

专有网络 VPC

用户指南

用户指南

概述

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彻底逻辑隔离。您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、负载均衡、RDS等。

创建专有网络

您可以通过专有网络管理控制台创建专有网络。具体操作步骤可参考快速入门中的 [创建专有网络](#)。

查看专有网络信息

您可以通过控制台查看所部署的专有网络的基本信息，及资源部署相关信息。

操作步骤

登录阿里云 [专有网络管理控制台](#)。

在左侧导航选择 **专有网络**，打开 **专有网络列表** 页面。

单击专有网络实例右侧的 **管理**，打开 **专有网路基本信息** 页面。您可在此页面上查看该专有网络的详细信息。

修改专有网络信息

您可以在管理控制台中修改专有网络的名称和描述信息，方便管理专有网络列表。

操作步骤

登录阿里云 [专有网络管理控制台](#)。

在左侧导航选择 **专有网络**，打开 **专有网络列表** 页面。

单击专有网络实例右侧的 **编辑**，弹出 **编辑专有网络** 对话框。

根据您的需求，对专有网络进行重命名，并可以增加描述信息进行说明，然后单击 **提交**。

删除专有网络

如果您不再需要某专有网络，可以通过控制台删除该专有网络。

前提条件

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

操作步骤

登录阿里云 **专有网络管理控制台**。

选择左侧导航的 **专有网络**，打开 **专有网络列表** 页面。

选择您要删除的专有网络所在的地域。

单击需要删除的专有网络右侧的 **删除**。

在弹出的删除确认对话框内单击 **确定**，完成专有网络的删除。

查看默认专有网络

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

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

删除默认专有网络

您可以删除默认类型的专有网络，当您删除某地域的默认专有网络后，如果再次需要在该地域使用默认类型的专有网络时，阿里云会为您再次创建。

API

专有网络相关接口：

- 新建专有网络

- 删除专有网络
- 查询专有网络列表
- 修改专有网络属性

概述

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

创建交换机

您可在专有网络管理控制台中创建交换机。具体操作请参考快速入门中的 [创建交换机](#)。

修改交换机信息

您可以在控制台修改交换机的名称及描述信息，方便交换机的管理。

操作步骤

登录 [专有网络管理控制台](#)。

在左侧导航选择 **专有网络**，打开 **专有网络列表** 页面。

选择相应地域下某一 VPC 实例，单击右侧的 **管理**，进入 **专有网络基本信息** 页面。

在左侧导航选择 **交换机**，进入 **交换机列表** 页面。

单击需要编辑的交换机右侧的 **编辑**，弹出 **编辑交换机** 对话框。

按照您的需要修改交换机名称及描述信息，单击 **提交**。

删除交换机

前提条件

删除交换机之前，必须先删除目标交换机所连接的云产品实例。

操作步骤

登录 专有网络管理控制台。

在左侧导航选择 **专有网络**，打开 **专有网络列表** 页面。

选择相应地域下某一 VPC 实例，单击右侧的 **管理**，进入 **专有网络基本信息** 页面。

在左侧导航选择 **交换机**，进入 **交换机列表** 页面。

单击需要删除的交换机右侧的 **删除**，弹出 **删除交换机** 确认对话框。

单击 **确定**，删除该交换机。

查看默认交换机

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

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

删除默认交换机

您可以删除默认交换机。当您删除某可用区的默认交换机后，如果再次需要在该可用区使用默认类型的交换机时，阿里云会为您再次创建。

API

- 新建交换机
- 删除交换机
- 查询交换机列表
- 修改交换机属性

概述

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

查看路由信息

您可以在管理控制台中查看专有网络的路由信息。

操作步骤

登录 专有网络管理控制台。

选择地域，列出该地域下的专有网络。

单击专有网络 **操作** 列中的 **管理**。

在左侧导航栏内单击 **路由器**，打开“虚拟路由器列表”页面。在此页面上，您可以查看到路由器基本信息和路由条目列表。您可以通过路由条目列表查看已有路由条目，包括系统路由（类型为 **系统**）和自定义路由（类型为 **自定义**）。

创建自定义路由条目

登录 专有网络管理控制台。

选择地域，列出该地域下的专有网络。

单击专有网络 **操作** 列中的 **管理**。

在左侧导航栏内单击 **路由器**，打开“虚拟路由器列表”页面。

单击右上角的 **添加路由**，弹出“添加路由”对话框。

根据您的需求，填写路由条目参数值，然后点击 **确定**，完成自定义路由条目的添加。

删除自定义路由条目

您可以删除自定义类型的路由表。

登录 专有网络管理控制台。

选择地域，列出该地域下的专有网络。

单击专有网络 **操作** 列中的 **管理**。

在左侧导航栏内单击 **路由器**，打开“虚拟路由器列表”页面。

在 **路由条目列表** 区域，单击需要删除的路由条目的 **操作** 列下的 **删除**。

在删除操作确认对话框内单击 **确定**，完成自定义路由条目的删除操作。

编辑路由器名称和描述信息

登录 专有网络管理控制台。

选择地域，列出该地域下的专有网络。

单击专有网络 **操作** 列中的 **管理**。

在左侧导航栏内单击 **路由器**，打开“虚拟路由器列表”页面。

在 **路由器基本信息** 区域内，单击右侧的 **编辑**，弹出“编辑路由器”对话框。

编辑路由器名称及相关描述信息，然后单击 **确定**。

API

路由器相关接口：

- 查询路由器列表
- 修改路由器属性

路由表相关接口：

- 新建自定义路由
- 删除自定义路由
- 查询路由表列表

专有网络中的实例管理

概述

您可在专有网络管理控制台上创建专有网络中的云产品实例。

前提条件

您已在专有网络中创建了交换机。在专有网络内创建云产品实例的时候，必须指定云产品实例所在的交换机。

操作步骤

登录阿里云 专有网络管理控制台。

在左侧导航选择 **专有网络**，进入“专有网络列表”页面。

选择地域，然后单击需要创建实例的专有网络右侧的 **管理**，进入“专有网络基本信息”页面。

在左侧导航选择 **交换机**，打开“交换机列表”页面。

单击交换机的 **操作** 列下的 **创建实例**，然后在弹出的下拉菜单中按照您的需求选择要创建的实例类型。

交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	描述	操作
vsw-25g6t73n1-vsw-1	1	192.168.1.0/24	可用	cn-hangzhou-d	248	2015-07-28 22:47:58	hangzhou DMZ	编辑 删除 创建实例
共有1条。每页显示：10条								

在实例购买页面选择实例的配置，完成购买流程后，实例即成功创建在所选交换机下。

应用场景

- 专有网络下每个交换机都是独立的一个网段，所以更换交换机后，ECS 的 IP 也随之发生变更。
- 专有网络内的服务器需要更换私网 IP 地址。

操作步骤

登录 云服务器管理控制台。

在左导航栏内单击 **实例**，打开实例列表，然后选择地域。

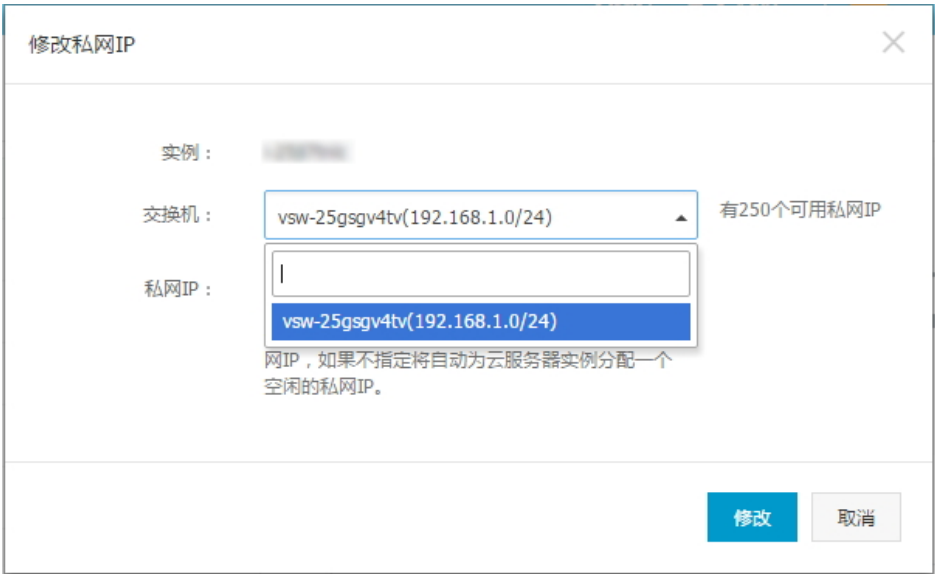
在目标实例的 **操作** 列中，单击 **更多 > 停止**。停止实例运行。

单击 **管理**，进入基本信息页面。

在 **配置信息** 区域，点击右侧的 **更多 > 修改私网 IP**。



在弹出的 “修改私网IP” 的配置页面里选择要接入的交换机，根据需要修改私网IP地址，然后单击 **修改**。



返回到实例列表页面，在 **操作** 列中单击 **启动**，ECS 启动后新的私网 IP 就生效了。

应用场景

在专有网络里有两个交换机，分别为网段 1 和网段 2。RDS 挂载在网段 1，现在想把 RDS 连接到网段 2 的交换机上。

前提条件

- 您已了解以下说明信息：
 - 切换 IP 会导致 RDS 的闪断。
 - RDS 白名单需要添加新的 IP 地址。
- 您已设置好连接 RDS 程序的自动重连机制。

操作步骤

登录 RDS 管理控制台。

在左侧导航选择 **实例列表**，进入“云数据库管理”页面。



选择相应的实例，点击右侧的 **管理** 链接，进入“基本信息”页面。

在左侧导航选择 **数据库连接**，进入相应的页面。

点击 **切换为经典网络**，并点击 **确定**。



点击 **切换为专有网络**，弹出“切换为专有网络”对话框。



在虚拟交换机下拉列表中，选择要切换去的目标网段交换机，点击 **确定**。



安全访问控制

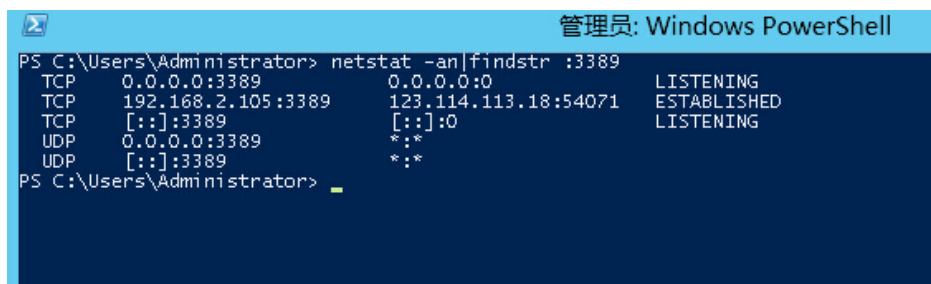
专有网络支持各个云产品实例的访问控制机制：

- ECS 通过 安全组 实现访问控制。
- RDS 通过 白名单 实现访问控制。
- SLB 通过 白名单 实现访问控制。

应用场景

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

下图示例的情况为，在没有限制的情况下，通过 `netstat -an|findstr :3389` 可以查看到 123.114.113.18 的客户端已经通过 IP 连接上了 VPC 的服务器。下文以限制服务器 3389 远程端口为例，讲解如何通过设置安全组，实现对专有网络中的 ECS 的访问控制。



```
管理员: Windows PowerShell
PS C:\Users\Administrator> netstat -an|findstr :3389
TCP    0.0.0.0:3389          0.0.0.0:0             LISTENING
TCP    192.168.2.105:3389    123.114.113.18:54071    ESTABLISHED
TCP    [::]:3389            [::]:0                 LISTENING
UDP    0.0.0.0:3389         *:                      *:*
UDP    [::]:3389            *:                      *:*
PS C:\Users\Administrator>
```

操作步骤

登录 云服务器管理控制台。

选择地域。

在目标实例的 **操作** 列下，单击 **更多 > 安全组配置**，打开该实例的安全组列表。

单击安全组 **操作** 列下的 **配置规则**，打开安全组规则配置页面。

单击页面右上角的 **添加安全组规则**，为这台实例的安全组规则中添加一条下图示例的规则，然后单击 **确定**。

协议类型选择定义的规则

添加安全组规则

网卡类型:

内网

规则方向:

入方向

授权策略:

拒绝

协议类型:

RDP (3389)

Linux选择SSH (22)

* 端口范围:

3389/3389

取值范围从1到65535; 设置格式例如"1/200"、"80/80", 其中"-1/-1"不能单独设置, 代表不限制端口。[教我设置](#)

授权类型:

地址段访问

* 授权对象:

123.114.113.18/32

请根据实际场景设置授权对象的CIDR, 另外, 0.0.0.0/0代表允许或拒绝所有IP的访问。设置时请务必谨慎。[教我设置](#)

优先级:

1

优先级可选范围为1-100, 默认值为1, 即最高优先级。

确定

取消

协议类型选择自定义规则

添加安全组规则

网卡类型：

内网

规则方向：

入方向

授权策略：

拒绝

协议类型：

自定义 TCP

* 端口范围：

3389/3389

Linux 设置为 22/22 或则 SSH 自定义端口

取值范围从 1 到 65535；设置格式例如 "1/200"、"80/80"，其中 "-1/-1" 不能单独设置，代表不限制端口。[教我设置](#)

授权类型：

地址段访问

* 授权对象：

123.114.113.18/32

请根据实际场景设置授权对象的 CIDR，另外，0.0.0.0/0 代表允许或拒绝所有 IP 的访问。设置时请务必谨慎。[教我设置](#)

优先级：

1

优先级可选范围为 1-100，默认值为 1，即最高优先级。

确定

取消

应用场景

通过配置安全组规则，使得同一专有网络下的三个交换机两两不能访问。

前提条件

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

操作步骤

创建三个安全组，为了方便分辨，可以用网段命名，选择所属专有网络。创建安全组的具体操作可参考 [创建安全组](#)。

13

云服务器 ECS

安全组列表

亚太 (新加坡) 华南 1 (深圳) 华北 1 (青岛) 华北 2 (北京) 华东 2 (上海) 华东 3 (香港) 华东 1 (杭州) 美国 (硅谷)

刷新 创建安全组

安全组ID

请输入专有网络ID进行查询

搜索

安全组ID/名称	所属专有网络	相关实例	网络类型	创建时间	描述	标签	操作
sg-258y5oy3	vpc-258y5oy3	0	专有网络	2016-03-29 15:47:39	System created s...		修改 管理实例 配置规则
sg-258y5oy3	vpc-258y5oy3	1	经典网络	2016-03-15 21:17:27	-	ros-aliyun-creat...	修改 管理实例 配置规则
sg-258y5oy3	vpc-258y5oy3	2	经典网络	2016-03-15 19:33:46	-		修改 管理实例 配置规则
sg-258y5oy3	vpc-258y5oy3	1	经典网络	2016-03-15 19:04:58	-		修改 管理实例 配置规则
sg-258y5oy3	vpc-258y5oy3	0	经典网络	2016-03-15 19:02:46	-		修改 管理实例 配置规则

创建安全组

* 安全组名称 :

s172.16.1.0

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

描述 :

172.16.1.0/16

长度为2-256个字符，不能以http://或https://开头。

网络类型 :

专有网络

* 专有网络 :

请选择专有网络

确定 取消

在“安全组列表”页面，单击某一实例的 **配置规则** 链接，进入“安全组规则”页面。

先添加一个允许 0.0.0.0 网段访问的规则，优先级可以设置 100，优先级数字越小，优先级越高。

添加安全组规则 ✕

网卡类型：

内网 ▼

规则方向：

入方向 ▼

授权策略：

允许 ▼

协议类型：

全部 ▼

* 端口范围：

-1/-1

取值范围为1~65535；例如“1/200”、“80/80”。

授权类型：

地址段访问 ▼

授权对象：

0.0.0.0/0

优先级：

100

优先级可选范围为1-100，默认值为1，即最高优先级。

确定

取消

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

添加安全组规则 ✕

网卡类型：

内网 ▼

规则方向：

入方向 ▼

授权策略：

拒绝 ▼

协议类型：

全部 ▼

* 端口范围：

-1/-1

取值范围为1~65535；例如“1/200”、“80/80”。

授权类型：

地址段访问 ▼

授权对象：

172.16.2.0/16

优先级：

90

优先级可选范围为1-100，默认值为1，即最高优先级。

确定

取消

再添加第三条规则，拒绝 172.16.3.0/16 网段。

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

想要设置两两网段不能互相访问，需要再在另外两个安全组里填写如上规则。

专有网络涉及的监控项为弹性公网 IP 的流量，流量监控的具体指标可以参考云监控中 EIP 的监控信息。具体内容请参见 弹性公网 IP 监控。