



NAT 网关

用户使用指南

天翼云科技有限公司

目 录

1 产品简介.....	4
1.1 什么是 NAT 网关.....	4
1.2 产品优势	6
1.3 应用场景	7
1.4 产品规格	9
1.5 约束与限制	9
1.6 区域和可用区	10
1.7 基本概念	11
2 快速入门.....	12
2.1 使用 SNAT 访问公网	12
2.1.1 简介	12
2.1.2 步骤 1：创建弹性 IP.....	13
2.1.3 步骤 2：创建 NAT 网关.....	13
2.1.4 步骤 3：添加 SNAT 规则	14
2.2 使用 DNAT 为云主机面向公网提供服务	15
2.2.1 简介	15
2.2.2 步骤 1：创建弹性 IP.....	16
2.2.3 步骤 2：创建 NAT 网关.....	16
2.2.4 步骤 3：添加 DNAT 规则.....	18
2.3 云间 NAT 网关高速访问互联网.....	19
2.3.1 简介	19
2.3.2 步骤 1：开通云专线	19
2.3.3 步骤 2：创建弹性 IP.....	20
2.3.4 步骤 3：创建 NAT 网关.....	20
2.3.5 步骤 4：添加 SNAT 规则	22
2.3.6 步骤 5：添加 DNAT 规则.....	23
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	30
4.3 删除 SNAT 规则	31
5 DNAT 规则管理.....	32
5.1 添加 DNAT 规则.....	32
5.2 查看 DNAT 规则.....	33
5.3 删除 DNAT 规则.....	34
6 监控管理.....	35
6.1 支持的监控指标	35
6.2 创建告警规则	36
6.3 查看监控指标	36
7 常见问题.....	37
7.1 NAT 网关	37
7.1.1 NAT 网关、弹性 IP 带宽、VPC 内弹性云服务器与 VPC 是什么样的关系?	37
7.1.2 NAT 网关如何实现高可用性?	37
7.1.3 NAT 网关的配额是什么?	37
7.2 SNAT	38
7.2.1 为什么使用 SNAT?	38
7.2.2 什么是 SNAT 连接数?	38
7.3 DNAT.....	38
7.3.1 为什么使用 DNAT?	38
7.3.2 DNAT 规则是否支持更新操作?	38
A 修订记录	错误!未定义书签。

1 产品简介

1.1 什么是 NAT 网关

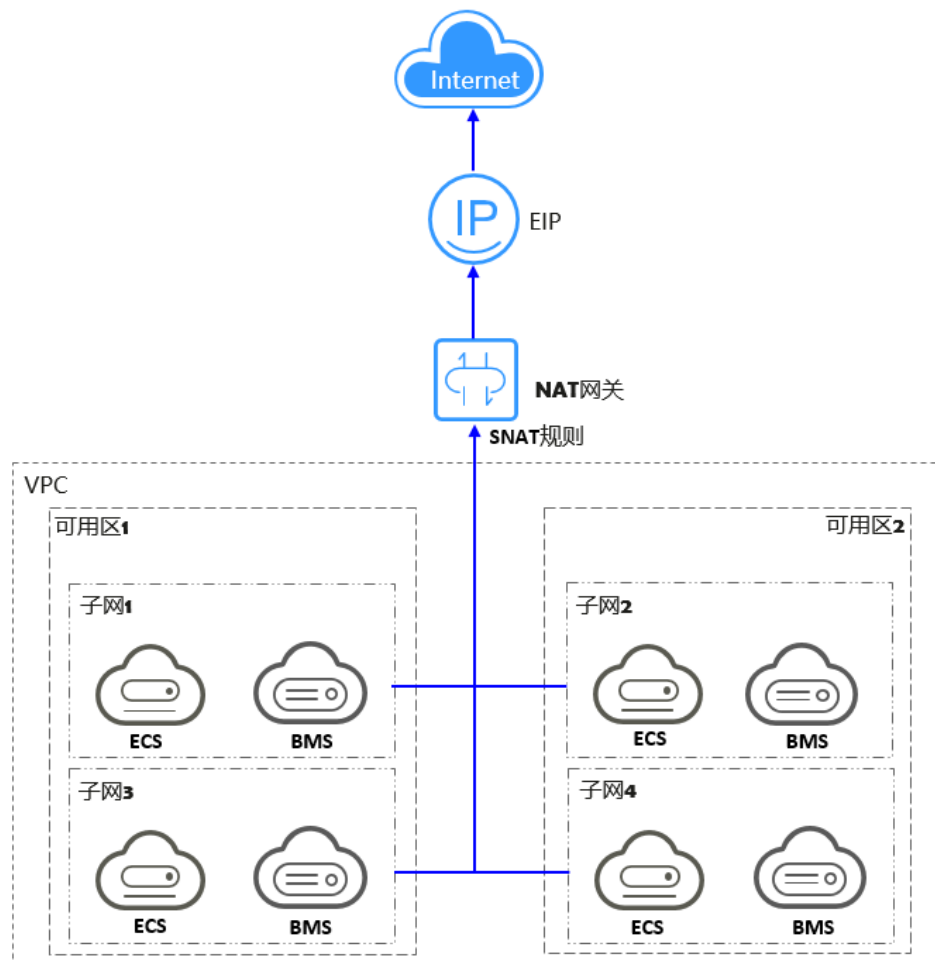
NAT 网关（NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）或者通过云专线/VPN 接入虚拟私有云的本地数据中心的服务器，提供最高 20Gbit/s 能力的网络地址转换服务，使多个云主机可以共享弹性 IP 访问 Internet 或使云主机提供互联网服务。

NAT 网关分为 SNAT 和 DNAT 两个功能。

- SNAT 功能通过绑定弹性 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 IP，安全，高效的访问互联网。

SNAT 架构如图 1-1 所示。

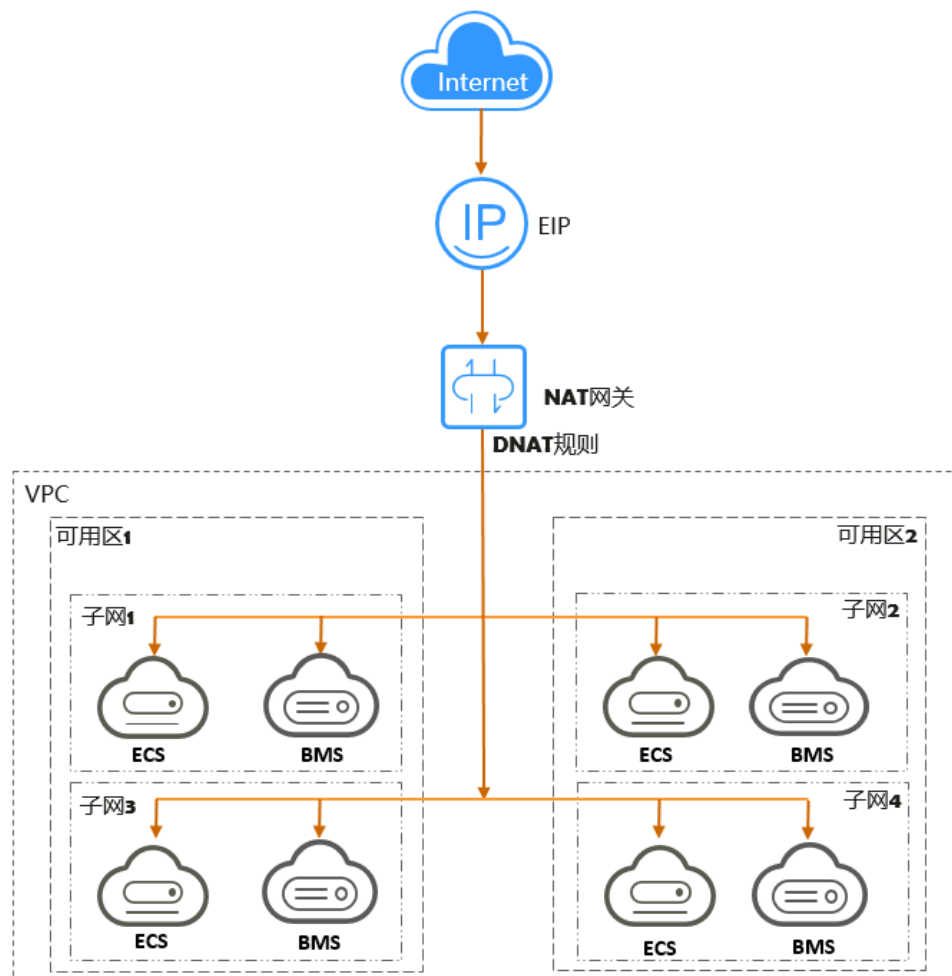
图1-1 SNAT 架构图



- DNAT 功能绑定弹性 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 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 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 IP 和带宽资源，多个云主机共享使用弹性 IP，有效降低成本。

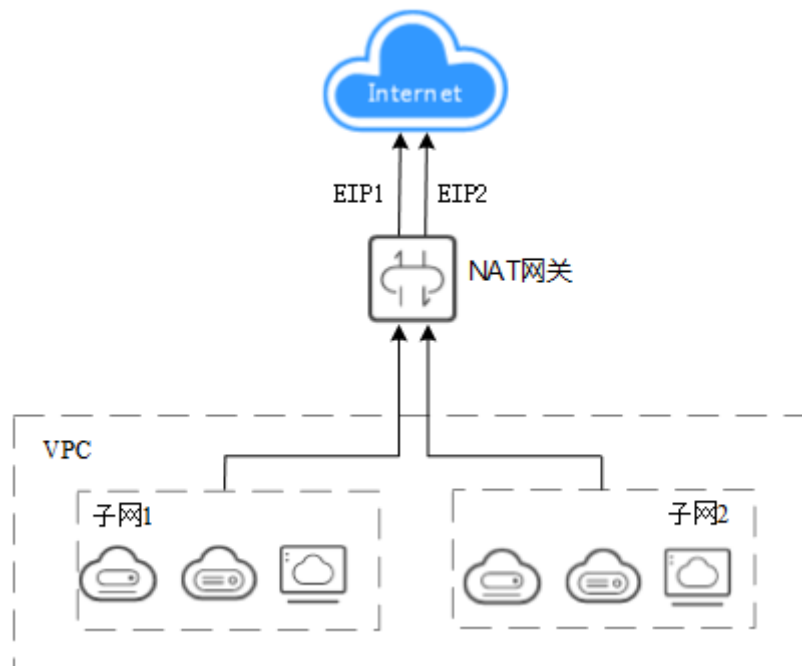
1.3 应用场景

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 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 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 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

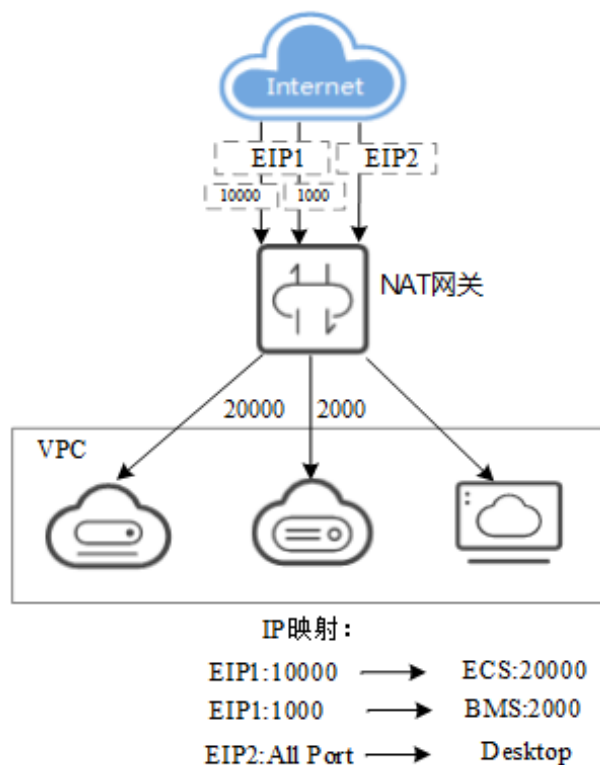
当 VPC 内的云主机需要面向公网提供服务时，可以使用 NAT 网关的 DNAT 功能。

DNAT 功能绑定弹性 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 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 IP，任何访问该弹性 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 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 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，裸金属服务器中的任何一个。

图1-4 使用 DNAT 为云主机面向公网提供服务

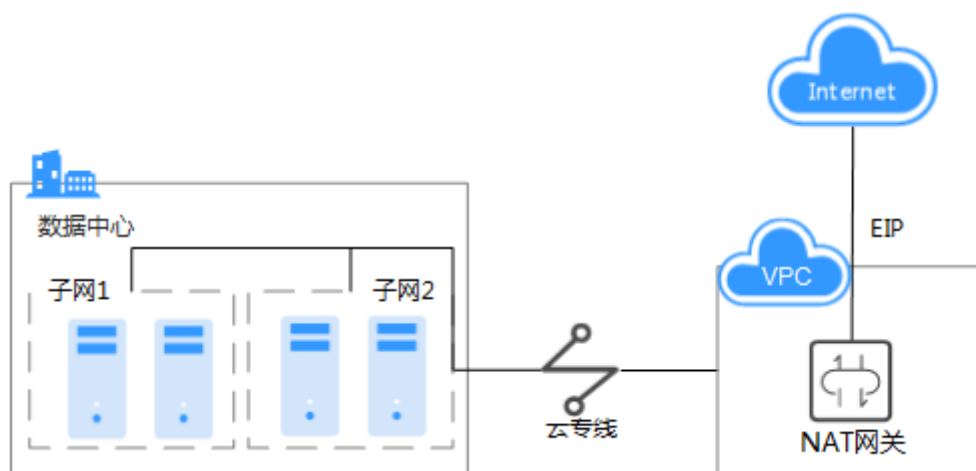


使用 SNAT 或 DNAT 高速访问互联网

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



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 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 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。

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 IP，不同网关下的规则必须使用不同的弹性 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 和 DNAT 不能共用同一个弹性 IP。
- DNAT 规则不支持将弹性 IP 绑定到虚拟 IP。
- 当云主机同时配置弹性 IP 服务和 NAT 网关服务时，数据均通过弹性 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。
- 一个云主机的一個端口对应一条 DNAT 规则，一个端口只能映射到一个 EIP，不能映射到多个 EIP。

1.6 区域和可用区

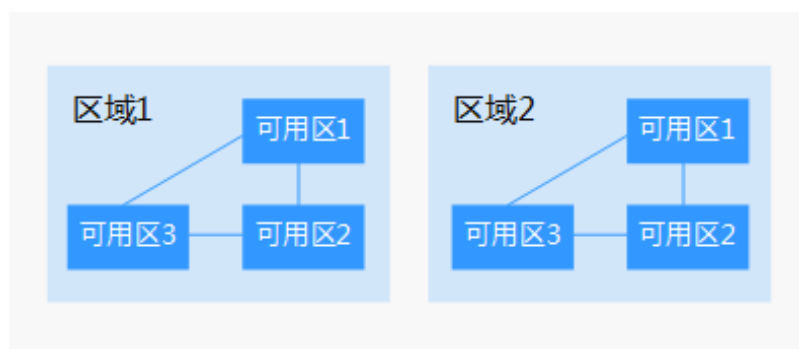
什么是区域、可用区？

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 1-6 阐明了区域和可用区之间的关系。

图1-6 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。请向管理员获取区域和终端节点信息。

1.7 基本概念

弹性 IP

弹性 IP 地址为可以直接访问 Internet 的 IP 地址。私有 IP 地址为云平台内局域网络所有的 IP 地址，私有 IP 地址禁止出现在 Internet 中。

弹性 IP 是基于互联网上的静态 IP 地址，将弹性 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 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 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 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 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）在没有绑定弹性 IP 的情况下需要访问公网，为了节省弹性 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 IP 的方式访问公网，可以按照图 2-1 所示，实现无弹性 IP 的云主机访问公网。

图2-1 无弹性 IP 的云主机访问公网流程图



2.1.2 步骤 1：创建弹性 IP

操作场景

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

操作步骤

详细步骤请参考《虚拟私有云用户指南》，这里创建弹性 IP 后，无需绑定云主机。

2.1.3 步骤 2：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 NAT 网关。

前提条件

- 创建 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

- 登录管理控制台。
- 在系统首页，单击“网络 > NAT 网关”。
- 在 NAT 网关页面，单击“创建 NAT 网关”，进入 NAT 网关创建页面。

图2-2 创建 NAT 网关页面

区域 西安类生产 温馨提示：页面右上角切换区域

名称

虚拟私有云 vpc-testjlp111 [查看虚拟私有云](#)

子网 subnet-testjlp (192.168.0.0/24)

规格 小型 中型 大型 超大型

描述

0/255

- 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。
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 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 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 IP	N/A	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 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。

6. 配置完成后，单击确定，完成“SNAT 规则”创建。

说明

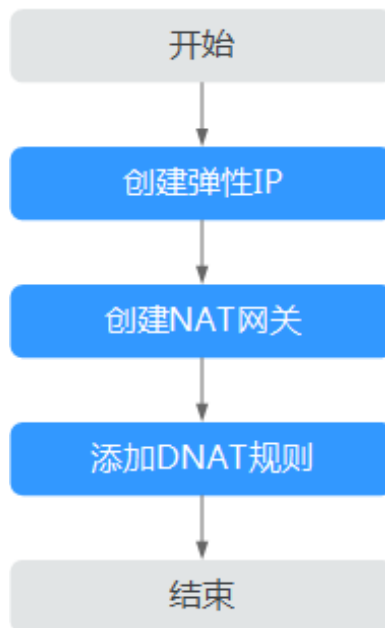
根据您的业务需求，可以为一个 NAT 网关添加多条 SNAT 规则。

2.2 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、裸金属服务器）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 IP

操作场景

通过创建弹性 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《虚拟私有云用户指南》，这里创建弹性 IP 后，无需绑定云主机。

2.2.3 步骤 2：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 NAT 网关。

前提条件

- 创建 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 NAT 网关”，进入 NAT 网关创建页面。

图2-4 创建 NAT 网关页面

区域 西安类生产 温馨提示：页面右上角切换区域

名称

虚拟私有云 vpc-testjlpiiii [查看虚拟私有云](#) 
仅能使用没有NAT网关以及默认路由的VPC。

子网 subnet-testjlp (192.168.0.0/24) 
NAT网关会在该子网中分配一个IP地址，请确保子网有可用IP地址。

规格 小型 中型 大型 超大型
NAT网关支持最大连接数10,000，每秒新建连接数1,000。 [了解更多...](#)

描述

0/255

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。
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。
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 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。 • 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 IP，任何访问该弹性 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 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 IP	弹性 IP 地址。 这里只能选择没有被绑定的弹性 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。
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。

参数	说明
	端口类型为具体端口时，需要配置私网 IP 的端口。

7. 配置完成后，单击“确定”，完成“DNAT 规则”创建。

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 规则实现访问公网或配置 DNAT 规则为互联网提供服务。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

1. 登录控制台。
 2. 在管理控制台左上角单击  图标，选择区域和项目。
 3. 在系统首页，单击“网络 > 云专线”。
 4. 导航栏选择“云专线 > 物理专线”，在物理专线页面，创建物理专线，详细步骤请参考《云专线用户指南》。
 5. 导航栏选择“云专线 > 虚拟网关”，在虚拟网关页面，创建虚拟网关，在“创建虚拟网关”对话框中，输入对应的参数，其中“VPC 网段”建议设置为“0.0.0.0/0”。
- 详细步骤请参考《云专线用户指南》。
6. 导航栏选择“云专线 > 虚拟接口”，在控制台虚拟接口页面，创建虚拟接口，在“创建虚拟接口”对话框中，输入对应的参数。详细步骤请参考《云专线用户指南》。

2.3.3 步骤 2：创建弹性 IP

操作场景

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

操作步骤

详细步骤请参考《虚拟私有云用户指南》，这里创建弹性 IP 后，无需绑定云主机。

2.3.4 步骤 3：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 NAT 网关。

前提条件

- 创建 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 NAT 网关”，进入 NAT 网关创建页面。

图2-6 创建 NAT 网关页面

区域 西安类生产 温馨提示：页面右上角切换区域

名称

虚拟私有云 vpc-testjlpiiii [查看虚拟私有云](#)

子网 subnet-testjlp (192.168.0.0/24)

规格 小型 中型 大型 超大型

描述

0/255

NAT网关支持最大连接数10,000，每秒新建连接数1,000。 [了解更多...](#)

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 and 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。
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。

2.3.5 步骤 4：添加 SNAT 规则

操作场景

NAT 网关创建成功后，您可以为 NAT 网关添加 SNAT 规则。通过添加 SNAT 规则，云专线用户侧端的服务器可以通过共享弹性 IP 访问互联网。

一个网段对应一条 SNAT 规则，如果云专线用户侧有多个网段中的服务器需要访问公网，则可以通过创建多个 SNAT 规则实现共享一个或多个弹性 IP 资源。

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，详情请参见表 2-6。

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 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 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。

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 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”。
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。 • 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 IP，任何访问该弹性 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 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。
弹性 IP	弹性 IP 地址。 这里只能选择没有被绑定的弹性 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。
私网 IP	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

参数	说明
	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。

7. 配置完成后，单击“确定”，完成“DNAT 规则”创建。

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 NAT 网关。

前提条件

- 创建 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 NAT 网关”，进入 NAT 网关创建页面。

图3-1 创建 NAT 网关页面

区域 西安类生产 温馨提示：页面右上角切换区域

名称

虚拟私有云 vpc-testjlpiiii [查看虚拟私有云](#)

子网 subnet-testjlp (192.168.0.0/24)

规格 小型 中型 大型 超大型

描述

0/255

NAT网关支持最大连接数10,000，每秒新建连接数1,000。 [了解更多...](#)

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。
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，可以通过修改 NAT 网关的名称、规格或者描述来完成。

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。
5. 修改完成后，单击“确认”，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，节省费用。

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 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 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 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，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，	云主机访问公网的方式。

参数	场景条件	说明
	需要配置此参数。	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。
弹性 IP	- 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。	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 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。
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。 - 使用场景为云专线时，需要配置此参数。	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。 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。

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 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”。
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，一个端口只能映射到一个 EIP，不能映射到多个 EIP。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”。

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。

6. 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	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 IP，为公网提供服务。

参数	说明
	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。 - 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 IP，任何访问该弹性 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 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 IP	弹性 IP 地址。 这里只能选择没有被绑定的弹性 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 IP，或者被绑定到当前 NAT 网关中 SNAT 规则上的弹性 IP。
私网 IP	- 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。

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 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”。
6. 在弹出的对话框中单击“是”，完成 DNAT 规则的删除。

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

表6-1 NAT 网关支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	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：count	≥ 0 个	NAT 网关实例	1 分钟
云主机 IP 地址集	SNAT TOP 连接数云主机 IP 地址集	该指标用于统计占用 SNAT 连接数最高的个云主机的 IP。 单位：个	≥ 0 个	NAT 网关实例	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”，根据界面提示，填写对应参数。
5. 规则参数设置完成后，单击“下一步”，根据界面提示，配置规则信息参数。
6. 单击“创建”，完成 SNAT 连接数告警规则的创建。设置告警规则后，超过设置的阈值，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. 在左上角中的切换区域下拉列框中，选择目标区域。
 3. 选择“管理与部署 > 云监控”。
 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“查看监控图表”，查看 NAT 网关的监控指标详情。
- 支持查看“近 1 小时”、“近 3 小时”和“近 12 小时”的数据。

7 常见问题

7.1 NAT 网关

7.1.1 NAT 网关、弹性 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 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 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，降低风险提高可用性。

7.1.3 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. 单击页面右上角的“My Quota”图标。

系统进入“服务配额”页面。

3. 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：

- 帐号名，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“我的凭证”，在“我的凭证”页面获取“帐号名”。

- 配额信息，包括：服务名、配额类别、需要的配额值。

7.2 SNAT

7.2.1 为什么使用 SNAT？

一些弹性云服务器不仅需要系统提供的服务，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。

7.3 DNAT

7.3.1 为什么使用 DNAT？

DNAT 功能绑定弹性 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 IP，为互联网提供服务。详见 5.1 添加 DNAT 规则。

7.3.2 DNAT 规则是否支持更新操作？

DNAT 规则支持更新操作。