网络流日志

快速入门

产品文档

腾讯云

快速入门

最近更新时间：2022-05-18 11:22:09

本文以内网互通场景下，为弹性网卡创建流日志为例，演示流日志的快速入门操作。弹性网卡创建网络流日志后，即可将网络流量进行实时存储、分析，适用于故障排查、合规审计、安全检测等场景。

前提条件

- 确保您的云服务器在网络流日志 支持列表。
- 由于流日志数据需要投递到日志服务 CLS，请确保已完成授权 CLS，方可查看日志数据，具体操作请参见 授权流日志访问 CLS 权限 。
- 您已创建日志主题，具体操作请参见 新增日志主题。

背景信息

服务器 A（10.16.0.22）和服务器 B（10.16.0.40）在同一 VPC 中，登录服务器 A 对服务器 B 执行 ping 命令将触发服务器弹性网卡上发生流量，若为服务器 A 的弹性网卡创建网络流日志，流日志中将会记录该流量数据。

```
[root@VM-0-22-centos ~]# ping 10.16.0.40
PING 10.16.0.40 (10.16.0.40) 56(84) bytes of data.
64 bytes from 10.16.0.40: icmp_seq=1 ttl=64 time=0.490 ms
64 bytes from 10.16.0.40: icmp_seq=2 ttl=64 time=0.449 ms
64 bytes from 10.16.0.40: icmp_seq=3 ttl=64 time=0.437 ms
64 bytes from 10.16.0.40: icmp_seq=4 ttl=64 time=0.429 ms
64 bytes from 10.16.0.40: icmp_seq=5 ttl=64 time=0.471 ms
64 bytes from 10.16.0.40: icmp_seq=6 ttl=64 time=0.665 ms
64 bytes from 10.16.0.40: icmp_seq=7 ttl=64 time=0.682 ms
64 bytes from 10.16.0.40: icmp_seq=8 ttl=64 time=0.451 ms
64 bytes from 10.16.0.40: icmp_seq=9 ttl=64 time=0.415 ms
```

操作步骤

1. 登录 私有网络控制台，在左侧导航栏选择**流日志 > 日志列表**。

2. 在“流日志”页面左上角选择地域，然后单击 **+新建**，并在“新建流日志”对话框中配置以下参数：

字段	含义
名称	该流日志的名称。
采集范围	指定流日志采集范围，本例选择弹性网卡。
私有网络	弹性网卡所在私有网络，本例选择服务器 A 所在的私有网络。
子网	弹性网卡所在子网，本例选择服务器 A 所在的子网。
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，本例选择“接受”。
日志集	指定流日志在日志服务内的存储集合，请选择您已创建的日志集，若暂未创建日志集，则单击**新建**前往日志服务控制台新建。
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，例如 Accept 日志等。 请选择您已创建的日志主题，若暂未创建日志主题，则前往日志服务控制台新建。
标签键	可选参数，您可以直接输入（即新建）或选择已有标签键，用于流日志查找和管理。
标签值	可选参数，您可以直接输入（即新建）或选择已有标签值，也可以为空值。

3. 单击**确定**。

> 注意
> - 首次创建流日志时，创建完成后需等待约10分钟后（5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，将按标准收费。

结果验证

约10分钟后，在“流日志”页面目标流日志右侧“操作”列单击**查看**。在“检索分析”页面选择时间，并输入服务器 B 的 IP 进行关键词检索。