私有网络

网络流日志

产品文档

腾讯云

文档目录

网络流日志
产品简介
产品概述

最近更新时间：2018-05-25 15:02:23

简介

网络流日志（Flow logs）为您提供 **全时、全流、非侵入** 的弹性网卡流量采集，可将网络流量进行实时的存储、分析，助力您解决 **故障排查、合规审计、架构优化、安全检测** 等问题，让您的云上网络更加稳定、安全和智能。

利用 VPC 流日志，您可捕获传入/传出 VPC 中弹性网卡 IP 流量。创建流日志后，您可以在 日志服务 中查看和检索其数据，或将用将指定流日志投递其它产品分析或存储，如：投递至 COS 存储桶中，对日志进行生命周期管理等，满足日志审计需求。

> **注意：**流日志正在火热内测中，欢迎申请。

主要场景

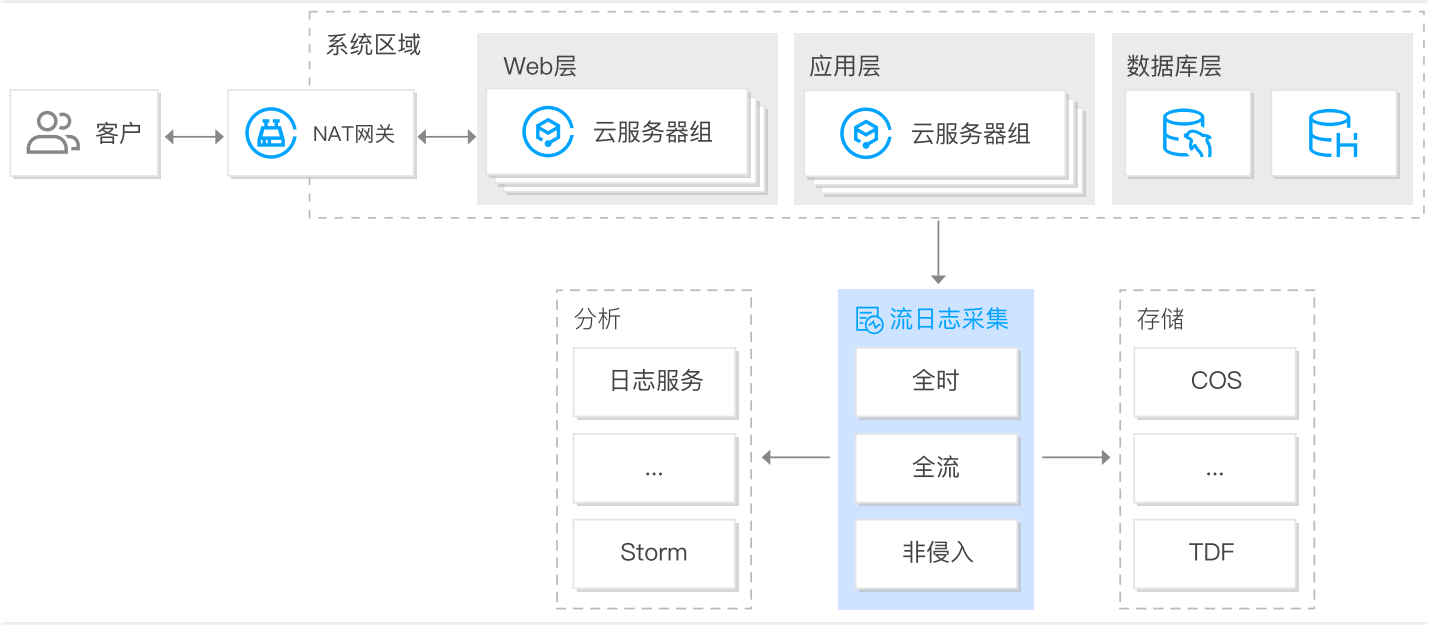
快速定位网络故障

网络质量是业务稳定的基石，通过流日志可保存故障现场，助力您快速定位网络故障，进行网络回溯取证，减少网络停用时间，如：

- 快速定位问题根源的云主机，如：广播风暴、带宽的过度使用的云主机。
- 快速定位云主机不可访问是否为安全组或 ACL 设置不合理。

配置建议：

- 创建流日志采集网卡流量。
- 网络日志投递至日志服务、COS 等服务进行查询、分析或存储。



合理优化网络架构

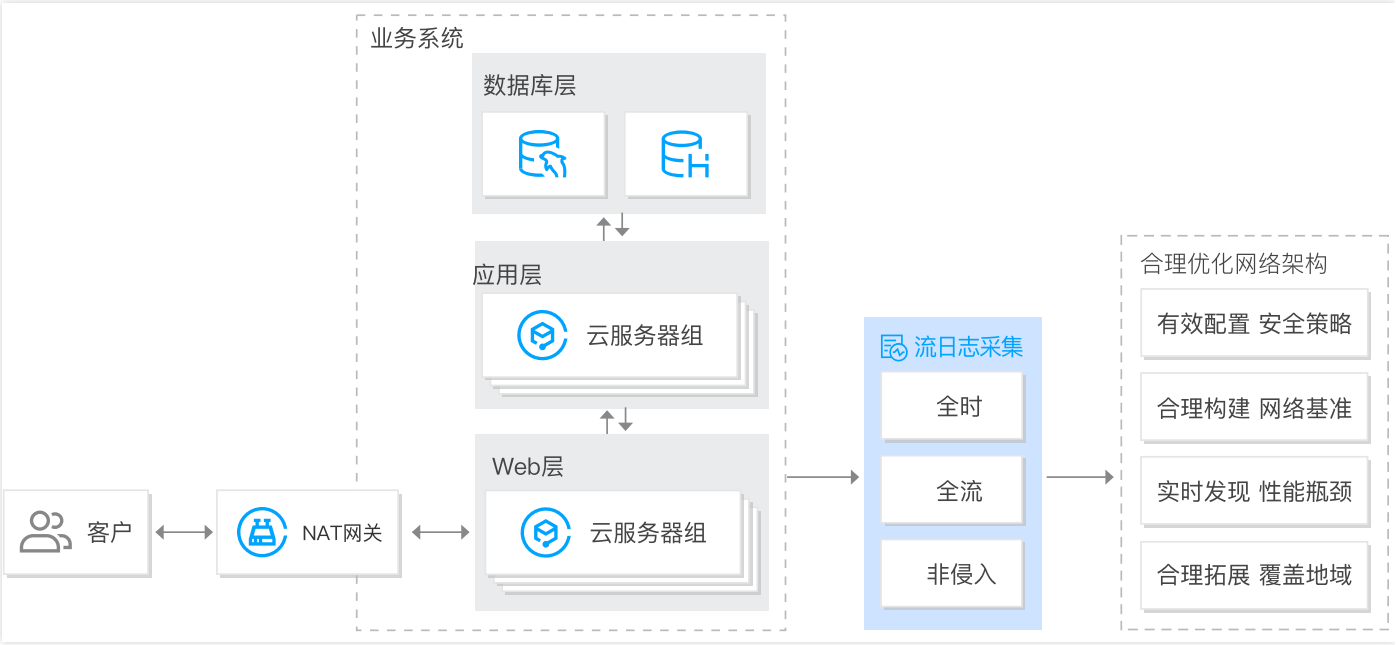
流日志可采集全网、全时、全流的弹性网卡流量，通过大数据分析及可视化，助力您提升数据驱动的网络运维能力，合理优化网络架构，如：

- 分析历史网络数据，构建业务网络基准。
- 及时发现性能瓶颈，合理扩容或流量降级。
- 分析访问用户地域，合理拓展覆盖域。
- 分析网络流量，优化网络安全策略。

配置建议：

- 创建流日志采集网卡流量。

- 网络日志至日志服务 /ELK/Splunk 等进行分析。



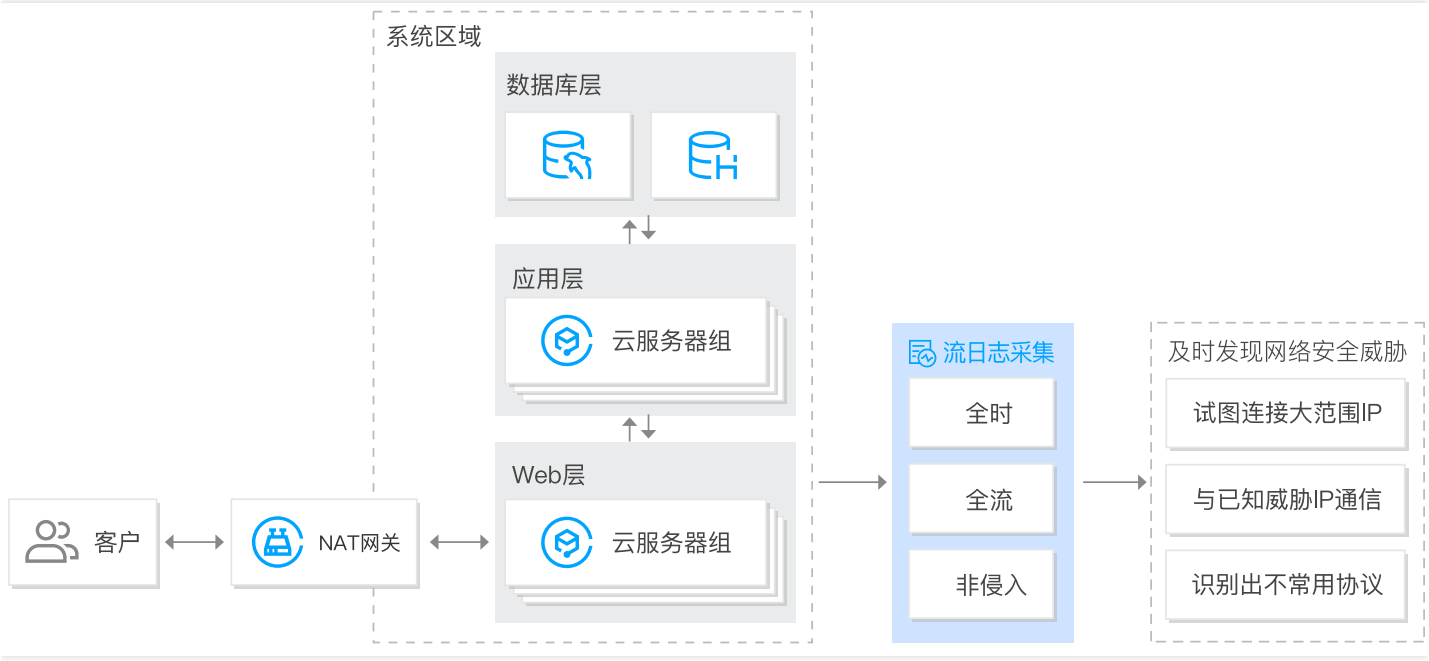
迅速发现网络安全威胁

传统流量检查点的增加，会引起云主机性能下降，流日志采用全时、全流、非侵入的采集方式，助力您在不影响云主机性能情况下，及时发现网络安全威胁，提升系统安全性，如：

- 试图连接大范围 IP。
- 与已知威胁 IP 通信。
- 识别出不常用协议。

配置建议：

- 创建流日志采集网络流量。
- 网络日志投递日志服务、ELK 等进行查询、分析。


系统区域
数据库层
应用层
云服务器组
Web层
云服务器组
客户
NAT网关
流日志采集
全时
全流
非侵入
及时发现网络安全威胁
试图连接大范围IP
与已知威胁IP通信
识别出不常用协议

产品优势

最近更新时间：2018-04-04 15:37:38

无性能损耗

非侵入的采集从根源上解决传统采集方式大量消耗云主机带宽及 CPU 的痛点。

安全

旁路采集使您无需在子机内安装任何插件，解决您的安全顾虑，故障发生时也可明确无采集方的责任。

全时全流

强大的包处理能力可采集全网的弹性网卡流量，准确展现业务网络状况，让您对云网络质量了如指掌。

实时性强

实时的海量网络流数据采集，帮助企业迅速实现业务分析、趋势判断与决策响应。

简单易管理

秒级开通、简单易管理，帮助您提升运维效率，使您的企业更专注于核心业务创新，提升企业竞争力。

产品功能

最近更新时间：2018-04-04 15:37:43

流日志采集

您可以为 **VPC、子网或弹性网卡** 创建流日志。如果您为 VPC 或子网创建流日志，则会采集该 VPC 或子网中的每个弹性网卡的流日志。流日志数据投递到日志服务中的主题，并且每个弹性网卡有唯一的日志流。日志流包含流日志记录。

流日志查询

您可在日志服务中实现查询，支持全文检索、多关键词检索、跨主题查询等功能，秒级返回查询结果，支持亿级日志数据检索。

流日志数据投递

- **投递至 COS：**日志服务支持将流日志数据投递至您账户下的 COS 存储桶中，实现对日志数据的存储与管理。
- **日志投递至 CAS（敬请期待）：**日志服务支持将流日志数据投递至您账户下的 CAS 归档存储中，实现日志数据的备份存储，满足日志审计的需求。
- **日志投递至 TDF（敬请期待）：**日志服务支持将流日志数据投递至 TDF ，满足日志数据定制化的数据分析需求。

流日志记录

流日志记录代表您的流日志中的网络流。每个记录捕获特定捕获窗口中的特定 5 元组的网络流。

- **5 元组：**指源、目标和协议。
- **捕获窗口：**指一段持续时间，在这段时间内流日志服务会聚合数据，然后再发布流日志记录。捕获窗口大约为 5-10 分钟，推送时间约为 5 分钟。流日志记录是以空格分隔的字符串，采用以下格式：
  `version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status`

字段	说明
version	流日志版本。

字段	说明
account-id	流日志的账户 appid。
interface-id	弹性网卡 ID。
srcaddr	源IP。
dstaddr	目标IP。
srcport	流量的源端口。
dstport	流量的目标端口。
protocol	流量的 IANA 协议编号。有关更多信息，请转到分配的 Internet 协议 编号。
packets	捕获窗口中传输的数据包的数量。
bytes	捕获窗口中传输的字节数。
start	捕获窗口启动的时间，采用 Unix 秒的格式。
end	捕获窗口结束的时间，采用 Unix 秒的格式。
action	与流量关联的操作： ACCEPT：安全组或网络 ACL 允许记录的流量。 REJECT：安全组或网络 ACL 未允许记录的流量。
log-status	流日志的日志记录状态： OK NODATA：捕获窗口中没有传入或传出弹性网卡的网络流量。 SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。

示例：流日志记录

已接受流量流日志记录

下面是流日志记录的示例，其中允许指向账户 1251762227 中的弹性网卡 eni-lq6mkcis 的 SSH 流量 (目标端口 22，TCP 协议)。

```
2 1251762227 eni-lq6mkcis 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010 1418530070 ACCEPT OK
```

已拒绝流量流日志记录

下面是流日志记录的示例，其中拒绝了指向账户1251762227 中的弹性网卡 eni-lq6mkcis 的 RDP 流量 (目标端口 3389，TCP 协议)。

```
2 1251762227 eni-lq6mkcis 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK
```

无数据流日志记录

以下示例的流日志记录在捕获窗口中未记录数据。

```
V1 1251762227 eni-lq6mkcis - - - - - - - 1431280876 1431280934 - NODATA
```

跳过记录的记录

以下示例的流日志记录在捕获窗口中跳过了记录。

```
V1 1251762227 eni-lq6mkcis - - - - - - - 1431280876 1431280934 - SKIPDATA
```

安全组和网络 ACL 规则

安全组是有状态的，即对所允许流量的响应也会被允许。相反，网络 ACL 是无状态的，即对所允许流量的响应需要遵守网络 ACL 规则。

例如，您从家中的计算机 (IP 地址为 203.0.113.12) 对您的实例 (网络接口的私有 IP 地址为 172.31.16.139) 使用 ping 命令。您的安全组入站规则允许 ICMP 流量，出站规则不允许 ICMP 流量，但是，由于安全组是有状态的，因此允许从您的实例响应 ping。
您的网络 ACL 允许入站 ICMP 流量，但不允许出站 ICMP 流量。由于网络 ACL 是无状态的，响应 Ping 将被丢弃，不会传输到您家中的计算机。在流日志中，它显示为 2 个流日志记录：

- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 ACCEPT 记录。
- 网络 ACL 拒绝的响应 ping 的 REJECT 记录。

```
V1 1251762227 eni-lq6mkcis 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
V1 1251762227 eni-lq6mkcis 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

如果您的网络 ACL 允许出站 ICMP 流量，流日志会显示两个 ACCEPT 记录 (一个针对发起 ping，一个针对响应 ping)。如果您的安全组拒绝入站 ICMP 流量，流日志会显示一个 REJECT 记录，因为流量未到达您的实例。

使用限制

最近更新时间：2018-04-04 15:37:50

流日志在使用时应注意以下事项：

- 仅支持 VPC 内弹性网卡启用流日志，暂不支持 基础网络云主机、数据库、网关、对等连接等服务创建流日志。
- 在创建流日志之后，您不能更改其配置（如修改流日志投递的日志服务）。不过，您可以删除流日志并使用必需的配置创建新的流日志。
- 流日志不会捕获所有类型的 IP 流量。以下类型的流量不予以记录：
  - Windows 实例为 Windows 许可证激活而生成的流量。
  - DHCP 流量。

计费方式

最近更新时间：2018-04-04 15:37:57

使用流日志暂不会收取费用，流日志的在日志服务使用将按日志服务的 标准收费。

操作指南

最近更新时间：2018-04-04 15:38:03

创建流日志

1. 登录腾讯云控制台，选择【私有网络】选项卡，选择【流日志】。

> **注意：**
> 流日志正在火热内测中，欢迎申请。

2. 单击左上角【新建】按钮，在弹出框中依次输入或确定以下参数：
【采集类型】指定流日志应捕获被安全组或ACL已拒绝流量、已接受流量、所有流量。
【日志集】指定流日志在日志服务内的存储集合。
【日志主题】指定日志存储的最小维度，用于区别不同类型日志，比如 Accept 日志等。

> **注意：**
> 如果您需创建日志集和日志主题对象，请参考下文： 创建日志集和日志主题。

3. 选择结束后单击【确认】按钮，即可完成流日志的创建。

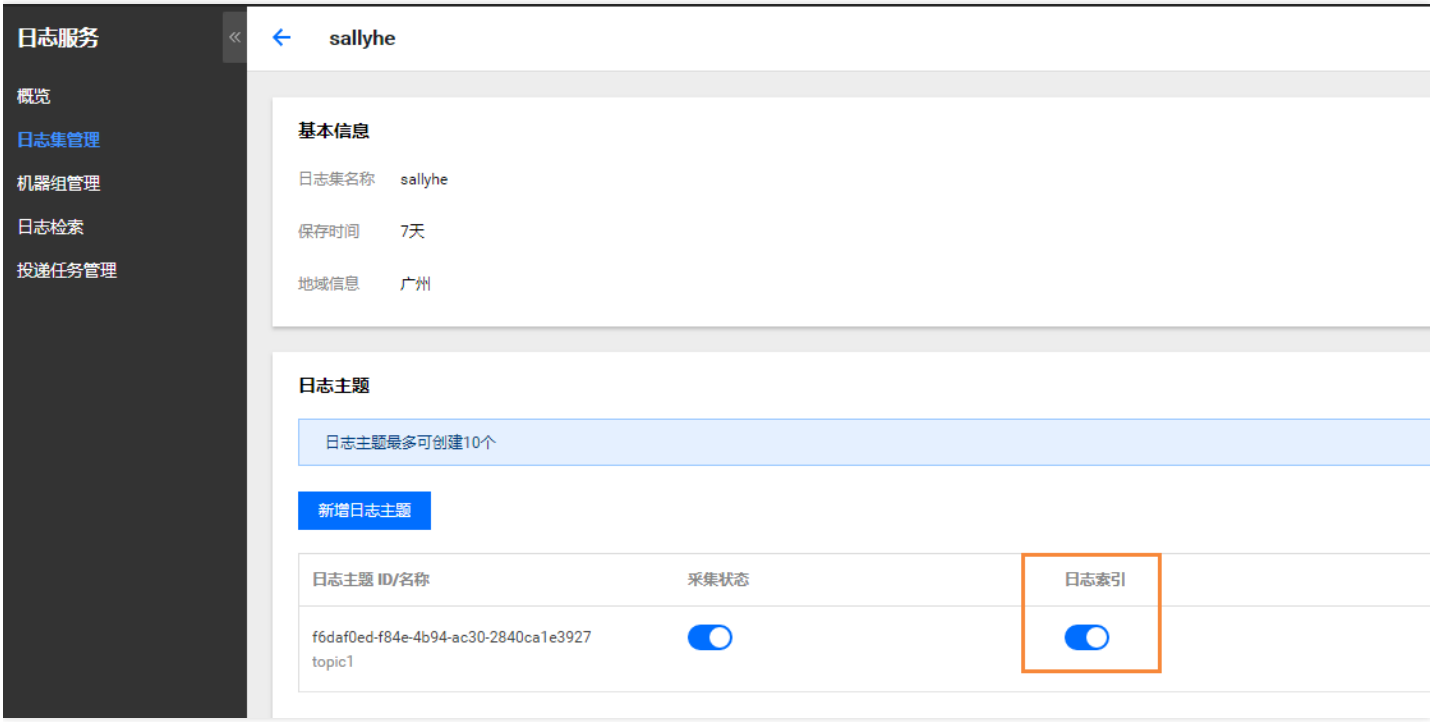
> **注意：**
> - 创建完 流日志，首次创建流日志需要约 15 分钟后（10 分钟捕获窗口，5 分钟数据推送时间），方可在日志服务中查看流日志。
> - 流日志本身不会产生费用，数据存储在日志服务中，将按日志服务的 标准收费。

创建日志集和日志主题

您需创建日志集和日志主题来存储、查看流日志。

1. 登录腾讯云控制台，选择【日志服务】选项卡，选择【日志集管理】。
2. 创建日志集服务，注意**无需开启 agent。**
3. 创建成功，请开启 **索引** 来查看和检索流日志。

> **注意：**
> - 您 **无需安装 agent**,也无需关心机器组状态。
> - 如果您没有将流日志导至 cos 等服务的需求，也 **无需关心投递任务。**



删除流日志

1. 登录腾讯云控制台，选择【私有网络】选项卡，选择【流日志】。
2. 选择需要删除的流日志，单击【删除】按钮即可删除该流日志。

> **注意：**
> 流日志的删除并不会删除日志集合日志主题。

查看流日志记录

您可在日志服务中查看流日志，帮助您快速定位业务问题。您可以选择同一个日志集中的多个日志主题，进行跨日志主题的查询，操作指南请点击查看 日志检索。