

ALIBABA CLOUD

阿里云

NAT网关
用户指南

文档版本：20210103

 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

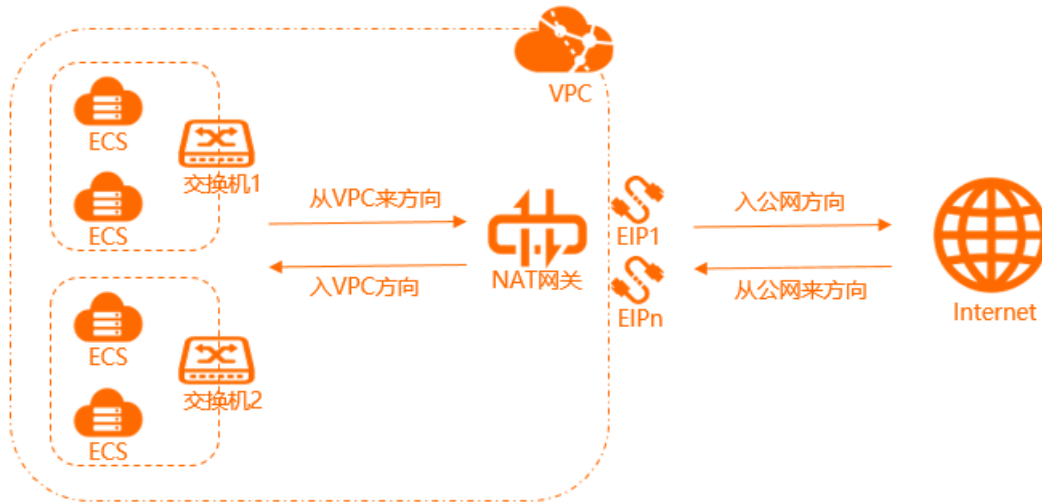
格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置>网络>设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，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

目录

1.使用云监控来监控NAT网关	05
-----------------	----

1.使用云监控来监控NAT网关

您可以使用阿里云云监控服务来监控NAT网关。云监控可以从NAT网关中监控并收集近乎实时的指标，并在NAT网关控制台生成可视化的时序曲线图，您可以根据各监控指标来排查问题。



查看NAT网关监控

1. 登录[NAT网关管理控制台](#)。
2. 在顶部菜单栏处，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关，单击监控列下的



图标查看监控。

NAT网关类型不同，监控指标也不同。

增强型NAT网关

监控指标分类	监控项	说明
Snat Session统计	并发连接数	NAT网关可同时容纳的TCP/UDP连接数量。
	并发丢弃连接数	NAT网关连接数超过并发连接数限制，而导致无法新建被丢弃的连接数。
	新建连接速率	NAT网关每秒可新建的TCP/UDP连接数量。
	新建丢弃连接数	NAT网关每秒新建连接数超过每秒最大新建连接限制，而导致无法新建被丢弃的连接数。
	并发连接水位	已消耗连接数占总连接数的百分比。
	新建连接水位	已消耗的新建连接数占总新建连接数的百分比。

监控指标分类	监控项	说明
入方向统计	入方向流量速率	入方向每秒接受的流量，包括： <ul style="list-style-type: none"> 从公网来流量速率。 入VPC流量速率。
	入方向流量	入方向所消耗的流量，包括： <ul style="list-style-type: none"> 从公网来流量。 入VPC流量。
	入方向包速率	入方向每秒接受的数据包数量，包括： <ul style="list-style-type: none"> 从公网来包速率。 入VPC包速率。
	入方向包量	入方向所消耗的数据包数量，包括： <ul style="list-style-type: none"> 从公网来包量。 入VPC包量。
出方向统计	出方向流量速率	出方向每秒接受的流量，包括： <ul style="list-style-type: none"> 入公网流量速率。 从VPC来流量速率。
	出方向流量	出方向所消耗的流量，包括： <ul style="list-style-type: none"> 入公网流量。 从VPC来流量。
	出方向包速率	出方向每秒接受的数据包数量，包括： <ul style="list-style-type: none"> 入公网包速率。 从VPC来包速率。
	出方向包量	出方向所消耗的数据包数量，包括： <ul style="list-style-type: none"> 入公网包量。 从VPC来包量。

普通型NAT网关

监控项	说明
SNAT连接数	NAT网关实例每分钟的SNAT连接数。

监控项	说明
容量限制丢弃连接数	<p>NAT网关的不同规格，对应不同的SNAT最大连接数限制。该指标表示实例连接数超过NAT网关规格对应的SNAT最大连接数限制，而导致无法新建被丢弃的SNAT连接数。</p> <p> 说明 该指标为累积值，不会清零。</p> <ul style="list-style-type: none"> 如果容量限制丢弃连接数在一定时间内持续上升，您需要考虑升配NAT网关的规格。 如果容量限制丢弃连接数在一定时间为一条水平线，则表明这段时间没有出现由NAT网关规格对应的最大连接数限制而导致的丢包。
限速丢弃连接数	<p>NAT网关的不同规格，对应着不同的SNAT每秒最大新建连接数限制。该指标表示实例SNAT每秒新建连接数超过NAT网关规格对应的SNAT每秒最大新建连接限制，而导致无法新建被丢弃的SNAT连接数。</p> <p> 说明 该指标为累积值，不会清零。</p> <ul style="list-style-type: none"> 如果限速丢弃连接数在一定时间内持续上升，则您需要考虑升配NAT网关的规格。 如果限速丢弃连接数在一定时间为一条水平线，则表明这段时间没有出现由NAT网关规格对应的SNAT每秒最大连接数限制而导致的丢包。

查看NAT绑定的弹性公网IP监控


1. 登录[NAT网关管理控制台](#)。
2. 在顶部菜单栏处，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关，单击操作列下的**管理**。
4. 单击**监控**页签。
5. 单击**NAT绑定的弹性公网IP监控**页签查看监控指标。

监控项	说明
流入带宽	从公网进入ECS实例的带宽，单位：bps。
流出带宽	从ECS实例发往公网的带宽，单位：bps。
流入包速率	每秒从公网进入ECS实例的包数量。
流出包速率	每秒从ECS实例发往公网的包数量。
限速丢包速率	限制每秒丢包的数量。
网络流入带宽利用率	从公网进入ECS实例的带宽的利用率。
网络流出带宽利用率	从ECS实例发往公网的带宽的利用率。

查看网关流量监控

异常的ECS实例流量会影响其他ECS实例的SNAT公网访问。开启网关流量监控功能，您可以查看SNAT转发流量监控数据，快速定位流量消耗最大的ECS实例，然后您可以对该ECS实例进行流量管控，实现快速收敛故障，提高业务的稳定性。

- 您已经创建了增强型NAT网关实例，具体操作，请参见[购买NAT网关](#)。

 **注意** 目前创建在华北1（青岛）、中国（香港）、美国（弗吉尼亚）和美国（硅谷）的NAT网关暂不支持网关流量监控功能。

- 您已经提交了查看网关流量监控的工单申请。如需使用，请[提交工单](#)。
 - 登录[NAT网关管理控制台](#)。
 - 在顶部菜单栏处，选择NAT网关的地域。
 - 在[NAT网关](#)页面，找到目标NAT网关实例，单击操作列下的[管理](#)。
 - 在[基本信息](#)页面，单击[监控](#)页签。
 - 单击[网关流量情况](#)页签，然后打开[开启网关流量监控](#)开关。您可以在时间栏中设置要查看流量监控数据的时间，时间为分钟级。例如，您设置要查看的时间为2020年12月15日16:00，则您可以查看2020年12月15日16:00:00~2020年12月15日16:01:00的流量监控数据。

说明

- 开启网关流量监控后，您需要等待15分钟，才能查看网关流量监控数据。
- 网关流量监控功能展示的监控数据可能存在3~5分钟的延迟。例如，您只能在2020年12月15日16:30查看2020年12月15日16:25时间点之前的流量监控数据，而不能查看2020年10月14日16:25时间点之后的流量监控数据。
- 网关流量监控功能可以展示流量消耗最大的前1000个ECS实例的流量信息，如需更多配额，请[提交工单](#)。

监控数据	单位	说明
并发连接数	个	ECS实例通过NAT网关访问公网的活跃连接数量。
新建连接数	个/秒	ECS实例通过NAT网关每秒发起的新建连接数量。
入方向流量	Kbps	从公网进入ECS实例的流量。
出方向流量	Kbps	从ECS实例发往公网的流量。
入方向包	个/秒	从公网进入ECS实例的包数量。
出方向包	个/秒	从ECS实例发往公网的包数量。

开启网关流量监控的前提条件

开启网关流量监控

创建阈值报警规则

如果您需要监控NAT网关实例的使用和运行情况，您可以通过创建阈值报警规则，实时监控NAT网关实例运行情况，保证业务的稳定。

1. 登录[云监控控制台](#)。
2. 在左侧导航栏，选择[报警服务 > 报警规则](#)。
3. 在[阈值报警](#)页签，单击[创建报警规则](#)。
4. 在[创建报警规则](#)页面，设置报警规则相关信息。

参数	说明
产品	云监控可管理的产品名称。例如：增强型NAT网关。
资源范围	报警规则的作用范围。取值： <ul style="list-style-type: none"> ◦ 全部资源：表示该规则作用在用户名下对应产品的全部实例上。例如：您设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。 ◦ 实例：表示该规则只作用在某个具体实例上。例如：您如果设置了实例粒度的主机CPU使用率大于80%报警，则当该实例CPU使用率大于80%时，会发送报警通知。
规则名称	报警规则的名称。
规则描述	报警规则的主体，定义在监控数据满足指定条件时，触发报警规则。例如：CPU使用率5分钟平均值>=90%，持续3个周期，则报警服务5分钟检查一次数据是否满足平均值>=90%，只检测3次。
通道沉默周期	指报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。
生效时间	报警规则的生效时间，报警规则只在生效时间内才会检查监控数据是否需要报警。
通知对象	发送报警的联系人组。
报警级别	<ul style="list-style-type: none"> ◦ 短信+邮件+钉钉机器人 ◦ 邮件+钉钉机器人
弹性伸缩	如果您选中 弹性伸缩 ，当报警发生时，会触发相应的伸缩规则。您需要设置弹性伸缩的 地域 、 弹性伸缩组 和 弹性伸缩规则 。 <ul style="list-style-type: none"> ◦ 创建弹性伸缩组的操作方法，请参见创建伸缩组。 ◦ 创建弹性伸缩规则的操作方法，请参见创建伸缩规则。
日志服务	如果您选中 日志服务 ，当报警发生时，会将报警信息写入日志服务。您需要设置日志服务的 地域 、 Project 和 Logstore 。 创建Project和Logstore的操作方法，请参见 快速入门 。
邮件备注	自定义报警邮件补充信息。填写邮件备注后，发送报警的邮件通知中会附带您的备注。
报警回调	填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

5. 单击[确认](#)。

相关文档

- [EnableNat GatewayEcsMetric](#)
- [List Nat GatewayEcsMetric](#)
- [DisableNat GatewayEcsMetric](#)
- [Put ResourceMetricRule](#)
- [CreateGroupMetricRules](#)