

ALIBABA CLOUD

阿里云

专有云企业版

专有网络VPC
用户指南

产品版本：v3.16.2

文档版本：20220915

 阿里云

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
 危险	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。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会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，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	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。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1. 产品详情	06
2. 登录专有网络管理控制台	08
3. 快速入门	09
3.1. 网络规划	09
3.2. 搭建IPv4专有网络	11
3.3. 搭建IPv6专有网络	14
4. 专有网络和交换机	19
4.1. 专有网络和交换机概述	19
4.2. 管理专有网络	21
4.2.1. 创建专有网络	21
4.2.2. 添加附加IPv4网段	23
4.2.3. 删除附加IPv4网段	24
4.2.4. 修改专有网络	24
4.2.5. 删除专有网络	25
4.2.6. 管理标签	25
4.3. 管理交换机	25
4.3.1. 创建交换机	26
4.3.2. 创建云资源	27
4.3.3. 修改交换机	27
4.3.4. 删除交换机	28
4.3.5. 管理标签	28
5. 路由表	30
5.1. 路由表概述	30
5.2. 创建自定义路由表	34
5.3. 添加自定义路由条目	36
5.4. 导出路由条目	37

5.5. 修改路由表	38
5.6. 删除自定义路由条目	38
5.7. 子网路由	38
6.高可用虚拟IP	42
6.1. 高可用虚拟IP概述	42
6.2. 创建高可用虚拟IP实例	44
6.3. 绑定后端云资源	44
6.3.1. 绑定ECS实例	45
6.3.2. 绑定弹性网卡	45
6.4. 绑定EIP	46
6.5. 解绑后端云资源	46
6.5.1. 解绑ECS实例	46
6.5.2. 解绑弹性网卡	47
6.6. 解绑EIP	47
6.7. 删除高可用虚拟IP	47
7.网络ACL	49
7.1. 网络ACL概述	49
7.2. 典型应用	50
7.3. 创建网络ACL	53
7.4. 绑定交换机	54
7.5. 添加网络ACL规则	54
7.5.1. 添加入方向规则	54
7.5.2. 添加出方向规则	55
7.5.3. 调整规则顺序	56
7.6. 解绑交换机	57
7.7. 删除网络ACL	57

1. 产品详情

专有网络VPC（Virtual Private Cloud）是用户自己独有的云上私有网络，是一个隔离的网络环境，专有网络之间逻辑上彻底隔离。用户可以掌控自己的专有网络也可以在自己定义的专有网络中使用阿里云资源。

专有网络

每个专有网络都由一个私网网段、至少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，用户需要以CIDR地址块的形式指定专有网络使用的私网网段。用户可以使用下表中标标准的私网网段及其子网作为专有网络的私网网段。

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
172.16.0.0/16	65,532

- 路由器（vRouter）：专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接专有网络内的各个交换机，同时也是连接专有网络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。
- 交换机（vSwitch）：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，用户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。用户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。

自定义路由表和路由条目

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。用户不能创建也不能删除系统路由表，但用户可以在专有网络内创建自定义路由表，将自定义路由表和交换机绑定来控制子网路由，更灵活地进行网络管理。

用户可以在专有网络的路由表（系统路由表和自定义路由表）中添加自定义路由，将流量转发到目标下一跳。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路由条目可以匹配目的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。

高可用虚拟IP

高可用虚拟IP（High-Availability Virtual IP Address，简称HaVip）是一种可以独立创建和释放的私网IP资源。HaVip可以与高可用软件（例如keepalived）配合使用，搭建高可用主备服务，提高业务的可用性。例如，ECS实例除了可以拥有主私网IP地址外，还可以绑定高可用虚拟IP，以获得多个私网IP地址。

网络ACL

网络ACL（Network Access Control List）是专有网络中的网络访问控制功能。用户可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中云服务器ECS实例的流量的访问控制。

多种连接方式

阿里云提供多种连接方式，用户可以将专有网络连接到互联网、用户的本地数据中心或其他专有网络：

- 连接到互联网
用户可以通过绑定弹性公网IP、配置NAT网关方式，将专有网络与互联网连接，使专有网络内的云服务可以和互联网通信。
- 连接到其他专有网络

用户可以通过创建一对路由器接口连接到其他专有网络，建立高速、安全地私网通信。

- 连接到本地数据中心

用户可以通过物理专线将本地数据中心和专有网络连接起来，将本地应用平滑迁移到云上。

2. 登录专有网络管理控制台

本节以Chrome浏览器为例，介绍专有网络VPC（Virtual Private Cloud）用户如何登录到Apsara Uni-manager运营控制台。


前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的访问地址，按回车键。
2. 输入正确的用户名及密码。


请向运营管理员获取登录控制台的用户名和密码。

 **说明** 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为 8~20 位，且至少包含以下两种类型：

- 英文大写或小写字母（A~Z、a~z）
- 阿拉伯数字（0~9）
- 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（\$）、百分号（%）等）

3. 单击**登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
 - 管理员强制开启MFA后的首次登录：
 - a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
 - b. 按照步骤2重新输入账号和密码，单击**账号登录**。
 - c. 输入6位MFA码后单击**认证**。
 - 您已开启并绑定MFA：

输入6位MFA码后单击**认证**。

 **说明** 绑定并开启MFA的操作请参见Apsara Uni-manager运营控制台用户指南中的**绑定并开启虚拟MFA设备**章节。

5. 在页面顶部的菜单栏中，选择**产品 > 网络 > 专有网络 VPC**。

3.快速入门

3.1. 网络规划

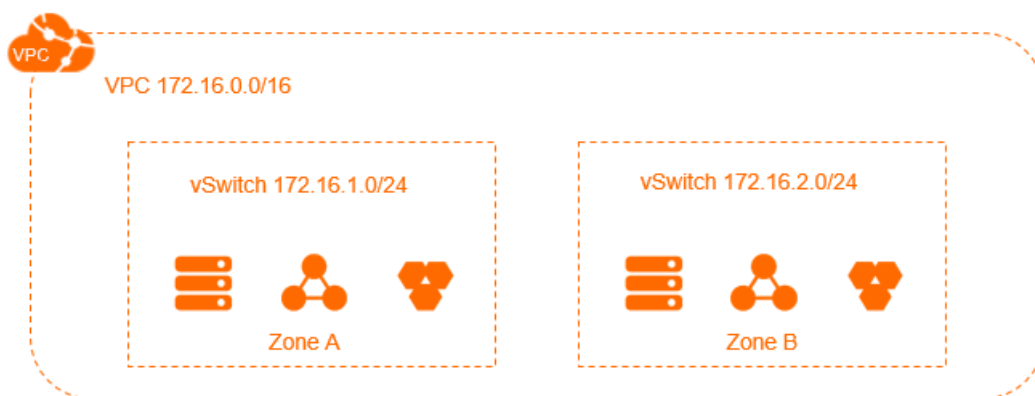
在创建VPC和交换机前，您需要结合具体的业务规划VPC和交换机的数量及网段等。

- 应该使用几个VPC？
- 应该使用几个交换机？
- 应该选择什么网段？
- VPC与VPC互通或VPC与本地数据中心互通有什么要求？

应该使用几个VPC？

- 一个VPC

如果您没有多地部署系统的要求且各系统之间也不需要通过VPC进行隔离，那么推荐使用一个VPC。

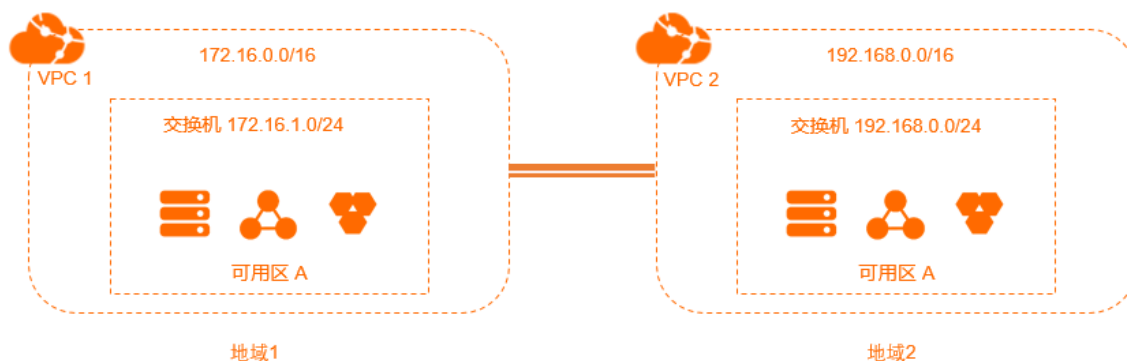


- 多个VPC

如果您有如下任何一个需求，推荐您使用多个VPC：

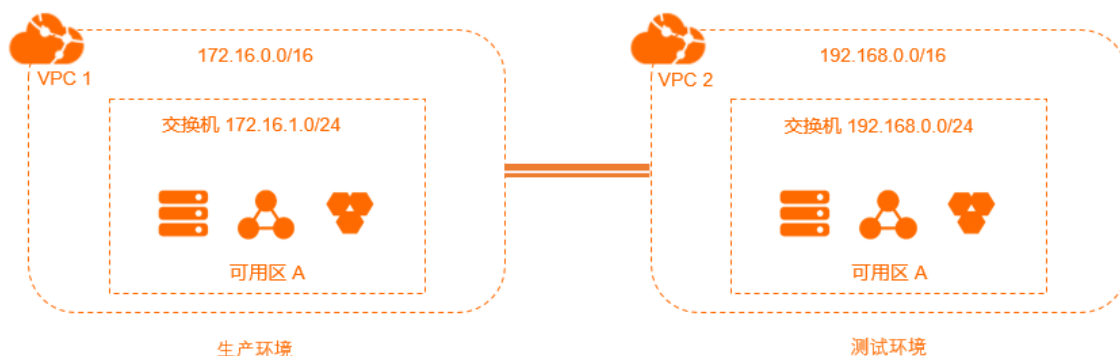
- 多地部署系统

VPC是地域级别的资源，是不能跨地域部署的。当您有多地域部署系统的需求时，就必须使用多个VPC。您可以通过使用高速通道、VPN网关等产品实现VPC互通。



多业务系统隔离

如果在一个地域的多个业务系统需要通过VPC进行严格隔离，例如生产环境和测试环境，那么也需要使用多个VPC，如下图所示。



应该使用几个交换机？

首先，即使只使用一个VPC，也尽量使用至少两个交换机，并且将两个交换机分布在不同可用区，这样可以实现跨可用区容灾。

同一地域不同可用区之间的网络通信延迟很小，但也需要经过业务系统的适配和验证。由于系统调用复杂加上系统处理时间、跨可用区调用等原因可能产生期望之外的网络延迟。建议您进行系统优化和适配，在高可用和低延迟之间找到平衡。

其次，使用多少个交换机还和系统规模、系统规划有关。如果前端系统可以被公网访问并且有主动访问公网的需求，考虑到容灾可以在不同的交换机下部署前端系统，在另外的交换机下部署后端系统。

应该选择什么网段？

在创建VPC和交换机时，您必须以无类域间路由块（CIDR block）的形式为您的专有网络划分私网网段。

● 规划VPC网段

您可以使用172.16.0.0/16或192.168.0.0/16私网网段及其子网作为VPC的私网地址范围。在规划VPC网段时，请注意：

- 如果云上只有一个VPC并且不需要和本地数据中心互通时，可以选择上述私网网段中的任何一个网段或其子网。
- 如果有多个VPC，或者有VPC和本地数据中心构建混合云的需求，建议使用上面这些标准网段的子网作为VPC的网段，掩码建议不超过16位。

● 规划交换机网段

交换机的网段必须是其所属VPC网段的子集。例如VPC的网段是192.168.0.0/16，那么该VPC下的交换机的网段可以是192.168.0.0/17，一直到192.168.0.0/29。

规划交换机网段时，请注意：

- 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。16位掩码能支持65532个ECS实例，而小于29位掩码又太小，没有意义。
- 每个交换机的第1个和最后3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。
- 交换机网段的确定还需要考虑该交换机下容纳ECS的数量。

VPC与VPC互通或VPC与本地数据中心互通有什么要求？

当您有VPC与VPC互通或VPC与本地数据中心互通的需求时，确保VPC的网段和要互通的网络的网段都不冲突。

在多VPC的情况下，建议遵循以下网段规划原则：

- 尽可能做到不同VPC的网段不同，不同VPC可以使用标准网段的子网来增加VPC可用的网段数。
- 如果不能做到不同VPC的网段不同，则尽量保证不同VPC的交换机网段不同。
- 如果也不能做到交换机网段不同，则保证要通信的交换机网段不同。

3.2. 搭建IPv4专有网络

本教程指引您搭建一个具有IPv4地址块的专有网络VPC（Virtual Private Cloud），并在专有网络中创建一个云服务器ECS（Elastic Compute Service）实例。

前提条件

在专有网络中使用云资源，您必须先做好网络规划。更多信息，请参见[网络规划](#)。

步骤一：创建专有网络

1. [登录专有网络管理控制台](#)。
2. 在专有网络页面，单击创建专有网络。
3. 在创建专有网络VPC页面，根据以下信息配置专有网络，然后单击提交。

配置	说明
区域	
组织	选择专有网络所属的组织。
资源集	选择专有网络所属的资源集。
地域	选择专有网络所属的地域。
基本配置	
共享范围	<p>选择VPC的共享范围。</p> <ul style="list-style-type: none">○ 本资源集：本资源集的管理员可以使用共享VPC创建资源。○ 本组织及下级组织：本组织及下级组织的管理员可以使用共享VPC创建资源。○ 本组织：本组织的管理员可以使用共享VPC创建资源。 <p>本教程选择本资源集。</p>
专有网络名称	<p>输入专有网络的名称。</p> <p>本教程输入 <i>VPCtest</i>。</p>

配置	说明
IPv4网段	<p>选择IPv4网段，支持以下两种方式选择IPv4网段：</p> <ul style="list-style-type: none"> ◦ 推荐网段：您可以使用192.168.0.0/16或172.16.0.0/16两个标准IPv4网段。 ◦ 高级配置网段：您可以使用192.168.0.0/16或172.16.0.0/16及其子网作为专有网络的网段，网段掩码有效范围为8~28位。填写示例：192.168.0.0/16。 <p>本教程选择推荐网段192.168.0.0/16作为VPC的IPv4网段。</p> <div>  说明 VPC创建后，不能再修改IPv4网段。 </div>
IPv6网段	<p>选择是否分配IPv6网段。</p> <ul style="list-style-type: none"> ◦ 不分配：系统不分配IPv6网段。 ◦ 分配：系统自动分配IPv6网段。 <p>本教程选择不分配。</p>
描述	输入专有网络的描述信息。

4. 在创建成功对话框，单击**确认**后，返回**专有网络**页面，查看创建的专有网络。

步骤二：创建交换机

1. 在左侧导航栏，单击**交换机**。
2. 在交换机页面，单击**创建交换机**。
3. 在创建虚拟交换机页面，根据以下信息配置交换机，然后单击**提交**。

配置	说明
基本配置	
组织	选择交换机所属的组织。
资源集	选择交换机所属的资源集。
区域	
地域	选择交换机所属的地域。
可用区	<p>选择交换机所属的可用区。</p> <p>在一个专有网络中，每个交换机只能位于一个可用区内，不能跨多个可用区。您可以通过在不同可用区的交换机内部署云资源，实现跨可用区容灾。</p> <div>  说明 一个云资源实例只能添加到一个交换机中。 </div>
详细配置	

配置	说明
共享范围	<p>选择交换机的共享范围。</p> <ul style="list-style-type: none"> ◦ 本资源集：本资源集的管理员可以使用共享交换机创建资源。 ◦ 本组织及下级组织：本组织及下级组织的管理员可以使用共享交换机创建资源。 ◦ 本组织：本组织的管理员可以使用共享交换机创建资源。 <p>本教程选择本资源集。</p>
VPC	<p>选择要创建交换机的专有网络。</p> <p>本教程选择 <i>VPCtest</i>。</p>
裸机专用	<p>指定要创建的交换机是否为裸机专用。</p> <p>关于裸机，请参见 飞天智能运维平台用户指南手册中专有网络裸机特性说明 章节。</p> <p>本教程选择否。</p>
虚拟交换机名称	输入交换机的名称。
IPv4网段	<p>指定交换机的IPv4网段。</p> <p>本教程使用系统默认的IPv4网段。</p>
IPv6网段	<p>交换机的IPv6网段。</p> <p>当专有网络没有设置IPv6网段时，交换机IPv6网段不分配，本教程不分配交换机的IPv6网段。</p>
描述	输入该交换机的描述信息。

步骤三：创建安全组

1. 在页面顶部的菜单栏中，选择产品 > 弹性计算 > 云服务器 ECS。
2. 在左侧导航栏，选择网络和安全 > 安全组。
3. 在安全组页面，单击创建安全组。
4. 在创建安全组页面，根据以下信息配置安全组，然后单击提交。

配置	说明
区域	
组织	选择安全组的所属组织。
资源集	选择安全组的所属资源集。
地域	<p>选择安全组的所属地域。</p> <p>确保安全组的地域和VPC的地域相同。</p>

配置	说明
可用区	选择安全组的所属可用区。
基本配置	
共享范围	<p>选择安全组的共享范围。</p> <ul style="list-style-type: none">◦ 本资源集：本资源集的管理员可以使用安全组创建资源。◦ 本组织及下级组织：本组织及下级组织的管理员可以使用安全组创建资源。◦ 本组织：本组织的管理员可以使用安全组创建资源。 <p>本教程选择本资源集。</p>
VPC	选择安全组所属的专有网络。
安全组名称	输入安全组的名称。
描述	输入安全组的描述信息。

步骤四：创建ECS实例

1. 在页面顶部的菜单栏中，选择产品 > 网络 > 专有网络 VPC。
2. 在左侧导航栏，单击交换机。
3. 在顶部菜单栏处，选择交换机的地域。
4. 在交换机页面，找到目标交换机，然后在操作列单击创建ECS实例。
5. 在创建云服务器页面，配置ECS实例的信息并完成创建。

关于如何配置ECS实例，请参见云服务器ECS用户指南手册中快速入门下的使用向导创建实例章节。

3.3. 搭建IPv6专有网络

本教程指引您搭建一个具有IPv6地址块的专有网络，然后在该专有网络VPC（Virtual Private Cloud）中创建一个带有IPv6地址的云服务器ECS（Elastic Compute Service）实例，并可以访问IPv6服务。

步骤一：创建专有网络和交换机

要在专有网络中使用云资源，您需要先创建专有网络和交换机。

1. [登录专有网络管理控制台](#)。
2. 在专有网络页面，单击创建专有网络。
3. 在创建专有网络VPC页面，根据以下信息配置专有网络，然后单击提交。

配置	说明
组织	选择专有网络所属的组织。
资源集	选择专有网络所属的资源集。
地域	选择专有网络所属的地域。

配置	说明
共享范围	<p>选择VPC的共享范围。</p> <ul style="list-style-type: none"> 本资源集：本资源集的管理员可以使用共享VPC创建资源。 本组织及下级组织：本组织及下级组织的管理员可以使用共享VPC创建资源。 本组织：本组织的管理员可以使用共享VPC创建资源。 <p>本教程选择本资源集。</p>
专有网络名称	<p>输入专有网络的名称。</p> <p>本教程输入 <i>VPCtest</i>。</p>
IPv4网段	<p>选择IPv4网段，支持以下两种方式选择IPv4网段：</p> <ul style="list-style-type: none"> 推荐网段：您可以使用192.168.0.0/16或172.16.0.0/16两个标准IPv4网段。 高级配置网段：您可以使用192.168.0.0/16或172.16.0.0/16及其子网作为专有网络的网段，网段掩码有效范围为8~28位。填写教程：192.168.0.0/16。 <p>本教程选择推荐网段192.168.0.0/16作为VPC的IPv4网段。</p> <div> ? 说明 VPC创建后，不能再修改IPv4网段。 </div>
IPv6网段	<p>选择是否分配IPv6网段。</p> <ul style="list-style-type: none"> 不分配：系统不分配IPv6网段。 分配：系统自动分配IPv6网段。 <p>本教程选择分配。</p>
描述	输入专有网络的描述信息。

- 在专有网络管理控制台页面，单击左侧导航栏的交换机。
- 在交换机页面，单击创建交换机。
- 在创建虚拟交换机页面，根据以下信息配置交换机，然后单击提交。

配置	说明
组织	选择交换机所属的组织。
资源集	选择交换机所属的资源集。
地域	选择交换机所属的地域。
可用区	<p>选择交换机所属的可用区。</p> <p>在一个专有网络中，每个交换机只能位于一个可用区内，不能跨多个可用区。您可以通过在不同可用区的交换机内部署云资源，实现跨可用区容灾。</p> <div> ? 说明 一个云资源实例只能添加到一个交换机中。 </div>

配置	说明
共享范围	选择交换机的共享范围。 <ul style="list-style-type: none">◦ 本资源集：本资源集的管理员可以使用共享交换机创建资源。◦ 本组织及下级组织：本组织及下级组织的管理员可以使用共享交换机创建资源。◦ 本组织：本组织的管理员可以使用共享交换机创建资源。 本教程选择 本资源集 。
VPC	选择要创建交换机的专有网络。 本教程选择 VPCtest 。
裸机专用	指定要创建的交换机是否为裸机专用。 关于裸机，请参见 飞天智能运维平台用户指南手册中专有网络裸机特性说明 章节。 本教程选择否。
虚拟交换机名称	输入交换机的名称。
IPv4网段	指定交换机的IPv4网段。 本教程使用系统默认的IPv4网段。
IPv6网段	指定交换机的IPv6网段。 本教程使用系统默认的IPv6网段。
描述	输入该交换机的描述信息。

步骤二：创建安全组

- 1. 在页面顶部的菜单栏中，选择产品 > 弹性计算 > 云服务器 ECS。
- 2. 在左侧导航栏，选择网络和安全 > 安全组。
- 3. 在页面，单击创建安全组。
- 4. 在创建安全组页面，根据以下信息配置安全组，然后单击提交。

配置	说明
组织	选择安全组的所属组织。
资源集	选择安全组的所属资源集。
地域	选择安全组的所属地域。 确保安全组的地域和VPC的地域相同。
可用区	选择安全组的所属可用区。

配置	说明
共享范围	选择安全组的共享范围。 <ul style="list-style-type: none">◦ 本资源集：本资源集的管理员可以使用安全组创建资源。◦ 本组织及下级组织：本组织及下级组织的管理员可以使用安全组创建资源。◦ 本组织：本组织的管理员可以使用安全组创建资源。 本教程选择 本资源集 。
VPC	选择安全组所属的专有网络。
安全组名称	输入安全组的名称。
描述	输入安全组的描述信息。

步骤三：创建并配置ECS实例

创建IPv6专有网络和交换机后，您需要创建一个具有IPv6地址的ECS实例。创建ECS实例后，您还需要将分配的IPv6地址配置到ECS实例的网卡上。

1. 在页面顶部的菜单栏中，选择**产品 > 网络 > 专有网络 VPC**。
2. 在左侧导航栏，单击**交换机**。
3. 在顶部菜单栏处，选择交换机的地域。
4. 在**交换机**页面，找到目标交换机，然后在操作列单击**创建ECS实例**。
5. 在**创建云服务器**页面，配置云服务器ECS，然后单击**提交**。

本操作中选择**分配IPv6地址**，其他参数配置，请参见**云服务器ECS用户指南手册中快速入门下的使用向导创建实例**章节。

6. 返回**实例列表**页面，单击实例ID，查看分配的IPv6地址。
7. 配置静态IPv6地址。
 - 如果您的ECS实例的镜像支持DHCPv6，您无需手动配置静态IPv6地址。支持DHCPv6镜像的ECS实例可以自动化配置IPv6地址，创建实例后即可使用分配的IPv6地址进行内网通信。

以下镜像支持DHCPv6：

 - Linux镜像：
 - CentOS 7.6 IPV6 64Bit
 - CentOS 6.10 64Bit
 - SUSE Linux Enterprise Server 12 SP4 64Bit
 - Windows Server镜像
 - 如果您的ECS实例的镜像不支持DHCPv6，您需要为ECS实例配置IPv6地址。更多信息，请查询各镜像ECS实例配置IPv6地址的方法。

步骤四：开通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，您需要开通IPv6公网带宽。

1. 在页面顶部的菜单栏中，选择产品 > 网络 > 专有网络 VPC。
2. 在左侧导航栏，单击IPv6网关。
3. 在顶部菜单栏处，选择IPv6网关的地域。
4. 在IPv6网关页面，找到目标IPv6网关，然后在操作列单击管理。
5. 在IPv6网关页面，单击IPv6公网带宽页签。
6. 在IPv6公网带宽页签，找到目标IPv6地址，然后在操作列单击开通公网带宽。
7. 选择要开通的IPv6网关带宽，然后单击提交。

免费版、企业版和企业增强版IPv6网关，单个IPv6最大公网带宽峰值均为2 Gbps。

步骤五：配置安全组规则

IPv4和IPv6通信彼此独立，如果当前的安全组规则不能满足业务需求，您需要为ECS实例单独配置IPv6安全组规则。

关于配置安全组规则的详细信息，请参见云服务器ECS用户指南手册中安全组下的添加安全组规则章节。

步骤六：测试网络连通性

登录ECS实例，ping一个IPv6服务测试通信是否正常。

```
[root@izbp1-73damf1fZ ~]# ping6 aliyun.com
PING aliyun.com(2401:b8:1::6 (2401:b8:1::6)) 56 data bytes
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=1 ttl=94 time=5.54 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=2 ttl=94 time=5.51 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=3 ttl=94 time=5.50 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=4 ttl=94 time=5.51 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=5 ttl=94 time=5.53 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=6 ttl=94 time=5.50 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=7 ttl=94 time=5.51 ms
64 bytes from 2401:b8:1::6 (2401:b8:1::6): icmp_seq=8 ttl=94 time=5.50 ms
^C
--- aliyun.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 701ms
rtt min/avg/max/mdev = 5.496/5.512/5.538/0.014 ms
```

4. 专有网络和交换机

4.1. 专有网络和交换机概述

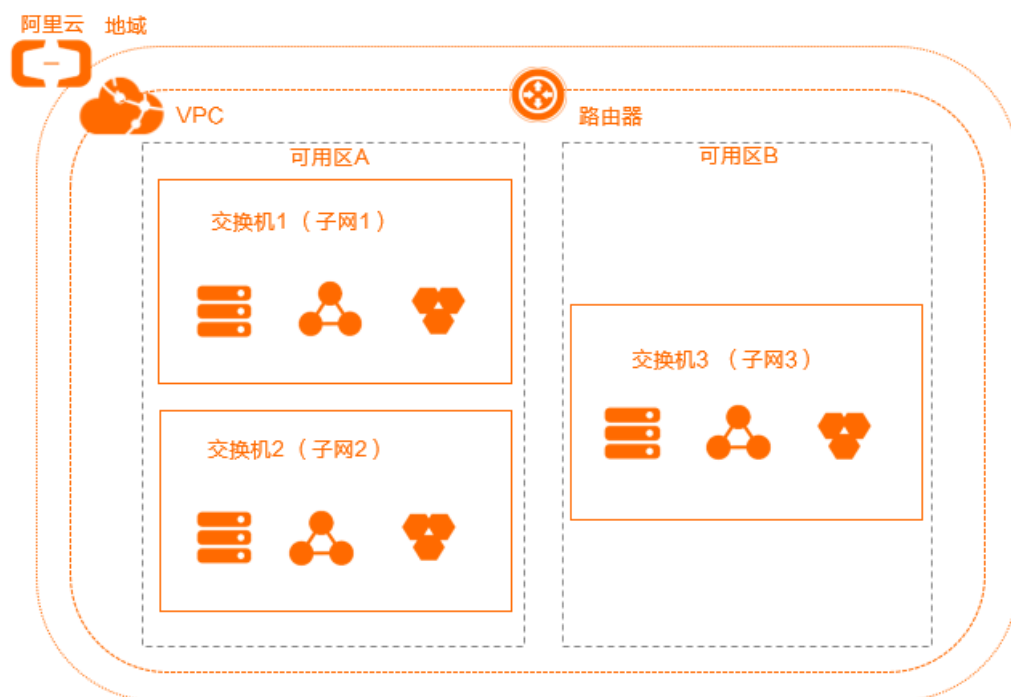
在专有网络VPC（Virtual Private Cloud）中使用云资源前，您必须先创建一个专有网络和交换机。您可以在一个专有网络中创建多个交换机来划分子网。一个专有网络内的子网默认私网互通。

专有网络和交换机

专有网络是您专有的云上私有网络，您可以将云资源部署在您自定义的专有网络中。

 **说明** 云资源不可以直接部署在专有网络中，必须属于专有网络内的一个交换机内。

交换机（vSwitch）是组成专有网络的基础网络设备，用来连接不同的云资源实例。专有网络是地域级别的资源，专有网络不可以跨地域，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。

专有网络可在双栈模式下运行。专有网络中的资源可通过IPv4和IPv6进行通信。IPv4和IPv6地址彼此独立，您需要在专有网络中分别针对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
32位二进制数。 表示方法：以半角句号（.）分隔的4个十进制数，例如192.168.1.11。	128位二进制数。 表示方法：以半角冒号（:）分隔的8组十六进制数，每组4个十六进制数，例如2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。
默认开启IPv4地址协议。	可以选择开通IPv6。
专有网络地址块大小可以从/8到/24。	专有网络地址块大小固定为/61。
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地址池中为您的专有网络选择IPv6地址块。
所有实例类型都支持。	部分实例类型不支持。 更多信息，请参见 云服务器ECS用户指南手册中什么是云服务器ECS下的实例规格 章节。
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。

默认情况下，专有网络的IPv4和IPv6地址都只支持私网通信。同一专有网络内不同交换机的云资源可通过私网通信。如果您需要专有网络连接其他专有网络或本地IDC，您可以配置高速通道或VPN网关等方式实现互通。

如果需要进行公网通信，需要分别进行配置：

- IPv4公网通信

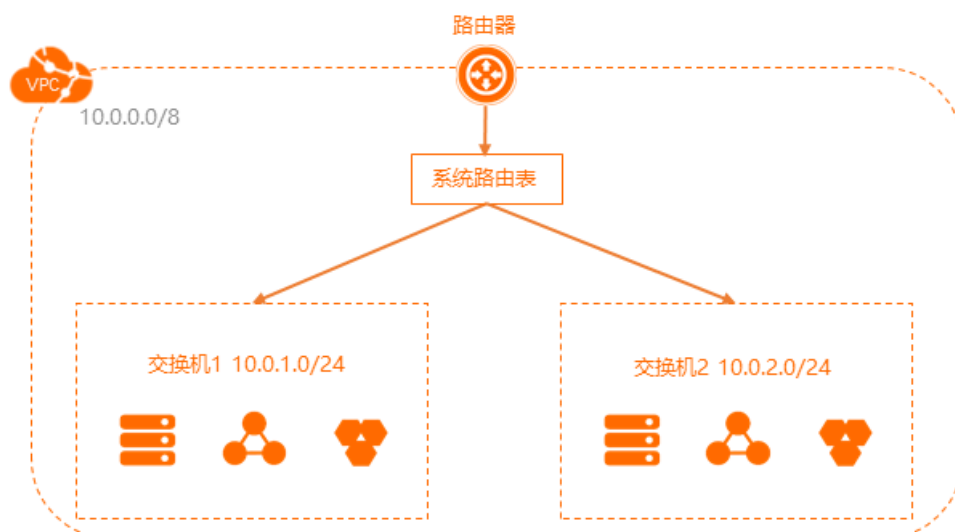
您可以通过配置弹性公网IP或NAT网关的方式使专有网络内的ECS实例通过IPv4地址进行公网通信。

- IPv6公网通信

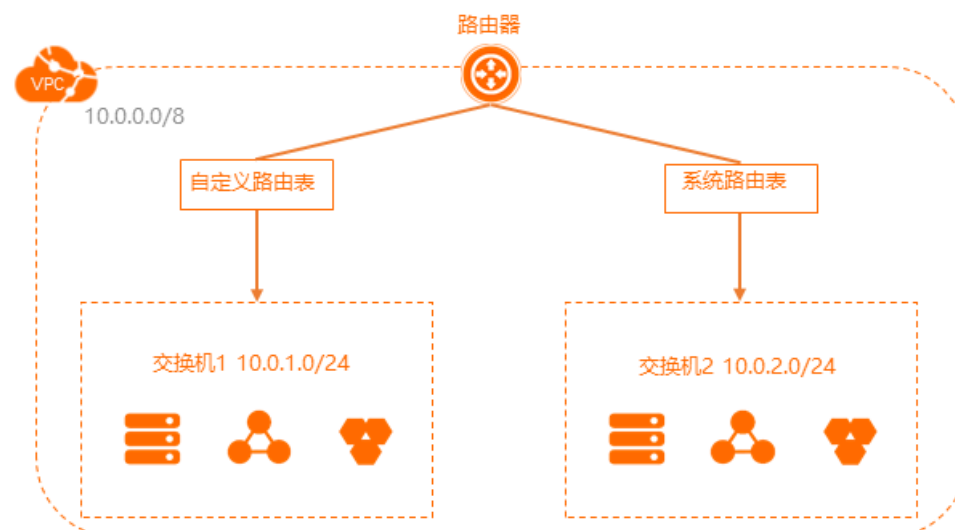
您需要为进行公网通信的IPv6地址购买公网带宽。您也可以为该IPv6地址配置仅主动出规则，只允许专有网络中的云产品实例经IPv6地址访问公网，而不允许IPv6客户端主动与专有网络中的云资源实例建立连接。

路由

创建专有网络后，系统会自动为您创建一张系统路由表并为其添加系统路由来管理专有网络的流量。一个专有网络只有一张系统路由表，您不能手动创建也不能删除系统路由表。



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。具体操作，请参见[创建自定义路由表](#)。



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路由条目可以匹配目的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。具体操作，请参见[添加自定义路由条目](#)。

4.2. 管理专有网络

4.2.1. 创建专有网络


专有网络VPC（Virtual Private Cloud）是您专有的云上私有网络。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。本文为您介绍如何创建专有网络。

前提条件

创建专有网络前，您必须先做好网络规划。更多信息，请参见[网络规划](#)。

操作步骤

- 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。

 说明 专有网络的地域和要部署的云资源的地域必须相同。

- 3. 在专有网络页面，单击创建专有网络。
- 4. 在创建专有网络VPC页面，根据以下信息配置专有网络，然后单击提交。

配置	说明
组织	选择专有网络所属的组织。
资源集	选择专有网络所属的资源集。
地域	选择专有网络所属的地域。
共享范围	<p>选择VPC的共享范围。</p> <ul style="list-style-type: none">本资源集：本资源集的管理员可以使用共享VPC创建资源。本组织及下级组织：本组织及下级组织的管理员可以使用共享VPC创建资源。本组织：本组织的管理员可以使用共享VPC创建资源。
专有网络名称	<p>输入专有网络的名称。</p> <p>名称长度在2~128个字符之间，必须以英文字母和中文字符开头，可包含数字、下划线（_）和短划线（-），但不能以 http:// 或 https:// 开头。</p>
IPv4网段	<p>选择IPv4网段，支持以下两种方式选择IPv4网段：</p> <ul style="list-style-type: none">推荐网段：您可以使用192.168.0.0/16或172.16.0.0/16和两个标准IPv4网段作为专有网络的网段。高级配置网段：您可以使用192.168.0.0/16或172.16.0.0/16及其子网作为专有网络的网段，网段掩码有效范围为8~28位。填写示例：192.168.0.0/24。 <p> 说明 VPC创建后，不能再修改IPv4网段。</p>
IPv6网段	<p>选择是否分配IPv6网段。</p> <ul style="list-style-type: none">不分配：系统不分配IPv6网段。分配：系统自动分配IPv6网段。 <p> 说明 如果此处选择不分配，您可以在创建完成专有网络后，在专有网络页面，在IPv6网段列单击开通IPv6。选中自动开启VPC内所有交换机IPv6功能，VPC内的所有交换机也会开启IPv6功能。</p> <p>系统将为您的VPC自动创建一个免费版的IPv6网关，并分配掩码为/61的IPv6网段，例如2XX1:db8::/61。默认IPv6地址只具备私网通能力。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，您需要开通IPv6公网带宽。具体操作，请参见IPv6网关用户指南手册中管理IPv6公网带宽下的开通IPv6公网带宽章节。</p>

配置	说明
描述	输入专有网络的描述信息。 描述长度在2~256个字符之间，不能以 <code>http://</code> 或 <code>https://</code> 开头。

4.2.2. 添加附加IPv4网段

专有网络VPC（Virtual Private Cloud）创建后，您可以添加附加IPv4网段来扩充专有网络的网段。

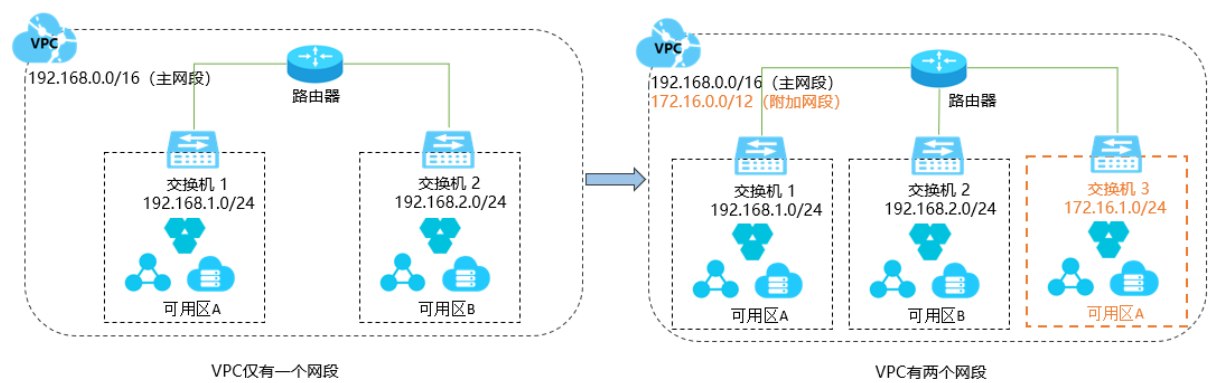
前提条件

您已经创建了专有网络。具体操作，请参见[创建专有网络](#)。

背景信息

创建专有网络时配置的IPv4网段是专有网络的主IPv4网段。专有网络创建后，您不能修改专有网络的主IPv4网段，但您可以添加附加IPv4网段来扩充专有网络的网段。添加后，主IPv4网段和附加IPv4网段同时生效。您可以选择使用主IPv4网段或附加IPv4网段来创建交换机，但每个交换机网段只能属于一个专有网络网段。

同主IPv4网段一样，使用附加IPv4网段创建交换机时，系统也会在专有网络路由表中自动添加一条交换机路由。交换机路由的目标网段是交换机使用的网段，该网段范围不得与所属专有网络路由表中的其它路由的目标网段范围相同或大于该范围。



说明 一个专有网络默认只支持添加1个附加IPv4网段，且无法提升配额。

操作步骤

1. [登录专有网络管理控制台](#)。
2. 在顶部菜单栏处，选择专有网络的地域。
3. 在专有网络页面，找到目标专有网络，然后在操作列单击[管理](#)。
4. 在网段管理页签下，单击[添加附加IPv4网段](#)。
5. 在添加附加IPv4网段对话框，根据以下信息配置附加IPv4网段，然后单击[确定](#)。

配置	说明
专有网络	显示要添加附加IPv4网段的专有网络。

配置	说明
附加网段	<p>选择一种方式配置附加网段。</p> <ul style="list-style-type: none"> ◦ 推荐网段：您可以使用192.168.0.0/16或172.16.0.0/12两个标准网段作为专有网络的附加IPv4网段。 ◦ 高级配置网段：您可以使用192.168.0.0/16或172.16.0.0/12及其子网作为专有网络的附加IPv4网段。 <p>添加附加IPv4网段时，应遵循以下原则。</p> <ul style="list-style-type: none"> ◦ 不能以0开头，掩码长度有效范围为8~24位。 ◦ 附加IPv4网段不得与专有网络主IPv4网段及已添加的附加IPv4网段重叠。 <p>例如，在主IPv4网段为192.168.0.0/16的专有网络中，您不能添加以下网段作为附加IPv4网段。</p> <ul style="list-style-type: none"> ■ 比192.168.0.0/16范围更大的网段，例如192.168.0.0/8。 ■ 与192.168.0.0/16范围相同的网段。 ■ 比192.168.0.0/16范围更小的网段，例如192.168.0.0/24。

4.2.3. 删除附加IPv4网段

您可以删除专有网络VPC（Virtual Private Cloud）的附加IPv4网段，但您不能删除主IPv4网段。

前提条件

请确保您已经删除了在附加IPv4网段下创建的交换机。具体操作，请参见[删除交换机](#)。



操作步骤

1. [登录专有网络管理控制台](#)。
2. 在顶部菜单栏处，选择专有网络的地域。
3. 在专有网络页面，找到目标专有网络，然后在操作列单击**管理**。
4. 在网段管理页签下，找到目标附加IPv4网段，然后在操作列单击**删除**。
5. 在弹出的对话框，单击**确定**。

4.2.4. 修改专有网络

您可以修改专有网络VPC（Virtual Private Cloud）的名称和描述信息。

操作步骤

1. [登录专有网络管理控制台](#)。
2. 在顶部状态栏处，选择专有网络的地域。
3. 在专有网络页面，找到目标专有网络，然后在操作列单击**管理**。
4. 在专有网络基本信息区域，在专有网络名称右侧单击图标，在弹出的对话框中修改专有网络的名称，然后单击**确定**。
5. 在专有网络基本信息区域，在描述右侧单击图标，在弹出的对话框中修改描述信息，然后单击**确定**。

定。

4.2.5. 删除专有网络

您可以删除一个不需要的专有网络VPC（Virtual Private Cloud）。删除专有网络后，专有网络关联的路由器和路由表也会被删除。

前提条件

删除专有网络前，请确保满足以下条件：

- 要删除的专有网络下没有交换机，如有请先删除交换机。具体操作，请参见[删除交换机](#)。
- 要删除的专有网络下没有IPv6网关，如有请先删除IPv6网关。具体操作，请参见[IPv6网关用户指南手册](#)中[管理IPv6网关节点删除IPv6网关](#)章节。


操作步骤

1. [登录专有网络管理控制台](#)。
2. 在顶部菜单栏处，选择专有网络的地域。
3. 在专有网络页面，找到要删除的专有网络，然后在操作列单击删除。
4. 在删除专有网络对话框，单击确定。

4.2.6. 管理标签

专有网络VPC（Virtual Private Cloud）支持标签功能，您可以通过标签功能来标记和分类专有网络，以便于您对专有网络进行搜索和筛选。

操作步骤

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。
3. 在专有网络页面，找到目标专有网络实例，鼠标悬停在标签列下-或已有标签右侧，然后单击图标。
4. 在编辑标签对话框中，单击添加，根据以下信息配置标签，然后单击确定。

配置	说明
标签键	标签的标签键，支持选择已有标签键或输入新的标签键。 标签键最多支持64个字符，不能以 <code>aliyun</code> 或 <code>acs:</code> 开头，不能包含 <code>http://</code> 和 <code>https://</code> 。
标签值	标签的标签值，支持选择已有标签值或输入新的标签值。 标签值最多支持128个字符，不能以 <code>aliyun</code> 或 <code>acs:</code> 开头，不能包含 <code>http://</code> 和 <code>https://</code> 。

5. 返回专有网络页面，单击标签筛选，可在弹出的对话框根据标签键和标签值来筛选专有网络。


4.3. 管理交换机

4.3.1. 创建交换机

交换机（vSwitch）是组成专有网络的基础网络模块，用来连接不同的云资源。

背景信息

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。云资源必须部署在交换机内，您可以在不同可用区的交换机部署应用，提高应用的可用性。

 **说明** 交换机不支持组播和广播。

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**交换机**。
3. 在顶部菜单栏，选择要创建交换机的专有网络所属的地域。
4. 在**交换机**页面，单击**创建交换机**。
5. 在**创建虚拟交换机**页面，根据以下信息配置交换机，然后单击**提交**。

配置	说明
组织	选择交换机所属的组织。
资源集	选择交换机所属的资源集。
地域	选择交换机所属的地域。
可用区	<div>选择交换机所属的可用区。</div> <div>在一个专有网络中，每个交换机只能位于一个可用区内，不能跨多个可用区。您可以通过在不同可用区的交换机内部署云资源，实现跨可用区容灾。</div> <div> 说明 一个云资源实例只能添加到一个交换机中。</div>
共享范围	<div>选择交换机的共享范围。</div> <div><ul style="list-style-type: none">◦ 本资源集：本资源集的管理员可以使用共享交换机创建资源。◦ 本组织及下级组织：本组织及下级组织的管理员可以使用共享交换机创建资源。◦ 本组织：本组织的管理员可以使用共享交换机创建资源。</div>
VPC	选择要创建交换机的专有网络。
裸机专用	<div>指定要创建的交换机是否为裸机专用。</div> <div>关于裸机，请参见 飞天智能运维平台用户指南手册中专有网络裸机特性说明 章节。</div>
虚拟交换机名称	输入交换机的名称。

配置	说明
IPv4网段	<p>输入交换机的网段。</p> <ul style="list-style-type: none"> 您需要以CIDR block的形式指定交换机的网段，每个交换机的网络掩码为16~29位，可以提供8~65536个IP地址。 交换机的网段必须是其所属VPC网段的真子集。 每个交换机的第1个和最后3个IP地址为系统保留地址。如果交换机网段为192.168.1.0/24，那么192.168.1.0和192.168.1.253、192.168.1.254、192.168.1.255是系统保留地址。 交换机的网段不能与所属VPC的路由条目的目标网段相同，但可以是路由条目的目标网段的真子集。 交换机创建成功后，网段无法修改。
IPv6网段	<p>交换机的IPv6网段。</p> <ul style="list-style-type: none"> 如果要创建的交换机所属的VPC未开通IPv6，则不能为交换机分配IPv6网段。 如果要创建的交换机所属的VPC已开通IPv6，则您可以输入十进制数字0~7，来自定义交换机IPv6网段的最后8比特位。 <p>例如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网段为2XX1:db8:ff::/64。</p>
描述	输入该交换机的描述信息。

4.3.2. 创建云资源

云资源不可以直接部署在专有网络VPC（Virtual Private Cloud）下，必须属于专有网络内的一个交换机（子网）。您可以在交换机中创建云资源。云资源包括云服务器ECS（Elastic Compute Service）实例、负载均衡SLB（Server Load Balancer）实例和云数据库RDS（Relational Database Service）实例。



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**交换机**。
3. 在顶部菜单栏，选择交换机所属专有网络的地域。
4. 在**交换机**页面，创建以下云资源。
 - 在操作列单击**创建ECS实例**，然后在**创建云服务器**页面完成创建。
关于如何配置ECS实例，请参见[云服务器ECS用户指南手册中快速入门下的使用向导创建实例](#)章节。
 - 在操作列选择 ... 图标 > **创建SLB实例**，然后在**创建负载均衡SLB**页面完成创建。
关于如何配置SLB实例，请参见[负载均衡用户指南手册中快速入门下的创建负载均衡实例](#)章节。
 - 在操作列选择 ... 图标 > **创建RDS实例**，然后在**创建云数据库RDS**页面完成创建。
关于如何配置RDS实例，请参见[云数据库RDS用户指南手册中快速入门下的创建实例](#)章节。

4.3.3. 修改交换机

创建交换机后，您可以修改交换机的名称和描述信息。

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[交换机](#)。
- 3. 在顶部菜单栏，选择交换机所属专有网络的地域。
- 4. 在[交换机](#)页面，找到目标交换机，然后在操作列单击[管理](#)。
- 5. 在[交换机基本信息](#)区域，在[交换机名称](#)右侧单击图标，在弹出的对话框修改交换机的名称。
- 6. 在[交换机基本信息](#)区域，在[描述](#)右侧单击图标，在弹出的对话框修改描述信息。

4.3.4. 删除交换机

您可以删除一个不需要的交换机。删除交换机后，云资源将不能部署在该交换机内。

前提条件

删除交换机前，请确保满足以下条件：

- 您已经删除交换机下创建的云资源，例如云服务器ECS（Elastic Compute Service）实例、负载均衡SLB（Server Load Balancer）实例和云数据库RDS（Relational Database Service）实例等。
- 如果要删除的交换机下配置了SNAT条目、高可用虚拟IP等，请确保您已经删除了这些关联的资源。


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[交换机](#)。
- 3. 选择交换机所属专有网络的地域。
- 4. 在[交换机](#)页面，找到目标交换机，然后在操作列单击[删除](#)。
- 5. 在[删除交换机](#)对话框，单击[确定](#)。

4.3.5. 管理标签

交换机支持标签功能，您可以通过标签功能来标记和分类交换机，以便于您对交换机进行搜索和筛选。

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[交换机](#)。
- 3. 在顶部菜单栏，选择交换机所属专有网络的地域。
- 4. 在[交换机](#)页面，找到目标交换机实例，鼠标悬停在[标签列下](#)-图标或已有标签右侧，然后单击图标。
- 5. 在[编辑标签](#)对话框，单击[添加](#)，根据以下信息配置标签，然后单击[确定](#)。

配置	说明
----	----

配置	说明
标签键	标签的标签键，支持选择已有标签键或输入新的标签键。 标签键最多支持64个字符，不能以 <code>aliyun</code> 或 <code>acs:</code> 开头，不能包含 <code>http://</code> 和 <code>https://</code> 。
标签值	标签的标签值，支持选择已有标签值或输入新的标签值。 标签值最多支持128个字符，不能以 <code>aliyun</code> 或 <code>acs:</code> 开头，不能包含 <code>http://</code> 和 <code>https://</code> 。

6. 返回交换机页面，单击**标签筛选**，可在弹出的对话框根据标签键和标签值来筛选交换机。

5. 路由表

5.1. 路由表概述

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系统路由表，但您可以在专有网络内创建自定义路由表，将自定义路由表和交换机绑定来控制子网路由，更灵活地进行网络管理。交换机绑定自定义路由表绑定后，交换机会与系统路由表解绑。具体操作，请参见[子网路由](#)。

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。

系统路由

创建专有网络后，系统会在路由表中自动添加以下系统路由：

- 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。

例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以下三条系统路由，表中的“-”表示VPC内部：

目标网段	下一跳	下一跳类型
100.64.0.0/10	-	系统路由
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。
- NAT网关：将指向目标网段的流量转发到一个NAT网关。
当需要通过NAT网关连接互联网时，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。具体操作，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路由条目可以匹配目的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。

例如下表为某专有网络的路由表，表中的“-”表示VPC内部。

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

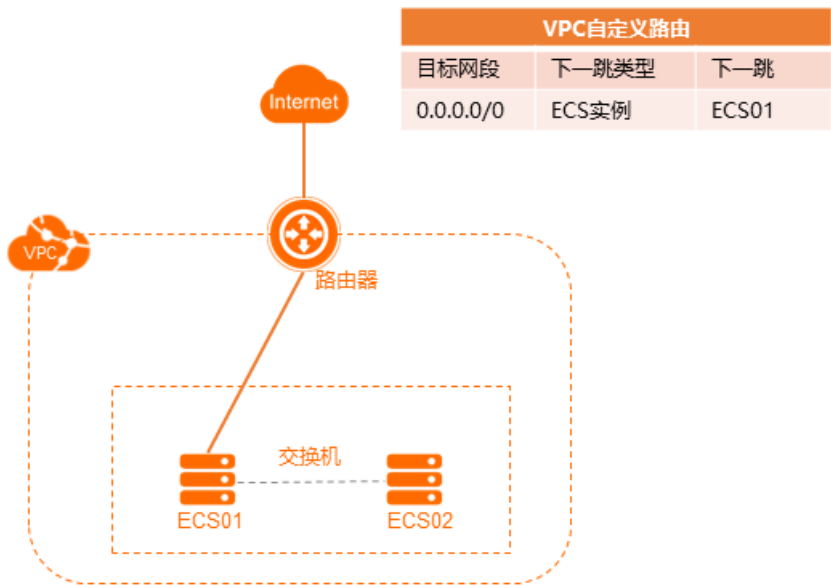
目标网段为 100.64.0.0/10 和 192.168.0.0/24 的两条路由均为系统路由。目标网段为 0.0.0.0/0 和 10.0.0.0/24 的两条路由为自定义路由，表示将访问 0.0.0.0/0 地址段的流量转发至ID为 i-12345678 的ECS实例，将访问 10.0.0.0/24 地址段的流量转发至ID为 i-87654321 的ECS实例。根据最长前缀匹配规则，在该专有网络中，访问 10.0.0.1 的流量会转发至 i-87654321，而访问 10.0.1.1 的流量会转发至 i-12345678。

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）

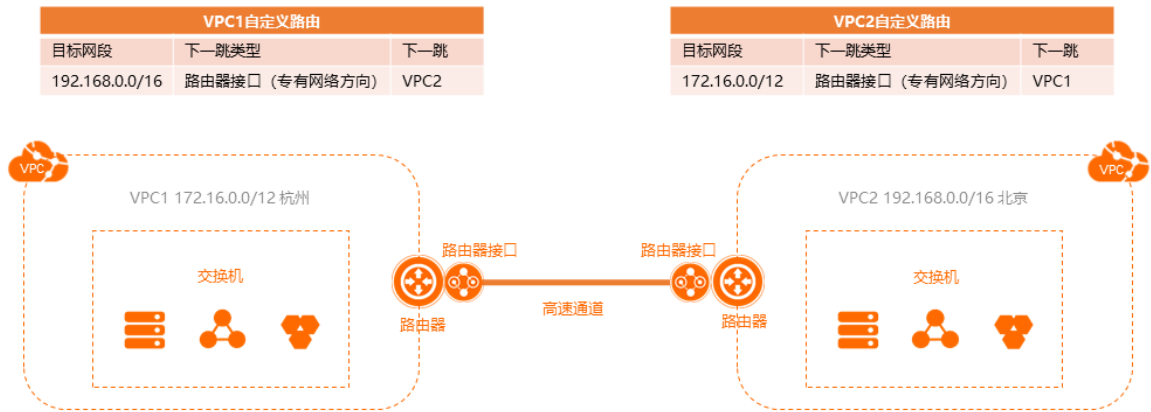
如下图所示，当使用高速通道连接两个VPC（VPC1 172.16.0.0/12和VPC2 192.168.0.0/16）时，创建完两个互相连接的路由器接口后，您还需要在两个VPC中分别添加如下一条路由：

○ 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）

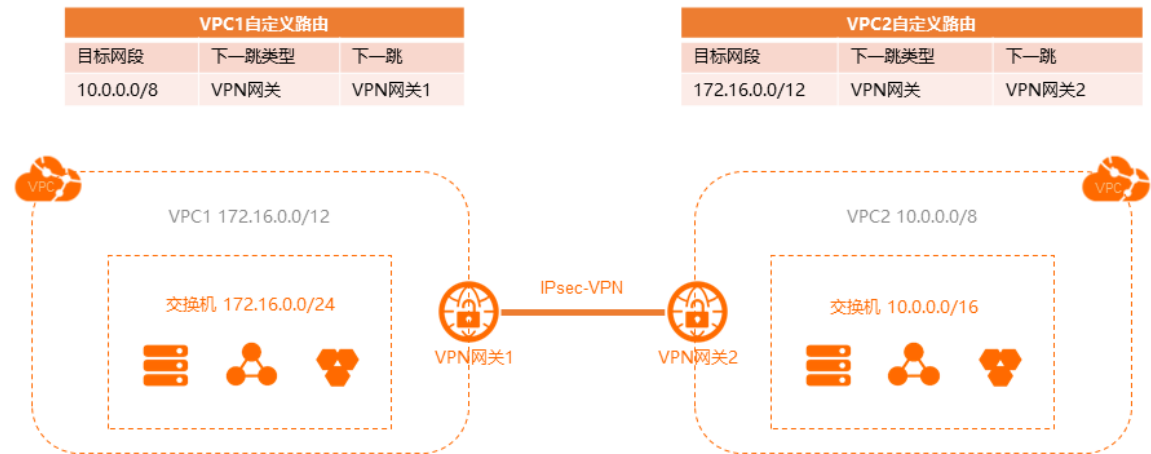
如下图所示，当使用VPN网关连接两个VPC（VPC1 172.16.0.0/12和VPC2 10.0.0.0/8）时，配置完VPN网关后，需要在VPC中分别添加如下路由：

◦ 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

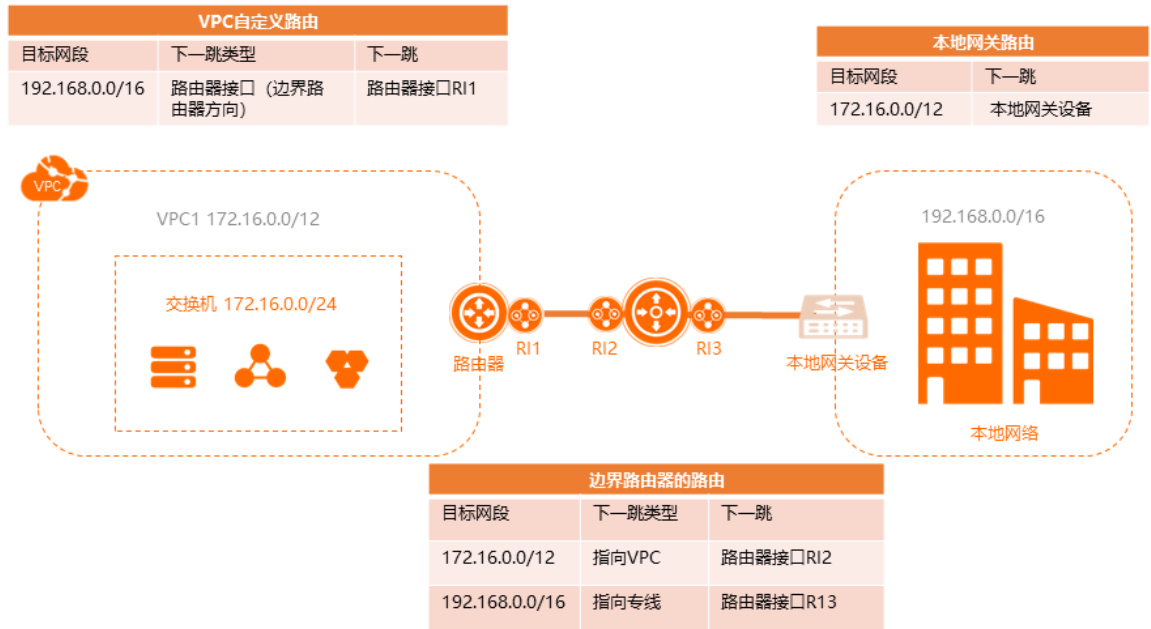
目标网段	下一跳类型	下一跳
192.168.0.0/16	路由器接口（普通路由）	路由器接口RI1

◦ 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
172.16.0.0/12	指向VPC	路由器接口RI2

本地网络的路由配置

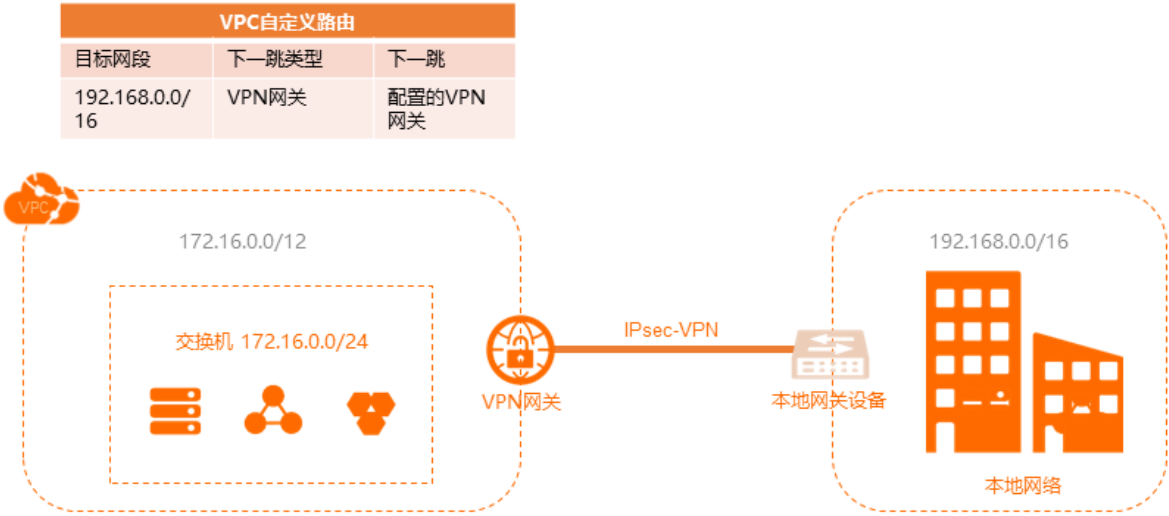
目标网段	下一跳类型	下一跳
172.16.0.0/12	本地网关	本地网关设备



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



5.2. 创建自定义路由表

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

- 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. 在顶部菜单栏，选择要创建的路由表的地域。
- 4. 在路由表页面，单击创建路由表。
- 5. 在创建路由表对话框，根据以下信息配置路由表，然后单击确定。

配置	说明
基本信息	
组织	选择路由表所属的组织。
资源集	选择路由表所属的资源集。
地域	选择路由表所属的地域。
VPC	选择路由表所属的专有网络。
名称	输入路由表的名称。
描述	输入路由表的描述。

创建路由表后，您可以在路由表页面查看路由表类型为自定义的路由表。

绑定交换机和路由表

您可以绑定交换机与自定义路由表。

- 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. 在顶部菜单栏，选择路由表所属的地域。
- 4. 在路由表页面，找到目标自定义路由表，单击路由表的ID。
- 5. 在路由表基本信息区域，单击已绑定交换机页签，然后单击绑定交换机。
- 6. 在弹出的对话框，选择要绑定的交换机，然后单击确定。

解绑交换机和路由表

您可以解除交换机中已绑定的自定义路由表，解除绑定后，该交换机自动绑定其系统路由表。

- 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. 在顶部菜单栏，选择路由表所属的地域。
- 4. 在路由表页面，找到目标路由表，单击路由表的ID。
- 5. 在路由表基本信息区域，单击已绑定交换机页签，找到目标交换机，然后在操作列单击解绑。
- 6. 在弹出的对话框，单击确定。

删除自定义路由表

您可以删除自定义路由表，但您不能删除系统路由表。如果删除的自定义路由表绑定了交换机，请先解绑交换机。

- 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. 在顶部菜单栏，选择路由表所属的地域。
- 4. 在路由表页面，找到目标路由表，然后在操作列单击删除。
- 5. 在弹出的对话框，单击确定。

5.3. 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条目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。路由条目由目标网段、下一跳类型、下一跳三部分组成，指定了网络流量的导向目的地。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条目。

操作步骤

- 1. 登录[专有网络管理控制台](#)。
- 2. 在左侧导航栏，单击路由表。
- 3. 在顶部菜单栏，选择路由表所属的地域。
- 4. 在路由表页面，找到目标路由表，然后在操作列单击管理。
- 5. 在路由条目列表页签，单击添加路由条目。
- 6. 在添加路由条目对话框，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	输入路由条目的目标网段。 <ul style="list-style-type: none">◦ IPv4网段：目标网段为IPv4网段。◦ IPv6网段：目标网段为IPv6网段。

配置	说明
下一跳类型	<p>选择下一跳类型：</p> <ul style="list-style-type: none">◦ 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。◦ 高可用虚拟IP：将目的地址在目标网段范围内的流量路由至选择的高可用虚拟IP实例。◦ 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。 <p>此种模式下，您还需要选择路由的方式：</p> <ul style="list-style-type: none">■ 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。 <div><p>② 说明 当目标网段选择IPv6网段时，下一跳类型支持选择路由器接口（边界路由器方向）。</p></div>
ECS实例/VPN网关/NAT网关/辅助弹性网卡/高可用虚拟IP/路由器接口（专有网络方向）/路由器接口（边界路由器方向）	选择下一跳实例。

5.4. 导出路由条目

您可以导出路由表中的路由条目，导出的路由条目可以作为备份保存在本地。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击路由表。



3. 在顶部菜单栏处，选择路由表所属的地域。
4. 在路由表页面，找到目标路由表，然后单击操作列下的管理。
5. 在路由表基本信息区域，单击路由条目列表页签，然后单击导出。

导出的路由条目为.csv文件，您可以在本地查看导出的路由条目。

5.5. 修改路由表

创建路由表后，您可以修改路由表的名称和描述信息。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击路由表。
3. 在顶部菜单栏处，选择路由表所属的地域。
4. 在路由表页面，找到目标路由表，然后单击操作列下的管理。
5. 在路由表基本信息区域，在路由表名称右侧单击图标，在弹出的对话框修改路由表的名称，然后单击确定。
6. 在路由表基本信息区域，在描述右侧单击图标，在弹出的对话框修改路由表的描述信息，然后单击确定。

5.6. 删除自定义路由条目

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。您可以删除自定义路由条目，但您不能删除系统路由条目。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击路由表。
3. 在顶部菜单栏处，选择路由表所属的地域。
4. 在路由表页面，找到目标路由表，然后单击操作列下的管理。
5. 在路由条目列表页签，找到目标自定义路由条目，单击操作列下的删除。
6. 在删除路由条目对话框，单击确定。

5.7. 子网路由

您可以在专有网络VPC（Virtual Private Cloud）内创建自定义路由表，并在自定义路由表中添加自定义路由条目，然后将自定义路由表绑定至交换机来控制该交换机的流量，方便您更灵活地进行网络管理，以上操作被称为子网路由。

前提条件

您已经创建了专有网络。具体操作，请参见[创建专有网络](#)。

步骤一：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. 在顶部菜单栏，选择要创建的路由表的地域。
4. 在**路由表**页面，单击**创建路由表**。
5. 在**创建路由表**面板，根据以下信息配置路由表，然后单击**确定**。

配置	说明
专有网络	选择路由表所属的VPC。
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（_）和短划线（-）。
描述	输入路由表的描述。 描述长度为2~256个字符，不能以 <code>http://</code> 和 <code>https://</code> 开头。

创建路由表后，您可以在**路由表**页面查看路由表类型为自定义的路由表。

步骤二：添加自定义路由条目到自定义路由表

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. 在顶部菜单栏，选择路由表所属的地域。
4. 在**路由表**页面，找到目标路由表，然后在操作列单击**管理**。
5. 在**路由表基本信息**区域，单击**添加路由条目**。
6. 在**添加路由条目**面板，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	输入路由条目的目标网段。 <ul style="list-style-type: none">◦ IPv4网段：目标网段为IPv4网段。◦ IPv6网段：目标网段为IPv6网段。

配置	说明
下一跳类型	<p>选择下一跳类型：</p> <ul style="list-style-type: none">◦ 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。◦ 高可用虚拟IP：将目的地址在目标网段范围内的流量路由至选择的高可用虚拟IP实例。◦ 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。 <p>此种模式下，您还需要选择路由的方式：</p> <ul style="list-style-type: none">■ 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。 <ul style="list-style-type: none">◦ IPv6网关：将目的地址在目标IPv6网段范围内的流量路由至选择的IPv6网关。 <div><p> 说明 当目标网段选择IPv6网段时，下一跳类型支持选择IPv6网关和路由器接口（边界路由器方向）。</p></div>
ECS实例/VPN网关/NAT网关/辅助弹性网卡/高可用虚拟IP/路由器接口（专有网络方向）/路由器接口（边界路由器方向）/IPv6网关	选择下一跳实例。

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. 登录[专有网络管理控制台](#)。
- 2. 在左侧导航栏，单击路由表。

3. 在顶部菜单栏，选择路由表所属的地域。
4. 在路由表页面，找到目标自定义路由表，单击路由表的ID。
5. 在路由表基本信息区域，单击已绑定交换机页签，然后单击绑定交换机。
6. 在绑定交换机对话框，选择要绑定的交换机，然后单击确定。

6. 高可用虚拟IP

6.1. 高可用虚拟IP概述

高可用虚拟IP（High-Availability Virtual IP Address，简称HaVip）是一种可以独立创建和释放的私网IP资源。HaVip可以与高可用软件（例如keepalived）配合使用，搭建高可用主备服务，提高业务的可用性。

功能简介


ECS实例除了可以拥有主私网IP地址外，还可以绑定HaVip，以获得多个私网IP地址。HaVip不仅具备与ECS实例主私网IP地址一样的网络接入能力，还可以与高可用软件（例如keepalived）配合使用，搭建高可用主备服务，提高业务的可用性。HaVip可以通过以下两种方式绑定ECS实例：

- HaVip直接与ECS实例绑定。

一个HaVip支持同时绑定两个不同的ECS实例，绑定成功后，两个ECS实例可以通过地址解析协议ARP（Address Resolution Protocol）宣告同一个HaVip。宣告成功后，一个ECS实例作为主ECS实例，一个ECS实例作为备ECS实例。当主ECS实例出现故障时，备ECS实例可以转换为主ECS实例，继续提供服务。

- 先将ECS实例与辅助弹性网卡绑定，然后将HaVip绑定到辅助弹性网卡。

一个HaVip支持同时绑定两个不同的ECS实例的辅助弹性网卡上，绑定成功后，两个ECS实例可以通过ARP协议宣告同一个HaVip。宣告成功后，一个ECS实例作为主ECS实例，一个ECS实例作为备ECS实例。当主ECS实例出现故障时，备ECS可以转换为主ECS实例，继续提供服务。

 说明 HaVip绑定辅助弹性网卡前，请确保辅助弹性网卡已经绑定到两个不同的ECS实例上。

HaVip具有以下特点：

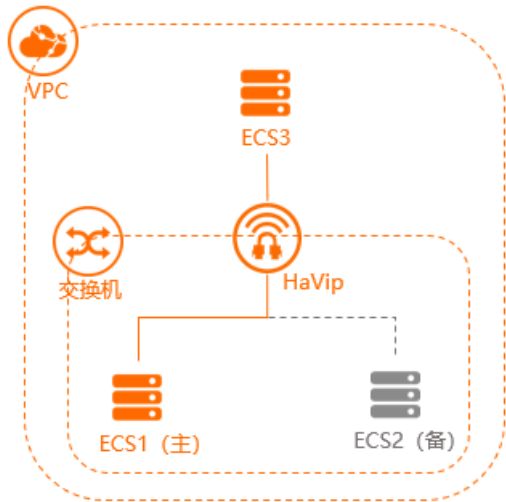
- HaVip是一个浮动的私网IP，不会固定在指定的ECS实例上。ECS实例通过ARP协议宣告可更改与HaVip的绑定关系。
- HaVip具有子网属性，仅支持绑定到同一交换机下的ECS实例或辅助弹性网卡上。
- 一个HaVip支持同时绑定两个ECS实例或同时绑定两个辅助弹性网卡，但一个HaVip不能既绑定ECS实例又绑定辅助弹性网卡。

使用场景

HaVip配置灵活，可满足不同的使用场景。

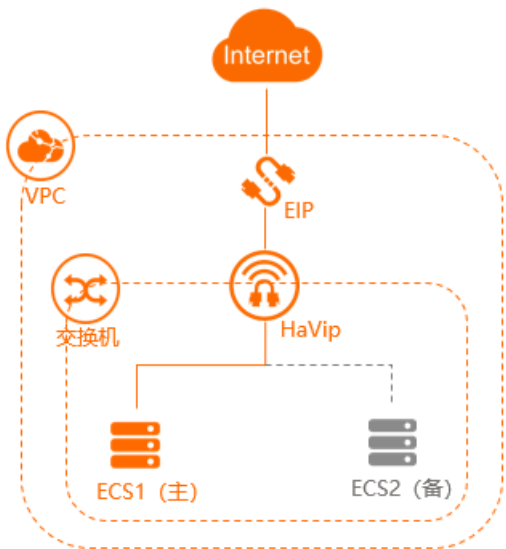
- 场景一：面向私网的高可用服务

如下图所示，两个ECS实例基于HaVip，使用Keepalived组合成一个高可用的私网服务。VPC内的其他实例可以通过私网访问该服务，服务地址为HaVip的地址。当主ECS实例发生故障时，备用ECS实例会自动调用自身的接管程序，接管主ECS实例的服务，实现业务高可用。



● 场景二：面向公网的高可用服务

如下图所示，两个ECS实例基于HaVip，使用Keepalived并且将HaVip与EIP绑定，对外提供高可用的公网服务，服务地址为HaVip绑定的EIP。当主ECS实例发生故障时，备用ECS实例会自动调用自身的接管程序，接管主ECS实例的服务，实现业务高可用。



使用限制

使用HaVip前，请了解以下限制。

资源	默认限制
单个VPC支持创建的HaVip的数量	5个
单个ECS实例支持同时绑定的HaVip数量	5个
单个辅助弹性网卡支持同时绑定的HaVip数量	5个
单个HaVip支持同时绑定的ECS实例数量	2个

资源	默认限制
单个HaVip支持同时绑定的辅助弹性网卡数量	2个
单个VPC内，目的地址指向HaVip的路由条目的数量	5条
HaVip是否支持广播和组播通信	不支持 <div><div>?</div>说明HaVip只支持单播，如果您使用keepalived等第三方软件实现高可用，需要将配置文件中的通信方式修改为单播通信。</div>

6.2. 创建高可用虚拟IP实例

高可用虚拟IP（HaVip）是一种可以独立创建和释放的私网IP资源。本文为您介绍如何在控制台创建高可用虚拟IP。

前提条件

您已经创建了专有网络和交换机。具体操作，请参见[创建专有网络](#)和[创建交换机](#)。

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[高可用虚拟IP](#)。
3. 在顶部菜单栏，选择要创建高可用虚拟IP的地域。
4. 在高可用虚拟IP页面，单击[创建高可用虚拟IP](#)。
5. 在[创建高可用虚拟IP](#)页面，根据以下信息配置高可用虚拟IP，然后单击[提交](#)。

配置	说明
组织	选择高可用虚拟IP所属的组织。
资源集	选择高可用虚拟IP所属的资源集。
地域	选择高可用虚拟IP的地域。
专有网络vpc	选择高可用虚拟IP所属的专有网络。
交换机vswitch	选择高可用虚拟IP所属的交换机。
私网IP地址	指定高可用虚拟IP的私网IP。 <div><div>?</div>说明指定的私网IP必须为所选交换机的网段中未被占用的私网IP。</div>

6.3. 绑定后端云资源

6.3.1. 绑定ECS实例

您可以将高可用虚拟IP（High-Availability Virtual IP Address，简称HaVip）绑定到专有网络类型的ECS实例上，绑定成功后，ECS实例可以通过地址解析协议ARP（Address Resolution Protocol）宣告高可用虚拟IP，以获得多个私网IP。每个高可用虚拟IP最多可以绑定两个ECS实例。

前提条件

您已经创建了ECS实例。具体操作，请参见云服务器ECS用户指南手册中快速入门下的创建实例章节。

背景信息

一个高可用虚拟IP支持同时绑定两个ECS实例或同时绑定两张弹性网卡，但一个高可用虚拟IP不能既绑定ECS实例又绑定弹性网卡。

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[高可用虚拟IP](#)。
3. 在顶部菜单栏处，选择高可用虚拟IP的地域。
4. 在高可用虚拟IP页面，找到目标高可用虚拟IP实例，然后在操作列单击[管理](#)。
5. 在绑定资源区域，找到弹性网卡（主）或弹性网卡（备），然后单击[立即绑定](#)。
6. 在弹出的对话框，根据以下信息选择要绑定资源，然后单击[确定](#)。

配置	说明
绑定类型	选择要绑定高可用虚拟IP的资源类型，支持选择以下两种资源类型： <ul style="list-style-type: none">◦ ECS实例◦ 弹性网卡 本文选择ECS实例。
绑定资源	选择要绑定高可用虚拟IP的ECS实例。 要绑定高可用虚拟IP的ECS实例必须满足以下条件： <ul style="list-style-type: none">◦ ECS实例的网络类型为专有网络类型。◦ ECS实例所属的交换机与高可用虚拟IP所属的交换机相同。

6.3.2. 绑定弹性网卡

您可以将高可用虚拟IP（High-Availability Virtual IP Address，简称HaVip）绑定到弹性网卡上，绑定成功后，ECS实例可以通过地址解析协议ARP（Address Resolution Protocol）宣告高可用虚拟IP，以获得多个私网IP。

前提条件

您已经创建了弹性网卡。具体操作，请参见云服务器ECS用户指南手册中弹性网卡下的创建弹性网卡章节。

背景信息

一个高可用虚拟IP支持同时绑定两个ECS实例或同时绑定两个弹性网卡，但一个高可用虚拟IP不能既绑定ECS

实例又绑定弹性网卡。

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**高可用虚拟IP**。
3. 在顶部菜单栏处，选择高可用虚拟IP的地域。
4. 在高可用虚拟IP页面，找到目标高可用虚拟IP实例，然后在操作列单击**管理**。
5. 在绑定资源区域，找到**弹性网卡（主）**或**弹性网卡（备）**，然后单击**立即绑定**。
6. 在弹出的对话框，根据以下信息选择要绑定的弹性网卡，然后单击**确定**。

配置	说明
绑定类型	选择要绑定高可用虚拟IP的资源类型，支持选择以下两种资源类型： <ul style="list-style-type: none">◦ ECS实例◦ 弹性网卡 本文选择 弹性网卡 。
绑定资源	选择要绑定高可用虚拟IP的弹性网卡。 要绑定高可用虚拟IP的弹性网卡所属的交换机与高可用虚拟IP所属的交换机必须相同。

6.4. 绑定EIP

您可以绑定高可用虚拟IP（HaVip）到弹性公网IP（Elastic IP Address，简称EIP）上，绑定后该高可用虚拟IP可以通过EIP提供公网服务。

前提条件

您已经申请了EIP。具体操作，请参见[弹性公网IP用户指南手册中快速入门下的申请EIP](#)章节。

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**高可用虚拟IP**。
3. 在顶部菜单栏处，选择高可用虚拟IP的地域。
4. 在高可用虚拟IP页面，找到目标高可用虚拟IP实例，然后在操作列单击**绑定弹性公网IP**。
5. 在弹出的对话框，选择需要绑定的EIP，然后单击**确定**。

要绑定的EIP必须满足以下条件：

- EIP的地域必须和高可用虚拟IP的地域相同。
- EIP实例的状态必须处于可用状态。

6.5. 解绑后端云资源

6.5.1. 解绑ECS实例

您可以将高可用虚拟IP（HaVip）从ECS实例上解绑，解绑后，该ECS实例将不能通过地址解析协议ARP（Address Resolution Protocol）宣告解绑的HaVip。

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[高可用虚拟IP](#)。
3. 在顶部菜单栏处，选择HaVip的地域。
4. 在高可用虚拟IP页面，找到目标HaVip，单击操作列下的[管理](#)。
5. 在绑定资源区域，找到目标ECS实例，单击[解除关联](#)。
6. 在弹出的对话框中，单击[确定](#)。

6.5.2. 解绑弹性网卡

您可以将高可用虚拟IP（HaVip）从弹性网卡上解绑，解绑后，绑定弹性网卡的ECS实例将不能通过地址解析协议ARP（Address Resolution Protocol）宣告解绑的HaVip。

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[高可用虚拟IP](#)。
3. 在顶部菜单栏处，选择HaVip的地域。
4. 在高可用虚拟IP页面，找到目标HaVip，单击操作列下的[管理](#)。
5. 在绑定资源区域，找到目标弹性网卡，单击[解除关联](#)。
6. 在弹出的对话框中，单击[确定](#)。

6.6. 解绑EIP

当高可用虚拟IP（HaVip）不需要通过弹性公网IP（Elastic IP Address，简称 EIP）提供公网服务时，您可以解绑高可用虚拟IP与EIP。

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[高可用虚拟IP](#)。
3. 在顶部菜单栏处，选择高可用虚拟IP的地域。
4. 在高可用虚拟IP页面，找到目标高可用虚拟IP，然后在操作列单击[解绑弹性公网IP](#)。
5. 在弹出的对话框，单击[确定](#)。

6.7. 删除高可用虚拟IP

您可以删除不再需要的高可用虚拟IP（HaVip）。

前提条件

- 高可用虚拟IP未绑定弹性公网IP（Elastic IP Address，简称EIP），如果高可用虚拟IP绑定了EIP，请先解绑EIP。具体操作，请参见[解绑EIP](#)。

- 高可用虚拟IP未绑定ECS实例，如果高可用虚拟IP绑定了ECS实例，请先解绑ECS实例。具体操作，请参见[解绑ECS实例](#)。
- 高可用虚拟IP未绑定弹性网卡，如果高可用虚拟IP绑定了弹性网卡，请先解绑弹性网卡。具体操作，请参见[绑定弹性网卡](#)。

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**高可用虚拟IP**。
3. 在顶部菜单栏处，选择高可用虚拟IP的地域。
4. 在**高可用虚拟IP**页面，找到要删除的高可用虚拟IP，然后在**操作**列单击**删除**。
5. 在弹出的对话框，单击**确定**。

7.网络ACL

7.1. 网络ACL概述

网络ACL（Network Access Control List）是专有网络VPC中的网络访问控制功能。您可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中云服务器ECS实例的流量的访问控制。

功能特性

网络ACL具有以下特性：

- 网络ACL规则仅过滤绑定的交换机中的ECS实例的流量（包括SLB实例转发给ECS实例的流量）。
- 网络ACL的规则是无状态的，即设置入方向规则的允许请求后，需要同时设置相应的出方向规则，否则可能会导致请求无法响应。
- 网络ACL无任何规则时，会拒绝所有出入方向的访问。
- 网络ACL与交换机绑定，不过滤同一交换机内的ECS实例间的流量。

规则说明

您可以在网络ACL中添加或删除规则，更改规则后会自动应用到与其绑定的交换机。新创建的网络ACL，默认会在出方向和入方向分别生成一条规则，表示允许所有出、入方向流量。您可以删除默认规则。出方向和入方向默认规则如下所示。

- 入方向规则

生效顺序	协议类型	源地址	源端口范围	策略	类型
1	all	0.0.0.0/0	-1/-1	允许	自定义

- 出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	类型
1	all	0.0.0.0/0	-1/-1	允许	自定义

网络ACL中的元素说明如下：

- 生效顺序：值越小，规则的优先级越高。系统从生效顺序为1的规则开始判断，只要有一条规则与流量匹配，即应用该规则，并忽略其他规则。

例如，ECS实例请求访问目的地址为172.16.0.1的数据包，在经过如下表所示的ACL规则配置后，172.16.0.1匹配生效顺序2和生效顺序3规则中的目的地址，由于生效顺序2的优先级高于生效顺序3，所以会根据生效顺序2规则拒绝该请求。

生效顺序	协议类型	目标地址	目的端口范围	策略	类型
1	all	10.0.0.0/8	-1/-1	允许	自定义
2	all	172.16.0.0/12	-1/-1	拒绝	自定义
3	all	172.16.0.0/12	-1/-1	允许	自定义

- 策略：针对特定流量选择允许或拒绝。
- 协议类型：指定协议的类型，可选择all、icmp、gre、tcp和udp。
- 源地址（限入方向规则）：数据流的源地址。
- 目标地址（限出方向规则）：数据流的目标地址。
- 目的端口范围（限入方向规则）：入方向规则作用的端口范围。
- 目的端口范围（限出方向规则）：出方向规则作用的端口范围。

网络ACL与安全组

与交换机绑定的网络ACL规则控制流入和流出交换机的数据流，与ECS实例相关的安全组规则控制流入和流出ECS实例的数据流。网络ACL和安全组的基本差异如下表所示。

网络ACL	安全组
在交换机级别运行。	在实例级别运行。
无状态：返回数据流必须被规则明确允许。	有状态：返回数据流会被自动允许，不受任何规则的影响。
不评估所有规则，按照规则的生效顺序处理所有规则。	执行规则前，会评估所有规则。
ECS实例所属的交换机仅允许绑定一个网络ACL。	一个ECS实例可加入多个安全组。

网络ACL和安全组提供的安全层如下图所示。

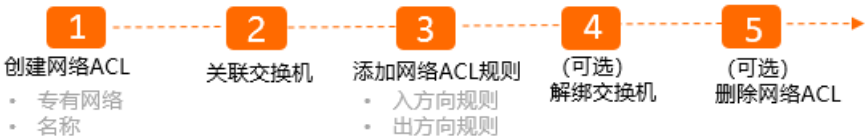
使用限制

网络ACL具有以下限制。

资源	默认限制
单个VPC支持创建的网络ACL数量	200个
单个交换机支持绑定的网络ACL数量	1个
单个网络ACL支持创建的规则数量	<ul style="list-style-type: none">● 入方向规则20条● 出方向规则20条

使用流程

网络ACL的使用流程图如下所示。



7.2. 典型应用

如果您了解ECS实例的常用端口，您可以更准确的添加网络ACL规则。本文为您介绍ECS实例常用端口及常用端口的典型应用。

常用端口列表


常用端口及服务如下表所示。

端口	服务	说明
21	FTP	FTP服务所开放的端口，用于上传、下载文件。
22	SSH	SSH端口，用于通过命令行模式使用用户名密码验证连接Linux实例。
23	Telnet	Telnet端口，用于Telnet远程登录ECS实例。
25	SMTP	SMTP服务所开放的端口，用于发送邮件。
80	HTTP	用于HTTP服务提供访问功能，例如，IIS、Apache、Nginx等服务。
110	POP3	用于POP3协议，POP3是电子邮件收发的协议。
143	IMAP	用于IMAP（Internet Message Access Protocol）协议，IMAP是用于接收电子邮件的协议。
443	HTTPS	用于HTTPS服务提供访问功能。HTTPS是一种能提供加密和通过安全端口传输的一种协议。
1433	SQL Server	SQL Server的TCP端口，用于供SQL Server对外提供服务。
1434	SQL Server	SQL Server的UDP端口，用于返回SQL Server使用了哪个TCP/IP端口。
1521	Oracle	Oracle通信端口，ECS实例上部署了Oracle SQL需要放行的端口。
3306	MySQL	MySQL数据库对外提供服务的端口。
3389	Windows Server Remote Desktop Services	Windows Server Remote Desktop Services（远程桌面服务）端口，可以通过这个端口使用软件连接Windows实例。
8080	代理端口	同80端口，8080端口常用于WWW代理服务，实现网页浏览。

自定义网络ACL

和显示了一个仅支持IPv4的VPC的网络ACL示例。其中：

- 生效顺序1、2、3、4的入方向规则分别为允许HTTP、HTTPS、SSH、RDP数据流进入交换机的规则，出方向响应规则为生效顺序3的出方向规则。
- 生效顺序1、2的出方向规则分别为允许HTTP和HTTPS流量离开交换机的规则，入方向响应规则为生效顺序5的入方向规则。
- 生效顺序6的入方向规则为拒绝所有入方向IPv4流量，该规则会确保在数据包不匹配任何其他规则时拒绝此数据包。
- 生效顺序4的出方向规则为拒绝所有出方向IPv4流量，该规则会确保在数据包不匹配任何其他规则时拒绝此数据包。

 **说明** 无论是入方向规则还是出方向规则，请确保每一条规则都存在允许响应流量的相应入方向或出方向规则。

入方向规则

生效顺序	协议类型	源地址	目的端口范围	策略	说明
1	tcp	0.0.0.0/0	80/80	允许	允许来自任意IPv4地址的入方向HTTP流量。
2	tcp	0.0.0.0/0	443/443	允许	允许来自任意IPv4地址的入方向HTTPS流量。
3	tcp	0.0.0.0/0	22/22	允许	允许来自任意IPv4地址的入方向SSH流量。
4	tcp	0.0.0.0/0	3389/3389	允许	允许来自任意IPv4地址的入方向RDP流量。
5	tcp	0.0.0.0/0	32768/65535	允许	允许来自互联网的入方向返回IPv4流量。 此端口范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见 临时端口 。
6	all	0.0.0.0/0	-1/-1	拒绝	拒绝所有入方向IPv4流量。

出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	说明
1	tcp	0.0.0.0/0	80/80	允许	允许出方向IPv4 HTTP流量从交换机流向互联网。
2	tcp	0.0.0.0/0	443/443	允许	允许出方向IPv4 HTTPS流量从交换机流向互联网。
3	tcp	0.0.0.0/0	32768/65535	允许	允许对互联网客户端的出站IPv4响应。 此端口范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见 临时端口 。
4	all	0.0.0.0/0	-1/-1	拒绝	拒绝所有出方向IPv4流量。

负载均衡的网络ACL

绑定网络ACL的交换机中的ECS作为负载均衡SLB的后端服务器时，您需要添加如下网络ACL规则。

- 入方向规则

生效顺序	协议类型	源地址	目的端口范围	策略	说明
1	SLB监听协议	允许接入SLB的客户端IP	SLB监听端口	允许	在SLB监听端口上允许来自指定客户端IP的入方向流量。
2	健康检查协议	100.64.0.0/10	健康检查端口	允许	在健康检查端口上允许来自健康检查地址的入方向流量。

- 出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	说明
1	all	允许接入SLB的客户端IP	-1/-1	允许	允许所有流向指定客户端IP的出方向流量。
2	all	100.64.0.0/10	-1/-1	允许	允许所有流向健康检查地址的出方向流量。

临时端口

不同类型的客户端发起请求时使用的端口不同，您需要根据自己使用的或作为通信目标的客户端的类型为网络ACL使用不同的端口范围。常用客户端的临时端口范围如下。

客户端	端口范围
Linux	32768/61000
Windows Server 2003	1025/5000
Windows Server 2008及更高版本	49152/65535
NAT网关	1024/65535

7.3. 创建网络ACL

网络ACL是专有网络VPC中的网络访问控制功能。您可以在专有网络VPC中创建网络ACL。

前提条件

您已经创建了专有网络。具体操作，请参见[创建专有网络](#)。

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[网络ACL](#)。
3. 在顶部菜单栏处，选择要创建网络ACL的地域。
4. 在[网络ACL](#)页面，单击[创建网络ACL](#)。

5. 在创建网络ACL页面，根据以下信息配置网络ACL，然后单击提交。

配置	说明
组织	选择网络ACL所属的组织。
资源集	选择网络ACL所属的资源集。
地域	选择网络ACL所属的地域。
名称	网络ACL的名称。
描述	网络ACL的描述。
专有网络VPC	<div>选择网络ACL所属的专有网络。<div><div>?</div>说明 要关联的专有网络的地域必须与网络ACL的地域相同。</div></div>

7.4. 绑定交换机

创建网络ACL后，您可以将网络ACL与交换机绑定，实现对交换机中ECS实例流量的访问控制。

前提条件

将网络ACL绑定到交换机前，请确保满足以下条件：

- 您已经创建了网络ACL。具体操作，请参见[创建网络ACL](#)。
- 您已经创建了交换机，且交换机所属的VPC与要绑定的网络ACL所属的VPC相同。具体操作，请参见[创建交换机](#)。

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[网络ACL](#)。
3. 在顶部菜单栏，选择网络ACL的地域。
4. 在[网络ACL](#)页面，找到目标网络ACL，然后在操作列单击[管理](#)。
5. 在已绑定资源页签，单击[关联资源](#)。
6. 在关联资源对话框，选择需要绑定的交换机，然后单击[确定](#)。

?

说明 网络ACL仅允许绑定所属VPC内的交换机，且每个交换机仅允许绑定一个网络ACL。

7.5. 添加网络ACL规则

7.5.1. 添加入方向规则

创建网络ACL后，您可以为网络ACL添加入方向规则，管控公网或私网对交换机中ECS实例的访问。

前提条件

您已经创建了网络ACL。具体操作，请参见[创建网络ACL](#)。

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**网络ACL**。
- 3. 在顶部菜单栏处，选择网络ACL的地域。
- 4. 在**网络ACL**页面，找到目标网络ACL，然后在操作列单击**设置入方向规则**。
- 5. 在**入方向规则**页签，单击**创建入方向规则**。
- 6. 在**创建入方向规则**对话框，根据以下信息配置入方向规则，然后单击**确定**。

配置	说明
名称	入方向规则的名称。 长度为2~128个字符，必须以字母或中文开头，可包含数字、下划线（_）和短划线（-）
生效顺序	输入入方向规则的生效顺序，数字越小优先级越高。
策略	选择入方向规则的授权策略： <ul style="list-style-type: none">◦ 允许：允许访问交换机中ECS实例。◦ 拒绝：拒绝访问交换机中ECS实例。
协议类型	选择协议，支持选择以下类型的协议： <ul style="list-style-type: none">◦ all：所有协议。◦ icmp：网络控制报文协议。◦ gre：通用路由封装协议。◦ tcp：传输控制协议。◦ udp：用户数据报协议。
源地址	数据流的源地址网段。 默认为0.0.0.0/32。
目的端口范围	输入目的端口范围。 端口范围为1~65535，使用斜线（/）隔开起始端口和终止端口，格式为1/200、80/80，其中-1/-1不能单独设置，代表不限制端口。 <div> 说明 只有当协议类型为tcp或udp时，才可以输入端口范围。选择其他协议类型时，不能输入端口范围。</div>

7.5.2. 添加出方向规则

创建网络ACL后，您可以为网络ACL添加出方向规则，管控交换机中的ECS实例对公网或私网的访问。

前提条件

您已经创建了网络ACL。具体操作，请参见[创建网络ACL](#)。

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**网络ACL**。
- 3. 在顶部菜单栏处，选择网络ACL的地域。
- 4. 在**网络ACL**页面，找到目标网络ACL，然后在操作列单击**设置出方向规则**。
- 5. 在**出方向规则**页签，单击**创建出方向规则**。
- 6. 在**创建出方向规则**对话框，根据以下信息配置出方向规则，然后单击**确定**。


配置	说明
名称	出方向规则的名称。 名称长度为2~128个字符，必须以字母或中文开头，可包含数字、下划线（_）和短划线（-）。
生效顺序	输入出方向规则的生效顺序，数字越小优先级越高。
策略	选择出方向规则的授权策略： <ul style="list-style-type: none">允许：允许交换机中的ECS实例访问公网或私网。拒绝：拒绝交换机中的ECS实例访问公网或私网。
协议类型	选择协议，支持选择以下类型的协议： <ul style="list-style-type: none">all：所有协议。icmp：网络控制报文协议。gre：通用路由封装协议。tcp：传输控制协议。udp：用户数据报协议。
目标地址	数据流的目标地址网段。 默认为0.0.0.0/32。
目的端口范围	输入目的端口范围。 端口范围为1~65535，使用斜线（/）隔开起始端口和终止端口，格式为1/200、80/80，其中-1/-1不能单独设置，代表不限制端口。 <div><p> 说明 只有当协议类型为tcp或udp时，才可以输入端口范围。选择其他协议类型时，不能输入端口范围。</p></div>

7.5.3. 调整规则顺序

网络ACL按照规则生效顺序执行规则，生效顺序的值越小，优先级越高。您可以为规则排序来指定规则执行的先后顺序。


调整入方向规则顺序

1. [登录专有网络管理控制台](#)。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，然后在操作列单击**管理**。
5. 单击**入方向规则**页签，然后单击**排序**。
6. 在**排序**对话框，上下拖动规则，然后单击**确定**。

 **说明** 规则顺序越上，优先级越高。

调整出方向规则顺序

1. [登录专有网络管理控制台](#)。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，然后在操作列单击**管理**。
5. 单击**出方向规则**页签，然后单击**排序**。
6. 在**排序**对话框，上下拖动规则，然后单击**确定**。

 **说明** 规则顺序越上，优先级越高。

7.6. 解绑交换机

您可以解除网络ACL与交换机的绑定关系，解除后，网络ACL不再管控交换机中的ECS实例的流量。

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**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，在操作列单击**管理**。
5. 在**已绑定资源**页签，找到需要解绑网络ACL的交换机，在操作列单击**解绑**。
6. 在弹出的对话框，单击**确定**。

7.7. 删除网络ACL

您可以删除一个不需要的网络ACL。

前提条件

确保要删除的网络ACL未绑定任何交换机，如有绑定，请先解除与交换机的绑定。具体操作，请参见[解绑交换机](#)。

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**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击操作列下的**删除**。
5. 在**删除网络ACL**对话框中，单击**确定**。