专有网络 VPC

VPC 产品简介

VPC 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

- 新加坡
- 华南 1
- 华北 2
- 华东 2
- 美东 1
- 香港
- 华东 1
- 美西 1

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

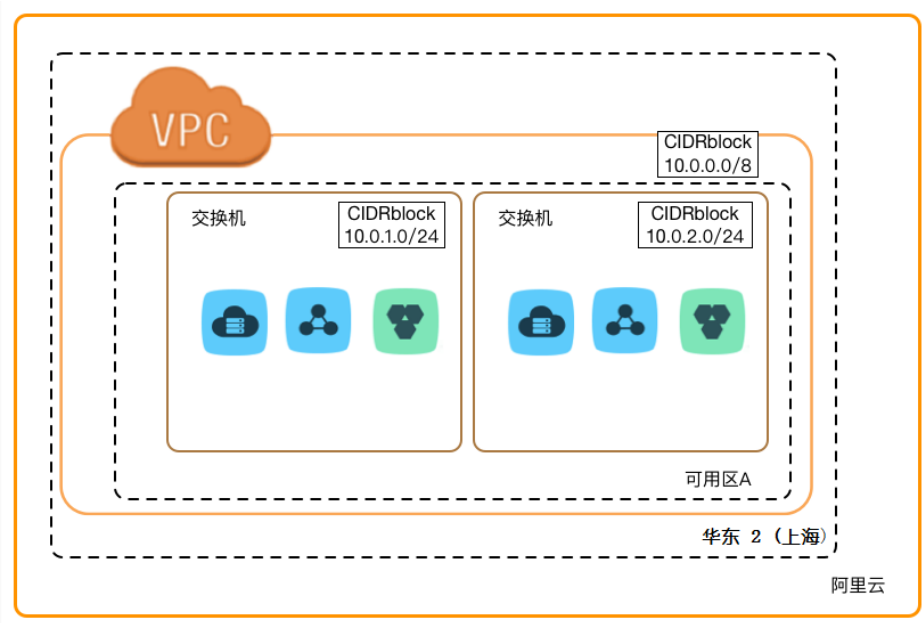
- 支持软件VPN
- 支持专线连接

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。

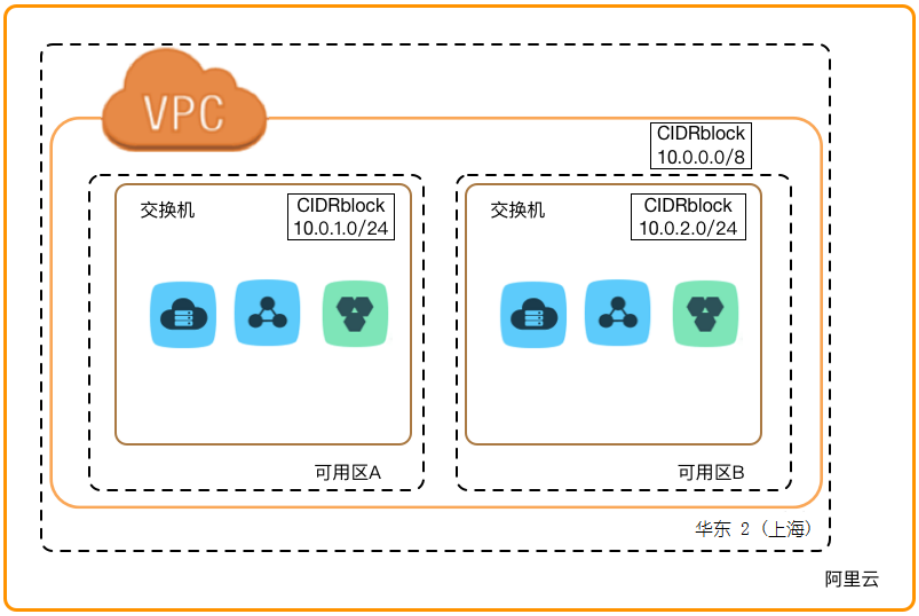
场景一：在阿里云上管理用户专属的网络

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。



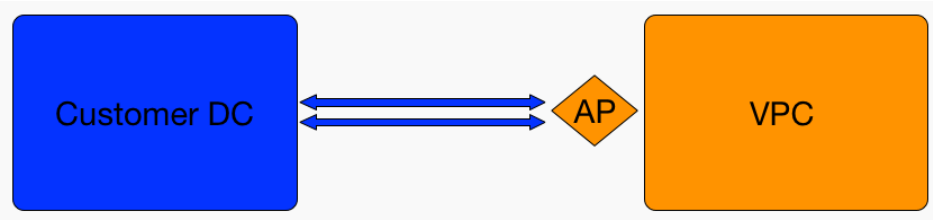
场景二：VPC中跨可用区部署资源

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，支持最多4条线路做ECMP流量负载。



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。

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。

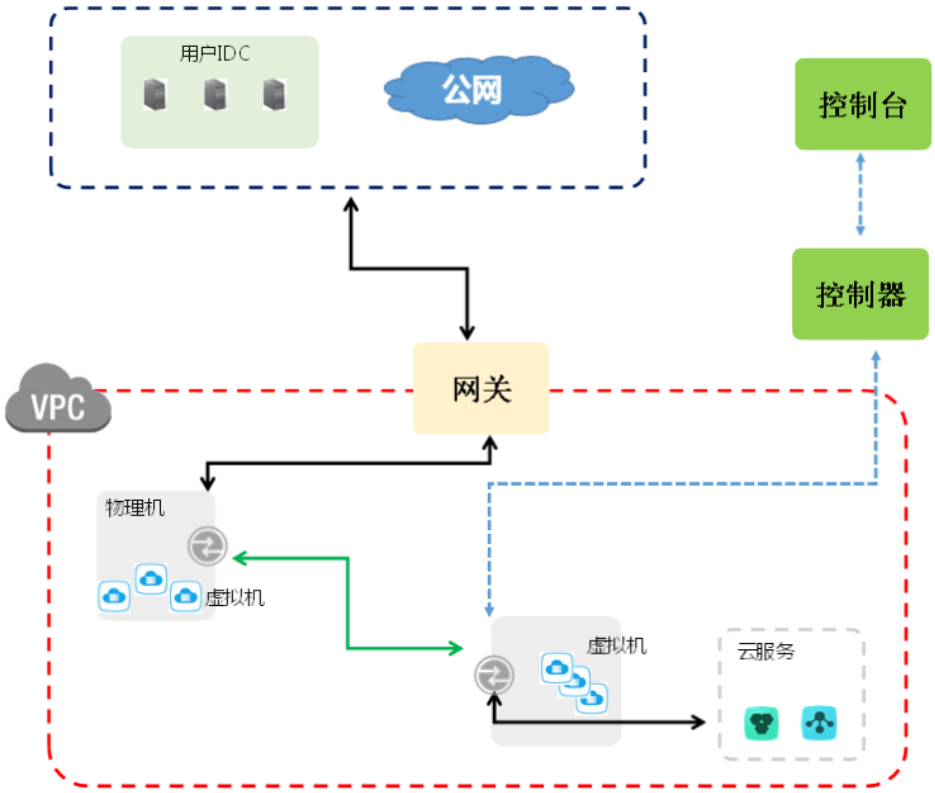
原理描述

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。

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

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。

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

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