ALIBABA CLOUD

阿里云

NAT网关

通用配置

文档版本：20210730

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.服务关联角色 ---------- 05
2.DDoS基础防护 ---------- 08
3.管理配额 ---------- 09

1.服务关联角色

本文为您介绍NAT网关的服务关联角色（AliyunServiceRoleForNatgw）以及如何删除NAT网关服务关联角色。

背景信息

服务关联角色是指与某个云服务关联的RAM角色。在某些场景下，为了完成云服务的某个功能，需要获取其他云服务的访问权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多信息，请参见服务关联角色。

创建服务关联角色

创建增强型NAT网关时，如果服务关联角色不存在，系统会自动创建一个名称为AliyunServiceRoleForNatgw的服务关联角色，并且为该角色添加名称为AliyunServiceRolePolicyForNatgw的权限策略，授予NAT网关访问其他云资源的权限，策略内容如下。

> **说明** 如果您要创建的NAT网关类型为普通型NAT网关，系统不会自动创建名称为AliyunServiceRoleForNatgw的服务关联角色，也能成功创建NAT网关。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:RevokeSecurityGroup",
        "ecs:DeleteSecurityGroup",
        "ecs:JoinSecurityGroup",
        "ecs:DeleteSecurityGroup",
        "ecs:LeaveSecurityGroup",
        "ecs:DescribeSecurityGroups",
        "ecs:AttachNetworkInterface",
        "ecs:DetachNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission",
        "ecs:CreateSecurityGroupPermission",
        "ecs:AuthorizeSecurityGroupPermission",
        "ecs:RevokeSecurityGroupPermission",
        "ecs:DeleteSecurityGroupPermission",
        "ecs:JoinSecurityGroupPermission",
```

```
        "ecs:DeleteSecurityGroupPermission",
        "ecs:LeaveSecurityGroupPermission",
        "ecs:DescribeSecurityGroupPermissions",
        "ecs:AttachNetworkInterfacePermissions",
        "ecs:DetachNetworkInterfacePermissions"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "nat.aliyuncs.com"
        }
      }
    }
  ]
}
```

删除服务关联角色

如果您要删除NAT网关服务关联角色（AliyunServiceRoleForNatgw），请先删除NAT网关实例。具体操作，请参见：

1. 删除NAT网关
2. 删除服务关联角色

常见问题

为什么我的RAM用户无法自动创建NAT网关服务关联角色（AliyunServiceRoleForNatgw）？

您需要拥有指定的权限，才能自动创建或删除NAT网关服务关联角色（AliyunServiceRoleForNatgw）。因此，在RAM用户无法自动创建NAT网关服务关联角色（AliyunServiceRoleForNatgw）时，您需为其添加以下权限策略。

```
{
  "Statement": [
    {
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "nat.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

相关文档

- 服务关联角色

2.DDoS基础防护

DDoS攻击是一种针对目标系统的恶意网络攻击行为，会导致被攻击者的业务无法正常访问。阿里云免费为NAT网关提供最高5 Gbps的DDoS基础防护，DDoS基础防护服务可以有效防止DDoS攻击。

DDoS基础防护工作原理

启用DDoS基础防护功能后，所有来自Internet的流量都将先经过云盾再到达NAT网关，云盾会针对常见的攻击进行清洗过滤。云盾DDoS基础防护可以防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood 和DNS Flood等DDoS攻击。

云盾DDoS基础防护根据NAT网关实例的EIP带宽自动设定清洗阈值和黑洞阈值。当入方向流量达到阈值上限时，触发清洗和黑洞：

- 清洗：当来自Internet的攻击流量超过清洗阈值或符合攻击流量模型特征时，云盾将启动清洗操作，清洗操作包括过滤攻击报文、流量限速、包限速等。
- 黑洞：当来自Internet的攻击流量超过黑洞阈值时，为保护集群安全，流量将会被黑洞处理，即所有入流量全部被丢弃。

清洗阈值

NAT网关的清洗阈值计算方式如下表所示：

EIP带宽	最大bps清洗阈值	最大pps清洗阈值	默认黑洞阈值
小于等于800 Mbps	800 Mbps	12万	1.5 Gbps
大于800 Mbps	设定的带宽值	设定的带宽值×150	设定的带宽值×2

例如EIP带宽为1000 Mbps，则最大bps清洗阈值为1000 Mbps，最大pps清洗阈值15万，默认黑洞阈值为2 Gbps。

3.管理配额

您可以通过专有网络管理控制台查询NAT网关的配额使用情况。如果某个资源的剩余配额不满足业务需求，您可以申请提升配额。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，选择**运维与监控 > 配额管理**。
3. 在**配额管理**页面，单击**NAT网关**页签，查看当前账号下NAT网关的配额使用情况。
4. 如果需要提升配额，在**操作**列单击**申请**。
5. 在**提交配额申请**对话框，根据以下信息提交配额申请。
   - **申请数量**：选择要申请的配额数量。
   - **申请原因**：请详细描述申请配额的原因、业务场景和必要性。
   - **手机/固话**：申请配额的用户的电话号码。
   - **电子邮箱**：申请配额的用户的电子邮箱。
6. 单击**确定**。

   系统会自动审批配额申请是否合理，如果不合理，申请状态为**拒绝**；如果合理，申请状态为**通过**，配额立即自动提升为申请的数量。