NAT 网关

用户指南

文档版本 01

发布日期 2024-12-24

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

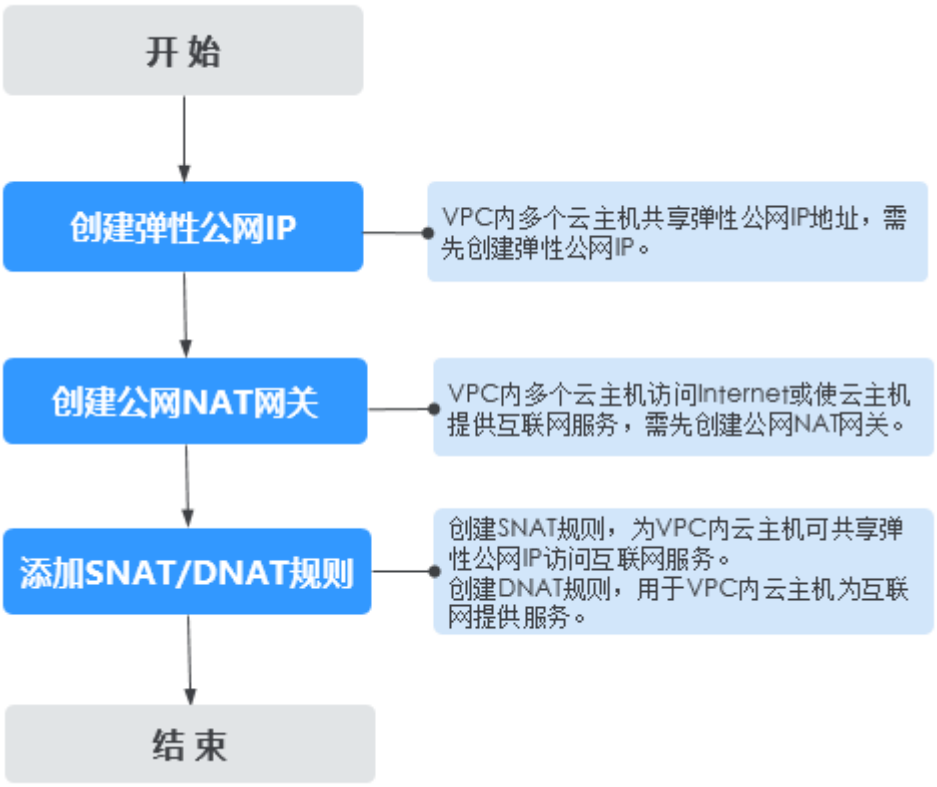
1.1 公网 NAT 网关简介

公网NAT网关（Public NAT Gateway）能够为虚拟私有云内的云主机或者通过云专线/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。

公网NAT网关可以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。

公网NAT网关使用流程如下：

图 1-1 公网 NAT 使用流程



1.2 购买公网 NAT 网关

操作场景

如果您要通过公网NAT网关访问公网或为公网提供服务，则需要购买公网NAT网关。

约束与限制

- 同一个公网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。
- 一个VPC支持关联多个公网NAT网关。
- SNAT、DNAT可以共用同一个弹性公网IP，节省弹性公网IP资源。但是在选用全端口模式下，DNAT优先占用全部端口，这些端口不能被 SNAT 使用。因此SNAT规则不能和全端口的DNAT规则共用EIP，以免出现业务相互抢占问题。
- 公网NAT网关支持转换的资源类型不包括企业型VPN。
- 当云主机同时配置弹性公网IP服务和公网NAT网关服务时，数据均通过弹性公网IP转发。
- 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

前提条件

- 购买公网NAT网关必须指定公网NAT网关所在VPC、子网。
- 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在购买公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所购买的公网NAT网关。如果在购买公网NAT网关前，VPC默认路由表下已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关购买成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。

操作步骤

1. 进入**购买公网NAT网关页面**。
2. 根据界面提示，配置公网NAT网关的基本信息，配置参数请参见**表1-1**。

表 1-1 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
计费模式	公网NAT网关支持按需计费、包年/包月。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四规格类型，可通过“了解更多”查看各规格详情。
名称	公网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点号）。
虚拟私有云	公网NAT网关所属的VPC。 VPC仅在购买公网NAT网关时可以选择，后续不支持修改。 **说明** 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在购买公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所购买的公网NAT网关。如果在购买公网NAT网关前，VPC默认路由表下已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关购买成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。

参数	参数说明
子网	公网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在购买公网NAT网关时可以选择，后续不支持修改。 本子网仅为系统配置NAT网关使用，NAT网关对整个VPC生效，需要在购买后继续添加规则，才能够连通Internet。
企业项目	配置公网NAT网关归属的企业项目。当公网NAT网关配置企业项目时，该公网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。
高级配置（可选）	单击下拉箭头，可配置公网NAT网关的高级参数，比如描述。
高级配置 > SNAT连接TCP老化时间（秒）	通过SNAT规则建立的TCP连接的超时时间，如果TCP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。
高级配置 > SNAT连接UDP老化时间（秒）	通过SNAT规则建立的UDP连接的超时时间，如果UDP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。
高级配置 > SNAT连接ICMP老化时间（秒）	通过SNAT规则建立的ICMP连接的超时时间，如果ICMP连接在该时间内没有数据交换将被关闭。 取值范围：10~7200。
高级配置 > TCP连接延迟关闭时间（秒）	TCP连接关闭时TIME_WAIT状态持续时间。 取值范围：0~1800。
高级配置 >描述	公网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。
高级配置 >标签	公网NAT网关的标识，包括键和值。可以创建20个标签。 如您的组织已经设定公网NAT网关的相关标签策略，则需按照标签策略规则为公网NAT网关添加标签。标签如果不符合标签策略的规则，则可能会导致公网NAT网关创建失败，请联系组织管理员了解标签策略详情。 标签的命名规则请参考**表1-2**。

表 1-2 标签命名规则

参数	规则
键	• 不能为空。 • 对于同一NAT网关键值唯一。 • 长度不超过36个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。
值	• 长度不超过43个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。

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

说明

公网NAT网关创建成功后，查看该公网NAT网关所在的VPC的默认路由表下是否存在0.0.0.0/0的默认路由指向该公网NAT网关，如果不存在，请在默认路由表中添加一条指向该公网NAT网关的路由，或创建一个自定义路由表并在自定义路由表中添加0.0.0.0/0的默认路由指向该公网NAT网关。添加路由规则详情请参考**在路由表中添加路由**。

高频问题

NAT 网关连接数超过规格限制怎么办?

- 为避免因连接数超过公网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公网NAT网关监控指标，并为SNAT连接数合理设置告警。
- 如果您的业务连接数超过当前NAT网关规格，建议您及时通过**修改公网NAT网关**进行扩容。

修改 NAT 网关规格对业务有影响吗?

提升公网NAT网关规格不影响业务；降低公网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。

1.3 管理公网 NAT 网关

1.3.1 修改公网 NAT 网关

操作场景

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

提升公网NAT网关规格不影响业务；降低公网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。

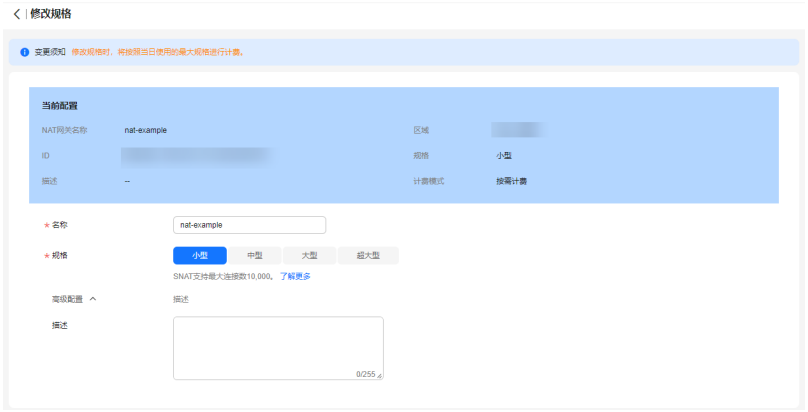
说明

- 降低公网NAT网关规格需要评估当前业务量是否超过降低后的规格上限，避免造成业务中断。
- 提升公网NAT网关规格，业务不受影响。

修改公网 NAT 网关

1. 进入**公网NAT网关列表页面**。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在公网NAT网关页面，单击需要修改的公网NAT网关操作列中的“修改”。
4. 根据界面提示，修改公网NAT网关的名称、规格或者描述信息。

图 1-2 修改 NAT 网关



5. 修改完成后，单击“确认”，完成公网NAT网关信息的修改，在公网NAT网关列表可以看到修改后的信息。

1.3.2 删除/退订公网 NAT 网关

操作场景

公网NAT网关创建后，如果您不再需要使用公网NAT网关，可以通过删除/退订公网NAT网关，释放资源，节省费用。

说明

- 对于按需计费模式的公网NAT网关，直接按照如下步骤**删除公网NAT网关**，即可完成退订。

操作前提

- 必须保证公网NAT网关下的SNAT规则和DNAT规则已全部删除。如果公网NAT网关下的SNAT规则和DNAT规则未被全部删除，则无法执行删除，请先在公网NAT网关页面进行**删除SNAT规则**和**删除DNAT规则**操作。

操作步骤

1. 进入**公网NAT网关列表页面**。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在公网NAT网关页面，单击需要删除的公网NAT网关操作列中的“删除”。
4. 在删除确认对话框，输入“DELETE”。
5. 单击“确定”。

1.4 管理 SNAT 规则

1.4.1 添加 SNAT 规则

操作场景

公网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/云连接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。

约束与限制

- VPC内的每个子网只能添加一条SNAT规则。
- 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。
- 公网NAT网关支持添加的SNAT规则的数量没有限制。

添加 SNAT 规则

1. 进入**公网NAT网关列表页面**。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在公网NAT网关页面，单击需要添加SNAT规则的公网NAT网关名称。
4. 在SNAT规则页签中，单击“添加SNAT规则”。

图 1-3 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1-3**。

表 1-3 SNAT 规则参数说明

参数	说明
使用场景	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/云连接。
网段	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/云连接时，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。
公网IP类型	用来提供互联网访问的公网IP的类型。 使用弹性公网IP时，支持选择未绑定的弹性公网IP或者被绑定在当前VPC中SNAT规则上的弹性公网IP。 使用全域弹性公网IP时，支持选择未被使用的全域弹性公网IP或者已经被当前NAT网关的SNAT规则所使用的全域弹性公网IP。
监控	为SNAT连接数设置告警。 可通过设置告警及时了解SNAT连接数运行状况，从而起到预警作用。

参数	说明
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

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，可以为一个公网NAT网关添加多条SNAT规则。
   - VPC内的每个子网只能添加一条SNAT规则。

1.4.2 查看 SNAT 规则

操作场景

SNAT规则添加完成后，可以查看为目标公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。
   进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 在SNAT页签的SNAT规则列表中，查看目标公网NAT网关已经创建的SNAT规则详细信息。

1.4.3 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。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

操作前提

公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。
   进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 系统跳转至目标公网NAT网关详情页面，单击“SNAT规则”页签。
6. 在SNAT规则列表中，单击目标SNAT规则操作列中的“修改”。
7. 在弹出的对话框中，修改参数中的内容。
8. 单击“确定”，完成SNAT规则的修改。

1.4.4 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

公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。
   进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 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”。
6. 如果您确定要删除，在弹出的对话框中输入 “DELETE”，然后单击“确定”，完成SNAT规则的删除。

1.5 管理 DNAT 规则

1.5.1 添加 DNAT 规则

操作场景

公网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。

约束限制

- 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。
- 公网NAT网关支持添加的DNAT规则的数量为200个。

操作步骤

1. 进入**公网NAT网关列表页面**。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在公网NAT网关页面，单击需要添加DNAT规则的公网NAT网关名称。
4. 在公网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 1-4 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1-4**。

表 1-4 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/云连接表示通过云专线/云连接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。公网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。
公网IP类型	用来提供互联网访问的公网IP的类型。 使用弹性公网IP时，支持选择未绑定的弹性公网IP或者被绑定在当前VPC中DNAT规则上的弹性公网IP。 使用全域弹性公网IP时，支持选择未被使用的全域弹性公网IP或者已经被当前NAT网关的DNAT规则所使用的全域弹性公网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。
实例类型	选择对外部公网提供服务的实例类型。 ● 服务器 ● 虚拟IP地址 ● 自定义
网卡	服务器网卡。实例类型为服务器时，需要配置此参数。
私网IP	● 当使用场景为虚拟私有云时，私网IP地址只能为本虚拟私有云下云主机的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/云连接时，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/云连接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。

参数	说明
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，且不能包含“<”和“>”。

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。

须知

配置DNAT规则后，需在对应的云主机中放通对应的安全组规则，否则DNAT规则不能生效。

1.5.2 查看 DNAT 规则

操作场景

DNAT规则添加完成后，可以查看为目标公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。
   进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，查看目标公网NAT网关已经创建的DNAT规则详细信息。

1.5.3 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。

当您修改DNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

操作前提

公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
7. 在弹出的对话框中，修改参数中的内容。
8. 单击“确定”，完成DNAT规则的修改。

1.5.4 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

公网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. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标公网NAT网关的名称。
5. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
7. 如果您确定要删除，在弹出的对话框中输入 “DELETE”，然后单击“确定”，完成DNAT规则的删除。

1.5.5 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

公网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. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
4. 在公网NAT网关页面，单击目标NAT网关的名称。
5. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，勾选目标DNAT规则，单击“删除DNAT规则”。
7. 在弹出的对话框中单击“确定”，完成DNAT规则的批量删除。

1.5.6 DNAT 规则模板导入导出

操作场景

公网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。

在不同环境或多个NAT网关间迁移配置规则时，您可以通过DNAT规则的导入和导出功能，简化DNAT规则配置的过程，提高DNAT规则配置的灵活性和效率。

导入 DNAT 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. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
4. 在公网NAT网关页面，单击需要导入DNAT规则的公网NAT网关名称。
5. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
6. 在DNAT规则页签中，单击“导入”后，下载模板。
7. 根据模板中的表头，填写DNAT规则参数，详情请参见**表1-5**。

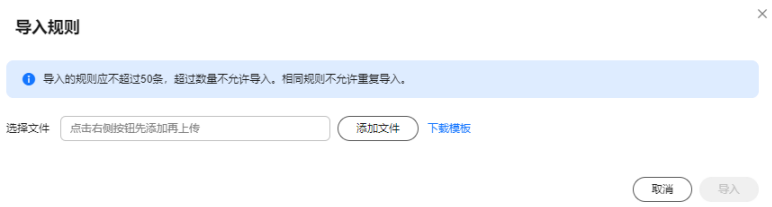
表 1-5 DNAT 规则参数说明

参数	说明
使用场景	分为虚拟私有云和云专线/云连接两种方式。 • 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/云连接：表示通过云专线/云连接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的方式为公网提供服务。

参数	说明
支持协议	协议类型分为TCP、UDP、全部三种类型。
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。
全域弹性公网IP	支持选择未被使用的全域弹性公网IP或者已经被当前NAT网关的DNAT规则所使用的全域弹性公网IP。
公网端口	弹性公网IP的端口。当端口类型为“全部”时，不需要配置此参数。 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	• 当使用场景为虚拟私有云时，私网IP地址只能为本虚拟私有云下云主机的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/云连接时，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/云连接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。 • 协议类型为TCP、UDP时，需要配置私网IP的端口。
私网端口	• 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/云连接时，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“全部”时，不需要配置此参数。 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。
描述	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

8. 模板填写完后，单击“添加文件”，选择本地模板，单击“导入”。

图 1-5 导入 DNAT 规则模板



9. 可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示导入成功。

导出 DNAT 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. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。
   进入公网NAT网关页面。
4. 在公网NAT网关页面，单击需要导出DNAT规则的公网NAT网关名称。
5. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
6. 在DNAT规则列表页，选择目标规则后，单击“导出”。
   a. 选择“导出全部数据到XLSX”：系统会将当前区域内所有数据自动导出为Excel文件，并下载至本地。
   b. 选择“导出已选中数据到XLSX”：系统会将当前区域内您所选中的数据自动导出为Excel文件，并下载至本地。

2 私网 NAT 网关

2.1 私网 NAT 网关简介

什么是私网 NAT 网关?

私网NAT网关（Private 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）提供私网地址转换服务。您可以在私网NAT网关上配置SNAT、DNAT规则，可将源、目的网段地址转换为中转IP，通过使用中转IP实现VPC内的云主机与其他VPC、云下IDC互访。

私网NAT网关分为SNAT和DNAT两个功能：

- SNAT功能通过绑定中转IP，可实现VPC内跨可用区的多个云主机共享中转IP，访问外部数据中心或其他VPC。
- 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。

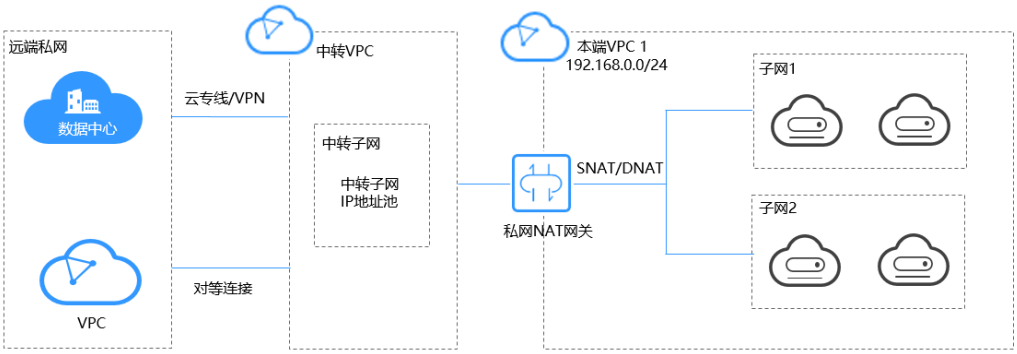
中转子网

中转子网相当于一个中转网络，您可以在中转子网中创建私网IP，即中转IP，使本端VPC中的云主机可以共享该中转IP访问用户IDC或其他远端VPC。

中转VPC

中转子网所在VPC。

图 2-1 私网 NAT 网关



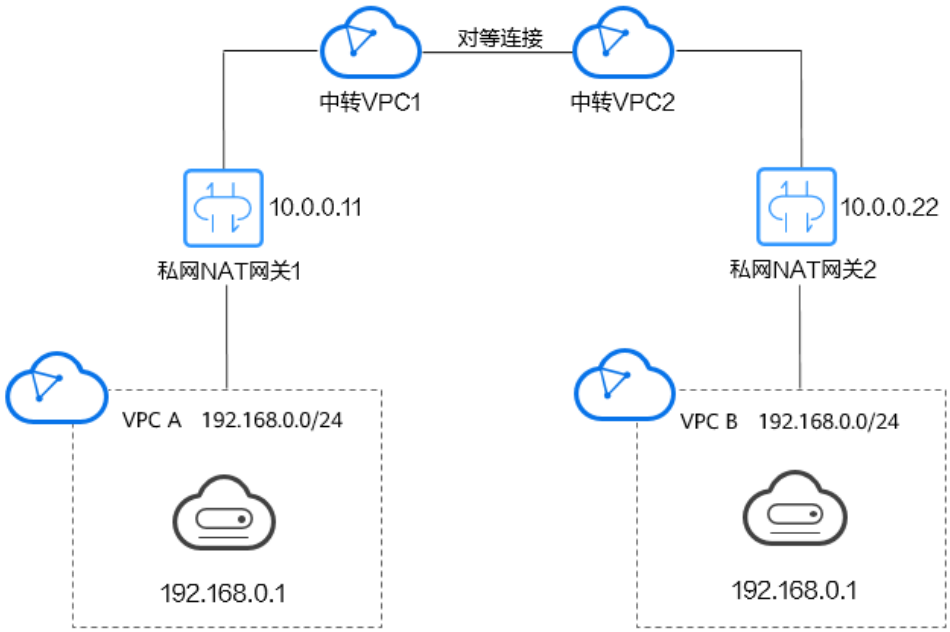
应用场景

- 重叠网段VPC间互通

  私网NAT网关提供私网地址转换服务，利用两个私网NAT网关，配置SNAT、DNAT规则，可同时将源、目的网段地址转换为中转IP，通过使用中转IP实现两VPC间互通。私网NAT网关解决了两个重叠网段虚拟私有云中的云主机互相访问的问题。

  如下图所示，创建一个中转VPC，然后使用两个私网NAT网关将VPC A中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.11、将VPC B中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.22，通过转化后的IP地址相互访问。

  图 2-2 重叠网段 VPC 间互通

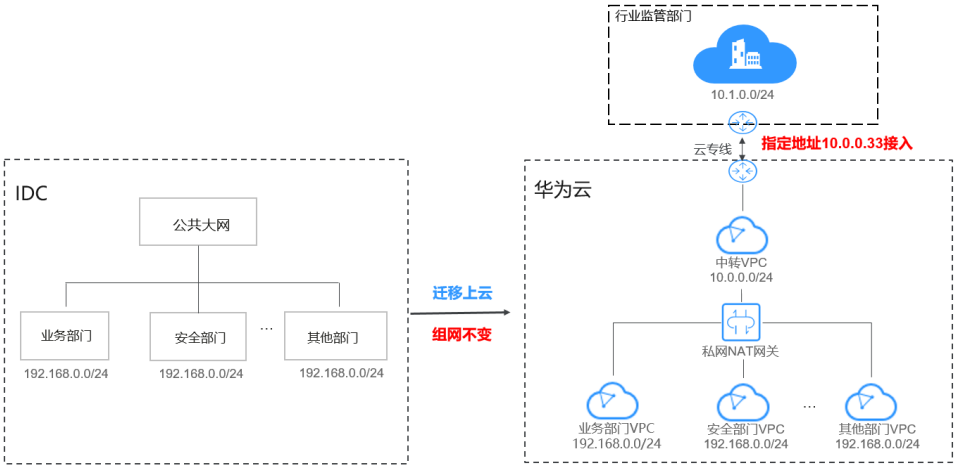
  

- 企业网络上云及指定IP接入

  大企业等机构上云，希望迁移上云保持组网不变，使用私网NAT网关无需对网络做任何更改即可保持原有方式互通。同时，行业监管部门要求指定地址接入，使用私网NAT网关将各部门的IP地址映射为指定地址接入行业监管部门，满足企业安全规范。

  如下图所示，企业部门间存在网段重叠，使用私网NAT网关，实现企业各部门迁移上云后组网不变，部门间保持原有方式互通，简化了IDC上云的网络规划；使用私网NAT网关，配置SNAT规则，将各部门的IP地址映射为符合要求的10.0.0.33地址接入行业监管部门，提升企业的安全性。

图 2-3 企业网络上云及指定 IP 接入



公网 NAT 网关与私网 NAT 网关对比

公网NAT网关通过配置SNAT规则将私有IP映射为弹性公网IP，实现VPC内的云主机通过共享弹性公网IP访问互联网；配置DNAT规则共享弹性公网IP为公网提供服务。

私网NAT网关通过配置SNAT规则将私有IP映射为中转IP，实现VPC内的云主机访问私网中的用户数据中心或其他VPC；配置DNAT规则共享中转IP为私网提供服务。

表1概括了公网NAT网关和私网NAT网关间的差异：

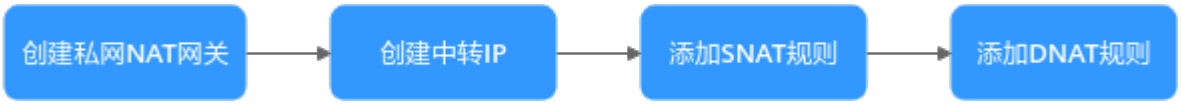
表 2-1 公网 NAT 网关与私网 NAT 网关对比

功能项	公网NAT网关	私网NAT网关
功能	私网和公网间互通	私网和私网间互通
SNAT功能	访问公网	访问私网中的IDC或其他VPC
DNAT功能	为公网提供服务	为私网中的IDC或其他VPC提供服务
互通媒介	弹性公网IP	中转IP

私网 NAT 网关使用流程

私网NAT网关的使用流程如下：

图 2-4 私网 NAT 网关使用流程



私网NAT网关配置完成，如果需要连接IDC或其他虚拟私有云，请参考**连接IDC或其他虚拟私有云**。

2.2 购买私网 NAT 网关

操作场景

如果您的VPC中的资源要通过私网NAT网关访问用户本地数据中心（IDC）或其他虚拟私有云，或面向私网提供服务，则需要私网NAT网关。

约束与限制

- 用户需要在VPC下手动添加私网路由，即通过创建对等连接或开通云专线/VPN连接远端私网。
- SNAT规则和DNAT规则不能共用同一个中转IP。
- 私网NAT网关支持添加的DNAT规则和SNAT规则的数量如下：
  - 小型：DNAT规则和SNAT规则的总数不超过20个。
  - 中型：DNAT规则和SNAT规则的总数不超过50个。
  - 大型：DNAT规则和SNAT规则的总数不超过200个。
  - 超大型：DNAT规则和SNAT规则的总数不超过500个。

⚠ 注意

购买私网NAT网关必须指定私网NAT网关所在VPC、子网、私网NAT网关规格。

操作步骤

1. 进入**购买私网NAT网关页面**。
2. 根据界面提示，配置私网NAT网关的基本信息，配置参数请参见**表2-2**。

表 2-2 参数说明

参数	参数说明
计费模式	私网NAT网关支持按需计费。
区域	私网NAT网关所在的区域。
名称	私网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点）。
虚拟私有云	私网NAT网关所属的VPC。 VPC仅在购买私网NAT网关时可以选择，后续不支持修改。
子网	私网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在购买私网NAT网关时可以选择，后续不支持修改。

参数	参数说明
规格	私网NAT网关的规格。 私网NAT网关共有小型、中型、大型、超大型四种规格类型。规格详情参见**产品规格**。
企业项目	配置私网NAT网关归属的企业项目。当私网NAT网关配置企业项目时，该私网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。
标签	私网NAT网关的标识，包括键和值。可以创建20个标签。 如您的组织已经设定私网NAT网关的相关标签策略，则需按照标签策略规则为私网NAT网关添加标签。标签如果不符合标签策略的规则，则可能会导致私网NAT网关创建失败，请联系组织管理员了解标签策略详情。 标签的命名规则请参考**表2-3**。
描述	私网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。

表 2-3 标签命名规则

参数	规则
键	• 不能为空。 • 对于同一NAT网关键值唯一。 • 长度不超过36个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。
值	• 长度不超过43个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。

3. 单击“立即购买”。

更多操作

- **创建中转IP**
- **添加SNAT规则**
- **添加DNAT规则**
- **管理私网NAT网关**

2.3 管理私网 NAT 网关

私网NAT网关创建后，您可对您的私网NAT网关进行统一管理，包括修改私网NAT网关信息和删除私网NAT网关。

修改私网 NAT 网关

私网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，可以修改私网NAT网关规格、名称和描述。

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击需要修改的私网NAT网关操作列中的“修改”。
3. 根据界面提示，修改私网NAT网关的名称、规格或者描述等信息。
4. 修改完成后，单击“下一步”。
5. 确认私网NAT网关信息的修改，单击“提交”。

删除私网 NAT 网关

私网NAT网关创建后，如果您不再需要使用私网NAT网关，可以通过删除私网NAT网关，释放资源，节省费用。

说明

必须保证私网NAT网关下的SNAT规则和DNAT规则已全部删除。如果私网NAT网关下的SNAT规则和DNAT规则未被全部删除，则无法执行删除，请先在私网NAT网关页面进行**删除SNAT规则**和**删除DNAT规则**操作。

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击目标私网NAT网关操作列中的“删除”。
3. 在删除确认对话框，输入“DELETE”。
4. 单击“确定”。

2.4 管理 SNAT 规则

2.4.1 添加 SNAT 规则

操作场景

私网NAT网关创建成功后，您需要创建SNAT规则。通过创建SNAT规则，VPC子网中全部或部分云主机可以通过共享中转IP访问用户本地数据中心（IDC）或其他VPC。

约束与限制

VPC内的每个子网只能添加一条SNAT规则。

前提条件

- 私网NAT网关创建成功。

- 中转IP创建成功。
- 云专线接入的用户，云专线的虚拟网关中，“VPC网段”参数建议设置为"0.0.0.0/0"。具体配置请参考**创建虚拟网关**。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击需要添加SNAT规则的私网NAT网关名称。
3. 在SNAT规则页签中，单击“添加SNAT规则”。
4. 根据界面提示，配置添加SNAT规则参数，详情请参见**表2-4**。

表 2-4 参数说明

参数	参数说明
子网	SNAT规则的子网类型，选择“使用已有”或“自定义”。 选择业务VPC中需要做地址映射的子网。
监控	可以为SNAT连接数设置告警，实时监控运行状态。
中转IP	选择已创建好的中转IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

5. 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，可以为一个私网NAT网关添加多条SNAT规则。

相关链接

管理SNAT规则

2.4.2 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。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

前提条件

私网NAT网关下存在成功添加的SNAT规则。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击目标私网NAT网关的名称。
3. 系统跳转至目标私网NAT网关详情页面，单击“SNAT规则”页签。
4. 在SNAT规则列表中，单击目标私网SNAT规则操作列中的“修改”。
5. 在弹出的对话框中，修改参数中的内容。
6. 单击“确定”，完成SNAT规则的修改。

2.4.3 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。

前提条件

私网NAT网关下存在成功添加的SNAT规则。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击目标私网NAT网关的名称。
3. 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”。
4. 在弹出的对话框中单击“确定”，完成SNAT规则的删除。

2.5 管理 DNAT 规则

2.5.1 添加 DNAT 规则

操作场景

私网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内的云主机实例对外部私网（IDC或其他VPC）提供服务。

云主机的每个端口分别对应一条DNAT规则，一个云主机的多个端口或者多个云主机需要为外部私网提供服务，则需要创建多条DNAT规则。

约束与限制

DNAT的全端口模式不能和具体端口模式共用同一个中转IP。

前提条件

- 已成功创建私网NAT网关。
- 中转IP创建成功。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击需要添加DNAT规则的私网NAT网关名称。
3. 在私网NAT网关详情页面中，单击“DNAT规则”页签。
4. 在DNAT规则页签中，单击“添加DNAT规则”。

须知

配置DNAT规则后，需在目标云主机实例中放通对应的安全组规则，否则DNAT规则不能生效。

5. 根据界面提示，配置添加DNAT规则参数，详情请参见**表2-5**。

表 2-5 DNAT 规则参数说明

参数	说明
本端网络	
端口类型	分为具体端口和所有端口两种类型。 • 具体端口：属于端口映射方式。私网NAT网关会将以指定协议和端口访问该中转IP的请求转发到目标云主机实例的指定端口上。 • 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私网IP（中转IP），任何访问该中转IP的请求都将转发到目标云服务器实例上。
支持协议	协议类型分为TCP和UDP两种类型。端口类型为所有端口时，此参数默认设置为All。 端口类型为具体端口时，可配置此参数。
实例类型	选择对外部私网提供服务的实例类型。 • 服务器 • 虚拟IP地址 • 负载均衡器 • 自定义
网卡	服务器网卡。实例类型为服务器时，需要配置此参数。
IP地址	对外部私网提供服务的云主机IP地址。实例类型为自定义时，需要配置此参数。
业务端口	实例对外提供服务的协议端口号。端口范围是1～65535。 端口类型为具体端口时，需要配置此参数。
中转网络	

参数	说明
中转IP	通过该中转IP访问用户IDC或其他VPC。 这里只能选择没有被绑定的中转IP，或者被绑定在当前私网NAT网关中非“所有端口”类型DNAT规则上的中转IP，或者被绑定到当前私网NAT网关中SNAT规则上的中转IP。
中转IP端口	中转IP对外提供服务的端口号。端口范围是1～65535。 端口类型为具体端口时，需要配置此参数。
描述	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

6. 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。

相关链接

管理DNAT规则

2.5.2 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。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

前提条件

私网NAT网关下存在成功添加的DNAT规则。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击目标私网NAT网关的名称。
3. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
4. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
5. 在弹出的对话框中，修改参数中的内容。
6. 单击“确定”，完成DNAT规则的修改。

2.5.3 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。

前提条件

私网NAT网关下存在成功添加的DNAT规则。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击目标私网NAT网关的名称。
3. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
4. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
5. 在弹出的对话框中单击“确定”，完成DNAT规则的删除。

2.6 管理中转 IP

2.6.1 创建中转 IP

操作场景

通过创建中转IP，使虚拟私有云内多个云主机可以共享中转IP访问用户本地数据中心（IDC）或其他虚拟私有云，或面向私网提供服务。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在私网NAT网关页面，单击“中转IP > 创建中转IP”，进入创建中转IP页面。

图 2-5 创建中转 IP

3. 根据界面提示，配置中转IP的基本信息，配置参数请参见**表2-6**。

表 2-6 中转 IP 参数说明

参数	参数说明
中转VPC	中转IP所在的VPC。
中转子网	中转子网相当于一个中转网络，是中转IP所属的子网。 子网至少有一个可用的IP地址。
中转IP	中转IP的分配方式有以下两种。 **自动分配**：由系统自动分配中转IP地址。 **手动分配**：手动指定中转IP地址。
IP地址	当中转IP的分配方式选择“手动分配”时，需要指定中转IP地址。 单击下方“查看已使用IP地址”可以查看所选子网中已使用的IP地址。
企业项目	中转IP所属的企业项目。
标签	私网NAT网关的标识，包括键和值。可以创建20个标签。

4. 单击“确定”，完成中转IP创建。

2.6.2 查看中转 IP

操作场景

中转IP创建完成后，您可以查看已创建的中转IP。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在“中转IP”页签，单击目标中转IP名称。
3. 进入中转IP详情页，即可查看已创建的中转IP的详细信息。
   您可以查看到该中转IP所属的中转VPC、中转子网和关联的私网NAT网关等信息。

2.6.3 删除中转 IP

操作场景

当您不需要某个中转IP时，可以进行删除操作。

操作步骤

1. 进入**私网NAT网关列表页**。
2. 在“中转IP”页签，单击目标中转IP操作列的“释放”。
3. 单击“确定”。

说明

当中转IP已关联SNAT或DNAT规则时，无法删除。此时，如果要删除中转IP，请先释放该中转IP所关联的所有规则。

2.7 连接 IDC 或其他虚拟私有云

连接 IDC

当您需要VPC内的多个云主机与用户IDC进行连通时，可通过在中转VPC与用户IDC间创建云专线/VPN来实现。

高质量连通选择云专线，具体请参见**开通云专线**。

低成本连通选择VPN，具体请参见**开通VPN**。

连接其他 VPC

当您需要VPC内的多个云主机与其他远端VPC进行连通时，可通过在中转VPC与其他远端VPC间创建对等连接来实现。

对等连接内容请参见**对等连接**。

3 权限管理

3.1 创建用户并授权使用 NAT 网关

如果您需要对您所拥有的NAT网关（NAT Gateway，简称NAT网关）进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用NAT网关。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将NAT网关委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用NAT网关服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图3-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的NAT网关权限，并结合实际需求进行选择，NAT网关支持的系统权限，请参见：**NAT网关权限**。若您需要对除NAT网关之外的其它服务授权，IAM支持服务的所有策略请参见**系统权限**。

示例流程

图 3-1 给用户授权 NAT 网关权限流程

1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予NAT网关服务权限“NATReadOnlyAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1.创建用户组并授权**中创建的用户组。
3. **用户登录**并验证权限。
   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择NAT网关，进入NAT网关主界面，单击右上角“购买NAT网关”，如果无法购买NAT网关（假设当前权限仅包含NATReadOnlyAccess），表示“NATReadOnlyAccess”已生效。
   - 在“服务列表”中选择除NAT网关外（假设当前策略仅包含NATReadOnlyAccess）的任一服务，若提示权限不足，表示“NATReadOnlyAccess”已生效。

3.2 NAT 网关自定义策略

如果系统预置的NAT网关权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**策略及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。
  具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的NAT网关自定义策略样例。

策略样例

- 示例1：授权用户创建和删除NAT网关

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "nat:natGateways:create",
                "nat:natGateways:delete"
            ]
        }
    ]
}
```

- 示例2：拒绝用户删除NAT网关

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予NAT FullAccess的系统策略，但不希望用户拥有NAT FullAccess中定义的删除NAT网关权限，您可以创建一条拒绝删除NAT网关的策略，然后同时将NAT FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对NAT网关执行除了删除NAT网关外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "nat:natGateways:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:update",
        "nat:natGateways:create"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:update"
      ],
      "Effect": "Allow"
    }
  ]
}
```


4 标签管理

应用场景

NAT网关标签是NAT网关的标识。为NAT网关添加标签，可以方便用户识别和管理拥有的NAT网关。您可以在创建NAT网关时增加标签或者在已经创建的NAT网关详情页添加标签，最多可以给NAT网关添加20个标签。

如您的组织已经设定公网NAT网关的相关标签策略，则需按照标签策略规则为公网NAT网关添加标签。标签如果不符合标签策略的规则，则可能会导致公网NAT网关创建失败，请联系组织管理员了解标签策略详情。

标签共由两部分组成：“键”和“值”，其中，“键”和“值”的命名规则如表4-1所示。

表 4-1 标签命名规则

参数	规则
键	• 不能为空。 • 对于同一NAT网关键值唯一。 • 长度不超过36个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。
值	• 长度不超过43个字符。 • 不能包含“=”、“*”、“<”、“>”、“\\”、“,”、“|”和“/”，且首尾字符不能为空格。

管理 NAT 网关实例的标签

管理NAT网关实例的标签有以下两种方法。

- 在创建NAT网关实例的时候，输入标签的“键”和“值”。
  操作步骤和配置参数，请参见购买公网NAT网关和购买私网NAT网关。
- 为已创建的NAT网关实例修改标签。

a. 进入**NAT网关列表页面**。
b. 在公网NAT网关列表页面或私网NAT网关列表页面，单击目标NAT网关实例。
c. 切换到“标签”页签下，单击“编辑标签”。
d. 在“编辑标签”页面：
   i. 添加新标签：单击“添加新标签”后，输入“键”和“值”。
   ii. 修改标签：在需要修改的标签所在行，输入修改的“值”。
e. 确认正确，单击“确认”。

说明

- 一个NAT网关实例最多可以增加20个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

管理中转 IP 的标签

管理私网NAT网关实例中转IP的标签有以下两种方法。

- 在创建中转IP的时候，输入标签的“键”和“值”。
  操作步骤和配置参数，请参见**创建中转IP**。
- 为已创建的中转IP修改标签。
  a. 进入**私网NAT网关中转IP列表页面**。
  b. 在私网NAT网关中转IP列表页面，单击目标中转IP。
  c. 单击“编辑标签”。
  d. 在“编辑标签”页面：
     i. 添加新标签：单击“添加新标签”后，输入“键”和“值”。
     ii. 修改标签：在需要修改的标签所在行，输入修改的“值”。
  e. 确认正确，单击“确认”。

说明

- 一个中转IP最多可以增加20个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

5 管理 NAT 网关的配额

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. 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 5-1 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。

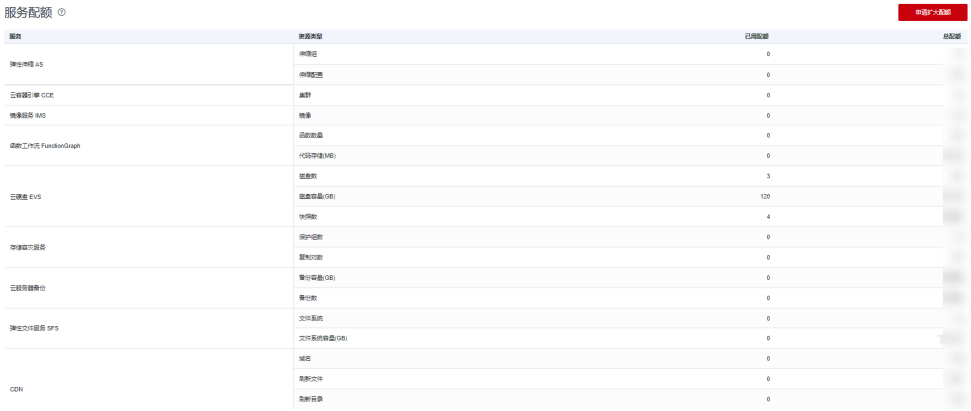
如何申请扩大配额?

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 5-2 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 5-3 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”。

6 使用 CES 监控 NAT 网关

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 公网 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：个	≥ 0个	公网NAT网关	1分钟
inbound_bandwidth	入方向带宽	该指标用于统计入方向带宽。 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
outbound_bandwidth	出方向带宽	该指标用于统计SNAT出方向带宽。 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
inbound_pps	入方向PPS	该指标用于统计SNAT入方向PPS。 单位：个	≥0个	公网NAT网关	1分钟

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）
outbound_pps	出方向PPS	该指标用于统计SNAT出方向PPS。 单位：个	≥0个	公网NAT网关	1分钟
inbound_traffic	入方向流量	该指标用于统计SNAT入方向流量。 单位：字节	≥0 bytes	公网NAT网关	1分钟
outbound_traffic	出方向流量	该指标用于统计SNAT出方向流量。 单位：字节	≥0 bytes	公网NAT网关	1分钟
snat_connection_ratio	SNAT连接数使用率	该指标用于统计测量对象的SNAT连接数使用率。连接数最大为规格限制的连接数。详情可查看**产品规格**。 单位：百分比	≥0	公网NAT网关	1分钟
inbound_bandwidth_ratio	入方向带宽使用率	该指标用于统计SNAT入方向带宽使用率。 公网NAT网关最大带宽20Gbit/s，则入方向带宽使用率为：**实际使用带宽/公网NAT实例最大带宽***100%。 单位：百分比 **说明** 该监控项为针对公网NAT实例性能的监控而不是针对EIP带宽的监控。	≥0	公网NAT网关	1分钟
outbound_bandwidth_ratio	出方向带宽使用率	该指标用于统计SNAT出方向带宽使用率。 公网NAT网关最大带宽为20Gbit/s，则出方向带宽使用率为：**实际使用带宽/公网NAT实例最大带宽***100%。 单位：百分比 **说明** 该监控项为针对公网NAT网关性能的监控而不是针对EIP带宽的监控。	≥0	公网NAT网关	1分钟

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）
total_inbound_udp_bandwidth	入方向UDP总带宽	该指标用于统计从公网引到当前公网NAT网关实例的UDP总带宽。 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
total_outbound_udp_bandwidth	出方向UDP总带宽	该指标用于统计虚拟私有云(VPC)内引到当前公网NAT网关实例的UDP总带宽。 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
total_inbound_tcp_bandwidth	入方向TCP总带宽	该指标用于统计从公网引到当前公网NAT网关实例的TCP总带宽 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
total_outbound_tcp_bandwidth	出方向TCP总带宽	该指标用于统计虚拟私有云(VPC)内引到当前公网NAT网关实例的TCP总带宽。 单位：比特/秒	≥0 bit/s	公网NAT网关	1分钟
packets_drop_count_snat_connection_beyond	丢包数（SNAT连接数超限）	该指标用于统计当前公网NAT网关实例由于SNAT连接数超限导致的丢包数。 单位：个	≥ 0 个	公网NAT网关	1分钟
packets_drop_count_pps_beyond	丢包数（PPS超限）	该指标用于统计当前公网NAT网关实例由于PPS超限导致的丢包数。 单位：个	≥ 0 个	公网NAT网关	1分钟
packets_drop_count_eip_port_alloc_beyond	丢包数（EIP端口分配超限）	该指标用于统计当前公网NAT网关实例由于EIP端口分配超限导致的丢包数。 单位：个	≥ 0 个	公网NAT网关	1分钟

表 6-2 私网 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：个	≥ 0 个	私网NAT网关	1分钟
inbound_bandwidth	入方向带宽	该指标用于统计入方向带宽。 单位：比特/秒	≥0 bit/s	私网NAT网关	1分钟
outbound_bandwidth	出方向带宽	该指标用于统计出方向带宽。 单位：比特/秒	≥0 bit/s	私网NAT网关	1分钟
inbound_pps	入方向PPS	该指标用于统计入方向PPS。 单位：个	≥0个	私网NAT网关	1分钟
outbound_pps	出方向PPS	该指标用于统计出方向PPS。 单位：个	≥0个	私网NAT网关	1分钟
inbound_traffic	入方向流量	该指标用于统计入方向流量。 单位：字节	≥0 bytes	私网NAT网关	1分钟
outbound_traffic	出方向流量	该指标用于统计出方向流量。 单位：字节	≥0 bytes	私网NAT网关	1分钟

维度

Key	Value
nat_gateway_id	公网NAT网关
vpc_nat_gateway_id	私网NAT网关

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. 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. 在左侧导航树栏，选择“告警 > 告警规则”。
5. 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。
6. 在“创建告警规则”界面，根据界面提示配置参数。
   a. 根据界面提示，配置告警规则的基本信息。

表 6-3 配置规则信息

参数	参数说明
名称	系统会随机产生一个名称，用户也可以进行修改。 取值样例：alarm-b6al
描述	告警规则描述（此参数非必填项）。
企业项目	告警规则所属的企业项目。只有拥有该企业项目权限的用户才可以查看和管理该告警规则。创建企业项目请参考：**创建企业项目**。

   b. 选择监控对象，配置告警内容参数。

表 6-4 配置告警内容

参数	参数说明	取值样例
资源类型	配置告警规则监控的服务名称。	NAT网关
维度	用于指定告警规则对应指标的维度名称	公网NAT网关

参数	参数说明	取值样例
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。 **说明** • 当选择资源分组时，该分组下任何资源满足告警策略时，都会触发告警通知。 • 选择指定资源时，勾选具体的监控对象，单击  将监控对象同步到右侧对话框。	指定资源
选择类型	根据需要可选择从模板导入或自定义创建。	自定义创建
模板	选择需要导入的模板。 您可以选择系统预置的默认告警模板，或者选择自定义模板。	-
告警策略	触发告警规则的告警策略。 当资源类型选择站点监控、日志监控、自定义监控、具体的云服务时，是否触发告警取决于连续周期的数据是否达到阈值。例如SNAT连接数监控周期为1分钟，连续三个周期原始值≥8000个，则触发告警。	-
告警级别	根据告警的严重程度不同等级，可选择紧急、重要、次要、提示。	重要

c. 根据界面提示，配置告警通知参数。

表 6-5 配置告警通知

参数	参数说明
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知对象	需要发送告警通知的对象，可选择云账号联系人或主题名称。 • 云账号联系人为注册账号时的手机和邮箱。 • 主题是消息发布或客户端订阅通知的特定事件类型，若此处没有需要的主题则需先创建主题并添加订阅，创建主题并添加订阅请参见《云监控用户指南》。
生效时间	该告警规则仅在生效时间内发送通知消息。 如生效时间为08:00-20:00，则该告警规则仅在08:00-20:00发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

7. 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. 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

6.4 查看 NAT 网关后端实例对应的监控指标

操作场景

如果您需要查看特定NAT网关的某个监控指标下各个后端实例对应的该监控指标情况，您可以按照如下步骤操作。

操作步骤

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，单击“网络 > NAT网关”。
   进入NAT网关页面。
4. 在NAT网关页面，单击需要查看监控指标的NAT网关名称。
5. 切换至“监控”页签，单击页面中间的“查看更多指标详情”。
   进入云监控服务的查看NAT网关监控指标页面。
6. 选择所需查看的监控指标时间段。
7. 单击页面右上角的切换视图图标 ，来切换各个监控指标展示的方式。
8. 选择所需查看的监控指标并在显示的监控指标图中选择某一时间点。
   在页面下方就可以查看到NAT网关后端实例对应的该监控指标情况。

图 6-2 查看 NAT 网关后端实例对应的监控指标

7 使用 CTS 审计 NAT 网关

7.1 支持审计的关键操作列表

通过云审计服务，您可以记录与NAT网关相关的操作事件，便于日后的查询、审计和回溯。

云审计支持的公网NAT网关操作事件列表如表7-1所示。

云审计支持的私网NAT网关操作事件列表如表7-2所示。

表 7-1 云审计服务支持的公网 NAT 网关操作列表

操作名称	资源类型	事件名称
创建公网NAT网关	natgateway	createNatGateway
修改公网NAT网关	natgateway	updateNatGateway
删除公网NAT网关	natgateway	deleteNatGateway
创建公网NAT网关DNAT规则	dnatrule	createDnatRule
修改公网NAT网关DNAT规则	dnatrule	updateDnatRule
删除公网NAT网关DNAT规则	dnatrule	deleteDnatRule
创建公网NAT网关SNAT规则	snatrule	createSnatRule
修改公网NAT网关SNAT规则	snatrule	updateSnatRule
删除公网NAT网关SNAT规则	snatrule	deleteSnatRule

表 7-2 云审计服务支持的私网 NAT 网关操作列表

操作名称	资源类型	事件名称
创建私网NAT网关	privateNat	createPrivateNat
修改私网NAT网关	privateNat	updatePrivateNat
删除私网NAT网关	privateNat	deletePrivateNat
创建私网NAT网关DNAT规则	privateDnatRule	createPrivateDnatRule
修改私网NAT网关DNAT规则	privateDnatRule	updatePrivateDnatRule
删除私网NAT网关DNAT规则	privateDnatRule	deletePrivateDnatRule
创建私网NAT网关SNAT规则	privateSnatRule	createPrivateSnatRule
修改私网NAT网关SNAT规则	privateSnatRule	updatePrivateSnatRule
删除私网NAT网关SNAT规则	privateSnatRule	deletePrivateSnatRule
创建中转子网	transitSubnet	createTransitSubnet
修改中转子网	transitSubnet	updateTransitSubnet
删除中转子网	transitSubnet	deleteTransitSubnet
创建中转IP	transitIp	createTransitIp
删除中转IP	transitip	deleteTransitIp

7.2 查看审计日志

操作场景

在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看最近7天的操作记录。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击“服务列表”，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型。
     在下拉框中选择查询条件。
     其中筛选类型选择事件名称时，还需选择某个具体的事件名称。
     选择资源ID时，还需选择或者手动输入某个具体的资源ID。
     选择资源名称时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
   - 时间范围：可选择查询最近七天内任意时间段的操作事件。
6. 在需要查看的记录左侧，单击 展开该记录的详细信息。如**图 展开记录**所示。

图 7-1 展开记录

7. 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如**图 查看事件**所示，显示了该操作事件结构的详细信息。

图 7-2 查看事件


```
"context": {
    "code": "204",
    "source_ip": "10.45.152.59",
    "trace_type": "ApiCall",
    "event_type": "system",
    "project_id": "0503dda897000fed2f78c00909158a4d",
    "trace_id": "116a2aff-deb8-11e9-95f5-d5c0b02a9b97",
    "trace_name": "deleteMember",
    "resource_type": "member",
    "trace_rating": "normal",
    "api_version": "v2.0",
    "service_type": "ELB",
    "response": "{\"member\": {\"project_id\": \"0503dda897000fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-
    "resource_id": "
    "tracker_name": "system",
    "time": "1569321775225",
    "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
    "record_time": "1569321775903",
    "user": {
        "domain": {
            "name": "
            "id": "0503dda878000fed0f75c0096d70a960"
        },
```


关于云审计服务事件结构的关键字段详解，请参见**《云审计服务用户指南》**的事件结构。

