ALIBABA CLOUD

Alibaba Cloud

NAT网关

最佳实践

文档版本：20220526

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.通过VPC NAT网关实现使用云上固定私网地址与本地IDC互访

本文指导您通过VPC NAT网关的SNAT和DNAT功能实现云上固定私网地址与本地数据中心IDC（Internet Data Center）互访。

场景示例

本文以下图场景为例。某企业在阿里云华北2（北京）地域已经部署了一个专有网络VPC（Virtual Private Cloud）和交换机，交换机中创建了多台ECS实例。该企业云下总部已通过物理专线和边界路由器VBR（Virtual Border Router）接入阿里云。云上的VPC与总部已经通过云企业网CEN（Cloud Enterprise Network）互通。然而，企业要求VPC与总部互访时的私网IP地址固定。

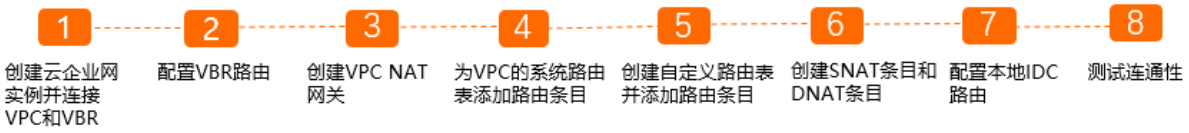
您可以通过VPC NAT网关的SNAT功能和DNAT功能，实现VPC内ECS实例使用固定私网IP地址与总部IDC互访。本文示例中的网段规划如下表所示。您也可以自行规划网段，请确保您的网段之间没有重叠。

配置项	地址段
云上VPC1网段	192.168.0.0/16
云上交换机网段	• VSW1：192.168.10.0/24 • VSW2：192.168.20.0/24 • NATVSW：192.168.3.0/24
云上ECS实例的IP地址	• ECS1：192.168.10.55 • ECS2：192.168.20.30
本地IDC网段	172.16.0.0/12
本地IDC中服务器的IP地址	172.16.10.137
互联IP	• 云端VBR地址：10.0.0.2/30 • 本地IDC端：10.0.0.1/30

前提条件

- 您已经注册了阿里云账号。具体操作，请参见账号注册。
- 您已经在华北2（北京）地域创建了名称为VPC1的专有网络，并在VPC1创建了名称为VSW1和VSW2的交换机。VSW1位于可用区H，VSW2位于可用区G。具体操作，请参见创建和管理专有网络。
- 您已经在VPC1中创建了名称为NATVSW的中转交换机，位于可用区H。
- 您在VSW1和VSW2中分别创建名称为ECS1和ECS2的ECS实例并部署了应用服务。具体操作，请参见使用向导创建实例。
- 您已经创建了物理专线和边界路由器VBR（Virtual Private Cloud）。具体操作，请参见创建独享专线连接和创建边界路由器。

配置步骤



步骤一：创建云企业网实例并连接VPC和VBR

在您连接网络实例前，您需要先创建一个云企业网实例。云企业网实例是创建和管理一体化网络的基础资源，一个云企业网实例创建和管理一张网络。

1. 登录云企业网管理控制台。
2. 执行以下操作，创建云企业网实例。
   i. 在**云企业网实例**页面，单击**创建云企业网实例**。
   ii. 在**创建云企业网实例**对话框，配置以下参数信息，然后单击**确认**。

参数	说明
名称	云企业网实例的名称。 名称在2~128个字符之间，以大小写字母或中文开头，可包含数字、短划线（-）或下划线（_）。
描述	云企业网实例的描述。 描述可以为空或可以填写2~256个中英文字符，不能以 `http://` 和 `https://` 开头。

3. 执行以下步骤，创建VPC连接。
   i. 在**云企业网实例**页面，单击已创建的云企业网实例ID。
   ii. 在云企业网实例详情页面，单击**VPC**下侧的⊕图标。

iii. 在**连接网络实例**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
实例类型	系统默认选择**专有网络（VPC）**。
地域	选择要连接的网络实例所在的地域。本文选择**华北2（北京）**。
转发路由器	系统自动为您在该地域创建转发路由器。本文创建的为企业版转发路由器。关于转发路由器的更多信息，请参见转发路由器工作原理。
设定转发路由器的主/备可用区	选择转发路由器的主备可用区。 **说明** 在执行此操作时，系统会自动为您创建一个服务关联角色，角色名称为AliyunServiceRoleForCEN。该角色将会允许转发路由器在目标VPC实例的交换机上创建ENI，作为VPC发往转发路由器的流量入口。更多信息，请参见AliyunServiceRoleForCEN。 本文**主可用区**选择**北京 可用区H**，**备可用区**选择**北京 可用区G**。
资源归属UID	选择要连接的网络实例所归属的账号类型。本文使用默认值**同账号**。
付费方式	本文使用默认值**按量付费**。
连接名称	输入连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
网络实例	选择要连接的VPC网络实例ID。本文选择VPC1。
交换机	分别从主备可用区中选择交换机。本文主可用区选择VSW1，备可用区选择VSW2。
高级配置	系统默认选中高级功能。本文使用默认配置。

4. 执行以下步骤，创建VBR连接。

i. 创建VPC连接后，单击**继续创建连接**。

ii. 在**连接网络实例**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
实例类型	选择**边界路由器（VBR）**。
地域	选择要连接的网络实例所在的地域。本文选择**华北2（北京）**。
转发路由器	系统自动选择当前地域已创建的转发路由器。此处选择北京的转发路由器。
资源归属UID	选择要连接的网络实例所归属的账号类型。本文使用默认值**同账号**。
连接名称	输入连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
网络实例	选择要连接的VBR网络实例ID。本文选择已创建的VBR实例。
高级配置	系统默认选中高级功能。本文使用默认配置。

步骤二：配置VBR路由

在VBR上配置指向本地IDC的路由。

1. 登录高速通道管理控制台。
2. 在顶部菜单栏，选择目标地域，然后在左侧导航栏，单击**边界路由器（VBR）**。
3. 在**边界路由器（VBR）**页面，单击目标VBR实例ID。
4. 在边界路由器详情页面，单击**路由条目**页签，然后单击**添加路由条目**。
5. 在**添加路由条目**面板，配置以下参数信息，然后单击**确定**。

参数	说明
下一跳类型	选择路由条目的下一跳类型。本文选择**物理专线接口**。
目标网段	本文输入本地IDC中服务器的IP地址：*172.16.10.137*。
下一跳	选择物理专线接口。

步骤三：创建VPC NAT网关

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在**VPC NAT网关**页面，单击**创建VPC NAT网关**。
4. 在**VPC NAT网关（按量付费）**页面，配置以下参数信息，然后单击**立即购买**。

参数	说明
地域	选择需要创建VPC NAT网关实例的地域。本文选择**华北2（北京）**。

参数	说明
VPC ID	选择VPC NAT网关实例所属的VPC。创建VPC NAT网关实例后，不能修改其所属的VPC。本文选择VPC1。
可用区	选择VPC NAT网关实例所属的可用区。本文选择NATVSW的可用区，即**可用区H**。
交换机ID	选择VPC NAT网关实例所属的交换机。本文选择NATVSW。
实例名称	设置VPC NAT网关实例的名称。 名称长度为1~128个字符。本文设置为*VPC_NATGW*。
服务关联角色	显示是否已有VPC NAT网关的服务关联角色。 首次使用NAT网关（包含公网NAT网关和VPC NAT网关），需要单击**创建服务关联角色**完成创建。

5. 在**确认订单**页面，确认参数的配置信息并选中服务协议，然后单击**立即开通**。
   当出现**恭喜，开通成功！**的提示后，说明您创建成功。

步骤四：为VPC1的系统路由表添加路由条目

为VPC1的系统路由表添加指向VPC NAT网关的路由条目。

1. 登录专有网络管理控制台。
2. 在**专有网络**，找到VPC1，然后单击VPC的ID。
3. 在VPC详情页面，单击**资源管理**页签，单击**路由表**下方的链接。
4. 在**路由表**页面，找到**路由表类型**为**系统**的路由表，单击其ID。
5. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。
6. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。本文输入*VPCENTRY*。
目标网段	输入要转发到的目标网段。本文输入本地IDC中服务器的IP地址：*172.16.10.137*。
下一跳类型	选择下一跳的类型。本文选择**NAT网关**。
NAT网关	选择具体的NAT网关实例。本文选择VPC NAT网关。

步骤五：创建自定义路由表并添加路由条目

为NATVSW交换机创建自定义路由表并添加指向转发路由器的路由条目。

关于支持创建自定义路由表的地域信息，请参见自定义路由表发布及地域支持情况。

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. 执行以下步骤，创建自定义路由表并绑定交换机。

i. 在**路由表**页面，单击**创建路由表**。

ii. 在**创建路由表**页面，配置以下参数信息，然后单击**确定**。

参数	说明
资源组	选择路由表所属的资源组。本文选择**全部**。
专有网络	选择路由表所属的VPC。本文选择VPC1。
名称	输入路由表的名称。本文输入*NATVTB*。
描述	输入路由表的描述。本文输入*VPCNAT的自定义路由表。*。

iii. 单击**已绑定交换机**页签，然后单击**绑定交换机**。

iv. 在**绑定交换机**对话框，选择要绑定的交换机，然后单击**确定**。

本文选择NATVSW交换机。

5. 执行以下步骤，为自定义路由表添加路由条目。

i. 在**路由表**，找到已创建的自定义路由表，单击路由表的ID。

ii. 选择**路由条目列表 > 自定义**页签，单击**添加自定义路由条目**。

iii. 在**添加路由条目**面板，配置以下参数信息，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。本文输入*VPCNATENTRY*。
目标网段	输入要转发到的目标网段。本文输入本地IDC中服务器的IP地址：*172.16.10.137*。
下一跳类型	选择下一跳的类型。本文选择**转发路由器**。
转发路由器	选择具体的转发路由器实例。本文选择VPC1连接的转发路由器。

步骤六：使用默认NAT IP创建SNAT条目和DNAT条目

创建SNAT条目，使得云上ECS实例可以访问本地IDC。创建DNAT条目，使得云上ECS实例可以被本地IDC访问。

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在顶部菜单栏，选择公网NAT网关的地域。
4. 执行以下步骤，创建SNAT条目。

i. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**SNAT管理**。

ii. 在**SNAT管理**页签，单击**创建SNAT条目**。

iii. 在**创建SNAT条目**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
SNAT条目粒度	选择SNAT条目的粒度。本文选择**交换机粒度**，然后在**选择交换机**列表中选择云上ECS实例所在交换机。本文选择VSW1。**交换机网段**处会显示VSW1的网段。
选择NAT IP地址	在下拉列表中选择用来访问外部私有网络的NAT IP地址。本文选择默认NAT IP地址。
条目名称	SNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

5. 返回**VPC NAT网关**页面，然后执行以下操作，创建DNAT条目。
   i. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**DNAT管理**。
   ii. 在**DNAT管理**页签，单击**创建DNAT条目**。
   iii. 在**创建DNAT条目**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
选择NAT IP地址	选择供外部私有网络访问的NAT IP地址。 本文选择默认NAT IP地址。
选择私网IP地址	选择要通过DNAT规则进行通信的私网IP地址。本文以**通过ECS或弹性网卡进行选择**方式，选择云上ECS1的私网IP地址。
端口设置	选择DNAT映射的方式。本文选择端口映射方式。**具体端口**，**前端端口**输入*22*，**后端端口**输入*22*，**协议类型**选择**TCP**。
条目名称	输入DNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

步骤七：配置本地IDC路由

上述步骤已完成阿里云上的配置，您还需要在物理专线接入设备上配置指向VPC的路由。

在本地网关设备配置到云上VPC的路由，配置的路由示例如下。

> **说明** 路由示例仅供参考，不同厂商的不同设备可能会有所不同。

```
ip route 192.168.0.0 255.255.0.0 10.0.0.1
```

步骤八：测试连通性

测试云上ECS实例是否与本地IDC互访。

1. 登录VSW1的ECS1。具体操作，请参见ECS连接方式概述。
2. 执行 `ping本地IDC内服务器IP地址` 命令，测试ECS1是否能访问本地IDC内的服务器。

本文执行以下命令。

```
ping 172.16.10.137
```

如果能接收到回复报文，表示连接成功。

3. 登录本地IDC内的服务器，执行 `ssh root@NAT IP` 命令，此处的NAT IP为VPC NAT网关的默认NAT IP地址，然后输入ECS1的登录密码，测试本地IDC内的服务器是否可以远程连接到ECS1。

   本文执行以下命令。

   ```
   ssh 192.168.3.132
   ```

   如果能接收到回复报文，表示连接成功。

2.使用VPC NAT网关实现VPC地址冲突时的互相访问

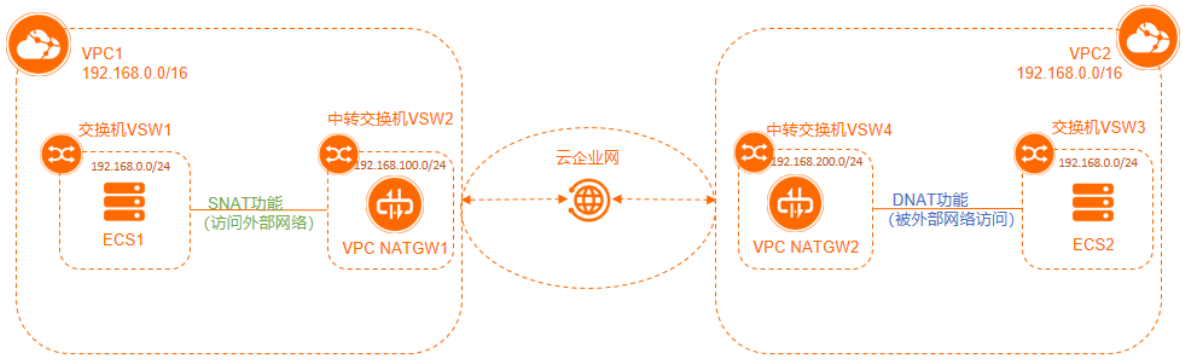
本文指导您通过使用VPC NAT网关实现当VPC地址冲突时的互相访问。

背景信息

由于早期网络规划单一或后期的业务合并，可能存在云上需要互通的两个业务VPC地址冲突的情况。您可以为两个业务VPC各配置一个VPC NAT网关并配置两个不冲突的中转私网地址（NAT IP地址）。主动访问的业务VPC使用SNAT功能将源地址转换为VPC NAT网关的中转私网地址，被访问的业务VPC通过DNAT功能使用VPC NAT网关的中转私网地址对外提供私网服务，从而实现地址冲突的两个业务VPC能够访问。

配置场景

本文以下图场景为例。某公司在华北1（青岛）地域创建了两个专有网络VPC（Virtual Private Cloud），名称分别为VPC1和VPC2，网段均为192.168.0.0/16。在VPC1中创建了网段为192.168.0.0/24的业务交换机VSW1，VSW1中创建了一台名为ECS1的云服务器ECS（Elastic Compute Service）。在VPC2中创建了网段为192.168.0.0/24的业务交换机VSW3，VSW3中创建了一台名为ECS2的ECS实例。因公司业务发展，VPC1需要访问VPC2。由于VPC1与VPC2的网段相同，无法直接通过云企业网CEN（Cloud Enterprise Network）实现互访。您可以在VPC1中创建网段为192.168.100.0/24的中转交换机VSW2。在VPC2中创建网段为192.168.200.0/24的中转交换机VSW4。然后在中转交换机中创建VPC NAT网关。通过VPC NAT网关的SNAT功能和DNAT功能实现VPC1访问VPC2。



操作流程

前提条件

- 您已经注册了阿里云账号。具体操作，请参见账号注册。
- 您已经参考下表完成了VPC和交换机的创建。具体操作，请参见搭建IPv4专有网络。

VPC名称	地域	网段	交换机名称	可用区	网段
VPC1	华北1（青岛）	192.168.0.0/16	○ 业务交换机：VSW1 ○ 中转交换机：VSW2	青岛 可用区B	○ VSW1：192.168.0.0/24 ○ VSW2：192.168.100.0/24
VPC2	华北1（青岛）	192.168.0.0/16	○ 业务交换机：VSW3 ○ 中转交换机：VSW4	青岛 可用区B	○ VSW3：192.168.0.0/24 ○ VSW4：192.168.200.0/24

- 您已在VSW1中创建了一台名称为ECS1的ECS实例。在VSW3中创建了一台名称为ECS2的ECS实例。具体操作，请参见使用向导创建实例。
- 您已经创建了一个云企业网CEN实例。具体操作，请参见创建云企业网实例。

步骤一：创建两个VPC NAT网关实例

重复以下步骤，在VSW2中创建一个名为VPC NAT GW1的VPC NAT网关；在VSW4中创建一个名为VPC NAT GW2的VPC NAT网关。

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在**VPC NAT网关**页面，单击**创建VPC NAT网关**。
4. 在**VPC NAT网关（按量付费）**页面，配置以下参数信息，然后单击**立即购买**。

   下表列出了NAT GW1和NAT GW2的配置参数。

参数	说明	配置值
地域	选择需要创建VPC NAT网关实例的地域。	此处均选择**华北1（青岛）**。
VPC ID	选择VPC NAT网关实例所属的VPC。创建VPC NAT网关实例后，不能修改其所属的VPC。	○ VPC NAT GW1：VPC1。 ○ VPC NAT GW2：VPC2。
可用区	选择VPC NAT网关实例所属的可用区。	○ VPC NAT GW1：VSW2的可用区。 ○ VPC NAT GW2：VSW4的可用区。
交换机ID	选择VPC NAT网关实例所属的交换机，建议选择独立的交换机。	○ VPC NAT GW1：VSW2。 ○ VPC NAT GW2：VSW4。
实例名称	设置VPC NAT网关实例的名称。 名称长度为1~128个字符。	○ 设置为**VPC NAT GW1**。 ○ 设置为**VPC NAT GW2**。

参数	说明	配置值
服务关联角色	显示是否已有VPC NAT网关的服务关联角色。	首次使用NAT网关（包含公网NAT网关和VPC NAT网关），需要单击**创建服务关联角色**完成创建。

5. 在**确认订单**页面，确认参数的配置信息并选中服务协议，然后单击**立即开通**。
   当出现**恭喜，开通成功！**的提示后，说明您创建成功。

步骤二：创建自定义路由表

重复以下步骤，为VSW1和VSW3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，选择路由表所属的地域。
4. 在**路由表**页面，单击**创建路由表**。
5. 在**创建路由表**页面，配置以下参数，然后单击**确定**。
   下表列出了为VSW1和VSW3创建自定义路由表的配置参数。

参数	说明	配置值
资源组	选择路由表所属的资源组。	此处均选择**全部**。
专有网络	选择路由表所属的VPC。	○ 为VSW1创建路由表：选择VPC1。 ○ 为VSW3创建路由表：选择VPC2。
名称	输入路由表的名称。	○ 为VSW1创建路由表：**VSW1VTB**。 ○ 为VSW3创建路由表：**VSW3VTB**。
描述	输入路由表的描述。	○ 为VSW1创建路由表：输入**VSW1自定义路由表**。 ○ 为VSW3创建路由表：输入**VSW3自定义路由表**。

6. 单击**已绑定交换机**页签，然后单击**绑定交换机**。
7. 在**绑定交换机**对话框，选择要绑定的交换机，然后单击**确定**。
   - 为VSW1创建路由表时，请选择VSW1交换机。
   - 为VSW3创建路由表时， 请选择VSW3交换机。

步骤三：为自定义路由表添加路由条目

重复以下步骤，为创建的VSW1VTB和VSW3VTB自定义路由表添加路由条目。

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. 选择**路由条目列表 > 自定义**页签，单击**添加自定义路由条目**。
6. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

   下表列出了为VSW1VTB和VSW3VTB自定义路由表添加的路由条目配置参数。

参数	说明	配置值
名称	输入路由条目的名称。	○ VSW1VTB：**VPCNATGW1ENTRY**。 ○ VSW3VTB：**VPCNATGW2ENTRY**。
目标网段	输入要转发到的目标网段。	此处配置为对端交换机的网段。 ○ VSW1VTB：**192.168.200.0/24**。 ○ VSW3VTB：**192.168.100.0/24**。
下一跳类型	选择下一跳的类型。	此处均选择**NAT网关**。
NAT网关	选择具体的NAT网关实例。	○ VSW1VTB：选择VPC NATGW1。 ○ VSW3VTB：选择VPC NATGW2。

步骤四：加入云企业网

以下操作请使用云企业网旧版控制台执行。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面右上角，单击**回到旧版**。
3. 在**云企业网实例**页面，找到已创建的云企业网实例，单击云企业网实例ID。
4. 单击**网络实例管理**页签，然后单击**加载网络实例**。

   本文将VPC1和VPC2加载到同一个云企业网中。具体操作，请参见加载网络实例。
5. 单击**路由策略**页签，然后单击**添加路由策略**。
6. 在**添加路由策略**面板，配置以下信息，然后单击**确定**。

   重复步骤和步骤，配置四条路由策略。

参数	说明	配置值
策略优先级	路由策略的优先级。 优先级数字越小，优先级越高。	○ 策略1：**1**。 ○ 策略2：**2**。 ○ 策略3：**3**。 ○ 策略4：**4**。

参数	说明	配置值
描述	输入路由策略的描述信息。	○ 策略1：**systemVTB1**。 ○ 策略2：**systemVTB2**。 ○ 策略3：**VSW1VTB**。 ○ 策略4：**VSW3VTB**。
地域	选择路由策略应用的地域。	四条路由策略均选择**华北1（青岛）**。
应用方向	选择路由策略应用的方向。	四条路由策略均选择**出地域网关**。
匹配条件	路由策略的匹配条件。	○ 策略1：选择**目的路由表**，然后输入VPC1的系统路由表实例ID。 ○ 策略2：选择**目的路由表**，然后输入VPC2的系统路由表实例ID。 ○ 策略3：选择**目的路由表**，然后输入VSW1的自定义路由表实例ID。 ○ 策略4：选择**目的路由表**，然后输入VSW3的自定义路由表实例ID。
策略行为	选择策略行为。	○ 策略1：选择**允许**。 ○ 策略2：选择**允许**。 ○ 策略3：选择**拒绝**。 ○ 策略4：选择**拒绝**。

配置完策略路由之后，VPC1系统路由表和VPC2系统路由表中会学习到指向对端VPC的动态路由。

7. 返回专有网络控制台。
8. 在左侧导航栏，单击**路由表**。
9. 在**路由表**页面，找到VPC1的系统路由表，然后单击路由表实例ID。
10. 在**路由条目列表 > 系统**页签，找到冲突的路由条目，然后在**CEN中状态**列单击**撤回**。

    重复步骤和步骤，将VPC2的系统路由表中的冲突路由条目撤回。

步骤五：为VPC NATGW1配置SNAT条目

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在顶部菜单栏，选择VPC NAT网关的地域。
4. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**SNAT管理**。
5. 在**SNAT管理**页签，单击**创建SNAT条目**。
6. 在**创建SNAT条目**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明

参数	说明
SNAT条目粒度	选择SNAT条目的粒度。本文选择**VPC粒度**，即VPC NAT网关所属VPC下的所有地址段可以通过配置的SNAT规则访问外部网络。
选择NAT IP地址	在下拉列表中选择用来访问外部网络的NAT IP地址。本文选择默认NAT IP地址。
条目名称	SNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

步骤六：为VPC NATGW2配置DNAT条目

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在顶部菜单栏，选择VPC NAT网关的地域。
4. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**DNAT管理**。
5. 在**DNAT管理**页签，单击**创建DNAT条目**。
6. 在**创建DNAT条目**页面，配置以下参数，然后单击**确定创建**。

配置	说明
选择NAT IP地址	选择供外部网络访问的NAT IP地址。 本文选择默认NAT IP地址。
选择私网IP地址	选择要通过DNAT规则进行通信的私网IP地址。本文以**通过ECS或弹性网卡进行选择**方式选择ECS2实例的私网IP地址。
端口设置	选择DNAT映射的方式。本文选择端口映射方式。**具体端口**，**前端端口**输入22，**后端端口**输入22，**协议类型**选择**TCP**。
条目名称	输入DNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

步骤七：测试连通性

1. 登录VSW1下的ECS1实例。具体操作，请参见ECS连接方式概述。
2. 执行`ping`命令，`ping` VPC NATGW2的默认NAT IP地址，测试ECS1实例是否能访问ECS2实例。

   经测试，ECS1实例可以访问ECS2实例。

```
[root@iZm5edcse[redacted]0h5sy5Z ~]# ping 192.168.200.249
PING 192.168.200.249 (192.168.200.249) 56(84) bytes of data.
64 bytes from 192.168.200.249: icmp_seq=1 ttl=64 time=0.912 ms
64 bytes from 192.168.200.249: icmp_seq=2 ttl=64 time=0.789 ms
64 bytes from 192.168.200.249: icmp_seq=3 ttl=64 time=0.757 ms
64 bytes from 192.168.200.249: icmp_seq=4 ttl=64 time=0.796 ms
64 bytes from 192.168.200.249: icmp_seq=5 ttl=64 time=0.773 ms
64 bytes from 192.168.200.249: icmp_seq=6 ttl=64 time=0.785 ms
64 bytes from 192.168.200.249: icmp_seq=7 ttl=64 time=0.832 ms
64 bytes from 192.168.200.249: icmp_seq=8 ttl=64 time=0.789 ms
^C
--- 192.168.200.249 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 201ms
rtt min/avg/max/mdev = 0.757/0.804/0.912/0.047 ms
```

3. 执行 `ssh root@NAT IP` 命令，此处的NAT IP为VPC NAT GW2的默认NAT IP地址，然后输入ECS2实例的登录密码，测试ECS1实例是否可以远程连接到ECS2实例。

   若界面上出现 `Welcome to Alibaba Cloud Elastic Compute Service!` 时，表示您已经成功连接到实例。

   经测试，ECS1实例可以通过VPC NAT GW2的DNAT功能访问ECS2实例。

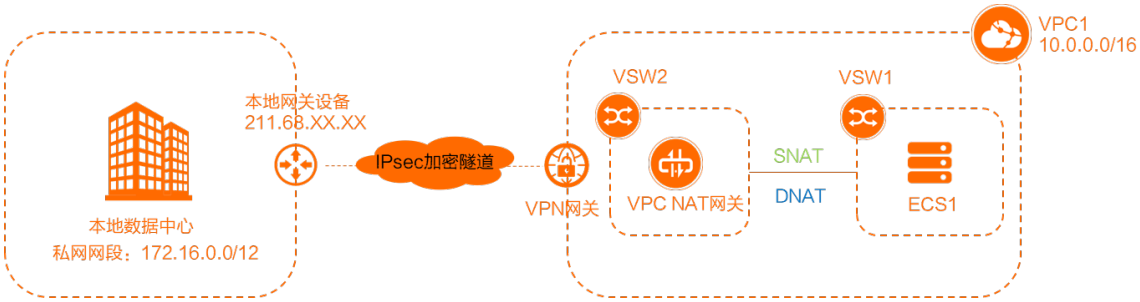
```
[root@iZm5[redacted]0h5sy5Z ~]# ssh 192.168.200.249
root@192.168.200.249's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Mon Aug 30 15:26:08 2021 from 1[redacted].220
[root@iZm5e[redacted]neyanq6Z ~]#
```

3.VPC NAT网关实现云上与云下通过指定私网IP互访

本文指导您使用VPC NAT网关联动VPN网关实现云上VPC与本地数据中心IDC（Internet Data Center）通过指定私网IP地址互访。

场景示例

本文以下图场景为例。某企业在华北1（青岛）地域拥有一个名称为VPC1的专有网络VPC（Virtual Private Cloud）。该企业在华北2（北京）地域拥有本地IDC。因业务发展，企业需要VPC1能以指定私网IP地址访问本地IDC，本地IDC也能以指定私网IP地址访问VPC1。



企业计划使用VPC NAT产品联动VPN网关产品实现上述需求。

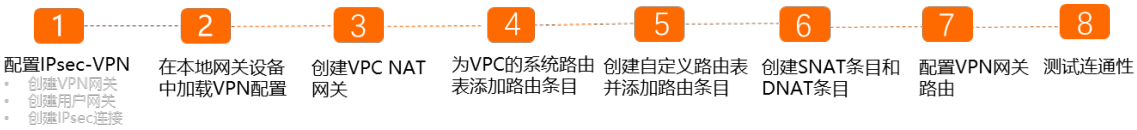
您可以通过VPN网关的IPsec-VPN连接，建立本地IDC与云上VPC的连接，实现云上和云下的安全互通；通过VPC NAT网关的SNAT和DNAT功能，实现VPC内指定IP地址与本地IDC互访。本文示例中的网段规划如下表所示。您也可以自行规划网段，请确保您的网段之间没有重叠。

配置项	地址段
云上VPC1网段	10.0.0.0/16
云上交换机网段	• VSW1：10.0.0.0/24 • VSW2：10.0.1.0/24
云上ECS实例的IP地址	ECS1：10.0.0.81
本地IDC网段	172.16.0.0/12
本地IDC内服务器IP地址	172.16.0.124
本地IDC网关设备IP地址	211.68.XX.XX

前提条件

- 您已经在华北1（青岛）地域创建了名称为VPC1的专有网络，并在VPC1创建了名称为VSW1和VSW2的交换机。具体操作，请参见创建和管理专有网络。
- 您已经在VSW1中创建了名称为ECS1的云服务器ECS（Elastic Compute Service）实例并部署了应用服务。具体操作，请参见使用向导创建实例。

配置步骤



步骤一：配置IPsec-VPN

通过IPsec-VPN功能可建立VPC与本地IDC之间的VPN连接。使用IPsec-VPN功能，您需要创建VPN网关、用户网关和IPsec连接。关于IPsec-VPN功能的更多信息，请参见IPsec-VPN入门概述。

1. 登录VPN网关管理控制台。
2. 执行以下操作，创建VPN网关。
   i. 在**VPN网关**页面，单击**创建VPN网关**。
   ii. 在购买页面，配置以下参数信息，然后单击**立即购买**并完成支付。

参数	说明
实例名称	输入VPN网关实例的名称。
地域	选择VPN网关实例所属的地域。本文选择**华北1（青岛）**。
网关类型	默认为**普通型**。
专有网络	选择要连接的VPC实例。本文选择VPC1。
指定交换机	是否指定VPN网关创建在VPC实例中的某一个交换机下。如果您选择了**是**，您还需要指定具体的**虚拟交换机**。 本文选择**否**。
带宽峰值	选择VPN网关实例的公网带宽峰值。单位为Mbps。 本文选择**5 Mbps**。
流量	VPN网关默认按使用流量计费。更多信息，请参见按量计费。
IPsec-VPN	选择是否开启IPsec-VPN功能。本文选择**开启**。
SSL-VPN	选择是否开启SSL-VPN功能。本文选择**关闭**。
购买时长	VPN网关默认按小时计费。

   iii. 返回**VPN网关**页面，查看已创建的VPN网关实例。
   创建好的VPN网关实例初始状态为**准备中**，约1~5分钟会变为**正常**状态，表明VPN网关实例已经完成初始化，可以正常使用。
3. 执行以下操作，创建用户网关。
   i. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
   ii. 在顶部菜单栏，选择创建用户网关实例的地域。本文选择**华北1（青岛）**。
   iii. 在**用户网关**页面，单击**创建用户网关**。

iv. 在**创建用户网关**面板，配置以下参数信息，然后单击**确定**。

参数	说明
名称	输入用户网关实例的名称。
IP地址	输入VPC1要连接的本地IDC的网关设备的公网IP。本文输入*211.68.XX.XX*。
自治系统号	输入本地数据中心网关设备的自治系统号。
描述	输入用户网关实例的描述信息。

更多参数信息，请参见创建用户网关。

4. 执行以下操作，创建IPsec连接。
   i. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
   ii. 在顶部菜单栏，选择创建IPsec连接实例的地域。本文选择**华北1（青岛）**。
   iii. 在**IPsec连接**页面，单击**创建IPsec连接**。
   iv. 在**创建IPsec连接**页面，配置以下参数信息，然后单击**确定**。

参数	说明
名称	输入IPsec连接的名称。
VPN网关	选择已创建的VPN网关。
用户网关	选择已创建的用户网关。
路由模式	选择路由模式。本文选择**目的路由模式**。
立即生效	选择是否立即生效。 ■ **是**：配置完成后立即进行协商。 ■ **否**：当有流量进入时进行协商。 本文选择**否**。
预共享密钥	输入共享密钥。建立IPsec连接需保证该值与本地网关设备的预共享密钥一致。如果不输入该值，系统默认生成一个16位的随机字符串。

其他选项使用默认配置。更多信息，请参见创建IPsec连接。

步骤二：在本地网关设备中加载VPN配置

使用IPsec-VPN建立VPC到本地IDC的连接时，在配置完阿里云VPN网关后，您还需在本地IDC的网关设备中进行VPN配置。

1. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
2. 在**IPsec连接**页面，找到目标IPsec连接实例，然后在**操作**列下选择 ⋮ **> 下载对端配置**。
3. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。具体操作，请参见本地网关配置。

步骤三：创建VPC NAT网关

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在**VPC NAT网关**页面，单击**创建VPC NAT网关**。
4. 在**VPC NAT网关（按量付费）**页面，配置以下参数信息，然后单击**立即购买**。

参数	说明
地域	选择需要创建VPC NAT网关实例的地域。本文选择**华北1（青岛）**。
VPC ID	选择VPC NAT网关实例所属的VPC。创建VPC NAT网关实例后，不能修改其所属的VPC。本文选择VPC1。
可用区	选择VPC NAT网关实例所属的可用区。本文选择VSW2的可用区。
交换机ID	选择VPC NAT网关实例所属的交换机，建议您选择独立的交换机。本文选择VSW2。
实例名称	设置VPC NAT网关实例的名称。 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（-）。
服务关联角色	显示是否已有VPC NAT网关的服务关联角色。 首次使用NAT网关（包含公网NAT网关和VPC NAT网关），需要单击**创建服务关联角色**完成创建。

5. 返回**VPC NAT网关**页面，查看已创建的VPC NAT网关。
   - 单击VPC NAT网关的实例ID，在**基本信息**页签，查看VPC NAT网关的VPC、交换机等信息。
   - 单击**NAT IP**页签，查看默认NAT IP地址段和默认NAT IP地址。

> **说明** 默认NAT IP地址段为该VPC NAT网关所属交换机的网段，默认NAT IP地址为系统在交换机网段中随机分配的一个IP地址。默认NAT IP地址段和默认NAT IP地址均不能删除。

步骤四：为VPC1的系统路由表添加路由条目

为VPC1的系统路由表添加指向VPC NAT网关的路由条目。

1. 登录专有网络管理控制台。
2. 在**专有网络**，找到VPC1，然后单击VPC的ID。
3. 在VPC详情页面，单击**资源管理**页签，单击**路由表**下方的链接。
4. 在**路由表**页面，找到**路由表类型**为**系统**的路由表，单击其ID。
5. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。
6. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。本文输入*VPCENTRY*。
目标网段	输入要转发到的目标网段。本文输入本地IDC内服务器IP地址，*172.16.0.124/32*。

参数	说明
下一跳类型	选择下一跳的类型。本文选择**NAT网关**。
NAT网关	选择具体的NAT网关实例。本文选择步骤三：创建VPC NAT网关创建的VPC NAT网关。

步骤五：创建自定义路由表并添加路由条目

为VSW2交换机创建自定义路由表并添加指向VPN网关的路由条目。

关于支持创建自定义路由表的地域信息，请参见自定义路由表发布及地域支持情况。

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，单击**创建路由表**。
5. 在**创建路由表**页面，配置以下参数，然后单击**确定**。

参数	说明
资源组	选择路由表所属的资源组。本文选择**全部**。
专有网络	选择路由表所属的VPC。本文选择VPC1。
名称	输入路由表的名称。本文输入*VPNVTB*。
描述	输入路由表的描述。本文输入*VPCNAT的自定义路由表*。

6. 单击**已绑定交换机**页签，然后单击**绑定交换机**。
7. 在**绑定交换机**对话框，选择要绑定的交换机，然后单击**确定**。

   本文选择VSW2交换机。
8. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。
9. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。本文输入*VPCNATENTRY*。
目标网段	输入要转发到的目标网段。本文输入本地IDC内服务器IP地址，*172.16.0.124/32*。
下一跳类型	选择下一跳的类型。本文选择**VPN网关**。
VPN网关	选择具体的VPN网关实例。本文选择步骤一：配置IPsec-VPN创建的VPN网关。

步骤六：使用默认NAT IP创建SNAT条目和DNAT条目

1. 登录NAT网关管理控制台。
2. 在左侧导航栏，选择**NAT网关 > VPC NAT网关**。
3. 在顶部菜单栏，选择公网NAT网关的地域。

4. 执行以下步骤，创建SNAT条目。
   i. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**SNAT管理**。
   ii. 在**SNAT管理**页签，单击**创建SNAT条目**。
   iii. 在**创建SNAT条目**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
SNAT条目粒度	选择SNAT条目的粒度。本文选择**交换机粒度**，然后在**选择交换机**列表中选择ECS1所在交换机。本文选择VSW1。**交换机网段**处会显示VSW1的网段。
选择NAT IP地址	在下拉列表中选择用来访问外部私有网络的NAT IP地址。本文选择默认NAT IP地址。
条目名称	SNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

5. 返回**VPC NAT网关**页面，然后执行以下操作，创建DNAT条目。
   i. 在**VPC NAT网关**页面，找到目标VPC NAT网关实例，然后在**操作**列单击**DNAT管理**。
   ii. 在**DNAT管理**页签，单击**创建DNAT条目**。
   iii. 在**创建DNAT条目**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
选择NAT IP地址	选择供外部私有网络访问的NAT IP地址。本文选择默认NAT IP地址。
选择私网IP地址	选择要通过DNAT规则进行通信的私网IP地址。本文以**通过ECS或弹性网卡进行选择**方式，选择ECS1的私网IP地址。
端口设置	选择DNAT映射的方式。本文选择**具体端口**，即端口映射方式。 **前端端口**输入*22*，**后端端口**输入*22*，**协议类型**选择**TCP**。
条目名称	输入DNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

步骤七：配置VPN网关的路由

您需要在VPN网关中配置路由，并发布路由到VPC路由表以实现本地IDC和VPC的通信。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
4. 在**VPN网关**页面，找到目标VPN网关实例，单击实例ID。
5. 在**目的路由表**页签，单击**添加路由条目**。
6. 在**添加路由条目**面板，配置以下参数信息，然后单击**确定**。

参数	说明
目标网段	输入本地数据中心的私网网段。本文输入本地IDC的网段，*172.16.0.0/12*。
下一跳类型	选择**IPsec连接**。
下一跳	选择IPsec连接实例。本文选择步骤一：配置IPsec-VPN创建的IPsec连接。
发布到VPC	选择是否将新添加的路由发布到VPC路由表。本文选择**是**。
权重	选择路由的权重值。本文选择**100**。 ○ **100**：高优先级。 ○ **0**：低优先级。

步骤八：测试连通性

1. 登录VSW1的ECS1。具体操作，请参见连接方式概述。
2. 执行 `ping 本地IDC内服务器IP地址` 命令，测试ECS1是否能访问本地IDC内的服务器。

   本文执行以下命令。

   ```
   ping 172.16.0.124
   ```

   经测试，ECS1可以访问本地IDC内的服务器。

   ```
   [root@iZm5ed[redacted]6xsog69bpZ ~]# ping 172.16.0.124
   PING 172.16.0.124 (172.16.0.124) 56(84) bytes of data.
   64 bytes from 172.16.0.124: icmp_seq=1 ttl=62 time=15.6 ms
   64 bytes from 172.16.0.124: icmp_seq=2 ttl=62 time=15.6 ms
   64 bytes from 172.16.0.124: icmp_seq=3 ttl=62 time=15.7 ms
   64 bytes from 172.16.0.124: icmp_seq=4 ttl=62 time=15.6 ms
   64 bytes from 172.16.0.124: icmp_seq=5 ttl=62 time=15.6 ms
   64 bytes from 172.16.0.124: icmp_seq=6 ttl=62 time=15.6 ms
   64 bytes from 172.16.0.124: icmp_seq=7 ttl=62 time=15.6 ms
   ^C
   --- 172.16.0.124 ping statistics ---
   7 packets transmitted, 7 received, 0% packet loss, time 6008ms
   rtt min/avg/max/mdev = 15.578/15.605/15.665/0.136 ms
   ```

3. 登录本地IDC内的服务器，执行 `ssh root@NAT IP` 命令，此处的NAT IP为VPC NAT网关的默认NAT IP地址，然后输入ECS1的登录密码，测试本地IDC内的服务器是否可以远程连接到ECS1。

   本文执行以下命令。

   ```
   ssh 10.0.1.43
   ```

   经测试，本地IDC内的服务器可以通过VPC NAT网关的DNAT功能访问ECS1。

```
[root@iZ2ze9r3t[redacted]z25cs7cfZ ~]# ssh 10.0.1.43
root@10.0.1.43's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Updates Information Summary: available
    6 Security notice(s)
        6 Moderate Security notice(s)
Run "dnf upgrade-minimal --security" to apply all updates.
Last login: Tue Nov 30 17:40:43 2021 from 172.16.0.124
[root@iZm5edtfg[redacted]xsog69bpZ ~]#
```

4.统一公网出口IP

4.1. 通过公网NAT网关实现云上统一公网出入口IP

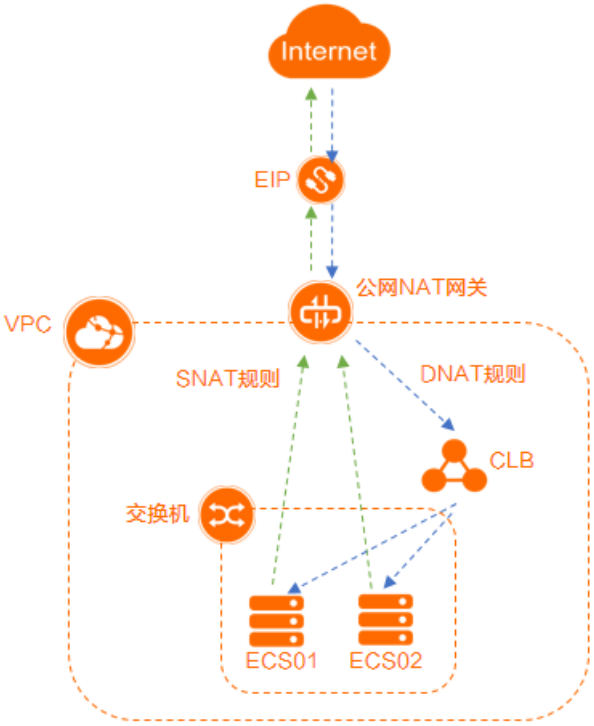
本文介绍如何联动公网NAT网关和

传统型负载均衡CLB

（Classic Load Balancer）实现互联网业务的高可用性，且通过公网NAT网关绑定弹性公网IP（Elastic IP Address，简称EIP）实现统一云上出入口IP，帮助您高效地管理互联网业务。

场景示例

本文以下图场景为例。



某公司在华东2（上海）地域创建了两台ECS实例，并在两台ECS实例部署了业务系统。由于业务的特殊性，要求业务满足以下条件：

- 业务具有高可用性，避免单ECS实例故障导致的业务中断。
- 两台ECS实例均可以主动访问互联网。
- 互联网访问ECS实例使用的公网IP与ECS实例主动访问互联网使用的公网IP一致。

您可以联动公网NAT网关、

CLB

和EIP实现上述需求：

- 公网NAT网关的DNAT功能与

  CLB

组合使用可以增强业务的高可用性，当其中一台ECS实例出现故障时，

CLB

会自动屏蔽故障的ECS实例，并将请求分发给正常运行的ECS实例，保证业务系统仍能正常工作。

- 公网NAT网关的SNAT功能可以实现ECS实例主动访问互联网。
- 公网NAT网关的DNAT功能和SNAT功能同时使用一个EIP，可以实现

  CLB

  的后端服务器ECS实例访问互联网的出入口IP一致，有利于您更高效地管理互联网业务。

前提条件

- 您已经在华东2（上海）地域创建了VPC和交换机。具体操作，请参见搭建IPv4专有网络。
- 您已经在交换机中创建了两台ECS实例，名称分别为ECS01和ECS02，且在ECS实例中均部署了业务系统。具体操作，请参见使用向导创建实例。
- 您已经确认ECS实例的安全组规则允许ECS实例访问互联网和被互联网访问。具体操作，请参见添加安全组规则。

配置步骤

步骤一：创建

CLB

实例

CLB

是将访问流量根据转发策略分发到多台后端服务器ECS实例的流量分发控制服务。

CLB

扩展了应用的服务能力，增强了应用的可用性。

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，单击**创建传统型负载均衡**。
3. 在实例购买页面，配置以下信息，然后单击**立即购买**并完成支付。
   - **地域**：由于

     CLB

     默认不支持跨地域部署，因此创建

     CLB

     实例时应选择与ECS实例相同的地域。本文选择**华东2（上海）**。
   - **可用区类型**：默认选择为**多可用区**。
   - **主可用区**：本文选择**华东2可用区D**。
   - **备可用区**：本文选择**华东2可用区B**。
   - **实例名称**：输入实例名称，或者使用系统自动创建的实例名称。

- **实例类型**：本文选择**私网**。
- **负载均衡规格**：本文选择**简约型I(slb.s1.small)**。
- **网络类型**：选择

  CLB

  实例的网络类型。本文选择**专有网络**。
- **IP版本**：默认选择为**IPv4**。
- **功能特性**：默认选择为**标准功能**。
- **专有网络**：本文选择已创建的VPC。
- **虚拟交换机**：本文选择已创建的交换机。
- **计费方式**：显示

  CLB

  实例的计费方式，默认为**按使用流量计费**。
- **资源组**：选择负载均衡实例所属的资源组。
- **购买数量**：本文购买1个

  CLB

  实例。

CLB

实例创建完成后，系统会为

CLB

实例分配一个私网IP地址，用于私网接入。

步骤二：配置

CLB

实例

创建

CLB

实例后，您需要对

CLB

实例进行配置。配置完成后，

CLB

实例才能进行流量转发。在配置时，您至少需要添加一个监听和一组后端服务器。

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，找到步骤一创建的

   CLB

实例，然后在**操作**列单击**监听配置向导**。

3. 在**协议&监听**配置向导页面，配置以下信息，然后单击**下一步**。
   - **选择负载均衡协议**：本文选择**TCP**。
   - **监听端口**：用来接收请求并向后端服务器进行转发的

     CLB

     实例端口。

     本文输入*80*。
   - **监听名称**：本文不填写，系统默认以 `协议_端口` 定义名称。

   其余参数使用默认配置。
4. 在**后端服务器**配置向导页面，选择**默认服务器组**，然后单击**继续添加**，添加后端服务器。
   i. 在**我的服务器**面板，选中ECS01和ECS02实例，然后单击**下一步**。
   ii. 配置权重，然后单击**添加**。

   权重越大转发的请求越多，默认权重为**100**，本文使用默认值。
   iii. 在**后端服务器**配置向导页面，配置后端协议端口，即ECS实例开放的用来接收请求的后端端口。后端端口在同一个

   CLB

   实例内可以重复。本文设置为*80*。
5. 在**后端服务器**配置向导页面，单击**下一步**，配置健康检查，本文使用默认值。

   开启健康检查功能后，当后端服务器中某个ECS实例健康检查出现问题时，

   CLB

   会将请求转发到其它健康检查正常的ECS实例上；而当该ECS实例恢复正常运行时，

   CLB

   会自动将请求转发到该ECS实例。
6. 在**健康检查**配置向导页面，单击**下一步**，进入**配置审核**配置向导，确认配置无误后，单击**提交**。
7. 在弹出的对话框，单击**知道了**，返回**实例管理**页面，单击图标查看

   CLB

   实例。

   当后端服务器中的ECS实例的健康检查状态为**正常**时，表示后端ECS实例可以正常处理

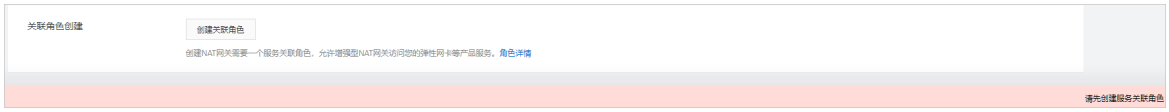
   CLB

   实例转发的请求。

步骤三：创建公网NAT网关实例

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，单击**创建NAT网关**。

3. 首次使用NAT网关时，在创建公网NAT网关页面**关联角色创建**区域，单击**创建关联角色**。角色创建成功后即可创建NAT网关。



关于NAT网关服务关联角色的更多信息，请参见服务关联角色。

4. 在创建公网NAT网关页面，配置以下购买信息，然后单击**立即购买**。

配置	说明
付费模式	默认选择为**按量付费**，即一种先使用后付费的付费模式。更多信息，请参见公网NAT网关计费。
所属地域	选择需要创建公网NAT网关的地域。
所属专有网络	选择公网NAT网关所属的VPC。创建后，不能修改公网NAT网关所属的VPC。
关联交换机	选择公网NAT网关实例所属的交换机。
计费类型	默认选择为**按使用量计费**，即按公网NAT网关实际使用量收费。更多信息，请参见公网NAT网关计费。
计费周期	默认选择为**按小时**，即按使用量计费公网NAT网关的计费周期为1小时，不足1小时按1小时计算。
实例名称	设置公网NAT网关实例的名称。 实例名称长度为2~128个字符，以英文大小字母或中文开头，可包含数字、下划线（_）和短划线（-）。
访问模式	选择公网NAT网关的访问模式。支持以下两种模式： ○ **VPC全通模式（SNAT）**：选择了VPC全通模式，在公网NAT网关创建成功后当前VPC内所有实例即可通过该公网NAT网关访问公网。 选择**VPC全通模式（SNAT）**后，您需要配置弹性公网IP（Elastic IP Address，简称EIP）的相关信息。 ○ **稍后配置**：如需稍后配置或有更多配置需求，可在购买完成后，前往控制台进行配置。 选择**稍后配置**，则只购买公网NAT网关实例。 本文选择**稍后配置**。

5. 在**确认订单**页面确认公网NAT网关的配置信息，选中服务协议并单击**确认订单**。
当出现**恭喜，购买成功！**的提示后，说明您创建成功。

创建成功后，您可以在**公网NAT网关**页面查看网关类型为**增强型**的公网NAT网关。

步骤四：绑定EIP

您可以将EIP绑定到公网NAT网关上。公网NAT网关绑定EIP后，可以使用EIP配置DNAT条目和SNAT条目。

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，找到步骤三创建的公网NAT网关实例，然后在**操作**列选择 ⋮ > **绑定弹性公网IP**。
3. 在**绑定弹性公网IP**对话框，配置以下参数，然后单击**确定**。
   - **所在资源组**：选择EIP所在的资源组。
   - **选择弹性公网IP**：选择要绑定到公网NAT网关的EIP。
     - **从已有弹性公网IP中选择**：在下拉列表中选择已有的EIP实例。
     - **新购弹性公网IP并绑定**：系统将为您创建1个按使用流量计费的EIP实例，并绑定到公网NAT网关。

     本文选择**新购弹性公网IP并绑定**。

EIP绑定完成后，您可以在**公网NAT网关**页面查看绑定的EIP。

步骤五：创建DNAT条目

公网NAT网关支持DNAT功能，将公网NAT网关绑定的EIP映射给私网

CLB

实例使用，使私网

CLB

实例的后端服务器能够提供互联网服务。

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，找到步骤三创建的公网NAT网关实例，然后在**操作**列单击**设置DNAT**。
3. 在**DNAT条目列表**区域，单击**创建DNAT条目**。
4. 在**创建DNAT条目**页面，根据以下信息配置DNAT条目，然后单击**确定创建**。
   - **选择公网IP地址**：选择要提供互联网通信的EIP。本文选择步骤四中绑定到公网NAT网关的EIP。

     > **说明** 本文DNAT条目使用的EIP与SNAT条目使用的EIP相同。

   - **选择私网IP地址**：本文选择**通过手动输入**，然后输入

     CLB

     实例的私网IP地址*192.168.24.206*。
   - **端口设置**：选择DNAT映射的方式：

- **任意端口**：该方式属于IP映射，即任何访问该EIP的请求都将转发到目标ECS实例上。
- **具体端口**：该方式属于端口映射，公网NAT网关会将以指定协议和端口访问该EIP的请求转发到目标ECS实例的指定端口上。

本文选择**具体端口**，然后将**公网端口**设置为*80*、**私网端口**设置为*80*、**协议类型**设置为**TCP**。

- **条目名称**：输入DNAT条目的名称。

  名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

DNAT条目创建成功后，您可以在**DNAT条目列表**区域查看状态为**可用**的DNAT条目。

步骤六：创建SNAT条目

公网NAT网关支持SNAT功能，为VPC中无公网IP的ECS实例提供访问互联网的代理服务。

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，找到步骤三创建的公网NAT网关实例，然后在**操作**列单击**设置SNAT**。
3. 在**SNAT条目列表**区域，单击**创建SNAT条目**。
4. 在**创建SNAT条目**页面，根据以下信息配置SNAT条目，然后单击**确定创建**。
   - **SNAT条目粒度**：本文选择**VPC粒度**，即公网NAT网关实例所属VPC下的所有ECS实例都可以通过配置的SNAT规则访问互联网。
   - **选择公网IP地址**：选择用来提供互联网访问的EIP。本文选择**使用单IP**，然后在下拉列表选择步骤四中绑定到公网NAT网关的EIP。

     > **说明** 本文SNAT条目使用的EIP与DNAT条目使用的EIP相同。

   - **条目名称**：SNAT条目的名称。

     名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。

步骤七：访问测试

SNAT条目和DNAT条目创建成功后，您可以测试ECS实例的网络连通性。

1. 测试ECS实例是否可以访问互联网。
   i. 登录ECS01。具体操作，请参见ECS连接方式概述。

ii. 如下图所示，执行 `ping` 命令测试网络连通性。

经测试，ECS01可以访问互联网。

```
[root@iZb     Z ~]# ping www.aliyun.com
PING na61-na62.wagbr    aliyun.com    babadns.com (20    .114) 56(84) bytes of data.
64 bytes from 2    .114 (20    114): icmp_seq=1 ttl=93 time=35.4 ms
64 bytes from 2    .114 (20    114): icmp_seq=2 ttl=93 time=35.3 ms
64 bytes from 2    .114 (20    114): icmp_seq=3 ttl=93 time=35.2 ms
64 bytes from 2    .114 (20    114): icmp_seq=4 ttl=93 time=35.2 ms
^C
--- na61-na62.wagbri    .aliyun.com    babadns.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 35.219/35.272/35.371/0.145 ms
```

> **说明** 您可以参考上述操作，登录ECS02测试网络连通性。

iii. 执行 `curl myip.ipip.net` 命令探测ECS01的公网出口IP。

经测试，ECS01公网出口IP与公网NAT网关实例中SNAT条目中的IP一致，即ECS01通过公网NAT网关的SNAT功能主动访问互联网。

```
[root@iZb     Z ~]# curl myip.ipip.net
当前 IP: 4    .67  来自于：中国 浙江 杭州  阿里云/E    教育网
```

2. 测试部署在ECS实例的业务是否可以被互联网访问。

i. 打开互联网中任意一台电脑的浏览器。

ii. 输入绑定到公网NAT网关的EIP地址访问部署在ECS实例上的业务服务。

经验证，互联网可以访问部署在ECS实例上的业务服务，即ECS实例通过公网NAT网关的DNAT功能提供互联网访问服务，且公网出入口IP相同，都是绑定到公网NAT网关的EIP。

3. 测试

CLB

实例是否能够提供流量分发服务。

i. 停止ECS01。具体操作，请参见停止实例。

ii. 打开互联网中任意一台电脑的浏览器。

iii. 输入绑定到公网NAT网关的EIP地址访问部署在ECS实例上的业务服务。

经验证，互联网可以访问部署在ECS实例上的业务服务，此时提供业务服务的是ECS02，即当ECS01故障时，

CLB

将互联网访问转发至正常的ECS02，实现了业务的高可用性。

4.2. 为已分配固定公网IP的ECS实例统一公网出口IP

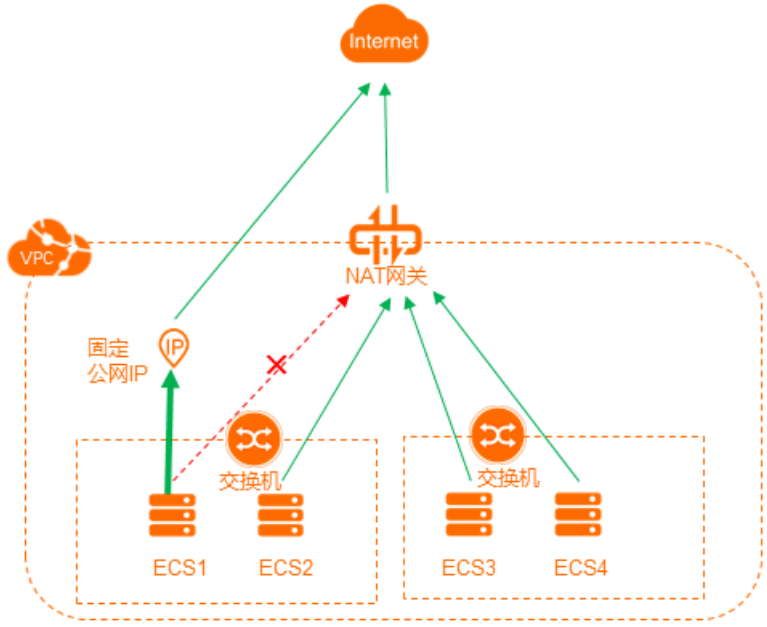
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为已分配固定公网IP的ECS实例统一公网出口IP。

前提条件

分配了固定公网IP的ECS实例所在的VPC已经配置了SNAT功能。更多信息，请参见创建SNAT实现访问公网服务。

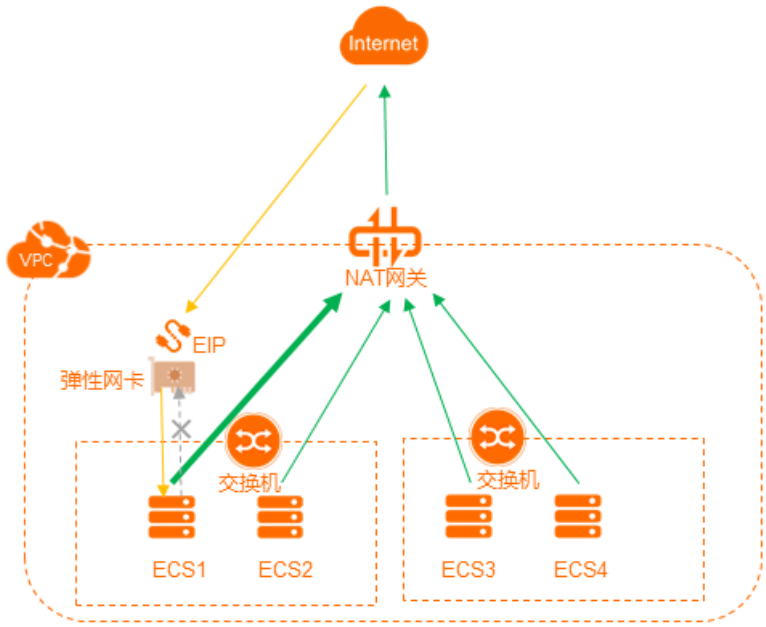
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经分配了固定公网IP，这些ECS实例会优先通过固定公网IP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能代理访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为ECS实例单独分配一块弹性网卡，并将固定公网IP转为EIP，然后将EIP绑定到弹性网卡，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一：固定公网IP转EIP

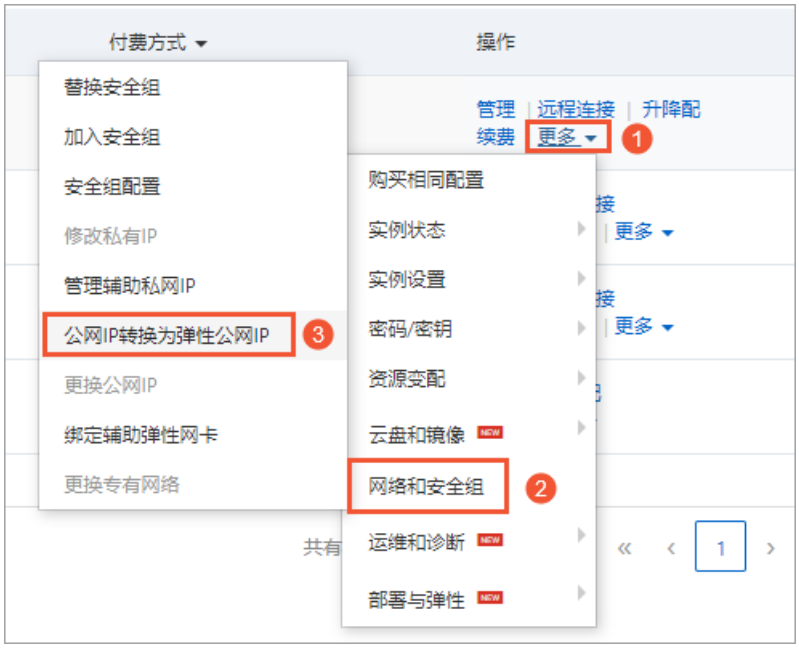
不同计费模式的ECS实例，对固定公网IP转EIP的支持不同：

- 按量付费类型的ECS实例，支持直接将固定公网IP转为EIP。
- 包年包月类型的ECS实例，不支持直接将固定公网IP转为EIP。您需要先将包年包月ECS实例转为按量付费ECS实例，再将按量付费ECS实例的固定公网IP转为EIP。包年包月ECS实例转为按量付费ECS实例的详细操作说明，请参见包年包月转按量付费。

完成以下操作，将按量付费ECS实例的固定公网IP转为EIP。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部状态栏处，选择ECS实例的地域。

4. 在**实例列表**页面，找到目标ECS实例，选择**操作**列下的**更多 > 网络和安全组 > 公网IP转换为弹性公网IP**。



5. 在弹出的对话框中，单击**确定**。
6. 刷新实例列表。

   转换成功后，原来的公网IP地址会标注为**弹性**。

步骤二：创建弹性网卡

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。

   > **说明**
   >
   > 弹性网卡的地域必须与ECS实例的地域相同。

4. 在**网卡列表**页面，单击**创建弹性网卡**。
5. 在**创建弹性网卡**对话框，根据以下信息配置弹性网卡，然后单击**确定**。
   - **网卡名称**：输入弹性网卡的名称。
   - **专有网络**：选择ECS实例所在的专有网络。

- **交换机**：选择ECS实例所在可用区的交换机。
- **主私网IP**（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。本文不指定主私网IP。
- **辅助私网IP**（可选）：单击相应选项进行设置。本文选择不设置。
- **安全组**：选择当前专有网络的一个安全组。

更多参数信息，请参见创建弹性网卡。

步骤三：将弹性网卡绑定到ECS实例

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。
4. 在**网卡列表**页面，找到目标弹性网卡，单击**操作**列下的**绑定实例**。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击**确定**。

步骤四：将EIP与ECS实例解绑

1. 登录弹性公网IP管理控制台。
2. 选择EIP的地域。
3. 在**弹性公网IP**页面，找到目标EIP，单击**操作**列下的**解绑绑定**。
4. 在弹出的对话框中，单击**确定**。

步骤五：将EIP绑定到弹性网卡

1. 登录弹性公网IP管理控制台。
2. 选择EIP的地域。
3. 在**弹性公网IP**页面，找到目标EIP，单击**操作**列下的**绑定资源**。
4. 在**绑定弹性公网IP至资源**对话框，根据以下信息绑定EIP至弹性网卡，然后单击**确定**。
   - **实例类型**：选择辅助弹性网卡。
   - **资源组**（可选）：选择该EIP所属的资源组。本文选择默认资源组。
   - **绑定模式**（可选）：选择EIP绑定模式。 本文选择**普通模式**。
   - **选择要绑定的**：选择要绑定的辅助弹性网卡。

步骤六：配置网卡路由

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。

3. 查看ECS实例的弹性网卡信息如下图所示。

网卡ID/名称	标签	交换机/专有网络	可用区	安全组ID	绑定实例ID	公网IP地址	私网IP地址	网卡类型/MAC地址（全部）
eni-m5eh :4wa2whgs te NAT		vsw p4... vpc- po8...	青岛 可用区B	sg-n 3z...	i-m cs...	.1 .62	192. （主私网）	辅助网卡 00:16 :2a:40
eni-m5e3z 7cmkhiobo -		vsw p4... vpc- po8...	青岛 可用区B	sg-r 3z...	i-r dcs...		192. .3 （主私网）	主网卡 00:1 :f0:24

4. 远程登录ECS实例，更多信息，请参见连接方式概述。

5. 执行 `ip a` 命令查看弹性网卡信息。

```
[root@iZ efag9zZ ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:04:40:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.10/28 brd 192.168.3.15 scope global dynamic noprefixroute eth0
       valid_lft 314948898sec preferred_lft 314948898sec
    inet6 fe80::216:3eff:fe04:404d/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:04:7e:50 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.11/28 brd 192.168.3.15 scope global dynamic noprefixroute eth1
       valid_lft 315294873sec preferred_lft 315294873sec
    inet6 fe80::f25d:3a11:4152:72d6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@iZ 2efag9zZ ~]#
```

经过查看，得到ECS实例弹性网卡的信息如下：

eth0：主网卡，私网地址：192.168.3.10

eth1：辅助弹性网卡，私网地址：192.168.3.11 公网地址：118.190.XX.XX

6. 按您的需要规划路由表里每块网卡的默认路由metric值。

执行以下命令，查看Gateway和metric值。

```
route -n
```

查询结果如下所示：

```
[root@]  ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.3.13    0.0.0.0         UG    100    0        0 eth0
0.0.0.0         192.168.3.13    0.0.0.0         UG    101    0        0 eth1
192.168.3.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.3.0     0.0.0.0         255.255.255.0   U     101    0        0 eth1
```

> **说明**
>
> 本文以一块辅助弹性网卡为例，查看到辅助弹性网卡的metric值大于主网卡的metric值，路由优先级低于主网卡，不需要执行重新规划网卡的metric值，保持默认配置即可。如有多块辅助弹性网卡，请根据实际情况配置，具体操作，请参见配置网卡路由。

7. 创建路由表并配置策略路由。

- 如果需要为ECS实例的弹性网卡配置单次策略路由，请执行以下操作。

  > **说明**
  > ECS实例重启后，配置的弹性网卡路由会失效。

  a. 执行以下命令创建路由表。

  ```
  ip -4 route add default via 192.168.3.13 dev eth1 table 101
  ```

  > **说明**
  > 建议路由表名称和网卡的默认路由metric取值保持一致，如本例中的101。

  b. 执行以下命令检查路由表是否创建成功。

  ```
  ip route list table 101
  ```

  查询结果如下所示：

  ```
  [root@iZm5ef     g9zZ ~]# ip route list table 101
  default via 192.168.3.13 dev eth1
  [root@iZm5ef     g9zZ ~]#
  ```

  c. 执行以下命令创建策略路由。

  ```
  ip -4 rule add from 192.168.3.11 lookup 101
  ```

  d. 执行以下命令查看路由规则。

  ```
  ip rule list
  ```

  查询结果如下所示：

  ```
  [root@iZ     fag9zZ ~]# ip rule list
  0:      from all lookup local
  32765:  from 192.168.3.11 lookup 101
  32766:  from all lookup main
  32767:  from all lookup default
  [root@iZ     fag9zZ ~]#
  ```

- 如果需要为ECS实例的弹性网卡配置多次路由，请执行以下操作。

  > **说明**
  > ECS实例重启后，配置的弹性网卡路由不会失效。

  a. 执行以下命令打开/etc/rc.local配置文件。

  ```
  vi /etc/rc.local
  ```

  b. 在配置文件末尾，按i进入编辑模式。

c. 在配置文件末尾，添加以下信息。

```
ip -4 route add default via 192.168.3.13 dev eth1 table 101
ip -4 rule add from 192.168.3.11 lookup 101
```

> **说明**
>
> 本文以一块辅助弹性网卡为例，查看到辅助弹性网卡的metric值大于主网卡的metric值，路由优先级低于主网卡，不需要重新规划网卡的metric值，保持默认配置即可。如有多块辅助弹性网卡，请将规划metric值的命令也添加到配置文件中。关于规划metric值的具体命令，请参见配置网卡路由。

d. 按下Esc键，输入:wq并回车以保存并关闭文件。

e. 执行以下命令修改/etc/rc.d/rc.local配置文件的可执行权限。

```
chmod +x /etc/rc.d/rc.local
```

> **说明**
>
> 由于/etc/rc.local配置文件是/etc/rc.d/rc.local配置文件的软链接，因此修改配置文件的权限时需要修改/etc/rc.d/rc.local配置文件的权限。执行 `ls -l /etc/rc.local` 命令可以查看到/etc/rc.local配置文件是/etc/rc.d/rc.local配置文件的软链接。

步骤七：测试网络连通性

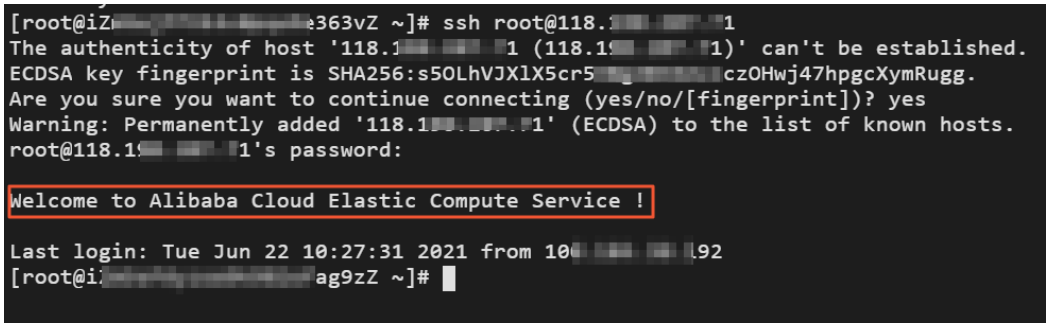
完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本操作以本地Linux设备远程连接ECS实例为例。

> **说明**

远程连接ECS实例，请确认ECS实例的安全组已放行SSH（22）端口。更多信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行 `ssh root@公网IP` 命令，然后输入ECS实例的登录密码，查看是否可以远程连接到实例。

   若界面上出现 `Welcome to Alibaba Cloud Elastic Compute Service!` 时，表示您已经成功连接到实例。



完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在ECS实例上查看公网出口IP为例。

1. 登录ECS实例。
2. 执行 `curl https://myip.ipip.net` 查看公网出口IP。

   若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。

```
[root@iZm5e                ag9zZ ~]# curl https://myip.ipip.net
当前 IP: 118.      9  来自于: 中国 山东 青岛  阿里云/电信/联通/移动/教育网
[root@iZm5e                g9zZ ~]#
```

4.3. 为已绑定EIP的ECS实例统一公网出口IP

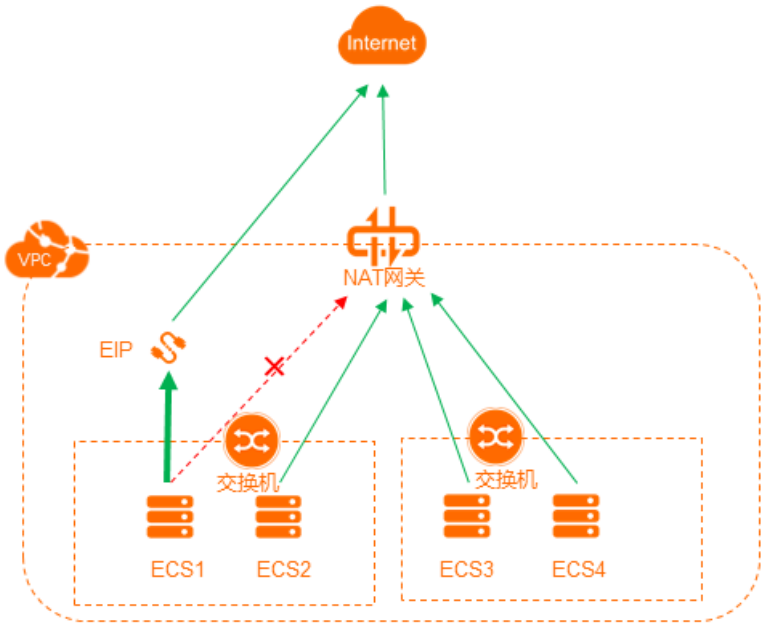
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为已绑定EIP的ECS实例统一公网出口IP。

前提条件

绑定了EIP的ECS实例所在的VPC已经配置了SNAT功能。更多信息，请参见创建和管理SNAT条目。

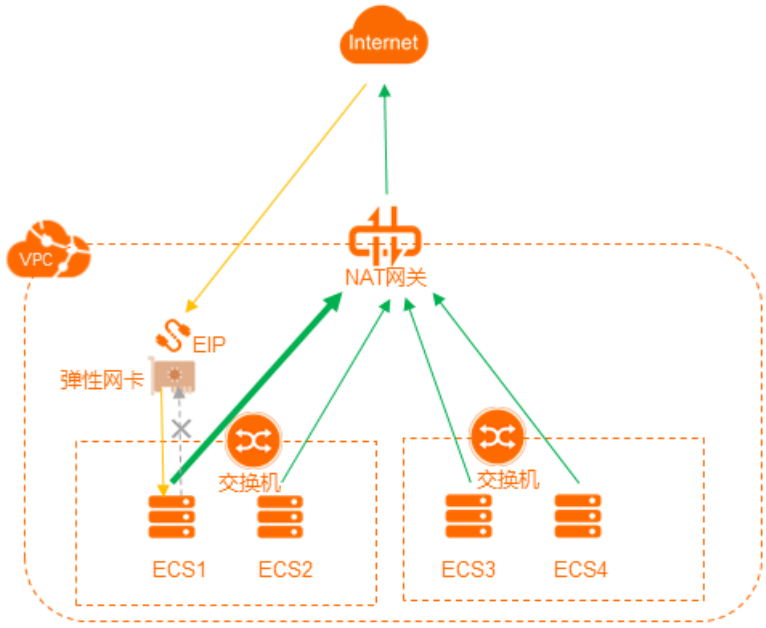
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经绑定了EIP，这些ECS实例会优先通过绑定的EIP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为绑定了EIP的ECS实例单独分配一块弹性网卡，并将EIP绑定到弹性网卡，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一：创建弹性网卡

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。

   > **说明** 弹性网卡的地域必须与ECS实例的地域相同。

4. 在**弹性网卡**页面，单击**创建弹性网卡**。
5. 在**创建弹性网卡**对话框，根据以下信息配置弹性网卡，然后单击**确定**。
   - **网卡名称**：输入弹性网卡的名称。
   - **专有网络**：选择ECS实例所在的专有网络。
   - **交换机**：选择ECS实例所在可用区的交换机。
   - **主私网IP**（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。本文不指定主私网IP。
   - **辅助私网IP**（可选）：单击相应选项进行设置。本文选择**不设置**。
   - **安全组**：选择当前专有网络的一个安全组。

   更多参数信息，请参见创建弹性网卡。

步骤二：将弹性网卡绑定到ECS实例

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。

4. 在**弹性网卡**页面，找到目标弹性网卡，然后在**操作**列单击**绑定实例**。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击**确定**。

步骤三：将EIP与ECS实例解绑

1. 登录弹性公网IP管理控制台。
2. 选择EIP的地域。
3. 在**弹性公网IP**页面，找到目标EIP，然后在**操作**列单击**解除绑定**。
4. 在弹出的对话框中，单击**确定**。

步骤四：将EIP绑定到弹性网卡

1. 登录弹性公网IP管理控制台。
2. 选择EIP的地域。
3. 在**弹性公网IP**页面，找到目标EIP，然后在**操作**列单击**绑定资源**。
4. 在**绑定弹性公网IP至资源**对话框，根据以下信息绑定EIP至弹性网卡，然后单击**确定**。
   - **实例类型**：选择辅助弹性网卡。
   - **资源组**（可选）：选择该EIP所属的资源组。本文选择默认资源组。
   - **绑定模式**（可选）：选择EIP绑定模式。本文选择**普通模式**。
   - **选择要绑定的**：选择要绑定的辅助弹性网卡。

步骤五：配置弹性网卡路由

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 查看ECS实例的弹性网卡信息如下图所示。

4. 远程登录ECS实例，更多信息，请参见ECS连接方式概述。
5. 执行以下命令查看弹性网卡信息。

```
ip a
```

```
[root@iZ[redacted]efag9zZ ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:04:40:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.10/28 brd 192.168.3.15 scope global dynamic noprefixroute eth0
       valid_lft 314948898sec preferred_lft 314948898sec
    inet6 fe80::216:3eff:fe04:404d/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:04:7e:50 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.11/28 brd 192.168.3.15 scope global dynamic noprefixroute eth1
       valid_lft 315294873sec preferred_lft 315294873sec
    inet6 fe80::f25d:3a11:4152:72d6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@iZ[redacted]2efag9zZ ~]#
```

经过查看，得到ECS实例弹性网卡的信息如下：

eth0为主网卡，对应的私网地址是192.168.3.10。

eth1为辅助弹性网卡，对应的私网地址是192.168.3.11，公网地址是118.190.XX.XX。

6. 按您的需要规划路由表里每块弹性网卡的默认路由metric值。

   执行以下命令，查看Gateway和metric值。

   ```
   route -n
   ```

   ```
   [root@[redacted]22 ~]# route -n
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   0.0.0.0         192.168.3.13    0.0.0.0         UG    100    0        0 eth0
   0.0.0.0         192.168.3.13    0.0.0.0         UG    101    0        0 eth1
   192.168.3.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
   192.168.3.0     0.0.0.0         255.255.255.0   U     101    0        0 eth1
   ```

   > **说明** 本文以一块辅助弹性网卡为例，查看到辅助弹性网卡的metric值大于主网卡的metric值，路由优先级低于主网卡，不需要执行重新规划网卡的metric值，保持默认配置即可。如有多块辅助弹性网卡，请根据实际情况配置，具体操作，请参见在Alibaba Cloud Linux 2、CentOS 7系统中配置路由。

7. 创建路由表并配置策略路由。

i. 如果需要为ECS实例的弹性网卡配置单次策略路由，请执行以下操作。

> **说明** ECS实例重启后，配置的弹性网卡路由会失效。

a. 执行以下命令创建路由表。

```
ip -4 route add default via 192.168.3.13 dev eth1 table 101
```

> **说明** 建议路由表名称和网卡的默认路由metric取值保持一致，如本例中的*101*。

b. 执行以下命令检查路由表是否创建成功。

```
ip route list table 101
```

查询结果如下所示：

```
[root@iZm5ef      g9zZ ~]# ip route list table 101
default via 192.168.3.13 dev eth1
[root@iZm5ef      g9zZ ~]#
```

c. 执行以下命令创建策略路由。

```
ip -4 rule add from 192.168.3.11 lookup 101
```

d. 执行以下命令查看路由规则。

```
ip rule list
```

查询结果如下所示：

```
[root@iZ      fag9zZ ~]# ip rule list
0:      from all lookup local
32765:  from 192.168.3.11 lookup 101
32766:  from all lookup main
32767:  from all lookup default
[root@iZ      fag9zZ ~]#
```

ii. 如果需要为ECS实例的弹性网卡配置多次路由，请执行以下操作。

> **说明** ECS实例重启后，配置的弹性网卡路由不会失效。

a. 执行以下命令打开/etc/rc.local配置文件。

```
vi /etc/rc.local
```

b. 在配置文件末尾，按i进入编辑模式。

c. 在配置文件末尾，添加以下信息。

```
ip -4 route add default via 192.168.3.13 dev eth1 table 101
ip -4 rule add from 192.168.3.11 lookup 101
```

> **说明** 本文以一块辅助弹性网卡为例，查看到辅助弹性网卡的metric值大于主网卡的metric值，路由优先级低于主网卡，不需要重新规划网卡的metric值，保持默认配置即可。如有多块辅助弹性网卡，请将规划metric值的命令也添加到配置文件中。关于规划metric值的具体命令，请参见在Alibaba Cloud Linux 2、CentOS 7系统中配置路由。

d. 按下*Esc*键，输入 `:wq` 并回车以保存并关闭文件。

e. 执行以下命令修改/etc/rc.d/rc.local配置文件的可执行权限。

```
chmod +x /etc/rc.d/rc.local
```

> **说明** 由于/etc/rc.local配置文件是/etc/rc.d/rc.local配置文件的软链接，因此修改配置文件的权限时需要修改/etc/rc.d/rc.local配置文件的权限。执行 `ls -l /etc/rc.local` 命令可以查看到/etc/rc.local配置文件是/etc/rc.d/rc.local配置文件的软链接。

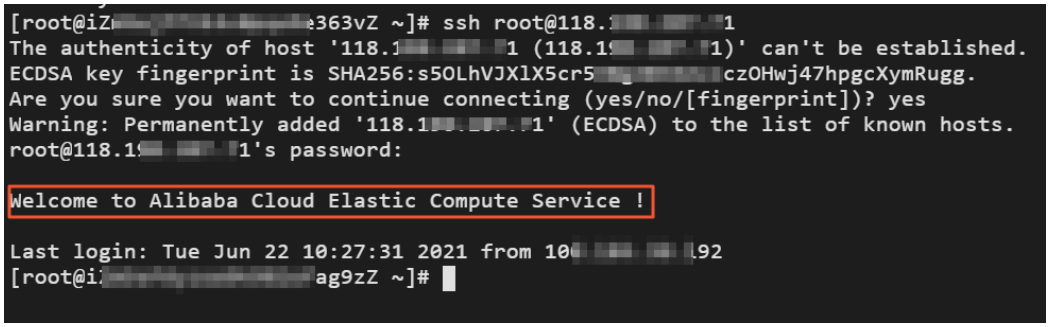
步骤六：测试网络连通性

完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本文以本地Linux设备远程连接ECS实例为例。

> **说明** 远程连接ECS实例，请确认ECS实例的安全组已放行SSH（22）端口。更多信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行 `ssh root@公网IP` 命令，然后输入ECS实例的登录密码，查看是否可以远程连接到实例。若界面上出现以下回显信息，表示您已经成功连接到实例。

```
Welcome to Alibaba Cloud Elastic Compute Service!
```



完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在ECS实例上查看公网出口IP为例。

1. 登录ECS实例。
2. 执行 `curl https://myip.ipip.net` 查看公网出口IP。若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。

4.4. 为设置了DNAT IP映射的ECS实例统一公网出口IP

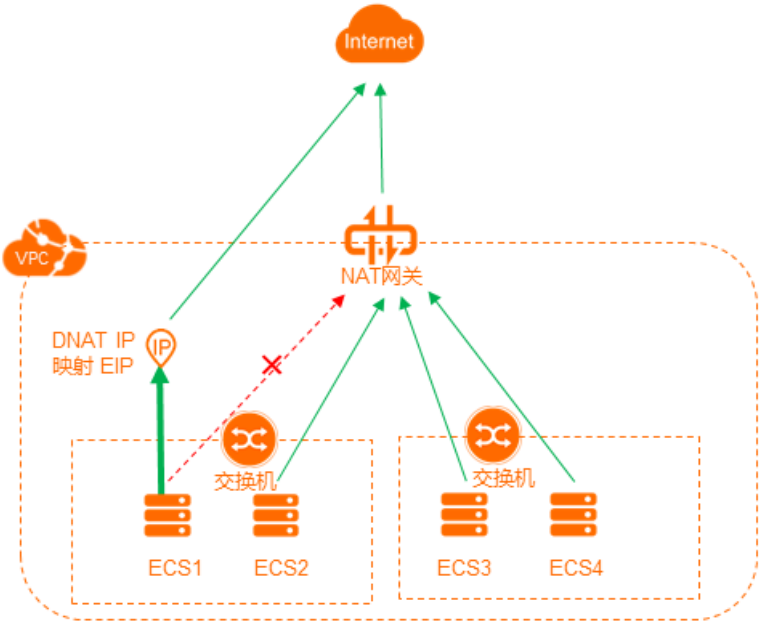
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为设置了DNAT IP映射的ECS实例统一公网出口IP。

前提条件

设置了DNAT IP映射的ECS实例所在的VPC已经配置了SNAT功能。详细信息，请参见创建和管理SNAT条目。

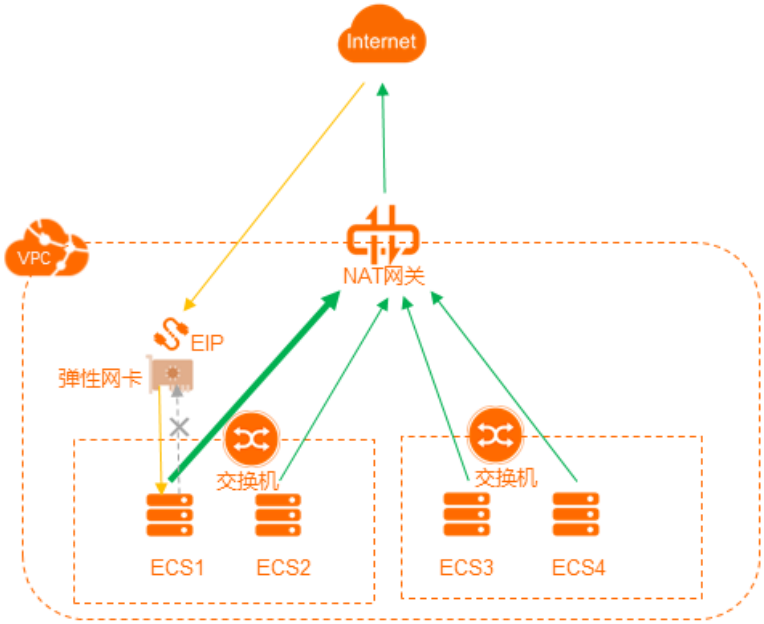
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经设置了DNAT IP映射（IP映射即所有端口映射），这些ECS实例会优先通过DNAT条目中的公网IP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能代理访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为ECS实例单独分配一块弹性网卡，然后移除NAT网关中的DNAT IP映射条目并创建新的DNAT条目，建立NAT网关上的公网IP与弹性网卡的映射关系，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一：创建弹性网卡

1. 登录云服务器ECS管理控制台。

2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。

> **说明** 弹性网卡的地域必须与ECS实例的地域相同。

4. 在**弹性网卡**页面，单击**创建弹性网卡**。
5. 在**创建弹性网卡**对话框，根据以下信息配置弹性网卡，然后单击**确定**。
   - **网卡名称**：输入弹性网卡的名称。
   - **专有网络**：选择ECS实例所在的专有网络。
   - **交换机**：选择ECS实例所在可用区的交换机。
   - **主私网IP**（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。本文不指定主私网IP。
   - **辅助私网IP**（可选）：单击相应选项进行设置。本文选择**不设置**。
   - **安全组**：选择当前专有网络的一个安全组。

   更多参数信息，请参见创建弹性网卡。

步骤二：将弹性网卡绑定到ECS实例

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择**网络与安全 > 弹性网卡**。
3. 选择弹性网卡的地域。
4. 在**弹性网卡**页面，找到目标弹性网卡，然后在**操作**列单击**绑定实例**。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击**确定**。

步骤三：删除DNAT IP映射

1. 登录NAT网关管理控制台。
2. 选择NAT网关的地域。
3. 在**NAT网关**页面，找到目标NAT网关实例，单击**操作**列下的**设置DNAT**。
4. 在**DNAT管理**页签，找到目标DNAT条目，单击**操作**列下的**删除**。
5. 在弹出的对话框中，单击**确定**。

步骤四：创建DNAT条目

完成以下操作，创建DNAT条目，建立NAT网关上的公网IP与弹性网卡的映射关系。

1. 登录NAT网关管理控制台。
2. 在**NAT网关**页面，找到目标NAT网关实例，单击**操作**列下的**设置DNAT**。
3. 在**DNAT管理**页签，单击**创建DNAT条目**。
4. 在**创建DNAT条目**页面，根据以下信息配置DNAT条目，然后单击**确定创建**。
   - **选择公网IP地址**：选择一个可用的公网IP。
   - **选择私网IP地址**：通过ECS或弹性网卡进行选择。
   - **端口设置**：选择**任意端口**。

- **条目名称**：输入DNAT条目的名称。

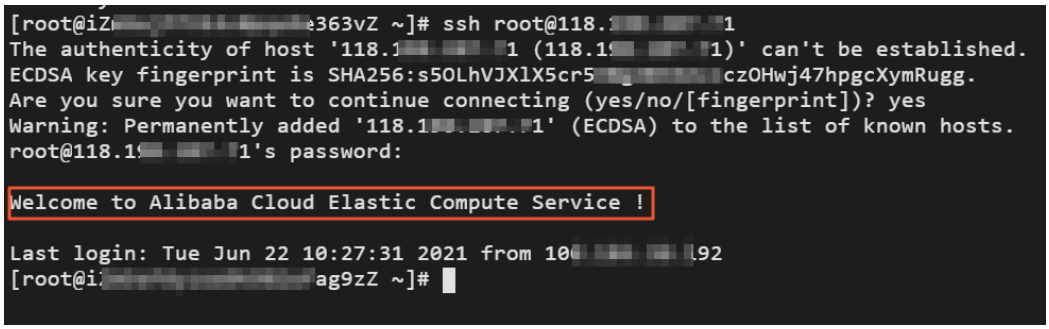
步骤五：测试网络连通性

完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本文以本地Linux设备远程连接ECS实例为例。

> **说明** 远程连接ECS实例，请确认ECS实例的安全组已放行SSH（22）端口。更多信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行 `ssh root@公网IP` 命令，然后输入ECS实例的登录密码，查看是否可以远程连接到实例。若界面上出现以下回显信息，表示您已经成功连接到实例。

```
Welcome to Alibaba Cloud Elastic Compute Service!
```



完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在ECS实例上查看公网出口IP为例。

1. 登录ECS实例。
2. 执行 `curl https://myip.ipip.net` 查看公网出口IP。若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。

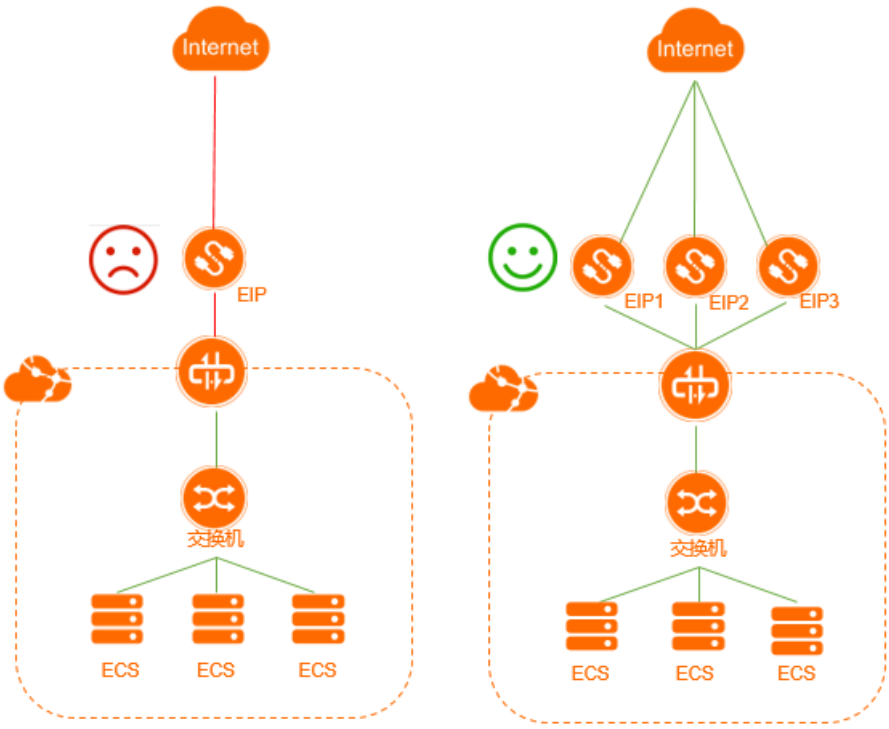
5.创建SNAT IP地址池

您可以在创建SNAT条目时，将多个EIP加入到一个SNAT地址池。ECS实例可以随机通过SNAT地址池中的EIP访问互联网。创建SNAT条目时，您可以将多个EIP加入同一个SNAT地址池，ECS实例可以灵活使用SNAT地址池中的EIP访问公网。

背景信息

公网NAT网关是一款企业级的VPC公网网关，提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。创建SNAT条目时，如果您只为指定的VPC、交换机或ECS实例配置1个EIP，当ECS实例负载激增时，1个EIP可能无法支撑巨大的访问量，从而导致业务访问中断等问题。

为了解决上述场景中的问题，您可以选择添加多个EIP到一个SNAT地址池中，当ECS实例主动发起对外的访问连接时，ECS实例会随机通过SNAT地址池中的EIP访问互联网。

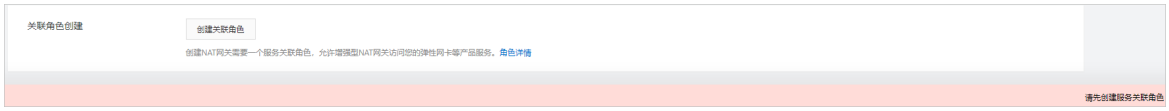


前提条件

- 您已创建专有网络和交换机。具体操作，请参见搭建IPv4专有网络。
- 您已申请待加入到SNAT地址池的EIP，本文以申请按量付费EIP为例。具体操作，请参见申请EIP。
- 您已申请按量计费类型的共享带宽。具体操作，请参见创建共享带宽实例。

步骤一：创建公网NAT网关

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，单击**创建NAT网关**。
3. 首次使用NAT网关时，在创建公网NAT网关页面**关联角色创建**区域，单击**创建关联角色**。角色创建成功后即可创建NAT网关。



关于NAT网关服务关联角色的更多信息，请参见服务关联角色。

4. 在创建公网NAT网关页面，配置以下购买信息，然后单击**立即购买**。

配置	说明
付费模式	默认选择为**按量付费**，即一种先使用后付费的付费模式。更多信息，请参见公网NAT网关计费。
所属地域	选择需要创建公网NAT网关的地域。
所属专有网络	选择公网NAT网关所属的VPC。创建后，不能修改公网NAT网关所属的VPC。
关联交换机	选择公网NAT网关实例所属的交换机。
计费类型	默认选择为**按使用量计费**，即按公网NAT网关实际使用量收费。更多信息，请参见公网NAT网关计费。
计费周期	默认选择为**按小时**，即按使用量计费公网NAT网关的计费周期为1小时，不足1小时按1小时计算。
实例名称	设置公网NAT网关实例的名称。 实例名称长度为2~128个字符，以英文大小字母或中文开头，可包含数字、下划线（_）和短划线（-）。
访问模式	选择公网NAT网关的访问模式。支持以下两种模式： ○ **VPC全通模式（SNAT）**：选择了VPC全通模式，在公网NAT网关创建成功后当前VPC内所有实例即可通过该公网NAT网关访问公网。 选择**VPC全通模式（SNAT）**后，您需要配置弹性公网IP（Elastic IP Address，简称EIP）的相关信息。 ○ **稍后配置**：如需稍后配置或有更多配置需求，可在购买完成后，前往控制台进行配置。 选择**稍后配置**，则只购买公网NAT网关实例。 本文选择**稍后配置**。

5. 在**确认订单**页面确认公网NAT网关的配置信息，选中服务协议并单击**确认订单**。
当出现**恭喜，购买成功！**的提示后，说明您创建成功。

步骤二：将多个EIP绑定到公网NAT网关

1. 登录NAT网关管理控制台。

2. 在顶部菜单栏处，选择公网NAT网关的地域。
3. 在**公网NAT网关**页面，找到目标公网NAT网关实例，然后在**弹性公网IP**列单击**立即绑定**。
4. 在**绑定弹性公网IP**对话框，配置以下参数，然后单击**确定**。

配置	说明
所在资源组	选择EIP所在的资源组。
选择弹性公网IP	本文选择**从已有弹性公网IP中选择**，然后在列表中选择已创建的按量付费EIP。

5. 重复以上步骤绑定更多EIP。

步骤三：将多个EIP加入共享带宽

1.
2. 在顶部菜单栏处，选择EIP的地域。
3. 在**弹性公网IP**页面，找到目标EIP，然后在**操作**列选择 > **加入共享带宽**。
4. 选择已创建的共享带宽，然后单击**确定**。
5. 重复以上步骤将多个EIP加入共享带宽。

步骤四：创建SNAT条目

完成以下操作，创建SNAT条目，将多个EIP加入到一个SNAT地址池。

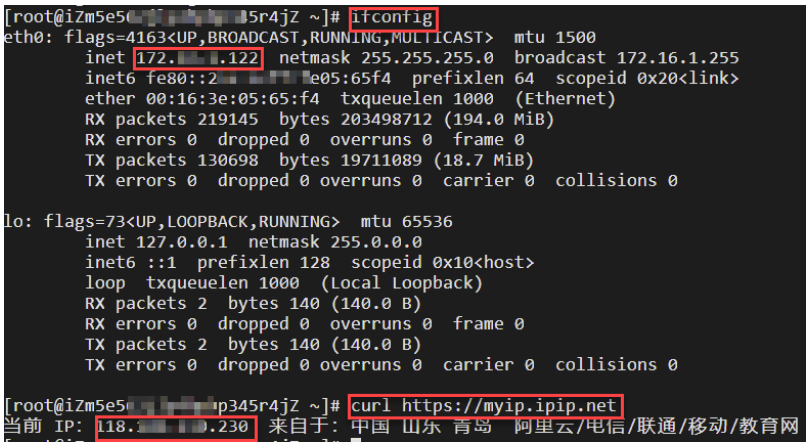
1. 登录NAT网关管理控制台。
2. 在顶部菜单栏处，选择公网NAT网关的地域。
3. 在**公网NAT网关**页面，找到目标NAT公网网关实例，然后在**操作**列单击**设置SNAT**。
4. 在**SNAT管理**页签，单击**创建SNAT条目**。
5. 在**创建SNAT条目**页面，根据以下信息配置SNAT条目，然后单击**确定创建**。

配置	说明
SNAT条目粒度	本文选择**交换机粒度**。
选择交换机	选择VPC中的交换机。该交换机下所有ECS实例都将通过SNAT功能进行公网访问。
交换机网段	显示该交换机的网段。
选择公网IP地址	选择用来提供互联网访问的公网IP。本文选择**使用多IP**。
使用多IP	从**公网IP**列表中选择已经被加入到选定共享带宽中的EIP。
条目名称	输入SNAT条目的名称。

步骤五：测试访问

1. 登录设置了SNAT规则的ECS实例。具体操作，请参见ECS实例连接方式概述。
2. 执行 `ifconfig` 查看ECS实例的私网IP。
3. 执行 `curl https://myip.ipip.net` 命令，查看ECS实例访问互联网的源IP地址。

经测试，该IP地址即为SNAT IP地址池中随机的EIP。

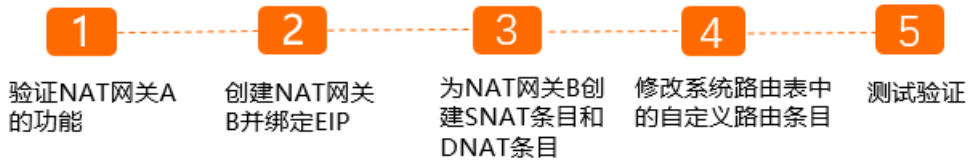


6.在同一个VPC内切换公网NAT网关实例

NAT网关控制台不支持在同一个VPC内直接切换公网NAT网关实例。您可以通过在同一个VPC内新建一个公网NAT网关，再修改目标网段为0.0.0.0/0的路由条目的方式实现公网NAT网关所属交换机或私网IP地址的变更。

操作流程

本文以在同一个VPC内切换公网NAT网关来变更公网NAT网关所属交换机为例进行介绍。



前提条件

开始前，请确保满足以下条件：

- 您已经在华东1（杭州）地域创建了一个VPC（名称为VPC1），并在该VPC中创建了两个交换机（名称为VSW1，位于可用区B；名称为VSW2，位于可用区H）。具体操作，请参见搭建IPv4专有网络。
- 您已经在交换机VSW1创建了一个名称为ECS1的ECS实例且不配置固定公网IP地址。具体操作，请参见使用向导创建实例。
- 您已经在交换机VSW1创建了一个公网NAT网关A实例，且已配置了VPC1的SNAT条目和端口映射方式的DNAT条目（私网IP地址为ECS1的IP地址，公网端口和私网端口均为22，协议类型为TCP）。

步骤一：验证NAT网关A实例的功能

1. 登录VSW1下的ECS1实例。具体操作，请参见ECS连接方式概述。
2. 执行 `ping` 命令测试网络连通性。
3. 使用 `curl myip.ipip.net` 命令探测ECS1实例的公网出口IP。

   经测试，ECS1实例公网出口IP与NAT网关A实例中SNAT条目中的IP一致，即ECS1实例通过NAT网关A实例的SNAT功能主动访问互联网。

```
[root@iZm5e5[illegible]345r4jZ ~]# curl myip.ipip.net
当前 IP: 118.[illegible].230  来自于: 中国 山东 青岛  阿里云/电信/联通/移动/教育网
```

4. 登录本地Linux设备。
5. 执行 `ssh root@公网IP` 命令，此处的公网IP即为NAT网关A实例的DNAT条目中的公网IP地址，然后输入ECS1实例的登录密码，查看是否可以远程连接到实例。

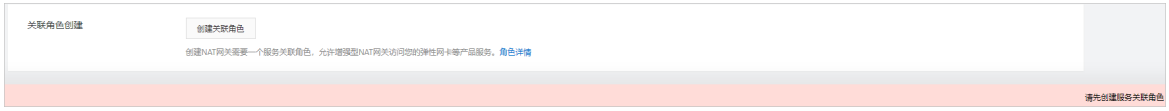
   若界面上出现Welcome to Alibaba Cloud Elastic Compute Service!时，表示您已经成功连接到实例，即ECS1实例通过NAT网关A实例的DNAT功能提供公网访问能力。

```
[root@iZm5e6[illegible]jfzdlZ ~]# ssh 118.[illegible].230
The authenticity of host '118.[illegible].230 (118.[illegible].230)' can't be established.
ECDSA key fingerprint is SHA256:uyobLEZ[illegible]md4f/sqWRrcnqjL[illegible]pNQnCyBzNw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '118.[illegible].230' (ECDSA) to the list of known hosts.
root@118.[illegible].230's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Thu Aug 12 17:26:53 2021 from 100.[illegible].237
[root@iZm5e5[illegible]45r4jZ ~]#
```

步骤二：创建NAT网关B实例并绑定EIP

NAT网关B实例关联的交换机为VSW2。

1. 登录NAT网关管理控制台。
2. 在**公网NAT网关**页面，单击**创建NAT网关**。
3. 首次使用NAT网关时，在创建公网NAT网关页面**关联角色创建**区域，单击**创建关联角色**。角色创建成功后即可创建NAT网关。



关于NAT网关服务关联角色的更多信息，请参见服务关联角色。

4. 在创建公网NAT网关页面，配置以下购买信息，然后单击**立即购买**。

配置	说明
付费模式	默认选择为**按量付费**，即一种先使用后付费的付费模式。更多信息，请参见公网NAT网关计费。
所属地域	选择需要创建公网NAT网关的地域。
所属专有网络	选择公网NAT网关所属的VPC。创建后，不能修改公网NAT网关所属的VPC。
关联交换机	选择公网NAT网关实例所属的交换机。
计费类型	默认选择为**按使用量计费**，即按公网NAT网关实际使用量收费。更多信息，请参见公网NAT网关计费。
计费周期	默认选择为**按小时**，即按使用量计费公网NAT网关的计费周期为1小时，不足1小时按1小时计算。
实例名称	设置公网NAT网关实例的名称。 实例名称长度为2~128个字符，以英文大小字母或中文开头，可包含数字、下划线（_）和短划线（-）。
访问模式	选择公网NAT网关的访问模式。支持以下两种模式： ○ **VPC全通模式（SNAT）**：选择了VPC全通模式，在公网NAT网关创建成功后当前VPC内所有实例即可通过该公网NAT网关访问公网。 选择**VPC全通模式（SNAT）**后，您需要配置弹性公网IP（Elastic IP Address，简称EIP）的相关信息。 ○ **稍后配置**：如需稍后配置或有更多配置需求，可在购买完成后，前往控制台进行配置。 选择**稍后配置**，则只购买公网NAT网关实例。 本文选择**稍后配置**。

5. 在**确认订单**页面确认公网NAT网关的配置信息，选中服务协议并单击**确认订单**。
   当出现**恭喜，购买成功！**的提示后，说明您创建成功。
6. 返回**公网NAT网关**页面，找到已创建的NAT网关B实例，然后在**弹性公网IP**列单击**立即绑定**。
7. 在**绑定弹性公网IP**对话框，配置以下参数，然后单击**确定**。

   选择弹性公网IP：选择要绑定到公网NAT网关的EIP。本文选择**新购弹性公网IP并绑定**。

步骤三：为NAT网关B实例创建SNAT条目和DNAT条目

为NAT网关B实例创建的SNAT条目和DNAT条目除了公网IP地址外，其余的规则需要与NAT网关A实例的相同。

1. 登录NAT网关管理控制台。
2. 在顶部菜单栏，选择公网NAT网关的地域。
3. 在**公网NAT网关**页面，找到目标公网NAT网关实例，然后在**操作**列单击**设置SNAT**。
4. 在**SNAT管理**页签，单击**创建SNAT条目**。
5. 在**创建SNAT条目**页面，配置以下参数，然后单击**确定创建**。

配置	说明
SNAT条目粒度	选择SNAT条目的粒度。 本文选择**VPC粒度**，即NAT网关B实例所属VPC1下的所有ECS实例都可以通过配置的SNAT规则访问互联网。
选择公网IP地址	选择用来提供互联网访问的公网IP。 本文选择**使用单IP**，然后在下拉列表中选择绑定到NAT网关B实例的EIP。
条目名称	SNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

6. 返回**公网NAT网关**页面，找到已创建的NAT网关B实例，然后在**操作**列单击**设置DNAT**。
7. 在**DNAT管理**页签，单击**创建DNAT条目**。
8. 在**创建DNAT条目**页面，配置以下参数，然后单击**确定创建**。

配置	说明
选择公网IP地址	选择要提供互联网通信的公网IP。本文选择绑定到NAT网关B实例的EIP。
选择私网IP地址	选择要通过DNAT规则进行公网通信的ECS实例。 本文选择**通过ECS或弹性网卡进行选择**，然后在下拉列表中选择ECS1。
端口设置	选择DNAT映射的方式。 本文选择**具体端口**，即DNAT端口映射方式，然后**公网端口**输入*22*，**私网端口**输入*22*，**协议类型**选择**TCP**。

配置	说明
条目名称	输入DNAT条目的名称。 名称长度为2~128个字符，以大小写字母或中文开头， 可包含数字、下划线（_）和短划线（-）。

步骤四：修改系统路由表中的自定义路由条目

在VPC内创建第一个公网NAT网关时，系统会在VPC系统路由表中自动添加一条目标网段为0.0.0.0/0，下一跳为公网NAT网关的路由条目，用于将流量路由到该公网NAT网关。因此创建了NAT网关B实例后，VPC系统路由表中并没有目标网段为0.0.0.0/0，下一跳为NAT网关B实例的路由条目，NAT网关B实例无法使用。您必须手动修改VPC系统路由表中目标网段为0.0.0.0/0的路由条目指向NAT网关B实例，才能完成将VPC中的NAT网关A实例切换为NAT网关B实例。

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VPC1的路由表，然后单击路由表的ID。
5. 选择**路由条目列表 > 自定义路由条目**页签，找到目标网段为0.0.0.0/0，下一跳指向NAT网关A实例的自定义路由条目，然后在**操作**列单击**删除**。
6. 在**删除路由条目**对话框，单击**确定**。
7. 单击**添加路由条目**，在**添加路由条目**面板，根据以下信息配置自定义路由条目，然后单击**确定**。

配置	说明
名称	输入路由条目的名称。 名称长度为2~128个字符之间，以英文字母或中文开头，可包含数字、短划线（-）和下划线（_）。
目标网段	输入需要将流量转发到的目标网段。本文选择**IPv4网段**，然后输入*0.0.0.0/0*。
下一跳类型	选择下一跳的类型。本文选择**NAT网关**。
NAT网关	选择下一跳实例。本文选择NAT网关B实例。

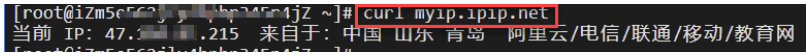
> **说明** 路由条目切换后，存量的访问连接需要重连之后才能恢复，建议您在业务低峰期执行路由条目切换操作。

步骤五：测试验证

验证NAT网关A实例的功能是否已经切换到NAT网关B实例。本文是以变更NAT网关所属交换机为例进行介绍，在操作的过程中，同时完成了变更NAT网关的私网IP地址。如果您需要通过在同一个交换机下切换NAT网关来变更其私网IP地址，也可以参考本文进行操作。

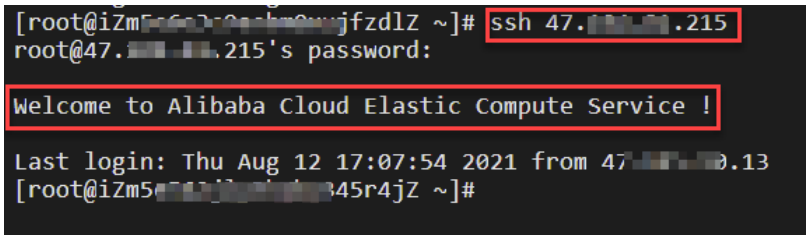
1. 登录VSW1下的ECS1实例。
2. 执行`ping`命令测试网络连通性。
3. 使用`curl myip.ipip.net`命令探测ECS1实例的公网出口IP。

经测试，ECS1实例公网出口IP与NAT网关B实例中SNAT条目中的IP一致，即ECS1实例通过NAT网关B实例的SNAT功能主动访问互联网。



4. 登录本地Linux设备。
5. 执行 `ssh root@公网IP` 命令，此处的公网IP即为NAT网关B实例的DNAT条目中的公网IP地址，然后输入ECS1实例的登录密码，查看是否可以远程连接到实例。

   若界面上出现Welcome to Alibaba Cloud Elastic Compute Service!时，表示您已经成功连接到实例，即ECS1实例通过NAT网关B实例的DNAT功能提供公网访问能力。



7.自建SNAT网关平滑迁移到NAT网关

通过使用路由表的最长匹配原则，您可以将搭建在ECS实例的SNAT网关平滑迁移至阿里云NAT网关。

背景信息

如果您已经在VPC中基于ECS搭建了SNAT网关，又想将架构切换为基于NAT网关实现的SNAT，您可以将原有自建SNAT网关拆除，再进行NAT网关的创建和配置。但该操作会导致SNAT功能中断一段时间。

本教程的迁移方法利用路由表的一些特性（主要是“最长匹配原则”），实现从自建SNAT网关到阿里云NAT网关的无缝切换。切换过程中，不会出现SNAT功能不可用，仅在切换的一瞬间发生已有TCP连接的断开，应用进行重连即可。

本操作中作为示例的VPC和ECS配置如下：

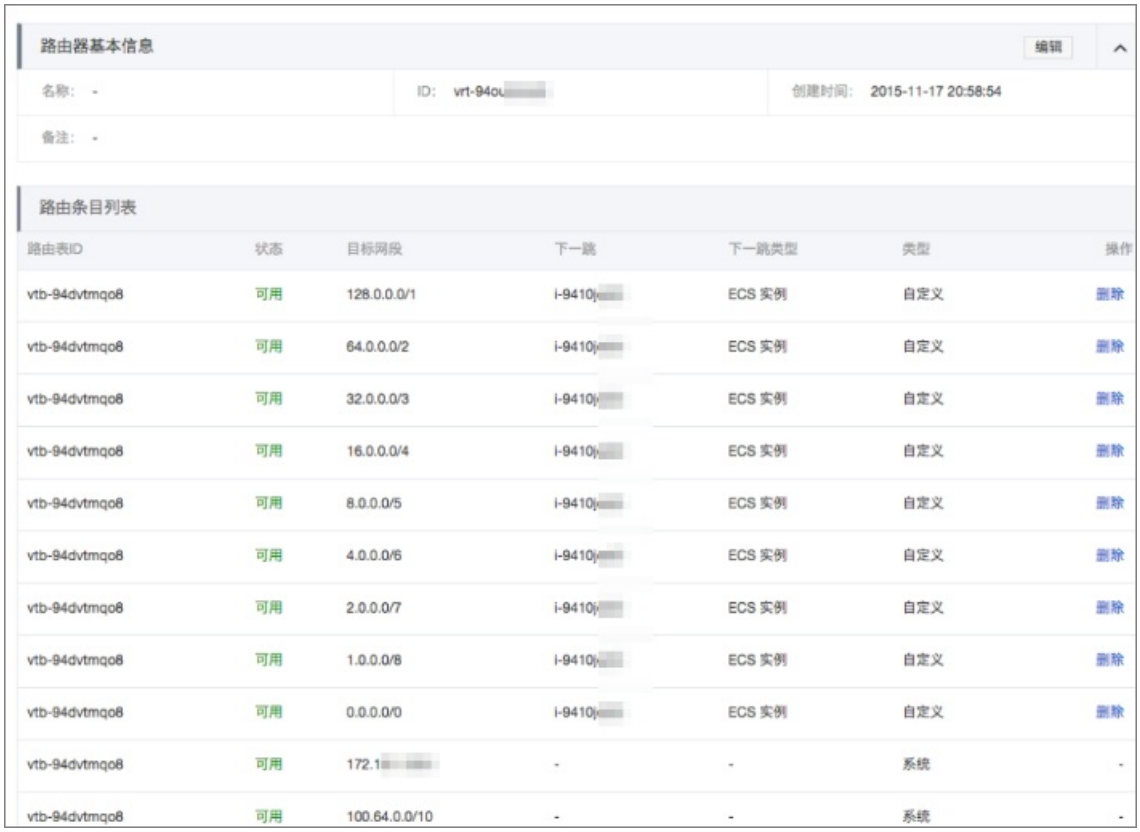
- VPC中有两个ECS实例：
  - i-9410jxxxx配置了自建的SNAT网关。这台ECS上绑定了一个EIP，并且开启了转发服务、配置了iptables规则以实现SNAT转发。
  - i-94kjwxxxx为需要SNAT功能来访问互联网的服务器。
- VPC的路由器上，添加了一条自定义路由（目标网段为0.0.0.0/0），将公网访问请求转发给i-9410jxxxx。

操作步骤

1. 在VPC中添加8条路由条目，对原有路由进行覆盖。

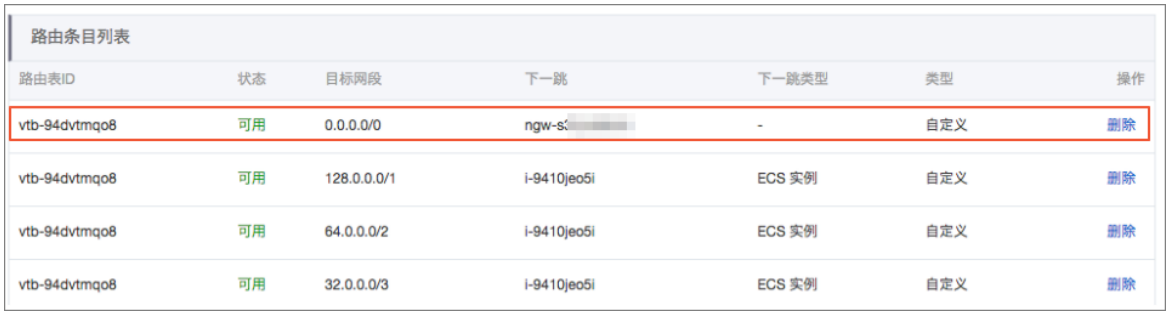
   路由条目的目标网段分别为1.0.0.0/8、2.0.0.0/7、4.0.0.0/6、8.0.0.0/5、16.0.0.0/4、32.0.0.0/3、64.0.0.0/2、128.0.0.0/1，下一跳均为i-9410jxxxx。

   由于路由表按照最长匹配原则，会优先匹配子网掩码最长的路由条目；而去往任意IP地址的数据包，都会匹配到这8条中的一条；因此，0.0.0.0/0这条路由实际上已经不再有用了。



2. 删除目标网段为0.0.0.0/0的路由条目。
3. 创建NAT网关。

   创建NAT网关后，系统会自动添加一条0.0.0.0/0的路由，指向NAT网关。



4. 绑定弹性公网IP。

   > 注意　确保EIP的带宽和自建NAT的带宽一致。因为只要在NAT网关添加了SNAT规则，SNAT规则中的ECS的出公网方向的流量就会受EIP带宽的限速。

5. 配置SNAT规则。
6. 删除VPC中添加的8条路由条目，使路由器把公网访问请求不再转发给自建SNAT，而是转发给NAT网关。

   至此，已经完成了从自建SNAT网关到使用官方NAT网关的SNAT功能的全部切换流程。