阿里云
专有网络VPC

产品简介

文档版本：20190908

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

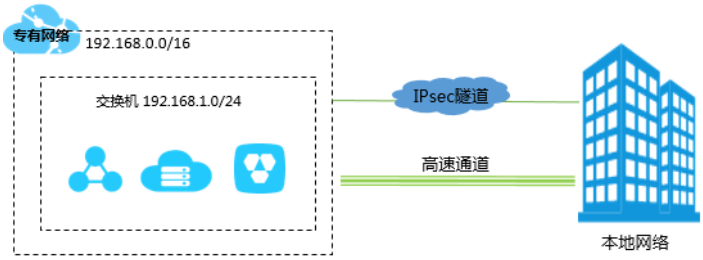
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
##	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *{stand | slave}*

目录

1 什么是专有网络

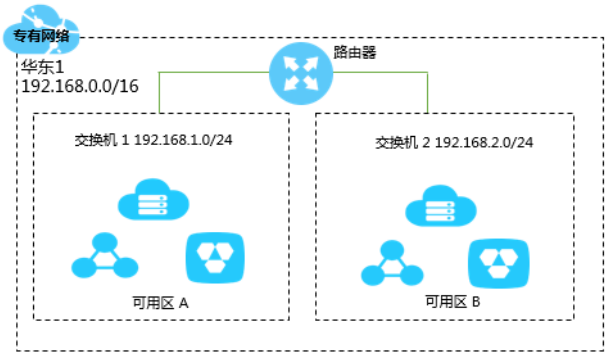
专有网络是您自己独有的云上私有网络。您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等，您可以在自己定义的专有网络中使用阿里云资源如云服务器、云数据库RDS版和负载均衡等。

您可以将专有网络连接到其他专有网络或本地网络，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。



组成部分

每个VPC都由一个私网网段、一个路由器和至少一个交换机组成。



- 私网网段

  在创建专有网络和交换机时，您需要以CIDR地址块的形式指定专有网络使用的私网网段。

  您可以使用下表中标准的私网网段及其子网作为VPC的私网网段。详细信息，请参见#unique_4。

网段	可用私网IP数量（不包括系统保留地址）
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

- 路由器

  路由器（VRouter）是专有网络的枢纽。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和其他网络的网关设备。每个专有网络创建成功后，系统会自动创建一个路由器。每个路由器关联一张路由表。

  详细信息，请参见#unique_5。

- 交换机

  交换机（VSwitch）是组成专有网络的基础网络设备，用来连接不同的云资源。创建专有网络后，您可以通过创建交换机为专有网络划分一个或多个子网。同一专有网络内的不同交换机之间内网互通。您可以将应用部署在不同可用区的交换机内，提高应用的可用性。

  详细信息，请参见交换机。

2 VPC连接

阿里云提供了丰富的解决方案以满足VPC内的云产品实例与公网（Internet）、其他VPC、或本地数据中心（IDC）互连的需求。

连接公网

您可以使用下表中的产品或功能，将专有网络和公网（Internet）打通。

产品	功能	优势
ECS固定公网IP	创建专有网络类型的ECS实例时，您可以选择分配公网IPv4地址，系统会为您自动分配一个支持访问公网和被公网访问的IP地址。 目前，ECS实例固定公网IP不能动态与VPC ECS实例解绑，但可以将固定公网IP转换为EIP。详细信息，请参见#unique_8。	支持使用共享流量包，将公网IP转换为EIP后也可以使用共享带宽。
弹性公网IP（EIP）	能够动态和VPC ECS实例绑定和解绑，支持VPC ECS实例访问公网（SNAT）和被公网访问（DNAT）。	EIP可以随时和ECS实例绑定和解绑。 可以使用共享带宽和共享流量包，降低公网成本。
NAT网关	支持多台VPC ECS实例访问公网（SNAT）和被公网访问（DNAT）。 说明: 和负载均衡相比，NAT网关本身没有均衡流量的功能。	NAT网关和EIP的核心区别是NAT网关可用于多台VPC ECS实例和公网通信，而EIP只能用于一台VPC ECS实例和公网通信。

产品	功能	优势
负载均衡	基于端口提供四层和七层负载均衡功能，支持用户从公网通过负载均衡（SLB）访问ECS。  说明: 负载均衡不支持VPC网络的ECS通过负载均衡主动访问公网（SNAT）。	在DNAT方面，负载均衡是基于端口的负载均衡，即一个负载均衡的一个端口可以对应多台ECS。 负载均衡通过对多台ECS进行流量分发，可以扩展应用系统对外的服务能力，并通过消除单点故障提升应用系统的可用性。 绑定EIP后，支持使用共享带宽和共享流量包，降低公网成本。

连接VPC

您可以使用下表中的产品或功能，连接两个VPC。

产品	功能	优势
云企业网	支持将多个不同地域、不同账号的VPC连接起来，构建互联网络。 详细信息，请参见#unique_11。	· 一网通天下。 · 低时延高速率。 · 就近接入与最短链路互通。 · 链路冗余及容灾。 · 系统化管理。
VPN网关	您可以通过在两个VPC之间创建IPsec连接，建立加密通信通道。 详细信息，请参见#unique_12。	· 安全。 · 高可用。 · 低成本。 · 配置简单。

连接本地IDC

您可以使用下表中的产品或功能，将本地IDC和云上专有网络打通。

产品	功能	优势
高速通道	通过物理专线接入使VPC与本地IDC网络互通。 详细信息，请参见物理专线接入。	· 基于骨干网络，延迟低。 · 专线连接更加安全、可靠。

产品	功能	优势
VPN网关	· 您可以通过建立IPsec-VPN，将本地IDC网络和云上VPC连接起来。 · 您可以通过建立SSL-VPN，将本地客户端远程接入VPC。	· 安全。 · 高可用。 · 低成本。 · 配置简单。
云企业网	· 与本地IDC互通 支持将要互通的本地IDC关联的边界路由器（VBR）加载到已创建的云企业网实例，构建互联网络。 · 多VPC与IDC互通 支持将要互通的多个网络实例（VPC和VBR）加载到已创建的云企业网实例，构建企业级互联网络。	· 一网通天下。 · 低时延高速率。 · 就近接入与最短链路互通。 · 链路冗余及容灾。 · 系统化管理。
智能接入网关	· 可实现线下机构（IDC/分支机构/门店等）接入阿里云数据中心，轻松构建混合云。 · 可实现线下机构之间互通。	· 配置高度自动化，即插即用，网络拓扑变化自适应快速收敛。 · 城域内Internet就近接入，可通过设备及链路级主备方式实现线下多机构可靠上云。 · 混合云私网加密互连，Internet传输过程中加密认证。

3 基础架构

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，一个隧道号对应一个虚拟化网络。

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，例如弹性（scalability）、安全性（security）、可靠性（reliability）和私密性（privacy），并且还有极高的互联性能（performance）需求，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。随着虚拟化网络规模的扩大，这种方案中的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，无法支撑公共云的巨大用户量。

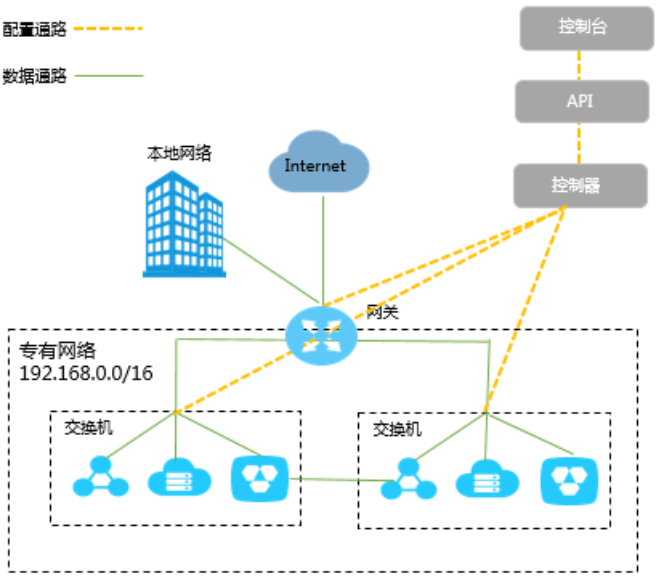
原理描述

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个虚拟化网络。一个VPC内的ECS（Elastic Compute Service）实例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实例因为所在的隧道ID不同，本身处于两个不同的路由平面，所以不同VPC内的ECS实例无法进行通信，天然地进行了隔离。

基于隧道技术和软件定义网络（Software Defined Network，简称SDN）技术，阿里云的研发在硬件网关和自研交换机设备的基础上实现了VPC产品。

逻辑架构

如下图所示，VPC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，网关和控制器都是集群部署并且是多机房互备的，并且所有链路上都有冗余容灾，提升了VPC产品的整体可用性。


配置通路
数据通路
控制台
API
控制器
本地网络
Internet
网关
专有网络
192.168.0.0/16
交换机
交换机

4 产品优势

专有网络安全性高、配置灵活、支持多种连接方式。

安全

每个VPC都有一个独立的隧道号，一个隧道号对应着一个虚拟化网络。专有网络之间通过隧道ID进行隔离：

- 专有网络内部由于交换机和路由器的存在，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交换机互联，不同子网间使用路由器互联。
- 不同专有网络之间内部网络完全隔离，可以通过对外映射的IP（弹性公网IP和NAT IP）互连。
- 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，因此也实现了不同专有网络间二层网络隔离。
- 专有网络内的ECS使用安全组防火墙进行三层网络访问控制。

可控

您可以通过安全组规则、访问控制白名单等方式灵活地控制访问专有网络内云资源的出入流量。

易用

您可以通过专有网络控制台快速创建、管理专有网络。专有网络创建后，系统会自动为其创建一个路由器和路由表。

可扩展

您可以在一个专有网络内创建不同的子网，部署不同的业务。此外，您可以将一个VPC和本地数据中心或其他VPC相连，扩展网络架构。

5 应用场景

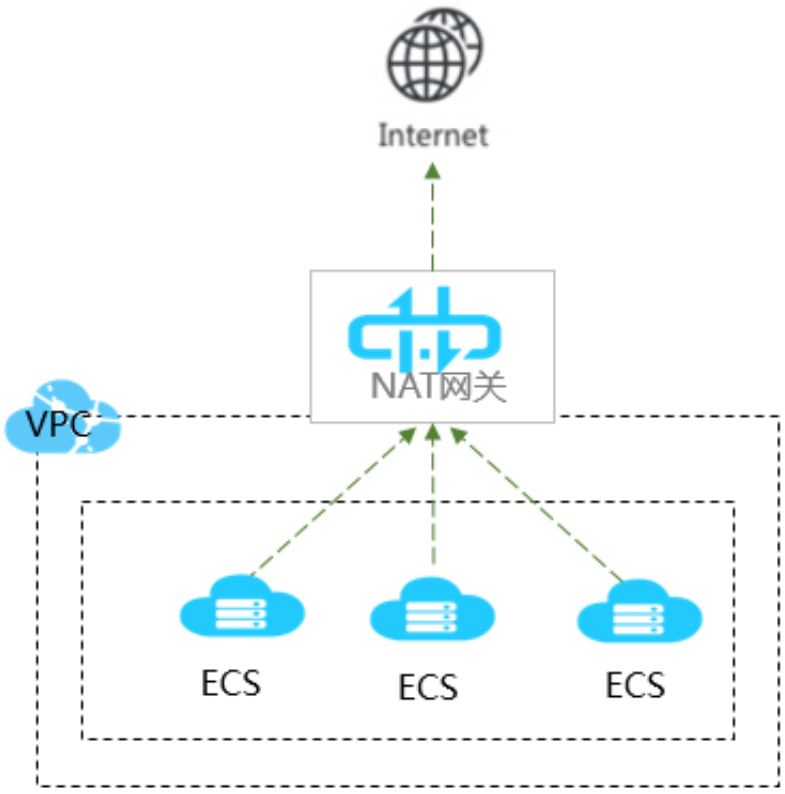
专有网络（VPC）是完全隔离的网络环境，配置灵活，可满足不同的应用场景。

托管应用程序

您可以将对外提供服务的应用程序托管在VPC中，并且可以通过创建安全组规则、访问控制白名单等方式控制Internet访问。您也可以在应用程序服务器和数据库之间进行访问控制隔离，将Web服务器部署在能够进行公网访问的子网中，将应用程序的数据库部署在没有配置公网访问的子网中。

托管主动访问公网的应用程序

您可以将需要主动访问公网的应用程序托管在VPC中的一个子网内，通过网络地址转换（NAT）网关路由其流量。通过配置SNAT规则，子网中的实例无需暴露其私网IP地址即可访问Internet，并可随时替换公网IP，避免被外界攻击。

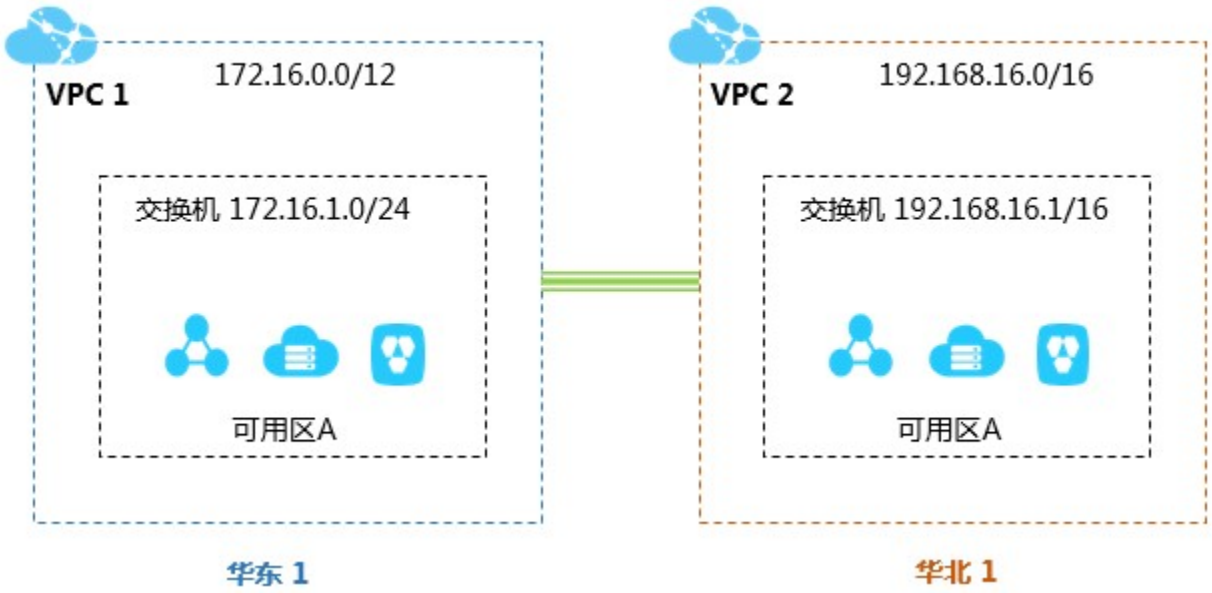


跨可用区容灾

您可以通过创建交换机为专有网络划分一个或多个子网。同一专有网络内不同交换机之间内网互通。您可以通过将资源部署在不同可用区的交换机中，实现跨可用区容灾。

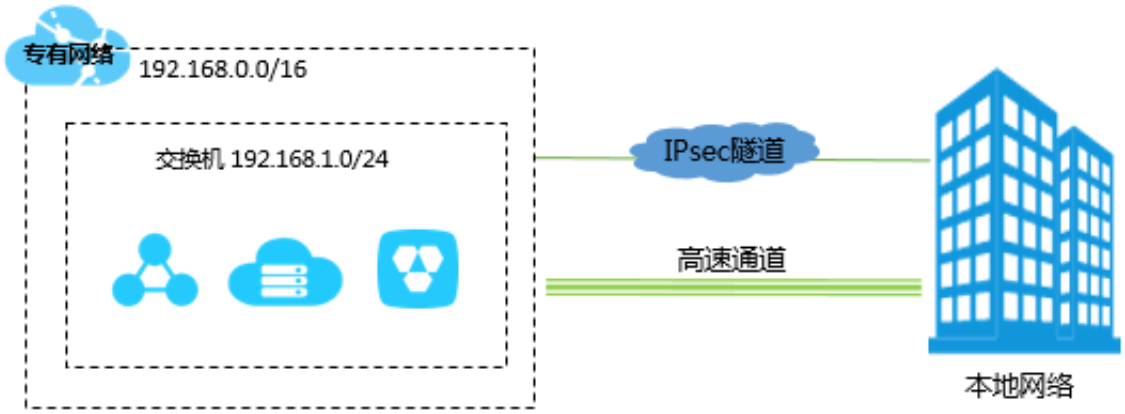
业务系统隔离

不同的VPC之间逻辑隔离。如果您有多个业务系统例如生产环境和测试环境要严格进行隔离，那么可以使用多个VPC进行业务隔离。当有互相通信的需求时，可以在两个VPC之间建立对等连接。



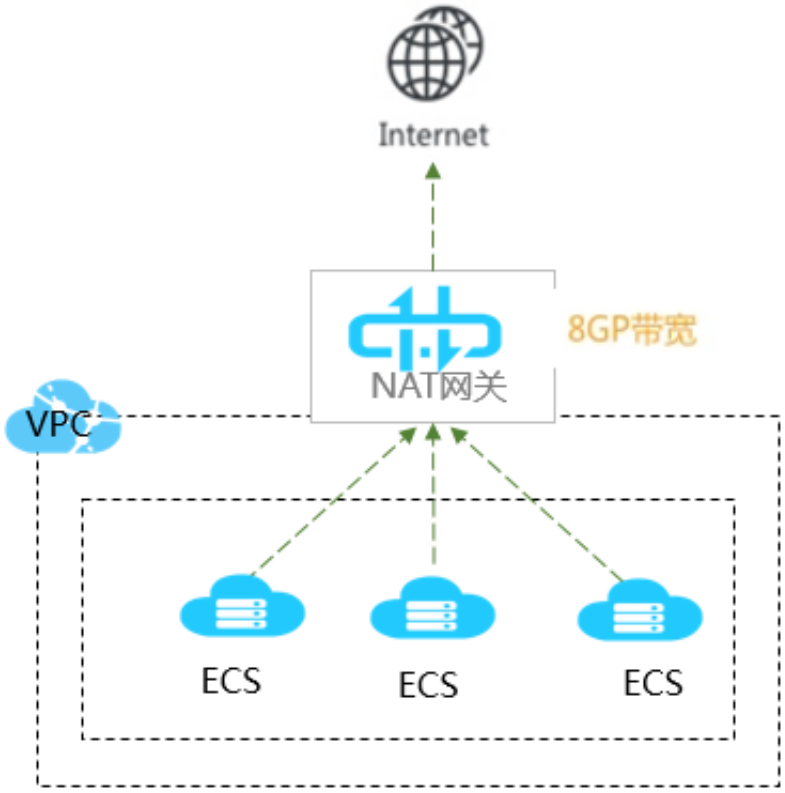
构建混合云

VPC提供专用网络连接，可以将本地数据中心和VPC连接起来，扩展本地网络架构。通过该方式，您可以将本地应用程序无缝地迁移至云上，并且不必更改应用程序的访问方式。



多个应用流量波动大

如果您的应用带宽波动很大，您可以通过NAT网关配置DNAT转发规则，然后将EIP添加到共享带宽中，实现多IP共享带宽，减轻波峰波谷效应，从而减少您的成本。


Internet
NAT网关
8GP带宽
VPC
ECS
ECS
ECS

6 基本概念

本章节介绍专有网络VPC涉及的基本概念，以便于您更好地理解专有网络。

术语	说明
专有网络 （VPC）	专有网络是您基于阿里云创建的自定义私有网络，不同的专有网络之间逻辑上彻底隔离。您可以在自己创建的专有网络内创建和管理云资源，例如ECS，SLB，RDS等。
交换机（VSwitch）	交换机是组成专有网络的基础网络设备。交换机可以连接不同的云资源。在专有网络内创建云资源时，必须指定云资源所连接的交换机。
路由器（VRouter）	路由器是专有网络的枢纽。路由器可以连接专有网络的各个交换机，同时也是连接专有网络与其它网络的网关设备。路由器根据路由条目来转发网络流量。
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）	路由表中的每一项是一条路由条目。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。

7 使用限制

使用专有网络VPC前，请了解下表中的使用限制。

资源	默认限制	提升配额
每个地域可创建的专有网络数量	10	提交工单
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及其子网	提交工单
单个专有网络的路由器数量	1	无法调整
单个专有网络的交换机数量	24	提交工单
单个专有网络的路由表数量	10	提交工单
单个路由表的自定义路由条目数量	48	提交工单
单个专有网络支持云资源使用网络地址数量 例如，ECS实例仅有一个私网IP时，该ECS实例使用一个网络地址。当ECS实例绑定了多个网卡或网卡配置了多个IP时，该ECS使用的网络地址数为这些与之绑定的网卡上分配的VPC地址数量之和	15,000	无法调整