网络流日志

产品简介

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

产品简介

产品概述

最近更新时间：2021-08-31 16:53:18

网络流日志（Flow logs）为您提供全时、全流、非侵入的流量采集服务，可将采集的网络流量进行实时的存储、分析，适用于故障排查、合规审计、架构优化、安全检测等场景，让您的云上网络更加稳定、安全和智能。

您可以为弹性网卡等创建网络流日志，采集传入/传出的流量。创建流日志后，您可以在 日志服务（CLS） 中查看和检索数据。若需对流日志数据进行生命周期管理，则可以在日志服务（CLS）中将指定流日志投递其他云产品进行分析或存储，例如投递至 COS 存储桶中。

> 说明：
> 目前网络流日志处于内测中，如有需要，请提交 工单申请。

产品优势

最近更新时间：2021-08-31 16:49:42

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服务器带宽及 CPU 的痛点。

安全

旁路采集使您无需在云服务器内安装任何插件，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：2021-07-16 16:22:52

流日志具有日志采集、查询、数据管理、数据记录等功能，帮助您降低运维门槛，轻松定位业务问题。

流日志采集

为弹性网卡创建流日志后，系统将自动采集弹性网卡的日志流，并将日志数据同步至 日志服务 CLS。在 CLS 的主题中，每个弹性网卡有唯一的日志流，其中包含流日志记录。

流日志查询

日志服务 CLS 支持亿级日志数据检索。您可以进行全文检索、多关键词检索、跨主题查询等操作，秒级返回查询结果。

流日志数据

流日志与 日志服务 CLS 深度结合，实现对日志数据的存储与管理。

流日志记录

流日志将记录特定捕获窗口中，按五元组规则过滤的网络流。

- **五元组**
  即源 IP 地址，源端口，目的 IP 地址，目的端口和传输层协议这五个量组成的一个集合。
- **捕获窗口**
  即一段持续时间，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。
account-id	流日志的账户 AppID。

字段	说明
interface-id	弹性网卡 ID。
srcaddr	源 IP。
dstaddr	目标 IP。
srcport	流量的源端口。当流量为 ICMP 协议时，该字段表示 ICMP 的 id。
dstport	流量的目标端口。当流量为 ICMP 协议时，该字段表示 ICMP 的 type（高8bit）+code（低8bit）组合。
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：表示数据正常记录到指定目标。 NODATA：表示捕获窗口中没有传入或传出网络流量，此时“packets”和“bytes”字段会显示为“-1”。 SKIPDATA：表示捕获窗口中跳过了一些流日志记录。可能是内部容量限制或内部错误引起的。

示例

- 若允许接受账户 1251762227 中的弹性网卡 eni-lq6mkcis 的 SSH 流量（目标端口 22，TCP 协议），流日志记录如下：

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

- 若拒绝账户1251762227中的弹性网卡 eni-lq6mkcis 的 RDP 流量（目标端口3389，TCP 协议），流日志记录如下：

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

- 若在捕获窗口中未记录数据，流日志记录如下：

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

- 若在捕获窗口中跳过了记录，流日志记录如下：

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

- 安全组和网络 ACL 规则的流日志记录
  - 安全组为有状态，因此允许响应所有的流量。
  - 网络 ACL 为无状态，因此对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 14329
17142 ACCEPT OK
```

```
V1 1251762227 eni-lq6mkcis 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 14329
17142 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。

应用场景

最近更新时间：2021-03-03 17:45:43

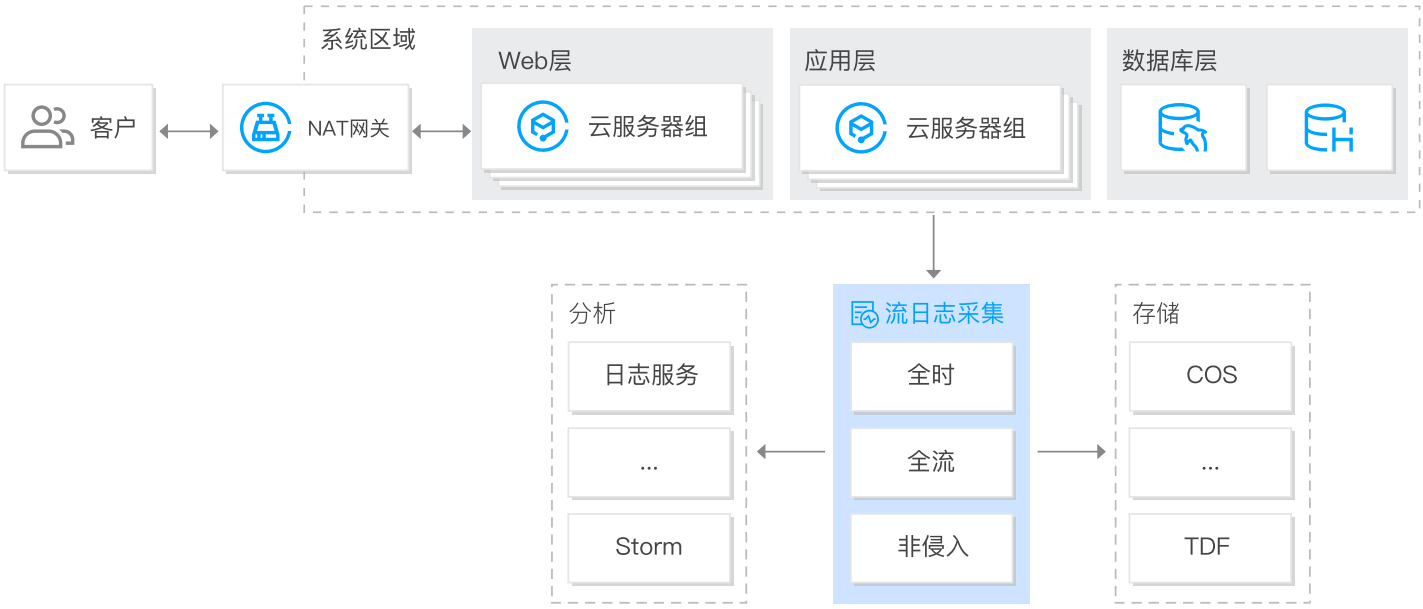
快速定位网络故障

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。具体如下：

- 快速定位问题根源的云服务器，例如广播风暴、带宽过度使用的云服务器。
- 快速定位云服务器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。



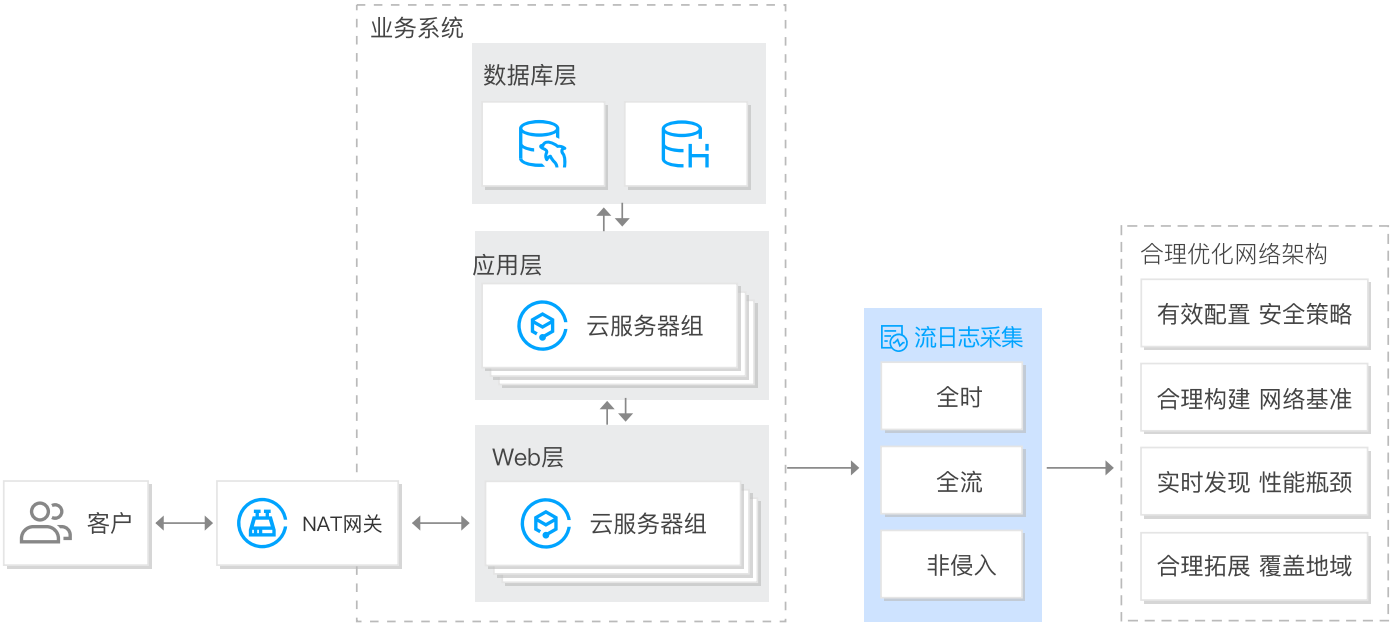
合理优化网络架构

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。具体如下：

- 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。
- 网络日志投递至日志服务 /ELK/Splunk 等进行分析。



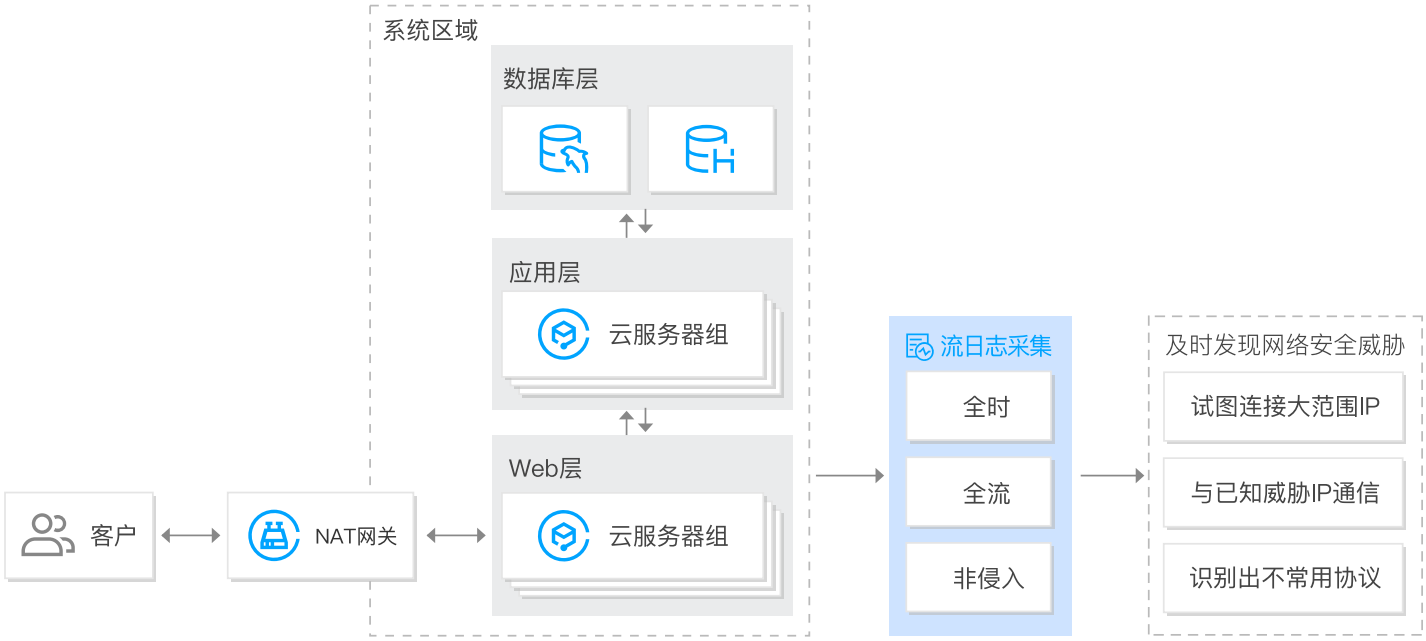
迅速发现网络安全威胁

传统流量检查点的增加，会引起云服务器性能下降，流日志采用全时、全流、非侵入的采集方式，助力您在不影响云服务器性能情况下，及时发现网络安全威胁，提升系统的安全性。具体如下：

- 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。
- 网络日志投递至日志服务、ELK 等进行查询与分析。

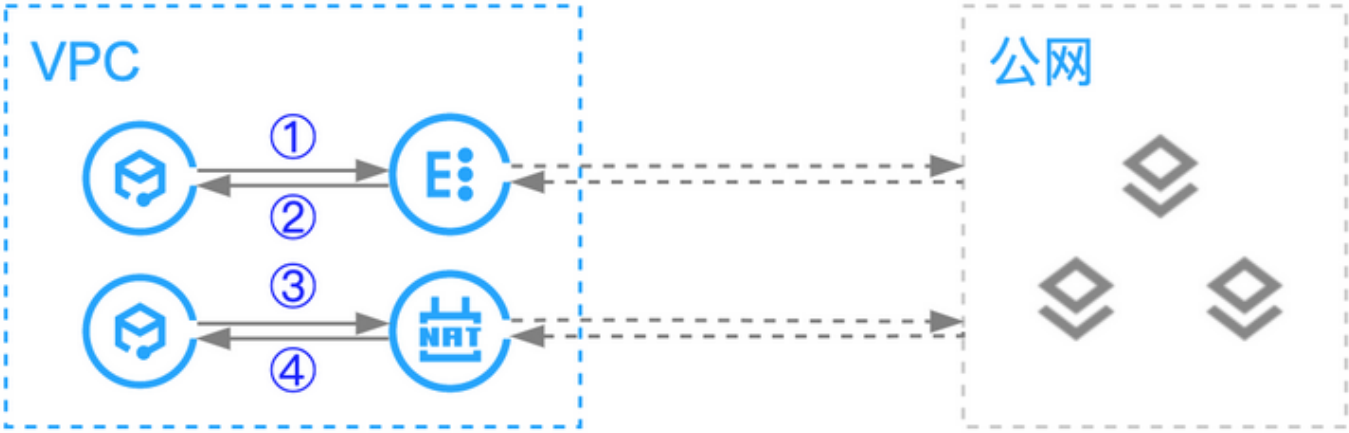

系统区域
数据库层
应用层
云服务器组
Web层
云服务器组
客户
NAT网关
流日志采集
全时
全流
非侵入
及时发现网络安全威胁
试图连接大范围IP
与已知威胁IP通信
识别出不常用协议

使用限制

最近更新时间：2021-01-27 17:36:24

注意事项

- 网络流日志仅支持采集 VPC 内弹性网卡上的流日志，暂不支持采集基础网络云服务器、数据库、网关、对等连接等服务的日志。
- 创建流日志后，您不能更改其配置（如修改流日志投递的日志服务）。
- 流日志不支持采集的 IP 流量类型：
  - Windows 实例为 Windows 许可证激活而生成的流量。
  - DHCP 流量。
- 网络流日志采集云服务器上弹性网卡的流量时，出方向采集限速前的流量，入方向是限速后的流量。
  例如，若为云服务器的弹性网卡创建网络流日志：
  - 当云服务器通过负载均衡访问公网时，则出方向采集箭头1的流量，入方向采集箭头2的流量。
  - 当云服务器通过 NAT 网关访问公网时，则出方向采集箭头3的流量，入方向采集箭头4的流量。



支持列表

网络流日志支持采集流量的弹性网卡所属云服务器的地域和机型如下：

地域	广州、上海、北京、上海金融、深圳金融、成都、美国-美西。
机型	标准型 S1、标准型 S2、标准型 S3、内存型 M1、内存型 M2、内存型 M3、高 IO 型 I1、高 IO 型 I2、高 IO 型 I3、计算型 C2、计算型 C3、计算增强型 CN3、大数据型 D1。

相关产品

最近更新时间：2021-08-31 16:08:58

网络流日志的相关产品信息，请参见下表：

产品名称	与网络流日志的关系
云服务器	网络流日志可快速定位问题根源的云服务器
COS 存储	网络流日志可投递至 COS 存储桶中，满足日志审计需求
安全组	网络流日志可快速检测云服务器不可访问的原因是否为安全组设置不合理
网络 ACL	网络流日志可快速检测云服务器不可访问的原因是否为网络 ACL 设置不合理