阿里云
专有网络VPC

用户指南

文档版本：20190617

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 专有网络和子网

1.1 概述

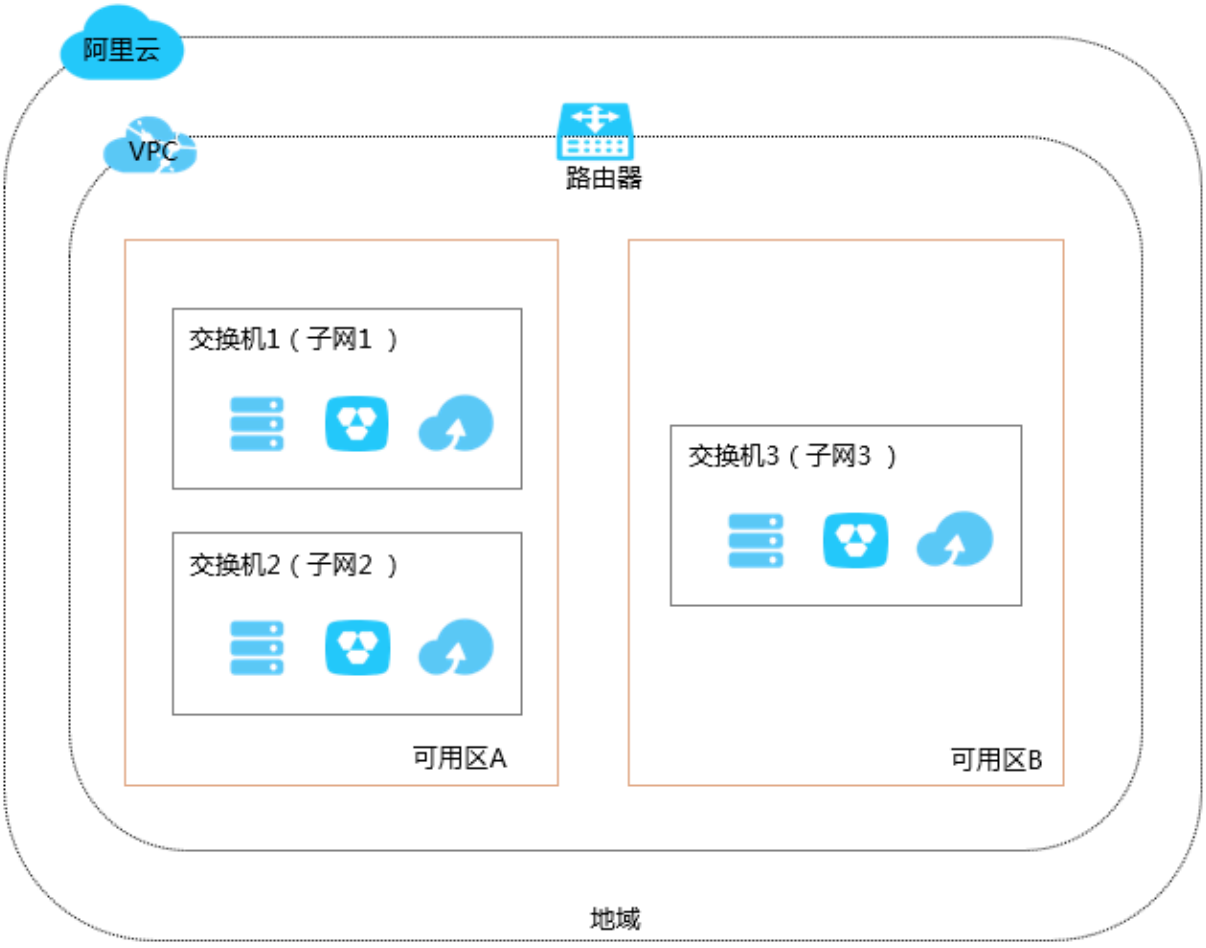
在专有网络（VPC）中使用云资源前，您必须要创建一个VPC和交换机。您可以在一个VPC中创建多个交换机来划分子网。一个VPC内的子网默认私网互通。

专有网络和子网

专有网络VPC（Virtual Private Cloud）是您独有的云上虚拟网络。您可以将云产品部署在您自定义的VPC中。

> **说明:**
> 云产品不可以直接部署在VPC内，必须属于VPC内的一个交换机（子网）内。

交换机（VSwitch）是组成专有网络的基础网络设备，用来连接不同的云产品实例。VPC是地域级别的资源，VPC不可以跨地域，但包含所属地域的所有可用区。您可以在每个可用区内创建一个或多个交换机来划分子网。



网段和IP地址

专有网络支持IPv4和IPv6寻址协议。默认情况下，专有网络使用IPv4寻址协议。您可以根据需要开通IPv6寻址协议。详细说明，请参见开通IPv6。

VPC可在双栈模式下运行。VPC中的资源可通过IPv4和IPv6进行通信。IPv4和IPv6地址是彼此独立的，您需要在VPC中分别针对IPv4和IPv6配置路由和安全组。

下表总结了IPv4地址和IPv6地址的差异。

IPv4 VPC	IPv6 VPC
格式为32位，4组，每组最多3个数字。	格式为128位，8组，每组4个十六进制数字。
默认开启IPv4地址协议。	可以选择开通。
VPC地址块大小可以从 /8 到 /24。	VPC地址块大小固定为 /56。
交换机地址块大小可以从 /16 到 /29。	交换机地址块大小固定为 /64。
可以选择要使用的IPv4地址块。	无法选择要使用的IPv6地址块。系统会从IPv6地址池中为您的VPC选择IPv6地址块。
所有实例类型都支持。	部分实例类型不支持。 详细说明，请参见实例规格族汇总。
支持配置ClassicLink连接。	不支持配置ClassicLink连接。
支持弹性公网IPv4地址。	不支持弹性公网IPv6地址。
支持配置VPN网关和NAT网关。	不支持配置VPN网关和NAT网关。

默认，VPC的IPv4和IPv6地址都只支持私网通信。同一VPC内不同交换机的云产品可通过私网通信。如果您需要连接其他VPC或本地IDC，可配置智能接入网关、高速通道和VPN网关等方式实现互通。详细说明，请参见连接本地IDC。

如果需要进行公网通信，需要分别进行配置：

- IPv4公网通信

  您可以通过配置弹性公网IP或NAT网关的方式使VPC内的ECS实例通过IPv4地址进行通信。

  详细说明，请参见绑定ECS实例和配置NAT网关。

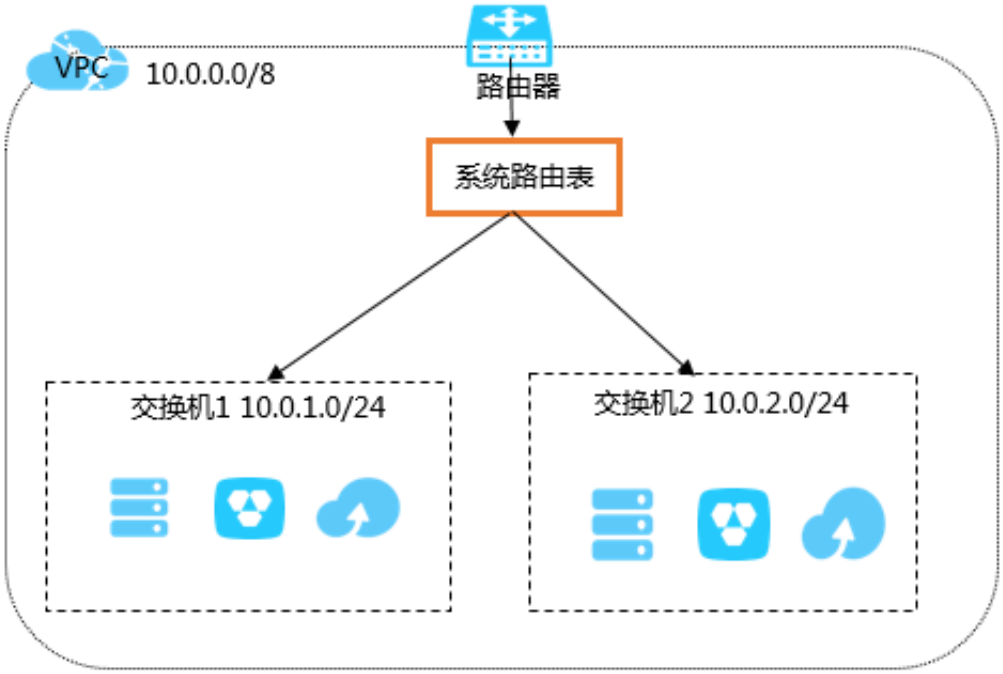
- IPv6公网通信

  您需要为进行公网通信的IPv6地址购买公网带宽。您也可以为该IPv6地址配置仅出公网规则，只允许VPC中的云产品实例经IPv6地址访问公网，而不允许IPv6客户端主动与VPC中的云产品实例建立连接。

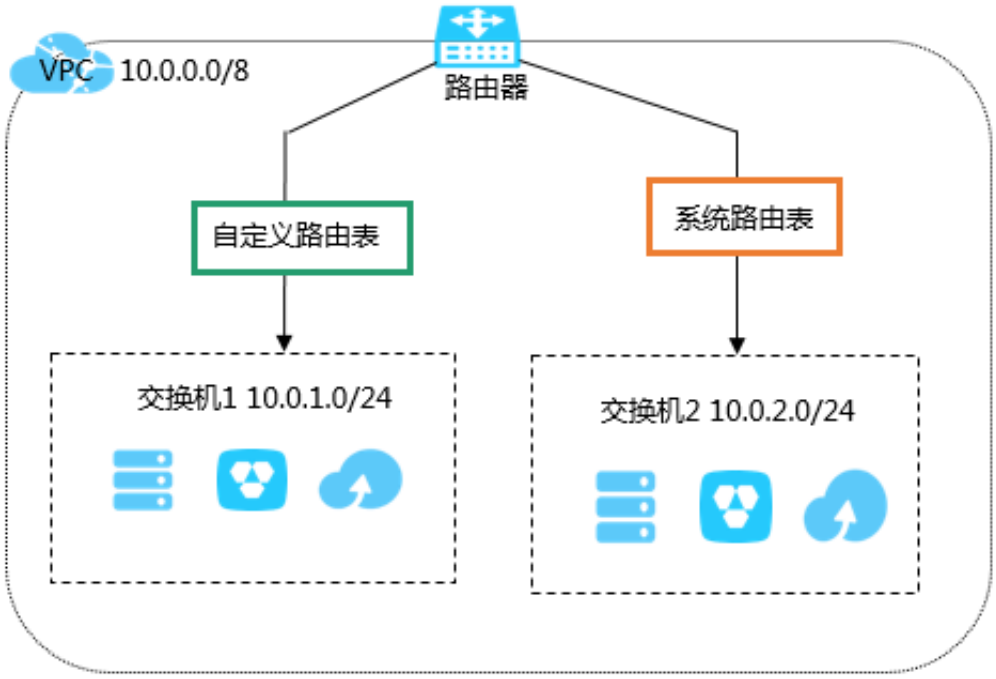
  详细说明，请参见开通IPv6公网带宽和创建仅主动出规则。

路由

创建专有网络后，系统会自动为您创建一张默认路由表并为其添加系统路由来管理专有网络的流量。一个VPC只有一张系统路由表。该系统路由表在创建VPC的时候自动为您创建，您不能手动创建也不能删除默认系统路由表。



您可以在专有网络内创建自定义路由表，然后将其和交换机绑定来控制子网路由，更灵活地进行网络管理。每个交换机只能关联一张路由表。详细说明，请参见管理路由表。



路由表采用最长前缀匹配原则作为流量的路由选路规则。最长前缀匹配是指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。您可以添加自定义路由条目将目标流量路由到指定的目的地。详细说明，请参见添加自定义路由条目。

1.2 创建默认专有网络和交换机

当创建一个云产品实例时，如果没有可用的专有网络和交换机，您可以使用默认专有网络和交换机。在实例创建后，一个默认的专有网络和交换机也会随之创建好。本文以ECS为例介绍如何创建默认专有网络和交换机。

背景信息

每个地域只有一个默认专有网络，但每个专有网络内的每个可用区都可创建一个默认交换机。默认专有网络和交换机的说明如下：

默认专有网络VPC	默认交换机
每个地域的默认专有网络唯一。	每个可用区的默认交换机唯一。
默认专有网络的网段掩码是16位，如172.31.0.0/16，最多可提供65536个私网IP地址。	默认交换机的网段掩码是20位，如172.16.0.0/20，最多可提供4096个私网IP地址。
默认专有网络不占用阿里云为您分配的专有网络配额。	默认交换机不占用专有网络中可创建交换机的配额。
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。

默认专有网络VPC	默认交换机
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。	默认交换机与非默认交换机的操作方式与规格限制一致。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，单击实例，然后单击创建实例。
3. 选择自定义购买。
4. 在基础配置页面，设置实例的基本配置，然后单击下一步：网络和安全组。
5. 在网络和安全组配置页面，选择使用默认专有网络和默认交换机。配置完成后，单击下一步：系统配置。

图 1-1: 默认VPC和交换机

6. 配置实例名称和登录凭证，然后单击确认订单。

   实例创建后，在ECS实例的所属地域也会随之创建一个默认专有网络和交换机。

图 1-2: 默认VPC

图 1-3: 默认交换机

1.3 管理专有网络

专有网络（Virtual Private Cloud，简称VPC）是您自己独有的的云上私有网络。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。您可以在专有网络中使用阿里云资源如云服务器ECS、云数据库RDS和负载均衡等。

创建专有网络和交换机

在专有网络中部署云资源，您必须至少创建一台交换机。

完成以下操作步骤，创建专有网络和交换机：

1. 登录专有网络管理控制台。
2. 在顶部菜单栏，选择专有网络的地域。

   专有网络的地域和要部署的云资源的地域必须相同。
3. 单击创建专有网络，根据以下信息配置专有网络和交换机，然后单击确定。

> 说明：
> 目前，仅华北5（呼和浩特地域）支持开通IPv6。开通后，系统会创建一个IPv6网关。详细信息，请参见什么是IPv6网关#

配置	说明
专有网络配置	
名称	专有网络的名称。 长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。

配置	说明
IPv4网段	建议您使用RFC私网地址作为专有网络的网段。 · 您可以使用192.168.0.0/16、172.16.0.0/12和10.0.0.0/8这三个标准网段或其子集。如果要使用标准网段的子网作为VPC的网段，需要使用CreateVpc创建VPC。详细信息，请参见CreateVpc。 · 如果有多个VPC，或者VPC和本地数据中心互连构建混合云的需求，建议使用上面这些标准网段的子网作为VPC的网段，掩码不超过/16。 · 如果云上只有一个VPC并且不需要和本地数据中心互通，那么选择以上任何一个网段或其子网。 注意: VPC创建后，不能再修改IPv4网段。
IPv6网段	选择是否给VPC分配IPv6网段，默认不分配IPv6网段。 如果您选择分配IPv6网段，系统将为您的VPC自动分配掩码为/56的IPv6网段，如2xx1:db8::/56。 注意: VPC创建后，不能再修改IPv6网段。
描述	输入VPC的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。
资源组	选择VPC所属的资源组。
交换机配置	
名称	交换机的名称。 长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
可用区	交换机的可用区。同一VPC内不同可用区的交换机内网互通。

配置	说明
IPv4网段	交换机的IPv4网段。交换机的网段限制如下： · 交换机的网段可以和其所属的VPC网段相同或者是其VPC网段的子集。 例如，VPC的网段是192.168.0.0/16，那么该VPC内的交换机的网段可以是192.168.0.0/16，也可以是192.168.0.0/17，一直到192.168.0.0/29。 说明： 如果交换机的网段和专有网络的网段相同，您只能创建一个交换机。 · 交换机的网段的大小在16位网络掩码与29位网络掩码之间，可提供8-65536个地址。 · 每个交换机的第一个和最后三个IP地址为系统保留地址。 以192.168.1.0/24为例，192.168.1.0、 192.168.1.253、 192.168.1.254和192.168.1.255这些地址是系统保留地址。 · 如果该交换机有和其他专有网络的交换机，或本地数据中心通信的需求，确保交换机的网段和要通信的网段不冲突。 注意： 交换机创建后，不能再修改网段。
IPv6网段	交换机的IPv6网段。 交换机的IPv6网段的掩码默认为/64，您可以输入十进制数字0-255，来自定义交换机IPv6网段的最后8比特位。 如VPC的IPv6网段为2xx1:db8::/64，在交换机的IPv6网段输入十进制数字255（对应十六进制为ff），则交换机的IPv6网段将为2xx1:db8:ff::/64。
描述	输入交换机的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。

删除专有网络

确保您已删除该专有网络下的所有交换机。专有网络删除后，关联的路由器和路由表也会随之删除。

完成以下操作，删除专有网络：

1. 在专有网络控制台，选择VPC的所属地域。
2. 找到目标VPC，然后单击删除。
3. 在弹出的对话框中，单击确定。

开启ClassicLink功能

开启ClassicLink功能建立ClassicLink连接后，经典网络的ECS实例便可和专有网络中的云资源进行私网通信。详细信息，请参见ClassicLink概述。

完成以下操作，开启ClassicLink功能：

1. 在专有网络控制台，选择VPC的所属地域。
2. 单击目标VPC的ID。
3. 在专有网络详情页面，单击开启ClassicLink。

4. 单击确定。
5. 建立ClassicLink连接。

   详细说明，请参见建立ClassicLink连接。

加入云企业网

您可以将VPC加入一个已创建的云企业网（Cloud Enterprise Network，简称CEN）实例中，使VPC和云企业网实例中的其他VPC或本地数据中心互通。详细信息，请参见什么是云企业网。

完成以下操作，快速加入同账号下的云企业网实例：

1. 在专有网络控制台，选择VPC的所属地域。
2. 单击目标VPC的ID。

3. 在专有网络详情页面，单击加入云企业网。

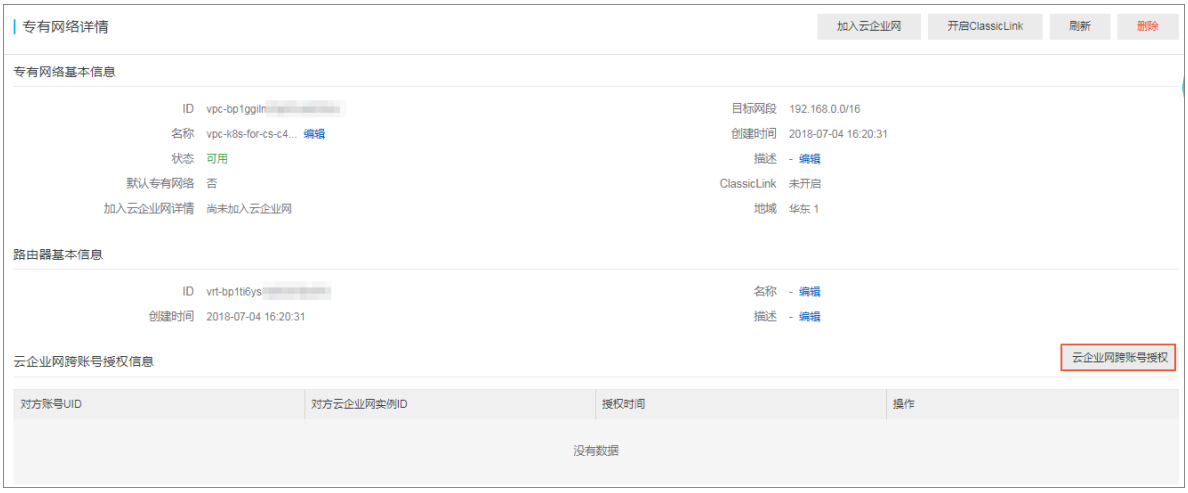
4. 选择已创建的云企业网实例，然后单击确定。

CEN跨账号授权

如果您需要将该VPC加载到其他账号所属的CEN实例中，实现和其他网络实例互通，您需要先进行授权。

完成以下操作，授权其他账号的CEN加载该VPC：

1. 在专有网络控制台，选择VPC的所属地域。
2. 单击目标VPC的ID。
3. 在云企业网跨账号授权信息区域，单击云企业网跨账号授权。



4. 在加入云企业网对话框中，输入云企业网实例所属的账号ID和云企业网实例ID，然后单击确定。

相关API

CreateVpc

DescribeVpcAttribute

DeleteVpc

DescribeVpcs

1.4 管理交换机

交换机（VSwitch）是组成专有网络的基础网络模块，用来连接不同的云产品实例。

创建专有网络之后，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。云资源必须部署在交换机内，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。

说明:

交换机不支持组播和广播。

创建交换机

完成以下操作创建一个交换机：

1. 登录专有网络管理控制台。
2. 选择交换机所属VPC的地域。
3. 在左侧菜单栏，单击交换机。
4. 单击创建交换机，根据以下信息配置交换机，然后单击确定。

说明:

目前，仅华北5（呼和浩特地域）支持开通IPv6地址块。开通后，系统会创建一个IPv6网关。详细信息，请参见什么是IPv6网关#

配置	说明
资源组	选择交换机的所属资源组。
专有网络	选择交换机的所属专有网络。
IPv4网段	所选专有网络的IPv4网段。
IPv6网段	所选专有网络的IPv6网段。  **说明:** 如果选择的专有网络未开启IPv6网段，单击开通IPv6网段。开通后，系统将为您创建免费版IPv6网关。
描述	输入VPC的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。

配置	说明
名称	交换机的名称。 长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
可用区	交换机的可用区。同一VPC内不同可用区的交换机内网互通。
IPv4网段	交换机的IPv4网段。交换机的网段限制如下： · 交换机的网段可以和其所属的VPC网段相同或者是其VPC网段的子集。 例如，VPC的网段是192.168.0.0/16，那么该VPC内的交换机的网段可以是192.168.0.0/16，也可以是192.168.0.0/17，一直到192.168.0.0/29。 说明: 如果交换机的网段和专有网络的网段相同，您只能创建一个交换机。 · 交换机的网段的大小在16位网络掩码与29位网络掩码之间，可提供8-65536个地址。 · 每个交换机的第一个和最后三个IP地址为系统保留地址。 以192.168.1.0/24为例，192.168.1.0、 192.168.1.253、 192.168.1.254和192.168.1.255这些地址是系统保留地址。 · 如果该交换机有和其他专有网络的交换机，或本地数据中心通信的需求，确保交换机的网段和要通信的网段不冲突。 注意: 交换机创建后，不能再修改网段。
可用IP数量	显示交换机可用的IPv4地址数量。

配置	说明
IPv6网段	交换机的IPv6网段。 交换机的IPv6网段的掩码默认为/64，您可以输入十进制数字0-255，来自定义交换机IPv6网段的最后8比特位。 如VPC的IPv6网段为2001:db8::/64，在交换机的IPv6网段输入十进制数字255（对应十六进制为ff），则交换机的IPv6网段将为2001:db8::ff/64。
描述	输入交换机的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。

在交换机中创建云资源

完成以下操作，在交换机中创建云资源：

1. 登录专有网络管理控制台。
2. 选择VPC的地域。
3. 在左侧菜单栏，单击交换机。
4. 找到目标交换机，单击购买，选择要创建的云资源。

> 说明：
> 目前，支持在交换机中创建的云资源包括：ECS实例，SLB实例和RDS实例。

删除交换机

在删除交换机前，确保：

- 您已经删除该交换机下创建的云资源如ECS、SLB、RDS等。
- 如果该交换机配置了SNAT条目、HAVIP等，确保您已经删除这些关联的资源。

完成以下操作，删除交换机：

1. 登录专有网络管理控制台。
2. 选择VPC的地域。
3. 在左侧菜单栏，单击交换机。
4. 找到目标交换机，然后单击删除。

5. 在弹出的对话框中，单击确定。

相关API

CreateVSwitch

DescribeVSwitchAttributes

DeleteVSwitch

DescribeVSwitches

2 路由

2.1 概述

创建专有网络后，系统会自动为您创建一张默认路由表并为其添加系统路由来管理专有网络的流量。您不能创建系统路由，也不能删除系统路由，但您可以创建自定义路由，将指定目标网段的流量路由至指定的目的地。

路由表

创建专有网络后，系统会默认创建一个路由表控制专有网络的路由，所有专有网络内的交换机默认使用该路由表。您不能创建也不能删除默认路由表，但您可以在专有网络内创建自定义路由表，然后将其和交换机绑定来控制子网路由，更灵活地进行网络管理。详细说明，请参见管理路由表。

路由表中的每一项是一条路由条目。路由条目指定了网络流量的导向目的地，由目标网段、下一跳类型、下一跳三部分组成。路由条目包括系统路由和自定义路由。

在管理路由表时，注意：

- 每个专有网络最多可以有10张路由表，包括系统路由表。
- 每个交换机只能绑定一张路由表。交换机（子网）的路由策略由其关联的路由表管理。
- 交换机创建后，该交换机默认与系统路由表绑定。
- 如果您需要将交换机绑定的自定义路由表更换成系统路由表，直接将自定义路由表与交换机解绑即可。如果您需要绑定其他路由表，需要先将交换机与当前路由表解绑，再绑定指定的自定义路由表。
- 目前，除华北2（北京）、华南1（深圳）和华东1（杭州）外所有地域都已支持自定义路由表。
- 自定义路由表不支持主备路由和负载路由。

系统路由

创建专有网络后，系统会在路由表中自动添加如下系统路由：

- 以100.64.0.0/10为目标网段的路由条目，用于VPC内的云产品通信。
- 以交换机网段为目标网段的路由条目，用于交换机内的云产品通信。

比如您创建了一个网段为192.168.0.0/16的专有网络，并在该专有网络下创建了两个网段为192.168.1.0/24和192.168.0.0/24的交换机，则该专有网络的路由表中会有如下三条系统路由：

目标网段	下一跳	类型
100.64.0.0/10	-	系统路由

目标网段	下一跳	类型
192.168.1.0/24	-	系统路由
192.168.0.0/24	-	系统路由

自定义路由

您可以添加自定义路由来替换系统路由或将目标流量路由到指定的目的地。在添加自定义路由时，您可以指定以下下一跳类型：

- ECS实例：将指向目标网段的流量转发到专有网络内的一台ECS实例。

  当需要通过该ECS实例部署的应用访问互联网或其他应用时，配置此类型的路由。
- VPN网关：将指向目标网段的流量转发到一个VPN网关。

  当需要通过VPN网关连接本地网络或者其他专有网络时，配置此类型的路由。
- 路由器接口（专有网络方向）：将指向目标网段的流量转发到一个专有网络内。

  当需要使用高速通道连接两个专有网络时，配置此类型的路由。
- 路由器接口（边界路由器方向）：将指向目标网段的流量转发到一个边界路由器。

  当需要使用高速通道连接本地网络（物理专线接入）时，配置此类型的路由。
- 辅助弹性网卡：将指向目标网段的流量转发到指定的辅助弹性网卡。

IPv6路由

如果您的VPC开通了IPv6。VPC的系统路由表中会自动添加以下路由条目：

- 以::/0为目标网段，下一跳为IPv6网关实例的自定义路由条目，用于VPC内云产品经IPv6地址与互联网通信。
- 以交换机IPv6网段为目标网段的系统路由条目，用于交换机内的云产品通信。

> 说明：
> 如果您创建了自定义路由表，并且绑定了开通了IPv6网段的交换机，您需要手动添加一条以::/0为目标网段，下一跳为IPv6网关实例的自定义路由条目。详细说明，请参见添加自定义路由条目。

选路规则

路由表采用最长前缀匹配原则作为流量的路由选路规则。最长前缀匹配是指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。

某专有网络的路由表如下表所示。

目标网段	下一跳类型	下一跳	路由条目类型
100.64.0.0/10	-	-	系统
192.168.0.0/24	-	-	系统
0.0.0.0/0	Instance	i-12345678	自定义
10.0.0.0/24	Instance	i-87654321	自定义

目标网段为`100.64.0.0/10`和`192.168.0.0/24`的两条路由均为系统路由。目标网段为`0.0.0.0/0`和`10.0.0.0/24`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`10.0.0.0/24`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-87654321`，而访问`10.0.1.1`的流量会转发至`i-12345678`。

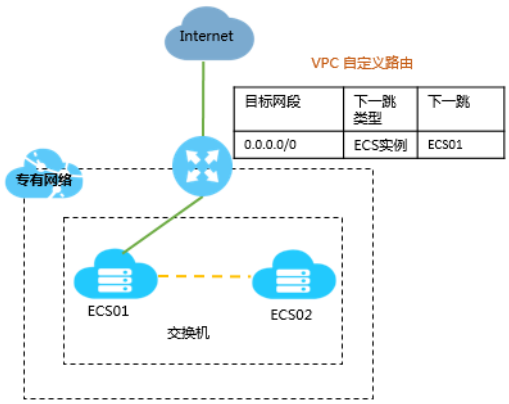
路由示例

您可以通过在路由表中添加自定义路由条目控制专有网络的出入流量。

- VPC内网路由

  如下图所示，当您在VPC内的一台ECS实例（ECS01）自建了NAT网关，专有网络内的云资源需要通过该ECS实例访问公网时，可以添加如下一条自定义路由：

目标网段	下一跳类型	下一跳
0.0.0.0/0	ECS实例	ECS01



- VPC互通（高速通道）

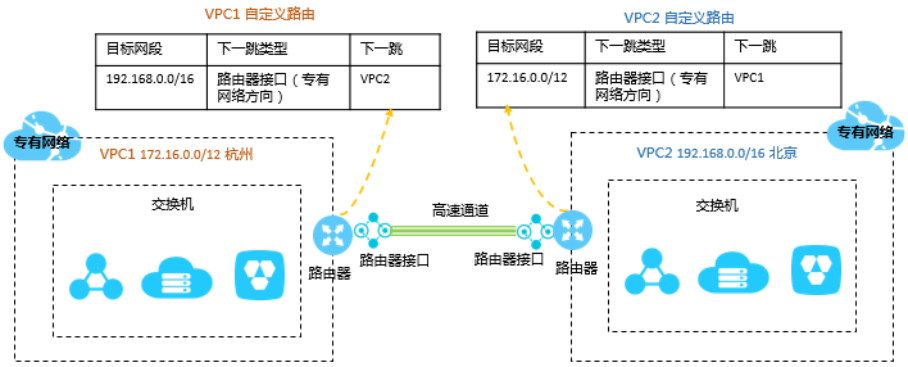
  如下图所示，当使用高速通道连接两个VPC（VPC1 172.16.0.0/12和VPC2 192.168.0.0/16）时，创建完两个互相连接的路由器接口后，您还需要在两个VPC中分别添加如下一条路由：

  - VPC1的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口（专有网络方向）	VPC2

  - VPC2的路由配置

目标网段	下一跳类型	下一跳
172.16.0.0/12	路由器接口（专有网络方向）	VPC1



- VPC互通（VPN网关）

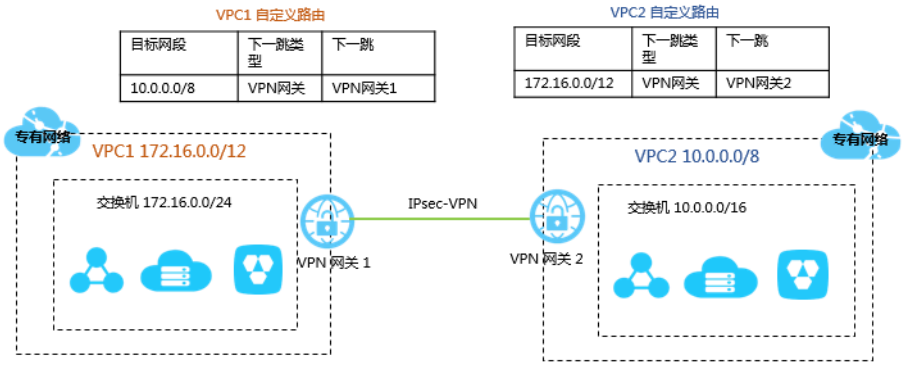
  如下图所示，当使用VPN网关连接两个VPC（VPC1 172.16.0.0/12和VPC2 10.0.0.0/8）时，配置完VPN网关后，需要在VPC中分别添加如下路由：

  - VPC1的路由配置

目标网段	下一跳类型	下一跳
10.0.0.0/8	VPN网关	VPN网关1

  - VPC2的路由配置

目标网段	下一跳类型	下一跳
172.16.0.0/12	VPN网关	VPN网关2



- 连接本地IDC（高速通道）

  如下图所示，当使用高速通道物理专线连接专有网络和本地网络时，配置完专线和边界路由器后，需要配置如下路由：

  - VPC端的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口（普通路由）	路由器接口RI1

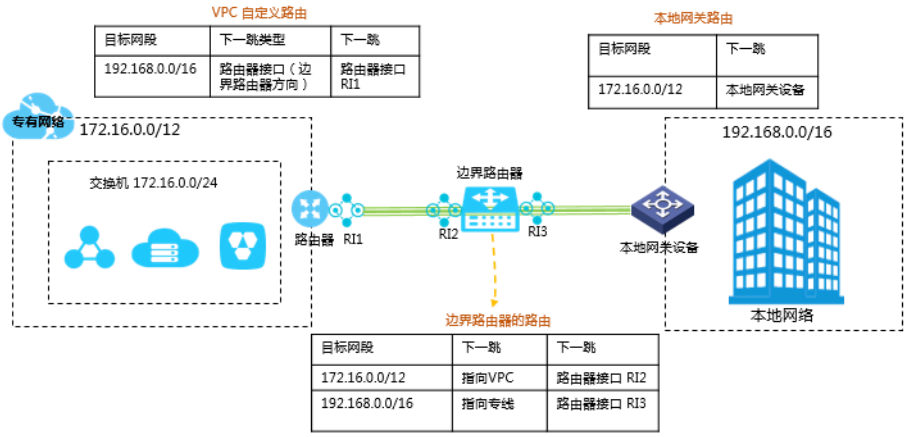
  - 边界路由器的路由配置

目标网段	下一跳类型	下一跳
192.168.0.0/16	指向专线	路由器接口RI3

目标网段	下一跳类型	下一跳
172.16.0.0/12	指向VPC	路由器接口RI2

- 本地网络的路由配置

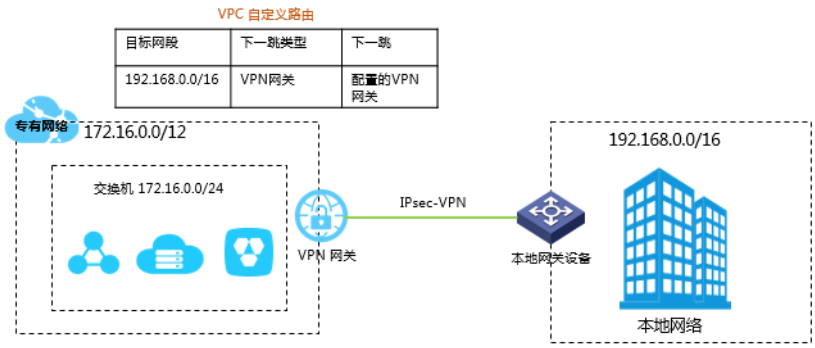
目标网段	下一跳类型	下一跳
172.16.0.0/12	—	本地网关设备



· 连接本地IDC（VPN网关）

如下图所示，当使用VPN网关连接VPC（网段：172.16.0.0/12）和本地网络（网段：192.168.0.0/16）时，配置好VPN网关后，需要在VPC内添加如下一条路由：

目标网段	下一跳类型	下一跳
192.168.0.0/16	VPN网关	已创建的VPN网关



2.2 管理路由表

路由表由路由条目组成，每个路由条目指定了网络流量的目的地。除默认路由表外，您还可以创建自定义路由表，管理子网路由流量。

创建自定义路由表

完成以下操作，创建自定义路由表：

1. 登录专有网络控制台。
2. 在左侧导航栏，单击路由表。
3. 在路由表页面，单击创建路由表。
4. 根据以下信息配置路由表，然后单击确定。

配置	说明
名称	输入路由表的名称。 名称长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
专有网络	选择路由表的所属专有网络。
描述	输入路由表的描述。 描述长度为在2-256个字符，不能以`http://`和`https://`开始。

您可以在路由表页面，查看管理自定义路由表。

绑定交换机

您可以将创建的路由表绑定到交换机上，控制该交换机（子网）的路由。一个交换机只能关联一张路由表包括系统路由表。

完成以下操作，将创建的自定义路由表绑定到一个交换机上：

1. 登录专有网络控制台。
2. 在左侧导航栏，单击路由表。
3. 在路由表页面，单击目标自定义路由表的ID。
4. 单击已绑定交换机页签，然后单击绑定交换机。

5. 在弹出的对话框，选择要绑定的交换机，然后单击确定。
6. 单击路由条目列表页签，添加自定义路由。

   详细信息，请参见添加自定义路由条目。

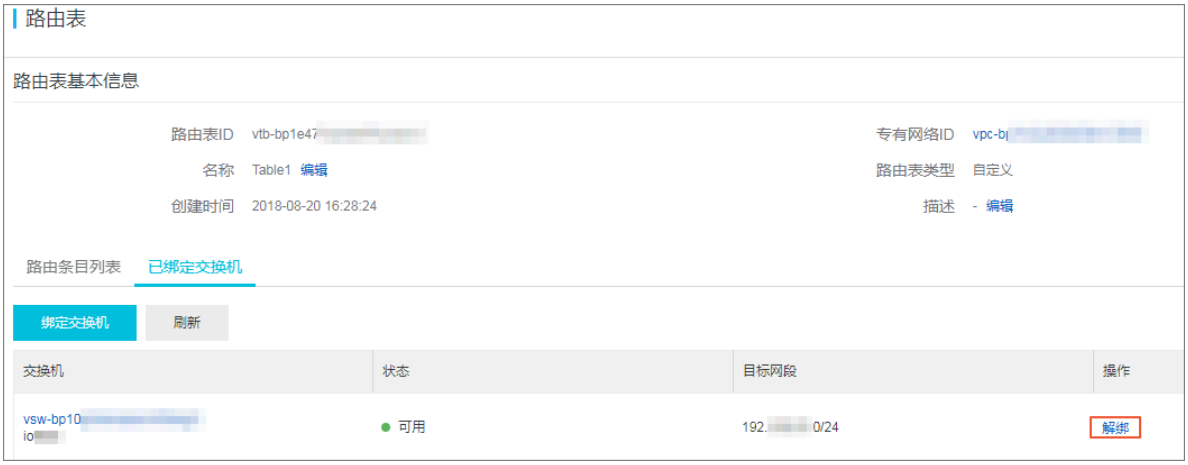
解绑交换机

您可以将自定义路由表和交换机解绑。解绑后，如果不再绑定其他路由表，则使用系统路由表。

完成以下操作，将自定义路由表和交换机解绑：

1. 登录专有网络控制台。
2. 在左侧导航栏，单击路由表。
3. 在路由表页面，单击目标自定义路由表的ID。
4. 单击已绑定交换机页签，找到目标交换机。

5. 单击解绑，然后在弹出的对话框，单击确定。



编辑自定义路由表

完成以下操作，修改自定义路由表的名称和描述：

1. 登录专有网络控制台。
2. 在左侧导航栏，单击路由表。
3. 在路由表页面，单击目标自定义路由表的ID。
4. 在路由表基本信息区域，修改其名称和描述。

2.3 添加自定义路由条目

创建专有网络后，系统会自动为您创建一张默认路由表并为其添加系统路由来管理专有网络的流量。您不能创建系统路由，也不能删除系统路由，但您可以创建自定义路由将指定目标网段的流量路由至指定的目的地。

背景信息

路由表中的每一项是一条路由条目。路由条目指定了网络流量的导向目的地，由目标网段、下一跳类型、下一跳三部分组成。路由条目包括系统路由和自定义路由。

无论是系统路由表还是自定义路由表，都可以添加自定义路由。

操作步骤

1. 登录专有网络控制台。
2. 选择VPC的所属地域。
3. 在左侧导航栏，单击路由表。

4. 单击目标路由表ID，然后单击路由条目列表页签。

5. 单击添加路由条目。

6. 在弹出的对话框，根据以下信息配置路由条目，然后单击确定。

配置	说明
目标网段	要转发到的目标网段。 · IPv4网段：转发IPv4地址的流量。 · IPv6网段：转发IPv6地址的流量。

配置	说明
下一跳类型和下一跳	选择下一跳类型： · ECS实例：将目的地址在目标网段范围内的流量路由至选择的ECS实例。 适用于将指定网络访问路由至ECS实例进行流量统一转发和管理的场景，例如将一台ECS实例配置为公网网关管理其他ECS实例访问公网。 · VPN网关：将目的地址在目标网段范围内的流量路由至选择的VPN网关。 · NAT网关：将目的地址在目标网段范围内的流量路由至选择的NAT网关。 · 辅助弹性网卡：将目的地址在目标网段范围内的流量路由至选择的辅助弹性网卡。 · 路由器接口（专有网络方向）：将目的地址在目标网段范围内的流量路由至选择的VPC。 适用于使用高速通道连接VPC的场景。 · 路由器接口（边界路由器方向）：将目的地址在目标网段范围内的流量路由至边界路由器关联的路由器接口。 适用于使用高速通道连接本地数据中心的场景。 此种模式下，您还需要选择路由的方式： - 普通路由：选择一个关联的路由器接口。 - 主备路由：主备路由仅支持两个实例作为下一跳，主路由下一跳权重为100，备份路由下一跳权重为0。当主路由健康检查失败时，备份路由生效。 - 负载路由：负载分担路由需要选择2-4个路由器接口作为下一跳，且作为下一跳的路由器接口的对端路由器类型必须为边界路由器。实例权重的有效范围为1-255的整数，默认值为100。每个实例的权重必须相同，系统会将流量平均分配给下一跳实例。 · IPv6网关：将目的地址在目标网段范围内的流量路由至选择的IPv6网关实例。 说明： 该选项只有当目标网段为IPv6网段时才可用。

2.4 添加子网路由到路由表

您可以在专有网络内创建自定义路由表，并在自定义路由表中添加子网路由，然后将自定义路由表绑定交换机，来控制该交换机的流量，更灵活地进行网络管理。

前提条件

您已经创建了专有网络和交换机。详细信息，请参见管理专有网络。

使用限制

添加子网路由到路由表，您必须了解以下限制：

- 每个专有网络最多可以有10张路由表，包括系统路由表。
- 每个交换机只能绑定一张路由表。
- 自定义路由表不支持主备路由和负载路由。
- 目前，除华北2（北京）、华南1（深圳）和华东1（杭州）地域外，其它地域均支持创建自定义路由表。

步骤一：创建自定义路由表

完成以下操作，创建自定义路由表：

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击路由表。
3. 选择路由表的地域。
4. 在路由表页面，单击创建路由表。
5. 在创建路由表页面，根据以下信息配置路由表，然后单击确定。

配置	说明
名称	输入路由表的名称。 名称长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
专有网络	选择路由表所属的专有网络。
描述	输入路由表的描述。 描述长度为在2-256个字符，不能以`http://`和`https://`开始。

步骤二：添加子网路由

完成以下操作，添加子网路由到路由表：

1. 在左侧导航栏，单击路由表。
2. 在路由表页面，找到目标路由表，单击操作列下的管理。
3. 在路由条目列表页签，单击添加路由条目。
4. 在添加路由条目页面，根据以下信息配置子网路由条目，然后单击确定。

配置	说明
目标网段	要转发到的目标网段。 · IPv4网段：转发IPv4地址的流量。 · IPv6网段：转发IPv6地址的流量。

配置	说明
下一跳类型和下一跳	选择下一跳类型： · ECS实例：将目的地址在目标网段范围内的流量路由至选择的ECS实例。 适用于将指定网络访问路由至ECS实例进行流量统一转发和管理的场景，例如将一台ECS实例配置为公网网关管理其他ECS实例访问公网。 · VPN网关：将目的地址在目标网段范围内的流量路由至选择的VPN网关。 · NAT网关：将目的地址在目标网段范围内的流量路由至选择的NAT网关。 · 辅助弹性网卡：将目的地址在目标网段范围内的流量路由至选择的辅助弹性网卡。 · 路由器接口（专有网络方向）：将目的地址在目标网段范围内的流量路由至选择的VPC。 适用于使用高速通道连接VPC的场景。 · 路由器接口（边界路由器方向）：将目的地址在目标网段范围内的流量路由至边界路由器关联的路由器接口。 适用于使用高速通道连接本地数据中心的场景。 此种模式下，您还需要选择路由的方式： - 普通路由：选择一个关联的路由器接口。 - 主备路由：主备路由仅支持两个实例作为下一跳，主路由下一跳权重为100，备份路由下一跳权重为0。当主路由健康检查失败时，备份路由生效。 - 负载路由：负载分担路由需要选择2-4个路由器接口作为下一跳，且作为下一跳的路由器接口的对端路由器类型必须为边界路由器。实例权重的有效范围为1-255的整数，默认值为100。每个实例的权重必须相同，系统会将流量平均分配给下一跳实例。 · IPv6网关：将目的地址在目标网段范围内的流量路由至选择的IPv6网关实例。 说明: 该选项只有当目标网段为IPv6网段时才可用。

关于子网路由的应用示例，请参见路由示例。

步骤三：绑定交换机

您可以将创建的路由表绑定到交换机上，控制该交换机（子网）的路由。一个交换机只能关联一张路由表包括系统路由表。 完成以下操作，将创建的自定义路由表绑定到一个交换机上：

1. 在左侧导航栏，单击路由表。
2. 在路由表页面，找到目标路由表，单击操作列下的管理。
3. 单击已绑定交换机页签，然后单击绑定交换机。

4. 在绑定交换机页面，选择要绑定的交换机，然后单击确定。

3 使用IPv6

3.1 开通IPv6

专有网络支持IPv4和IPv6双栈协议，云产品可通过IPv4和IPv6进行通信。IPv4和IPv6通信彼此独立。

IPv6说明

默认情况下，专有网络使用IPv4寻址协议。您可以根据需要开通IPv6寻址协议。

说明:

目前，仅华北5（呼和浩特）地域支持开通IPv6。

下表总结了IPv4地址和IPv6地址的差异。

IPv4 VPC	IPv6 VPC
格式为32位，4组，每组最多3个数字。	格式为128位，8组，每组4个十六进制数字。
默认开启IPv4地址协议。	可以选择开通。
VPC地址块大小可以从 /8 到 /24。	VPC地址块大小固定为 /56。
交换机地址块大小可以从 /16 到 /29。	交换机地址块大小固定为 /64。
可以选择要使用的IPv4地址块。	无法选择要使用的IPv6地址块。系统会从IPv6地址池中为您的VPC选择IPv6地址块。
所有实例类型都支持。	部分实例类型不支持。 详细说明，请参见实例规格族汇总。
支持配置ClassicLink连接。	不支持配置ClassicLink连接。
支持弹性公网IPv4地址。	不支持弹性公网IPv6地址。
支持配置VPN网关和NAT网关。	不支持配置VPN网关和NAT网关。

开通IPv6后，系统会为您的VPC自动创建一个IPv6网关。

IPv6网关（IPv6 Gateway）是VPC的一个IPv6互联网流量网关。您可以通过配置IPv6互联网带宽和仅主动出规则，灵活定义IPv6互联网出流量和入流量。更多详细信息，请参见什么是IPv6网关#。

此外，您需要为IPv6地址配置安全组规则，并添加路由。

配置方法，请参见配置IPv6安全组和配置IPv6路由。

新建VPC时开通IPv6

您可以在创建VPC时开通IPv6协议。默认开启IPv4协议，且不可取消。

完成以下操作，在创建VPC时开通IPv6：

1. 登录专有网络管理控制台。
2. 在顶部菜单栏，选择专有网络的地域。

   专有网络的地域和要部署的云资源的地域必须相同。
3. 单击创建专有网络，根据以下信息配置专有网络和交换机，然后单击确定。

配置	说明
专有网络配置	
名称	专有网络的名称。 长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
IPv4网段	建议您使用RFC私网地址作为专有网络的网段。 · 您可以使用192.168.0.0/16、172.16.0.0/12和10.0.0.0/8这三个标准网段或其子集。如果要使用标准网段的子网作为VPC的网段，需要使用CreateVpc创建VPC。详细信息，请参见CreateVpc。 · 如果有多个VPC，或者VPC和本地数据中心互连构建混合云的需求，建议使用上面这些标准网段的子网作为VPC的网段，掩码不超过/16。 · 如果云上只有一个VPC并且不需要和本地数据中心互通，那么选择以上任何一个网段或其子网。 注意： VPC创建后，不能再修改IPv4网段。

配置	说明
IPv6网段	选择是否给VPC分配IPv6网段，默认不分配IPv6网段。 如果您选择分配IPv6网段，系统将为您的VPC自动分配掩码为/56的IPv6网段，如2xx1:db8::/56。 注意: VPC创建后，不能再修改IPv6网段。
描述	输入VPC的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。
资源组	选择VPC所属的资源组。
交换机配置	
名称	交换机的名称。 长度为2-128个字符，以英文字母或中文开头，可包含数字，下划线（_）和短横线（-）。
可用区	交换机的可用区。同一VPC内不同可用区的交换机内网互通。

配置	说明
IPv4网段	交换机的IPv4网段。交换机的网段限制如下： · 交换机的网段可以和其所属的VPC网段相同或者是其VPC网段的子集。 例如，VPC的网段是192.168.0.0/16，那么该VPC内的交换机的网段可以是192.168.0.0/16，也可以是192.168.0.0/17，一直到192.168.0.0/29。 说明： 如果交换机的网段和专有网络的网段相同，您只能创建一个交换机。 · 交换机的网段的大小在16位网络掩码与29位网络掩码之间，可提供8-65536个地址。 · 每个交换机的第一个和最后三个IP地址为系统保留地址。 以192.168.1.0/24为例，192.168.1.0、 192.168.1.253、 192.168.1.254和192.168.1.255这些地址是系统保留地址。 · 如果该交换机有和其他专有网络的交换机，或本地数据中心通信的需求，确保交换机的网段和要通信的网段不冲突。 注意： 交换机创建后，不能再修改网段。
IPv6网段	交换机的IPv6网段。 交换机的IPv6网段的掩码默认为/64，您可以输入十进制数字0-255，来自定义交换机IPv6网段的最后8比特位。 如VPC的IPv6网段为2xx1:db8::/64，在交换机的IPv6网段输入十进制数字255（对应十六进制为ff），则交换机的IPv6网段将为2xx1:db8:ff::/64。
描述	输入交换机的描述信息。 描述可包含2-256个中英文字符，不能以http://和https://开头。

为已有VPC开通IPv6

完成以下操作，为已创建的VPC开通IPv6：

1. 登录专有网络管理控制台。
2. 在专有网络列表页面，选择目标VPC，然后单击开通IPv6。

> 说明:
> 目前，仅华北5（呼和浩特地域）支持开通IPv6。

3. 在弹出的对话框，选择自动开启VPC内所有交换机IPv6功能，然后单击确定。

   开通后，系统会为您的VPC从IPv6地址池中分配一个56位掩码的IPv6网段并创建一个免费版的IPv6网关。

3.2 配置IPv6路由

IPv4和IPv6通信彼此独立。您需要在路由表中添加针对IPv6地址的路由控制IPv6的访问。

背景信息

如果您的VPC开通了IPv6。VPC的系统路由表中会自动添加以下路由条目：

- 以::/0为目标网段，下一跳为IPv6网关实例的自定义路由条目，用于VPC内云产品经IPv6地址与互联网通信。
- 以交换机IPv6网段为目标网段的系统路由条目，用于交换机内的云产品通信。

> 说明:
> 如果您创建了自定义路由表，并且绑定了开通IPv6网段的交换机，您需要手动添加一条以::/0为目标网段，下一跳为IPv6网关实例的自定义路由条目。

操作步骤

1. 登录专有网络管理控制台。
2. 选择VPC的所属地域。
3. 在左侧导航栏，单击路由表。
4. 单击目标路由表ID，然后路由条目列表页签。
5. 单击添加路由条目。

6. 在弹出的对话框，根据以下信息配置路由条目，然后单击确定。

配置	说明
目标网段	选择IPv6网段。
下一跳类型和下一跳	选择IPv6网关，然后选择要使用的IPv6网关。

3.3 配置IPv6安全组

IPv4和IPv6通信彼此独立。您需要为ECS实例单独配置IPv6安全组规则。

操作步骤

1. 登录*ECS*控制台。
2. 在左侧导航栏，单击网络和安全 > 安全组。
3. 找到目标安全组，然后单击配置规则。
4. 单击添加安全组规则。

5. 配置安全组规则，授权类型选择IPv6地址段访问，然后输入授权的IPv6地址段。如果输入::/0则代表所有IPv6地址。

   安全组详细的配置说明，请参考#unique_40。

3.4 迁移至IPv6

您可以为已创建的IPv4协议的VPC开启IPv6通信，IPv4和IPv6通信彼此独立。

教程说明

本教程以一个IPv4网段为192.168.0.0/16的VPC为例。该VPC的交换机部署了一个对外提供服务的Web服务器，该ECS实例通过绑定的弹性公网IP对外提供服务。

在完成以下操作后，您部署在ECS实例上的Web应用可以被IPv6客户端通过互联网访问：

- 步骤一#为已有IPv4 VPC开通IPv6

  为已有的VPC开通IPv6，分配IPv6地址段。开通后，系统会为您的VPC创建一个IPv6网关。您可以通过IPv6网关管理IPv6访问。更多详细信息，请参考什么是IPv6网关#。

- 步骤二#为ECS实例分配IPv6地址

  为已有的ECS实例分配IPv6地址。确保您的ECS实例类型支持IPv6，实例规格参见实例规格族。

- 步骤三#配置ECS实例

  配置ECS实例，将分配的IPv6地址添加到实例网卡上。

- 步骤四#配置安全组规则

  为了使ECS实例通过IPv6接收和发送流量，您需要添加针对IPv6地址的安全组规则。

- #可选#步骤五#配置IPv6公网带宽

  默认IPv6地址只具备私网通信能力。如果您需要通过该IPv6地址访问互联网或被互联网中的IPv6客户端访问，您需要该IPv6地址购买公网带宽。

步骤一：为已有IPv4 VPC开通IPv6

完成以下操作，为已创建的VPC开通IPv6：

1. 登录专有网络管理控制台。
2. 在专有网络列表页面，选择目标VPC，然后单击开通IPv6。

   > **说明：**
   > 目前，仅华北5（呼和浩特地域）支持开通IPv6。

3. 在弹出的对话框，选择自动开启VPC内所有交换机IPv6功能，然后单击确定。

   开通后，系统会为您的VPC从IPv6地址池中分配一个56位掩码的IPv6网段并创建一个免费版的IPv6网关。

步骤二：为ECS实例分配IPv6地址

在分配IPv6地址前，确保您的ECS实例类型支持IPv6，且ECS实例的状态为运行中或已停止。实例规格请参见实例规格族。

完成以下操作，为ECS实例分配IPv6地址：

1. 登录ECS控制台。
2. 在左侧导航栏，单击实例。
3. 单击目标ECS实例的ID。
4. 在 配置信息 区域， 单击更多 > 管理辅助私网IP 。

5. 单击 分配IPv6地址。
6. 选择IPv6地址分配方式。本操作选择自动分配。

7. 单击修改。

刷新实例详情页面，查看分配的IPv6地址。

步骤三：配置ECS实例

分配IPv6地址后，您需要将分配的IPv6地址配置到网络接口上。您可以为实例自动配置IPv6地址和手动配置IPv6地址，推荐您使用更高效的自动配置工具配置IPv6地址。

详细信息，请参考为*Linux*实例配置*IPv6*地址和为*Windows*实例配置*IPv6*地址。

本操作以CentOS 7系统为例，为您示范如何自动配置IPv6地址。

1. 远程连接实例。

2. 执行`wget http://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/ipv6/rhel/ecs-utils-ipv6`下载CentOS 7系统自动配置工具。
3. 执行`chmod +x ./ecs-utils-ipv6`修改执行权限，然后执行`./ecs-utils-ipv6`。
4. 执行`ifconfig`查看IPv6地址信息。

```
[root@iZhp3                    ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.      25  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::216:3e      763b  prefixlen 64  scopeid 0x20<link>
        inet6 2408:4004:1c0:700:1      :1426:da3e  prefixlen 64  scopeid 0x0<g
lobal>
        ether 00:16:3e:00:76:3b  txqueuelen 1000  (Ethernet)
        RX packets 17475  bytes 15611557 (14.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9064  bytes 919264 (897.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

步骤四：配置安全组规则

为了使ECS实例通过IPv6接收和发送流量，您需要添加针对IPv6地址的安全组规则。

本操作中ECS实例部署的服务要通过公网被IPv6客户端访问，所以需要添加一条入方向的安全组规则。操作如下：

1. 在ECS实例列表页面，单击已创建的ECS实例ID。
2. 在ECS实例详情页面，单击本实例安全组，然后单击安全组列表页签。
3. 单击配置规则，然后单击添加安全组规则进行配置。

   本操作中的安全组配置如下：

   - 规则方向：入
   - 授权策略：允许
   - 协议类型：全部
   - 授权类型：IPv6地址段访问
   - 授权对象：::/0

（可选）步骤五：配置IPv6公网带宽

默认IPv6地址只具备私网通信能力。如果您需要通过该IPv6地址访问互联网或被互联网中的IPv6客户端访问，您需要该IPv6地址购买公网带宽。

完成以下操作，购买公网带宽：

1. **在专有网络控制台的左侧导航栏，单击IPv6网关。**
2. **找到目标IPv6网关，然后单击管理。**
3. **在左侧导航栏，单击IPv6公网带宽。**
4. **找到ECS实例使用的IPv6地址，然后单击开通公网带宽。**

5. **选择一种费方式和公网带宽，然后完成支付。**

4 网络连接

4.1 网络连接概述

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
VPC ECS固定公网IP	在专有网络内创建ECS时自动分配的公网IP，支持VPC ECS访问公网（SNAT）和用户从公网访问VPC ECS（DNAT）。 目前默认不能动态和VPC ECS解绑，但可以将公网IP转换为EIP。详细说明，请参见*ECS固定公网IP转换为EIP*。	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绑定和解绑，支持VPC ECS访问公网（SNAT）和用户从公网访问VPC ECS（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访问公网（SNAT）和用户从公网访问VPC ECS（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和公网通信，而EIP只能用于一台VPC ECS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
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。 详细说明，请参见配置VPV到VPC连接。	· 成本低，安全，配置简单、即开即用，但网络质量依赖公网（Internet）。 · IPsec-VPN支持IKEv1和IKEv2协议。只要支持这两种协议的设备都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和Ixia等。
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。 详细说明，请参见教程概览。	· 配置简单，自动学习分发路由。 · 低时延高速率。 · 加载到同一个云企业网实例的网络实例（VPC/VBR）全互通。 · 同地域网络实例互通免费。

连接本地IDC

您可以使用下表中的产品或功能，将本地网络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与本地数据中心网络互通。 详细说明，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、速度更快、延迟更低。
VPN网关	· 您可以通过IPsec连接，可以将本地数据中心网络和云上VPC连接起来。 · 多本地IDC连接 VPN网关默认开始VPN-Hub功能，支持多站点连接。各连接的站点不仅可以和VPC互通，并且各站点之间也可以通过VPN-Hub通信。 · 客户端远程接入 通过建立SSL-VPN连接，客户端可以远程接入VPC。	· 成本低、安全、配置简单，即开即用，但网络质量依赖公网（Internet）。 · IPsec-VPN支持IKEv1和IKEv2协议。只要支持这两种协议的设备都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和Ixia等。 · SSL-VPN连接支持Windows、Linux、Mac、IOS和Android等操作系统多终端接入。
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。	· 配置简单，自动学习分发路由。 · 低时延高速率。 · 加载到同一个云企业网实例的网络实例（VPC/VBR）全互通。 · 同地域网络实例互通免费。

产品	功能	优势
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。 · 支持线下机构互通。	· 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。

4.2 连接Internet

您可以通过使用弹性公网IP、NAT网关使专有网络中的云资源可以访问公网（Internet）。

概述

专有网络是您自定义的云上私有网络。专有网络中的云资源默认无法访问Internet，也无法被Internet访问。您可以通过配置公网IP或NAT网关的方式连接Internet。

并且，专有网络提供共享带宽和共享流量包产品，帮助您节省公网成本。详细信息，请参见如何节约公网成本#。

弹性公网IP

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。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的资源上。和云资源绑定后，云资源可以通过EIP与公网通信。

目前，EIP可绑定到专有网络类型的ECS实例、弹性网卡、专有网络类型的私网SLB实例和NAT网关。更多配置说明，请参见*EIP*用户指南。

EIP的优势如下：

· 独立购买与持有

  您可以单独持有一个弹性公网IP，作为您账户下一个独立的资源存在，无需与其它计算资源或存储资源绑定购买。

· 弹性绑定

  您可以在需要时将弹性公网IP绑定到需要的资源上；在不需要时，将之解绑并释放，避免不必要的计费。

- 可配置的网络能力

  您可以根据需要随时调整弹性公网IP的带宽值，带宽的修改即时生效。

NAT网关

NAT网关（NAT Gateway）是一款企业级的VPC公网网关，提供NAT代理（SNAT和DNAT）、高达10Gbps级别转发能力以及跨可用区的容灾能力。

NAT网关支持多台专有网络ECS实例通过一个公网IP访问Internet。更多配置说明，请参见*NAT网关用户指南*。

NAT网关的优势如下：

- 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和DNAT功能。无需自己搭建NAT网关，可直接配置SNAT和DNAT规则。

- 高可用

  NAT网关是基于阿里云自研分布式网关，使用SDN技术虚拟化推出的一款虚拟网络硬件。NAT网关支持10Gbps级别的转发能力，为大规模公网应用提供支撑。

- 按需购买

  NAT网关的规格、EIP的规格和个数，均可以随时升降，轻松应对业务变化。

4.3 VPC互连

您可以通过使用云企业网和高速通道连接不同的专有网络。

概述

针对不同场景和需求，阿里云提供了不同的私网互通产品。您可以通过云企业网和高速通道实现VPC互通。云企业网的配置更加简单而且可以自动分发学习路由，因此推荐您使用云企业网。

- 云企业网

  云企业网（Cloud Enterprise Network）帮助您在VPC间，VPC与本地数据中心间搭建私网通信通道，通过自动路由分发及学习，提高网络的快速收敛和跨网络通信的质量和安全性，实现全网资源的互通。

- 高速通道

  您可以通过创建对等连接，在两个专有网络（VPC）之间搭建内网通信通道。

互通场景

场景	产品	配置方法
同账号同地域VPC互通	云企业网	同账号同地域VPC互连
	高速通道	同账号VPC互连
跨账号同地域VPC互通	云企业网	跨账号同地域VPC互连
	高速通道	跨账号VPC互连
同账号跨地域VPC互通	云企业网	同账号跨地域VPC互连
	高速通道	同账号VPC互连
跨账号跨地域VPC互通	云企业网	跨账号跨地域VPC互连
	高速通道	跨账号VPC互连

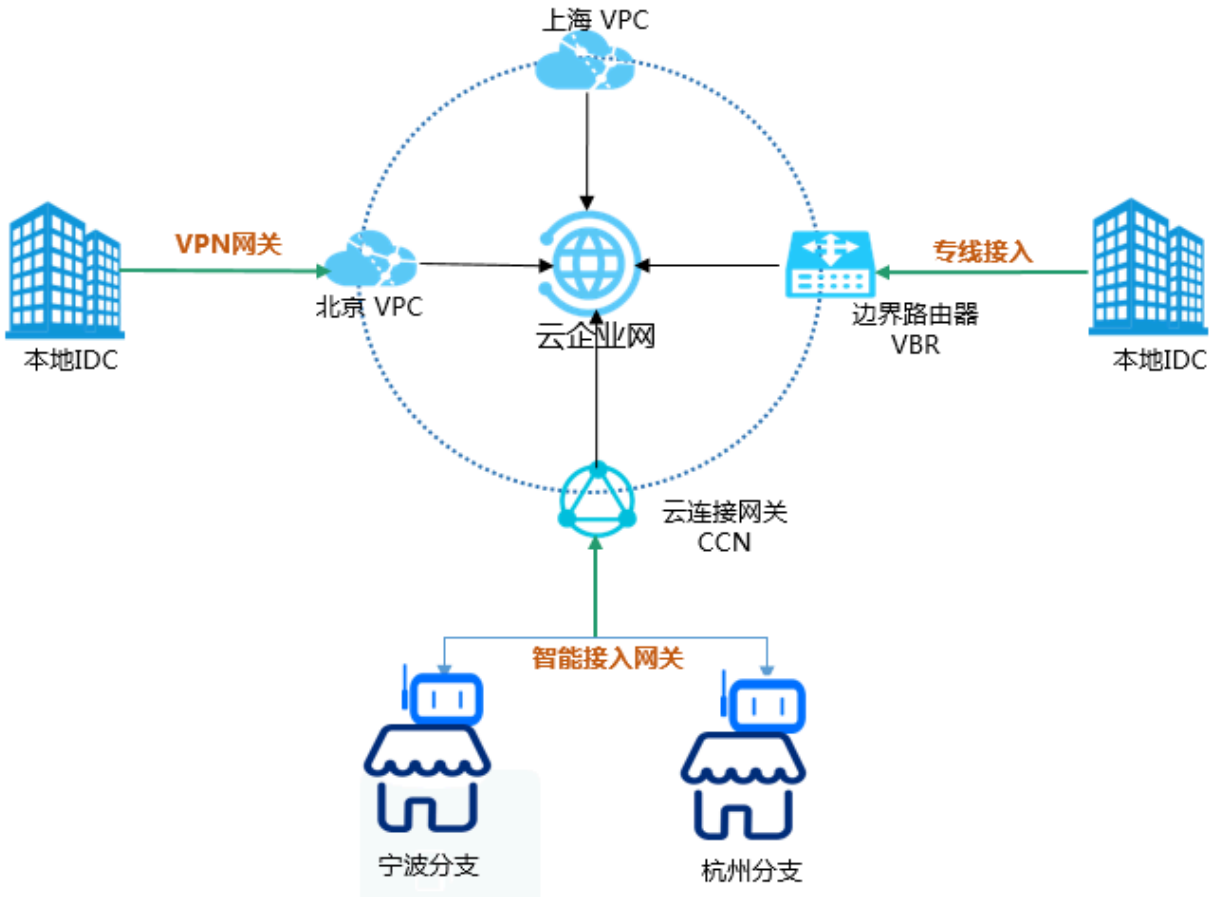
4.4 连接本地IDC

您可以通过VPN网关、高速通道物理专线、智能接入网关将本地数据中心和云上VPC打通，构建混合云。

概述

您可以在本地数据中心和阿里云专有网络间建立私网通信，构建混合云。然后将本地的IT基础架构无缝地扩展到阿里云上，借助阿里云海量的计算、存储、网络、CDN资源，应对业务波动，提高应用的稳定性。

您可以通过VPN网关、高速通道物理专线、智能接入网关将本地数据中心和云上VPC打通。并且，可以通过云企业网实现全球网络互通。



连接方案

方案	说明
VPN接入	您可以通过VPN网关的IPsec-VPN将本地数据中心和VPC连接起来。VPN网关默认包含了两个不同的网关实例形成主备双机热备，主节点故障时自动切换到备节点。 VPN网关基于Internet通信，网络延迟和可用性取决于Internet。如果您对网络延迟没有特别高的需求，建议您选择VPN网关。 配置详情，请参见建立VPC到本地数据中心的连接。

方案	说明
专线接入	您可以通过租用一条运营商的专线将本地数据中心连接到阿里云接入点，建立专线连接。高速通道提供自主接入和一站式接入服务。 物理专线接入网络质量好，带宽高。如果您对网络质量有很高的要求，建议您选择高速通道专线接入。 配置详情，请参见物理专线接入。
冗余专线接入	通过冗余物理专线将您的本地数据中心接入到阿里云，在您的本地数据中心和阿里云上的VPC间建立高质量、高可靠的内网通信。阿里云目前支持最多4条物理专线实现等价多路径路由（ECMP）。 配置详情，请参见冗余专线接入。
智能接入网关接入	智能接入网关（Smart Access Gateway）是阿里云提供的一站式快速上云解决方案。企业可通过智能接入网关实现Internet就近加密接入，获得更加智能、更加可靠、更加安全的上云体验。 智能接入网关配置简单，成本低。如果您有多个本地分支上云的需求，建议您选择智能接入网关。 配置详情，请参见智能接入网关上云。
通过BGP主备链路接入	通过专线接入和云企业网组合的方式，实现本地IDC通过主备链路上云，并和云上不同地域VPC互通。 配置详情，请参见IDC通过BGP主备链路上云方案。
专线备份接入	将智能接入网关作为已有物理专线的备用链路接入阿里云，构建高可用的混合云环境。 配置详情，请参见专线备份配置教程。

4.5 ClassicLink

4.5.1 ClassicLink概述

专有网络提供ClassicLink功能，使经典网络的ECS实例可以和VPC中的云资源通过内网互通。

使用限制

在使用ClassicLink功能前，请注意如下限制：

- 最多允许1000台经典网络ECS实例连接到同一个VPC。
- 一台经典网络ECS实例只能连接到一个VPC（同账号且同地域）。

  若进行跨账号连接，比如将账号A的ECS实例连接到账号B的VPC，可以将ECS实例从账号A过户到账号B。

  您可以提交工单申请ECS实例过户。过户前，确保您已了解*ECS实例过户须知*。
- VPC要开启ClassicLink功能，需要满足以下条件：

专有网络网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。
10.0.0.0/8	- 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 - 确保和经典网络ECS实例通信的交换机的网段在10.111.0.0/16内。
192.168.0.0/16	- 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 - 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，单击此处下载路由脚本。 说明: 在运行脚本前，请仔细阅读脚本中包含的readme。

连接场景

经典网络ECS和VPC互通的连接场景如下表所示。

连接发起端网络类型	地域/账号	接收端网络类型/内网互通	
		经典网络（Classic）	专有网络（VPC）

<table>
<tr><td rowspan="4">经典网络（Classic）</td><td>同地域
同账号</td><td>安全组同账号授权</td><td>建立ClassicLink连接</td></tr>
<tr><td>同地域
跨账号</td><td>安全组跨号授权</td><td>· 方案A：
1. 经典网络ECS实例迁移至VPC
2. VPC互连
· 方案B：
1. 经典网络ECS实例过户至VPC的所属账号下
2. 建立ClassicLink连接</td></tr>
<tr><td>跨地域
同账号</td><td rowspan="2">1. 将两端ECS实例都迁移至VPC网络
2. 两端VPC互连</td><td rowspan="2">1. 将发起端ECS实例迁移至VPC网络
2. 两端VPC互连</td></tr>
<tr><td>跨地域
跨账号</td></tr>
<tr><td rowspan="4">专有网络（VPC）</td><td>同地域
同账号</td><td>建立ClassicLink连接</td><td rowspan="4">VPC互连</td></tr>
<tr><td>同地域
跨账号</td><td>· 方案A：
1. 经典网络ECS实例迁移至VPC
2. VPC互连
· 方案B：
1. 经典网络ECS实例过户至VPC的所属账号下
2. 建立ClassicLink连接</td></tr>
<tr><td>跨地域
同账号</td><td rowspan="2">1. 将接收端经典网络ECS实例迁移至VPC
2. VPC互连</td></tr>
<tr><td>跨地域
跨账号</td></tr>
</table>

ClassicLink互通原理

经典网络和VPC互通与经典网络和经典网络互通的底层实现是一致的，因此内网延迟不变，内网带宽限速不变。宕机迁移、热迁移、停止、启动、重启、更换系统盘等操作不会改变已建立的ClassicLink连接。

经典网络是一个网络平面，VPC是另一个网络平面，ClassicLink是通过路由将这两个网络平面拉齐，让其具备互通的条件。因此使用ClassicLink功能，首先要避免网络地址冲突，做好网络地址规划。

阿里云经典网络中使用的地址段是10.0.0.0/8(不包括10.111.0.0/16)，因此只要VPC的地址段与经典网络的地址段不冲突，就可以通过ClassicLink功能通信。可以与经典网络互通的VPC地址段有172.16.0.0/12、10.111.0.0/16、192.168.0.0/16。

ClassicLink互通原则

使用ClassicLink功能打通经典网络ECS实例和VPC的私网通信后：

- 经典网络ECS实例可以访问目标VPC内的云资源。

  ClassicLink连接成功后，经典网络的ECS实例可以访问已连接的VPC内的云资源，包括ECS实例、RDS、SLB等。比如经典网络ECS实例连接到了地址段为10.0.0.0/8的VPC，该VPC内有个网段为10.111.1.0/24的交换机。如果该交换机内部署了ECS实例、RDS等云资源，则经典网络的ECS实例可以通过ClassicLink功能访问这些云资源。
- ClassicLink连接成功后，VPC内的ECS实例只能访问已连接到该VPC的经典网络ECS实例，不能访问未连接的经典网络ECS实例，也不能访问经典网络内的其它云资源。

4.5.2 建立ClassicLink连接

您可以通过建立ClassicLink连接，使经典网络的ECS实例可以和专有网络内的云资源通信。

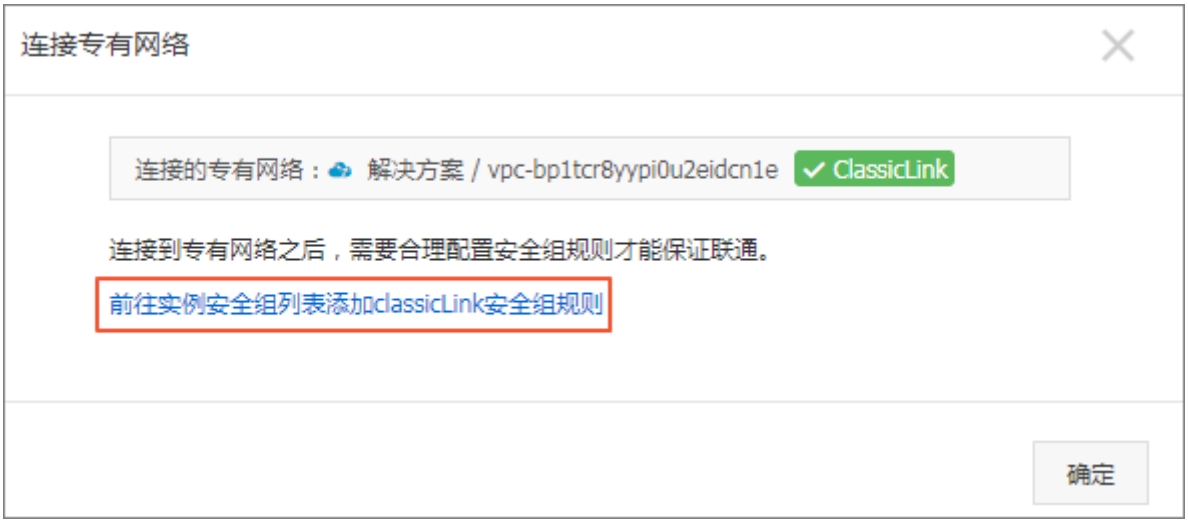
前提条件

确保您已经了解建立连接的限制。详细说明，请参见*ClassicLink概述*。

操作步骤

1. 登录专有网络管理控制台。
2. 选择目标专有网络的地域，然后单击目标专有网络的ID。
3. 在专有网络详情页面，单击开启ClassicLink， 然后在弹出的对话框，单击确定。
4. 登录ECS管理控制台。
5. 在左侧导航栏，单击实例。
6. 选择实例的所属地域，找到目标经典网络实例。
7. 单击更多 > 网络和安全组 > 设置专有网络连接状态。

8. 在弹出的对话框中选择目标VPC，单击确定，然后单击配置安全组的链接。



9. 单击添加ClassicLink安全组规则，根据以下信息配置ClassicLink安全组规则，然后单击确定。

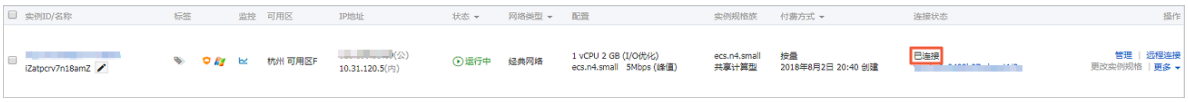
配置	说明
经典网络安全组	显示经典网络安全组的名称。
选择专有网络安全组	选择专有网络的安全组。
授权方式	选择一种授权方式： · 经典网络 <=> 专有网络：相互授权访问，推荐使用这种授权方式。 · 经典网络 => 专有网络：授权经典网络ECS访问专有网络内的云资源。 · 专有网络 => 经典网络：授权专有网络内的云资源访问经典网络ECS。
协议类型和端口范围	选择授权通信的协议和端口。端口的输入格式为xx/xx，比如授权80端口，则输入80/80。
优先级	设置该规则的优先级。数字越小，优先级越高。
描述	输入安全组描述。

10.返回ECS管理控制台，单击右侧的配置图标，在弹出的对话框中勾选连接状态，然后单击确定查看ECS实例的连接状态。

图 4-1: 自定义列表选项

图 4-2: 连接状态选项

图 4-3: 已连接状态



4.5.3 取消ClassicLink连接

当您不再需要经典网络ECS实例与VPC之间的私网连接时，可以随时取消。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，单击实例。
3. 选择实例的所属地域，然后找到目标经典网络实例。

4. 单击更多 > 网络和安全组 > 设置专有网络连接状态。
5. 在弹出的对话框，单击确定。

4.5.4 关闭ClassicLink

在取消ClassicLink连接后，您可以关闭VPC的ClassicLink功能。

操作步骤

1. 登录专有网络管理控制台。
2. 选择目标专有网络的地域，然后单击目标专有网络的ID。
3. 在专有网络详情页面，单击关闭ClassicLink， 然后在弹出的对话框，单击确定。

5 访问控制

5.1 VPC访问控制概述

专有网络目前没有独立的访问控制策略。当前在专有网络中进行访问控制，依赖各个云产品的访问控制能力。比如云服务器（ECS）通过设置安全组来进行访问控制，负载均衡（SLB）和云数据库RDS通过白名单来进行访问控制。

ECS安全组

安全组是一种虚拟防火墙，具备状态检测包过滤功能。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

当您创建专有网络类型的ECS实例时，可以使用系统提供的默认安全组规则。您可以更改默认安全组的规则，但无法删除默认安全组。

RDS白名单

基于云数据库RDS版的白名单功能，您可定义允许访问RDS的IP地址，指定之外的IP地址将被拒绝访问。在专有网络中使用RDS产品时，需要将云服务器的IP地址加入到需要访问的RDS的白名单后，云服务器才能访问RDS实例。

SLB白名单

负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。您可以为负载均衡监听设置仅允许哪些IP访问，适用于应用只允许特定IP访问的场景。

5.2 ECS安全组配置案例

当您创建专有网络类型的ECS实例时，可以使用系统提供的默认安全组规则，也可以选择VPC中已有的其它安全组。安全组是一种虚拟防火墙用来控制ECS实例的出站和入站流量。

本文档介绍了常用的专有网络ECS实例的安全组设置。

案例 一：内网互通

VPC类型的ECS实例互通分以下两种情况：

· 同一VPC内的相同安全组下的ECS实例，默认互通。

- 不同VPC内的ECS实例，无法互通。首先需要使用高速通道、VPN网关、云企业网等产品打通两个VPC之间的通信，然后确保两个VPC内的ECS实例的安全组规则允许互相访问，如下表所示。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
VPC 1中的ECS实例的安全组配置	入方向	允许	Windows: RDP 3389/3389	地址段访问	要访问的VPC2中的ECS实例的私网IP。 说明: 如果允许任意ECS实例登录，填写0.0.0.0/0。
	入方向	允许	Linux: SSH 22/22	地址段访问	
	入方向	允许	自定义TCP 自定义	地址段访问	
VPC 2中的ECS实例的安全组配置	入方向	允许	Windows: RDP 3389/3389	地址段访问	要访问的VPC1中的ECS实例的私网IP。 说明: 如果允许任意ECS实例登录，填写0.0.0.0/0。
	入方向	允许	Linux: SSH 22/22	地址段访问	
	入方向	允许	自定义TCP 自定义	地址段访问	

案例二：拒绝特定IP或特定端口的访问

您可以通过配置安全组拒绝特定IP或特定端口对专有网络ECS实例的访问，如下表所示。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
拒绝特定IP地址段对ECS实例所有端口的入站访问	入方向	拒绝	全部 -1	地址段访问	要拒绝访问的IP地址段，如10.0.0.1/32。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
拒绝特定IP地址段对ECS实例TCP 22端口的入站访问	入方向	拒绝	SSH(22) 22/22	地址段访问	要拒绝访问的IP地址段，如10.0.0.1/32。

案例三：只允许特定IP远程登录ECS

如果您为VPC中的ECS实例配置了公网IP，如NAT网关、EIP等。您可以根据具体情况，添加如下安全组规则允许Windows远程登录或Linux SSH登录。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
允许Windows远程登录	入方向	允许	RDP 3389/3389	地址段访问	允许登录ECS实例的指定IP地址。 说明: 如果允许任意公网IP登录ECS，填写0.0.0.0/0。
允许Linux SSH登录	入方向	允许	SSH 22/22	地址段访问	允许登录ECS实例的指定IP地址。 说明: 如果允许任意公网IP登录ECS，填写0.0.0.0/0。

案例四：允许从公网访问ECS实例部署的HTTP/HTTPS服务

如果您在专有网络的ECS实例上部署了一个网站，通过EIP、NAT网关对外提供服务，您需要配置如下安全组规则允许用户从公网访问您的网站。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
允许来自HTTP 80端口的入站访问	入方向	允许	HTTP 80/80	地址段访问	0.0.0.0/0

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
允许来自HTTPS 443端口的入站访问	入方向	允许	HTTPS 443/443	地址段访问	0.0.0.0/0
允许来自TCP 80端口的入站访问	入方向	允许	TCP 80/80	地址段访问	0.0.0.0

6 流日志

VPC提供流日志功能，可以记录VPC网络中弹性网卡（ENI）的传入和传出流量信息，帮助您检查访问控制规则、监控网络流量、进行网络故障排查。

说明:

流日志功能目前仅在华北5、马来西亚、印度尼西亚、英国、印度地域开放。

功能介绍

您可以捕获指定弹性网卡的流量，也可以指定一个VPC或交换机。如果选择为交换机或VPC创建流日志，则会捕获VPC和交换机中所有弹性网卡的流量，包括在开启流日志功能后新建的弹性网卡。

捕捉到的流量信息存储在阿里云日志服务中，您可以在日志服务中查看和分析相关数据。流日志功能测试期间暂不收取费用，日志服务将收取相应的存储和检索费用。详细说明，请参见按量付费。

流日志功能捕获的流量信息会以流日志记录的方式写入日志服务。每个记录捕获特定捕获窗口中的特定5元组网络流。捕获窗口大约为10分钟。该段时间内流日志服务会聚合数据，大约需要5分钟，然后再发布流日志记录。

流日志记录的字段信息如下表所示。

字段	说明
version	流日志版本。
vswitch-id	弹性网卡所在交换机ID。
vm-id	弹性网卡绑定的云服务器ID。
vpc-id	弹性网卡所在专有网络ID。
account-id	账号ID。
eni-id	弹性网卡ID。
srcaddr	源地址。
srcport	源端口。
dstaddr	目的地址。
dstport	目的端口。
protocol	流量的IANA协议编号。 详细信息，请参见 *Internet* 协议编号。

字段	说明
direction	流量方向： · in：入方向流量。 · out：出方向流量。
packets	数据包包数量。
bytes	数据包大小。
start	捕捉窗口开始时间。
end	捕捉窗口结束时间。
log-status	流日志的日志记录状态： · OK：数据记录正常。 · NODATA：捕获窗口中没有传入或传出网络接口的网络流量。 · SKIPDATA：捕获窗口中跳过了一些流日志记录。
action	与流量关联的操作： · ACCEPT：安全组允许记录的流量。 · REJECT：安全组未允许记录的流量。

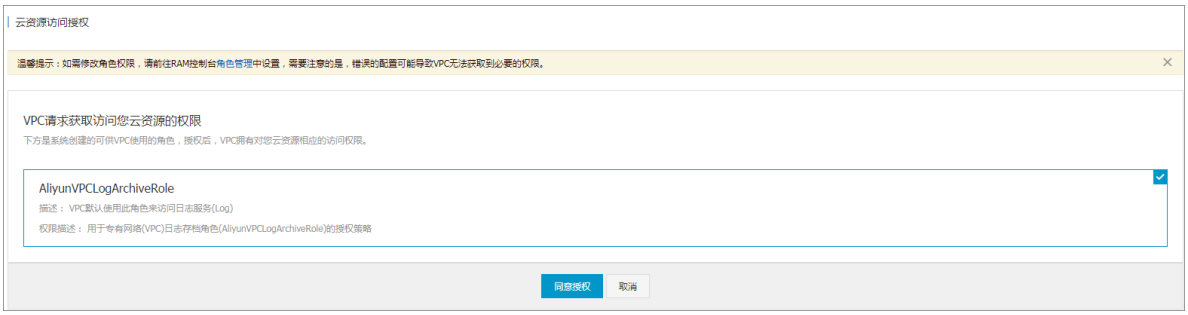
创建流日志

> **注意：**
> 在创建流日志前，确保您已经开通了日志服务。

完成以下操作，创建流日志：

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击流日志。
3. 如果您的账号是初次使用流日志功能，单击同意授权授权VPC可以向日志库中写数据。

> **注意：**
> 该操作只有主账号首次开通流日志功能时才需要。



4. 选择捕获日志资源的所属地域，然后单击创建流日志。

5. 在创建流日志页面，根据以下信息完成配置，然后单击确定。

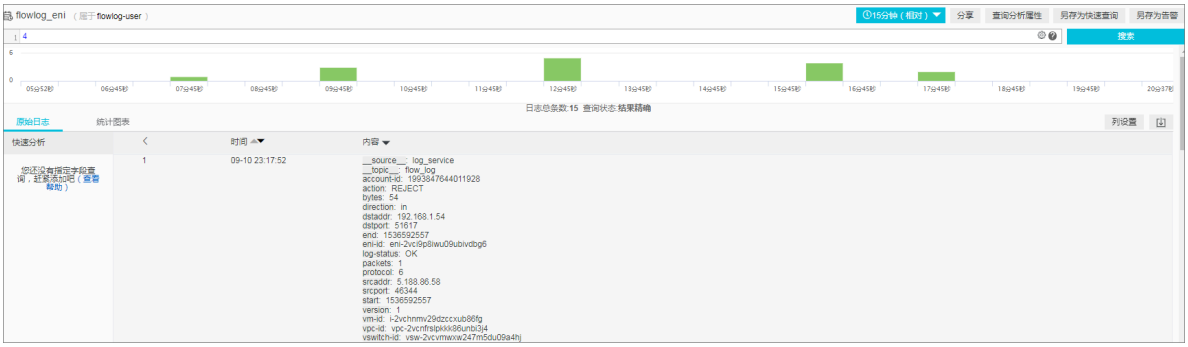
参数	说明
名称	输入流日志名称。
资源类型	选择要捕获流量的资源类型： · 弹性网卡：捕获指定的弹性网卡的流量信息。 · 交换机：捕获指定的交换机内所有弹性网卡的流量信息。 · 专有网络：捕获指定的专有网络内所有弹性网卡的流量信息。
流量类型	选择要捕获流量的类型： · 全部流量：捕获指定资源的全部流量。 · 被访问控制允许的流量：捕获指定资源被安全组规则允许的流量。 · 被访问控制拒绝的流量：捕获指定资源被安全组规则拒绝的流量。
LogStore	选择存储写入数据的LogStore。
开启流日志分析报表功能	选择该功能后，所选的LogStore会开启索引并建立仪表盘，支持对数据进行SQL和可视化分析。 日志服务索引功能按流量收费，仪表盘不收费。详细信息请参考日志服务计费说明。 说明： 该选项只有当选择的LogStore未开通报表功能时才显示。
描述	输入流日志的描述。

查看日志

完成以下操作，查看记录的日志数据：

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击流日志。
3. 选择一个地域，然后单击存储目标流日志的日志库链接。

4. 在日志管理控制台，单击目标日志库的查询。
5. 查看日志分析数据。



停止流日志

当暂时不需要某个流日志捕捉数据时，可以将其停止，再次需要时可以重新启动已停止的流日志。

完成以下操作，停止流日志：

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击流日志。
3. 选择一个地域，找到目标流日志，然后单击停止。

使用限制

在使用流日志功能时，请注意：

- 流日志捕获流量的对象：弹性网卡（ENI）。
- 支持创建流日志的资源类型：专有网络VPC、交换机和弹性网卡。
- 每个地域可创建的流日志实例数量：10。

  如果您需要创建更多流日志实例，提交工单申请。

7 管理配额

您可以通过专有网络VPC控制台查询当前资源配额使用情况。如果某个资源的剩余配额不满足业务需求，您可以直接申请增加配额。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击配额管理。
3. 在配额管理页面，选择专有网络VPC页签，可以查看当前账号下专有网络VPC的资源使用情况。
4. 如果需要提升配额，可以单击操作列的申请，提交提升配额申请。
   - 申请数量：需要的资源配额数量，申请数量必须为数字且大于当前配额。专有网络VPC的资源默认使用限制，请参见使用限制。
   - 申请原因：请详细描述申请配额的原因、业务场景和必要性。
   - 手机/固话：申请配额的用户电话号码。
   - 电子邮箱：申请配额的用户电子邮箱。
5. 单击确定。

   系统会自动审批配额申请是否合理：

   - 如果不合理，申请状态为拒绝。
   - 如果合理，申请状态为通过，配额立即自动提升为申请的数量。

   在申请历史列单击申请历史，可以查看配额申请历史。