NAT 网关

私网 NAT 网关操作指南

产品文档

腾讯云

文档目录

私网 NAT 网关操作指南
- 创建与管理 NAT 网关
- 配置指向私网 NAT 网关的路由
- 管理 SNAT 规则
- 管理 DNAT 规则
- 访问管理

私网 NAT 网关操作指南
创建与管理 NAT 网关

最近更新时间：2024-08-01 14:19:33

创建私网 NAT 网关

说明

私网 NAT 网关正在灰度测试中，如需使用，请 提交工单 申请。

1. 登录 NAT 网关控制台。
2. 选择地区和私有网络，单击**新建**。
3. 在**私网 NAT 网关**购买页中按需输入或确定相关参数，根据官网指引完成购买。

参数	说明
网关配置	计费模式：按量计费。 网关名称：按需输入 NAT 网关名称，支持60个字符。 地域：选择 NAT 网关所属地域 关联实例：支持选择专线网关、私有网络、云联网三种 NAT 网关关联的实例类型。 专线网关：主要解决同地域内 VPC 与专线 IDC 的地址转换（例如北京地域内），用于 VPC 和专线资源的互访。 云联网：主要解决跨地域 VPC 与 VPC 间，VPC 与专线 IDC 间的地址转换（例如北京到上海），用于 VPC 跨地域通过云联网对其他外部资源访问。 私有网络：主要解决 VPC 内指定子网的地址转换，用于 VPC 内指定子网和外部资源的互访。
其他配置	可选配置，可根据需要选择是否为该实例设置标签信息，如不需要可跳过。

修改私网 NAT 网关信息

1. 登录 私网 NAT 网关控制台，在列表中单击需要修改的**私网 NAT 网关 ID** 进入详情页
2. 在详情页可以完成如下操作：

单击网关名称后面的

，可修改网关名称，网关名称不能超过60个字符。

单击标签行的


，可添加标签，通过标签可进行权限管理。

删除私网 NAT 网关

注意

删除时会将含有此 NAT 网关的所有策略一并删除，Internet 转发请求将立即中断，请提前做好网络中断准备。

在确定无需使用 NAT 网关后，您可以随时将其删除。

1. 登录 私网 NAT 网关控制台，在列表中找到需要删除的 NAT 网关，单击操作栏下的**删除**。
2. 在弹窗中，单击**确定**。

配置指向私网 NAT 网关的路由

最近更新时间：2024-08-01 14:18:27

创建私网 NAT 网关后，需要配置路由规则，将子网流量指向私网 NAT 网关后，子网的云资源才可通过私网 NAT 网关访问外部资源。

本章节介绍如何配置指向私网 NAT 网关的路由策略，有如下两种方式，您可选择任一操作方式：

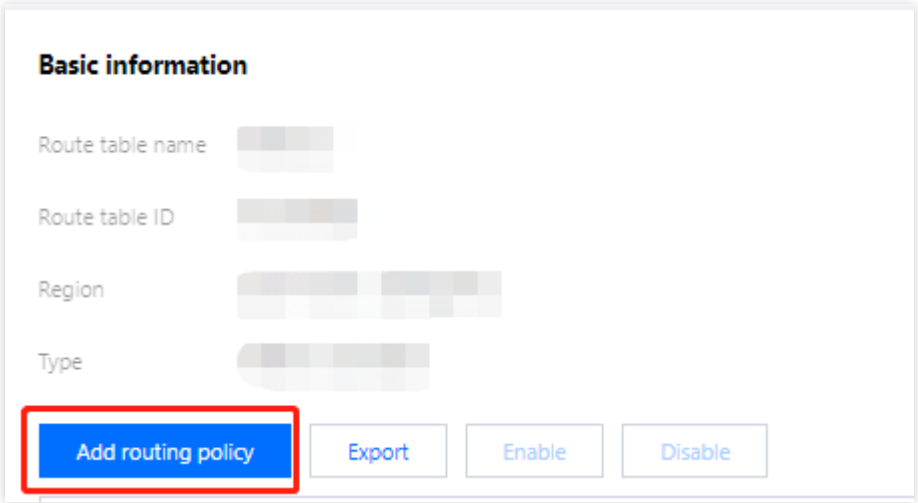
方式一：从私网 **NAT 网关**控制台开始操作。

方式二：从**路由表**控制台开始操作。

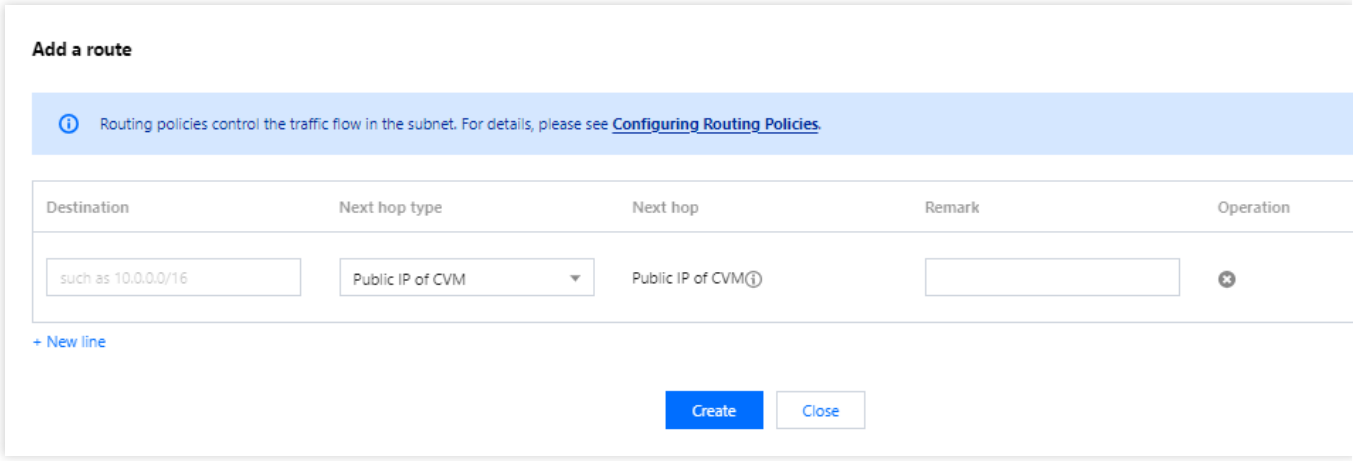
操作步骤

方式一：从 NAT 网关控制台开始操作

1. 登录 NAT 控制台。
2. 单击左侧**私网 NAT 网关**，在私网 NAT 网关实例列表中，单击目标 NAT 实例**所属网络的 ID**。
3. 在目标 私有网络 **详情** > **基本信息** > **包含资源**中，单击**子网**。
4. 在子网列表中，选择需要访问外部 VPC/专线/云联网的子网所在行的**关联路由表 ID**。
5. 在路由表基本信息页面，单击**新增路由策略**。



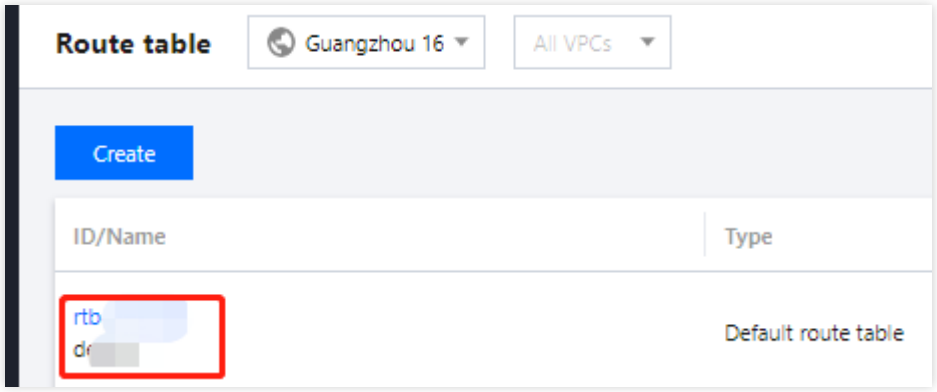
6. 在**新增路由**弹框中，输入目的端（目的端对应的 IP 地址段）、下一跳类型选择**私网 NAT 网关**、下一跳选择已创建的私网 NAT 网关 ID。



7. 单击**创建**完成以上配置后，关联此路由表的子网内的云服务器访问目的端地址的流量，将指向该私网 NAT网关。

方式二：从路由表控制台开始操作

1. 登录 路由表控制台。
2. 在路由表列表中，单击需要访问外部 VPC/专线/云联网的子网所关联的**路由表 ID** 进入详情页。



3. 在路由表基本信息页面，单击**新增路由策略**。
4. 在**新增路由**弹框中，输入目的端（目的端对应的 IP 地址段）、下一跳类型选择**私网 NAT 网关**、下一跳选择已创建的**私网 NAT 网关 ID**。
5. 单击**创建**完成以上配置后，关联此路由表的子网内的云服务器访问目的端地址的流量，将指向该私网 NAT网关。

管理 SNAT 规则

最近更新时间：2024-08-01 14:17:32

不同类型的私网 NAT 网关实例对应的 SNAT 规则不同，本文详细介绍不同关联实例对应的 SNAT 规则。

前提条件

创建 SNAT 规则前，请确保子网所在的路由表需指向对应的 NAT 网关，详细操作请参见 配置指向私网 NAT 网关的路由。

新建 SNAT 规则

专线网关

专线网关型的私网 NAT 网关主要解决同地域内 VPC 与专线 IDC 的地址转换（例如北京地域内），用于 VPC 和专线资源的互访。此类型私网 NAT 网关，新建 SNAT 规则，可以按照以下步骤操作。

1. 登录 NAT 网关控制台，单击需要新建 SNAT 规则的**私网 NAT 网关实例**，进入详情页。
2. 在私网 NAT 网关实例详情页中，单击 **SNAT 规则**页签 > **新建**，填入对应映射方向、映射类型、原 IP、映射 IP、备注等信息，完成 SNAT 规则的新建，其中各标签信息如下。

映射方向：

本端：对 VPC 内网 IP 地址转换。

对端：对 VPC 对端网络的内网 IP 地址进行转换，如对端为 IDC 网络，则可转换 IDC 内的 IP 地址。

映射类型：

三层：仅转换 IP 地址。

四层：将 IP 和端口映射为指定 IP 池内随机端口。

原 IP：需要转换的 IP 地址。当映射方向为“本端”时，为私有网络中的 IP 地址；当映射方向为“对端”时，为 IDC 内机器的 IP 地址。

映射 IP/映射 IP 池：配置转换后的 IP/IP 池，原 IP 是通过该映射后的 IP/IP 池对外提供服务能力的。

3. 新建 SNAT 规则后，针对“本端”映射支持编辑 ACL 规则，“对端”映射不支持编辑 ACL 规则。

在配置 SNAT 规则之后，需要继续在专线侧绑定NAT网关。上述流程，您可参考最佳实践文档 通过专线接入+VPC NAT 网关实现本地 IDC 与云上资源互访 **来实现。**

说明：

SNAT 规则不能重复。

SNAT 规则不支持对端四层。

三层规则优先级大于四层规则。

同 ACL 优先级靠前的四层规则优先匹配，后面的不再匹配。

每条规则下可折叠展示 ACL 规则，ACL 规则支持分页展示。

云联网

云联网型的私网 NAT 网关主要解决跨地域 VPC 与 VPC 间，VPC 与专线 IDC 间的地址转换（如北京到上海），用于 VPC 跨地域通过云联网对其他外部资源访问。

说明：

创建私网 NAT 网关实例时，关联实例选择**云联网**后，该实例创建后会自动生成两个 VPC，用于地址转换时的路由配置。

这两个 VPC 不能单独删除，生命周期同 NAT 网关实例，名称分别为：本端 VPC，对端 VPC，均为 NAT 网关的所属 VPC。

云联网型的私网 NAT 网关支持 fullnat 内网地址，在通过云联网打通的多网络场景下，配置 SNAT 规则前，请先规划本端网络和对端网络。

本端网络：支持对该网络的内网 IP 进行三层 SNAT、四层 SNAPT，四层 DNAT 规则。

对端网络：仅支持对该网络的内网 IP 进行三层 SNAT。

注意：

如转换的是 VPC 和 IDC 两个网络的内网地址，则 IDC 为对端网络，VPC 为本端网络，因为 IDC 只能进行三层 SNAT 转换。

规划完成本端及对端网络之后，您可按照以下步骤新建 SNAT 规则：

1. 登录 NAT 网关控制台，在左侧导航栏单击**私网 NAT 网关。**
2. 在私网 NAT 网关实例列表页面，单击需要新建 SNAT 规则的**私网 NAT 网关实例**，进入详情页。
3. 在**私网 NAT 网关实例**详情页中，单击 **SNAT 规则**页签 > **新建**，填入对应映射方向、映射类型、原 IP、映射 IP、备注等信息后，单击**确定**，完成 SNAT 规则的新建，其中各标签信息如下：

映射方向：

本端：对 VPC 内网IP地址转换。

对端：对 VPC 对端网络的内网 IP 地址进行转换，如对端为 IDC 网络，则可转换 IDC 内的 IP 地址。

映射类型：

三层：仅转换 IP 地址。

四层：将 IP 和端口映射为指定 IP 池内随机端口。

原 IP：私有网络中的 local 子网的 IP 地址，即需要转换的 IP 地址。

映射 IP/映射 IP 池：配置转换后的 IP/IP 池，原 IP 是通过该映射后的 IP/IP 池对外提供服务能力的。

4. 新建 SNAT 规则后，针对“本端”映射支持编辑 ACL 规则，“对端”映射不支持编辑 ACL 规则。

在配置 SNAT 规则之后，需要进一步配置 NAT 网关的两个中转 VPC 的路由策略，才可实现云联网类型的 NAT 实例的正常运行。具体流程如下所述：

1. 配置 NAT 两个中转 VPC 的路由策略。
2. 在云联网中新建两个自定义路由表，分别绑定 NAT 的两个中转 VPC，关联后，中转 VPC 的路由会发布到云联网中自定义路由表中。
3. 边界网络1加入云联网，并绑定云联网路由表1，边界网络2加入到云联网，并绑定云联网路由表2。

配置完成后，数据流为：边界网络1 > 云联网 > NAT 本端中转 VPC > NAT 对端中转 VPC 端点 > 云联网 > 边界网络2。

私有网络

私有网络类型的私网 NAT 网关主要解决 VPC 内指定子网的地址转换，用于 VPC 内制定子网的内网 IP 经过 NAT 后，转换为新的 IP 后，再与其他网络通信。此类型私网 NAT 网关，新建 SNAT 规则，可以按照以下步骤操作。

1. 登录 NAT网关控制台，单击需要新建 SNAT 规则的 NAT 网关实例。
2. 在 SNAT 规则页签，单击**新建**，填入对应映射类型、原 IP、映射 IP、备注等信息，完成 SNAT 规则的新建，其中各标签信息如下。

映射类型：

三层：仅转换 IP 地址。

四层：将 IP 和端口映射为指定 IP 池内随机端口。

原 IP：填写需要转换的原 IP，例如某客户 local 子网的 IP，仅三层时需要填写具体的原 IP，四层不需要填写，默认指向 NAT 的 local 子网的所有 IP。

映射IP/映射 IP 池：填写转换后的 IP 或 IP 段，三层 IP 转换则填写 IP 地址，四层 IP 端口转换则填写 IP 段或 IP 地址。

3. 新建 SNAT 规则后，支持编辑 ACL 规则

每条 SNAT 规则下面有一个 ACL 规则，默认全放通，如需要指定某些数据流可以匹配 NAT 规则，可以设置 ACL 规则，如需要所有报文都按照匹配 NAT 规则，则无需处理。

每条规则下可折叠展示 ACL 规则，ACL 规则支持分页。

编辑 SNAT 规则

1. 登录 NAT 网关控制台，单击需要编辑 SNAT 规则的**私网 NAT 网关实例**。
2. 在**私网 NAT 网关实例**详情页中，单击 **SNAT 规则**页签，在 SNAT 规则条目右侧，单击**修改**，进入编辑对话框。
3. 修改 SNAT 规则中的原 IP 地址、映射 IP/IP 需求池或描述，然后单击**确定**完成修改。

查询 SNAT 规则

1. 登录 NAT 网关控制台，单击需要查询 SNAT 规则的**私网 NAT 网关实例**。
2. 在**私网 NAT 网关实例**详情页中，单击 **SNAT 规则**页签 > **SNAT 列表** > 右上方的搜索框，单击选择筛选条件，支持按照原 IP 和映射 IP 进行查询。
3. 单击

进行快速检索。

删除 SNAT 规则

单条删除

1. 登录 NAT 网关控制台，单击需要编辑 SNAT 规则的**私网 NAT 网关实例**。
2. 在**私网 NAT 网关实例**详情页中，单击 **SNAT 规则**页签，单击 SNAT 规则条目右侧的**删除**。
3. 单击**确认**，删除该条 SNAT 规则。

批量删除

1. 登录 NAT 网关控制台，单击需要编辑 SNAT 规则的**私网 NAT 网关实例**。
2. 在**私网 NAT 网关实例**详情页中，单击 **SNAT 规则**标签页，勾选多条 SNAT 规则，单击上方的**删除**。
3. 在弹出的提示框中，单击**删除**，完成批量删除。

管理 DNAT 规则

最近更新时间：2024-08-01 14:17:22

DNAT（Destination Network Address Translation，目的网络地址转换）能力可将 VPC 内云服务器的**内网 IP**，**协议**，**端口**映射成**其他 IP**，**协议**，**端口**，使得云服务器上的资源可隐藏原地址被其他网络访问。

新建 DNAT 规则

1. 登录 NAT 网关控制台，在左侧导航栏单击**私网 NAT 网关**。
2. 在**私网 NAT 网关**列表页，单击需要查询 DNAT 规则的**私网 NAT 网关实例**，进入详情页。
3. 在**私网 NAT 网关**实例详情页中，单击 DNAT 页签 > **新建**，选择协议、原 IP、原端口、映射后 IP 及映射后端口后，单击**确定**即可。

原 IP 和原端口：为私有网络中的 local 子网的 IP 地址及端口，即需要转换的 IP 地址和端口。
映射后 IP 和映射后端口：配置转换后的 IP 及端口，原 IP 和端口是通过该映射后的 IP 和端口对外提供服务能力的。仅支持对端网络主动访问私有网络时，需访问映射后的 IP 端口与私有网络内原 IP 端口进行通信，回包不受影响。
原端口、映射端口范围为：1-65535。
单次批量添加，最多支持50条规则，如规则数量较多，可分多次添加。

查询 DNAT 规则

1. 登录 NAT 网关控制台，在左侧导航栏单击**私网 NAT 网关**。
2. 在私网 NAT 网关列表页，单击需要查询 DNAT 规则的私网 NAT 网关实例，进入详情页。
3. 在私网 NAT 网关实例详情页中，单击 **DNAT** 页签，在右侧搜索框中，支持根据协议、原 IP、原端口、映射后 IP、映射后端口进行查询。

修改 DNAT 规则

1. 登录 NAT 网关控制台，在左侧导航栏单击**私网 NAT 网关**。
2. 在私网 NAT 网关列表页，单击需要修改 DNAT 规则的**私网 NAT 网关实例**，进入详情页。
3. 在私网 NAT 网关实例详情页中，单击 **DNAT** 页签，选择某条固定的 DANT 规则，单击操作栏的**修改**，可支持根据协议、原 IP、原端口、映射后 IP、映射后端口进行修改对应规则。

删除 DNAT 规则

删除 DNAT 规则支持**单条删除**和**多条删除**。

单条删除：

1. 登录 NAT 网关控制台，在左侧导航栏单击**私网 NAT 网关**。
2. 在私网 NAT 网关列表页，单击需要删除 DNAT 规则的私网 NAT 网关实例，进入详情页。
3. 在私网 NAT 网关实例详情页中，单击 **DNAT** 页签，选择某条固定的 DANT 规则，单击操作栏的**删除**，可删除对应单条规则。

批量删除：

在私网 NAT 网关实例详情页中，单击 **DNAT** 页签，左侧选择多条 DNAT 规则，单击列表上方**删除**，可批量删除 DNAT 规则。

访问管理

最近更新时间：2024-08-01 14:15:29

操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略，让用户拥有在控制台中查看和使用特定资源的权限。本文档提供了查看和使用私网 NAT 网关特定资源的权限示例，指导用户如何使用控制台的特定部分的策略。

授权定义

CAM 中可对私网 NAT 网关进行授权的资源

资源类型	授权策略中的资源描述方法
NAT 网关实例	`qcs::vpc:{region_short_name}:uin/{Uin}:nat/{NatGatewayId}`
NAT 网关接口	qcs::vpc:{region_short_name}:uin/{Uin}:nat/*

其中：
所有 `{region_short_name}` 应为某个 region 的 ID，可以为空。
所有 `{Uin}` 应为资源拥有者的 AccountId，或者“*”。
所有 `{NatGatewayId}` 应为某个 NAT 实例的 ID，或者“*”。
以此类推。

CAM 中可对私网 NAT 网关进行授权的接口

在 CAM 中，可以对一个 NAT 资源进行以下 Action 的授权。

API 操作	资源描述	接口说明
CreatePrivateNatGateway	创建私网 NAT 网关	qcs::vpc:$region:$account:intranat/ qcs::vpc:$region:$account:vpc/*
DeletePrivateNatGateway	删除私网	qcs::vpc:$region:$account:intranat/

	NAT 网关	
ModifyPrivateNatGatewayAttribute	修改私网 NAT 网关属性	qcs::vpc:$region:$account:intranat/
DescribePrivateNatGateways	查询私网 NAT 网关	qcs::vpc:$region:$account:intranat/
DescribePrivateNatGatewayLimits	查询可创建的私网 NAT 网关配额数量	qcs::vpc:$region:$account:intranat/ qcs::vpc:$region:$account:vpc/$vp
CreatePrivateNatGatewayTranslationNatRule	创建私网 NAT 网关源端转换规则	qcs::vpc:$region:$account:intranat/
DeletePrivateNatGatewayTranslationNatRule	删除私网 NAT 网关源端转换规则	qcs::vpc:$region:$account:intranat/
ModifyPrivateNatGatewayTranslationNatRule	修改私网 NAT 网关源端转换规则	qcs::vpc:$region:$account:intranat/

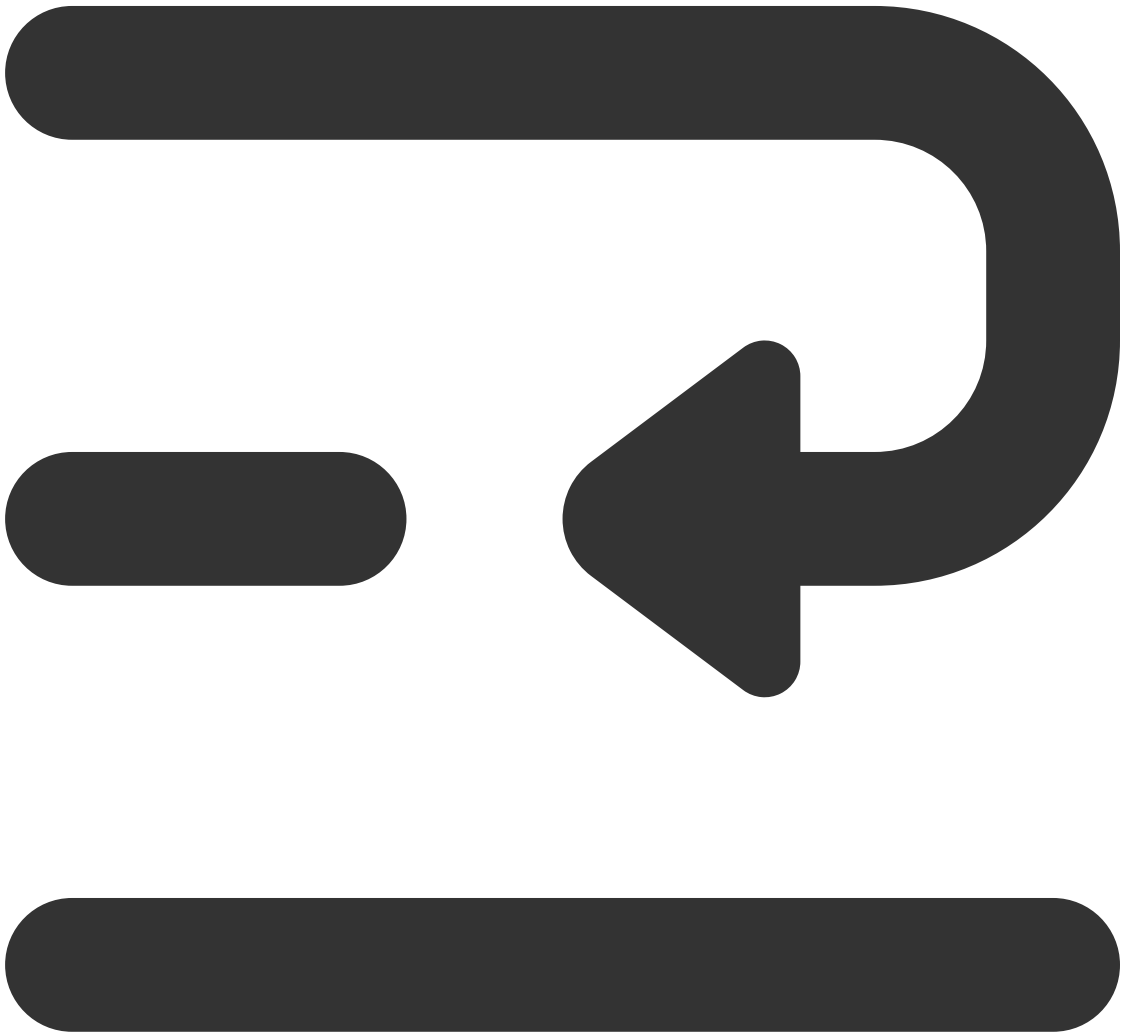
DescribePrivateNatGatewayTranslationNatRules	查询私网NAT网关源端转换规则	qcs::vpc:$region:$account:intranat/
CreatePrivateNatGatewayTranslationAclRule	创建私网NAT网关源端转换访问控制规则	qcs::vpc:$region:$account:intranat/
DeletePrivateNatGatewayTranslationAclRule	删除私网NAT网关源端转换访问控制规则	qcs::vpc:$region:$account:intranat/
ModifyPrivateNatGatewayTranslationAclRule	修改私网NAT网关源端转换访问控制规则	qcs::vpc:$region:$account:intranat/
DescribePrivateNatGatewayTranslationAclRules	查询私网NAT网关源端转换访问	qcs::vpc:$region:$account:intranat/

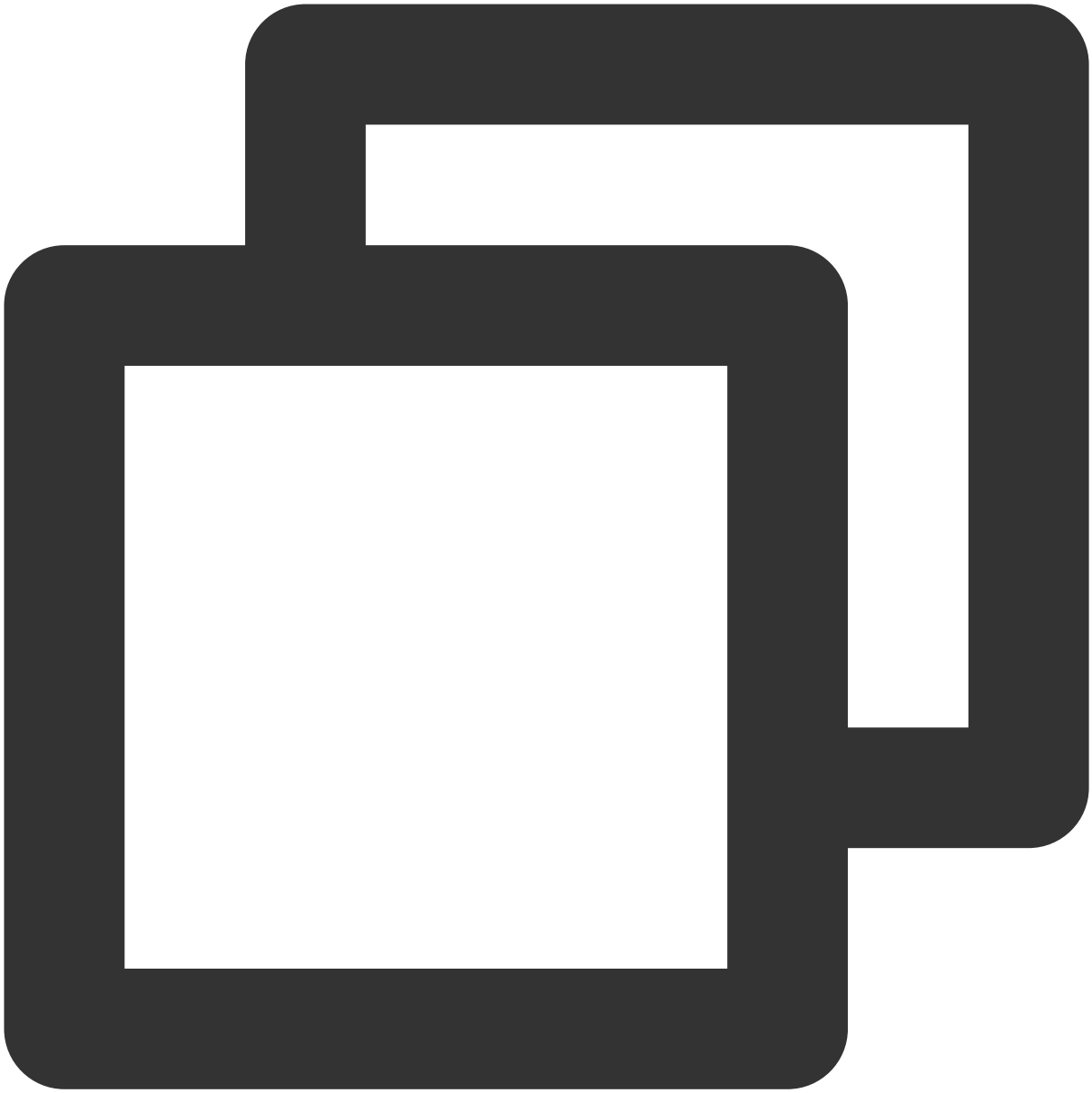
	控制规则	
CreatePrivateNatGatewayDestinationIpPortTranslationNatRule	创建私网NAT网关目的端口转换规则	qcs::vpc:$region:$account:intranat/
DeletePrivateNatGatewayDestinationIpPortTranslationNatRule	删除私网NAT网关目的端口转换规则	qcs::vpc:$region:$account:intranat/
ModifyPrivateNatGatewayDestinationIpPortTranslationNatRule	修改私网NAT网关目的端口转换规则	qcs::vpc:$region:$account:intranat/
DescribePrivateNatGatewayDestinationIpPortTranslationNatRules	查询私网NAT网关目的端口转换规则	qcs::vpc:$region:$account:intranat/
DescribePrivateNatGatewayRegions	查询私网NAT网关可支持地域	qcs::vpc:$region:$account:intranat/

策略示例

所有 NAT 的全读写策略

授权一个子账户以 NAT 服务的完全管理权限，包括创建、管理等全部操作。



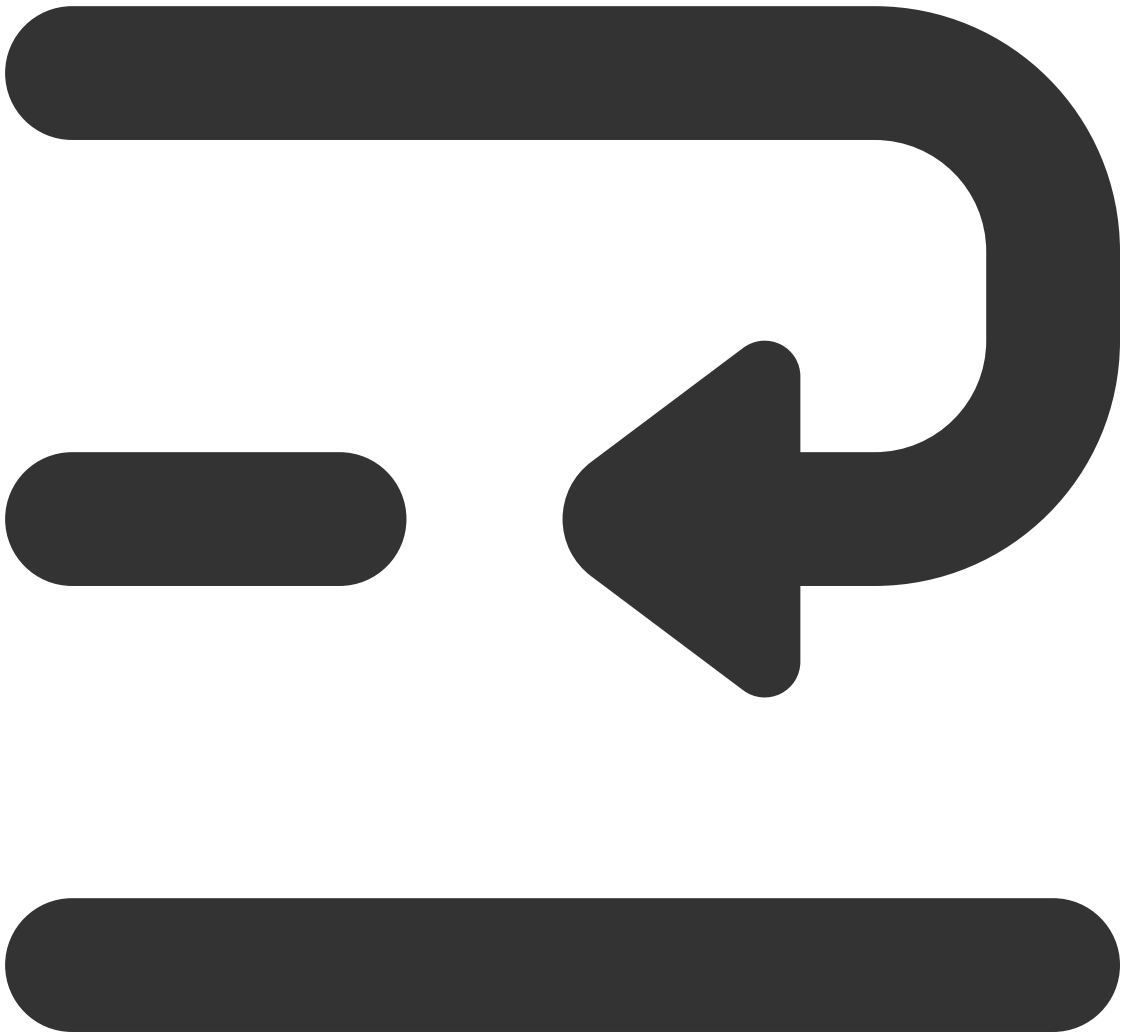


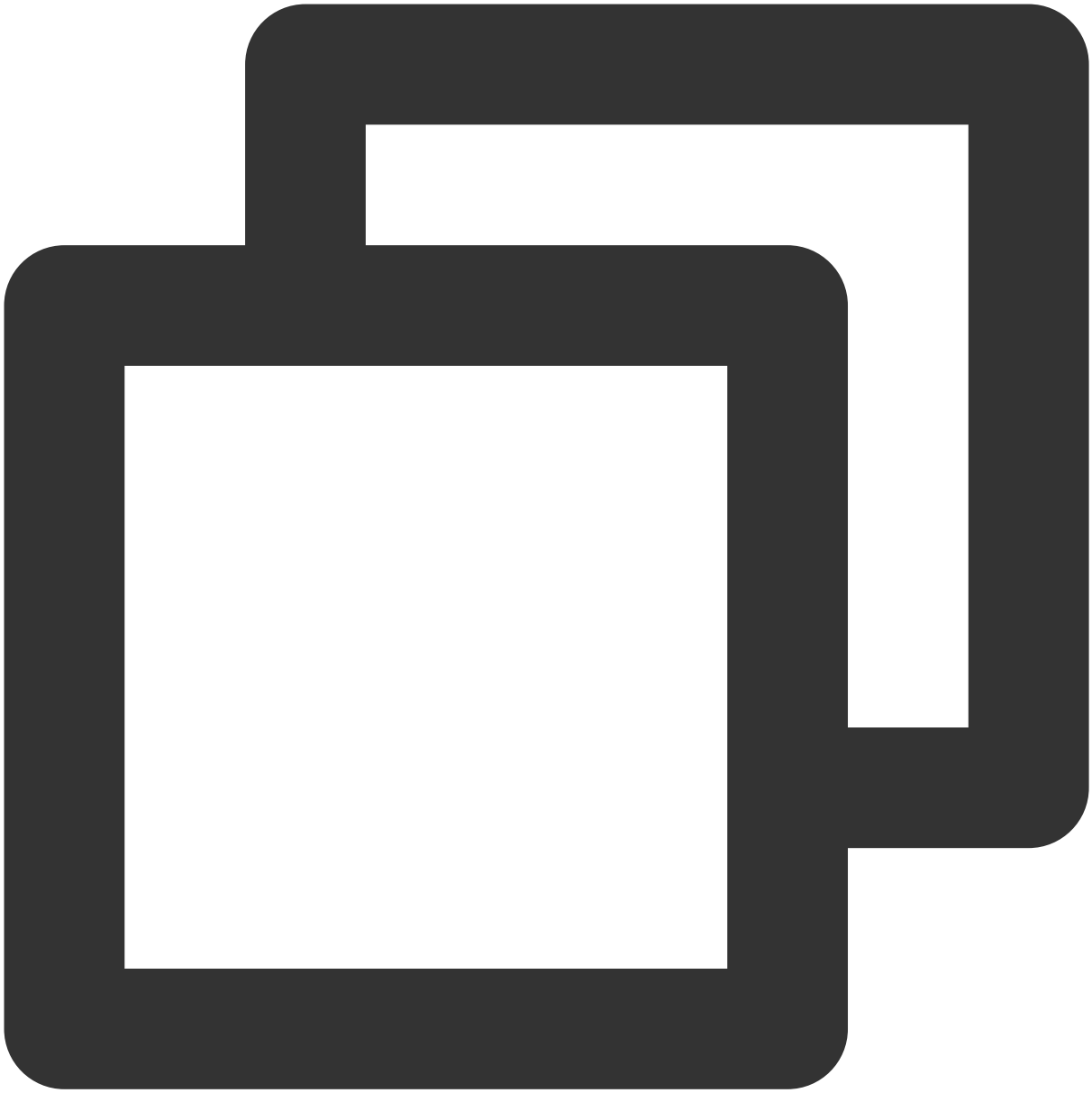
```
{
"version": "2.0",
"statement": [{
"action": [
"vpc:*"
],
"resource": "qcs::vpc::$uin:nat/*",
"effect": "allow"
}]}
{
"version": "2.0",
```

```
"statement": [{
"action": [
"vpc:*"
],
"resource": "qcs::vpc::$uin:intranat/*",
"effect": "allow"
}]}
```

只读策略

授权一个子账户只读访问 NAT 的权限。

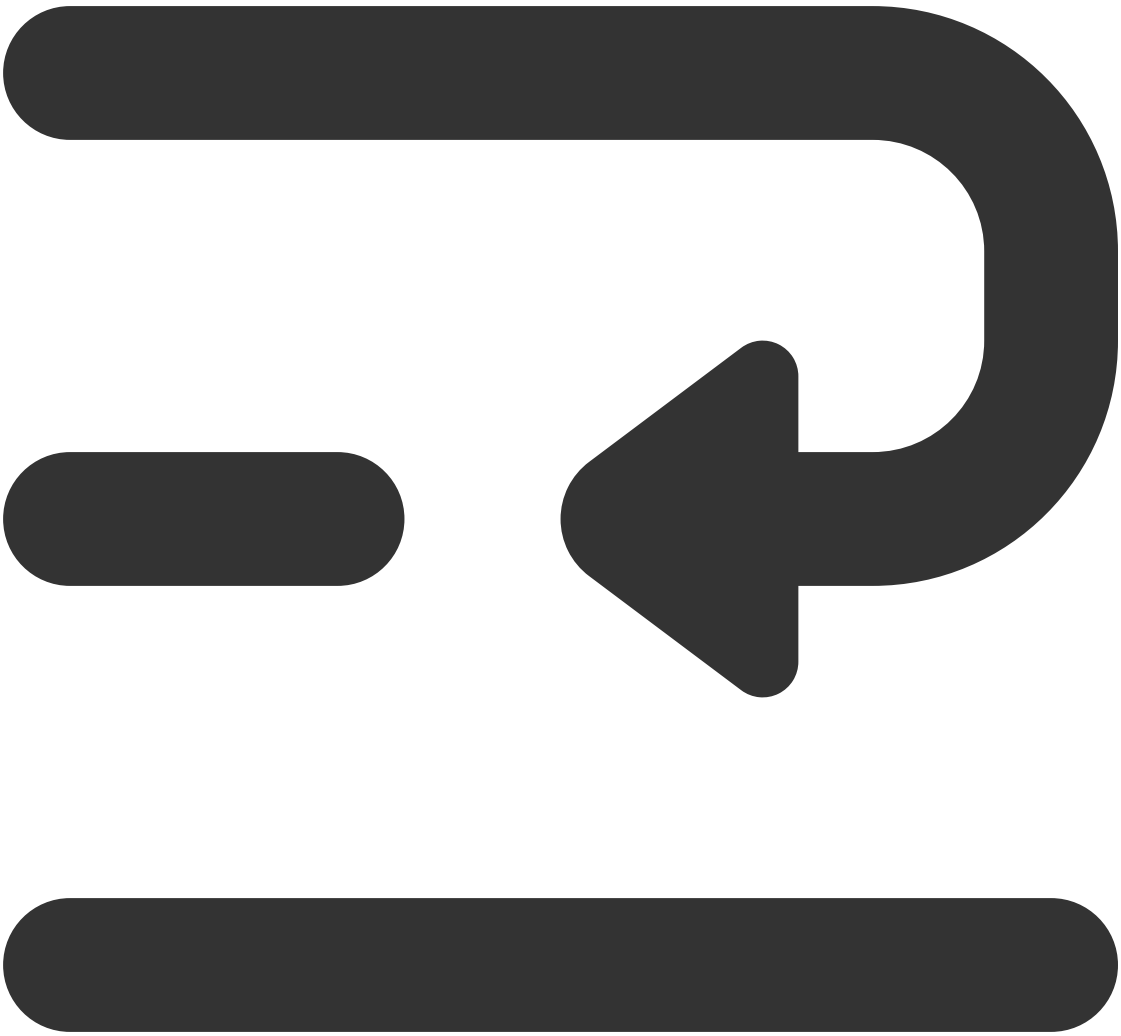


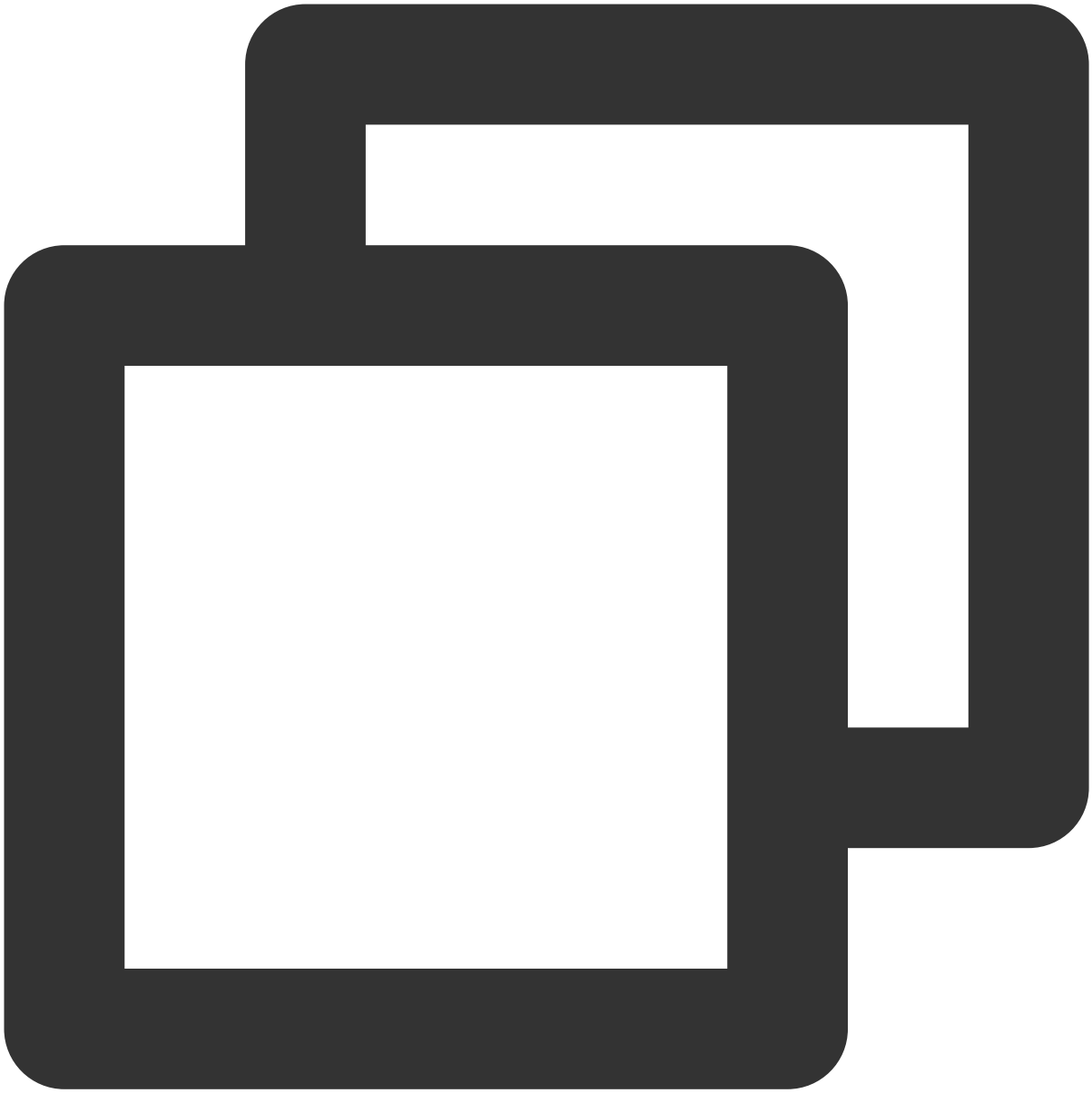


```
{
"version": "2.0",
"statement": [{
 "action": [
 "vpc:Describe*"
 ],
  "resource": "qcs::vpc::$uin:nat/*",
  "effect": "allow" }]}
{
"version": "2.0",
 "statement": [{
```

```
"action": [
"vpc:Describe*"
],
"resource": "qcs::vpc::$uin:intranat/*",
"effect": "allow"
}]}
```

某个标签下 NAT 的全读写策略





```
{
"version":"2.0",
"statement":[{
"effect":"allow",
"action":"*",
"resource":"*",
"condition":{
"for_any_value:string_equal":{
"qcs:tag":[
"tagkey&tagvalue"
]}}}]}
```