NAT 网关

常见问题

文档版本 01

发布日期 2023-11-14

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 公网 NAT 网关

1.1 公网 NAT 网关、弹性公网 IP 带宽、VPC 内弹性云服务器与 VPC 是什么样的关系?

- VPC是虚拟私有云，通过逻辑方式进行网络隔离，提供安全、隔离的网络环境。
- 公网NAT网关能够为VPC内的弹性云服务器提供访问外网的能力。
- 弹性公网IP是可以提供互联网上合法的静态IP地址的服务，VPC的吞吐量由弹性公网IP带宽决定。
- 弹性云服务器是VPC内的运行实例，使用公网NAT网关访问外网。

1.2 公网 NAT 网关如何实现高可用性?

公网NAT网关后台已通过双机热备实现自动容灾，同时为用户提供云监控和告警服务，降低风险提高可用性。

1.3 哪些端口无法访问?

出于安全因素考虑，部分运营商会对下列端口进行拦截，导致无法访问。建议避免使用下列端口：

协议	不支持端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

1.4 弹性云服务器使用公网 NAT 网关和直接绑定弹性公网 IP 有区别吗?

公网NAT网关提供SNAT和DNAT功能，可允许多台弹性云服务器共享弹性公网IP。

弹性云服务器直接绑定弹性公网IP为独占IP的方式。

当同一个弹性云服务器同时设置了SNAT和弹性公网IP时，会优先使用弹性公网IP进行转发。

当同一个弹性云服务器同时设置了DNAT和弹性公网IP时，入云方向的弹性公网IP取决于客户端用户的自主选择（DNAT规则绑定的弹性公网IP或ECS直接绑定的弹性公网IP），而出云方向优先使用弹性云服务器直接绑定的弹性公网IP，所以如果入云和出云使用的弹性公网IP不一致，流量会不通。

不建议弹性云服务器同时使用公网NAT网关和直接绑定弹性公网IP。

1.5 通过公网 NAT 网关访问 Internet 失败该如何处理?

用户通过公网NAT网关访问Internet失败，可能是由于VPC路由表配置错误引起的，可以通过以下方法重新配置VPC路由表。

1. 找到VPC对应的子网关联的路由表。
2. 查看路由表是否有到NAT网关的路由，如果不包含，请添加对应的路由。
3. 如果用户自行修改到公网NAT网关的路由，请确保路由的目的地址包含待访问的目的地址。

1.6 公网 NAT 网关是否支持更换 VPC?

不支持。

公网NAT网关在购买时选定VPC，不支持后续进行更换。

1.7 公网 NAT 网关的配额是什么?

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您创建的SNAT最多可关联多少条EIP。如果有需要，您可以申请扩大配额。

本节指导您如何查询指定区域下，公网NAT网关服务各资源的使用情况，以及总配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

图 1-1 我的配额

4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

图 1-2 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 1-3 申请扩大配额

4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

1.8 公网 NAT 网关是否支持 IPV6?

目前公网NAT网关不支持IPV6协议。

1.9 基于公网 NAT 网关的用户网络，可以配置哪些安全策略实现访问限制?

基于公网NAT网关的用户网络，可以通过配置安全组和网络ACL实现访问限制。

- 安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。
- 网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。

安全组对弹性云服务器进行防护，网络ACL对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

安全组与网络ACL的详情，请参见**《VPC用户指南》安全性**章节。

1.10 公网 NAT 网关配置完成后，网络不通如何处理?

问题描述

您创建了一个公网NAT网关，并按照步骤配置了SNAT、DNAT规则，但是您的云主机不能访问互联网或不能为互联网提供服务。配置了公网NAT网关的网络是否可以连通互联网与路由表配置、安全组配置、网络ACL配置等多个环节相关联。任意一个环节出现问题，都会导致网络不通。本节操作介绍公网NAT网关配置完成后，网络不通时的排查思路。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 1-4 网络不通排查思路

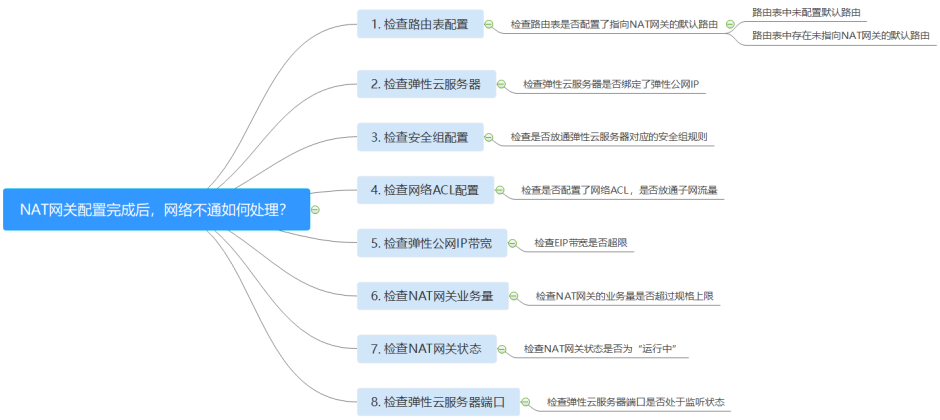


表 1-1 网络不通排查思路

可能原因	处理措施
路由表配置不正确	请在路由表中添加指向公网NAT网关的默认路由或路由，详细操作请参考**检查路由表是否配置指向公网NAT网关网关的默认路由**。
弹性云服务器绑定了弹性公网IP	请为弹性云服务器解绑弹性公网IP，详细操作请参考**检查弹性云服务器是否绑定了弹性公网IP**。
安全组规则未放通	请放通弹性云服务器对应的安全组规则，详细操作请参考**检查安全组规则**。
网络ACL配置不正确	请配置网络ACL规则放通子网流量，详细操作请参考**检查网络ACL是否放通子网流量**。
弹性公网IP的带宽超限	请扩大EIP带宽，详细操作请参考**检查弹性公网IP的带宽是否超限**。
公网NAT网关业务量超过规格上限	请提升公网NAT网关规格，详细操作请参考**检查公网NAT网关业务量是否超过规格上限**。
公网NAT网关的状态异常	请确保公网NAT网关资源状态为“运行中”，详细操作请参考**检查公网NAT网关状态是否异常**。
弹性云服务器端口未监听	请重新开启弹性云服务器端口，详细操作请参考**检查弹性云服务器端口**。

检查路由表是否配置指向公网 NAT 网关网关的默认路由

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“路由表”。

5. 在路由表列表中，单击公网NAT网关所在VPC的路由表名称。
6. 检查路由列表中是否存在指向公网NAT网关的默认路由（0.0.0.0/0）。
   - 如果未存在默认路由，请在路由表中添加指向公网NAT网关的默认路由。
     i. 单击“添加路由”，按照提示配置参数。

图 1-5 添加路由

表 1-2 参数说明

参数	参数说明
目的地址	目的地址网段。 配置为0.0.0.0/0。
下一跳类型	下一跳资源类型选择“NAT网关”。
下一跳	下一跳资源选择创建的公网NAT网关。
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

     ii. 单击“确定”，完成添加。
   - 如果存在默认路由，但是未指向公网NAT网关，请在路由表中添加指向公网NAT网关的路由或者新增路由表并添加指向公网NAT网关的默认路由。
     - 路由表中添加指向公网NAT网关的路由详细步骤：
       1) 单击“添加路由”，按照提示配置参数。

图 1-6 添加路由

表 1-3 参数说明

参数	参数说明
目的地址	目的地址网段。
下一跳类型	下一跳资源类型选择“NAT网关”。
下一跳	下一跳资源选择创建的公网NAT网关。
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

2) 单击“确定”，完成添加。

- 新增路由表并添加指向公网NAT网关的默认路由：

  说明

  新增路由表，请在创建路由表对话框单击“申请扩大配额”或在页面右上角单击“工单 > 新建工单”申请扩大路由表配额。更多提交工单信息请参考**提交工单**。

  1) 在路由表列表页面右上角，单击“创建路由表”，按照提示配置参数。

  表 1-4 参数说明

参数	说明	取值样例
路由表名称	路由表的名称，必填项。 路由表的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	rtb-001
所属VPC	选择路由表归属的VPC，必填项。	vpc-001
描述	路由表的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

参数	说明	取值样例
添加路由	路由规则信息。 路由规则可以在此处添加，单击“继续添加”。 添加目的地址为“0.0.0.0/0”，下一跳资源类型选择“NAT网关”，下一跳资源选择创建的公网NAT网关。	-

2) 单击“确定”，完成创建。
   系统出现信息提示页面，您可根据提示选择立即关联子网。
3) 单击“关联子网”，进入路由表详情页面的“关联子网”页签。
4) 单击“关联子网”，选择需要关联的子网。
5) 单击“确定”，完成关联。

检查弹性云服务器是否绑定了弹性公网 IP

当同一个弹性云服务器同时设置了SNAT和弹性公网IP时，会优先使用弹性公网IP进行转发。

当同一个弹性云服务器同时设置了DNAT和弹性公网IP时，入云方向的弹性公网IP取决于客户端用户的自主选择（DNAT规则绑定的弹性公网IP或ECS直接绑定的弹性公网IP），而出云方向优先使用弹性云服务器直接绑定的弹性公网IP，所以如果入云和出云使用的弹性公网IP不一致，流量会不通。

如果弹性云服务器绑定了弹性公网IP，请为弹性云服务器解绑弹性公网IP。

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，查看“IP地址”列，检查弹性云服务器是否绑定了弹性公网IP。
   - 如果弹性云服务器未绑定弹性公网IP，请检查下一项。
   - 如果弹性云服务器绑定了弹性公网IP，请为弹性云服务器解绑弹性公网IP。
     为弹性云服务器解绑弹性公网IP详情请参见**解绑弹性公网IP**。

检查安全组规则

如果安全组没有放通弹性云服务器访问和对外提供服务使用的端口，需要在弹性云服务器实例对应的安全组中添加放行该端口的规则。

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待检查安全组规则的弹性云服务器名称。
5. 选择“安全组”页签，展开安全组规则。

6. 检查入方向规则和出方向规则是否已经配置放行弹性云服务器使用端口的规则。
   - 如果已配置放行弹性云服务器使用端口规则，请检查下一项。
   - 如果未配置放行弹性云服务器使用端口的规则，请单击“配置规则”，进入安全组详情页。

     在安全组详情页，单击“入方向规则”或“出方向规则”，分别根据弹性云服务器使用的端口添加入方向规则或出方向规则。入方向和出方向规则参数详情请参见**添加安全组规则**。

检查网络 ACL 是否放通子网流量

检查VPC的子网是否关联了网络ACL，如果关联了网络ACL，请检查“ 网络ACL”规则。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“子网”。
5. 查看NAT网关对应的子网是否关联了网络ACL。

   显示具体的网络ACL名称说明已关联网络ACL。

图 1-7 网络 ACL

6. 单击网络ACL名称查看网络ACL的详细信息。

图 1-8 网络 ACL 详情

7. 检查入方向规则和出方向规则是否添加了放通子网流量的规则。

   如果未添加放通子网流量的规则，请添加入方向、出方向规则放通子网流量或者将网络ACL与子网取消关联。

   详情请参见**添加网络ACL规则**和**解除网络ACL关联子网**。

   说明

   需要注意“网络ACL”的默认规则是丢弃所有出入方向的包，若关闭“网络ACL”后，其默认规则仍然生效。

检查弹性公网 IP 的带宽是否超限

公网NAT网关绑定了弹性公网IP时，通过带宽提供公网和公网NAT网关间的访问流量。

如果出现网络不通，请排查弹性公网IP带宽是否超过带宽最大上限。

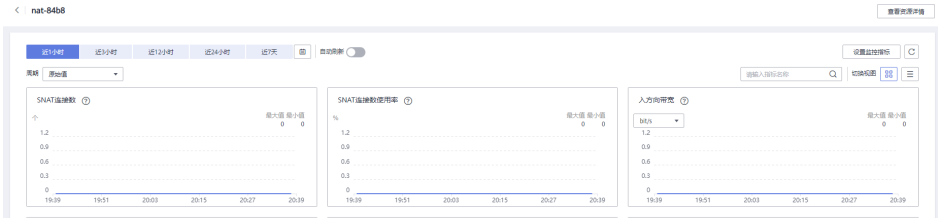
排查带宽超限的方法请参考**如何排查带宽超过限制?**

扩大带宽的操作请参考**修改弹性公网IP的带宽**。

检查公网 NAT 网关业务量是否超过规格上限

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“管理与监管 > 云监控服务”。
4. 单击页面左侧的“云服务监控”，选择“NAT网关”。
5. 单击“操作”列的“查看监控指标”，查看公网NAT网关的监控指标详情。

图 1-9 NAT 网关指标详情



6. 检查公网NAT网关SNAT连接数是否超过NAT网关规格上限。
   - 如果SNAT连接数未超过公网NAT网关规格上限，请检查下一项。
   - 如果SNAT连接数超过公网NAT网关规格上限，请提升公网NAT网关规格。
     提升公网NAT网关规格请参见**修改公网NAT网关**。

检查公网 NAT 网关状态是否异常

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“网络 > NAT网关”。
4. 在公网NAT网关列表，检查公网NAT网关状态是否异常。
   - 如果公网NAT网关状态为“运行中”，请检查下一项。
   - 如果公网NAT网关状态不是“运行中”，主要有以下情况：
     - 公网NAT网关因未及时续费，导致状态异常，请为公网NAT网关续费。
       为公网NAT网关续费请参见**欠费还款**。
     - 因使用华为云资源违反了相关安全要求或法律法规，导致您的账号或资源被冻结。如果您在整改期限内完成整改并达到相关安全和法律要求，那么就可以解冻您的账号和资源；如果您在整改期限内未完成整改，那么将删除您的资源。

检查弹性云服务器端口

确保弹性云服务器端口正常工作，处于LISTEN状态。表1-5为常见TCP状态。

- Linux操作系统云服务器端口通信问题排查
  使用**netstat -antp**命令检查服务的状态，确认端口是否正常监听。
  例如：**netstat -ntulp |grep 80**

  图 1-10 查看端口监听状态_linux

  ```
  [root@elb-mq02 ~]# netstat -antpu | grep sshd
  tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7178/sshd
  ```

  如果端口没有被正常监听，请重新开启弹性云服务器端口。
- Windows操作系统云服务器端口通信问题排查
  使用远程端口检测命令：
  a. 打开CMD命令行窗口。
  b. 执行**netstat -ano | findstr “***PID***”**命令查看进程使用的端口号。
  例如：**netstat -ano | findstr “80”**

  图 1-11 查看端口监听状态_windows

  ```
  C:\Users\Administrator>netstat -ano |findstr "80"
    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
    TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       880
    TCP    [::]:80                [::]:0                 LISTENING       4
    TCP    [::]:49155             [::]:0                 LISTENING       880
    UDP    0.0.0.0:123            *:*                                    808
    UDP    [::]:123               *:*                                    808
  ```

  如果端口没有被正常监听，请重新开启弹性云服务器端口。

表 1-5 常见 TCP 状态

TCP状态	说明	对应场景
LISTEN	侦听来自远方的TCP端口的连接请求	正常TCP服务端
ESTABLISHED	代表一个打开的连接	正常TCP连接
TIME-WAIT	等待足够的时间以确保远程TCP接收到连接中断请求的确认	已关闭的TCP连接，一般1分钟后清除。
CLOSE-WAIT	等待从本地用户发来的连接中断请求	应用程序BUG，没有关闭socket。出现在网络中断后。一般是进程死循环或等待其他条件。可以重启对应进程。
FIN-WAIT-2	从远程TCP等待连接中断请求	网络中断过，需要12分钟左右自行恢复。

TCP状态	说明	对应场景
SYN-SENT	再发送连接请求后等待匹配的连接请求	TCP连接请求失败。一般是服务端CPU占用率过高，处理不及时导致。DDos攻击也会出现此情况。
FIN-WAIT-1	等待远程TCP连接中断请求，或先前的连接中断请求的确认	网络中断过，此状态可能不会自行修复（等15分钟以上确认），如果长期占用端口需要重启OS恢复。

1.11 公网 NAT 网关是否可以限制具体某个服务器的带宽?

不可以。公网NAT网关的SNAT功能通过绑定弹性公网IP，实现云主机私有IP到公网IP的转换。云主机通过公网NAT网关访问外网时，其带宽大小和您购买弹性公网IP时选择的带宽大小有关，无法单独在NAT网关上做限制。

2 私网 NAT 网关

2.1 私网 NAT 配置后组网不通怎么排查?

检查安全组规则

如果安全组没有放通弹性云服务器访问和对外提供服务使用的端口，需要在弹性云服务器对应的安全组中添加放行该端口的规则。

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 ，选择区域和项目。

步骤3 选择“计算 > 弹性云服务器”。

步骤4 在弹性云服务器列表，单击待检查安全组规则的弹性云服务器名称。

步骤5 选择“安全组”页签，展开安全组规则。

步骤6 检查入方向规则和出方向规则是否已经配置放行弹性云服务器使用端口的规则。

- 如果已配置放行弹性云服务器使用端口规则，请**检查路由表是否配置指向私网NAT网关的路由**。
- 如果未配置放行弹性云服务器使用端口的规则，请单击“配置规则”，进入安全组详情页，按**步骤7**进行配置。

步骤7 在安全组详情页，单击“入方向规则”或“出方向规则”，分别根据弹性云服务器使用的端口添加入方向规则或出方向规则。

----结束

检查路由表是否配置指向私网 NAT 网关的路由

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 ，选择区域和项目。

步骤3 在系统首页，选择“网络 > 虚拟私有云”。

步骤4 在左侧导航栏选择“路由表”。

步骤5 在路由表列表中，单击私网NAT网关所在VPC的路由表名称。

步骤6 检查路由列表中是否存在指向私网NAT网关的路由。

----结束

2.2 一个 VPC 最多支持购买多少个私网 NAT?

当前单个VPC最多支持购买10个私网NAT。

2.3 私网 NAT 支持创建的 SNAT 和 DNAT 规则数能否增加?

可以，需要通过**提交工单**来解决。工单提交请参见**提交工单**。

2.4 私网 NAT 支持 SNAT 规则和 DNAT 规则共用一个中转 IP 吗?

私网NAT目前暂不支持SNAT规则和DNAT规则共用一个中转IP。

2.5 私网 NAT 支持云专线的 IP 转换吗?

支持。在创建DNAT规则时，选择自定义模式，可添加通过云专线接入的客户云下IP。

2.6 私网 NAT 和公网 NAT 有什么区别?

私网NAT是实现**私网IP**与**私网IP**之间的地址转换。

私网NAT的作用有：

- 通过私网IP地址转换，解决私网IP地址冲突的问题。
- 通过私网IP地址转换，满足指定地址接入的需求。

公网NAT是实现**私网IP**与**公网IP**之间的地址转换。

公网NAT的作用有：

- 更安全：避免云主机公网IP直接暴露在外。
- 省成本：共享EIP，共享带宽，节约EIP资源。

2.7 私网 NAT 的收费情况是怎么样的?

目前私网NAT在部分区域限时免费，在部分区域已开始计费，关于私网NAT计费情况详见**计费说明（私网NAT网关）**。

2.8 私网 NAT 是否支持跨账号使用?

私网NAT本身不支持跨账号使用，但可以通过**VPC对等连接**实现跨账户通信，VPC对等连接打通两个账号的中转VPC，实现两个私网NAT转换IP后的跨账号通信。

3 SNAT 规则

3.1 为什么使用 SNAT?

对公网NAT网关来说，一些弹性云服务器不仅需要使用系统提供的服务，还需要访问外网以获取信息或下载软件。但是，给弹性云服务器分配公网IP需要消耗稀缺资源（如IPv4地址），增加额外的成本，并有可能增加虚拟环境遭受攻击的几率。因此，多个弹性云服务器共享同一公网IP是一种可行的方法，具体实施方法为源地址转换（SNAT）。

对**私网NAT网关**来说，在大企业不同部门间存在大量重叠网段，上云后无法互通，通过私网SNAT可以将一个部门多个弹性云服务器的IP转化为一个中转IP去访问别的部门；因为安全受限等原因，行业监管部门要求各机构和单位按指定IP地址接入，通过私网SNAT可以将多个弹性云服务器的IP转化为一个中转IP，去访问行业监管部门。

3.2 什么是 SNAT 连接数?

由源IP地址、源端口、目的IP地址、目的端口、传输层协议这五个元素组成的集合视为一条连接。连接能够区分不同会话，并且对应的会话是唯一的。其中源IP地址和源端口指SNAT转换之后的IP和它的端口。

由于SNAT支持TCP、UDP和ICMP三种协议，每一个目的IP和目的端口，NAT网关最多可支持55000个并发连接。如果目的IP、端口或者协议（TCP/UDP/ICMP）发生变化，则可以再创建55000个连接。弹性云服务器中通过netstat命令看到ESTABLISHED状态的连接数和实际SNAT连接数有时会不一致。假设一个弹性云服务器平均每秒钟创建100个与固定目的的连接，不考虑连接老化的话，大约10分钟会将55000个连接耗尽导致连接无法新建。

NAT网关中SNAT连接如果长时间没有数据报文，会超时断开。因此为防止连接中断您需要发起更多的数据包或使用TCP保持连接。同时，为避免出现因连接数规格用满而出现的影响业务的情况，建议经常关注CES监控中的NAT网关SNAT连接数并合理设置告警。

3.3 主机通过公网 NAT 网关访问外网，请问公网 NAT 网关的带宽是多少？在哪里设置?

公网NAT网关的SNAT功能通过绑定弹性公网IP，实现云主机私有IP到公网IP的转换。云主机通过公网NAT网关访问外网时，其带宽大小和您购买弹性公网IP时选择的带宽大小有关。

带宽大小调整操作请参考**修改带宽大小**。

3.4 NAT 网关丢包或连接不通该如何处理?

通过NAT网关上网的服务器出现丢包或连接不通的情况时，可以通过云监控查看NAT网关的SNAT连接数。若SNAT连接数超过NAT网关规格上限，则会导致使用NAT网关的服务器出现丢包或者连接不通的现象。请参考**查看监控指标**，查看SNAT的连接数是否超过NAT网关的规格上限。如果超过NAT网关规格上限，可修改NAT网关规格，增大NAT网关规格数。

3.5 通过公网 NAT 网关访问远端服务器概率性失败该如何处理?

弹性云服务器通过SNAT访问公网上服务器，出现TCP建链失败的情况，可通过以下方法进行排查。

1. 执行以下命令，查看远端服务器是否开启了“tcp_tw_recycle”。
   sysctl -a|grep tcp_tw_recycle
   tcp_tw_recycle取值为1时，表示开启。
2. 执行以下命令，查看远端服务器内核丢包数量。
   cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'
   如果ListenDrops数值非0，表示存在丢包，即存在网络问题。

处理方法:

方法一：修改远端服务器的内核参数

- 临时修改参数方法（重启远端服务器后该设置失效），设置如下:
  sysctl -w net.ipv4.tcp_tw_recycle=0
- 永久修改参数方法:
  a. 执行以下命令，修改“/etc/sysctl.conf”文件。
     vi /etc/sysctl.conf
     在该文件中添加以下内容:
     net.ipv4.tcp_tw_recycle=0
  b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。
  c. 执行以下命令，生效配置。
     sysctl -p

方法二：修改本地客户端的内核参数

- 临时修改参数方法（重启本地客户端后该设置失效），设置如下：
  sysctl -w net.ipv4.tcp_timestamps=0
- 永久修改参数方法：
  a. 执行以下命令，修改“/etc/sysctl.conf”文件。
     vi /etc/sysctl.conf
     在该文件中添加以下内容：
     net.ipv4.tcp_timestamps=0
  b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。
  c. 执行以下命令，生效配置。
     sysctl -p

3.6 NAT 网关里的网段设置与 SNAT 规则里的网段有什么关联与区别?

NAT网关里的网段是在创建NAT网关时必须指定NAT网关所在VPC及子网网段。此网段仅用于系统后台使用，并非SNAT使用的网段。

创建SNAT规则且当场景是虚拟私有云时，需要配置对应VPC的子网网段，使该网段中的云主机通过SNAT方式进行访问。

创建SNAT规则且当场景是云专线/云连接时，需要配置云专线/云连接对应的本地数据中心的某个网段或另一VPC的网段，使该网段中的云主机通过SNAT方式进行访问。

4 DNAT 规则

4.1 为什么使用 DNAT?

公网NAT网关的DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。详见**添加公网DNAT规则**。

私网NAT网关的DNAT功能通过绑定中转IP，可实现IP映射或端口映射，使VPC内跨可用区的多个云主机共享中转IP，为外部私网提供服务。详见**添加私网DNAT规则**。

4.2 DNAT 规则是否支持更新操作?

DNAT规则支持更新操作。公网NAT网关和私网NAT网关均支持修改DNAT规则。

4.3 DNAT 规则可以配置服务器访问指定网站吗?

不可以。NAT网关不具备访问控制功能，只能根据规则转送流量。如果需要设置限制访问的网站，您可以配置安全组和ACL规则进行限制。具体请参考**安全组配置示例**和**网络ACL配置示例**。