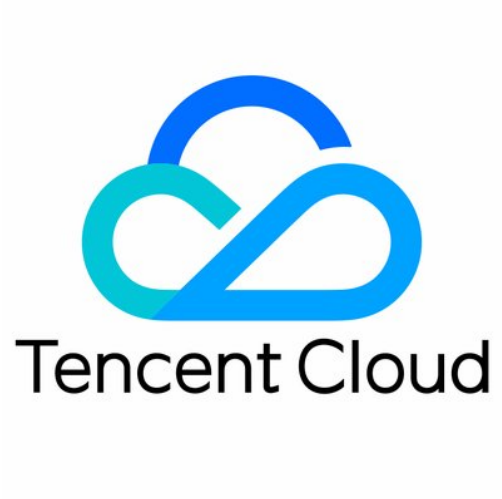
Flow Logs

Product Introduction

Product Documentation



Contents

Product Introduction
Product Overview

Last updated : 2021-01-22 19:06:24

Tencent Cloud Flow Logs (FL) provides a full-time, full-flow and non-intrusive ENI traffic collection service, enabling you to store and analyze network flow in real time for troubleshooting, compliance auditing, architecture optimization, and security detection. With FL, your cloud networks will become more stable, secure, and intelligent.

FL comes with the following features:

- Its flow logs allow you to capture inbound/outbound ENI IP traffic in VPC.
- After a flow log is created, you can view and search for its data in Cloud Log Storage (CLS). You can also publish specified flow logs to other Tencent Cloud products for analysis or storage; for example, you can publish a flow log to a COS bucket to manage its lifecycle.

Note :

The FL service is currently in beta. To try it out, please submit a ticket.

Product Advantages

Last updated : 2020-02-26 18:30:03

No Performance Loss

Non-intrusive collection completely avoids huge consumption of CVM bandwidth and CPU in traditional collection methods.

Secure

Non-intrusive collection requires no plug-in installed in the CVM, eliminating your security concerns. Besides, it helps to clarify that collector has no responsibility in case of failure.

Full-Time and Full-Flow

Powerful packet processing capability can collect the ENI traffic of the entire network and accurately reflect the status of your business network, helping you get a full picture of the cloud network quality.

Strong Real-Time Performance

Real-time collection of massive network flow data can help enterprises quickly perform business analysis, trend judgment and decision-making response.

Easy to Manage

The service can be activated instantly and is easy to manage. With this service, you can improve OPS efficiency, focus more on core business innovation, and enhance enterprise competitiveness.

Features

Last updated : 2021-01-22 19:06:24

Flow Logs (FL) service provides log collection, query, data management and record features, helping you easily perform OPS and quickly troubleshoot issues.

Flow Log Collection

After a flow log is created for an ENI, the log stream of the ENI will be automatically collected and the log data will be synced to CLS. In the CLS topic, each ENI has a unique log stream which contains flow log records.

Flow Log Query

CLS supports querying hundreds of millions of log data entries. You can search for data with full text or multiple keywords across topics, and the results can be returned within seconds.

Flow Log Data

FL integrates with CLS to store and manage log data.

Flow Log Record

A flow log records the network flow that passes through the capture window and matches the 5-tuple rules.

- **5-tuple**
  It refers to a collection of five values: source IP address, source port, destination IP address, destination port, and transport layer protocol.
- **Capture window**
  It refers to a time period of 5 to 10 minutes, during which FL aggregates data and takes about 5 minutes to publish the flow log records. Flow log records are strings separated with spaces as the following format:
  `version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status`

Field	Description
version	FL version.
account-id	AppID of the FL account.
interface-id	ENI ID.
srcaddr	Source IP.
dstaddr	Destination IP.
srcport	Source port of the traffic.
dstport	Destination port of the traffic.
protocol	IANA protocol number of the traffic. For more information, see the assigned Internet Protocol Numbers.
packets	Number of packets transferred in the capture window.
bytes	Number of bytes transferred in the capture window.
start	Start time of the capture window in Unix seconds.
end	End time of the capture window in Unix seconds.
action	Traffic-related action. Valid values: ACCEPT: the traffic allowed by the security group or network ACL. REJECT: the traffic rejected by the security group or network ACL.
log-status	Logging status of the flow log. OK: data is logging normally to the specified destination. NODATA: there was no network flow passing through the ENI in the capture window. SKIPDATA: some flow log records were skipped in the capture window. This may be caused by an internal capacity constraint or an internal error.

Samples

- The flow log recorded when the SSH traffic (destination port: 22; TCP) of the ENI `eni-lq6mkcis` under the account `1251762227` was accepted:

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

- The flow log recorded when the RDP traffic (destination port: 3389; TCP) of the ENI `eni-lq6mkcis` under the account `1251762227` was rejected:

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

- The flow log recorded when there was no data collected in the capture window:

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

- The flow log recorded when there was data skipped in the capture window:

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

- Flow log record of security group and network ACL rules:
  - The security group is stateful; therefore, it allows response to the accepted traffic.
  - The network ACL is stateless; therefore, the response to the accepted traffic should follow the network ACL rules.

  For example, if you ping your instance (private IP of the network interface: 172.31.16.139) from your home computer (IP: 203.0.113.12), and the security group's inbound rule allows the ICMP traffic while its outbound rule does not, your instance will respond to the ping request as the security group is stateful.
  If your network ACL allows the inbound but rejects the outbound ICMP traffic, response to the ping request will be discarded and will not be sent to your home computer as the network ACL is stateless. In this case, the flow log has two records:
  - The ACCEPT record for sending the ping request allowed by both network ACL and security group (so that the traffic can reach your instance).
  - The REJECT record for the response to ping request rejected by the network ACL.

```
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
```

If your network ACL allows the outbound ICMP traffic, your flow log will have two ACCEPT records (one for sending the ping request and the other for responding). If your security group rejects the inbound ICMP traffic and the traffic does not reach your instance, the flow log has one REJECT record.

Scenarios

Last updated : 2019-08-06 11:47:37

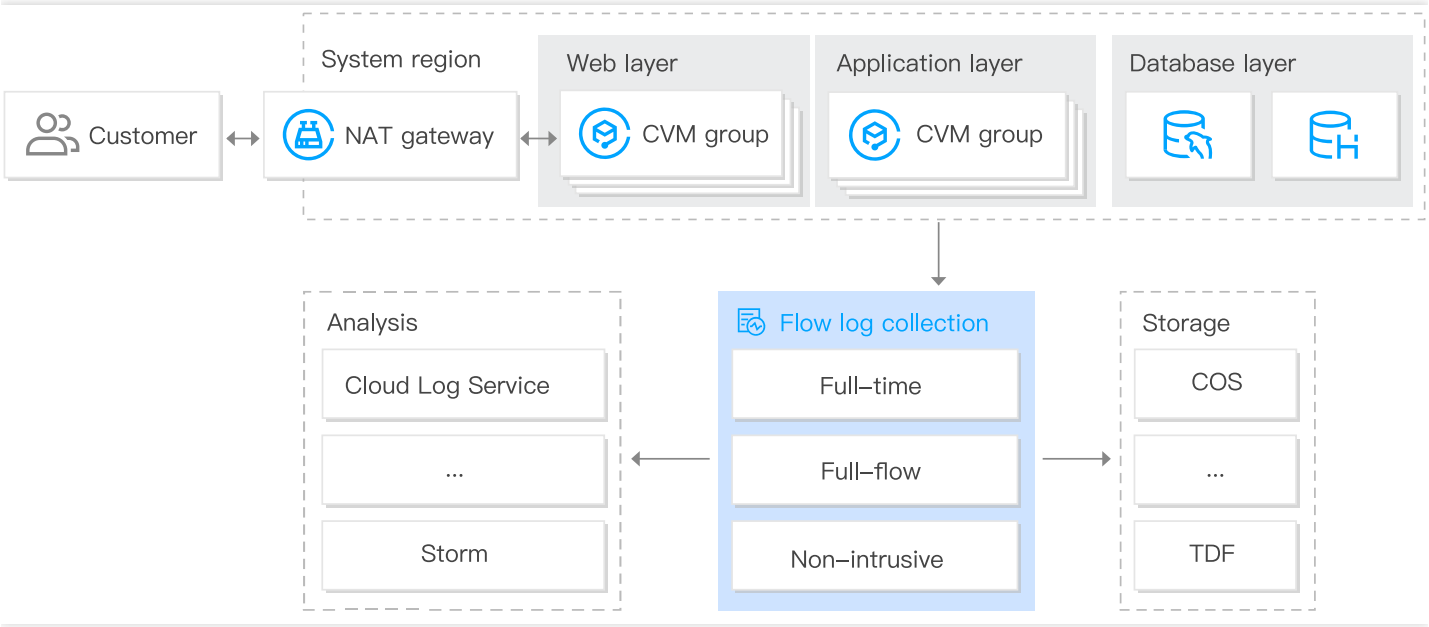
Pinpoint network problems quickly

A good network condition is a prerequisite for business stability. Flow Logs enables you to save the system status when a network failure occurs to pinpoint the failure quickly, perform network tracing and forensic investigation and shorten network downtime. For example:

- Pinpoint the CVM which is the root cause of the problem quickly, such as the CVM in a broadcasting storm or the CVM overusing bandwidth.
- Quickly verify whether the inaccessibility of a CVM is caused by the unreasonable settings for the security group or ACL.

Suggestions on Configuration:

- Create flow logs to capture ENI traffic.
- Deliver network logs to Cloud Log Service, COS and other services for query, analysis or storage.



Reasonable optimization of network architecture

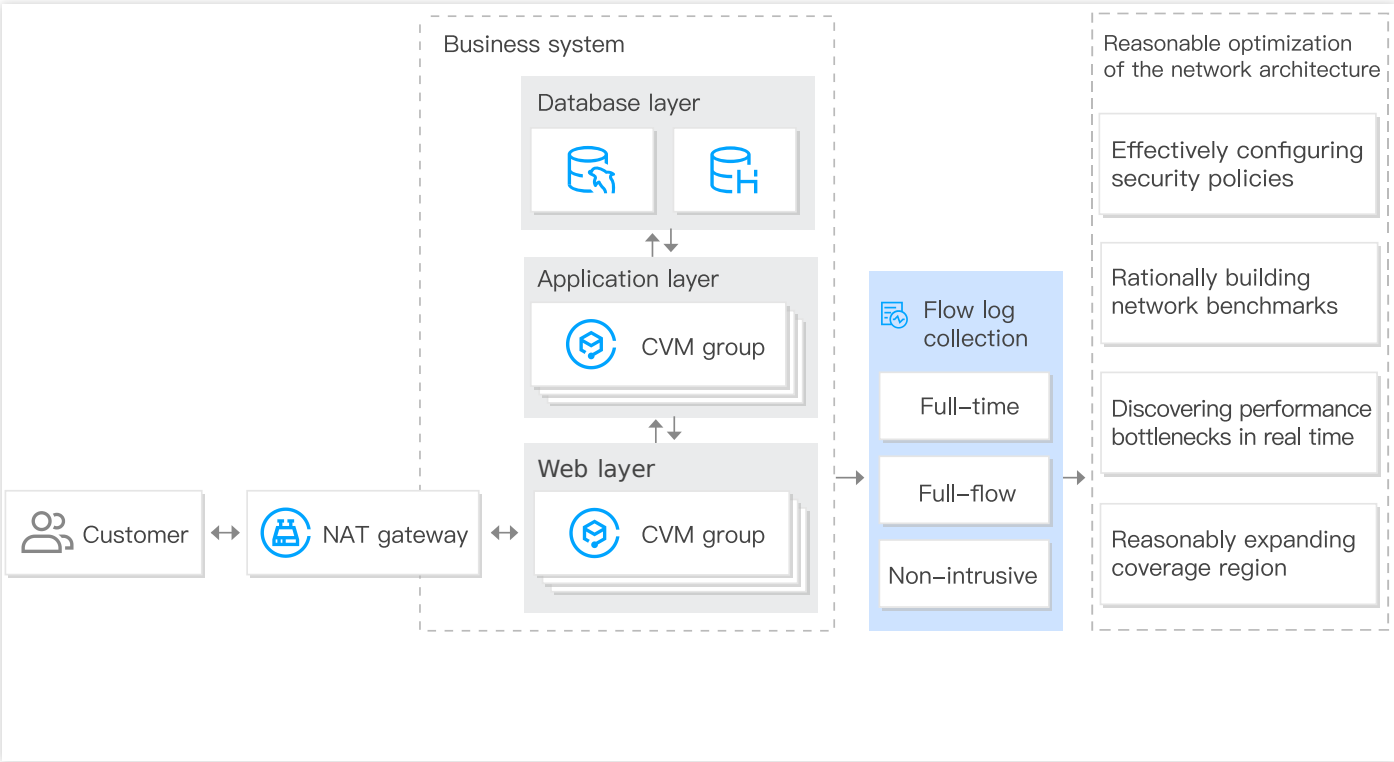
Flow Logs allows the full-time, full-flow capture of ENI traffic across the network to help you enhance data-driven network OPS capability and optimize network architecture based on big data analysis and visualization. For example:

- Analyze historical network data to build business network benchmarks.

- Identify performance bottlenecks as early as possible for a reasonable capacity expansion or traffic degrading.
- Analyze the regions of accessing users to expand coverage reasonably.
- Analyze network traffic to optimize network security policies.

Suggestions on Configuration:

- Create flow logs to capture ENI traffic.
- Deliver network logs to Cloud Log Service, ELK, Splunk and other services for analysis.



Identify threats to network security quickly

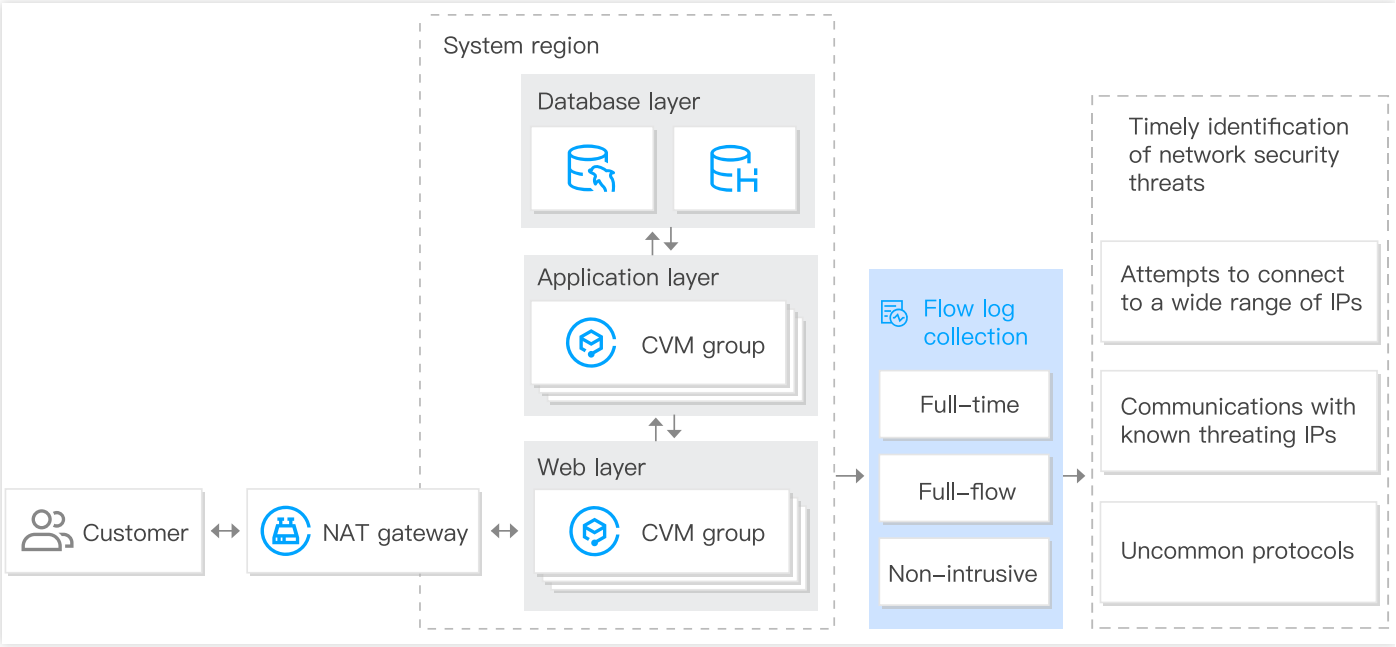
The addition of traditional traffic checkpoints can cause the performance degradation of CVM. Flow Logs allows full-time, full-flow, and non-intrusive capture of traffic to help you identify threats to network security as early as possible and enhance system security without affecting the CVM performance. For example:

- Try to connect a wide range of IPs.
- Communicate with an IP that is considered a known threat.
- Identify an uncommonly used protocol.

Suggestions on Configuration:

- Create flow logs to capture network traffic.

- Deliver network logs to Cloud Log Service, ELK and other services for query and analysis.

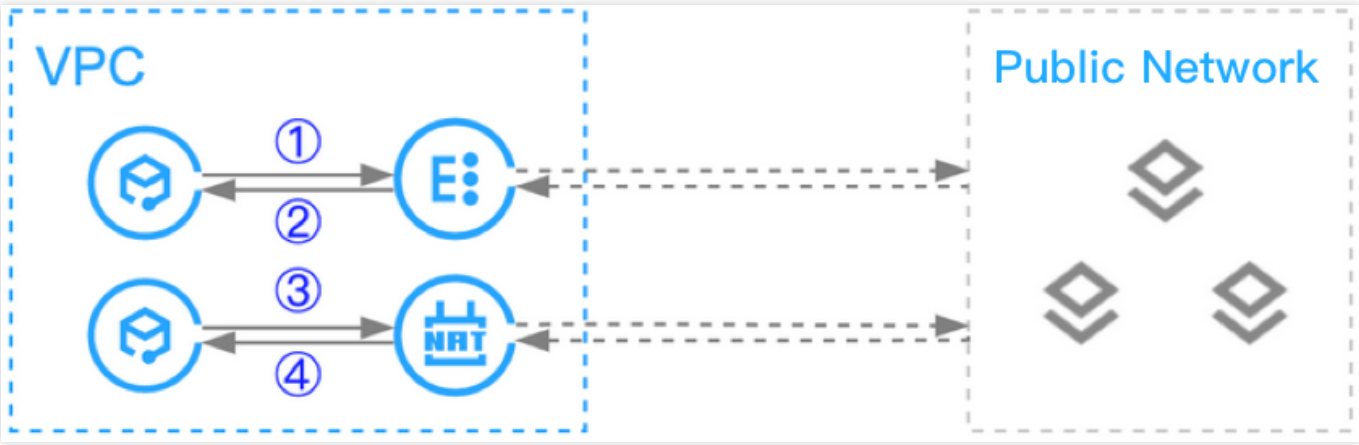


Use Limits

Last updated : 2021-02-02 16:55:07

Notes

- The Flow Logs (FL) service is only available to the ENI in VPC, while the flow logs of classic network-based CVM, database, gateway, peering connection and other services cannot be collected.
- The configurations of a flow log cannot be modified after creation. For example, the cloud log service (CLS) to which the flow log is published cannot be modified.
- FL does not support capturing the following IP traffic:
  - Traffic generated by Windows instances for activation of Windows license.
  - DHCP traffic.
- FL collects the original outbound traffic and limited inbound traffic of the ENI on a CVM.
  Assume you create a flow log for the ENI on a CVM:
  - When the CVM accesses the public network through a cloud load balancer, the “1” traffic will be collected for the outbound direction and the “2” traffic will be collected for the inbound direction.
  - When the CVM accesses the public network through a NAT Gateway, the “3” traffic will be collected for the outbound direction and the “4” traffic will be collected for the inbound direction.



Supported List

FL supports collecting ENI traffic on the following CVM instances in regions listed below.

Region	Guangzhou, Shanghai, Beijing, Chengdu and Western US
Model	Standard S1, Standard S2, Standard S3, MEM optimized M1, MEM optimized M2, MEM optimized M3, High IO I1, High IO I2, High IO I3, Compute C2, Compute C3, Compute Network-optimized CN3, and Big Data D1

Relevant Products

Last updated : 2020-02-26 18:32:08

For information on products relevant to Flow Logs, see the table below:

Product	Relationship with Flow Logs
CVM	Flow Logs pinpoints the CVM which is the root cause of the problem quickly.
COS	Flow Logs delivers logs to COS buckets for log audit.
Security Group	Flow Logs quickly verifies whether the inaccessibility of a CVM is caused by the unreasonable settings for the security group.
Network ACL	Flow Logs quickly verifies whether the inaccessibility of a CVM is caused by the unreasonable settings for the ACL.