端口转发表中的条目进行新增、修改和删除。
- 每个条目由[ExternalIp, ExternalPort, InternalIp, InternalPort, IpProtocol]五个元素组成；其中：
 - ExternalIp是NAT网关上的公网IP；
 - InternalIp是本VPC内的一个有效的私网IP；
- 一条portmap条目的效果是：NAT网关会将收到的发向ExternalIP:ExternalPort且为指定IpProtocol的数据转发给InternalIp:InternalPort。
- 端口转发条目的另一个用法是，将ExternalPort、InternalPort、IpProtocol均设为Any；此时，NAT网关会将发给该ExternalIp的所有消息转发给指定的InternalIp。
- 当用户需要删除某个共享带宽包时，需要先对端口转发表中的条目进行删减，确保要删除的共享带宽包中的所有IP都没有被端口转发表引用之后，再进行共享带宽包的删除。否则删除操作会被拒绝。

端口转发表产品约束：

- 单个端口转发表的条目数量：100个；如果您需要端口转发表中支持更多的规则条目，可以通过工单申请该数量上限。

SNAT表

SNAT表是NAT网关上的一张配置表，用于NAT网关上的SNAT功能配置。可以以VSwitch为精度进行SNAT规则配置，使指定的VSwitch下的ECS使用指定的公网IP访问互联网。

SNAT表管理：

- 每个NAT网关在创建时都会自带一张SNAT表。用户无法对SNAT表进行删除或新建。
- 用户可以对SNAT表中的条目进行新增、修改和删除。
- 每个SNAT条目由[SourceVSwitchId, SnatIp]组成；其中：
 - SourceVSwitchId是本VPC内一个已存在的VSwitch的Id；
 - SnatIp是NAT网关上的共享带宽包中的一个已存在的公网IP；
- 一个SNAT条目的效果是：
 - 指定的VSwitch下的ECS实例，在没有公网IP的情况下，可以直接使用指定的SnatIp进行互联网访问。
 - 配置该规则之前或之后创建的ECS，均可以使用到这个能力。

- 如果某台ECS已经绑定了EIP，则，该ECS进行公网访问时使用的IP是EIP，而不会去使用SNAT功能。
- 当用户需要删除某个共享带宽包时，需要先对SNAT表中的条目进行删减，确保要删除的共享带宽包中的所有IP都没有被SNAT表引用之后，再进行共享带宽包的删除。否则删除操作会被拒绝。

产品优势

灵活易用的转发能力

作为一款企业级VPC公网网关，NAT网关提供SNAT/DNAT功能，无需用户基于云服务器自己搭建，功能灵活、简单易用、稳定可靠。

高性能

NAT网关是基于阿里云自研分布式网关、使用SDN技术虚拟化出的一款虚拟网络硬件。NAT网关支持10Gbps级别的转发能力，为用户的大规模互联网应用提供支撑。

高可用

NAT网关具备跨可用区的可用性。单个可用区的任何故障都不会影响NAT网关的业务连续性。

按需购买

NAT网关的规格、其上的带宽和公网IP，均可以随时升降，让用户轻松应对业务变化。

DNAT

NAT网关支持DNAT功能，将NAT网关上的公网IP映射给ECS实例使用，使得ECS可以面向互联网提供服务。

端口转发表

NAT网关的DNAT功能的配置，抽象为一张端口转发表。

每个NAT网关在创建时即具备一张端口转发表。用户无法新建或删除端口转发表。用户可以在端口转发表中对端口转发规则条目进行增删改查，从而实现DNAT功能的配置。

端口转发规则条目

端口转发表由端口转发规则条目组成。用户可以对端口转发表中的条目进行新增、查询、删除、修改。

一条端口转发规则由五部分组成：[ExternalIp, ExternalPort, InternalIp, InternalPort, IpProtocol]。其中：

- ExternalIp是NAT网关上的公网IP；
- InternalIp是本VPC内的一个有效的私网IP；

一条portmap条目的效果是：NAT网关会将收到的发向ExternalIP:ExternalPort且为指定IpProtocol的数据转发给InternalIp:InternalPort。

下表是一个端口转发表与三个端口转发条目的示意。

ExternalIp	ExternalPort	InternalIp	InternalPort	IpProtocol
139.224.22.57	80	192.168.1.3	80	TCP
139.224.22.57	8080	192.168.1.4	8000	UDP
139.224.22.26	Any	192.168.1.5	Any	Any

端口映射与IP映射

DNAT功能有两种使用方式：端口映射与IP映射。

端口映射：

- 在端口转发规则中，将ExternalPort、InternalPort、IpProtocol均制定为具体值；

IP映射：

- 在端口转发规则中，将ExternalPort、InternalPort、IpProtocol均制定为Any；
- 其效果是：该InternalIp所属的ECS实例，完全独占该ExternalIp，入方向出方向均可通信。效果类似于绑定了一个EIP。

DNAT相关产品限制

当用户需要删除某个共享带宽包时，需要先对端口转发表中的条目进行删减，确保要删除的共享带宽包中的所有IP都没有被端口转发表引用之后，再进行共享带宽包的删除。否则删除操作会被拒绝。

单个端口转发表的条目数量：100个；如果您需要端口转发表中支持更多的规则条目，可以通过工单申请该数量上限。

当用户需要删除某个共享带宽包时，需要先对SNAT表中的条目进行删减，确保要删除的共享带宽包

中的所有IP都没有被SNAT表引用之后，再进行共享带宽包的删除。否则删除操作会被拒绝。

不允许同一个公网IP即被用于SNAT也被用于DNAT。

SNAT

NAT网关的SNAT功能，用于为VPC内无公网IP的ECS实例提供访问互联网的代理服务。

SNAT表

NAT网关的SNAT功能的配置，抽象为一张SNAT表。

每个NAT网关在创建时即具备一张SNAT表。用户无法新建或删除SNAT表。用户可以在SNAT表中对SNAT规则条目进行增删改查，从而实现SNAT功能的配置。

SNAT规则

SNAT表由SNAT规则条目组成。用户可以对SNAT表中的条目进行新增、查询、删除、修改。

一条SNAT规则由两部分组成：[SourceVSwitchId, SnatIp]。其中：

- SourceVSwitchId是本VPC内一个已存在的VSwitch；
- SnatIp是NAT网关上的公网IP；

一条SNAT规则的效果是：

当指定SourceVSwitchId下的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务（代理上网服务），且使用的公网IP地址为指定的SnatIP。

若某台持有公网IP的ECS实例（比如，已经绑定了EIP）发起互联网访问时，会优先使用其持有的公网IP，而不会激活NAT网关的SNAT功能。

下表是一个SNAT表与多个SNAT规则条目的示意。

SourceVSwitchId	SnatIp
vsw-184ipsw62	139.224.22.57
vsw-11qht5qjm	139.224.22.57

SNAT相关产品限制

- 当用户需要删除某个共享带宽包时，需要先对SNAT表中的条目进行删减，确保要删除的共享带宽包中的所有IP都没有被SNAT表引用之后，再进行共享带宽包的删除。否则删除操作会被拒绝。
- 不允许同一个公网IP即被用于SNAT也被用于DNAT。

共享带宽包

NAT网关作为一个网关设备，需要配置一些公网IP和公网带宽才能正常工作。

NAT网关上的公网IP和公网带宽，被抽象为共享带宽包。通过为NAT网关添加共享带宽包来实现为NAT网关配置公网IP和带宽。

一个NAT网关上最多可以配置四个共享带宽包。

共享带宽

一个共享带宽包，由一份公网带宽和一组公网IP组成。

区别于ECS的publicIP、EIP等产品的"一个IP上配置一份带宽"的带宽购置方式，共享带宽包中的所有公网IP可以共享这份带宽（QOS），从而增加带宽使用的灵活性、降低成本。

配置与价格

共享带宽包是一个付费资源，其收费模式和价格，参见：VPC产品价格总揽

规格说明

NAT网关的规格

NAT网关有规格概念。不同的规格会影响SNAT功能的最大连接数和每秒新建连接数，但不会影响数据吞吐量。

NAT网关不会限制DNAT功能的连接数和吞吐量。

具体规格设计如下：

规格	SNAT最大连接数	SNAT每秒新建连接数	DNAT最大连接数	DNAT每秒新建连接数
Small	1万	1千	不限	不限
Middle	5万	5千	不限	不限
Large	20万	1万	不限	不限

NAT网关的价格

不同规格的NAT网关，价格有所不同。具体价格见VPC产品价格总览

共享带宽包的规格

共享带宽包由一份带宽和一组公网IP组成。共享带宽没有"规格"概念。用户可以直接调整公网带宽大小、公网IP个数。

共享带宽包的价格

不同带宽大小、不同公网IP数量的共享带宽包，价格有所不同。具体价格见VPC产品价格总览

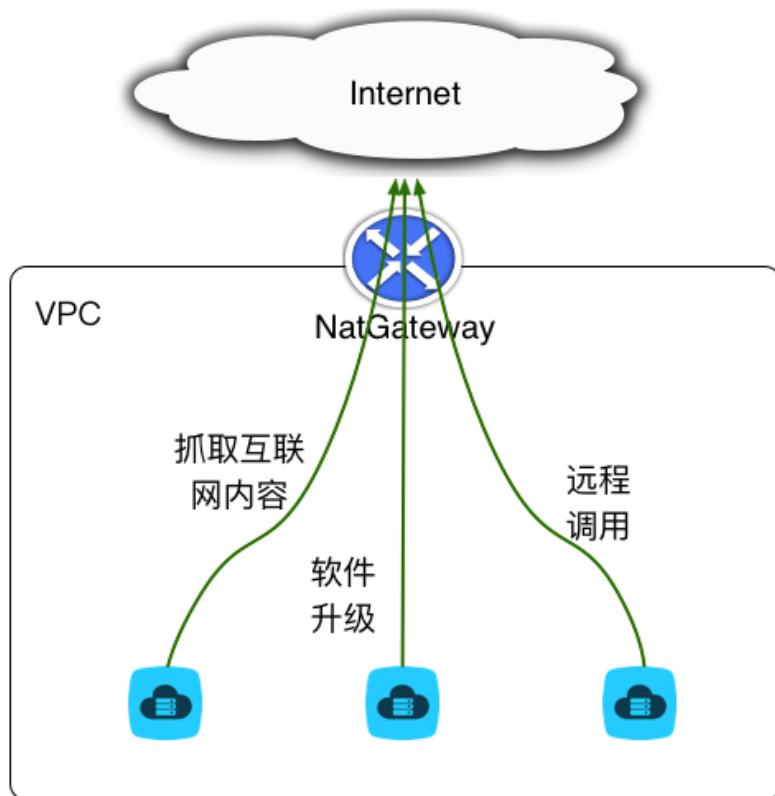
NAT网关与共享带宽包的规格关系

NAT网关的规格与共享带宽包的带宽大小/IP个数 之间没有相互制约关系。最小规格的NAT网关上也可以防止最大带宽的共享带宽包。

使用场景

场景1：无公网IP的ECS需要访问公网--高可用的SNAT网关需求

在一份IT系统中，往往存在一些服务器需要主动访问互联网，但又出于安全性考虑需要避免这些服务器持有公网IP而暴露在公网上。这就需要该IT系统中的网关设备提供SNAT功能。



该场景下的NAT网关使用方法，参见高可用的SNAT网关

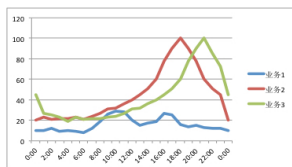
场景2：多个互联网应用流量变化较大--共享公网带宽

部署一个面向互联网提供的服务，需要为该服务购置公网带宽。通常，为了保证系统能够应对业务流量可能发生的各种变化，用户会在购买带宽时考虑一定的冗余。

当一份IT系统中同时存在多个面向互联网的应用时，为每个应用都冗余购置带宽会造成许多不必要的成本。这时，多IP共享带宽的功能能够帮助用户更好的进行公网带宽资源的管理和成本的控制。

另外，考虑到多个面向互联网的应用可能存在的流量错峰情况，多IP共享带宽的功能可以进一步缩减用户所需购置的公网带宽总量。

各自购买公网带宽

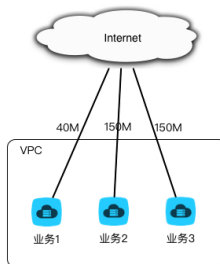


业务1: 峰值30M, 峰值出现时间点不稳定;
为了应对可能的突发高峰, 要购买40M;

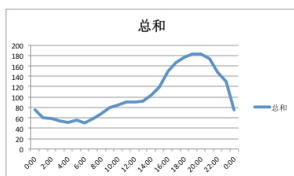
业务2: 峰值100M, 出现在18:00左右;
为了应对突发高峰, 要购买150M, 甚至更多;

业务3: 峰值100M, 峰值出现在21:00左右;
为了应对突发高峰, 要购买150M, 甚至更多;

共计要购买340Mbps的带宽。

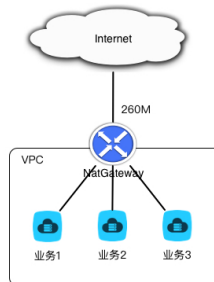


用NAT网关来共享带宽



使用共享带宽模式, 三个业务总和的峰值大约
180Mbps;

即使考虑可能的流量高峰, 购买260Mbps就可以了。



该场景下的NAT网关使用方法, 参见NAT网关最佳实践-多ECS共享带宽

发展历史

发布时间	发布内容
2016年5月	NAT网关上线, 面向白名单客户开放, 用户可以在官网申请使用资格。提供DNAT (port mapping/IP mapping) 功能, 提供共享带宽包 (多IP共享带宽)。暂无控制台, 需要用API/SDK/CLI进行购买使用
2016年7月	NAT网关上线SNAT功能;
2016年7月	NAT网关相关所有功能接入RAM, 支持跨账号、子账号授权等权限管理方式;

近期发布计划

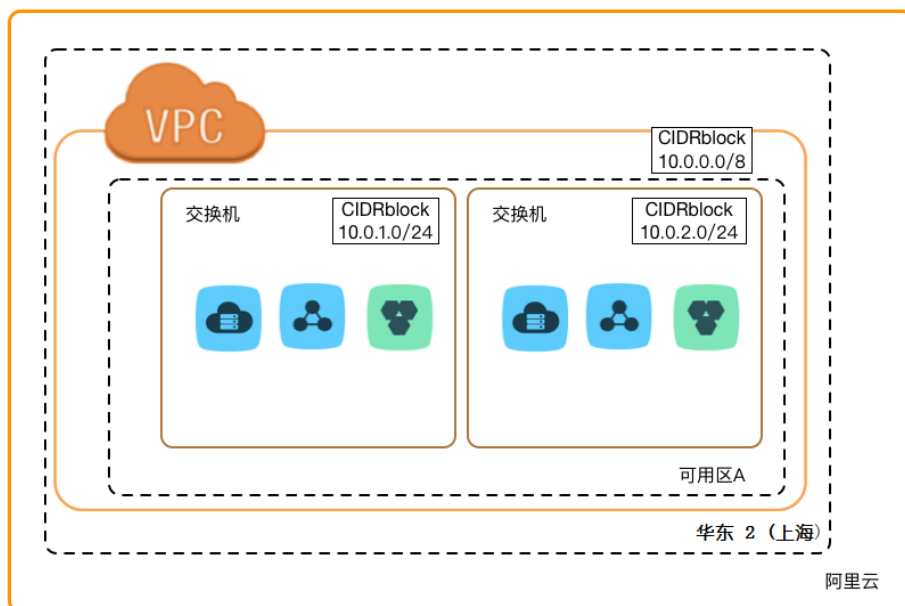
预计发布时间	发布内容
2016年7月	控制台上线;

最佳实践

在阿里云上管理用户专属的网络

应用场景

在阿里云上管理用户专属的网络，创建专有网络、交换机，并在该专有网络中创建云产品实例（如ECS、RDS、SLB、OCS等）并使用。假设地域规划为上海，用户使用上海可用区A上的云产品资源。



网络规划

- 地域为华东 2 (上海)，可用区为华东 2 可用区A
- 专有网络网段为10.0.0.0/8
- 将两个应用部署在两个交换机中，分别对公网和私网提供服务，子网网段分别是10.0.1.0/24、10.0.2.0/24
- 在两个交换机中分别部署私网ECS、公网SLB、私网RDS

操作步骤

1. 登陆专有网络管理控制台<https://vpc.console.aliyun.com/#/vpc/cn-shanghai/list>，地域选择华东 2 (上海)。

2. 点击<创建专有网络>，弹出"创建专有网络"对话框，填写如下信息。

- 专有网络名称：VPC_A
- 网段：10.0.0.0/8

3. 在专有网络VPC_A中，创建两个交换机。

a. 在上海地域的专有网络列表，选择VPC_A的管理链接，进入"专有网络基本信息"页面。

b. 在左侧导航选择"交换机"，点击<创建交换机>，弹出"创建交换机"对话框，填写下面的信息完成交换机1的创建。

- 名称：业务网络A
- 可用区：华东 2 可用区A
- 网段：10.0.1.0/24

c. 创建交换机2，同样在专有网络VPC_A下创建交换机。

- 名称：业务网络B
- 网段：10.0.2.0/24
- 可用区：华东 2 可用区A

4. 配置公网业务的云产品部署。

a. 在交换机列表的"业务网络A"中创建如下云产品实例：ECSx2、RDSx1、公网SLBx1。点击"创建实例"下拉菜单，分别创建ECS1、ECS2、RDS1、SLB1。

b. 登陆负载均衡控制台，通过"后端服务器"的"配置"，将两台ECS实例添加到公网负载均衡实例下。在左侧导航选择"服务器"，然后点击"未添加的服务器"页签，将ECS1和ECS2添加到公网SLB1实例下。

5. 配置私网业务的云产品部署。

a. 创建云产品实例：在交换机"业务网络B"中创建：ECSx2，RDSx1，SLBx1。点击"创建实例"下拉菜单，分别创建ECS3、ECS4、RDS2、SLB2。

b. 登陆负载均衡控制台，通过"后端服务器"的"配置"，将两台ECS实例添加到私网SLB实例下。在左侧导航选择"服务器"，然后点击"未添加的服务器"页签，将ECS3和ECS4添加到私网SLB2实例下。

API

涉及的相关API文档如下。

VPC

创建专有网络

新建交换机

ECS

- 创建实例

SLB

CreateLoadBalancer

AddBackendServers

RDS

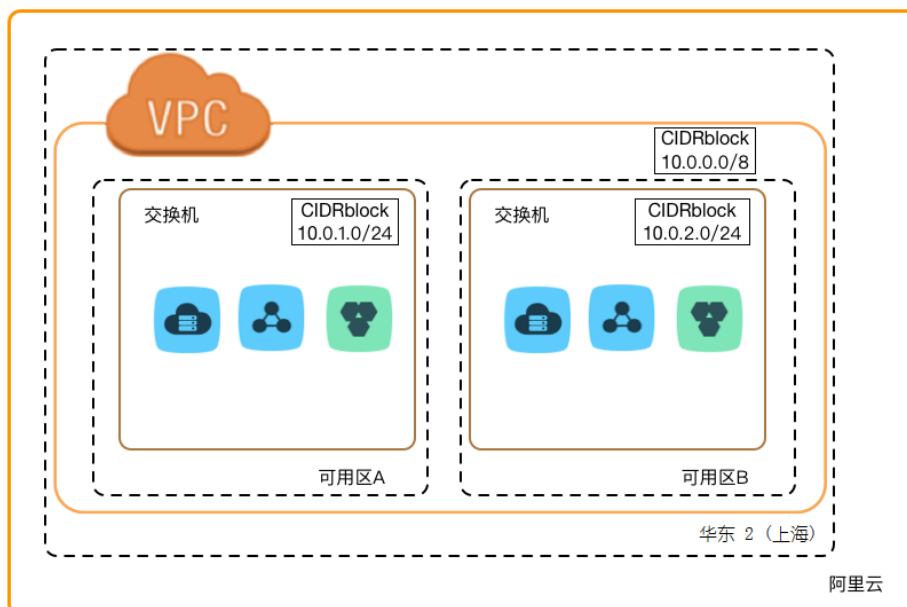
- 创建RDS实例

专有网络中跨可用区部署资源

应用场景

用户可以通过将资源部署在处于不同可用区的交换机中，从而实现利用阿里云可用区进行容灾。本文以地域上海为例，可用区使用华东 2 可用区A和华东 2 可用区B，进行跨可用区的资源部署。

当阿里云华东 2 可用区A机房发生异常时，仍能够通过部署在华东 2 可用区B机房的备服务器提供服务。



网络规划

- 地域：上海，可用区：华东 2 可用区A、华东 2 可用区B
- 专有网络网段为10.0.0.0/8
- 将两个应用部署在两个不同可用区的交换机中，子网网段分别是10.0.1.0/24、10.0.2.0/24
- 在两个不同可用区的交换机中分别部署ECS、SLB、RDS

操作步骤

1. 登陆专有网络管理控制台<https://vpc.console.aliyun.com/#/vpc/cn-shanghai/list>，地域选择"华东 2 (上海)"。

2. 点击<创建专有网络>，弹出"创建专有网络"对话框，填写如下信息。

- 专有网络名称：VPC_B
- 网段：10.0.0.0/8

3. 在专有网络VPC_B中，创建两个交换机。

a. 在"华东 2 (上海)"地域的专有网络列表，选择VPC_B的"管理"链接，进入"专有网络基本信息"页面。

b. 在左侧导航选择"交换机"，点击<创建交换机>，弹出"创建交换机"对话框，填写下面的信息完成交换机1的创建。

- 名称：业务网络主
- 可用区：华东 2 可用区A
- 网段：10.0.1.0/24

c. 创建交换机2，同样在专有网络VPC_B下创建交换机。

- 名称：业务网络备
- 网段：10.0.2.0/24
- 可用区：华东 2 可用区B

4. 配置业务相关云产品部署。

a. 在交换机列表的"业务网络主"中创建如下云产品实例：ECSx2、RDSx1，作为服务的主服务器和数据库。点击"创建实例"下拉菜单，分别创建ECS1、ECS2、RDS1。

b. 在交换机列表的"业务网络备"中创建如下云产品实例：ECSx2、RDSx1，作为服务的备服务器和数据库。点击"创建实例"下拉菜单，分别创建ECS3、ECS4、RDS2。

c. 在地域"华东 2 (上海)"下创建两台公网SLB，选择主可用区为：华东 2 可用区A，备可用区为：华东 2 可用区B。

d. 将两个交换机下的四台ECS实例分别添加到公网SLB实例下。

API

涉及的相关API文档如下。

VPC

创建专有网络

新建交换机

ECS

- 创建实例

SLB

- CreateLoadBalancer

- AddBackendServers

RDS

- 创建RDS实例

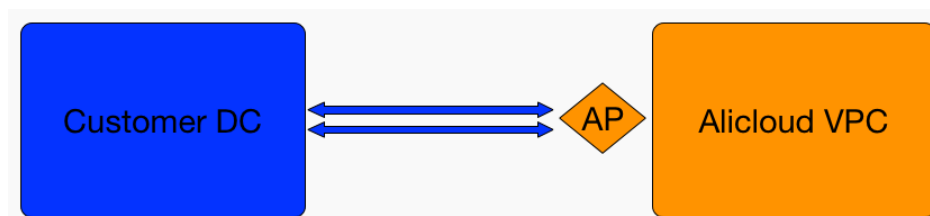
物理专线接入

应用场景

通过物理专线将自有数据中心和阿里云VPC连接起来，实现用户网络与阿里云专有网络之间的内网互通，支持2条线路通过链路汇聚方式实现主备或双活。

用户已经在"华北 2 (北京)"拥有一个物理数据中心（私网网段：172.16.0.0/12），在阿里云"华东 1 (杭州)"地域有一个专有网络（名称：云上数据中心，CIDRblock：192.168.0.0/16），通过某运营商的百兆物理专线，接入阿里云机房实现专有网络与物理机房间的内网融合。

客户的阿里云上VPC，需要与自有机房进行私网通信。使用高速通道的专线接入功能，可以实现两侧的私网通信，既可以避免绕行公网带来的网络质量不稳定问题，也可以免去数据在传输过程中被窃取的风险。



操作步骤

1. 开通高速通道服务。

a. 登陆网址<https://www.aliyun.com/product/expressconnect/>。

b. 点击<获取使用资格>，进行测试资格的申请。

说明：当高速通道产品，全网开放后，就不用申请了。

2. 申请物理专线及完成专线接入。

a. 登陆高速通道管理控制台，点击<申请专线接入>，填写相关信息。

- 专线名称：北京本地专线
- 接入点：北京 北京-大兴-A
- 使用运营商：中国其他
- 接入端口类型：100Base-T-百兆电口
- 接入带宽：100Mbps
- 专线对端地址：北京市xx区xx大街xx号
- 冗余物理专线：根据状况进行选择

b. 点击<确认申请>，华北 2 (北京)地域的"物理专线列表"页专线状态为"申请中"。

c. 专线接入审批通过的标志是状态变为"审批通过"。

d. 点击<支付接入费>，完成接入费用支付。

e. 专线状态变为"接入施工中"。

f. 接入施工完毕，确认专线接入。

g. 专线状态变为"等待确认"。

h. 点击<确认>，专线状态变为"正常"，完成专线接入。

3. 在物理专线上创建边界路由器。

a. 登陆高速通道控制台，在左侧导航树，选择"边界路由器"，点击<新建边界路由器>。

b. 选择成功接入的物理专线，填写相关参数。

- 名称：北京边界路由器
- 描述：
- 物理专线：pc-xxxxxx (物理专线"北京本地专线"的ID)
- VLANID：100
- 电路编码：SDHXXX
- 互联地址：阿里云侧 10.100.0.1；客户侧 10.100.0.10；子网掩码 255.255.255.0

c. 点击<确认新建>，返回"华北 2 (北京)"地域下的"边界路由器列表"页。

d. 创建的边界路由器状态为"正常"，说明新建边界路由器成功。

4. 在边界路由器上创建一个路由器接口A，角色为发起端。

a. 在"边界路由器详情页"或"路由器接口列表"页，点击<创建路由器接口>。

- 连接场景：自定义

本端配置

- 路由器类型：边界路由器
- 地域：华北 2 (北京)
- 本端接入点：北京-大兴-A
- 边界路由器：北京边界路由器

对端配置

- 对端路由器类型：VPC路由器
- 对端地域：华东 1 (杭州)

角色规格

- 连接角色：连接发起端
- 规格：大型1档

b. 点击<立即购买>完成购买。

c. 在高速通道控制台"路由器接口列表"页, 可以查看该路由器接口信息, 接口状态为"未连接"。

d. 为了便于查看, 通过"操作 > 更多 > 编辑本端接口信息", 将名称修改为"北京路由器接口"。

5. 在杭州专有网络 (名称：云上数据中心) 创建路由器接口, 角色为接收端。

a. 登陆高速通道管理控制台, 在"路由器接口列表"页, 点击<创建路由器接口>。

- 连接场景：自定义

本端配置

- 路由器类型：VPC路由器
- 地域：华东 1 (杭州)
- 专有网络：云上数据中心
- 路由器：vr-xxxxxxx (自动填写所选专有网络中的路由器ID, 无需修改)

对端配置

- 对端路由器类型：边界路由器
- 对端地域：华北 2 (北京)
- 对端接入点：北京-大兴-A

角色规格

- 连接角色：连接接受端
- 规格：默认

b. 点击<立即购买>完成购买。

c. 在高速通道控制台"路由器接口列表"页可以查看该路由器接口信息, 接口状态为"未连接"。

d.为了便于查看，选择"操作 > 更多 > 编辑本端接口信息"，将名称修改为"杭州路由器接口"。

6.配置并连接两个路由器接口。

将两个路由器接口互相配置为对端接口

a.在高速通道控制台"路由器接口列表"页，地域选择"华北 2 (北京)"。

b.选择创建在边界路由器上的接口，在对端路由器接口列，点击"添加"

- 所属账号：当前账号
- 对端路由器接口ID/名称：杭州路由器接口

勾选"将当前路由器接口配置为所选路由器接口的对端"

说明：若未勾选"将当前路由器接口配置为所选路由器接口的对端"，需在列表页重复本步骤，为VPC路由器上的路由器接口"杭州路由器接口"配置对端接口。

c.点击<确定>完成对端接口配置，此时两个路由器接口互相配置为对端接口。

在两个路由器接口之间建立连接

a.登陆高速通道控制台，进入"路由器接口列表"页，选择"北京路由器接口"，点击"发起连接"。

b.确认发起连接后，两个路由器接口状态均为"已激活"。

至此，已经完成通过物理专线接入将位于"华北 2 (北京)"的物理数据中心与阿里云上"华东 1 (杭州)"的专有网络内网连通。

7.配置路由，管理边界路由器与专有网络的流量转发。

将边界路由器上访问"192.168.0.0/16"的流量转发至专有网络

a.登陆高速通道控制台，选择边界路由器，点击"管理"，进入边界路由器详情页，点击"添加路由"，填写如下信息。

- 目标网段：192.168.0.0/16
- 下一跳方向：指向VPC方式
- 下一跳：北京路由器接口

b.点击<确定>，完成配置。

将边界路由器上访问"172.16.0.0/12"的流量转发至物理专线

a.登陆高速通道控制台，选择边界路由器，点击"管理"，进入边界路由器详情页，点击"添加路由"，填写如下信息。

- 目标网段：172.16.0.0/12
- 下一跳方式：指向专线方式

b.点击<确定>，完成配置。

将专有网络（名称：云上数据中心）中访问"172.16.0.0/12"的流量转发至边界路由器

a.登陆"专有网络"控制台，选择边界路由器，点击"管理"，选择"路由器"，点击"添加路由"，填写如下信息。

- 目标网段：172.16.0.0/12
- 下一跳类型：路由器接口
- 路由器接口：北京路由器接口

b.点击<确定>，完成配置。

8.用户根据需要进行网络设置。

说明：如果还需对两侧进行互访的资源进行访问控制设置，比如，可以对ECS的安全组进行规则添加，可以参考创建安全组，允许专线对对端网络的ECS实例访问等。

API

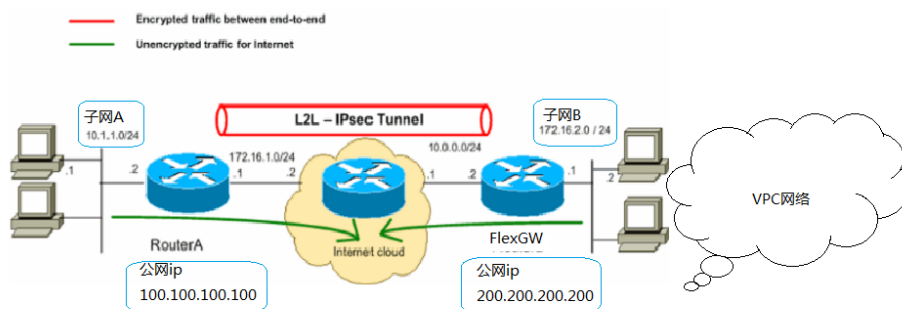
专线接入场景不推荐用户使用OpenAPI进行相关操作。

搭建VPN网关

概述

以下以使用驻云VPN镜像建立site to site VPN（又称L2L VPN）为例。

L2L VPN拓扑结构



两个子网通过路由器A和路由器B接入互联网，同时通过一个L2L的ipsec隧道在两台路由器之间建立一个虚拟的连接，将A、B两个网络互通起来，效果与Router A、RouterB之间拉一根物理专线一样。两端的vpn节点设备可以是路由器，也可以是专业的防火墙，也可以是基于x86服务器的系统软件。

环境准备

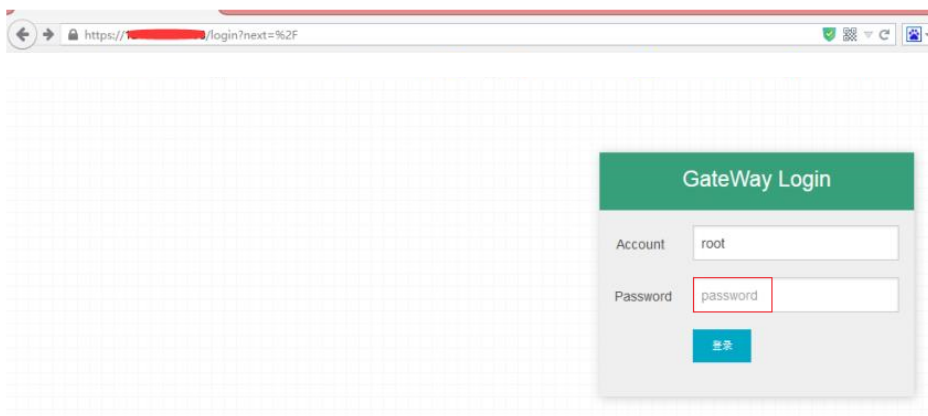
本文档环境如下：RouterA是VPC环境，采用一台ECS安装FlexGW的镜像，配置如下：

- 操作系统：centos 6.5 64位
- 软件包：Strongswan5.3.2-Openvpn2.3.8-FlexGW2.0

RouterB可以是思科或华为、华三的路由器、防火墙，也可以是另一个FlexGW服务器。

FlexGW配置

1.使用 VM的系统账号密码即可登入系统，登陆方式：浏览器访问"https: //公网IP"。



2.进入 VPN服务管理 -点击启动VPN服务。

Flex GateWay



3.增加隧道：点击<新增隧道>，按照下图内容填写，以下配置属于拓扑结构图中右边子网B的RouterB的配置。

隧道ID：互相连接的隧道两端ID 需要保持一致。本端对端子网：可以填写多个子网，用英文「,」分割。

隧道ID	tunnel-1	
IKE版本	IKEV1	请与对端版本保持一致
启动类型	服务启动自动连接	
IKE 加密算法	3DES	请与对端保持一致
IKE 验证算法	SHA1	请与对端保持一致
IKE DH 组	Group 2 modp1024	请与对端保持一致
ESP 加密算法	3DES	请与对端保持一致
ESP 验证算法	SHA1	请与对端保持一致
ESP DH 组	Group 2 modp1024	请与对端保持一致
本端ID	200.200.200.200	请与对端的「对端ID」保持一致
本端子网	172.16.2.0/24	
对端ID	100.100.100.100	请与对端的「本端ID」保持一致
对端公网IP	100.100.100.100	
对端子网	10.1.1.0/24	
预共享密钥	A1@345b	
保存		

- 隧道ID：最好配一端的路由器的域名或者公网IP，两端设备的这个部分要保持一致。
- IKE版本：为了安全健壮性，建议使用版本2
- 启动类型：选择自动连接
- IKE 加密算法：一般选择3DES模式
- IKE 验证算法：在以上选择了3DES后，这里一般选择sha-1
- IKE DH 组：默认第一项modp 768即可
- ESP 加密算法：默认3DES
- ESP 验证算法：默认MD5
- ESP DH 组：一般不需要
- 与共享密钥：请根据个人情况设置协商用密码

基于ike V1的配置

对端配置一，路由器配置说明：

```
access-list 111 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255 ip route 0.0.0.0 0.0.0.0 100.100.100.1
```

#增加默认路由与acl

```
crypto keyring 1 pre-shared-key address 200.200.200.200 key A1@456b
```

```
crypto isakmp policy 1 encr 3des authentication pre-share group 2crypto isakmp profile 1 keyring 1
self-identity address match identity address 200.200.200.200 255.255.255.255 local-address
100.100.100.100
```

```
crypto ipsec transform-set vsr esp-3des esp-sha-hmac
```

```
crypto map tunnel_1 100 ipsec-isakmp set peer 200.200.200.200 set security-association lifetime
seconds 86400 set transform-set vsr set pfs group2 match address 111
```

```
interface Ethernet1/0 ip address 100.100.100.100 255.255.255.0 full-duplex crypto map tunnel_1 #将
配置应用到接口下
```

注意：一定要使能配置：crypto isakmp enable 路由器默认此信息不显示，但必须配置。配置示例：

```
`R1#show runBuilding configuration...
```

```
Current configuration : 2106 bytes!version 12.4service timestamps debug datetime msecservice
timestamps log datetime msecno service password-encryption!hostname RouterA!boot-start-
markerboot-end-marker!!no aaa new-model!resource policy!memory-size iomem 5no ip icmp rate-
limit unreachableip tcp synwait-time 5!!ip cefno ip domain lookup!!crypto keyring 1 pre-shared-key
address 200.200.200.200 key A1@456b!crypto isakmp policy 1 encr 3des authentication pre-share
group 2crypto isakmp profile 1 keyring 1 self-identity address match identity address
200.200.200.200 255.255.255.255 local-address 100.100.100.100!!crypto ipsec transform-set vsr esp-
3des esp-sha-hmac!crypto map tunnel_1 100 ipsec-isakmp set peer 200.200.200.200 set security-
association lifetime seconds 86400 set transform-set vsr set pfs group2 match address
111!!!!interface Loopback0 ip address 10.1.1.1 255.255.255.0!interface FastEthernet0/0!
```

```
!interface Ethernet1/0 ip address 100.100.100.100 255.255.255.0 full-duplex crypto map
tunnel_1!interface Ethernet1/1 no ip address half-duplex!interface Ethernet1/2 no ip address
shutdown half-duplex!interface Ethernet1/3 no ip address shutdown half-duplex!interface Vlan1 no ip
address!no ip http serverno ip http secure-serverip route 0.0.0.0 0.0.0.0 100.100.100.1!!!access-list 111
permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255no cdp log mismatch duplex!!!control-plane!!!!!!line
con 0 exec-timeout 0 0 privilege level 15 logging synchronousline aux 0 exec-timeout 0 0 privilege
level 15 logging synchronousline vty 0 4 login!
```

,

对端配置二，ASA防火墙说明（IOS：8.2）：

```
access-list 100 extended permit ip 172.16.2.0 255.255.255.0 10.1.1.0 255.255.255.0
```

```
isakmp identity autocrypto isakmp policy 1authentication pre-shareencryption 3deshash shagroup
2lifetime 86400crypto isakmp enable OutSide
```

```
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```

```
crypto map OutSide_map 10 match address 100
crypto map OutSide_map 10 set pfs
crypto map OutSide_map 12 set peer 200.200.200.200
crypto map OutSide_map 12 set transform-set ESP-3DES-SHA
crypto map OutSide_map interface OutSide

tunnel-group 200.200.200.200 type ipsec-l2l
tunnel-group 200.200.200.200 ipsec-attributes pre-shared-key A1@456b
peer-id-validate nocheck
```

基于ike V2的配置

其他不变，当web上选择ike V2时，对方设备配置如下：

对端配置一，路由器配置说明：

```
crypto ikev2 proposal R1-proposal \创建一个proposal
encryption 3des aes-cbc-256 integrity md5 sha256 group 1 2 5

crypto ikev2 policy R1-policy \创建一个策略，以便可以调用proposal proposal R1-proposal

crypto ikev2 keyring R1-key \创建一个密钥文件 peer ASA \名字本地有效，作为一个标识而已。 address
200.200.200.200 \对方地址 pre-shared-key A1@345b \预共享密钥

crypto ikev2 profile ike-profile \创建一个ike的profile。 match identity remote address 200.200.200.200
255.255.255.255 \对方加密点地址 identity local address 100.100.100.100 \本地加密点地址。

authentication remote pre-share \认证方式 authentication local pre-share keyring local R1-key \调用
KEY文件

crypto ipsec transform-set aa esp-des esp-md5-hmac mode tunnel
crypto map VPN 1 ipsec-isakmp
set peer 200.200.200.200 set transform-set aa

set ikev2-profile ike-profile \调用 IKE的profile match address 100 crypto map VPN
```

接口下应用与路由配置同ike V1注意：一定要使能配置：crypto isakmp enable 路由器默认此信息不显示，但必须配置

对端配置二，防火墙配置说明（IOS 8.4以上）：

```
Crypto ikev2 enable outside \使能逻辑域
crypto ikev2 policy 10 \创建一个策略 encryption aes-256 3des
integrity sha256 md5 group 5 2 1 prf sha256 md5 \伪随机数。切记，这里默认是sha，如果两边不一样会
建立不起来

tunnel-group 100.100.100.100 type ipsec-l2l
tunnel-group 100.100.100.100 ipsec-attributes ikev2
remote-authentication pre-shared-key A1@345b ikev2 local-authentication pre-shared-key A1@345b

crypto ipsec ikev2 ipsec-proposal aa \相当于路由器上的转换集 protocol esp encryption des protocol
esp integrity md5

crypto map VPN 1 match address 100
crypto map VPN 1 set peer 100.100.100.100
crypto map VPN 1
```

set ikev2 ipsec-proposal aa \在map上调用转换集crypto map VPN interface outside

多应用共享带宽

概述

用户的系统中有多个应用要面向互联网提供服务；出于带宽管理、成本节省的角度，希望购买一份带宽给这些应用共享。

本文介绍如何利用NAT网关的DNAT功能和共享带宽功能实现多应用的共享带宽。

关于API与控制台

NAT网关产品，提供了web控制台供用户进行选购和配置；同时也提供了API，供用户通过代码实现资源的选购和配置，从而能够自动化的完成一些系统部署和变更动作。

本文侧重于使用API来完成操作。但是，**所有具体步骤均可以在控制台上找到相应的操作。**

为了方便用户调用API，本文给出了一个用python语言编写的Commond Line工具。见下面的 前期准备-CLI工具的准备 章节。基于此工具，用户可以用命令行方式进行NAT网关相关资源的购买和配置。具体的使用方法，可以参照本文每一步操作中给出的命令样例。用户可以根据自己的需求和资源的id对命令进行改写，完成操作。

前期准备

部署规划

假设我们的系统中有四个面向互联网的应用，需要使用三个公网IP；另外需要一个ECS和一个IP作为服务器管理的跳板机来使用；另准备一个公网IP暂时闲置，备用。整体资源规划如下：

```
带宽需求总量：150Mbps
公网IP需求总量：4个；另外多购买一个IP，以备使用；总共购买5个公网IP。
ECS需求总量：5个
公网IP与ECS的映射关系：
IP1->ECS1
IP2->ECS2
IP3->ECS3/ECS4;
其中，
80端口映射给ECS3的80端口；
443端口映射给ECS4的443端口；
IP4->ECS5（运维跳板机），仅开放22端口；
IP5：暂不添加DNAT规则；
```

VPC与ECS的准备

创建VPC与ECS，配置成如下图中所示的状态。注意，这些ECS实例不需要公网IP。

本文侧重于介绍多应用带宽共享部分的实现，因此，VPC和ECS的创建过程不予赘述。

假设现在已经创建好的VPC与ECS资源相关情况如下：

VPC:
VpcId: vpc-11af8lp67
ECS:
ECS1
PrivateIP: 192.168.1.1
ECS2
PrivateIP: 192.168.1.2
ECS3
PrivateIP: 192.168.1.3
ECS4
PrivateIP: 192.168.1.4
ECS5
PrivateIP: 192.168.1.5

实例名称

请输入实例名称进行模糊查询

搜索

标签

☐ 实例ID/名称	监控	所在可用区	IP地址	状态(全部)	网络类型(全部)
☐ i-11ug9f1my ecs1	 	华东 2 可用区 A	192.168.1.1 (私有)	 运行中	专有网络
☐ i-119kjqwj ecs2	 	华东 2 可用区 A	192.168.1.2 (私有)	 运行中	专有网络
☐ i-11v1odnz8 ecs3	 	华东 2 可用区 A	192.168.1.3 (私有)	 运行中	专有网络
☐ i-113vqdfk6 ecs4	 	华东 2 可用区 A	192.168.1.4 (私有)	 运行中	专有网络
☐ i-11hi8ub2v ecs5	 	华东 2 可用区 A	192.168.1.5 (私有)	 运行中	专有网络

CLI工具的准备

CLI工具下载

下载cli工具：api.py

linux环境下可以直接使用wget命令进行下载。命令和运行效果截图如下：

```
wget http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach/42691/cn_zh/1468947102311/api.py
```

```
admin@iZ119kjqwvjZ:~/nat_gw_cli_tool$ wget http://docs.aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach/32327/cn_zh/1463980436933/api.py
--2016-05-23 15:15:24-- http://docs.aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach/32327/cn_zh/1463980436933/api.py
Resolving docs.aliyun.cn-hangzhou.oss.aliyun-inc.com (docs.aliyun.cn-hangzhou.oss.aliyun-inc.com)... 42.120.230.2
Connecting to docs.aliyun.cn-hangzhou.oss.aliyun-inc.com (docs.aliyun.cn-hangzhou.oss.aliyun-inc.com)|42.120.230.2|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5398 (5.3K) [text/x-python-script]
Saving to: 'api.py'

100%[=====>] 5,398 --.-K/s in 0s

2016-05-23 15:15:24 (656 MB/s) - 'api.py' saved [5398/5398]

admin@iZ119kjqwvjZ:~/nat_gw_cli_tool$ ls
api.py
admin@iZ119kjqwvjZ:~/nat_gw_cli_tool$
```

创建并查看AccessKey

AccessKey可以在AccessKey管理控制台进行申请和管理。



为CLI工具配置AccessKey

配置命令如下图所示：

```
admin@iZ119kjqwvjZ:~/nat_gw_cli_tool$ python api.py config --id jZgi0oyrQ6ihgKp9 --secret
```

操作步骤

创建NAT Gateway

在当前VPC中创建一个NAT网关，并在该NAT网关上放置一个共享带宽包，其中包含150Mbps的带宽和5个公网IP；

相应的CLI命令和获取到的返回信息如下：

```
[admin@test:nat_gw_cli_tool]$ python api.py CreateNatGateway RegionId=cn-shanghai VpcId=vpc-11af8lp67
BandwidthPackage.1.IpCount=4 BandwidthPackage.1.Bandwidth=150 BandwidthPackage.1.Zone=cn-shanghai-a
Name=MyNatGW Description="My first NAT Gateway"
====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&VpcId=vpc-11af8lp67&Name=MyNatGW&Format=json&TimeStamp=2016-05-23T03%3A26%3A21Z&BandwidthPackage.1.IpCount=5&RegionId=cn-shanghai&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-26&Signature=I4KKhWgjdImTqk4rCifAB3LbLw%3D&action=CreateNatGateway&SignatureNonce=1ebae49c-2096-11e6-b781-2cf0ee28adf2&BandwidthPackage.1.Bandwidth=150&BandwidthPackage.1.Zone=cn-shanghai-a&Description=My+first+NAT+Gateway
```

```

=====Request URL end=====

===== Got Response =====
{
  "BandwidthPackageIds": {
    "BandwidthPackageId": [
      "bwp-11odxu2k7"
    ]
  },
  "ForwardTableIds": {
    "ForwardTableId": [
      "ftb-11tc6xgmv"
    ]
  },
  "NatGatewayId": "ngw-112za33e4",
  "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}

```

通过DescribeNatGateways、DescribeBandwidthPackages查看创建出来的NAT网关和共享带宽包的详细信息。

```

[admin@test:~]$ python api.py DescribeNatGateways RegionId=cn-shanghai VpcId=vpc-11af8lp67
=====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&VpcId=vpc-11af8lp67&Format=json&TimeStamp=2016-05-23T03%3A27%3A14Z&RegionId=cn-shanghai&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-26&Signature=JvXErs09g0fZdRTgBtNLepe%2F1e4%3D&action=DescribeNatGateways&SignatureNonce=3e1424eb-2096-11e6-bc31-2cf0ee28adf2
=====Request URL end=====

===== Got Response =====
{
  "NatGateways": {
    "NatGateway": [
      {
        "BandwidthPackageIds": {
          "BandwidthPackageId": [
            "bwp-11odxu2k7"
          ]
        },
        "BusinessStatus": "Normal",
        "CreationTime": "2016-05-23T03:26:23Z",
        "Description": "My first NAT Gateway",
        "ForwardTableIds": {
          "ForwardTableId": [
            "ftb-11tc6xgmv"
          ]
        },
        "InstanceChargeType": "PostPaid",
        "Name": "MyNatGW",
        "NatGatewayId": "ngw-112za33e4",
        "RegionId": "cn-shanghai",
        "Spec": "Small",
        "Status": "Available",
        "VpcId": "vpc-11af8lp67"
      }
    ]
  }
}

```

```

}
]
},
"PageNumber": 1,
"PageSize": 10,
"RequestId": "FE4C442C-9778-449A-BF7F-7F36C3AF5611",
"TotalCount": 1
}

```

```

[admin@tester:nat_gw_cli_tool]$ python api.py DescribeBandwidthPackages RegionId=cn-shanghai
NatGatewayId=ngw-112za33e4
=====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&Format=json&TimeStamp=2016-05-
23T03%3A33%3A30Z&RegionId=cn-shanghai&NatGatewayId=ngw-
112za33e4&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&Signature=KN0C2Q4TUZtfECBn1c2lOdBzrb8%3D&action=DescribeBandwidthPackages&SignatureNonce=1e89
41ae-2097-11e6-acbb-2cf0ee28adf2
=====Request URL end=====

```

```

===== Got Response =====
{
  "BandwidthPackages": {
    "BandwidthPackage": [
      {
        "Bandwidth": "150",
        "BandwidthPackageId": "bwp-11odxu2k7",
        "BusinessStatus": "Normal",
        "CreationTime": "2016-05-23T03:26:24Z",
        "Description": "",
        "InstanceChargeType": "PostPaid",
        "InternetChargeType": "PayByBandwidth",
        "IpCount": "5",
        "Name": "",
        "NatGatewayId": "ngw-112za33e4",
        "PublicIpAddresses": {
          "PublicIpAdresse": [
            {
              "AllocationId": "nateip-11iopy3sl",
              "IpAddress": "139.224.22.107"
            },
            {
              "AllocationId": "nateip-11pt1f9ph",
              "IpAddress": "139.224.22.55"
            },
            {
              "AllocationId": "nateip-111ul670c",
              "IpAddress": "139.224.22.79"
            },
            {
              "AllocationId": "nateip-11ogfjj85",
              "IpAddress": "139.224.22.59"
            },
            {
              "AllocationId": "nateip-11s2jempe",
              "IpAddress": "139.224.22.99"
            }
          ]
        }
      }
    ]
  }
}

```

```

}
]
},
"RegionId": "cn-shanghai",
"Status": "Available",
"ZoneId": "cn-shanghai-a"
}
]
},
"PageNumber": 1,
"PageSize": 10,
"RequestId": "14406B86-7CA1-4907-9755-86096F476A4F",
"TotalCount": 1
}

```

进行DNAT配置

在NAT网关的端口转发表中，添加五条端口映射规则；

```

Ip1:Any -> ecs-ip1:Any, protocol=Any
Ip2:Any -> ecs-ip2:Any, protocol=Any
Ip3:80 -> ecs-ip3:80, protocol=TCP
Ip3:443 -> ecs-ip3:443, protocol=TCP
IP4:22 -> ecs-ip4:22, protocol=TCP

```

CLI命令和获得的返回信息如下：

```

[admin@test:~]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.224.22.107 InternalIp=192.168.1.1 InternalPort=Any IpProtocol=Any
====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.107&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A53%3A18Z&RegionId=cn-shanghai&ExternalPort=Any&InternalIp=192.168.1.1&Signature=iR4GSzhJQtowMJOj%2FRth3ABP4FA%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=e2ceae11-2099-11e6-b548-2cf0ee28adf2&InternalPort=Any
====Request URL end=====

==== Got Response =====
[admin@test:~]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.224.22.107 InternalIp=192.168.1.1 InternalPort=Any IpProtocol=Any
====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.107&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A53%3A18Z&RegionId=cn-shanghai&ExternalPort=Any&InternalIp=192.168.1.1&Signature=iR4GSzhJQtowMJOj%2FRth3ABP4FA%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=e2ceae11-2099-11e6-b548-2cf0ee28adf2&InternalPort=Any
====Request URL end=====

==== Got Response =====
{
"ForwardEntryId": "fwd-119smw5tk",

```

```

"RequestId": "A4AEE536-A97A-40EB-9EBE-53A6948A6928"
}
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-
11tc6xgmv ExternalIp=139.224.22.55 ExternalPort=Any InternalIp=192.168.1.2 InternalPort=Any IpProtocol=Any
=====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.55&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-
23T03%3A53%3A42Z&RegionId=cn-
shanghai&ExternalPort=Any&InternalIp=192.168.1.2&Signature=mFBn%2BCd4LfHkKj53MwmWyMhzyfs%3D&Acce
ssKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=f09c1b38-2099-11e6-aa80-
2cf0ee28adf2&InternalPort=Any
=====Request URL end=====

===== Got Response =====
{
"ForwardEntryId": "fwd-11dz3ly9l",
"RequestId": "5DBC8F86-2D76-4BF4-B839-7FF31B61D516"
}
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-
11tc6xgmv ExternalIp=139.224.22.79 ExternalPort=80 InternalIp=192.168.1.3 InternalPort=80 IpProtocol=TCP
=====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.79&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-
23T03%3A54%3A10Z&RegionId=cn-
shanghai&ExternalPort=80&InternalIp=192.168.1.3&Signature=OpTui3SKbAjKXy6gKRoJb%2B9Lazg%3D&AccessKe
yId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=01c41d5c-209a-11e6-905e-
2cf0ee28adf2&InternalPort=80
=====Request URL end=====

===== Got Response =====
{
"ForwardEntryId": "fwd-11r23r7p5",
"RequestId": "67B7AAFD-E7AB-4EB8-AA5C-AA38CFFB4A95"
}
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$
[admin@test:nat_gw_cli_tool]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-
11tc6xgmv ExternalIp=139.224.22.79 ExternalPort=443 InternalIp=192.168.1.4 InternalPort=443 IpProtocol=TCP
=====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.79&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-
23T03%3A55%3A22Z&RegionId=cn-
shanghai&ExternalPort=443&InternalIp=192.168.1.4&Signature=X%2BZtHbTeKYf8xU%2FvWhPAmg%2B5scc%3D&
AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-
SHA1&Version=2014-05-26&IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=2c3f2573-209a-11e6-
be0f-2cf0ee28adf2&InternalPort=443
=====Request URL end=====

===== Got Response =====
{

```

```
"ForwardEntryId": "fwd-11cdhpljk",
"RequestId": "260A9673-5522-4F66-844A-1F1AB47CD21C"
}
[admin@tester:nat_gw_cli_tool]$
[admin@tester:nat_gw_cli_tool]$
[admin@tester:nat_gw_cli_tool]$
[admin@tester:nat_gw_cli_tool]$ python api.py CreateForwardEntry RegionId=cn-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.224.22.59 ExternalPort=22 InternalIp=192.168.1.5 InternalPort=22 IpProtocol=TCP
=====Request URL=====
https://ecs.aliyuncs.com/?ExternalIp=139.224.22.59&SignatureVersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A55%3A44Z&RegionId=cn-shanghai&ExternalPort=22&InternalIp=192.168.1.5&Signature=%2FZWf5%2ForHr%2BUR446eEBLC4LNYe8%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=39863cf3-209a-11e6-8f6d-2cf0ee28adf2&InternalPort=22
=====Request URL end=====

===== Got Response =====
{
"ForwardEntryId": "fwd-11iv34uj7",
"RequestId": "0884BC12-8EAD-4AAA-826E-30E5435D7C27"
}
```

查看已添加的DNAT规则

```
[admin@tester:nat_gw_cli_tool]$ python api.py DescribeForwardTableEntries RegionId=cn-shanghai ForwardTableId=ftb-11tc6xgmv
=====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A56%3A18Z&RegionId=cn-shanghai&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&Signature=x4%2B6oNYxIRBmND8rcIbJM9EJ8ts%3D&action=DescribeForwardTableEntries&SignatureNonce=4db93223-209a-11e6-81eb-2cf0ee28adf2
=====Request URL end=====

===== Got Response =====
{
"ForwardTableEntries": {
"ForwardTableEntry": [
{
"ExternalIp": "139.224.22.107",
"ExternalPort": "any",
"ForwardEntryId": "fwd-119smw5tk",
"ForwardTableId": "ftb-11tc6xgmv",
"InternalIp": "192.168.1.1",
"InternalPort": "any",
"IpProtocol": "any",
"Status": "Available"
},
{
"ExternalIp": "139.224.22.79",
"ExternalPort": "443",
"ForwardEntryId": "fwd-11cdhpljk",
"ForwardTableId": "ftb-11tc6xgmv",
```

```

"InternalIp": "192.168.1.4",
"InternalPort": "443",
"IpProtocol": "tcp",
"Status": "Available"
},
{
"ExternalIp": "139.224.22.55",
"ExternalPort": "any",
"ForwardEntryId": "fwd-11dz3ly9l",
"ForwardTableId": "ftb-11tc6xgmv",
"InternalIp": "192.168.1.2",
"InternalPort": "any",
"IpProtocol": "any",
"Status": "Available"
},
{
"ExternalIp": "139.224.22.59",
"ExternalPort": "22",
"ForwardEntryId": "fwd-11iv34uj7",
"ForwardTableId": "ftb-11tc6xgmv",
"InternalIp": "192.168.1.5",
"InternalPort": "22",
"IpProtocol": "tcp",
"Status": "Available"
},
{
"ExternalIp": "139.224.22.79",
"ExternalPort": "80",
"ForwardEntryId": "fwd-11r23r7p5",
"ForwardTableId": "ftb-11tc6xgmv",
"InternalIp": "192.168.1.3",
"InternalPort": "80",
"IpProtocol": "tcp",
"Status": "Available"
}
]
},
"PageNumber": 1,
"PageSize": 10,
"RequestId": "C84FDDCF-8550-4024-B89C-01E7459D7CF9",
"TotalCount": 5
}

```

增加公网IP个数

当用户需要更多公网IP时，可以在共享带宽包中增加公网IP个数，并为这些新增加的公网IP添加DNAT规则。

假设用户现在需要的公网IP个数从5个变成了6个，则使用下面的CLI命令：

```

[admin@test:~]$ python api.py AddBandwidthPackageIps RegionId=cn-shanghai
BandwidthPackageId=bwp-11odxu2k7 IpCount=6
====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&BandwidthPackageId=bwp-
11odxu2k7&Format=json&TimeStamp=2016-05-23T03%3A58%3A18Z&RegionId=cn-

```

```
shanghai&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&Signature=pSjC98nbDGgMI1tdjcXARIfW6t0%3D&action=AddBandwidthPackageIps&SignatureNonce=955c7d
70-209a-11e6-907e-2cf0ee28adf2&IpCount=6
=====Request URL end=====

===== Got Response =====
{
  "RequestId": "EC0B5C51-7F40-44D6-A642-1DE764B547EC"
}
```

执行成功后，可以通过DescribeBandwidthPackages来查看当前带宽包中的IP信息：

```
[admin@testernat_gw_cli_tool]$ python api.py DescribeBandwidthPackages RegionId=cn-shanghai
NatGatewayId=ngw-112za33e4
=====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&Format=json&TimeStamp=2016-05-
23T03%3A58%3A53Z&RegionId=cn-shanghai&NatGatewayId=ngw-
112za33e4&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&Signature=OnVBAnWbJKF7G5JAQRd44QhMJMo%3D&action=DescribeBandwidthPackages&SignatureNonce=
aa42a599-209a-11e6-92cc-2cf0ee28adf2
=====Request URL end=====

===== Got Response =====
{
  "BandwidthPackages": {
    "BandwidthPackage": [
      {
        "Bandwidth": "150",
        "BandwidthPackageId": "bwp-11odxu2k7",
        "BusinessStatus": "Normal",
        "CreationTime": "2016-05-23T03:26:24Z",
        "Description": "",
        "InstanceChargeType": "PostPaid",
        "InternetChargeType": "PayByBandwidth",
        "IpCount": "6",
        "Name": "",
        "NatGatewayId": "ngw-112za33e4",
        "PublicIpAddresses": {
          "PublicIpAdresse": [
            {
              "AllocationId": "nateip-1110a2l48",
              "IpAddress": "139.224.22.118"
            },
            {
              "AllocationId": "nateip-11iopy3sl",
              "IpAddress": "139.224.22.107"
            },
            {
              "AllocationId": "nateip-11pt1f9ph",
              "IpAddress": "139.224.22.55"
            },
            {
              "AllocationId": "nateip-111ul670c",
              "IpAddress": "139.224.22.79"
            }
          ]
        }
      }
    ]
  }
}
```

```
{
  "AllocationId": "nateip-11ogfjj85",
  "IpAddress": "139.224.22.59"
},
{
  "AllocationId": "nateip-11s2jempe",
  "IpAddress": "139.224.22.99"
}
],
},
"RegionId": "cn-shanghai",
"Status": "Available",
"ZoneId": "cn-shanghai-a"
}
]
},
"PageNumber": 1,
"PageSize": 10,
"RequestId": "EBF26EA4-15E9-44B6-B3EB-8111507321E9",
"TotalCount": 1
}
```

减少公网IP个数

当用户需要减少一些公网IP时，可以在共享带宽包中去除指定的公网IP。去除公网IP前，需要确保该IP没有被DNAT规则引用。如果有引用，需要先删除相应的DNAT规则，再去除公网IP。

假设用户现在要去掉两个指定的公网IP，CLI命令和回复信息如下：

```
[admin@tester:nat_gw_cli_tool]$ python api.py RemoveBandwidthPackageIps RegionId=cn-shanghai
BandwidthPackageId=bwp-11odxu2k7 RemovedIpAddresses.1=nateip-1110a2l48 RemovedIpAddresses.2=nateip-
11s2jempe
=====Request URL=====
https://ecs.aliyuncs.com/?RemovedIpAddresses.2=nateip-
11s2jempe&SignatureVersion=1.0&BandwidthPackageId=bwp-11odxu2k7&Format=json&TimeStamp=2016-05-
23T04%3A01%3A34Z&RegionId=cn-shanghai&RemovedIpAddresses.1=nateip-
1110a2l48&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&Signature=l4NbMQD5X1xkLrgBZm34Aj4uwiI%3D&action=RemoveBandwidthPackageIps&SignatureNonce=0a
34f3f3-209b-11e6-b183-2cf0ee28adf2
=====Request URL end=====

===== Got Response =====
{
  "RequestId": "7D275A59-1EB0-4775-8A20-2A47055EAC5C"
}
```

临时增减带宽

随着业务压力的变化，用户在某些时候需要增减自己购买的带宽。

下面的CLI命令，将共享带宽包上的带宽从150Mbps升级到200Mbps。

```
[admin@tester:nat_gw_cli_tool]$ python api.py ModifyBandwidthPackageSpec RegionId=cn-shanghai
BandwidthPackageId=bwp-11odxu2k7 Bandwidth=200
=====Request URL=====
https://ecs.aliyuncs.com/?SignatureVersion=1.0&BandwidthPackageId=bwp-
11odxu2k7&Format=json&TimeStamp=2016-05-23T04%3A03%3A08Z&RegionId=cn-
shanghai&Bandwidth=200&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014-05-
26&Signature=tozPphaDTYvhOI%2Bw%2FJjw7WaPn70%3D&action=ModifyBandwidthPackageSpec&SignatureNon
ce=42429561-209b-11e6-b869-2cf0ee28adf2
=====Request URL end=====

===== Got Response =====
{
  "RequestId": "079874CD-AEC1-43E6-AC03-ADD96B6E4907"
}
```

高可用的SNAT网关

概述

在一份IT系统中，往往存在一些服务器需要主动访问互联网，但又出于安全性考虑需要避免这些服务器持有公网IP而暴露在公网上。这就需要该IT系统中的网关设备提供SNAT功能。

本文介绍如何利用NAT网关的SNAT功能来满足这样的需求。

关于价格与费用

NAT网关和共享带宽包都是收费产品。具体收费方式和价格见价格总揽。

本文档中所使用的购买页截图中，价格显示为0，是因为编写文档使用的账号有特殊设置。

请用户在依照本文档进行操作时，确保对购买页上给出的报价有所了解后再进行购买。

前期准备

了解SNAT功能的设计

请阅读相关文档，了解NAT网关的SNAT功能设计，特别是SNAT表和SNAT规则的含义和效果。

NAT网关-SNAT功能介绍

部署规划

假设我们的系统中有许多ECS，部署在同一个VPC的两个不同的VSwitch下；其中：

- VSwitch1下的ECS实例都需要主动访问互联网；
- VSwitch2下的ECS实例都不需要主动访问互联网；
- 所有这些需要靠SNAT主动访问互联网的ECS实例，out方向（从阿里云数据中心流向互联网）总带宽需求大约为10Mbps。

那么，整体资源规划如下：

带宽需求总量：10Mbps
公网IP需求总量：1个；

VPC与ECS的准备

创建VPC与ECS，配置成如下图中所示的状态。本文档中使用的环境，如下面几张图所示。

注意，这些ECS实例不需要公网IP。



The screenshot shows the '专有网络基本信息' (VPC Basic Information) page in the Alibaba Cloud Management Console. The page displays the following details:

专有网络基本信息		
名称: -	ID: vpc-v32oacbu4	状态: 可用
地域: 华东2	网段: 172.16.0.0/12	创建时间: 2016-07-05 22:39:41
默认专有网络: 否	备注: -	

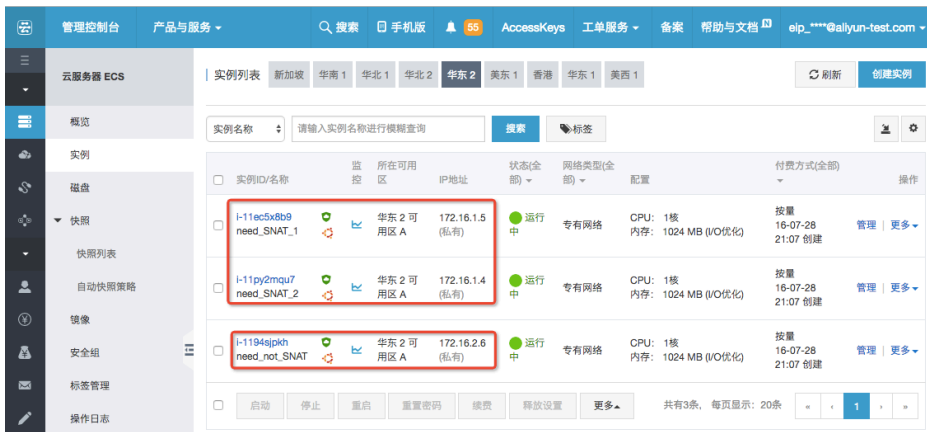
资源部署信息		
ECS实例: 3	SLB实例: -	交换机: 2
安全组: 1	NAT网关: -	



The screenshot shows the '交换机列表' (VSwitch List) page in the Alibaba Cloud Management Console. The page displays a table of VSwitches:

交换机ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-3cs5x25r1 need_not_SNA...	1	172.16.2.0/24	可用	华东2 可用区 A	251	2016-07-28 20:37:47	否		编辑 删除 创建实例
vsw-702g90io7 need_SNAT	2	172.16.1.0/24	可用	华东2 可用区 A	250	2016-07-28 20:37:32	否		编辑 删除 创建实例

共有2条，每页显示：10条



操作步骤

创建NAT Gateway

在当前VPC中创建一个NAT网关，并在该NAT网关上放置一个共享带宽包，其中包含10Mbps的带宽和1个公网IP；

进入VPC控制台，点击左侧导航中的"NAT网关"，进入NAT网关的管理界面。

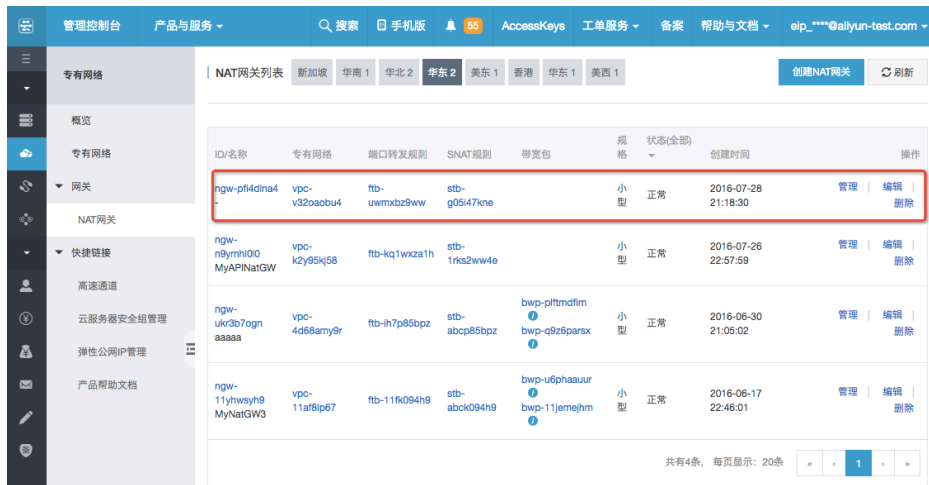
然后，点击右上角的"创建NAT网关"按钮，进入NAT网关选购界面。



按照您的需要进行参数设定。其中，关于NAT网关的规格，会影响SNAT功能的最大连接数和每秒新建连接数。不同规格下的具体参数，参见NAT网关-SNAT功能介绍



创建完成后，回到NAT网关管理界面，可以看到刚刚创建成功的NAT网关。



添加共享带宽包

NAT网关想要正常工作，需要在其上配置公网IP和公网带宽。NAT网关上的公网IP和公网带宽被封装成共享带宽包。一个共享带宽包由一份带宽和一组IP构成，这些IP共享这份带宽。

点击刚才创建的NAT网关，进入NAT网关详情页。

点击左侧导航中的"带宽包"，进入NAT网关上的带宽包管理界面。

点击"购买带宽包"，进入共享带宽包选配界面。



按照刚才的规划来设定需要的参数：1个公网IP，10Mbps的带宽。点击"立即购买"，完成共享带宽包的创建。

共享带宽包(按量付费)

地域: 华北 2 (北京) 华东 1 (杭州) 香港 华南 1 (深圳) 华东 2 (上海) 亚太 (新加坡) 美西 (硅谷) 美东 (弗吉尼亚)

NAT网关ID: ngw-tc7vja15r

公网IP个数: 1

带宽: 1250Mbps 2500Mbps 5000Mbps 10 Mbps

线路类型: BGP (多线)

计费方式: 按带宽计费

计费周期: Day(按天)

购买数量: 1

购买清单 0例

当前配置

地域: 华东 2 (上海)

公网IP个数: 1

带宽: 10

线路类型: BGP (多线)

计费方式: 按带宽计费

计费周期: 1天

购买数量: 1

配置费用: ￥0.00/天

原价¥34.08/天 省¥34.08/天

共享带宽包 0折优惠

共享带宽包 0折优惠

立即购买 加入清单

回到NAT网关上的带宽包管理界面，可以看到刚才创建的共享带宽包。

管理控制台 产品与服务 搜索 手机版 AccessKeys 工单服务 备案 帮助与文档 eip_****@aliyun-test.com

ngw-pf4dlna4带宽包

带宽包ID: bwp- 删除

带宽 10M IP数量 1个

购买带宽包

基本信息

带宽包ID: bwp-pqht1crp8l	名称:	地域: 华东 2
可用区: cn-shanghai-b	状态: 可用	关联网关ID: ngw-pf4dlna4
线路类型: BGP	描述:	

付费信息

实例付费方式: 后付费	创建时间: 2016-07-28 21:21:30	ISP: BGP
网络计费类型: 按带宽计费	带宽: 10 MB	

公网IP列表

公网IPID	公网IP地址	操作
nateip-t1vy7ephe	139.224.36.188	释放

配置SNAT规则

在NAT网关详情界面，点击左侧导航的"SNAT表"，进入SNAT配置界面。

管理控制台 产品与服务 搜索 手机版 AccessKeys 工单服务 备案 帮助与文档 eip_****@aliyun-test.com

ngw-pf4dlna4 SNAT表

创建SNAT条目 刷新

基本信息

端口转发表ID: ttb-uwmxbz9ww	NAT网关ID: ngw-pf4dlna4	创建时间: 2016-07-28 21:18:30
------------------------	-----------------------	---------------------------

SNAT条目列表

SNAT条目ID	源网段	交换机ID	外部IP地址	状态	操作
查询不到相关的记录					

点击右上角的"创建SNAT条目", 打开SNAT规则创建界面。

选择需要使用SNAT功能的ECS所在的交换机, 并选择为其分配的SNAT所使用的公网IP。点击确定, 完成规则创建。



回到SNAT配置界面, 可以看到刚才创建的SNAT规则



到此, 该VSwitch下的ECS实例已经可以经由NAT网关的SNAT能力访问互联网了。

验证SNAT效果

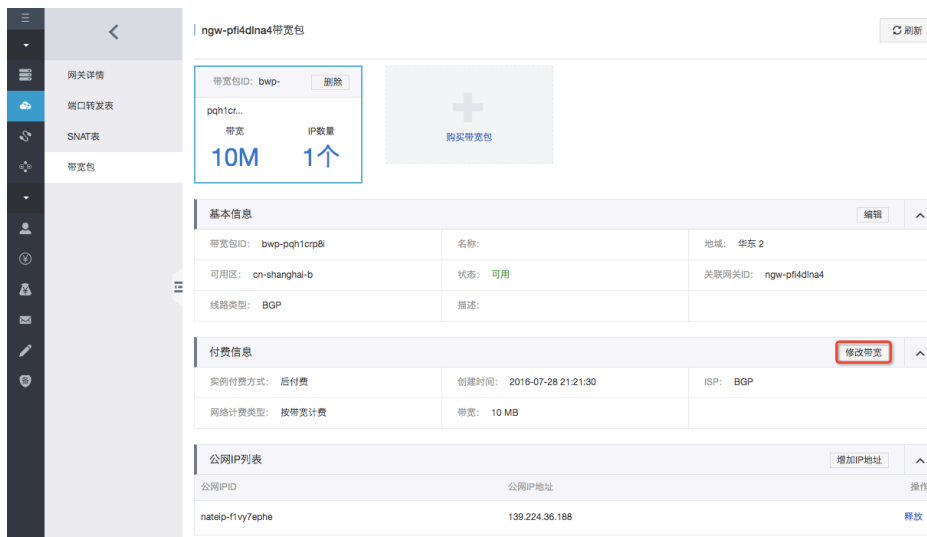
登录需要SNAT能力的ECS实例, 访问互联网内容, 验证SNAT效果。

需要注意的是, ECS实例向互联网发起的网络通信, 也会经由安全组进行ACL检查。如有需要, 请修改相应的ECS实例所关联的安全组的具体规则, 确保相应的访问被放行。

修改带宽/增加IP

如果您需要调整共享带宽包的带宽, 或者为共享带宽包增加IP, 您需要对共享带宽包进行配置变更。

在NAT网关的带宽包管理界面, 点击"修改带宽"或者"增加IP", 进入共享带宽包的变更配置界面。



ngw-pf4dina4带宽包

带宽包ID: bwp-... 删除

带宽: 10M IP数量: 1个 购买带宽包

基本信息 编辑

带宽包ID: bwp-pqh1crp8i	名称:	地域: 华东 2
可用区: cn-shanghai-b	状态: 可用	关联VPC ID: ngw-pf4dina4
线路类型: BGP	描述:	

付费信息 修改带宽

实例付费方式: 后付费	创建时间: 2016-07-28 21:21:30	ISP: BGP
网络计费类型: 按带宽计费	带宽: 10 MB	

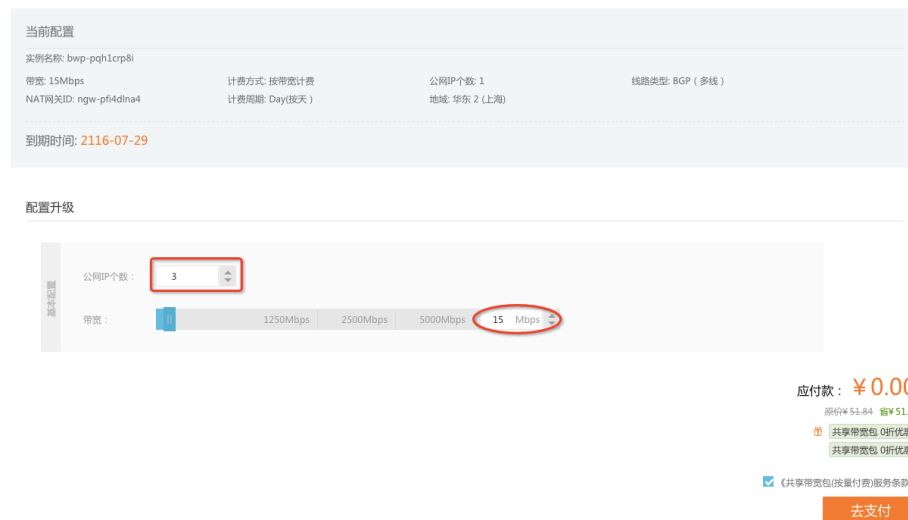
公网IP列表 增加IP地址

公网IP ID	公网IP地址	操作
nateip-f1vy7ephe	139.224.36.188	释放

按照实际需要修改带宽值和IP个数，完成带宽修改。

注意：当您只需要修改其中一个值时，务必确保另外一个值也设置为您实际需要的值，避免误操作。

共享带宽包(按量付费)



当前配置

实例名称: bwp-pqh1crp8i

带宽: 15Mbps 计费方式: 按带宽计费 公网IP个数: 1 线路类型: BGP (多线)

NAT网关ID: ngw-pf4dina4 计费周期: Day(按天) 地域: 华东 2 (上海)

到期时间: 2116-07-29

配置升级

公网IP个数: 3

带宽: 1250Mbps 2500Mbps 5000Mbps 15 Mbps

应付款: ¥0.00

原价¥51.84 省¥51.84

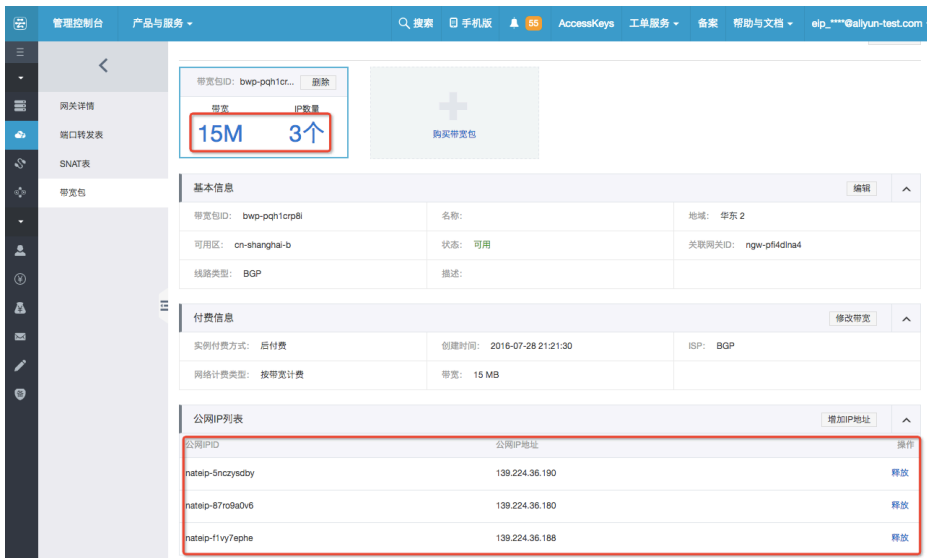
共享带宽包 0折优惠

共享带宽包 0折优惠

☒ 《共享带宽包(按量付费)服务条款》

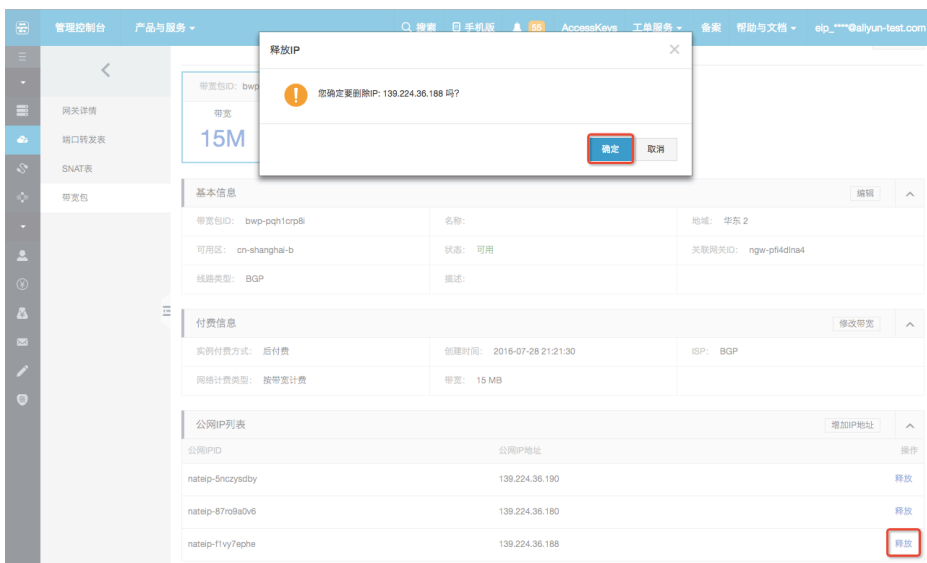
去支付

回到带宽包管理界面，可以看到配置变更后的共享带宽包参数。如果参数没有发生变化，请您等待一分钟再刷新界面。



移除IP

如果您需要减少共享带宽包中的IP，可以在共享带宽包的管理界面，找到钥匙房的IP，点击其“释放”按钮，即可完成操作。



自建SNAT网关平滑迁移到NAT网关

概述

在VPC中搭建一个SNAT网关，可以实现无公网IP的ECS实例安全的访问互联网。

用户可以选择使用ECS实例自己搭建SNAT网关（如何自建SNAT网关），也可以使用NAT网关的SNAT功能（

最佳实践-高可用的SNAT网关)。相比而言，后一种方案比前一种方案有更好的可用性和性能。

如果已经在VPC中基于ECS搭建了SNAT网关，又想将架构切换为基于NAT网关实现SNAT，需要先将原有自建SNAT网关拆除，再进行NAT网关的创建和配置。这样的操作会导致SNAT功能中断一段时间。

本文提供一种操作方法，可以利用路由表的一些特性（主要是“最长匹配原则”），实现自建SNAT网关和NAT网关的无缝切换。切换过程中，不会出现SNAT功能不可用，仅在切换的一瞬间发生已有TCP连接的断开，只需应用进行重连即可；

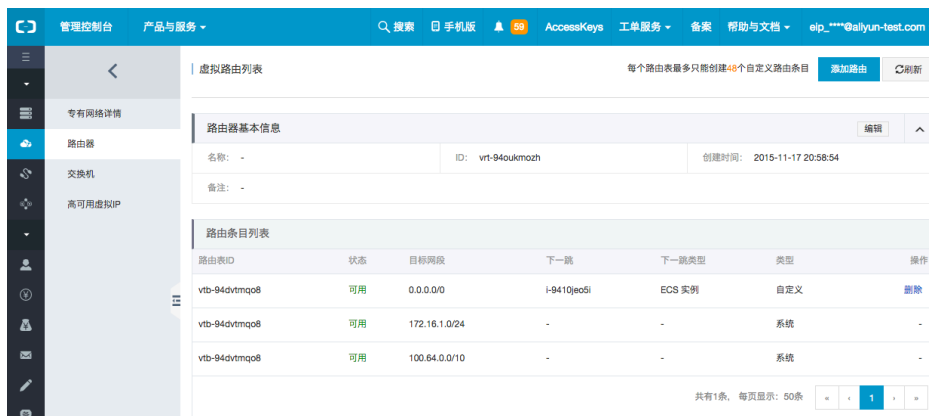
环境

当前VPC中有两个ECS实例：

- i-9410jeo5i为自建的SNAT网关；这台ECS上绑定了一个EIP，并且开启了转发服务、配置了iptables规则以实现SNAT转发；
- i-94kjwn5ds为需要SNAT功能来访问互联网的服务器；



当前VPC的路由器上，添加了一条自定义路由，将公网访问请求转发给i-9410jeo5i；



操作步骤

添加8条路由，对原有路由进行覆盖

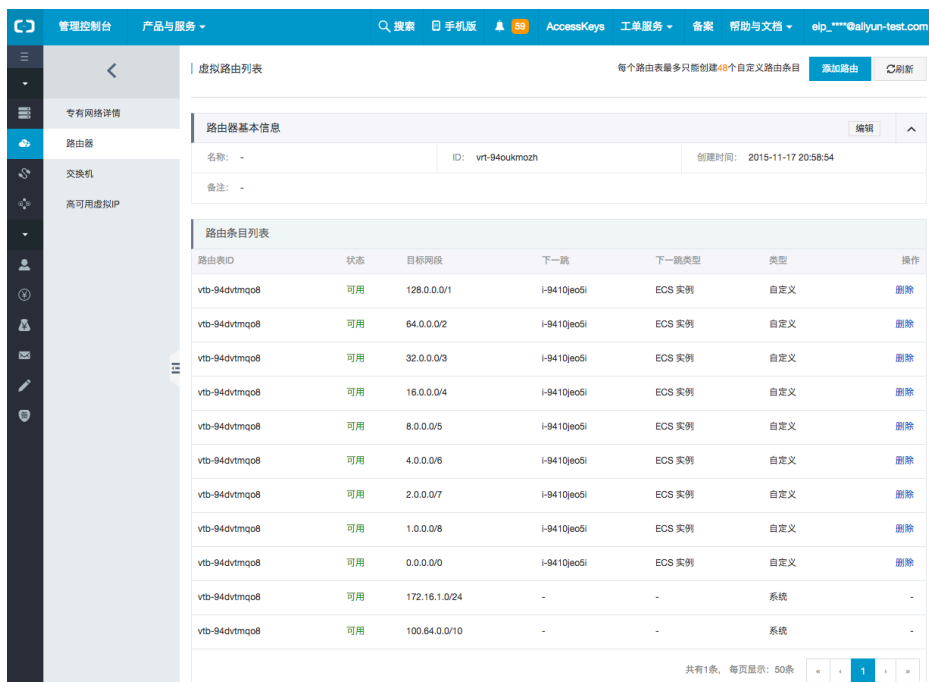
添加8条路由，目的CIDR分别为

1.0.0.0/8;2.0.0.0/7;4.0.0.0/6;8.0.0.0/5;16.0.0.0/4;32.0.0.0/3;64.0.0.0/2;128.0.0.0/1;下一跳均为i-

9410jeo5i.

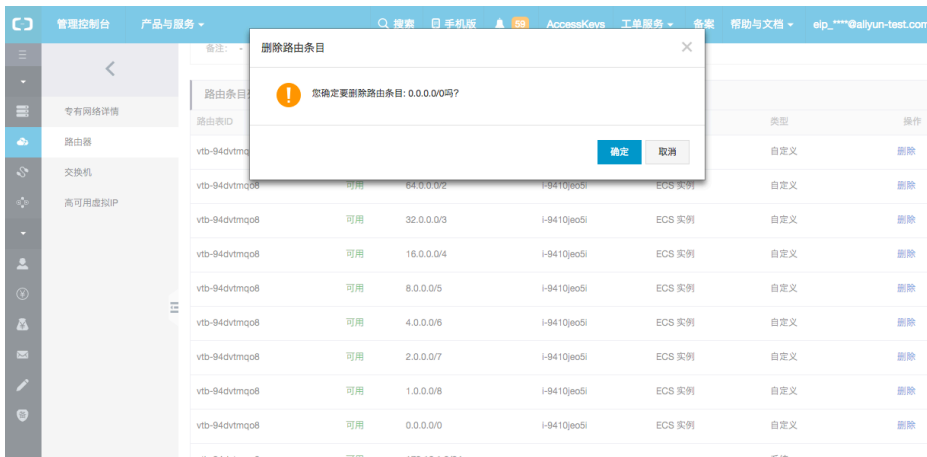


配置结果如下图所示：



由于路由表按照"最长匹配原则"，会优先匹配子网掩码最长的路由条目；而去往任意IP地址的数据包，都会匹配到这8条中的一条；因此，0.0.0.0/0这条路由实际上已经不再有用了。

删除目的地址段为0.0.0.0/0的路由



创建NAT网关

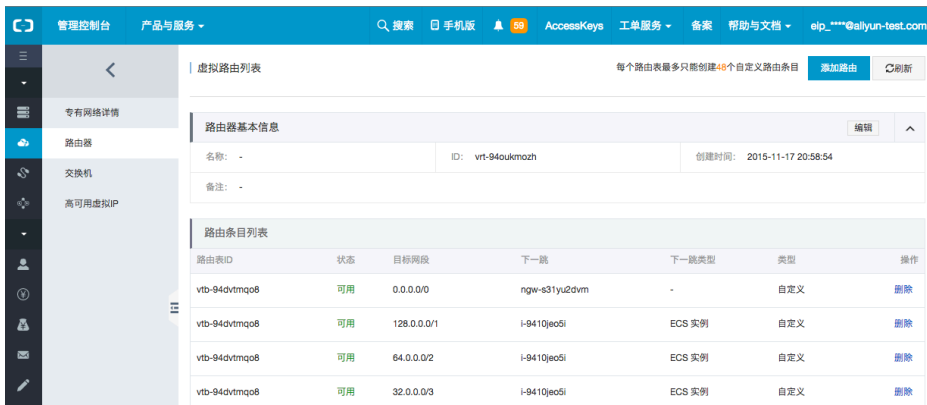
在该VPC中创建NAT网关。



创建出的NAT网关如图所示：

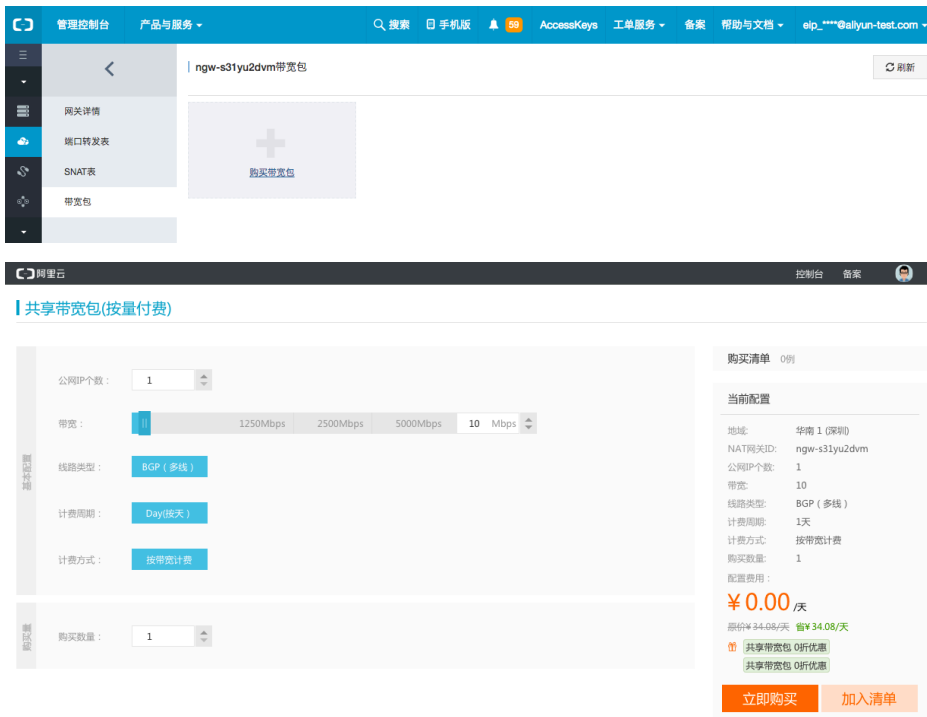


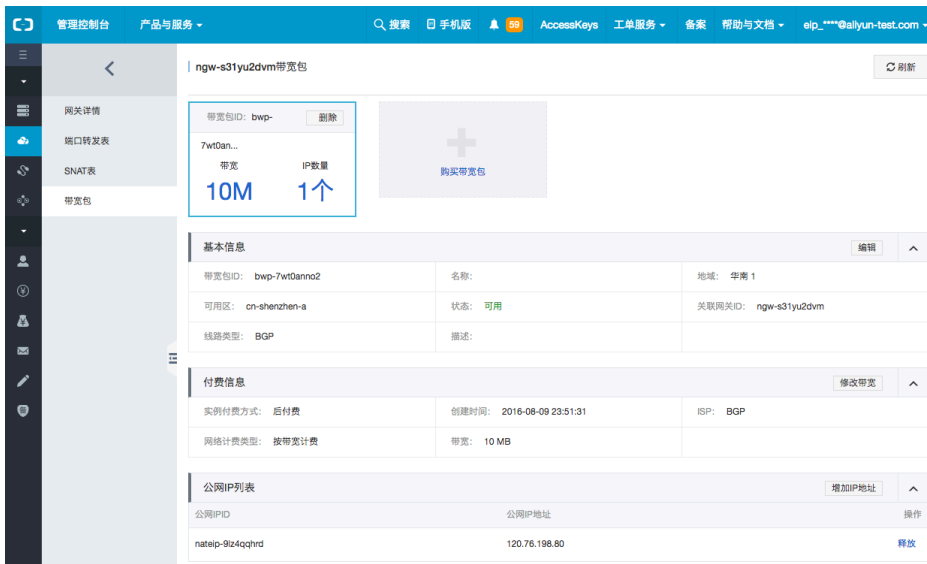
创建NAT网关时，系统会自动添加一条0.0.0.0/0的路由，指向NAT网关



为NAT网关配置公网IP与带宽

在NAT网关上创建一个公网带宽包，为NAT网关配置公网IP与带宽。



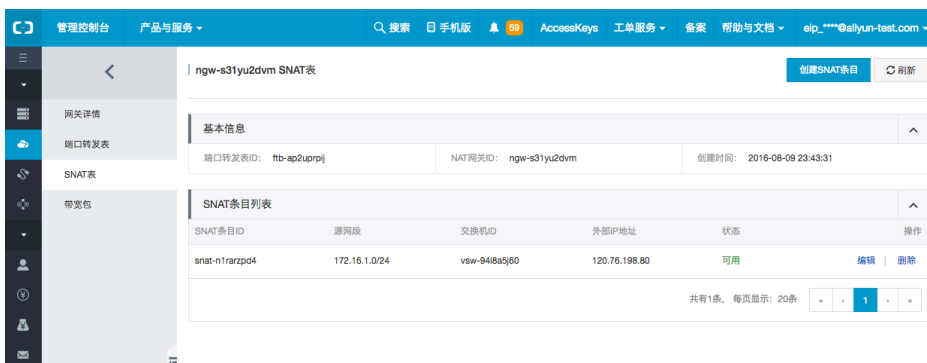


在NAT网关上配置SNAT规则

在NAT网关的控制台上，进入"SNAT表"管理界面，添加SNAT规则；交换机ID是需要SNAT功能的ECS所属的交换机的ID；外部IP地址 是NAT网关上执行SNAT转换时使用的公网IP地址。



添加出的SNAT规则如图所示：

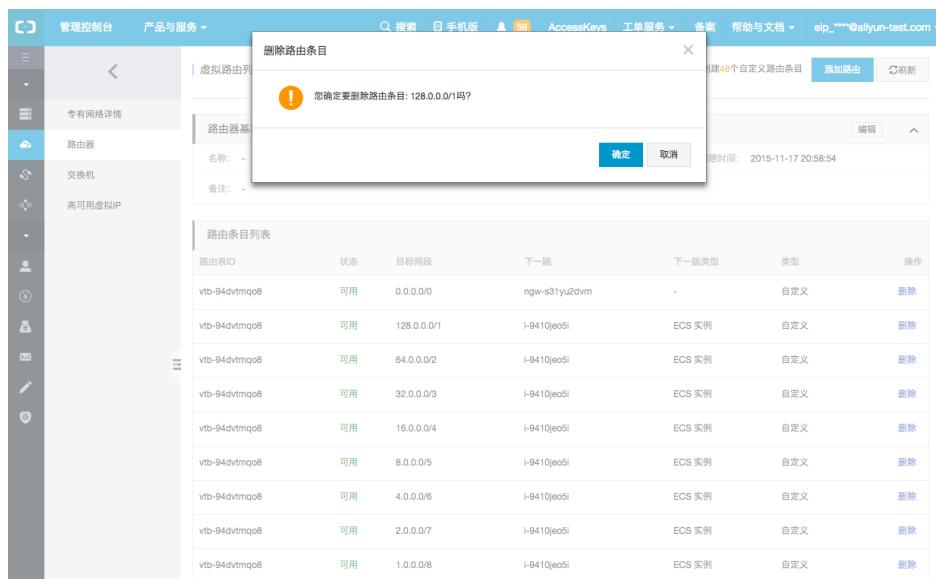


至此，NAT网关上SNAT相关的所有配置已经完成，NAT网关已经开始对收到的所有公网访问请求进行SNAT转换；但是，由于指向NAT网关的路由的优先级较低，因而没有数据包被转发到NAT网关上

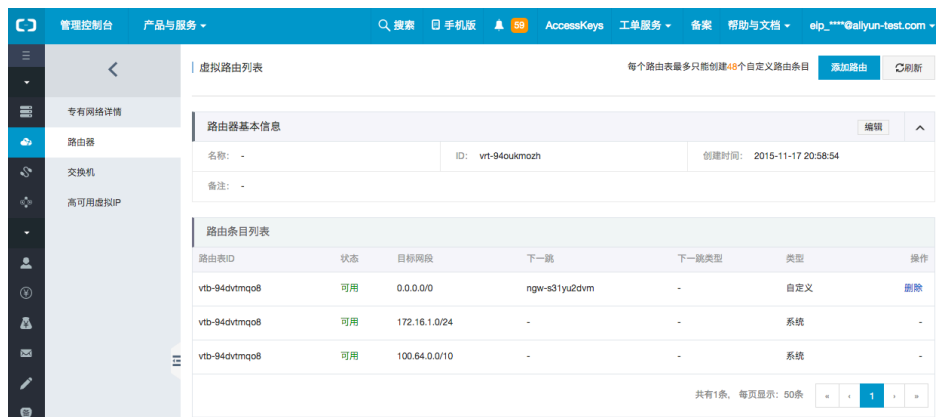
去除之前添加的八条路由，启用NAT网关

删除之前添加的八条指向i-9410jeo5i的明细路由，让路由器把公网访问请求不再转发给自建SNAT，而是转发

给NAT网关。



八条路由全部删除后，路由表中的内容如图所示：



至此，已经完成了从自建SNAT网关到使用官方NAT网关的SNAT功能的全部切换流程。

配置

专有网络环境做端口映射

应用场景

VPC环境下只想购买少量的EIP，但是后端内网主机有多台需要对外提供服务，想通过端口映射的方式，将绑定

EIP主机的端口映射到后端内网主机上。

操作步骤

1.将EIP绑定到某台ECS上，然后通过EIP登陆SSH，登陆成功如下图所示。

```
Xshell:\> ssh root@112.112.112.71

Connecting to 112.112.112.71:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Welcome to aliyun Elastic Compute Service!

[root@iZ9476537g0Z ~]#
[root@iZ9476537g0Z ~]#
[root@iZ9476537g0Z ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:00:04:A3
          inet addr:172.16.3.2  Bcast:172.16.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9315 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5474 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12280455 (11.7 MiB)  TX bytes:355941 (347.5 KiB)
          Interrupt:165

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@iZ9476537g0Z ~]#
```

2.开启这台ECS的IP转发功能。

```
sed -i 's/net.ipv4.ip_forward = 0/net.ipv4.ip_forward = 1/g' /etc/sysctl.conf
```

让IP转发生效

```
sysctl -p
```

```
[root@iZ9476537g0Z ~]# sysctl -p
net.ipv4.ip_forward = 1
```

3.iptables 添加DNAT转换规则

添加转发规则，访问EIP的80端口的所有请求，都转给172.16.3.1(另一台机器的ECS IP)处理

```
iptables -t nat -I PREROUTING -p tcp --dport 80 -j DNAT --to 172.16.3.1
```

使转发数据包实现"双向通路"，给数据包设置一个正确的返回通道：

```
iptables -t nat -I POSTROUTING -p tcp --dport 80 -j MASQUERADE
```

4.测试是否可以访问了。

访问EIP，最终访问到了172.16.3.1服务器上的页面。



说明:DNAT不用单独添加路由，二者同时添加的话有冲突，需要更精细的路由控制。

通过安全组对专有网络类型的ECS进行公网访问控制

应用场景

专有网络VPC下ECS如果绑定了EIP，并且需要限制某些IP访问某些端口，可以直接在安全组的内网入方向进行控制。

比如限制服务器3389远程端口方法。

在没有限制的情况下，通过netstat -an|findstr :3389可以查看到123.114.113.18的客户端已经通过IP连接上了VPC的服务器。



操作步骤

1.登陆云服务器管理控制台，选择相应的地域。

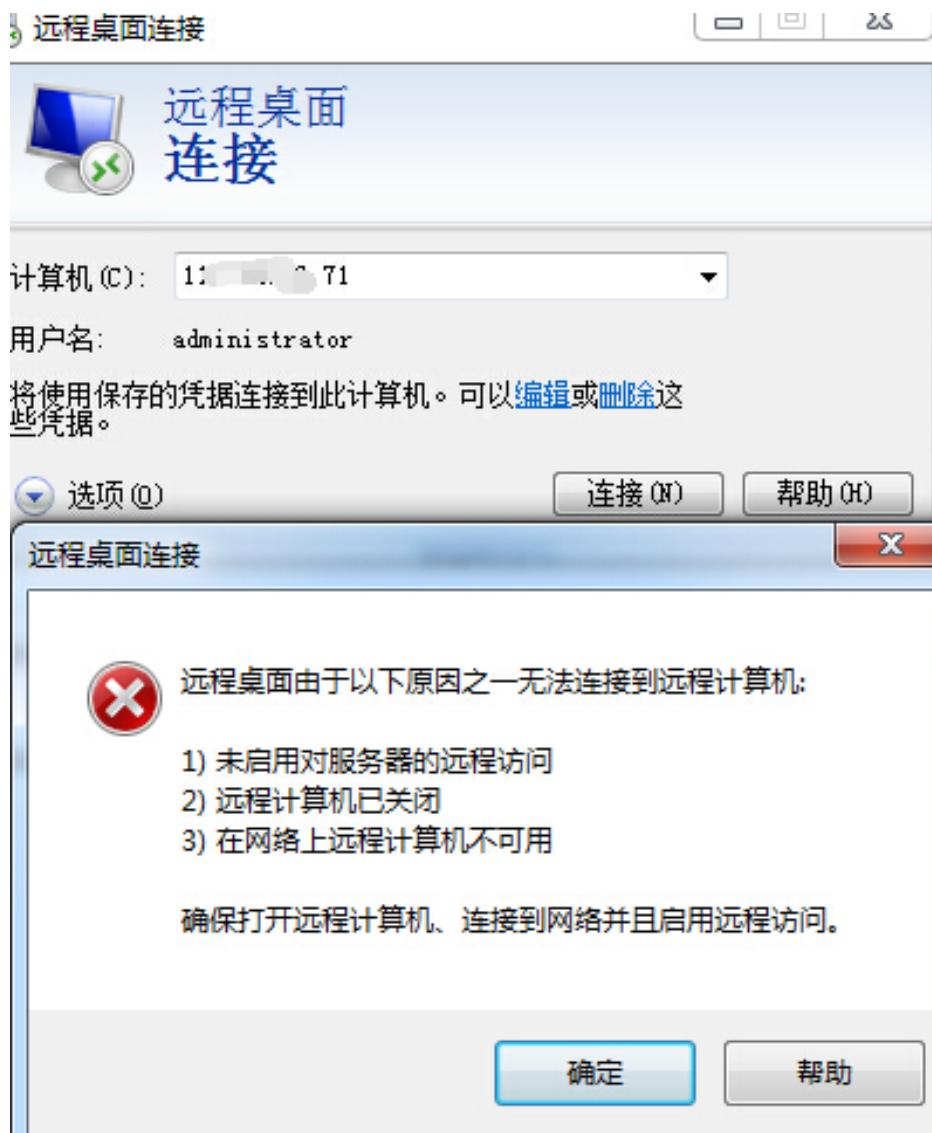
2.在ECS控制台中这台实例的安全组规则中添加一条规则，协议类型和端口范围选择需要的，本例是TCP 3389端口。

添加安全组规则
×

网卡类型：	内网
规则方向：	入方向
授权策略：	拒绝
协议类型：	TCP
* 端口范围：	3389/3389 取值范围为1~65535；例如“1/200”、“80/80”。
授权类型：	地址段访问
授权对象：	123.114.113.18
优先级：	1 优先级可选范围为1-100，默认值为1，即最高优先级。

确定
取消

3.设置安全组后，再次通过EIP连接服务器测试已经无法连接。



专有网络中云服务器修改交换机或者私网IP的方法

应用场景

- 专有网络下的ECS支持更换接入交换机，但是更换交换机后，ECS的IP也会有变化。
- 专有网络内的服务器需要更换私网IP地址。

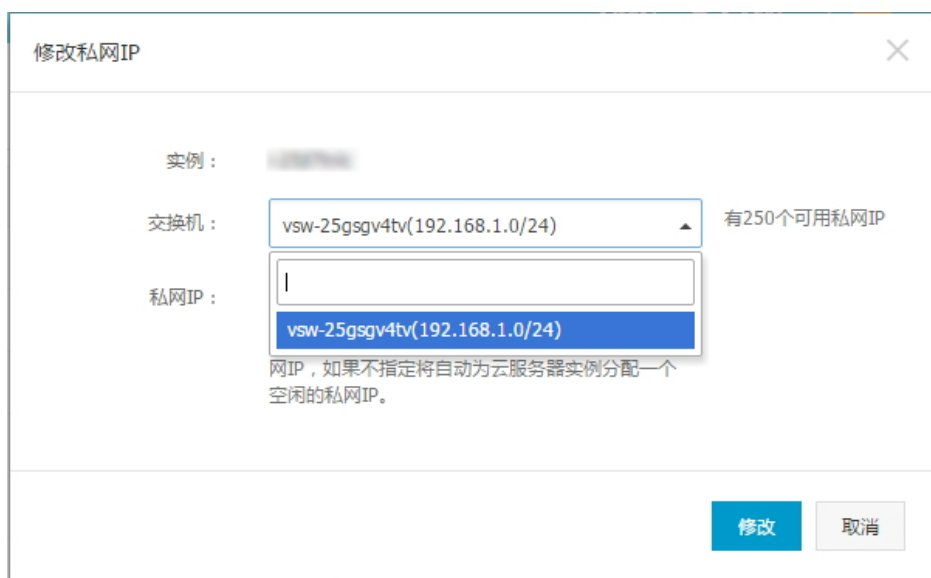
操作步骤

1. 登陆云服务器管理控制台，选择相应的地域。

2. 关闭该ECS，使ECS状态为停止状态。
3. 点击右侧的"管理"，进入"基本信息"页面。
4. 找到"配置信息"版块，点击右侧的"更多"按钮。



5. 然后在弹出"修改私网IP"的配置页面里选择要接入的交换机，用户根据需要修改私网IP地址，如果不修改系统会自动分配一个地址。



6. 点 <修改> 后，把ECS启动后就生效了。
- 说明：因为VPC下的每个交换机都是独立的一个网段，所以更换交换机后，ECS的IP也随之更改。

专有网络的ECS使用公网负载均衡

应用场景

- 经典网络类型的负载均衡实例具有公网IP地址，可以加专有网络类型的ECS实例。

- 不能使用经典网络类型私网IP的负载均衡加专有网络类型的ECS。

操作步骤

1. 创建经典网络的公网负载均衡实例。

负载均衡SLB开通 申请更高配置

① 若网站用于 Web 访问，请及时备案。私网实例不提供备案服务。请注意：添加经典网络的公网负载均衡实例仍会按小时收取租用费，如暂时不用可暂停需费释放。

地域： 华北 1 (青岛) 华东 1 (杭州) **华北 2 (北京)** 香港 华南 1 (深圳) 华东 2 (上海)

不同地域之间的产品内网不互通；订购后不支持更换地域，请谨慎选择 [教我选择>>](#) [查看我的产品地域](#) [各区域黑网触发规则>>](#)

可用区类型： **多可用区**

单可用区指实例只在一个可用区存在；多可用区指实例在两个可用区存在，当主可用区不可用时会在备可用区恢复服务。

主备可用区： 华北 2 可用区 A 华北 2 可用区 B

主可用区是当前承载流量的可用区，备可用区默认不承载流量；主可用区不可用时才承载流量 [教我选择>>](#)

网络类型： **经典网络** 专有网络 [教我选择>>](#)

实例类型： **公网** 私网

公网带宽： **按使用流量计费** 按固定带宽计费 [教我选择>>](#)

开通即按使用流量计费，停止或释放实例才不会产生流量费用

配置清单 0台

当前配置

地域： 华北 2 (北京)

网络： 经典网络

实例： 公网

购买量： 1台

配置费用：
¥0.02/时

公网流量费用：
¥0.80/GB

立即购买 **加入清单**

数量： 1 台

2. 在"实例管理"页面，选择开通实例右侧的"管理"链接。

3. 点击左侧导航的"服务器"，选择"未添加服务器"页签，点击"添加"链接添加专有网络的ECS。

说明：不支持同时添加经典网络和专有网络的ECS到同一个负载均衡实例。

4. 可以在"已添加的服务器"页签查看添加的服务器。

esolution [返回负载均衡实例列表](#) [使用限制和注意事项](#)

负载均衡服务实例 所在地域：华北 2 (北京) 可用区：华北 2 可用区 B (主)

已添加的服务器 未添加的服务器

云服务器ID [搜索](#) [刷新](#)

云服务器ID/名称	可用区	公网/内网IP地址	状态(全部)	网络类型(全部)	付费方式	健康检查状态	权重	操作
i-25sawv8l santtypc	华北 2 可用区 A	10.0.1.1 (私有)	运行中	专有网络 (vpc-25s8qkwb)	包年包月	(暂无法监听)	100	移除

[批量移除](#) [修改权重](#)

共有1条，每页显示：20条

专有网络下内网隔离设置

应用场景

通过配置安全组规则，使得同一专有网络下的三个交换机两两不能访问。

前提条件

- 三个交换机创建在同一个专有网络下。
- 已经创建三个交换机，网段分别为172.16.1.0/16、172.16.2.0/16、172.16.3.0/16。
- 创建在同一个路由器下面，默认是可以互相访问的。

操作步骤

1. 首先创建三个安全组，为了方便分辨，可以用网段命名，选择所属专有网络。

云服务器 ECS	安全组列表	亚太 (新加坡)	华南 1 (深圳)	华北 1 (青岛)	华北 2 (北京)	华东 2 (上海)	华东 1 (香港)	华东 1 (杭州)	美国 (硅谷)	刷新	创建安全组
快速	专有网络ID	请输入专有网络ID进行查询									搜索
实例	安全组ID/名称	所属专有网络	相关实例	网络类型	创建时间	描述	标签	操作			
快速	sg-25jy5oy3	vpc-25jy5oy3	0	专有网络	2016-03-29 15:47:39	System created s...		修改	管理实例	配置规则	
快速列表	sg-3547f00v		1	经典网络	2016-03-15 21:17:27	-	ros-aliyun-creat...	修改	管理实例	配置规则	
自助快照策略	sg-3547f00v		2	经典网络	2016-03-15 19:33:46	-		修改	管理实例	配置规则	
镜像	sg-3547f00v		1	经典网络	2016-03-15 19:04:58	-		修改	管理实例	配置规则	
安全组	sg-3547f00v		0	经典网络	2016-03-15 19:02:46	-		修改	管理实例	配置规则	
标签管理											

创建安全组

* 安全组名称：

s172.16.1.0

长度为2-128个字符，以大小写字母或中文开头，可包含数字，"，"，"_"或"-"

描述：

172.16.1.0/16

长度为2-256个字符，不能以http://或https://开头。

网络类型：

专有网络

* 专有网络：

请选择专有网络

st

172.16.1.0/16

确定

取消

2. 在"安全组列表"页面，选择某一实例的 **配置规则** 链接，进入"安全组规则"页面。

3. 首先添加一个 允许 0.0.0.0网段访问，优先级可以设置100，优先级数字越小，优先级越高。

添加安全组规则

网卡类型：

内网

规则方向：

入方向

授权策略：

允许

协议类型：

全部

* 端口范围：

-1/-1

取值范围为1~65535；例如“1/200”、“80/80”。

授权类型：

地址段访问

授权对象：

0.0.0.0/0

优先级：

100

优先级可选范围为1-100，默认值为1，即最高优先级。

确定

取消

4.再添加规则，禁止 172.16.2.0/16网段访问，优先级数字设置小一点，优先级会高于第一个。

添加安全组规则



网卡类型：	内网
规则方向：	入方向
授权策略：	拒绝
协议类型：	全部
* 端口范围：	-1/-1 取值范围为1~65535；例如“1/200”、“80/80”。
授权类型：	地址段访问
授权对象：	172.16.2.0/16
优先级：	90 优先级可选范围为1-100，默认值为1，即最高优先级。

确定

取消

5.使用同样的方法，填写拒绝 172.16.3.0/16 网段。

说明：如果这个VPC下只有这三个网段，通过如上设置，相当于网段 172.16.2.0/16 、 172.16.3.0/16 是不能访问172.16.1.0/16 的。

想要设置两两网段不能互相访问，需要再在另外两个安全组里填写如上规则。

专有网络类型的实例通过内网连接OSS的方式

VPC目前还不支持直接创建OSS实例，如果VPC用户需要访问OSS，可以通过域名进行访问，具体有哪些域名可参考VPC网络下Region和Endpoint对照表。

VPC中的RDS切换到不同的网段使用应用场景

在VPC里有两个交换机，分别为172.16.0.0/24和172.18.0.0/24两个网段。RDS挂接在172.16.0.0/24网络，现在想把RDS连接到172.18.0.0/24的交换机上是否可以，怎么操作。

注意事项

- 切换IP会导致RDS的闪断。
- RDS白名单是需要添加新的IP地址。
- 请设置好连接RDS程序的自动重连机制。

操作步骤

1. 登陆RDS控制台。
2. 在左侧导航选择"实例列表"，进入"云数据库管理"页面。



3. 选择相应的实例，点击右侧的"管理"链接，进入"基本信息"页面。
4. 在左侧导航选择"数据库连接"，进入相应的页面。
5. 点击<切换为经典网络>，并点击<确定>，完成切换。



6. 点击<切换为专有网络>，弹出"切换为专有网络"对话框。

切换为专有网络

RDS 实例将切换到专有网络，请选择网络类型：

VPC: VPC2(192.168.0.0/16)

虚拟交换机：VS-3(192.168.1.0/24)

如需其他专有网络或者虚拟交换机， [到控制台创建](#)

注：切换后，经典网络下的ECS将无法访问专有网络下的RDS

确定

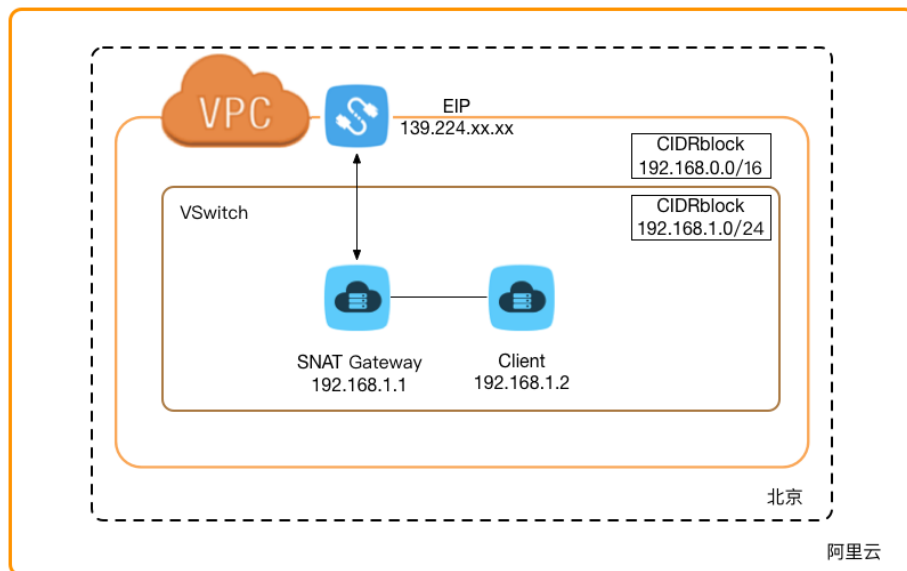
取消

7.选择相应的交换机，点击<确定>即可。

在专有网络中搭建SNAT网关

应用场景

专有网络环境下，没有公网IP地址的云服务器ECS实例，可以通过一台绑定了EIP的ECS实例访问公网。如下图所示。



假如Client ECS不能访问公网，ping www.aliyun.com 失败。下文告诉用户如何操作可以让Client ECS上公网。

数据规划

- SNAT GW ECS的规格参数举例如下。

条目	参数
地域	华东2
可用区	华东2 可用区B
I/O优化实例	I/O优化实例
实例规格	1核1GB
网络类型	专有网络
虚拟交换机ID	vsw-11xxj71x8
操作系统	Ubuntu 14.04 64位
系统盘	40GB高效云盘

- Client ECS的规格参数举例如下。

条目	参数
地域	华东2
可用区	华东2 可用区B
I/O优化实例	I/O优化实例
实例规格	1核1GB
网络类型	专有网络
虚拟交换机ID	vsw-11xxj71x8
操作系统	Ubuntu 14.04 64位
系统盘	40GB高效云盘

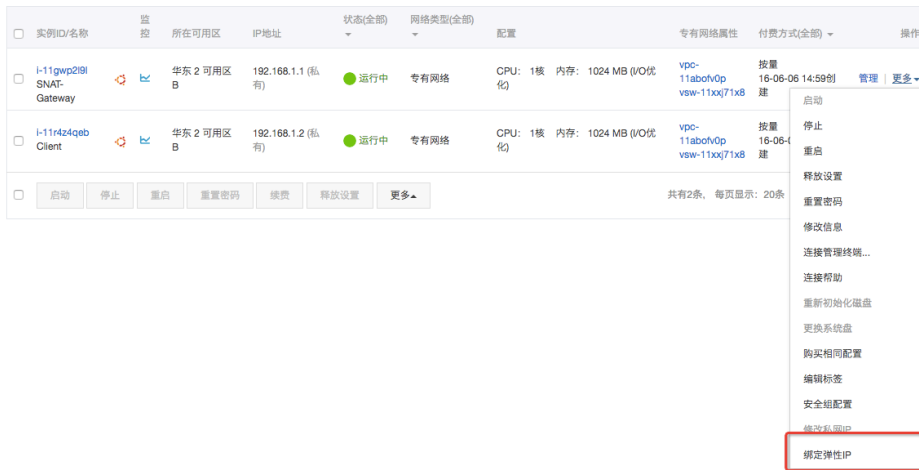
环境准备

- 1.创建一个VPC实例，具体操作可以参考创建专有网络实例。
- 2.创建一个VSwitch，具体操作请参考创建交换机。
- 3.创建EIP实例，具体操作请参考申请弹性公网IP。
- 4.创建ECS实例，具体操作可参考创建ECS实例。

说明：ECS各参数的选择，可以参考数据规划部分的配置。

操作步骤

- 1.将SNAT网关的ECS绑定EIP。



2.SNAT网关可以访问公网。

```
root@i211gwp2l9l2:~# ping www.aliyun.com
PING www-adns.aliyun.com.gds.alibabadns.com (42.156.220.114) 56(84) bytes of data:
64 bytes from 42.156.220.114: icmp_seq=1 ttl=47 time=4.98 ms
64 bytes from 42.156.220.114: icmp_seq=2 ttl=47 time=5.02 ms
64 bytes from 42.156.220.114: icmp_seq=3 ttl=47 time=5.02 ms
64 bytes from 42.156.220.114: icmp_seq=4 ttl=47 time=5.11 ms
64 bytes from 42.156.220.114: icmp_seq=5 ttl=47 time=5.02 ms
64 bytes from 42.156.220.114: icmp_seq=6 ttl=47 time=5.06 ms
```

3.配置Iptables。

a.打开iptables forward功能。

```
cd /etc/
```

```
vim sysctl.conf
```

b.添加 net.ipv4.ip_forward = 1

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

c.使用如下命令把192.168.1.0/24发出的包的源地址替换为192.168.1.1。

```
iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j SNAT -to-source 192.168.1.1
```

4.添加路由。

把发往0.0.0.0/0网段的包，发送给SNAT网关 (i-11gwp2l9l)。

添加路由

目标网段:

0.0.0.0/0

下一跳类型:

ECS 实例

下一跳ECS实例:

i-11gwp2l9l

确定

取消

路由表ID	状态	目标网段	下一跳	下一跳类型	类型	操作
vrb-11w6hqm0	可用	0.0.0.0/0	i-11gwp2l9l	ECS 实例	自定义	删除

5.登陆Client ECS，验证是否可以ping www.aliyun.com 成功。

```

[2]~ stopped ping www.aliyun.com
root@i21lr4z4qeb2:~# ping www.aliyun.com
PING www-adns.aliyun.com.gds.alibabadns.com (140.205.63.8) 56(84) bytes of data.
64 bytes from 140.205.63.8: icmp_seq=1 ttl=51 time=3.53 ms
64 bytes from 140.205.63.8: icmp_seq=2 ttl=51 time=2.18 ms
64 bytes from 140.205.63.8: icmp_seq=3 ttl=51 time=2.07 ms
64 bytes from 140.205.63.8: icmp_seq=4 ttl=51 time=2.08 ms
64 bytes from 140.205.63.8: icmp_seq=5 ttl=51 time=2.06 ms
64 bytes from 140.205.63.8: icmp_seq=6 ttl=51 time=2.10 ms
64 bytes from 140.205.63.8: icmp_seq=7 ttl=51 time=2.11 ms

```

安全性

VPC的安全性

VPC通过安全隔离的方式保证了数据传输的安全性。

安全隔离的详细描述如下：

不同用户的云服务器在不同的VPC里；

不同VPC之间通过隧道ID进行隔离。VPC内部由于虚拟交换机和虚拟机路由器的存在，所以可以像传统网络环境一样划分子网，每一个子网内部的不同云服务器使用同一个虚拟交换机互联，不同子网间使用虚拟路由器互联；

不同VPC之间内部网络完全隔离，只能通过对外映射的IP（弹性IP和NAT IP）互联；

由于使用隧道封装技术对云服务器的IP报文进行封装，所以云服务器的数据链路层（二层，mac地址）信息不会进入物理网络，实现了不同云服务器间二层网络隔离，因此也实现了不同VPC间二层网络隔离；

VPC内的ECS使用安全组防火墙进行三层网络访问控制。

访问控制

专有网络支持各个云产品实例的访问控制机制。

产品	链接
ECS	安全组
RDS	白名单
SLB	白名单

网络

专有网络和交换机

专有网络和交换机

专有网络

专有网络是用户基于阿里云创建的自定义私有网络, 不同的专有网络之间彻底逻辑隔离, 用户可以在自己创建的专有网络内创建和管理云产品实例, 比如ECS, SLB, RDS等。

专有网络管理：

- 在创建专有网络时，用户需要以CIDRBlock的形式指定专有网络内使用的私网网段
- 专有网络创建之后，用户需要继续创建交换机(VSwitch)，然后才能够在专有网络内创建云产品实例(ECS, SLB, RDS)
- 创建专有网络时，需要指定CIDRBlock。当新建VPC实例的状态变成Available之后，表示VPC创建成功，可以进行下一步的管理操作
- 删除指定的专有网络，必须首先删除专有网络内所有的云产品实例(包含安全组、交换机、云产品实例、路由条目等)

专有网络网段：

- 关于CIDRBlock的相关信息，请参见维基百科上的Classless Inter-Domain Routing条目说明
- 专有网络创建成功之后，CIDRBlock无法修改，建议使用比较大的网段作为VPC的CIDRBlock(比如直接使用192.168.0.0/16和172.16.0.0/12以及10.0.0.0/8 3个网段)，尽量避免后续扩容。系统不会根据VPC的CIDRBlock来创建系统路由，所以使用比较大的地址范围来创建VPC，不会影响业务的正常使用

交换机

交换机，是组成VPC网络的基础网络设备。它可以连接不同的云产品实例。在VPC网络内创建云产品实例的时候，必须指定云产品实例所在的交换机。

交换机管理：

- 只有当VPC的状态为Available时，才能创建新的交换机
- 交换机不支持并行创建，一个交换机创建成功之后，才能够创建下一个
- 交换机创建完成之后，无法修改CIDRBlock
- 删除交换机之前，必须先删除目标交换机所连接的云产品实例

交换机网段：

- 创建交换机时，需要指定一个CIDRBlock
- 新建交换机所使用的CIDRBlock必须从属于交换机所在的VPC的CIDRBlock
- 新建交换机所使用的CIDRBlock不能与已经存在的交换机的CIDRBlock冲突
- 新建交换机所使用的CIDRBlock不能包含已经存在的自定义路由的目标网段

创建专有网络

通过控制台可以对专有网络进行创建。

注意事项

在创建专有网络时，用户需要以CIDRBlock的形式指定专有网络内使用的私网网段。

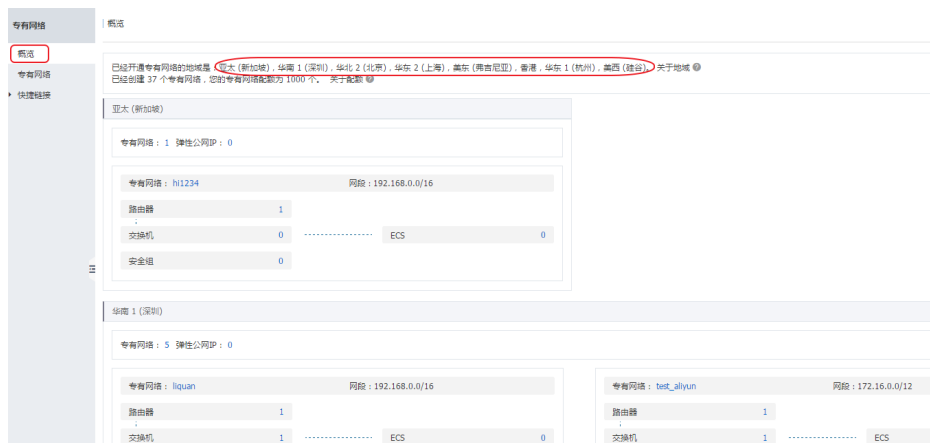
专有网络创建之后，您需要继续创建交换机(VSwitch)，然后才能够在专有网络内创建云产品实例(ECS、SLB、RDS)。

- 创建专有网络时，需要指定CIDRBlock。当新建VPC实例的状态变成Available之后，表示VPC创建成功，可以进行下一步的管理操作。

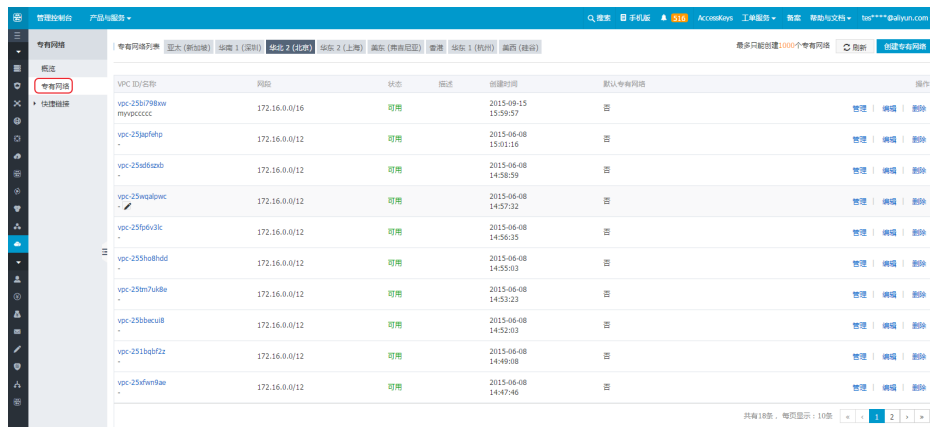
操作步骤

1. 打开阿里云专有网络 (VPC) 控制台<https://vpc.console.aliyun.com/#/overview/resources>。
2. 在页面的最上面了解已经开通专有网络的地域，并了解了用户自己要创建的专有网络的地域。

说明：因为实例无法在不同地域的专有网络中启动，所以请确保后续操作在相同的地域中。



3.在左侧导航选择"专有网络", 进入专有网络列表页。



4.在最上面的"专有网络列表"中选择地域。例如选择地域"北京"。说明：本文以地域"北京"为例。

5.选择右上角的按钮"创建专有网络", 弹出"创建专有网络"的窗口。

创建专有网络

*专有网络名称：

名称为2-128个字符，以大写字母或中文开头，可包含数字，"_"或"-"

描述：

描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

*网段：

192.168.0.0/16

① 一旦创建成功，网段不能修改

确定

取消

6.在配置页面上的"专有网络名称"（例如：helloVPC）、"描述"、"网段"(例如：192.168.0.0/16)输入相应的内容。

- 专有网络名称：这个帮助用户在创建专有网络和子网后以便在控制台识别。
- 描述：可选，用户可根据自身习惯填写，以便后续更好的在控制台识别。
- 网段：有三个选项192.168.0.0/16、172.16.0.0/12、10.0.0.0/8。

7.当创建的专有网络"状态"为"可用"时，完成专有网络的创建。

专有网络	专有网络列表 亚太（新加坡） 华东1（深圳） 华北2（北京） 华东2（上海） 华南1（香港） 香港（香港） 美国（硅谷） 欧洲（伦敦）					最多只能创建1,000个专有网络	刷新	创建专有网络
快速创建	VPC ID/名称	网段	状态	描述	创建时间	默认专有网络	操作	
	vpc-25b798xw myvpcccc	172.16.0.0/16	可用		2015-08-15 15:59:57	否	管理	编辑 删除
	vpc-25jefpfp	172.16.0.0/12	可用		2015-08-08 15:01:16	否	管理	编辑 删除
	vpc-25a6isob	172.16.0.0/12	可用		2015-08-08 14:58:59	否	管理	编辑 删除
	vpc-25eqabwec	172.16.0.0/12	可用		2015-08-08 14:57:32	否	管理	编辑 删除
	vpc-25p6v3lc	172.16.0.0/12	可用		2015-08-08 14:56:35	否	管理	编辑 删除
	vpc-259no8hdd	172.16.0.0/12	可用		2015-08-08 14:55:03	否	管理	编辑 删除

修改专有网络信息

应用场景

用户可以通过修改专有网络名称和描述信息，以便在专有网络列表中方便管理。

操作步骤

1.登陆专有网络控制台。

- 2.在左侧导航选择"专有网络", 进入"专有网络列表"页面。
- 3.选择某一实例, 点击右侧的 **编辑**按钮, 弹出"编辑专有网络"对话框。
- 4.用户根据自身需要, 对专有网络进行重命名, 并可以增加描述信息进行说明。

查看专有网络信息

应用场景

用户需要了解所部署的专有网络的基本信息, 及资源部署相关信息, 可以通过控制台进行查看。

操作步骤

- 1.登陆专有网络控制台。
- 2.在左侧导航选择"专有网络", 进入"专有网络列表"页面。
- 3.选择某一实例, 点击右侧的 **管理**按钮, 进入"专有网路基本信息"页面。
- 4.用户根据在此页面查看专有网络的基本信息以及资源部署信息。

具体查看信息项有：

- 名称
- ID
- 状态
- 地域
- 网段
- 创建时间
- 备注
- ECS实例
- SLB实例
- 交换机
- 安全组

删除专有网络

用户不再维护该专有网络, 可以通过控制台删除该专有网络。

注意事项

删除指定的专有网络, 必须首先删除专有网络内所有的云产品实例 (包含安全组、交换机、云产品实例、路由条目等)。

操作步骤

- 1.打开专有网络控制台, <https://vpc.console.aliyun.com/#/overview/resources>。
- 2.选择左侧导航的"专有网络", 选择地域北京下的专有网络列表。

3.选择待删除的VPC，点击<删除>。

专有网络	专有网络列表	亚太（新加坡）	华南1（深圳）	华北2（北京）	华东2（上海）	华东1（香港）	华东1（杭州）	美国（硅谷）
快速创建	VPC ID/名称	网段	状态	描述	创建时间	默认专有网络	管理	删除
	vpc-25b798xw myvpc0000	172.16.0.0/16	可用		2015-09-15 15:59:57	否		
	vpc-25jafahp haliyvp2	172.16.0.0/12	可用		2015-06-08 15:01:16	否		删除
	vpc-25af6zob	172.16.0.0/12	可用		2015-06-08 14:58:59	否		

4.弹出"删除专有网络"确认对话框，点击<确定>，完成专有网络的删除。

创建交换机

通过控制台可以对交换机进行创建。

注意事项

只有当VPC的状态为Available时，才能创建新的交换机。

交换机不支持并行创建，一个交换机创建成功之后，才能够创建下一个。

交换机创建完成之后，无法修改CIDRBlock。

操作步骤

1.打开阿里云专有网络控制台，<https://vpc.console.aliyun.com/#/overview/resources>。

2.选择左侧导航的"专有网络"，选择地域北京下的专有网络列表。

专有网络	专有网络列表	亚太（新加坡）	华南1（深圳）	华北2（北京）	华东2（上海）	华东1（香港）	华东1（杭州）	美国（硅谷）
快速创建	VPC ID/名称	网段	状态	描述	创建时间	默认专有网络	管理	删除
	vpc-25b798xw myvpc0000	172.16.0.0/16	可用		2015-09-15 15:59:57	否		
	vpc-25jafahp -	172.16.0.0/12	可用		2015-06-08 15:01:16	否	管理	删除
	vpc-25af6zob	172.16.0.0/12	可用		2015-06-08 14:58:59	否		

3.选择某个专有网络，点击"操作"下面的"管理"，进入"专有网络基本信息"页面。

<	专有网络基本信息	编辑专有网络	删除
路由表	专有网络基本信息	ID: vpc-25jafahp	状态: 可用
交换机	名称: haliyvp2	网段: 172.16.0.0/12	创建时间: 2015-06-08 15:01:16
	地域: 华北2（北京）	默认专有网络: 否	备注: -
	资源部署信息		
	ECS实例: 2	SLB实例: 3	交换机: 1
	安全组: 1		

4.在左侧导航选择"交换机"，进入"交换机列表"页面。

交换机列表

一个专有网络最多只能创建24个交换机

交换机ID	交换机名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-25n3gmd9fddda		2	192.168.1.0/24	可用	华北2 可用区 A	245	2015-08-14 11:59:23	否	ddd	编辑 删除 创建实例

共有1页，每页显示：10条

5. 点击右上角的"创建交换机"，弹出"创建交换机"窗口。

- 名称：本文命名为VS-1，便于用户查看即可。
- 专有网络：默认，不可编辑。创建专有网络时自动生成。
- 专有网络网段：默认，不可编辑。创建专有网络时自动生成。
- 可用区：地域中有哪些可用区，会呈现在下拉列表中，用户根据规划进行选择即可。
- 网段：例如填192.168.1.0/24。
- 可用IP数：系统自动计算。
- 描述：用户根据自身需要填写，以便后续方便查看。

创建交换机
 ✕

***名称：**

名称为2-128个字符，以大写字母或中文开头，可包含数字，"_"或"-"

***专有网络：**

专有网络网段：

***可用区：**

① 创建后无法修改

***网段：**

① 创建后无法修改

必须等于或属于该专有网络的网段，网段掩码必须在16和29之间。

例如：192.168.1.0/24

可用IP数： 0 个

描述：

描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

确定

取消

6.填写完成上述信息，点击<确定>，完成交换机的创建。

修改交换机信息

应用场景

用户可以通过在控制台修改交换机的名称及描述信息，方便交换机的管理。

操作步骤

- 1.登陆专有网络控制台。
- 2.在左侧导航选择"专有网络"，进入"专有网络列表"页面。
- 3.选择相应地域下某一VPC实例，点击右侧的 **管理**，进入"专有网络基本信息"页面。
- 4.在左侧导航选择"交换机"，进入"交换机列表"页面。
- 5.选择相应交换机，点击右侧的"编辑"，弹出"编辑交换机"对话框。
- 6.用户按照需要修改交换机名称及描述信息，点击 **提交**即可。

删除交换机

应用场景

用户不再需要该交换机。

注意事项

删除交换机之前，必须先删除目标交换机所连接的云产品实例

操作步骤

- 1.打开专有网络控制台，<https://vpc.console.aliyun.com/#/overview/resources>。
- 2.选择左侧导航的"专有网络"，选择地域北京下的专有网络列表。



VPC ID/名称	网段	状态	描述	创建时间	默认专有网络	操作
vpc-25b1798aw myvpc0000	172.16.0.0/16	可用		2015-09-15 15:59:57	否	管理 编辑 删除
vpc-25b1798aw helloVPC2	172.16.0.0/12	可用		2015-06-08 15:01:16	否	管理 编辑 删除
vpc-25b1798aw -	172.16.0.0/12	可用		2015-06-08 14:58:59	否	管理 编辑 删除

- 3.选择某行VPC，点击"操作"下面的"管理"，进入"专有网络基本信息"页面。

- 4.在左侧导航选择"交换机"，进入"交换机列表"页面。



交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-25b1798aw VSW2	2	172.16.1.0/24	可用	华北2 可用区 A	245	2015-06-14 11:59:23	否	ddd	编辑 删除

5. 点击<删除>，弹出"删除交换机"确认对话框。

说明：确保交换机下的ECS实例已经释放，否则需要先释放相应的ECS实例。

6. 点击<确定>，删除该交换机。

创建专有网络类型的云产品实例

用户可以通过专有网络控制台创建云产品实例。

注意事项

在专有网络内创建云产品实例的时候，必须指定云产品实例所在的交换机。

操作步骤

1. 登陆专有网络控制台。
2. 在左侧导航选择"专有网络"，进入"专有网络列表"页面。
3. 选择某地域下的某一实例，点击右侧的 **管理** 链接，进入"专有网络基本信息"页面。
4. 在左侧导航选择"交换机"，点击"操作"列下**创建实例**，在弹出的下拉菜单选择 **创建ECS实例**。

交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	描述	操作
vsw-23j873v1 VS-1	1	192.168.1.0/24	可用	cn-hangzhou-d	248	2015-07-28 22:47:09	hangzhou-DMZ	编辑 删除 创建实例
共有1条。每页显示：10条								

5. 在购买页面选择专有网络所在的地域、可用区，网络类型选择专有网络，并选择已经创建好的专有网络和交换机。

创建ECS实例的操作可以参考创建 Windows 系统实例或者创建 Linux 系统实例。

默认专有网络和默认交换机

背景信息

在提供默认专有网络功能之前，创建专有网络类型的云产品实例时，需要明确指定实例所属的专有网络或交换机，因此需要您首先了解专有网络的产品功能与使用方式，并于创建实例之前完成专有网络以及交换机的规划和创建。

为了简化专有网络类型的云产品实例的创建流程，阿里云提供了默认专有网络功能，在此基础上，创建云产品实例时不必再先行创建专有网络和交换机。当您选择将云产品实例创建在默认专有网络和默认交换机中时，阿里云会为您创建所需的默认专有网络用于创建云产品实例。

下面会进一步介绍默认专有网络和默认交换机的相关信息，如果您只希望在专有网络中使用云产品，不需要对专有网络本身进行规划和管理，可以跳过本节内容。跳过这些部分不会影响您对文档中其余部分的理解和使用。

。

客户价值

默认专有网络与默认交换机为您确定了您所使用专有网络实例时的一个唯一的默认网络位置，如果您创建云产品实例时没有明确指定实例所属的交换机，新实例就会创建在该唯一的默认网络位置中。如果某个云产品支持默认专有网络功能（如ECS），您在创建该云产品实例并选择网络类型为专有网络时，如果在售卖页选择默认专有网络和默认交换机，或在使用OpenAPI时未指定具体用于创建专有网络类型实例的交换机时，会根据您为云产品实例选择的区域和可用区，将该云产品实例创建在相应的默认专有网络和默认交换机中。

例如，在创建一个ECS时参数指定情况如下：

- 地域：北京
- 可用区：北京可用区A
- 网络类型：专有网络

此时，由于未指定具体的交换机，会选择北京地域的默认专有网络中可用区为北京可用区A的默认交换机用于创建ECS实例。

需要注意的是，即使您有已经创建的专有网络和交换机，在创建专有网络类型的云产品实例时，如果未指定具体的交换机，仍会将云产品实例创建在默认交换机中。如果您需要将云产品实例创建在非默认交换机中，请您在创建时务必指定正确的交换机。

使用限制

关于默认专有网络：

- 每个地域的默认专有网络唯一；
- 默认专有网络不占用阿里云为用户分配的专有网络配额；
- 默认专有网络由阿里云为您创建，您自行创建的均为非默认专有网络；
- 默认专有网络的CIDR为16位掩码的网段，如172.31.0.0/16，最多可提供65536个私有IP地址；
- 默认专有网络与非默认专有网络的操作方式与规格限制一致。

关于默认交换机：

- 每个可用区的默认交换机唯一；
- 默认交换机不占用专有网络中可创建交换机的配额；
- 默认交换机由阿里云为您创建，您自行创建的均为非默认交换机；
- 默认交换机只会创建在默认专有网络中；
- 默认交换机的CIDR为20为掩码的网段，如172.16.0.0/20，最多可提供4096个私网IP地址；
- 默认交换机与非默认交换机的操作方式与规格限制一致。

创建默认专有网络和默认交换机

默认类型的专有网络和交换机由阿里云为您按需创建，您无法主动创建默认专有网络和默认交换机，也无需关注该创建过程。当用户需要使用默认专有网络功能来创建云产品实例时：

- 若帐号中已经存在所需的默认专有网络和默认交换机，会将云产品实例创建在相应的默认交换机中；
- 若帐号中不存在所需的专有网络，会为您创建所需默认专有网络和默认交换机用于创建云产品实例；
- 若只有所需的默认专有网络，对应可用区的默认交换机尚未创建时，会为您在默认专有网络中创建所需默认交换机用于创建云产品实例。

删除默认专有网络和默认交换机

默认类型的专有网络和交换机支持删除操作，当您删除某地域的默认专有网络或某可用区的默认交换机后，再次需要在该地域或可用区使用默认类型的专有网络和交换机时，阿里云会为您再次创建。在默认专有网络中，其他云产品的使用方式与经典网络中的使用方式一致。具体使用请参考对应云产品的相关介绍。

查看默认专有网络和默认交换机

您可以通过控制台或专有网络 OpenAPI 中 DescribeVpcs 接口查看您的专有网络，其中在控制台标为"默认"或在 OpenAPI 查询结果中 IsDefault = true 的专有网络即默认专有网络。

您可以通过控制台或专有网络 OpenAPI 中 DescribeVSwitches 接口查看您的交换机，其中在控制台标为"默认"或在 OpenAPI 查询结果中 IsDefault = true 的交换机即默认交换机。

如果您的查询结果中没有默认专有网络或默认交换机，并不会影响您将云产品实例创建在默认专有网络中，阿里云会根据您的请求为您创建所需的默认专有网络或默认交换机。

API

专有网络相关接口：

- 新建专有网络
- 删除专有网络
- 查询专有网络列表
- 修改专有网络属性

交换机相关接口：

- 新建交换机
- 删除交换机
- 查询交换机列表
- 修改交换机属性

IP地址

IP 地址是用户访问云产品实例以及云产品实例对外提供服务的主要方式。当前使用专有网络时，会遇到私网 IP 和弹性公网 IP 两种类型的 IP 地址。

私网IP地址

私网IP是专有网络中的云产品实例在创建时会被分配专有网络中的私网IP地址，如专有网络类型云服务器ECS实例的私网IP、专有网络类型负载均衡实例的私网IP、专有网络类型云数据库实例的私网IP等。

与经典网络中私网IP地址由阿里云统一分配不同，专有网络的私网IP地址分配自实例所属交换机网段内，所以某个实例的私网IP地址在专有网络中唯一，分配给云产品实例的私网IP可以在该实例属性中查看。

私网IP地址可以用于专有网络中云产品的内网访问，如ECS实例之间内网互访、ECS实例与其他云服务（如OSS、RDS）之间内网互访、提供内网负载均衡服务等。

弹性公网IP地址

弹性公网IP，简称EIP，是可以独立购买和持有的公网IP地址资源，能动态绑定到不同的ECS实例上，绑定和解绑时无需停机。

弹性公网IP可以绑定到一台VPC类型的ECS实例上，可以使这台ECS实例具备公网通信的能力；您也可以根据您的需求进一步实现这些场景：

将这台ECS作为SNAT网关，为同VPC内其他实例提供公网访问能力

将这台ECS作为DNAT网关，使同VPC内其他实例可以面向公网提供服务

申请EIP

- 1.打开控制台<https://home.console.aliyun.com/#/>。
- 2.在导航栏或者主页面选择弹性公网IP。
- 3.点击右上角的按钮《申请弹性公网IP》。
- 4.在"弹性公网IP开通"页面，选择好地域、公网带宽、带宽峰值、购买数量，然后点击<立即购买>。
- 5.完成EIP服务的开通。

查看EIP流量

- 1.打开EIP控制台<https://ip.console.aliyun.com/#/eip/ap-southeast-1>。
- 2.在"弹性公网IP列表"选择某一实例。
- 3.点击"监控"列下的图标，弹出"网络监控信息"。
- 4.可以根据采样周期查看流量和带宽方面的监控信息。

修改EIP带宽

1. 打开EIP控制台<https://ip.console.aliyun.com/#/eip/ap-southeast-1>。
2. 在"弹性公网IP列表"选择某一实例。
3. 在"操作"列，点击"更多操作"，选择弹出的下拉菜单中的"修改带宽"。
4. 根据用户需求调整带宽峰值，并点击<确定变更>，完成带宽的调整。

将EIP与ECS绑定

1. 打开EIP控制台。
2. 在"弹性公网IP列表"选择某一实例。
3. 在"操作"列，选择"绑定"。
4. 选择要绑定的ECS实例，点击<确定>，完成EIP和ECS的绑定。

将EIP与ECS解绑

1. 打开EIP控制台。
2. 在"弹性公网IP列表"选择某一实例。
3. 在"操作"列，选择"解绑"。

释放EIP

1. 打开EIP控制台。
2. 在"弹性公网IP列表"选择某一实例。
3. 确保该实例的"状态"为"可用"。
4. 在"操作"列，点击"更多操作"，在下拉菜单选择"释放"即可。

API

网络相关接口：

- 申请弹性公网 IP
- 绑定弹性公网 IP
- 查询弹性公网 IP 列表
- 修改弹性公网 IP 属性
- 解绑弹性公网 IP
- 释放弹性公网 IP

监控相关接口：

- 查看弹性公网 IP 监控信息

修改专有网络类型ECS实例的私网IP地址

专有网络类型的ECS实例支持通过控制台或OpenAPI在专有网络内修改实例所属的交换机和私网IP地址。

管理控制台

1. 打开ECS控制台。
2. 确定要修改私网IP地址的ECS实例处于停止状态，若未停止请将其停止。
3. 在ECS"实例列表"中该实例所在行的"操作"列中点击"更多"，然后选择"修改私网IP"，或在该实例详情页内的配置信息栏中点击"更多"，然后选择"修改私网IP"。
4. 选择实例所属的交换机，指定所要修改的私网IP地址。如果未指定私网IP地址，会自动分配一个所指定交换机网段中未被使用的IP地址作为该实例的私网IP地址。

API

通过OpenAPI调用修改实例VPC属性接口可以实现。

实例相关接口：

修改实例VPC属性

路由器和路由表

核心概念

路由器

路由器是一个专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接VPC内的各个交换机，同时也是连接VPC与其他网络的网关设备。每个路由器中维护一张路由表，它会根据具体的路由条目的设置来转发网络流量。

产品约束

- 每个VPC有且只有一个路由器
- 路由器不支持BGP和OSPF等动态路由协议

路由器管理

- 创建VPC时，系统会自动为每个VPC创建1个路由器
- 删除VPC时，也会自动删除对应的路由器
- 不支持直接创建和删除路由器

路由表

路由表，是指路由器上管理路由条目的列表。

产品约束

- 每个路由器有且只有1个路由表
- 路由表的路由条目会影响VPC中的所有云产品实例。目前不支持指定交换机和云产品实例的源地址策略路由。

路由表管理

- 新建VPC时，系统会自动创建1个路由表
- 删除VPC时，系统会自动删除对应的路由表
- 不支持直接创建和删除路由表

路由条目

路由表中的每一项成为一条路由条目，路由条目定义了通向指定目标网段的网络流量的下一跳地址，路由条目包括系统路由和自定义路由两种类型。

说明：路由器只支持静态路由，不支持ECMP等价路由。

路由条目管理

- 专有网络创建时，会自动创建1条系统路由，用于专有网络内的云产品实例访问专有网络外的云服务
- 创建交换机，系统也会创建1条对应的系统路由，目的地址为所创建交换机的网段
- 用户可以创建和删除自定义路由条目
- 系统路由条目由系统自动管理，用户无法创建和删除

选路规则

路由表中采用最长前缀匹配作为流量的路由选路规则。最长前缀匹配是指IP网络中当路由表中有多条条目可以匹配目的IP时，采用掩码最长（最精确）的一条路由作为匹配项并确定下一跳。

例如某专有网络中路由表中路由条目如下表，其中目的地址为 100.64.0.0/10 和 192.168.0.0/24 的两条路由均为系统路由，前者为系统保留的地址段，后者为专有网络中为交换机配置的系统路由。另外，目的地址为 0.0.0.0/0 和 10.0.0.0/16 的两条路由为自定义路由，表示将访问 0.0.0.0/0 地址段的流量转发至id为 i-12345678 的ECS实例，将访问 10.0.0.0/16 地址段的流量转发至id为 i-87654321 的ECS实例。根据最长前缀匹配规则，在该专有网络中，访问 10.0.0.1 的流量会转发至 i-12345678,而访问 10.0.1.1 的流量会转发至 i-12345678。

DestinationCidrBlock	NextHopType	NextHopId	Type
100.64.0.0/10			System
192.168.0.0/24			Sytem
0.0.0.0/0	Instance	i-12345678	Custom

10.0.0.0/24	Instance	i-87654321	Custom
-------------	----------	------------	--------

配置路由表

路由表支持通过专有网络控制台和OpenAPI两种方式进行配置。

控制台操作如下：

- 1.登录专有网络控制台，在专有网络列表中选择需要配置的路由的专有网络，点击管理；
- 2.在专有网络详情页选择路由器，您可以通过路由条目列表查看已有路由条目，包括系统路由（类型为系统）和自定义路由（类型为自定义）；
- 3.如果需要增加一条自定义路由，请点击右上 添加路由，在弹框中填写目标网段、下一跳类型、下一跳实例。

创建自定义路由条目

您可以使用专有网络VPC控制台为VPC创建自定义路由条目。

- 1.打开专有网络控制台<https://vpc.console.aliyun.com/#/overview/resources>。
- 2.在左侧导航选择"专有网络"，进入"专有网络列表"。
- 3.选择地域"华北 2 (北京)"，进入该地域下的专有网络列表。
- 4.选择某一专有网络实例，点击"操作"列下的"管理"链接，进入"专有网络基本信息"页面。
- 5.在左侧导航选择"路由器"，进入"虚拟路由列表"。
- 6.点击右上角的<添加路由>，弹出"添加路由"对话框。
- 7.根据用户需求，填写目标网段、下一跳类型、下一跳ECS实例。
- 8.点击<确定>，完成自定义路由表的添加。

删除自定义路由条目

- 1.打开专有网络控制台<https://vpc.console.aliyun.com/#/overview/resources>。
- 2.在左侧导航选择"专有网络"，进入"专有网络列表"。
- 3.选择地域"华北 2 (北京)"，进入该地域下的专有网络列表。
- 4.选择某一专有网络实例，点击"操作"列下的"管理"链接，进入"专有网络基本信息"页面。
- 5.在左侧导航选择"路由器"，进入"虚拟路由列表"。
- 6.用户只能删除"类型"为"自定义"的路由表，选择某一自定义路由表，点击"操作"列下的<删除>按钮，弹出"删除路由规则"确认对话框。
- 7.点击<确定>，完成自定义路由表的删除操作。

编辑路由器

用户只能修改路由器基本信息中的名称和描述。

1. 打开专有网络控制台<https://vpc.console.aliyun.com/#/overview/resources>。
2. 在左侧导航选择"专有网络"，进入"专有网络列表"。
3. 选择地域"华北 2 (北京)"，进入该地域下的专有网络列表。
4. 选择某一专有网络实例，点击"操作"列下的"管理"链接，进入"专有网络基本信息"页面。
5. 在左侧导航选择"路由器"，进入"虚拟路由列表"。
6. 点击"路由器基本信息"右侧的按钮<编辑>，弹出"编辑路由器"对话框。
7. 在该对话框填写路由器名称及相关描述信息。
8. 点击<确定>，完成路由器基本信息的编辑。

API

路由器相关接口：

- 查询路由器列表
- 修改路由器属性

路由表相关接口：

- 新建自定义路由
- 删除自定义路由
- 查询路由表列表

通过高速通道实现VPC互联

概述

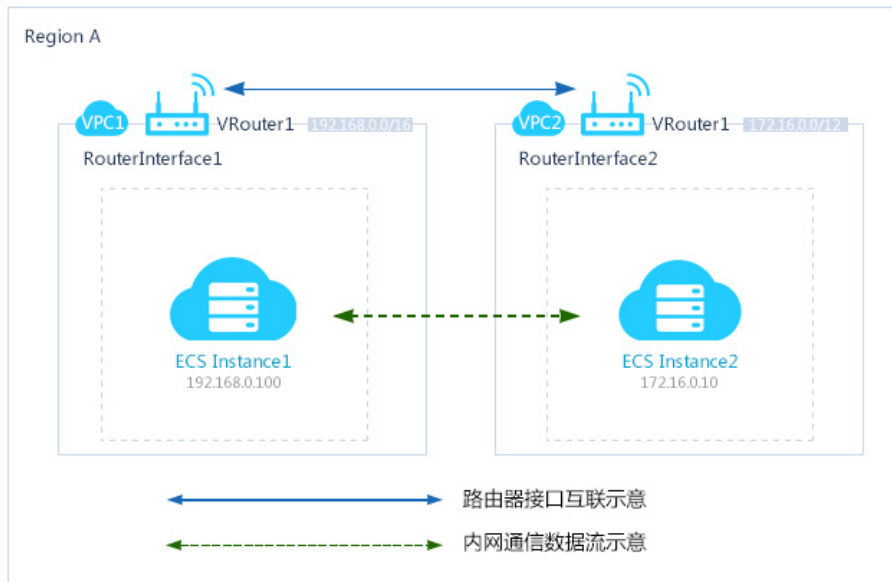
使用高速通道实现VPC之间的互联，通过高速通道，可以实现VPC之间的私网通信。用户可以在自己的VPC之间通信，也可以和同地域中的其他VPC通信，还可以和跨地域的VPC进行通信。

高速通道可以使得物理IDC和阿里云上的VPC之间进行内网通信，从而实现了网络的融合，帮助用户促进了数据的传输，建立起了文件共享网络。

配置

域内VPC之间的互联

使用高速通道，可以实现同一地域内两个VPC之间的私网通信。这样做的好处是既可以避免绕行公网带来的网络质量不稳定问题，又可以避免数据在传输过程中被窃取的风险。



数据规划

同一地域：Region A，下文以在地域"华北 2 (北京)"下创建专有网络为例

两个专有网络：VPC1、VPC2

路由器接口网段为：VRouter1(192.168.0.0/16)、VRouter2 (172.16.0.0/12)

云服务器的私网IP分别为：ECS1 (192.168.0.100)、ECS2 (172.16.0.10)

操作步骤

1. 登陆专有网络控制台，在地域"华北 2 (北京)"下，创建两个专有网络VPC1 (网段：192.168.0.0/16) 和 VPC2 (网段：172.16.0.0/12)，具体操作请参考创建专有网络。

2. 在"专有网络列表"页，选择"管理"，进入"专有网络基本信息"页面。

3. 在导航左侧选择"交换机"，在右侧"操作"列，选择创建实例，在下拉菜单选择"创建ECS实例"。

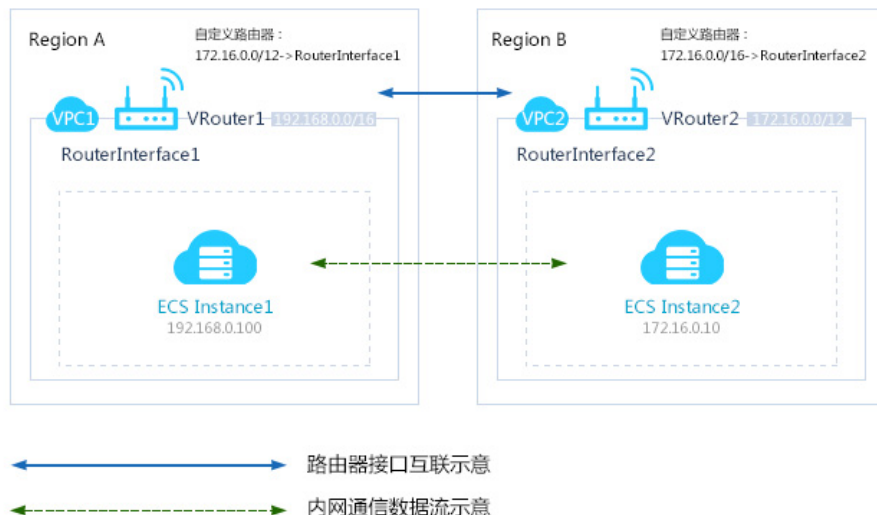
4. 登陆高速通道控制台，创建路由器接口。

- 连接场景：同账号VPC互联
- 本端配置和对端配置的地域均选择"华北 2 (北京)"
- 本端配置：专有网络选择VPC1
- 对端配置：对端专有网络选择VPC2

5. 点击购买和开通后，当状态为"已激活"时，完成域内VPC之间的互联设置。

域间VPC之间的互联

可以使用高速通道使得处于两个不同地域的VPC之间进行通信。



数据规划

- Region A代表"华北 2 (北京)", Region B代表"华东 1 (杭州)"
- 地域"华北 2 (北京)"的专有网络为VPC1, 地域"华东 1 (杭州)"的专有网络为VPC2
- 路由器接口网段VRouter1 (192.168.0.0/16), VRouter2 (172.16.0.0/12)
- VPC1中的云服务器ECS1私网IP为192.168.0.100, VPC2中的云服务器ECS2的私网IP为172.16.0.1
- VPC1中自定义路由器1网段为: 172.16.0.0/12, VPC2中自定义路由器2 网段为: 172.16.0.0/16

操作步骤

1. 登陆专有网络控制台, 在地域"华北 2 (北京)"下, 创建一个专有网络VPC1 (网段: 192.168.0.0/16), 具体操作请参考创建专有网络。
2. 在"专有网络列表"页, 选择"管理", 进入"专有网络基本信息"页面。
3. 在导航左侧选择"交换机", 在右侧"操作"列, 选择创建实例, 在下拉菜单选择"创建ECS实例"。创建ECS的私网IP为192.168.0.100。
4. 在左侧导航选择"路由器", 点击<添加路由>创建自定义路由, 自定义路由网段为"172.16.0.0/12"。
5. 在地域"华东 1 (杭州)"下, 创建一个专有网络VPC2 (网段: 172.16.0.0/12), 具体操作请参考创建专有网络。
6. 在"专有网络列表"页, 选择"管理", 进入"专有网络基本信息"页面。
7. 在导航左侧选择"交换机", 在右侧"操作"列, 选择创建实例, 在下拉菜单选择"创建ECS实例"。创建ECS的私网IP为172.16.0.1。

8.在左侧导航选择"路由器", 点击<添加路由>创建自定义路由, 自定义路由网段为"172.16.0.0/16"。

9.登陆高速通道控制台, 创建路由器接口。

- 连接场景：同账号VPC互联
- 本端配置地域选择"华北 2 (北京)"和对端配置的地域均选择"华东 1 (杭州)"
- 本端配置：专有网络选择VPC1
- 对端配置：对端专有网络选择VPC2

10.点击购买和开通后, 当状态为"连接"时, 完成域间VPC之间的互联设置。

跨账号VPC之间的互联

处于不同账号下的两个VPC之间也可以通过高速通道进行私网通信。这样可以避开公网带来的网络不稳定问题, 也可以避免数据在传输过程中被窃取的风险。

数据规划

- 用户：账号A、账号B
- 专有网络：账号A下的专有网络VPC1、账号B下的专有网络VPC2
- VPC1的地域为北京, VPC2的地域为杭州。
- VPC1的路由器接口为连接发起端, VPC2的路由器接口为连接接受端
- VPC1网段VRouter1 (192.168.0.0/16), VPC2网段VRouter2 (172.16.0.0/12)

操作步骤

1.使用账号A登陆控制台, 在地域"华北 2 (北京)"下, 创建专有网络VPC1, 网段为 (192.168.0.0/16)。

2.在专有网络内创建ECS实例。

3.登陆高速通道控制台, 点击右上角的按钮<创建路由器接口>, 弹出购买页面。

4.选择各配置项, 并点击购买, 完成账号A中的操作。

- "连接场景"选择<自定义>
- 本端配置：地域选择"华北 2 (北京)"、专有网络选择VPC1
- 对端配置：对端地域选择"华东 1 (杭州)"
- 角色规格：连接角色选择"连接发起端"

5.使用账号B登陆控制台, 在地域"华东 1 (杭州)"下, 创建专有网络VPC2, 网段为 (172.16.0.0/12)。

6.在专有网络内创建ECS实例。

7.登陆高速通道控制台, 点击右上角的按钮<创建路由器接口>, 弹出购买页面。

8.选择各配置项, 并点击购买, 完成账号B中的操作。

- "连接场景"选择<自定义>
- 本端配置：地域选择"华东 1 (杭州)"、专有网络选择VPC2
- 对端配置：对端地域选择"华北 2 (北京)"
- 角色规格：连接角色选择"连接接受端"

9.完成上述操作，账号A的ECS和账号B的ECS之间即可通信。

监控

监控

VPC涉及的监控项为流量，流量监控的具体指标可以参考云监控中EIP的监控信息。具体内容请参见链接中"弹性IP EIP监控"部分的内容。

专有网络安装云监控

具体请参考新版Agent安装方法。

使用限制

使用限制

专有网络

为了保证性能和安全性，专有网络内不支持组播和广播，如果需要使用组播和广播功能，需要提交工单获取组播和广播工具。

限制项	普通用户限制描述	例外申请方式
单个账号的专有网络个数	2个	工单
专有网络可选的网段范围	192.168.0.0/16，172.16.0.0/12，10.0.0.0/8以及它们的子网	工单
单个专有网络的路由器个数	1个	没有例外
单个专有网络的交换机个数	24个	没有例外
单个专有网络的路由表个数	1个	没有例外
单个路由表的路由条目数量	48条	工单

单个专有网络容纳云产品数量	5000个	没有例外
---------------	-------	------

路由器

- 每个VPC有且只有一个路由器
- 路由器不支持BGP和OSPF等动态路由协议

交换机

- VPC的交换机，是一个3层交换机，不支持2层广播和组播。
- 交换机本身对云产品实例数量没有限制，它能够容纳多少实例，取决于所在专有网络当前的云产品实例数量，即5000-当前已保有的云产品数量。
- 交换机的网段不可以进行修改。

专有网络ECS实例的迁移限制

VPC网络中支持将ECS实例从某一路由器下的一台交换机转移到另一台交换机。

不支持以下操作：

ECS实例不支持跨路由器切换。

ECS实例不支持网络类型之间的切换，比如不支持从专有网络迁移到经典网络和不支持从经典网络迁移到专有网络。

弹性公网IP

- 可创建弹性公网IP的地域为华东 1 (杭州)、华北 2 (北京)、华南 1 (深圳)、华东 2 (上海)、美西(硅谷)、亚太(新加坡)、美东(弗吉尼亚)、香港
- 目前支持绑定弹性公网IP的资源，有且只有ECS实例
- 弹性公网IP只能绑定在VPC类型的ECS实例上，不支持绑定在Classic网络类型的ECS实例上
- 一个ECS实例只能绑定一个弹性公网IP
- 一个弹性公网IP只能绑定一个ECS实例
- 弹性公网IP只能绑定在同地域的ECS实例上
- 单个账户下的弹性公网IP配额为20个

NAT网关-使用限制

NAT网关相关限制

- 资源个数
 - 每个VPC中，最多只能有一个NAT网关

共享带宽包相关限制

- 公网带宽值
 - 每个共享带宽包的带宽，最小为5MBps，最大为5000Mbps
 - 如果用户有需要，可以通过工单申请更大的带宽设置范围
- 公网IP个数
 - 每个共享带宽包的公网IP个数，最小为1个，最大为50个
 - 如果用户有需要，可以通过工单申请更大的IP个数设置范围

端口转发表相关限制

- 端口转发规则条目的唯一性
 - 详见 NAT网关使用说明
- 端口转发规则条目个数
 - 每个端口转发表中，最多存在100个端口转发规则条目
 - 如果用户有需要，可以通过工单申请更大的端口转发表容量

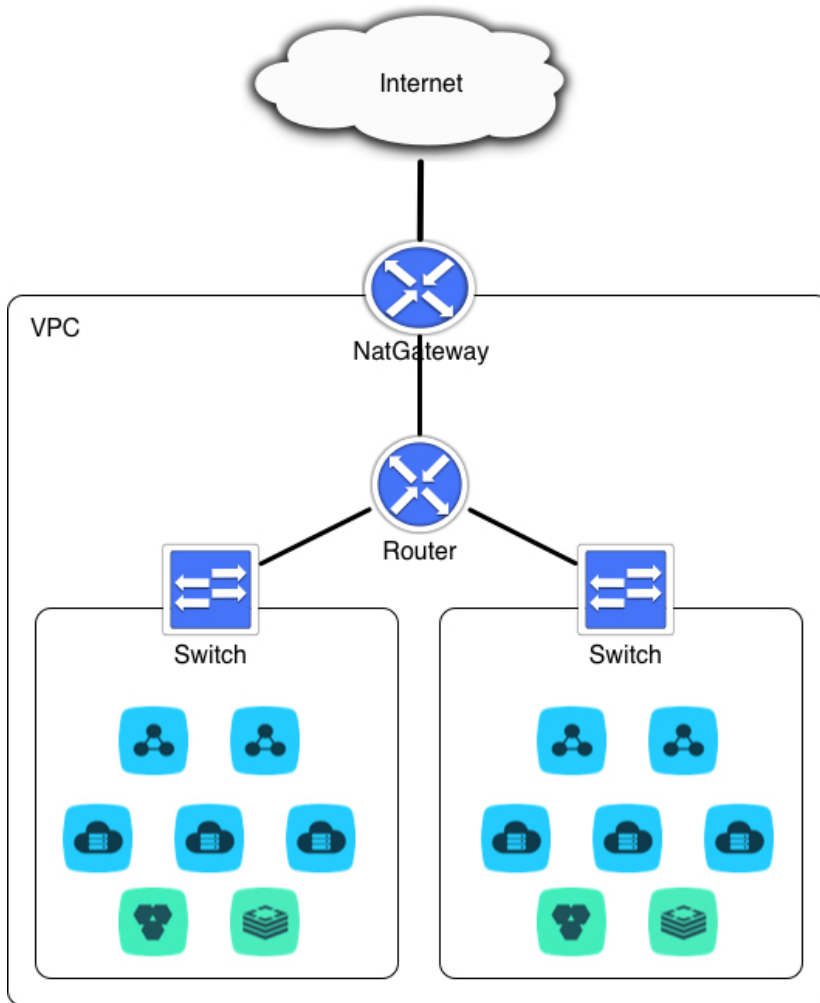
网关

NAT网关（NAT Gateway）

当用户需要在VPC中设立一个公网网关，来进行DNAT、SNAT配置时，可以使用NAT网关来实现。

NAT与VPC网络拓扑

如下图所示，NAT网关是一个VPC中的公网网关，处于VPC的边界，接在VPC的路由器上。由这样的拓扑图可知，NAT向内转发包时，会经过路由器、按照自定义路由表进行转发路由选择；VPC内ECS等资源通过NAT网关向外发送时，数据在送达NAT网关之前会经过路由器，也会按照自定义路由表进行路由选择。



DNAT

NAT网关的DNAT功能，可以按照用户设定的端口映射、IP映射规则，将NAT网关上的公网IP收到的数据，转发给VPC内的ECS。

用户的配置通过端口转发表来完成。每个NAT网关有且只有一张端口转发表。用户可以对端口转发表中的规则进行添加、修改、删除操作。所有配置动作均是即时生效的。

端口转发规则

一条端口转发规则的结构如下：

#in Chinese:
[外部IP, 外部端口, 内部IP, 内部端口, 通信协议]

```
#in English:
[ExternalIp, ExternalPort, InternalIp, InternalPort, IP Protocol]
```

其中，

- ExternalIp是NAT网关上的某个共享带宽包中的一个公网IP
- ExternalPort是ExternalIp的某个有效端口
- InternalIp是VPC中的某个有效私网IP
- InternalPort是InternalIp的某个有效端口
- Ip Protocol是通信协议，可以是TCP或者UDP

一条端口转发规则的效果是：告知NAT网关，当收到发向ExternalIp:ExternalPort的、协议为指定IP Protocol的数据时，请转发到InternalIp:InternalPort，并将回包原路返回。

IP映射

端口转发规则的一个特殊用法是，将ExternalPort、InternalPort、IP Protocol同时设为Any，从而实现某个公网IP与某个私网IP的全端口、全协议映射。

端口转发规则的生效条件

InternalIp必须是被ECS使用，且该ECS未绑定EIP时，端口转发规则才能生效。

具体的：下列情形中，端口转发规则可以在端口转发表中成功添加，但不会生效（不会生效是指，NAT网关不会进行相应的转发动作）；

InternalIp是VPC内的一个有效私网IP，但是并非被一个ECS实例使用；

InternalIP是VPC内的一个有效私网IP，且该IP被一个ECS实例使用，但该ECS实例绑定了EIP；

端口转发规则的唯一性

1. 条目的ID是进行删改查时的唯一ID，方便管理
2. 所有条目的[ExternalIp, ExternalPort, IpProtocol]一定是不同的；
3. 所有条目的[InternalIp, InternalPort, IpProtocol]一定是不同的；
4. 对于任何一个IP(不管是InternalIP还是ExternalIp)的任一种特定的协议，不能同时存在Any端口映射规则和指定端口映射规则；

示例1：以下两条规则是冲突的：

ExternalIp1: Any -> InternalIp1:Any TCP ExternalIp1:8080 -> InternalIp2:80 TCP

示例2：以下两条规则也是冲突的：ExternalIp1: Any -> InternalIp1:Any TCP ExternalIp2:8080 ->

InternalIp1:80 TCP

SNAT

SNAT功能即将上线，敬请期待。

带宽管理

NAT网关上可以防止多个公网IP。为了方便用户进行多个应用间带宽的复用，NAT网关支持多个IP共享一份购买的带宽。

为了使用户购买和管理时比较清晰，我们将IP资源和带宽资源抽象封装成了"共享带宽包"。

- 每购买一个共享带宽包，需要指定该共享带宽包中的公网带宽值和公网IP个数；
- 共享带宽包附着于一个指定的NAT网关，其上的公网IP会被配置在该NAT网关上，供NAT网关的SNAT、DNAT功能使用；
- 一个共享带宽包中的所有公网IP，共享该共享带宽包的带宽值；即，任一个公网IP都可以在单独使用时用满这份带宽值；多个IP一起使用时，总的瞬时流量无法超过该带宽值。
- 共享带宽包支持即时增减带宽、增减公网IP个数。

目前，仅支持每个NAT网关上放置一个共享带宽包；一个共享带宽包中可放置50个甚至更多的公网IP。

未来会支持一个NAT网关上放置更多的共享带宽包，方便用户进行更灵活细致的带宽管理。

计量与计费

详见价格总览

异常处理

VPC网络环境连接OSS地址失败的解决方法

现象描述

使用专有网络VPC，想实现VPC环境中的ECS和OSS通信，但是连接oss-cn-beijing-internal.aliyuncs.com（北京OSS节点内网地址）失败。

无法Ping通也无法连接到这个地址的80端口。

1.看是否能够ping通。

```
$ping oss-cn-beijing-internal.aliyuncs.com
```

2.看是否能telnet通80端口。

```
$telnet oss-cn-beijing-internal.aliyuncs.com 80
```

常见原因

OSS针对VPC有一套自己的内网地址，故除这些固定的内网地址外，连通其他地址都是不通的。

异常处理步骤

所以可以判断，在VPC的环境中ECS连接oss-cn-beijing-internal.aliyuncs.com这个地址不通。

需要说明的是，不仅连接这个地址不通，以下地址在相同地域中都是不通的：

华北 1 (青岛)节点内网地址：oss-cn-qingdao-internal.aliyuncs.com

华北 2 (北京)节点内网地址：oss-cn-beijing-internal.aliyuncs.com

华东 1 (杭州)节点内网地址：oss-cn-hangzhou-internal.aliyuncs.com

香港节点内网地址：oss-cn-hongkong-internal.aliyuncs.com

华南 1 (深圳)节点内网地址：oss-cn-shenzhen-internal.aliyuncs.com

美西(硅谷)节点内网地址：oss-us-west-1-internal.aliyuncs.com

这个是因为OSS针对VPC是有一套自己的内网地址如下：

华北 2 (北京)：vpc100-oss-cn-beijing.aliyuncs.com

华南 1 (深圳)：vpc100-oss-cn-shenzhen.aliyuncs.com

华东 1 (杭州)：vpc100-oss-cn-hangzhou.aliyuncs.com

华东 2 (上海)：vpc100-oss-cn-shanghai.aliyuncs.com

华北 1 (青岛)：vpc100-oss-cn-qingdao.aliyuncs.com

美西(硅谷)：vpc100-oss-us-west-1.aliyuncs.com

亚太（新加坡）：vpc100-oss-ap-southeast-1.aliyuncs.com

连接到对应的VPC地址，网络就可以进行互通。

如问题还未解决,请联系售后技术支持。

VPC中的ECS访问经典网络中的RDS失败

VPC的ECS默认无法通过内网访问经典网络的RDS，解决方法有两种：

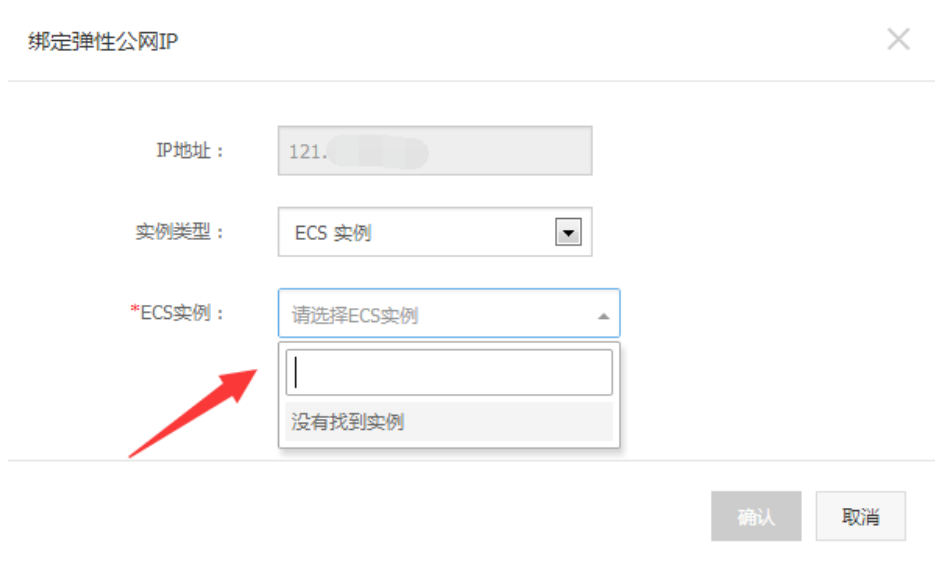
给VPC ECS绑定EIP，给RDS设置外网连接地址，在VPC ECS中访问RDS的公网地址，即通过公网访问RDS。

将经典网络的RDS实例切换到VPC下，这样切换后，经典网络的ECS将无法再访问该RDS实例。

绑定弹性公网IP界面提示没有找到ECS实例

现象描述

用户购买弹性公网IP，在绑定弹性IP时，控制台界面无法显示ECS实例，如下图所示。



可能原因

弹性公网IP只能绑定到专有网络VPC的ECS服务器上。

如果用户在弹性IP所属地域，没有专有网络的ECS服务器，只有经典网络的ECS服务器，经典网络的ECS实例是不会出现在绑定弹性IP的界面中的。

ECS实例的状态不是运行中或者已停止状态，同样不能进行绑定EIP。

处理步骤

- 1.在云服务器ECS控制台检查ECS实例是否有网络类型为专有网络的实例。
- 2.如果没有的话，登陆专有网络控制台，选择相应地域的VPC，创建ECS实例。
- 3.登陆EIP控制台，绑定弹性公网IP即可。

建议与总结

工程师在网络规划时，按照创建专有网络、创建交换机、创建ECS实例、绑定弹性公网IP的顺序创建实例，避免网络连不通的情况。

VPC创建vswitch提示Specified CIDR block overlapped with other subnets

现象描述

客户在VPC控制台vpc.console.aliyun.com创建交换机时，如果提示 Specified CIDR block overlapped with other subnets，如图所示。

创建交换机

×

*名称：

test

名称为2-128个字符，以大小字母或中文开头，可包含数字，"_"或"-"

*专有网络：

vpc-22iyk98ob

专有网络网段：

192.168.0.0/16

*可用区：

亚太1可用区A

① 创建后无法修改

*网段：

192.168.1.0/24

① 创建后无法修改

必须等于或属于该专有网络的网段，网段掩码必须在16和29之间。例如：192.168.1.0/24

可用IP数：

252 个

描述：

描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

✖ 指定的 CIDR 与其他 VSwitch 的 CIDR 重叠 或与已有的自定义路由的CIDR重叠。

可能原因

遇到这个问题时，一般情况是当前创建交换机的网段与该VPC下已有交换机网段重复导致，客户更换其他网段即可。

处理步骤

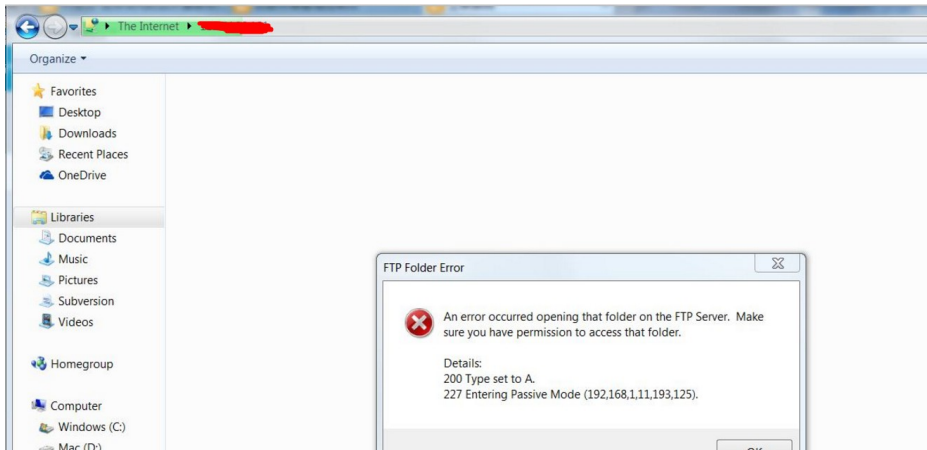
- 1.登陆专有网络管理控制台。
- 2.在左侧导航选择"专有网络"，进入"专有网络列表"页面。
- 3.选择相应的VPC实例，点击右侧的 **管理** 链接，进入"专有网络基本信息"页面。
- 4.在左侧导航选择"交换机"，进入"交换机列表"页面。
- 5.点击右上角的 **创建交换机** 按钮，弹出"创建交换机"对话框。
- 6.用户根据需要修改"网段"，点击 **确定** 即可。

在VPC下使用IIS搭建了FTP,在外部无法通过

Windows Explorer连接FTP的解决方法

现象描述

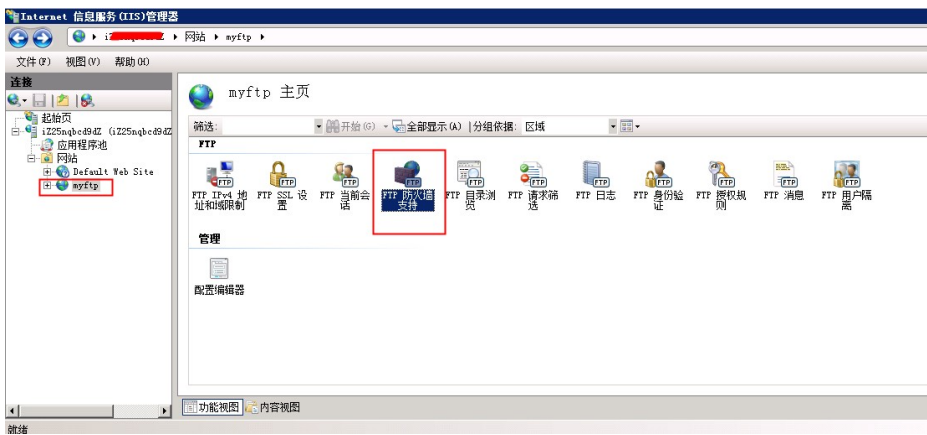
在专有网络(VPC)下，通过IIS搭建了FTP，通过Windows Explorer连接FTP时报如下错误。



但是使用FileZilla等客户端可以正常连接。

操作步骤

1.可以通过配置FTP 防火墙支持解决。参考如下方法：





弹性公网IP不通原因排查方法

弹性公网IP不通的原因及处理方法。

1.弹性公网IP没有绑定到ECS上

具体绑定方法[点击这里](#)。

2.查看主机内部是否有安全策略

如果ECS系统有安全组策略，比如禁止80端口访问，那么弹性公网IP80端口也是无法访问的。

修改安全组策略即可，具体方法请参考安全组的应用案例。

3、查看您的账号是否余额不足了

EIP有两种计费方式：按使用流量计费和按固定带宽计费，均为按量付费的方式。

登陆管理控制台，在首页的最上方可以查看用户的余额状态。

服务条款

产品SLA

VPC不提供独立的SLA，VPC中云产品实例（ECS, RDS, SLB, OCS, OSS等）适用各个产品的SLA和故障赔偿条款。

服务条款

前言

欢迎使用阿里云专有网络服务（VPC）

您开通专有网络（Virtual Private Cloud，简称VPC）前，请您仔细阅读阿里云在www.aliyun.com网站上公布的相关规范、规则和使用流程以及本服务条款的全部内容，如果您不同意前述任意内容，或者无法准确理解阿里云的解释，请不要进行后续操作。如您开通或实际使用了VPC服务，阿里云将视为您已完全理解并认同规范、规则、流程及服务条款的全部内容，届时您不应以未阅读、未理解或者未获得阿里云对您问询的解答等理由，主张本服务条款无效，或要求撤销本服务条款。

1. 签约主体

本服务条款是您因使用阿里云VPC服务与阿里云计算有限公司所订立的有效合约。

2. 协议的订立和生效

一旦您选择“免费开通”并进行后续操作，即表示您同意遵循本服务条款之所有约定，本服务条款即成为双方之间就VPC服务所达成的有效合约。

3. VPC服务的使用

3.1. 在使用阿里云VPC服务前，您应仔细阅读阿里云在官方页面上展示的相关服务说明、技术规范、使用流程，并理解相关内容及可能发生的后果，在使用VPC服务过程中，您应依照相关操作指引进行操作，请您自行把握风险谨慎操作。

3.2. 您理解并同意，使用阿里云VPC服务是您自行独立审慎判断的结果，您将自行对此负责，包括但不限于：

3.2.1. 在使用VPC服务过程中，如您对虚拟路由器/虚拟交换机/自定义路由/安全组的设置是您自行操作的部分，您将对自行操作的行为及其产生的结果负责；

3.2.2. 在使用VPC服务过程中，您对您自行提供的设备如专线或VPN负责；

3.2.3. 尽管目前使用VPC服务您仍不需付费，但在使用VPC过程中如您使用了阿里云的其他收费服务（包括但不限于弹性IP），您应按照阿里云相关收费规则支付相关服务费用。

3.3. 您理解并认可，您在使用VPC服务过程中：

3.3.1. 您不应进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDOS等）；

3.3.2. 您不应进行任何改变或试图改变阿里云提供的系统配置或破坏系统安全及网络安全的行为；

3.3.3. 您不应修改、翻译、改编、出租、转许可、在信息网络上传播或转让阿里云提供的软件或服务，也不得逆向工程、反编译或试图以其他方式发现阿里云提供的软件的源代码；

3.3.4. 非经阿里云事先书面同意，您不应复制、传播、转让、许可或提供他人使用阿里云提供的VPC服务；

3.3.5. 您不应以任何将会违反国家、地方法律法规、行业惯例和社会公共道德，及影响、损害或可能影响、损害阿里云、阿里巴巴集团利益的方式或目的使用VPC服务。

4. 责任限制

您理解并同意，在免费期间，阿里云虽然对VPC服务提供可用性支撑，但不对其中任何错误或漏洞提供任何担保，并不对您使用VPC服务的工作或结果承担任何责任。

5. 变更和终止

5.1. 您理解并认可，阿里云保留随时修改、取消、增强阿里云VPC服务一项或多项功能的权利，并有权要求您使用最新更新的版本；届时，阿里云将以提前通过在网站内合适版面发布公告或发送站内通知等方式通知您。

5.2. 如您有任何违反本服务条款的情形，或经阿里云根据自己的独立判断认为您对VPC的使用行为不符合阿里云的要求，阿里云除有权随时中断或终止您使用VPC而无须通知您；同时，如给阿里云造成损失的，阿里云有权要求您赔偿损失。

6. 保密

您及阿里云都应对对方的保密信息承担保密责任，除非经国家行政、司法等有权机关要求披露或该信息已进入公有领域。

7. 其他

7.1. 您理解并同意，阿里云目前为您提供免费的VPC服务，即您开通或使用VPC服务，并不需向阿里云支付费用；阿里云不排除日后收取费用的可能，届时阿里云将提前10个自然日通过在网站内合适版面发布公告或发送站内通知等方式公布收费政策及规范；如您仍使用VPC服务的，应按届时有效的收费政策及规范付费并应遵守届时阿里云公布的有效的服务条款。

7.2. 阿里云有权随时根据有关法律、法规的变化以及公司经营状况和经营策略的调整等修改本服务条款。修改后的服务条款会在阿里云网站（www.aliyun.com）上公布。如果不同意修改的内容，您应停止使用VPC服务。如果继续使用VPC服务，则视为您接受本服务条款的变动。

7.3. 如果本服务条款中的任何条款无论因何种原因完全或部分无效或不具有执行力，或违反任何适用的法律，则该条款被视为删除，但本服务条款的其余条款仍应有效并且有约束力。

7.4. 本服务条款受中华人民共和国法律管辖。在执行本服务条款过程中如发生纠纷，双方应及时协商解决。协商不成时，任何一方可直接向杭州市西湖区人民法院提起诉讼。

相关资源

论坛

要访问论坛，请点击[这里](#)。

联系我们

工单：

<https://workorder.console.aliyun.com/console.htm?spm=5176.1879446.1001.2.j4NqcG#/ticket/list/>

售前咨询：95187转1（5×8）

客服电话：95187

备案帮助：95187转3

变更记录

变更记录

发布时间	发布内容
2015年08月4日	全网开放，功能包括专有网络（VPC）、路由器（VRouter）、路由表（RouteTable）、交换机（VSwitch）
2015年12月28日	专有网络支持资源访问控制服务(RAM)
2016年03月29日	全文整改和优化
2016年03月30日	默认专有网络功能上线