

阿里云

NAT网关
SNAT

文档版本：20200928

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> <i>Instance_ID</i>
[] 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. SNAT概述	05
2. 创建SNAT条目	06
3. 修改SNAT条目	09
4. 删除SNAT条目	10
5. 使用SNAT功能实现ECS实例访问互联网	11

1.SNAT概述

NAT网关支持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。

SNAT条目

您可以通过在SNAT表中创建SNAT条目，实现代理上网功能。

每个SNAT条目由以下两部分组成：

- **交换机或ECS实例**：需要提供SNAT代理服务的交换机或ECS实例。
- **公网IP**：用来提供互联网访问的公网IP。

② 说明

- 支持选择多个公网IP，多公网IP构建SNAT IP地址池。当VPC ECS实例主动发起对外的访问连接时，VPC ECS实例会随机通过SNAT地址池中的公网IP地址访问互联网。
- 对于2017年11月3日之前账户下存在NAT带宽包的用户，SNAT条目中的公网IP为NAT带宽包提供的公网IP。

交换机粒度和ECS粒度

SNAT功能提供如下两种粒度，以实现VPC内ECS实例访问互联网。

- **交换机粒度**

选择交换机为粒度创建SNAT条目后，当指定交换机下的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务（代理上网服务），且使用的公网IP为指定的公网IP。默认情况，交换机下的所有ECS实例都可以使用配置的公网IP访问互联网。

② 说明 如果ECS实例已经持有了公网IP（例如分配了固定公网IP、绑定EIP和设置了DNAT IP映射），当该ECS实例发起互联网访问时，会优先通过持有的公网IP访问互联网，而不会使用NAT网关的SNAT功能访问互联网。如需统一公网出口IP，请参见[为已分配固定公网IP的ECS实例统一公网出口IP](#)、[为已绑定EIP的ECS实例统一公网出口IP](#)和[为设置了DNAT IP映射的ECS实例统一公网出口IP](#)。

- **ECS粒度**

选择ECS为粒度创建SNAT条目后，指定的ECS实例通过配置的公网IP访问互联网。当指定的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务（代理上网服务），且使用的公网IP为指定的公网IP。

2.创建SNAT条目

您可以使用NAT网关的SNAT功能，为专有网络中无公网IP的ECS实例提供访问互联网的代理服务。

前提条件

创建SNAT条目前，请确保满足以下条件：


- 您已经创建了NAT网关并绑定了弹性公网IP（EIP）。详细信息，请参见[创建NAT网关](#)和[绑定EIP](#)。

 **说明** 如果您在2017年11月3日之前购买过NAT带宽包，请确保NAT带宽包中有可用的公网IP。

- 如果要创建以交换机为粒度的SNAT条目，请确保NAT网关关联的VPC中已经创建了交换机。详细信息，请参见[创建交换机](#)。
- 如果要创建以ECS为粒度的SNAT条目，请确保NAT网关关联的VPC中已经创建了ECS实例。详细信息，请参见[使用向导创建实例](#)。

操作步骤

- 登录[NAT网关管理控制台](#)。
- 在顶部菜单栏处，选择NAT网关的地域。
- 在NAT网关页面，找到目标NAT网关实例，单击操作列下的设置SNAT。
- 在SNAT条目列表区域，单击创建SNAT条目。
- 在创建SNAT条目对话框，根据以下信息配置SNAT条目，然后单击确定。

配置	说明
交换机粒度：指定交换机下的ECS实例通过配置的公网IP访问互联网。	
交换机	<p>选择要访问互联网的交换机。该交换机下的所有ECS实例都将通过SNAT功能进行公网访问。</p> <p> 说明 如果ECS实例已经持有了公网IP（例如分配了固定公网IP、绑定EIP和设置了DNAT IP映射），当该ECS实例发起互联网访问时，会优先通过持有的公网IP访问互联网，而不会使用NAT网关的SNAT功能访问互联网。如需统一公网出口IP，请参见为已分配固定公网IP的ECS实例统一公网出口IP、为已绑定EIP的ECS实例统一公网出口IP和为设置了DNAT IP映射的ECS实例统一公网出口IP。</p>
交换机网段	显示交换机的网段。

配置	说明
公网IP地址	<p>选择用来提供互联网访问的公网IP。</p> <p>支持选择1个或多个公网IP，多个公网IP可以构建SNAT IP地址池。当VPC ECS实例主动发起对外的访问连接时，VPC ECS实例会随机通过SNAT地址池中的公网IP地址访问互联网。</p> <p> 说明 选择多个公网IP配置SNAT IP地址池时，需确保每个公网IP都加入到同一个共享带宽中。</p> <p>SNAT IP地址池中的公网IP具有以下限制：</p> <ul style="list-style-type: none"> 每个公网IP的最大带宽限制为200M。 每个公网IP的最大连接数为55000。 <p>为了使SNAT规则能充分利用共享带宽的带宽能力，及避免公网IP过少导致端口冲突，建议您按照以下配比关系添加公网IP：</p> <ul style="list-style-type: none"> 共享带宽的带宽峰值为1024M时，SNAT规则中的公网IP数量应至少为5个。 共享带宽的带宽峰值以1024M为基础每增加200M，SNAT规则中都应至少再新增1个公网IP。 <p> 说明</p> <ul style="list-style-type: none"> 普通型NAT网关不支持将一个公网IP同时用于DNAT条目和SNAT条目。 增强型NAT网关白名单支持将一个公网IP同时用于DNAT条目和SNAT条目。如需使用，请提交工单。
条目名称	<p>SNAT条目的名称。</p> <p>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（_）和短横线（-）。</p>
ECS粒度：指定的ECS实例通过配置的公网IP访问互联网。	
可用ECS列表	<p>选择要访问互联网的ECS实例。</p> <p>该ECS实例将通过配置的公网IP访问互联网。请确保ECS实例满足以下条件：</p> <ul style="list-style-type: none"> ECS实例的状态处于运行中。 ECS实例不具备固定公网IP且未绑定其他弹性公网IP。
ECS网段	显示ECS实例的网段。

配置	说明
公网IP地址	<p>选择用来提供互联网访问的公网IP。</p> <p>支持选择1个或多个公网IP，多个公网IP可以构建SNAT IP地址池。当VPC ECS实例主动发起对外的访问连接时，VPC ECS实例会随机通过SNAT地址池中的公网IP地址访问互联网。</p> <div><p> 说明 选择多个公网IP配置SNAT IP地址池时，需确保每个公网IP都加入到同一个共享带宽中。</p></div> <p>SNAT IP地址池中的公网IP具有以下限制：</p> <ul style="list-style-type: none">每个公网IP的最大带宽限制为200M。每个公网IP的最大连接数为55000。 <p>为了使SNAT规则能充分利用共享带宽的带宽能力，及避免公网IP过少导致端口冲突，建议您按照以下配比关系添加公网IP：</p> <ul style="list-style-type: none">共享带宽的带宽峰值为1024M时，SNAT规则中的公网IP数量应至少为5个。共享带宽的带宽峰值以1024M为基础每增加200M，SNAT规则中都应至少再新增1个公网IP。 <div><p> 说明 用于创建DNAT条目的公网IP不能再用来创建SNAT条目。</p></div>
条目名称	<p>SNAT条目的名称。</p> <p>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（_）和短横线（-）。</p>

相关文档


- [CreateSnatEntry](#)

3.修改SNAT条目

创建SNAT条目后，您可以修改SNAT条目的公网IP和名称，但您不能修改SNAT条目的交换机和ECS实例。

操作步骤

1. 登录[NAT网关管理控制台](#)。
2. 在顶部菜单栏处，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SNAT。
4. 在SNAT条目列表区域，找到目标SNAT条目，单击操作列下的编辑。
5. 在编辑SNAT条目对话框，修改SNAT条目的公网IP和名称，然后单击确定。

 **注意** 向存量SNAT条目添加或删除EIP会导致原有连接闪断，重连可以恢复，请谨慎操作。

相关文档

- [ModifySnatEntry](#)

4.删除SNAT条目

如果您不需要为VPC内无公网IP的ECS实例提供访问互联网的代理服务，您可以删除SNAT条目。

操作步骤

1. 登录[NAT网关管理控制台](#)。
2. 在顶部菜单栏处，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SNAT。
4. 在SNAT条目列表区域，找到目标SNAT条目，单击操作列下的移除。
5. 在弹出的对话框中，单击确认。

相关文档

- [DeleteSnatEntry](#)

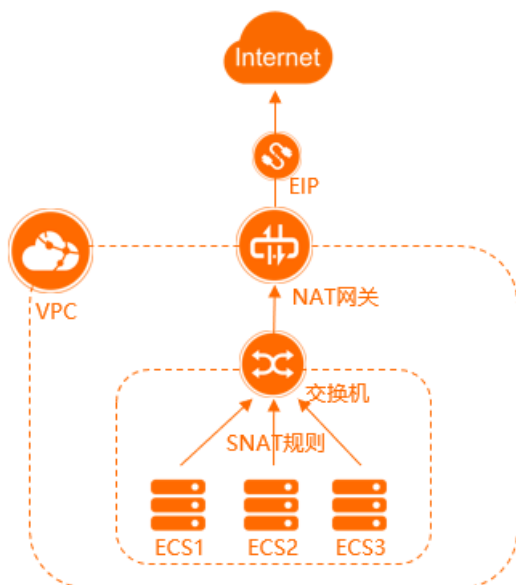
5.使用SNAT功能实现ECS实例访问互联网

本教程指导您配置NAT网关的SNAT功能，实现无公网IP的ECS实例访问互联网。

配置场景

本教程以下图场景为例。某公司在阿里云创建了VPC和交换机，交换机中创建了多个ECS实例。ECS实例均未分配固定公网IP，也未绑定弹性公网IP（EIP）。因公司业务发展，需要每台ECS实例都需要访问互联网。

您可以通过NAT网关的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。



前提条件

开始前，请确保满足以下条件：

- 您已经注册了阿里云账号。如未注册，请先完成[账号注册](#)。
- 您已经创建了专有网络（VPC）和交换机。详细信息，请参见[创建专有网络](#)。
- 您已经创建了EIP，且EIP的地域与要绑定的NAT网关的地域相同。详细信息，请参见[申请新EIP](#)。

配置步骤



步骤一：创建NAT网关

NAT网关是一款企业级的公网网关，提供NAT代理功能。在配置SNAT条目前，您需要先创建一个NAT网关实例。

完成以下操作，创建NAT网关。

1. 登录[NAT网关管理控制台](#)。

2. 在NAT网关页面，单击创建NAT网关。
3. 在创建NAT网关页面，根据以下信息配置NAT网关，然后单击立即购买并完成支付。

- 付费模式：选择NAT网关实例的付费模式。
 - 包年包月：包年包月是一种先付费后使用的付费模式。详细信息，请参见[包年包月](#)。
 - 按量付费：按量付费是一种先使用后付费的付费模式。详细信息，请参见[按量付费](#)。

本教程选择包年包月。

- 地域和可用区：选择需要创建NAT网关的地域。

② 说明 目前，除澳大利亚（悉尼）地域外的其他所有地域都已支持创建增强型NAT网关实例。

- VPC ID：选择NAT网关所属的VPC。创建NAT网关后，不能修改NAT网关所属的VPC。

② 说明 如果在VPC列表中，找不到目标VPC，请从以下方面进行排查：

- 查看该VPC是否已经配置NAT网关。一个VPC只能配置一个普通型NAT网关。
- 查看该VPC中是否存在目标网段为0.0.0.0/0的自定义路由。如果存在，请删除该路由条目。
- RAM账号不具备读取访问VPC的权限，请联系主账号进行授权。

- 交换机ID：选择NAT网关实例所属的交换机。

② 说明 仅创建增强型NAT网关时才支持选择NAT网关实例所属的交换机。

- 网关类型：选择要创建的NAT网关类型。

- 普通型
- 增强型

增强型NAT网关兼容普通型NAT网关的全部功能，并在普通型NAT网关的技术架构上作了升级，具有更优的弹性和更强的稳定性，帮助您更好的管理公网访问流量。本教程选择增强型。

- 名称：设置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（_）和短横线（-）。

- 规格：选择NAT网关的规格。

- 小型
- 中型
- 大型
- 超大型-1

NAT网关的规格会影响SNAT功能的最大连接数和每秒新建连接数，但不会影响DNAT性能。详细信息，请参见[实例规格](#)。

本教程选择小型。


- 购买数量：设置要购买NAT网关实例的数量。
- 计费周期：选择NAT网关实例的计费周期。

创建成功后，您可以在NAT网关页面查看已创建的NAT网关实例。

NAT网关									
<div>诚邀您参与阿里云控制台使用情况调研，有机会赢取精美阿里云礼品。立即填写</div> <div>随时随地安全上云，智能接入网关APP免费试用活动中。点击查看</div>									
<div>创建NAT网关 组合购买EIP 标签筛选 实例名称 请输入实例名称进行精确查询</div>									
<input type="checkbox"/>	实例ID/名称	标签	监控	最大带宽	规格/类型	专有网络	状态	付费类型	计费方式
<input type="checkbox"/>	ngw-hp3r...			5120 Mbps 申请调整	小型 增强型	vpc-hp3u...	✓ 可用	预付费 2020年9月26日 24:00:00 到期	按规格计费
<input type="checkbox"/>	设置标签								

步骤二：绑定EIP

NAT网关作为一个网关设备，需要绑定公网IP才能正常工作。创建NAT网关后，您可以为NAT网关绑定EIP。完成以下操作，为NAT网关绑定EIP。

1. 在NAT网关页面，找到步骤一创建的NAT网关实例，单击其操作列下的  > 绑定弹性公网IP。
2. 在绑定弹性公网IP对话框，根据以下信息绑定EIP，然后单击确定。
 - 可用EIP列表：选择要绑定到NAT网关的EIP。
 - 交换机：选择要添加SNAT条目的交换机。

系统会自动添加SNAT条目使交换机下的云资源可以主动访问互联网。您也可以不选择交换机，绑定EIP后手动添加SNAT条目。

本教程不选择交换机。

 说明 仅未绑定EIP的NAT网关显示该选项。

步骤三：创建SNAT条目

NAT网关的SNAT功能可以为VPC中无公网IP的ECS实例提供访问互联网的代理服务。

完成以下操作，创建SNAT条目。

1. 在NAT网关页面，找到步骤一创建的NAT网关实例，单击其操作列下的设置SNAT。
2. 在SNAT条目列表区域，单击创建SNAT条目。
3. 在创建SNAT条目对话框，配置SNAT条目。本教程以交换机粒度为例，介绍如何配置SNAT条目。
 - 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功能访问互联网。
 - 交换机网段：显示交换机的网段。
 - 公网IP地址：选择用来提供互联网访问的公网IP。


 说明 用于创建DNAT条目的公网IP不能再用来创建SNAT条目。

- 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（_）和短横线（-）。
4. 单击确定。

步骤四：测试连通性

SNAT条目配置成功后，您可以测试ECS实例的网络连通性。

 说明 请确保ECS实例的安全组规则允许ECS实例访问互联网。

本教程以Linux实例为例，测试ECS实例的连通性。

1. 登录交换机下的任意一台ECS实例。
2. 通过 `ping` 命令测试网络连通性。经测试，ECS实例可以访问互联网。

```
[root@izhp3c-574fi0iZ ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=45.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=45.3 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 45.286/45.360/45.572/0.287 ms
[root@izhp3c-574fi0iZ ~]#
```