ALIBABA CLOUD

阿里云

专有网络VPC

流日志

文档版本：20200817

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.流日志概述

VPC提供流日志功能，可以记录VPC网络中弹性网卡（ENI）传入和传出的流量信息，帮助您检查访问控制规则、监控网络流量和排查网络故障。

> 说明 目前，流日志功能正在公测中。您可以提交工单申请公测。
> - 公测期间，流日志功能不承诺任何服务等级协议（SLA）相关的保障条款。
> - 公测期间，仅华北5（呼和浩特）、华南1（深圳）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、英国（伦敦）、印度（孟买）地域支持流日志功能。

功能介绍

您可以捕获指定弹性网卡的流量，也可以捕获指定VPC或交换机的流量。如果选择为VPC或交换机创建流日志，则会捕获VPC和交换机中所有弹性网卡的流量，包括在开启流日志功能后新建的弹性网卡。

流日志功能捕获的流量信息会以流日志记录的方式写入日志服务中。每条流日志记录会捕获特定捕获窗口中的特定五元组网络流，捕获窗口大约为10分钟，该段时间内流日志服务会先聚合数据，然后再发布流日志记录。

流日志记录的字段信息如下表所示。

字段	说明
version	流日志版本。
vswitch-id	弹性网卡所在交换机ID。
vm-id	弹性网卡绑定的云服务器ID。
vpc-id	弹性网卡所在专有网络ID。
account-id	账号ID。
eni-id	弹性网卡ID。
srcaddr	源地址。
srcport	源端口。
dstaddr	目的地址。
dstport	目的端口。
protocol	流量的IANA协议编号。 详细信息，请参见 Internet 协议编号。
direction	流量方向： • in：入方向流量。 • out：出方向流量。

字段	说明
packets	数据包数量。
bytes	数据包大小。
start	捕捉窗口开始时间。
end	捕捉窗口结束时间。
log-status	流日志的日志记录状态： • OK：数据记录正常。 • NODATA：捕获窗口中没有传入或传出网络接口的网络流量。 • SKIPDATA：捕获窗口中跳过了一些流日志记录。
action	与流量关联的操作： • ACCEPT：安全组和网络ACL允许记录的流量。 • REJECT：安全组和网络ACL拒绝记录的流量。

功能计费

目前，流日志仅支持将提取到的网络日志投递到日志服务SLS进行日志分析，流日志的费用=网络日志提取费+日志服务SLS的服务费。

- 网络日志提取费

  流日志会按照提取的日志收取网络日志提取费。

  > 说明 公测期间，流日志免收日志提取费。

- 日志服务SLS的服务费

  流日志捕捉到的日志信息存储在阿里云日志服务中，您可以在日志服务中查看和分析相关数据，日志服务收取相应的存储和检索费用。详细信息，请参见日志服务计费。

使用限制

流日志的限制如下表所示。

资源	默认限制	提升配额
每个地域支持创建的流日志实例的数量	10个	提交工单

资源	默认限制	提升配额
不支持创建流日志的VPC	VPC中含有以下实例规格族中的任一实例： ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4	升级不支持VPC高级功能的ECS实例的规格或释放不支持VPC高级功能的ECS实例。 • 升级操作，请参见包年包月实例升配规格和按量付费实例变配规格。 • 释放操作，请参见释放实例。 说明 如果您的VPC、交换机所属VPC、弹性网卡所属VPC中含有实例规格族限制中的任一实例，且您已经创建了流日志，为了保证正常使用流日志功能，请升级实例规格或释放实例。更多信息，请参见VPC高级功能概述。
不支持创建流日志的交换机	交换机所属的VPC中含有以下实例规格族中的任一实例： ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4	
不支持创建流日志的弹性网卡	弹性网卡所属的VPC中含有以下实例规格族中的任一实例： ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4	

配置流程

配置流日志的流程如下：

1. 开通日志服务

   通过流日志功能捕获到的流量信息存储在阿里云日志服务中。创建流日志前，您需要在日志服务产品页开通日志服务。

2. （可选）创建密钥对

   如果您需要通过API/SDK写入数据，请创建密钥对；如果您通过Logtail采集日志，则不需要创建密钥对。

3. 创建Project

   您需要为日志服务创建一个Project。详细信息，请参见创建Project。

4. 创建Logstore

   Logstore是Project的资源集合，Logstore中的所有数据都来自于同一个数据源。创建Project后，您需要创建Logstore。详细信息，请参见创建Logstore。

5. 创建捕获资源

   创建流日志前，您需要创建捕获日志的资源。您可以捕获指定弹性网卡的日志，也可以捕获指定VPC或交换机的日志。详细信息，请参见创建弹性网卡、创建专有网络和创建交换机。

6. 创建流日志

   您可以创建流日志，流日志可以捕获加载到云企业网内不同地域的网络实例间的流量信息。详细信息，请参见创建流日志。

7. 查看流日志

   创建流日志后，您可以查看流日志。通过查看捕获的流量信息，您可以分析跨地域业务流量、优化使用成本和排查网络故障。详细信息，请参见查看流日志。

2.创建流日志

专有网络（VPC）提供流日志功能，可以捕获VPC网络中弹性网卡（ENI）的传入和传出流量信息，帮助您检查访问控制规则、监控网络流量和排查网络故障。在捕获流量前，您需要创建一个流日志。

前提条件

创建流日志前，请确保满足以下条件：

- 您已经在日志服务产品页开通了日志服务。登录日志服务产品页。
- 您已经创建了存储捕获流量的Project和Logstore。详细信息，请参见创建Project和创建Logstore。
- 您已经创建了捕获资源。详细信息，请参见创建弹性网卡、创建专有网络和创建交换机。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**流日志**。
3. （可选）如果您的账号是初次使用流日志功能，单击**立即授权**，然后单击**同意授权**。授权成功后才能保证流日志可以将相关日志写入日志服务中。

   > 注意 该操作只有主账号首次开通流日志功能时才需要。

4. 在顶部菜单栏处，选择要捕获日志的地域。
5. 在**流日志**页面，单击**创建流日志**。
6. 在**创建流日志**对话框，根据以下信息配置流日志，然后单击**确定**。

配置	说明
名称	输入流日志名称。 名称长度为2~128个字符之间，以英文字母或开头，可包含数字、短横线（-）和下划线（_），但不能以 `http://` 和 `https://` 开头。

配置	说明
资源类型	选择要捕获流量的资源类型，然后选择相应的资源。支持选择以下资源类型： ○ **弹性网卡**：捕获指定的弹性网卡的流量信息。 ○ **交换机**：捕获指定的交换机内所有弹性网卡的流量信息。 ○ **专有网络**：捕获指定的专有网络内所有弹性网卡的流量信息。 如果您的专有网络、交换机所属的专有网络、弹性网卡所属的专有网络中含有以下ECS实例规格族中的任一实例，则不支持为该专有网络、交换机、弹性网卡创建流日志。 ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4 如需创建流日志，请升级ECS实例规格或释放ECS实例。 ○ 升级操作，请参见包年包月实例升配规格和按量付费实例变配规格。 ○ 释放操作，请参见释放实例。 说明 如果您的专有网络、交换机所属专有网络、弹性网卡所属专有网络中含有实例规格族限制中的任一实例，且您已经创建了流日志，为了保证正常使用流日志功能，请升级ECS实例规格或释放ECS实例。详细信息，请参见VPC高级功能概述。
流量类型	选择要捕获流量的类型： ○ **全部流量**：捕获指定资源的全部流量。 ○ **被访问控制允许的流量**：捕获指定资源被安全组规则允许的流量。 ○ **被访问控制拒绝的流量**：捕获指定资源被安全组规则拒绝的流量。
项目（Project）	选择存储捕获流量的项目（Project）。
日志库（Logstore）	选择存储捕获流量的日志库（Logstore）。
开启流日志分析报表功能	选择该功能后，所选的LogStore会开启索引并建立仪表盘，支持对数据进行SQL和可视化分析。 日志服务索引功能按流量收费，仪表盘不收费。详细信息，请参见日志服务计费说明。 说明 该选项只有当选择的LogStore未开通报表功能时才显示。
描述	输入流日志的描述。 描述信息长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

相关文档

- CreateFlowLog

3.查看流日志

创建流日志后，您可以查看流日志。通过查看捕获的流量信息，您可以检查访问控制规则、监控网络流量和排查网络故障。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击流日志。
3. 选择流日志的地域。
4. 在流日志页面，找到目标流日志，单击日志库的链接。

5. 在日志管理控制台，单击查询/分析。
   显示日志后，您可以查看日志和分析数据。

4.启动流日志

您可以启动处于**未启动**状态的流日志。启动流日志后，流日志才会捕获弹性网卡的流量信息。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**流日志**。
3. 选择流日志的地域。
4. 在**流日志**页面，找到目标流日志，单击**操作**列下的**启动**。
   启动流日志后，流日志的状态变更为**已启动**。

5.停止流日志

如果您希望暂时停止捕获弹性网卡的流量信息，您可以停止流日志。

背景信息

停止流日志并非删除流日志，待希望再次捕获弹性网卡的流量信息时，您可以启动状态为**未启动**的流日志。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**流日志**。
3. 选择流日志的地域。
4. 在**流日志**页面，找到目标流日志，单击**操作**列下的**停止**。
   停止流日志后，流日志的状态变更为**未启动**。

6.修改流日志

创建流日志后，您可以修改流日志的名称和描述信息。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**流日志**。
3. 选择流日志的地域。
4. 在**流日志**页面，找到目标流日志，单击**实例ID/名称**列下的图标修改流日志的名称。 名称长度为2~128个字符，以英文字母或中文开头，可包含数字，下划线（_）或短横线（-）。
5. 单击**描述**列下的**编辑**修改流日志的描述信息。 描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

7.删除流日志

您可以删除处于**已启动**和**未启动**状态的流日志。删除流日志后，您仍可以通过日志管理控制台查看之前捕获的流量信息。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**流日志**。
3. 选择流日志的地域。
4. 在**流日志**页面，找到目标流日志，单击**操作**列下的**删除**。
5. 在**删除流日志**对话框，单击**确定**。