

NAT 网关

用户指南

文档版本

01

发布日期

2020-11-06



华为技术有限公司



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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 产品简介	1
1.1 什么是 NAT 网关	1
1.2 产品优势	3
1.3 应用场景	4
1.4 产品规格	6
1.5 约束与限制	7
1.6 与其它服务的关系	8
1.7 区域和可用区	8
1.8 基本概念	9
2 快速入门	10
2.1 使用 SNAT 访问公网	10
2.1.1 简介	10
2.1.2 步骤 1: 创建弹性公网 IP	11
2.1.3 步骤 2: 创建公网 NAT 网关	11
2.1.4 步骤 3: 添加 SNAT 规则	12
2.1.5 步骤 4: 结果验证	14
2.2 使用 DNAT 为云主机面向公网提供服务	14
2.2.1 简介	14
2.2.2 步骤 1: 创建弹性公网 IP	14
2.2.3 步骤 2: 创建公网 NAT 网关	15
2.2.4 步骤 3: 添加 DNAT 规则	16
2.2.5 步骤 4: 结果验证	18
2.3 云间 NAT 网关高速访问互联网	18
2.3.1 简介	18
2.3.2 步骤 1: 开通云专线	19
2.3.3 步骤 2: 创建弹性公网 IP	19
2.3.4 步骤 2: 创建公网 NAT 网关	19
2.3.5 步骤 4: 添加 SNAT 规则	21
2.3.6 步骤 5: 添加 DNAT 规则	22
3 NAT 网关管理	25
3.1 创建 NAT 网关	25
3.2 查看 NAT 网关	27

3.3 修改 NAT 网关.....	27
3.4 删除 NAT 网关.....	28
4 SNAT 规则管理.....	29
4.1 添加 SNAT 规则.....	29
4.2 查看 SNAT 规则.....	31
4.3 修改 SNAT 规则.....	32
4.4 删除 SNAT 规则.....	32
5 DNAT 规则管理.....	33
5.1 添加 DNAT 规则.....	33
5.2 查看 DNAT 规则.....	35
5.3 修改 DNAT 规则.....	36
5.4 删除 DNAT 规则.....	36
5.5 批量删除 DNAT 规则.....	37
5.6 DNAT 规则模板导入导出.....	37
6 监控管理.....	40
6.1 支持的监控指标.....	40
6.2 创建告警规则.....	43
6.3 查看监控指标.....	43
7 常见问题.....	45
7.1 NAT 网关.....	45
7.1.1 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?	45
7.1.2 NAT 网关如何实现高可用性?	45
7.1.3 哪些端口无法访问?	45
7.1.4 通过 NAT 网关访问 Internet 失败该如何处理?	45
7.1.5 NAT 网关是否支持更换 VPC?	46
7.1.6 NAT 网关的配额是什么?	46
7.2 SNAT.....	46
7.2.1 为什么使用 SNAT?	47
7.2.2 什么是 SNAT 连接数?.....	47
7.2.3 主机通过 NAT 网关访问外网, 请问 NAT 网关的宽带是多少? 在哪里设置?	47
7.2.4 NAT 网关丢包或连接不通该如何处理?	47
7.2.5 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?	47
7.3 DNAT.....	48
7.3.1 为什么使用 DNAT?.....	48
7.3.2 DNAT 规则是否支持更新操作?	48
7.3.3 ECS 变更规格后 NAT 网关规则失效怎么处理?	48
A 修订记录.....	49

1 产品简介

1.1 什么是 NAT 网关

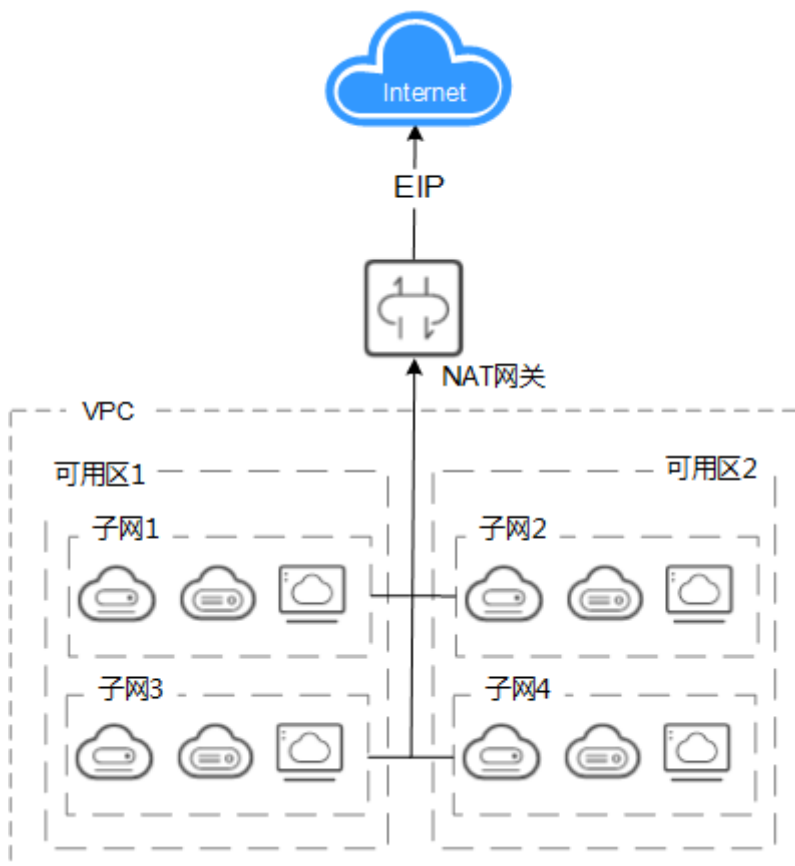
NAT网关（NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器云主机、裸金属服务器物理机、云桌面）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高10Gbit/s能力的网络地址转换服务，使多个云主机可以共享弹性公网IP访问Internet或使云主机提供互联网服务。

NAT网关分为SNAT和DNAT两个功能。

- SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内跨可用区的多个云主机共享弹性公网IP，安全，高效的访问互联网。

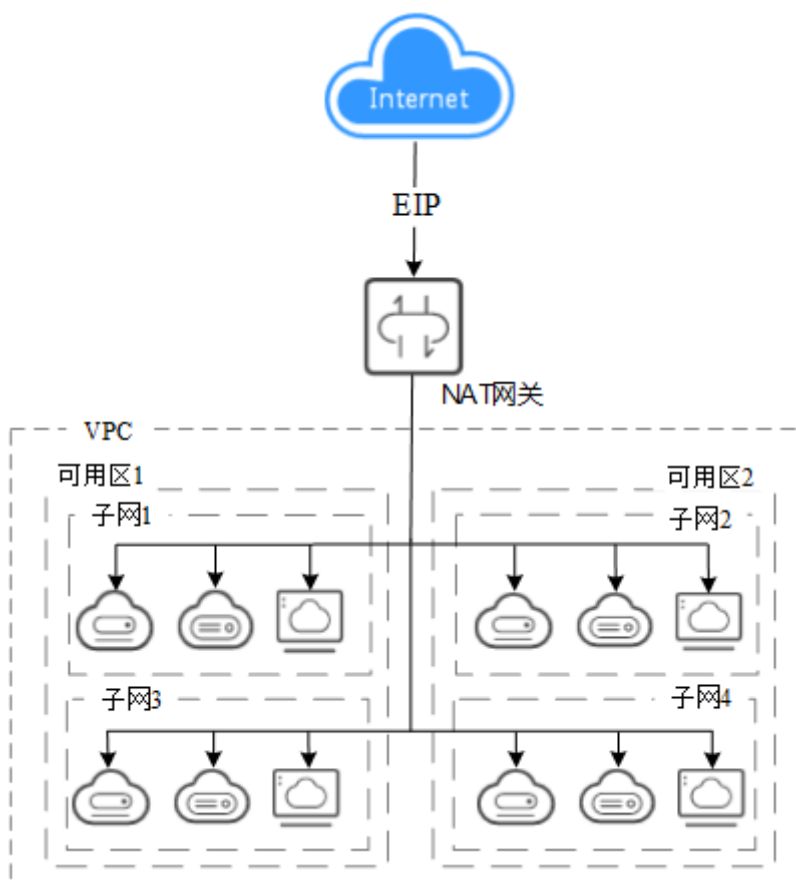
SNAT架构如[图1-1](#)所示。

图 1-1 SNAT 架构图



- 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。DNAT架构如图1-2所示。

图 1-2 DNAT 架构图



1.2 产品优势

NAT网关具有以下几大优势：

- 灵活部署
支持跨子网部署和跨可用区域部署。NAT网关支持跨可用区部署，可用性高，单个可用区的任何故障都不会影响NAT网关的业务连续性。NAT网关的规格、公网IP，均可以随时调整。
- 多样易用
多种网关规格可灵活选择。对NAT网关进行简单配置后，即可使用，运维简单，快速发放，即开即用，运行稳定可靠。
- 降低成本
多个云主机共享使用弹性公网IP。当您的私有IP地址通过NAT网关发送数据，或您的应用面向互联网提供服务时，NAT网关服务将私有地址和公网地址进行转换。用户无需为云主机访问Internet创建多余的弹性公网IP和带宽资源，多个云主机共享使用弹性公网IP，有效降低成本。

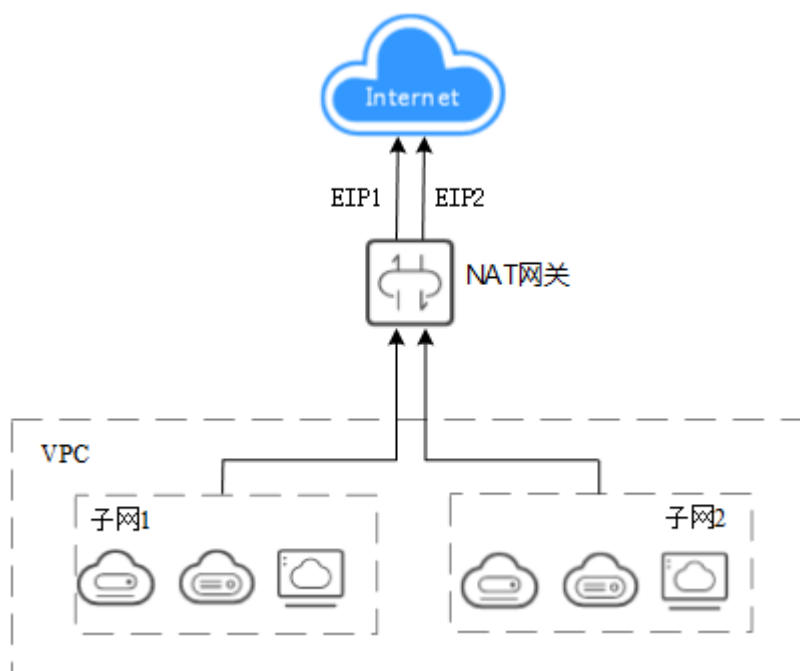
1.3 应用场景

使用 SNAT 访问公网

当VPC内的云主机需要访问公网，请求量大时，为了节省弹性公网IP资源并且避免云主机IP直接暴露在公网上，您可以使用NAT网关的SNAT功能。VPC中一个子网对应一条SNAT规则，一条SNAT规则配置一个弹性公网IP。NAT网关为您提供不同规格的连接数，根据业务规划，您可以通过创建多条SNAT规则，来实现共享弹性公网IP资源。

使用SNAT访问公网场景组网图如图1-3所示。

图 1-3 使用 SNAT 访问公网



使用 DNAT 为云主机面向公网提供服务

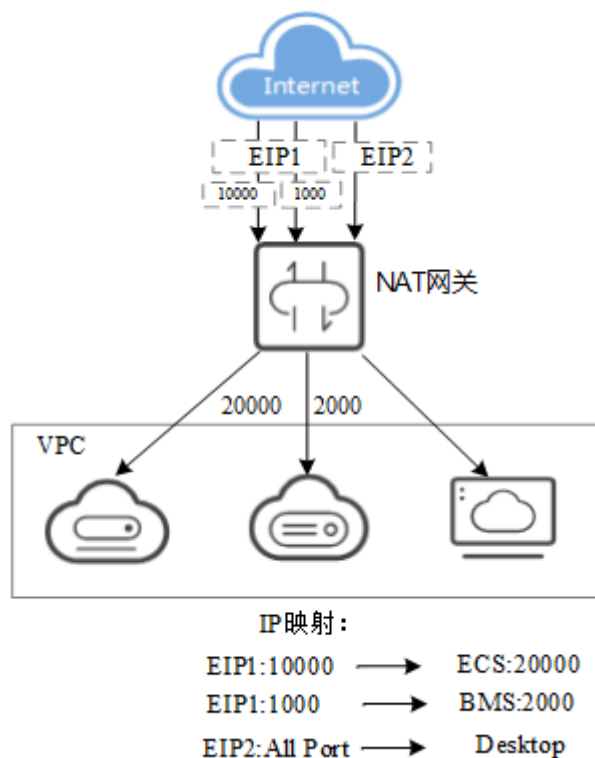
当VPC内的云主机需要面向公网提供服务时，可以使用NAT网关的DNAT功能。

DNAT功能绑定弹性公网IP，可通过端口映射方式，NAT网关会将以指定的协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。也可通过IP映射方式，为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云主机实例上。使多个云主机共享弹性公网IP和带宽，精确的控制带宽资源。

一个云主机配置一条DNAT规则，如果有多个云主机需要为公网提供服务，可以通过配置多条DNAT规则来共享一个或多个弹性公网IP资源。

使用DNAT为公网提供服务场景组网图如图1-4所示。图中示例的云主机类型均可以替换为弹性云服务器，云桌面中的任何一个。例如图中的云桌面可替换为或者。

图 1-4 使用 DNAT 为云主机面向公网提供服务

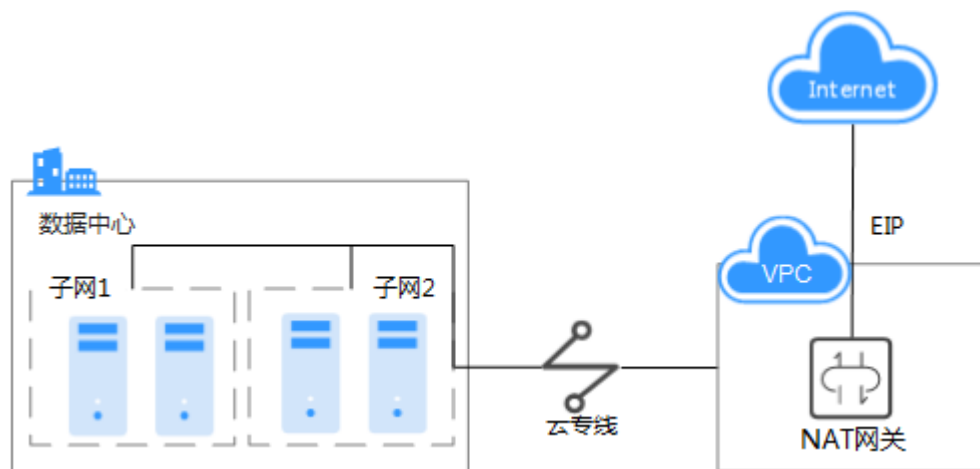


使用 SNAT 或 DNAT 高速访问互联网

用户线下私有云或跨区域使用云专线/VPN接入虚拟私有云的用户，若有大量的服务器需要实现安全，可靠，高速的访问互联网，或者为互联网提供服务，可通过NAT网关的SNAT功能或DNAT功能来实现。例如各类互联网、游戏、电商、金融等企业的跨云场景。

云间NAT网关高速访问互联网场景图如图1-5所示。

图 1-5 使用 SNAT 或 DNAT 高速访问互联网



搭建高可用的 SNAT

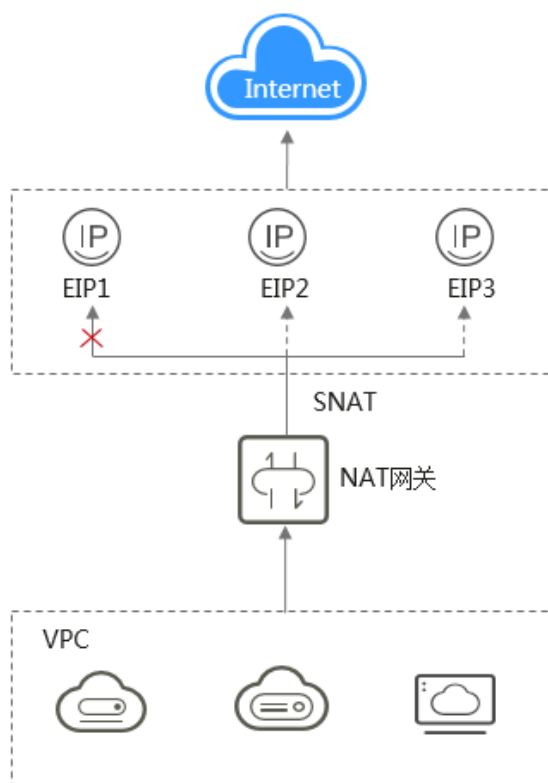
在IT系统中，往往存在绑定的弹性公网IP被攻击封堵的可能性。如果您想提高系统的高可靠性，可以在配置SNAT规则时，添加多个弹性公网IP，当其中一个弹性公网IP被攻击封堵时，可以最大程度保障使用其他弹性公网IP的业务正常运行。

当SNAT规则上绑定了多个EIP时，系统会随机选择一个弹性公网IP访问公网。

每条SNAT规则支持添加20个弹性公网IP，当SNAT规则中添加的弹性公网IP被攻击封堵或不可用时，需要手动从EIP池中删除。

搭建高可用的SNAT网关场景组网图如图1-6所示。

图 1-6 搭建高可用的 SNAT 网关



1.4 产品规格

NAT网关的规格指NAT网关支持的SNAT最大连接数。

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。其中源IP地址和源端口指SNAT转换之后的弹性公网IP和它的端口。连接能够区分不同会话，并且对应的会话是唯一的。

NAT网关数据的吞吐量被确定为DNAT规则的弹性公网IP的带宽之和，例如，一个NAT网关有两条DNAT规则，其中绑定到第一条规则的EIP带宽为10Mbit/s，绑定到第二条规则的EIP带宽为5Mbit/s，则NAT网关的吞吐量为15Mbit/s。

每个NAT网关支持的最大转发带宽为10Gbit/s。

NAT网关TCP SNAT的连接超时时间为600秒。

NAT网关UDP SNAT的连接超时时间为300秒。

在创建NAT网关时，请根据您的网络规划，合理选择NAT网关的规格。NAT网关支持的规格如表1-1所示。

表 1-1 NAT 网关规格

规格	SNAT最大连接数
小型	10000
中型	50000
大型	200000
超大型	1000000

说明

- 为避免因连接数超过NAT网关规格最大值，从而影响业务的情况，建议在云监控中设置NAT网关监控指标，并为SNAT连接数合理设置告警。
- DNAT规则与NAT网关的规格无关，NAT网关支持最多添加200条DNAT规则。

1.5 约束与限制

关于NAT网关的使用，您需要注意以下几点：

- 同一个NAT网关下的多条规则可以复用同一个弹性公网IP，不同网关下的规则必须使用不同的弹性公网IP。
- 每个VPC支持的NAT网关数为1。
- 用户不能在VPC下手动添加默认路由。
- VPC内的每个子网只能添加一条SNAT规则。
- SNAT规则和DNAT规则一般面向不同的业务，如果使用相同的EIP，会面临业务相互抢占问题，请尽量避免。SNAT规则不能和全端口的DNAT规则共用EIP。
- DNAT规则不支持将弹性公网IP绑定到虚拟IP。
- 当云主机同时配置弹性公网IP服务和NAT网关服务时，数据均通过弹性公网IP转发。
- SNAT规则中添加的自定义网段，对于虚拟私有云的配置，必须是虚拟私有云子网网段的子集，不能相等。
- SNAT规则中添加的自定义网段，对于云专线的配置，必须是云专线侧网段，且不能与虚拟私有云侧的网段冲突。
- 当执行云服务器底层资源操作（如变更规格）时，会导致已配置的NAT规则失效，需要删除后重新配置。

1.6 与其它服务的关系

表 1-2 与其他服务的关系

交互功能	相关服务	位置
通过云专线接入VPC的本地服务器，可以通过NAT网关访问公网或为公网提供服务。	云专线（ Direct Connect, DC ）	云间NAT网关高速访问互联网
通过VPN接入VPC的本地服务器，可以通过NAT网关访问公网或为公网提供服务。	虚拟专用网络（ Virtual Private Network, VPN ）	云间NAT网关高速访问互联网
NAT网关可以为其他云服务提供访问公网或者为公网提供服务的能力。	弹性云服务器（ Elastic Cloud Server, ECS ）	使用SNAT访问公网 使用DNAT为云主机面向公网提供服务

1.7 区域和可用区

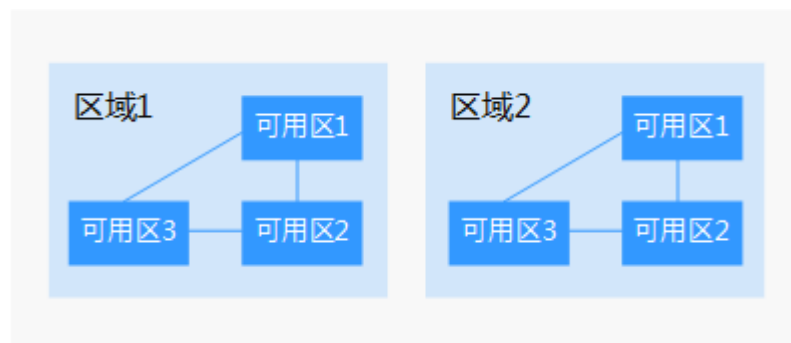
什么是区域、可用区？

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（ Region ）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（ AZ, Availability Zone ）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图1-7阐明了区域和可用区之间的关系。

图 1-7 区域和可用区



如何选择区域？

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关公有云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

1.8 基本概念

弹性公网 IP

弹性公网IP地址为可以直接访问Internet的IP地址。私有IP地址为公有云内局域网络所有的IP地址，私有IP地址禁止出现在Internet中。

弹性公网IP是基于互联网上的静态IP地址，将弹性公网IP地址和子网中关联的弹性云服务器绑定，可以实现VPC中的弹性云服务器通过固定的公网IP地址与互联网互通。

一个弹性公网IP只能给一个弹性云服务器使用。

SNAT 连接

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。其中源IP地址和源端口指SNAT转换之后的弹性公网IP和它的端口。连接能够区分不同会话，并且对应的会话是唯一的。

DNAT 连接

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。

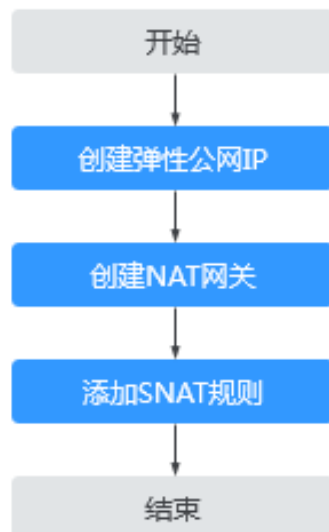
2 快速入门

2.1 使用 SNAT 访问公网

2.1.1 简介

当多个云主机（弹性云服务器、裸金属服务器、云桌面）在没有绑定弹性公网IP的情况下需要访问公网，为了节省弹性公网IP资源并且避免云主机IP直接暴露在公网上，可以通过NAT网关共享弹性公网IP的方式访问公网，可以按照图2-1所示，实现无弹性公网IP的云主机访问公网。

图 2-1 无弹性公网 IP 的虚机访问公网流程图



2.1.2 步骤 1：创建弹性公网 IP

操作场景

通过创建弹性公网IP来实现VPC中的云主机以NAT网关的形式共享弹性公网IP访问公网。

操作步骤

详细步骤请参考《弹性公网IP用户指南》，这里创建弹性公网IP后，无需绑定云主机。

2.1.3 步骤 2：创建公网 NAT 网关

操作场景

如果您要通过NAT网关访问公网或为公网提供服务，则需要创建公网NAT网关。

前提条件

- 创建公网NAT网关必须指定NAT网关所在VPC、子网、NAT网关规格。
- 确认VPC下没有默认路由。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击创建公网NAT网关，进入NAT网关创建页面。

图 2-2 创建公网 NAT 网关页面

The screenshot shows the 'Create Public NAT Gateway' page. The form includes the following fields and options:

- Region:** G42 (with a note: 'Different regions are not互通. Select the region closest to your customer to reduce network latency and improve access speed.')
- Name:** nat-7640
- Virtual Private Cloud:** vpc-d2e7 (with a link to 'View Virtual Private Cloud')
- Subnet:** subnet-d329 (192.168.0.0/24) (with a note: 'This subnet is used for NAT gateway. Rules must be added after creation to allow access to the Internet.')
- Instance Type:** Small, Medium, Large, Extra Large (with a note: 'SNAT supports a maximum of 10,000 connections. Learn more')
- Enterprise Project:** --Select Enterprise Project-- (with a link to 'New Enterprise Project')
- Description:** A text input field with a character count of 0/255.
- Tags:** A section with a note: 'If you need to use the same tag to identify multiple cloud resources, all services can select the same tag from the dropdown menu. It is recommended to create a custom tag in TMS. View Custom Tag'. It includes 'Tag Key' and 'Tag Value' input fields and a note: 'You can add up to 10 tags.'

A red '立即创建' (Create Immediately) button is located at the bottom right of the form.

4. 根据界面提示，配置NAT网关的基本信息，配置参数请参见表2-1。

表 2-1 参数说明

参数	参数说明
区域	NAT网关所在的区域。
名称	NAT网关名称。最大支持64个字符，仅支持数字、字母、_（下划线）、-（中划线）。
虚拟私有云	NAT网关所属的VPC。只能选择没有被其他NAT网关使用和没有默认路由的VPC。 VPC仅在创建NAT网关时可以选择，后续不支持修改。
子网	NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建NAT网关时可以选择，后续不支持修改。
规格	NAT网关的规格。 NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
企业项目	配置NAT网关归属的企业项目。当NAT网关配置企业项目时，该NAT网关将归属于该企业项目。当没有指定企业项目时，将默认使用项目名称为default的企业项目。
描述	NAT网关信息描述。最大支持255个字符。

5. 单击“立即创建”，在“规格确认”页面，您可以再次核对NAT网关信息。
6. 确认无误后，单击“提交”，开始创建NAT网关。
NAT网关的创建过程一般需要1-5分钟。
7. 在“NAT网关”列表，查看NAT网关状态。

2.1.4 步骤 3：添加 SNAT 规则

操作场景

NAT网关创建成功后，您需要创建SNAT规则。通过创建SNAT规则，您可以将该子网下的云主机通过共享弹性公网IP访问互联网。

一个子网或一条网段对应一条SNAT规则，如果VPC中有多个子网或网段需要访问公网，则可以通过创建多个SNAT规则实现共享弹性公网IP资源。

前提条件

NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加SNAT规则的NAT网关名称。
4. 在SNAT规则页签中，单击“添加SNAT规则”。
5. 根据界面提示，配置添加SNAT规则参数。配置参数请参见表2-2。

表 2-2 参数说明

参数	场景条件	说明
使用场景	N/A	在使用SNAT访问公网的场景下，此处选择虚拟私有云。 表示虚拟私有云中的云主机使用SNAT规则访问公网。
类型	当使用场景为虚拟私有云时，需要配置此参数。	云主机访问公网的方式。 当虚拟私有云子网中的全部云主机需要通过SNAT方式访问公网时，选择子网。 当虚拟私有云子网中的部分云主机需要通过SNAT方式访问公网时，选择自定义。
子网	当使用场景为虚拟私有云，类型为子网时，需要配置此参数。	选择虚拟私有云中的子网，可实现该子网中的云主机通过SNAT的方式访问公网。
网段	使用场景为虚拟私有云，类型为自定义时需要配置此参数。	通过配置虚拟私有云子网中的某个网段，使该网段中的云主机通过SNAT方式访问公网。
弹性公网IP	类型为虚拟私有云时需要配置此参数。	用来提供互联网访问的公网IP。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。
监控	N/A	为SNAT连接数设置告警。 可通过设置告警及时了解SNAT连接数运行状况，从而起到预警作用。
描述	N/A	SNAT规则信息描述。最大支持255个字符。

6. 配置完成后，单击确定，完成“SNAT规则”创建。

说明

根据您的业务需求，可以为一个NAT网关添加多条SNAT规则。

2.1.5 步骤 4：结果验证

操作场景

SNAT规则添加完成后，可以验证为目标NAT网关添加的SNAT规则。

操作前提

SNAT规则已经添加。

操作步骤

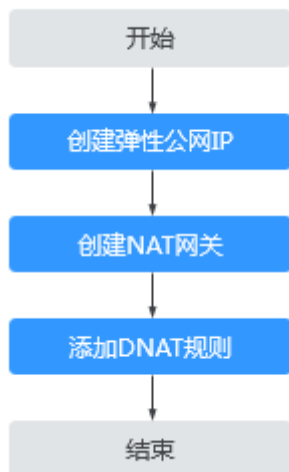
1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 在SNAT页签的SNAT规则列表中，可以看到SNAT规则详细信息，若“状态”为“运行中”，表示创建成功。

2.2 使用 DNAT 为云主机面向公网提供服务

2.2.1 简介

VPC内的一个或多个云主机（弹性云服务器、云桌面）需要面向公网提供服务时，可以根据图2-3实现对公网提供服务。

图 2-3 面向公网提供服务流程图



2.2.2 步骤 1：创建弹性公网 IP

操作场景

通过创建弹性公网IP来实现VPC中的云主机通过NAT的方式为互联网提供服务。

操作步骤

详细步骤请参考《弹性公网IP用户指南》，这里创建弹性公网IP后，无需绑定云主机。

2.2.3 步骤 2：创建公网 NAT 网关

操作场景

如果您要通过NAT网关访问公网或为公网提供服务，则需要创建公网NAT网关。

前提条件

- 创建公网NAT网关必须指定NAT网关所在VPC、子网、NAT网关规格。
- 确认VPC下没有默认路由。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击创建公网NAT网关，进入NAT网关创建页面。

图 2-4 创建公网 NAT 网关页面

The screenshot shows the '创建公网NAT网关' (Create Public NAT Gateway) page. The configuration is as follows:

- Region: G42
- Name: nat-7640
- VPC: vpc-d2e7
- Subnet: subnet-d329 (192.168.0.0/24)
- Instance Type: Small (selected)
- Enterprise Project: --选择企业项目--
- Description: (empty)
- Tags: (empty)

A red button labeled '立即创建' (Create Immediately) is located at the bottom right of the form.

4. 根据界面提示，配置NAT网关的基本信息，配置参数请参见表2-3。

表 2-3 参数说明

参数	参数说明
区域	NAT网关所在的区域。

参数	参数说明
名称	NAT网关名称。最大支持64个字符，仅支持数字、字母、_（下划线）、-（中划线）。
虚拟私有云	NAT网关所属的VPC。只能选择没有被其他NAT网关使用和没有默认路由的VPC。 VPC仅在创建NAT网关时可以选择，后续不支持修改。
子网	NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建NAT网关时可以选择，后续不支持修改。
规格	NAT网关的规格。 NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
企业项目	配置NAT网关归属的企业项目。当NAT网关配置企业项目时，该NAT网关将归属于该企业项目。当没有指定企业项目时，将默认使用项目名称为default的企业项目。
描述	NAT网关信息描述。最大支持255个字符。

5. 单击“立即创建”，在“规格确认”页面，您可以再次核对NAT网关信息。
6. 确认无误后，单击“提交”，开始创建NAT网关。
NAT网关的创建过程一般需要1-5分钟。
7. 在“NAT网关”列表，查看NAT网关状态。

2.2.4 步骤 3：添加 DNAT 规则

操作场景

NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机对互联网提供服务。

一个云主机的一个端口对应一条DNAT规则，如果您有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则。

操作前提

已成功创建NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加DNAT规则的NAT网关名称。

4. 在NAT网关详情页面中，单击“DNAT规则”页签。
5. 在DNAT规则页签中，单击“添加DNAT规则”。
6. 根据界面提示，配置添加DNAT规则参数，详情请参见表2-4。

表 2-4 DNAT 规则参数说明

参数	说明
使用场景	在使用DNAT为云主机面向公网提供服务场景下，此处选择虚拟私有云。 表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务。
端口类型	分为所有端口和具体端口两种类型。 <ul style="list-style-type: none">● 所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云主机实例上。● 具体端口：属于端口映射方式。NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。
支持协议	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。
弹性公网IP	弹性公网IP地址。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的。
公网端口	弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
私网IP	在使用DNAT为云主机面向公网提供服务场景下，指云主机的IP地址，表示此IP地址的云主机将通过DNAT方式为公网提供服务。 端口类型为具体端口时，需要配置私网IP的端口。
私网端口	在使用DNAT为云主机面向公网提供服务场景下，指云主机的端口号。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 私网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
描述	DNAT规则信息描述。最大支持255个字符。

7. 配置完成后，单击“确定”，完成“DNAT规则”创建。

2.2.5 步骤 4：结果验证

操作场景

DNAT规则添加完成后，可以验证为目标NAT网关添加的DNAT规则。

操作前提

DNAT规则已经添加。

操作步骤

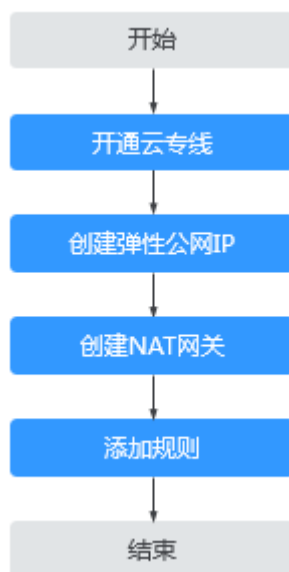
1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 在DNAT页签的DNAT规则列表中，可以看到DNAT规则详细信息，若“状态”为“运行中”，表示创建成功。

2.3 云间 NAT 网关高速访问互联网

2.3.1 简介

用户本地数据中心的服务器需要访问公网或为公网提供服务时，NAT网关可为您提供高效、优质的网络服务。可以通过开通云专线或VPN实现本地数据中心上云，然后创建NAT网关，通过配置SNAT规则实现访问公网。此快速入门流程以云专线用户为例，本地数据中心用户访问公网快速入门流程如图2-5所示。

图 2-5 本地数据中心用户访问公网流程图



2.3.2 步骤 1：开通云专线

操作场景

用户本地数据中心的服务器需要通过NAT网关实现访问公网或为公网提供服务，需要先通过云专线接入虚拟私有云。

操作步骤

详细步骤请参考《云专线用户指南》，申请开通云专线。

2.3.3 步骤 2：创建弹性公网 IP

操作场景

通过创建弹性公网IP来实现云专线/VPN接入公有云的用户，以NAT网关的形式共享弹性公网IP访问公网或为公网提供服务。

操作步骤

详细步骤请参考《弹性公网IP用户指南》，这里创建弹性公网IP后，无需绑定云主机。

2.3.4 步骤 2：创建公网 NAT 网关

操作场景

如果您要通过NAT网关访问公网或为公网提供服务，则需要创建公网NAT网关。

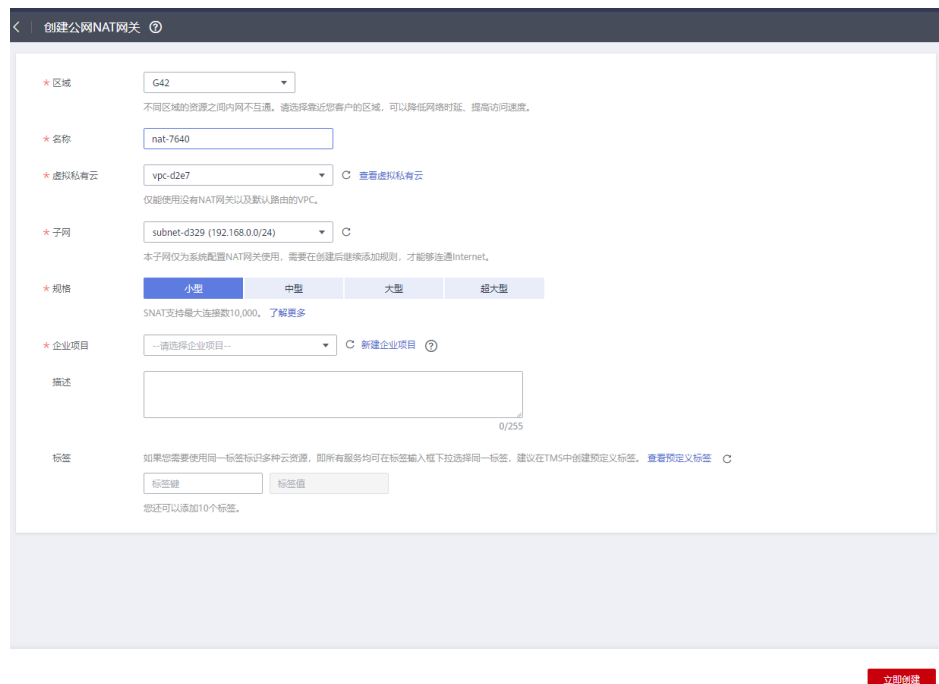
前提条件

- 创建公网NAT网关必须指定NAT网关所在VPC、子网、NAT网关规格。
- 确认VPC下没有默认路由。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击创建公网NAT网关，进入NAT网关创建页面。

图 2-6 创建公网 NAT 网关页面



4. 根据界面提示，配置NAT网关的基本信息，配置参数请参见表2-5。

表 2-5 参数说明

参数	参数说明
区域	NAT网关所在的区域。
名称	NAT网关名称。最大支持64个字符，仅支持数字、字母、_（下划线）、-（中划线）。
虚拟私有云	NAT网关所属的VPC。只能选择没有被其他NAT网关使用和没有默认路由的VPC。 VPC仅在创建NAT网关时可以选择，后续不支持修改。
子网	NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建NAT网关时可以选择，后续不支持修改。
规格	NAT网关的规格。 NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
企业项目	配置NAT网关归属的企业项目。当NAT网关配置企业项目时，该NAT网关将归属于该企业项目。当没有指定企业项目时，将默认使用项目名称为default的企业项目。
描述	NAT网关信息描述。最大支持255个字符。

表 2-6 SNAT 规则参数说明

参数	说明
使用场景	在云间NAT网关高速访问互联网的场景下，此处选择云专线。 表示通过云专线或VPN方式接入虚拟私有云的本地数据中心中的服务器，将通过SNAT的方式访问公网。
网段	通过配置云专线/VPN 本地数据中心的某个网段，使该网段中的服务器通过SNAT方式访问公网。
弹性公网IP	用来提供互联网访问的公网IP。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。
监控	为SNAT连接数设置告警。 可通过设置告警及时了解SNAT连接数的运行状况，从而起到预警作用。
描述	SNAT规则信息描述。最大支持255个字符。

6. 配置完成后，单击确定，完成“SNAT规则”创建。
7. 在SNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

说明

根据您的业务需求，可以为一个NAT网关添加多条SNAT规则。

2.3.6 步骤 5：添加 DNAT 规则

操作场景

NAT网关创建后，添加DNAT规则，则可以通过映射方式将您本地数据中心的服务器对互联网提供服务。

一个云主机的一个端口对应一条DNAT规则，如果您有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则来实现共享一个或多个弹性公网IP访问公网。

操作前提

已成功创建NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加DNAT规则的NAT网关名称。
4. 在NAT网关详情页面中，单击“DNAT规则”页签。
5. 在DNAT规则页签中，单击“添加DNAT规则”。

图 2-8 添加 DNAT 规则



6. 根据界面提示，配置添加DNAT规则参数，详情请参见表2-7。

表 2-7 DNAT 规则参数说明

参数	说明
使用场景	在云间NAT网关高速访问互联网的场景下，此处选择云专线。 表示通过云专线或VPN方式接入虚拟私有云的本地数据中心中的服务器，将通过DNAT的方式访问公网。
端口类型	分为所有端口和具体端口两种类型。 <ul style="list-style-type: none"> 所有端口：属于IP映射方式。此方式相当于为服务器配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标服务器实例上。 具体端口：属于端口映射方式。NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标服务器的指定端口上。
支持协议	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。

参数	说明
弹性公网IP	弹性公网IP地址。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。
公网端口	弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数，取值范围为1-65535。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
私网IP	用户本地数据中心的服务器的IP地址或者用户的私有IP地址。表示通过云专线或VPN接入到虚拟私有云的本地数据中心端的此私有IP服务器，可以通过DNAT方式为公网提供服务。端口类型为具体端口时，需要配置私网IP的端口。 表示此IP地址的云主机将通过DNAT方式为公网提供服务。
私网端口	在使用DNAT为云主机面向公网提供服务场景下，指云主机的端口号。当端口类型为具体端口时，需要配置此参数，取值范围为1-65535。 私网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
描述	DNAT规则信息描述。最大支持255个字符。

7. 配置完成后，单击“确定”，完成“DNAT规则”创建。
8. 在DNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

3 NAT 网关管理

3.1 创建 NAT 网关

操作场景

如果您要通过NAT网关访问公网或为公网提供服务，则需要创建公网NAT网关。

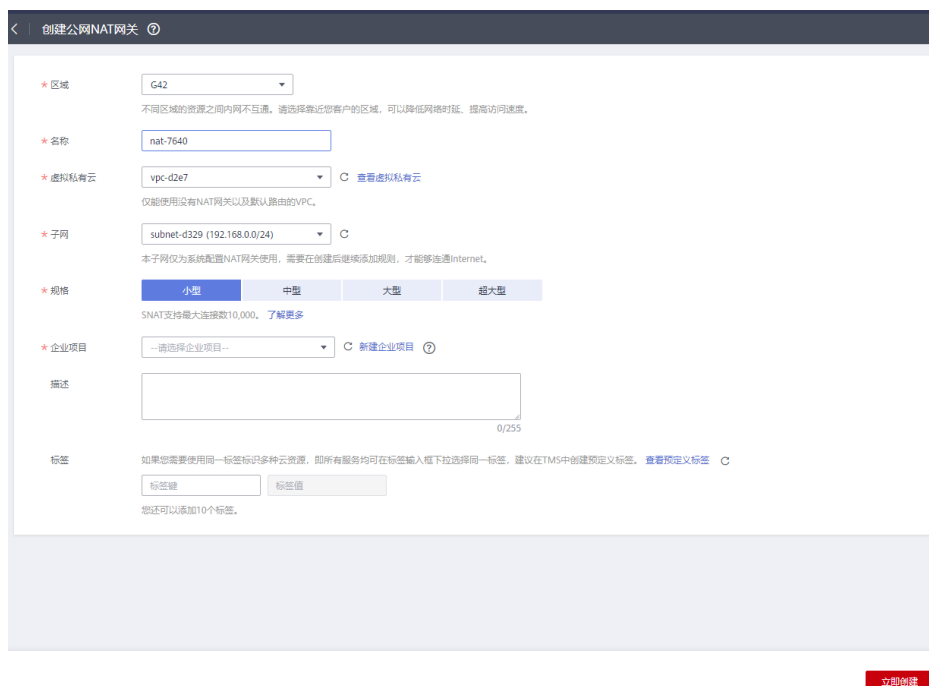
前提条件

- 创建公网NAT网关必须指定NAT网关所在VPC、子网、NAT网关规格。
- 确认VPC下没有默认路由。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击创建公网NAT网关，进入NAT网关创建页面。

图 3-1 创建公网 NAT 网关页面



4. 根据界面提示，配置NAT网关的基本信息，配置参数请参见表3-1。

表 3-1 参数说明

参数	参数说明
区域	NAT网关所在的区域。
名称	NAT网关名称。最大支持64个字符，仅支持数字、字母、_（下划线）、-（中划线）。
虚拟私有云	NAT网关所属的VPC。只能选择没有被其他NAT网关使用和没有默认路由的VPC。 VPC仅在创建NAT网关时可以选择，后续不支持修改。
子网	NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建NAT网关时可以选择，后续不支持修改。
规格	NAT网关的规格。 NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
企业项目	配置NAT网关归属的企业项目。当NAT网关配置企业项目时，该NAT网关将归属于该企业项目。当没有指定企业项目时，将默认使用项目名称为default的企业项目。
描述	NAT网关信息描述。最大支持255个字符。

5. 单击“立即创建”，在“规格确认”页面，您可以再次核对NAT网关信息。
6. 确认无误后，单击“提交”，开始创建NAT网关。
NAT网关的创建过程一般需要1-5分钟。
7. 在“NAT网关”列表，查看NAT网关状态。

3.2 查看 NAT 网关

操作场景

NAT网关创建后，可以查看已经创建的NAT网关的详情。

操作前提

NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要查看详情的NAT网关名称。
4. 系统跳转至目标NAT网关详情页面，即可查看目标NAT网关的详情。

3.3 修改 NAT 网关

操作场景

NAT网关创建后，如果您在使用过程中发现当前的NAT网关规格不能满足自己的需求，可以修改NAT网关规格、名称和描述。

提升NAT网关规格不影响业务；降低NAT网关规格取决于当前的业务量是否超过降档后规格的上限。

操作前提

NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要修改的NAT网关操作列中的“修改”。
4. 根据界面提示，修改NAT网关的名称、规格或者描述等信息。

图 3-2 修改 NAT 网关

修改规格

当前配置			
NAT网关名称	nat-b188	区域	G42
ID	87e286f8-91b3-4d09-8208-1f603c2c7577	规格	小型
描述	--		

* 名称

* 规格 小型 中型 大型 超大型
SNAT支持最大连接数10,000。 [了解更多](#)

描述
0/255

5. 修改完成后，单击“下一步”，进入信息确认页。
6. 确认修改详情后，单击“提交”，完成NAT网关信息的修改，在NAT网关列表可以看到修改后的信息。

3.4 删除 NAT 网关

操作场景

NAT网关创建后，如果您不再需要使用NAT网关，可以通过删除NAT网关，释放资源。

操作前提

必须保证NAT网关下的SNAT规则和DNAT规则已全部删除。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要删除的NAT网关操作列中的“删除”。
4. 在弹出的对话框中单击“是”，完成NAT网关的删除。

4 SNAT 规则管理

4.1 添加 SNAT 规则

操作场景

NAT网关创建成功后，您需要创建SNAT规则。通过创建SNAT规则，虚拟私有云子网中全部或部分云主机可以通过共享弹性公网IP访问公网，或云专线/VPN用户侧端该网段下的服务器可以通过共享弹性公网IP访问公网。

一个子网对应一条SNAT规则，如果VPC中有多个子网需要访问公网，则可以通过创建多个SNAT规则实现共享一个或多个弹性公网IP资源。

前提条件

- NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加SNAT规则的NAT网关名称。
4. 在SNAT规则页签中，单击“添加SNAT规则”。

图 4-1 添加 SNAT 规则



5. 根据界面提示，配置添加SNAT规则参数，详情请参见表4-1。

表 4-1 SNAT 规则参数说明

参数	场景条件	说明
使用场景	N/A	SNAT规则使用的场景。 当虚拟私有云中的云主机需要访问公网时，选择虚拟私有云。 当云专线/VPN本地数据中心端的服务器需要访问公网时，选择云专线。
类型	当使用场景为虚拟私有云时，需要配置此参数。	云主机访问公网的方式。 当虚拟私有云子网中的全部云主机需要通过SNAT方式访问公网时，选择子网，使该子网中的云主机通过SNAT方式访问公网。 当虚拟私有云子网中的部分云主机需要通过SNAT方式访问公网时，选择自定义，使该网段中的云主机通过SNAT方式访问公网。
子网	当使用场景为虚拟私有云，类型为子网时，需要配置此参数。	选择虚拟私有云中的子网，可实现该子网中的云主机通过SNAT的方式访问公网。

参数	场景条件	说明
弹性公网IP	<ul style="list-style-type: none"> 类型为虚拟私有云时需要配置此参数。 类型为云专线时需要配置此参数。 	<p>用来提供互联网访问的公网IP。</p> <p>这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。</p> <p>可选择多条EIP添加在SNAT规则中。一条SNAT规则最多添加20个EIP。SNAT规则使用多个EIP时，业务运行时会随机选取其中的一个。</p>
网段	<ul style="list-style-type: none"> 使用场景为虚拟私有云，类型为自定义时需要配置此参数。 使用场景为云专线时，需要配置此参数。 	<p>使用场景为虚拟私有云时，通过配置虚拟私有云子网中的某个网段，使该网段中的云主机通过SNAT方式访问公网。</p> <p>使用场景为云专线时，通过配置专线侧本地数据中心的某个网段，使该网段中的服务器通过SNAT方式访问公网。</p>
监控	N/A	<p>为SNAT连接数设置告警。</p> <p>可通过设置告警及时了解SNAT连接数的运行状况，从而起到预警作用。</p>
描述	N/A	NAT网关信息描述。最大支持255个字符。

6. 配置完成后，单击确定，完成“SNAT规则”创建。

说明

根据您的业务需求，可以为一个NAT网关添加多条SNAT规则。

4.2 查看 SNAT 规则

操作场景

SNAT规则添加完成后，可以查看为目标NAT网关添加的SNAT规则。

操作前提

SNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 在SNAT页签的SNAT规则列表中，查看目标NAT网关已经创建的SNAT规则详细信息。

4.3 修改 SNAT 规则

操作场景

添加SNAT规则后，如果SNAT规则设置有误，或者SNAT规则中的一些参数需要更新时，可以修改SNAT规则。

操作前提

NAT网关下存在成功添加的SNAT规则。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标NAT网关详情页面，单击“SNAT规则”页签。
5. 在SNAT规则列表中，单击目标SNAT规则操作列中的“修改”。
6. 在弹出的对话框中，修改参数中的内容。
7. 单击“确定”，完成SNAT规则的修改。

4.4 删除 SNAT 规则

操作场景

添加SNAT规则后，如果不再需要此SNAT规则，您可以删除SNAT规则。

操作前提

NAT网关下存在成功添加的SNAT规则。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 在SNAT页签的SNAT规则列表中，单击目标SNAT规则操作列中的“删除”。

图 4-2 删除 SNAT 规则



5. 在弹出的对话框中单击“是”，完成SNAT规则的删除。

5 DNAT 规则管理

5.1 添加 DNAT 规则

操作场景

NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机对互联网提供服务。

一个云主机的一个端口对应一条DNAT规则，如果您有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则。

操作前提

已成功创建NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加DNAT规则的NAT网关名称。
4. 在NAT网关详情页面中，单击“DNAT规则”页签。
5. 在DNAT规则页签中，单击“添加DNAT规则”。

图 5-1 添加 DNAT 规则



须知

配置DNAT规则后，需要放通对应的安全组规则，否则DNAT规则不能生效。

- 根据界面提示，配置添加DNAT规则参数，详情请参见表5-1。

表 5-1 DNAT 规则参数说明

参数	说明
使用场景	<p>虚拟私有云表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务。</p> <p>云专线表示通过云专线或VPN方式接入虚拟私有云的本地数据中心中的服务器，将通过DNAT的方式访问公网。</p>
端口类型	<p>分为所有端口和具体端口两种类型。</p> <ul style="list-style-type: none"> 所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云服务器实例上。 具体端口：属于端口映射方式。NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。

参数	说明
支持协议	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。
弹性公网IP	弹性公网IP地址。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。
公网端口	弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
私网IP	<ul style="list-style-type: none">当使用场景为虚拟私有云时，指云主机的IP地址。表示此IP地址的云主机将通过DNAT方式为公网提供服务。当使用场景为云专线时，指用户本地数据中心中服务器的IP地址或者用户的私有IP地址。表示通过云专线或VPN接入到虚拟私有云的本地数据中心端的此私有IP服务器，可以通过DNAT方式为公网提供服务。端口类型为具体端口时，需要配置私网IP的端口。
私网端口	在使用DNAT为云主机面向公网提供服务场景下，指云主机的端口号。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 私网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
描述	DNAT规则信息描述。最大支持255个字符。

7. 配置完成后，单击“确定”，可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

5.2 查看 DNAT 规则

操作场景

DNAT规则添加完成后，可以查看为目标NAT网关添加的DNAT规则。

操作前提

DNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。

3. 在NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，查看目标NAT网关已经创建的DNAT规则详细信息。

5.3 修改 DNAT 规则

操作场景

添加DNAT规则后，如果DNAT规则设置有误，或者DNAT规则中的一些参数需要更新时，可以修改DNAT规则。

操作前提

NAT网关下存在成功添加的DNAT规则。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
6. 在弹出的对话框中，修改参数中的内容。
7. 单击“确定”，完成DNAT规则的修改。

5.4 删除 DNAT 规则

操作场景

添加DNAT规则后，如果不需要此DNAT规则，您可以删除DNAT规则。

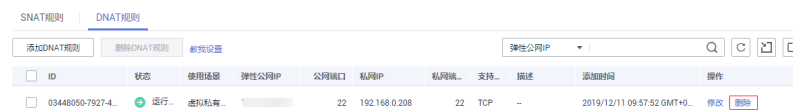
操作前提

NAT网关下存在成功添加的DNAT规则。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。

图 5-2 删除 DNAT 规则



ID	状态	使用场景	弹性公网IP	公网端口	私网IP	私网端口	支持	描述	添加时间	操作
03448050-7927-4...	运行	虚拟私有云		22	192.168.0.208	22	TCP	-	2019/12/11 09:57:52 GMT+0...	修改 删除

6. 在弹出的对话框中单击“是”，完成DNAT规则的删除。

5.5 批量删除 DNAT 规则

操作场景

添加DNAT规则后，如果不需要此DNAT规则，您可以删除DNAT规则。

操作前提

NAT网关下存在成功添加的DNAT规则。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，勾选目标DNAT规则，单击“删除DNAT规则”。
6. 在弹出的对话框中单击“是”，完成DNAT规则的批量删除。

5.6 DNAT 规则模板导入导出

操作场景

NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机对互联网提供服务。

一个云主机绑定一条DNAT规则，如果您有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则。

操作前提

已成功创建NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在NAT网关页面，单击需要添加DNAT规则的NAT网关名称。
4. 在NAT网关详情页面中，单击“DNAT规则”页签。
5. 在DNAT规则页签中，单击“导入DNAT规则列表”，下载模板。
6. 根据模板中的表头，填写DNAT规则参数，详情请参见[表5-2](#)。

表 5-2 DNAT 规则参数说明

参数	说明
使用场景	虚拟私有云表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务。 云专线表示通过云专线或VPN方式接入虚拟私有云的本地数据中心中的服务器，将通过DNAT的方式访问公网。
端口类型	分为所有端口和具体端口两种类型。 <ul style="list-style-type: none">所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云主机实例上。具体端口：属于端口映射方式。NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。
支持协议	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。
弹性公网IP	弹性公网IP地址及公网端口。 只能使用未绑定的弹性公网IP或者被绑定在当前VPC中DNAT规则上的弹性公网IP。
公网端口	弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
私网IP	<ul style="list-style-type: none">当使用场景为虚拟私有云时，指云主机的IP地址。表示此IP地址的云主机将通过DNAT方式为公网提供服务。当使用场景为云专线时，指用户本地数据中心中服务器的IP地址或者用户的私有IP地址。表示通过云专线或VPN接入到虚拟私有云的本地数据中心端的此私有IP服务器，可以通过DNAT方式为公网提供服务。端口类型为具体端口时，需要配置私网IP的端口。
私网端口	<ul style="list-style-type: none">当使用场景为虚拟私有云时，指云主机的端口号。当使用场景为云专线时，指用户本地数据中心中服务器的端口号或私有端口号。端口类型为具体端口时，需要配置此参数。 私网端口需要与对应弹性公网IP的公网端口数量保持一致。

7. 模板填写完后，单击“导入DNAT规则列表”图标，选择本地模板，单击“导入”。

图 5-3 导入 DNAT 规则模板



8. 可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。
9. 在DNAT规则页签中，单击“导出DNAT规则列表”，可导出已配置好的DNAT规则模板。

6 监控管理

6.1 支持的监控指标

功能说明

本节定义了NAT网关上报云监控的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控提供的管理控制台或API接口来检索NAT网关产生的监控指标。

命名空间

SYS.NAT

监控指标

指标	指标名称	含义	取值范围	测量对象&维度	监控周期 (原始指标)
snat_connection	SNAT连接数	该指标用于统计测量对象的SNAT连接数。 单位：个	≥ 0 个	测量对象： NAT网关主节点 测量维度： nat_gateway_id	1分钟
snat_connection	监控明细TOP20	该指标用于统计占用SNAT连接数最高的20个云主机的IP。 单位：个	≥0 个	测量对象： NAT网关实例 测量维度： nat_gateway_id	1分钟

指标	指标名称	含义	取值范围	测量对象&维度	监控周期 (原始指标)
inbound_bandwidth	入方向带宽	该指标用于统计SNAT入云方向带宽。 单位：比特/秒	≥0 bit/s	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
inbound_bandwidth	监控明细 TOP20	该指标用于统计占用SNAT入云方向带宽最高的20个云主机的IP。 单位：比特/秒	≥0 bit/s	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
outbound_bandwidth	出方向带宽	该指标用于统计SNAT出云方向带宽。 单位：比特/秒	≥0 bit/s	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
outbound_bandwidth	监控明细 TOP20	该指标用于统计占用SNAT出云方向带宽最高的20个云主机的IP。 单位：比特/秒	≥0 bit/s	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
inbound_pps	入方向PPS	该指标用于统计SNAT入云方向PPS。 单位：个	≥0个	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
inbound_pps	监控明细 TOP20	该指标用于统计占用SNAT入云方向PPS最高的20个云主机的IP。 单位：个	≥0 个	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟

指标	指标名称	含义	取值范围	测量对象&维度	监控周期 (原始指标)
outbound_pps	出方向PPS	该指标用于统计SNAT出云方向PPS。 单位：个	≥0个	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
outbound_pps	监控明细TOP20	该指标用于统计占用SNAT出云方向PPS最高的20个云主机的IP。 单位：个	≥0 个	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
inbound_traffic	入方向流量	该指标用于统计SNAT入云方向流量。 单位：字节	≥0 bytes	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
inbound_traffic	监控明细TOP20	该指标用于统计占用SNAT入云方向流量最高的20个云主机的IP。 单位：字节	≥0 bytes	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
outbound_traffic	出方向流量	该指标用于统计SNAT出云方向流量。 单位：字节	≥0 bytes	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟
outbound_traffic	监控明细TOP20	该指标用于统计占用SNAT出云方向流量最高的20个云主机的IP。 单位：字节	≥0 bytes	测量对象： NAT网关 SNAT 测量维度： nat_gateway_id	1分钟

维度

Key	Value
nat_gateway_id	NAT网关实例标识

6.2 创建告警规则

操作场景

通过设置NAT网关告警规则，用户可自定义监控目标与通知策略，及时了解NAT网关运行状况，从而起到预警作用。

操作步骤

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 在左侧导航树栏，选择“告警 > 告警规则”。
4. 在“告警规则”界面，单击“创建告警规则”进行添加，或者选择已有的告警规则进行修改，设置NAT网关的告警规则。
5. 规则参数设置完成后，单击“立即创建”。

NAT网关告警规则设置完成后，当符合规则的告警产生时，系统会自动进行通知。

说明

更多关于设置告警规则的信息，请参见《云监控用户指南》。

6.3 查看监控指标

前提条件

- NAT网关正常运行，并且已经创建SNAT规则。
- 由于监控数据的获取与传输会花费一定时间，因此，请等待一段时间后再查看监控数据。

操作场景

查看NAT网关的监控指标详情。

操作步骤

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 单击页面左侧的“云服务监控”，选择“NAT网关”。
4. 单击“操作”列的“查看监控指标”，查看NAT网关的监控指标详情。
支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”和“近7天”的数据。

图 6-1 查看监控指标



7 常见问题

7.1 NAT 网关

7.1.1 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。
- 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NAT网关访问外网。

7.1.2 NAT 网关如何实现高可用性？

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。

7.1.3 哪些端口无法访问？

出于安全因素考虑，部分运营商会下列端口进行拦截，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 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9996

7.1.4 通过 NAT 网关访问 Internet 失败该如何处理？

用户通过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。

7.1.5 NAT 网关是否支持更换 VPC?

不支持。

NAT网关在创建时选定VPC，不支持后续进行更换。


7.1.6 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，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. 单击页面右上角的“**My Quota**”图标 。
系统进入“服务配额”页面。
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?

目前系统暂不支持在线调整配额大小。如您需要调整配额，请拨打热线或发送邮件至客服，客服会及时为您处理配额调整的需求，并以电话或邮件的形式告知您实时进展。

在拨打热线或发送邮件之前，请您准备好以下信息：

- Account Name、Project Name、Project ID。
获取方式如下：登录云帐户管理控制台，在右上角单击帐户名，选择“我的认证”，在“我的认证”页面获取相关信息。
- 配额信息，包括：
 - 服务名
 - 配额类别
 - 需要的配额值

如您需要调整配额，请联系管理员。

7.2 SNAT

7.2.1 为什么使用 SNAT?

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）。

7.2.2 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EIP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。

7.2.3 主机通过 NAT 网关访问外网，请问 NAT 网关的宽带是多少？在哪里设置？

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NAT网关访问外网时，其带宽大小和您创建弹性公网IP时选择的带宽大小有关。

。

7.2.4 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。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。

7.2.5 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方式访问外网。

创建SNAT规则且当场景是云专线时，需要配置云专线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方式访问公网。

7.3 DNAT

7.3.1 为什么使用 DNAT?

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。

7.3.2 DNAT 规则是否支持更新操作?

DNAT规则不支持更新操作。

7.3.3 ECS 变更规格后 NAT 网关规则失效怎么处理?

ECS变更规格时，会导致已配置的NAT规则失效，需要删除后重新配置。

A 修订记录

发布日期	修改说明
2020-07-30	第一次正式发布。