Flow Logs

Product Introduction

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Product Introduction

Overview

Last updated：2024-01-10 16:10:45

Tencent Cloud Flow Logs (FL) provides a full-time, full-flow and non-intrusive traffic collection service. FL enables you to store and analyze the collected 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.

You can create a flow log within the specified collection range (such as ENI, NAT Gateway, and cross-region CCN traffic) to collect inbound/outbound traffic within the range. Then, you can view and search for data in CLS, as well as view log data in the advanced analysis dashboard.

Note:

The FL service for NAT Gateway and cross-region CCN traffic is currently in beta. To try it out, submit a ticket.

Strengths

Last updated：2024-01-10 16:10:45

Lossless Performance

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

Security

Non-intrusive collection requires no plugins 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 Collection

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-Timeness

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

Ease of Management

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.

Visual Analysis

You can visually view and analyze flow log data in the dashboard, which is easy to use and delivers a higher Ops efficiency.

Features

Last updated：2024-01-10 16:10:45

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

Flow Log Collection

After a flow log is created, the log stream in the specified range (such as ENI, NAT Gateway, or cross-region CCN traffic) will be automatically collected, and the log data will be delivered to CLS for storage. In the CLS topic, each ENI has a unique log stream which contains flow log records.

Note:

The FL service for NAT Gateway and cross-region CCN traffic is currently in beta. To try it out, submit a ticket.

Flow Log Query

Flow logs are queried and consumed in CLS. 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 Storage

FL integrates with CLS to store and manage log data.

Creating Dashboard to Display Log Data in Multiple Dimensions

In the logset "flowlog_logset" dedicated to flow logs, you can create a dashboard for ENI flow logs to visualize and analyze flow log data. One dashboard can be created for each log topic.

Data display in the dashboard is as shown below. For more information, see Advanced Analysis.

Flow Log Record

A flow log records the network flow that passes through the capture window and matches particular rules.

Flow log records of cross-region CCN traffic

Flow log records of other types

The flow logs record the network flows filtered by the "quintuple + traffic source region + traffic destination region" rule in a specific capture window; that is, only flow logs that meet the rule in the capture window can be recorded as flow logs of cross-region CCN traffic.

Quintuple + traffic source region + traffic destination region

A quintuple refers to a collection of five values: source IP address, source port, destination IP address, destination port, and transport layer protocol.

The traffic source region refers to the region from which cross-region CCN traffic is sent.

The traffic destination region refers to the region to which cross-region CCN traffic arrives.

Capture window

It refers to the time period during which FL takes 1 minute to aggregate data and takes about 5 minutes to publish the flow log records. Flow log records are strings separated with spaces as the following format:

```
srcaddr dstregionid dstport start dstaddr version packets ccnid protocol
srcregionid bytes action region-id srcport end log-status
```

Field	Data Type	Description
srcaddr	text	Source IP.
dstregionid	text	Traffic destination region.
dstport	long	Traffic destination port. This field will take effect only for UDP/TCP protocols and will be displayed as "-" for other protocols.
start	long	The timestamp when the first packet is received in the current capture window. If there are no packets in the capture window, it will be displayed as the start time of the capture window in Unix seconds.
dstaddr	text	Destination IP.
version	text	Flow log version.
packets	long	Number of packets transferred in the capture window. This field will be displayed as "-" when `log-status` is `NODATA` .
ccn-id	text	Unique CCN instance ID. To get the information of your CCN instance, contact us.
protocol	long	IANA protocol number of the traffic. For more information, see Assigned Internet Protocol Numbers.
srcregionid	text	Traffic source region.
bytes	long	Number of bytes transferred in the capture window. This field will be displayed as "-" when `log-status` is `NODATA` .

action	text	Operation associated with the traffic: ACCEPT: Cross-region traffic normally forwarded over CCN. REJECT: Cross-region traffic prevented from being forwarded due to traffic throttling.
region-id	text	Region where logs are recorded.
srcport	text	Traffic source port. This field will take effect only for UDP/TCP protocols and will be displayed as "-" for other protocols.
end	long	The timestamp when the last packet is received in the current capture window. If there are no packets in the capture window, it will be displayed as the end time of the capture window in Unix seconds.
log-status	text	Logging status of the flow log. Valid values: OK: Data is normally logged to the specified destination. NODATA: There was no inbound or outbound network flow in the capture window, in which case both the `packets` and `bytes` fields will be displayed as `-1` .

A flow log records the network flow that passes through the capture window and matches the quintuple rules.

Quintuple

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 the time period during which FL takes around 5 minutes to aggregate 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. This field indicates the ICMP ID for ICMP traffic.

dstport	Destination port of the traffic. This field indicates a combination of ICMP type (bits 0-7) and code (bits 8-15) for ICMP 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: <br/>ACCEPT: the traffic allowed by the security group or network ACL. <br/>REJECT: the traffic rejected by the security group or network ACL.
log-status	Logging status of the flow log. Valid values:<br>OK: data is logging normally to the specified destination.<br/>NODATA: there was no incoming or outgoing network flow in the capture window. In this case, both `packets` and `bytes` fields are displayed as `-1` .<br/>SKIPDATA: some flow log records were skipped in the capture window. This may be caused by an internal capacity constraint or an internal error.

Example

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
```

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 1
```

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 command as the security group is stateful.

If your network ACL allows the inbound but rejects the outbound ICMP traffic, response to the ping command 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 command allowed by both network ACL and security group (so that the traffic can reach your instance).

The REJECT record for the response to the ping command rejected by the network ACL.

```
V1 1251762227 eni-lq6mkcis 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 143291
```

```
V1 1251762227 eni-lq6mkcis 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 143291
```

If your network ACL allows the outbound ICMP traffic, your flow log will have two ACCEPT records (one for sending the ping command 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：2024-01-10 16:10:45

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:

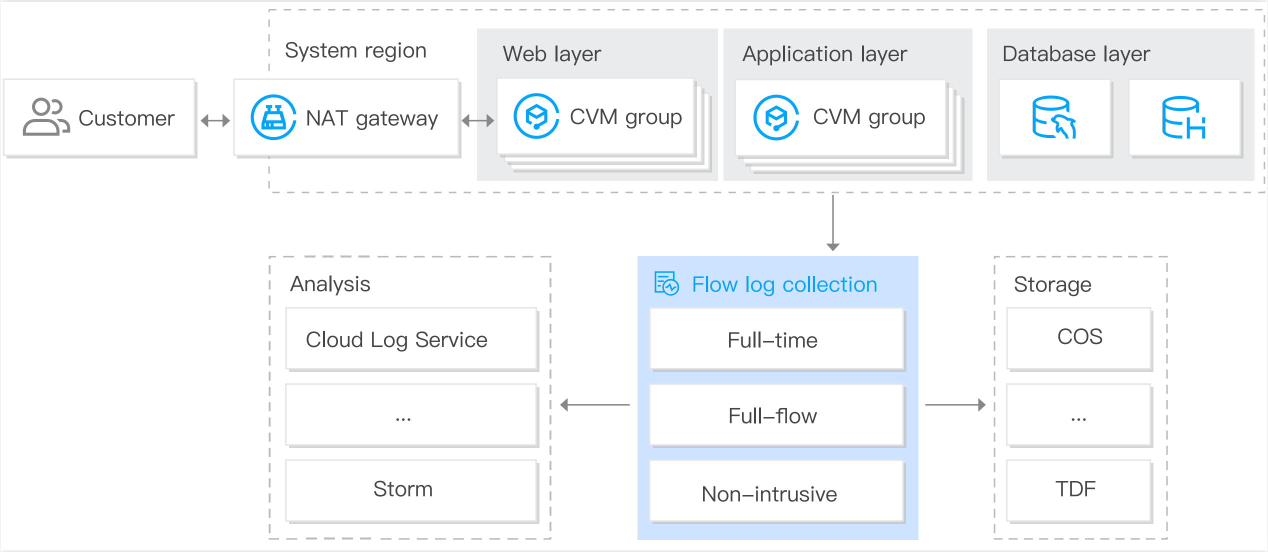
Pinpoint the CVM which is the root cause of the problem quickly, such as the CVM in a broadcasting storm or the CVM overusing bandwidth.

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 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.

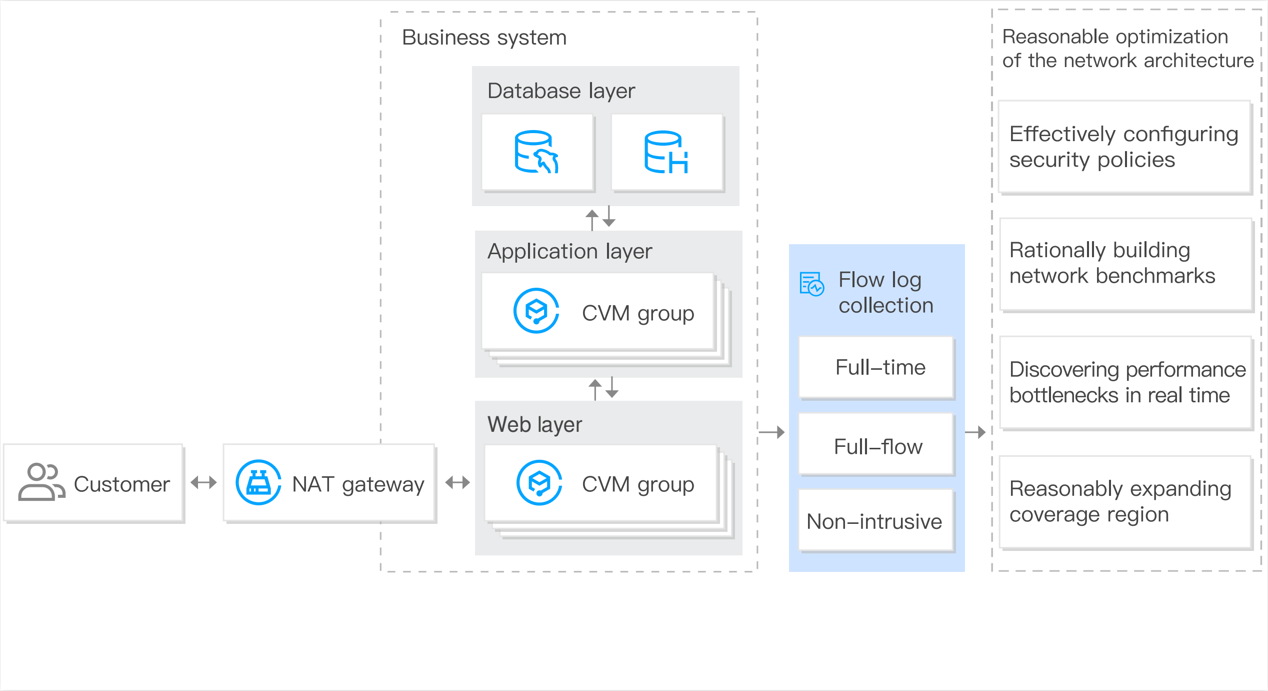
Analyze the regions of accessing users to expand coverage reasonably.

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 for analysis.


Business system
Database layer
Application layer
CVM group
Web layer
CVM group
Customer
NAT gateway
Flow log collection
Full–time
Full–flow
Non–intrusive
Reasonable optimization of the network architecture
Effectively configuring security policies
Rationally building network benchmarks
Discovering performance bottlenecks in real time
Reasonably expanding coverage region

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.

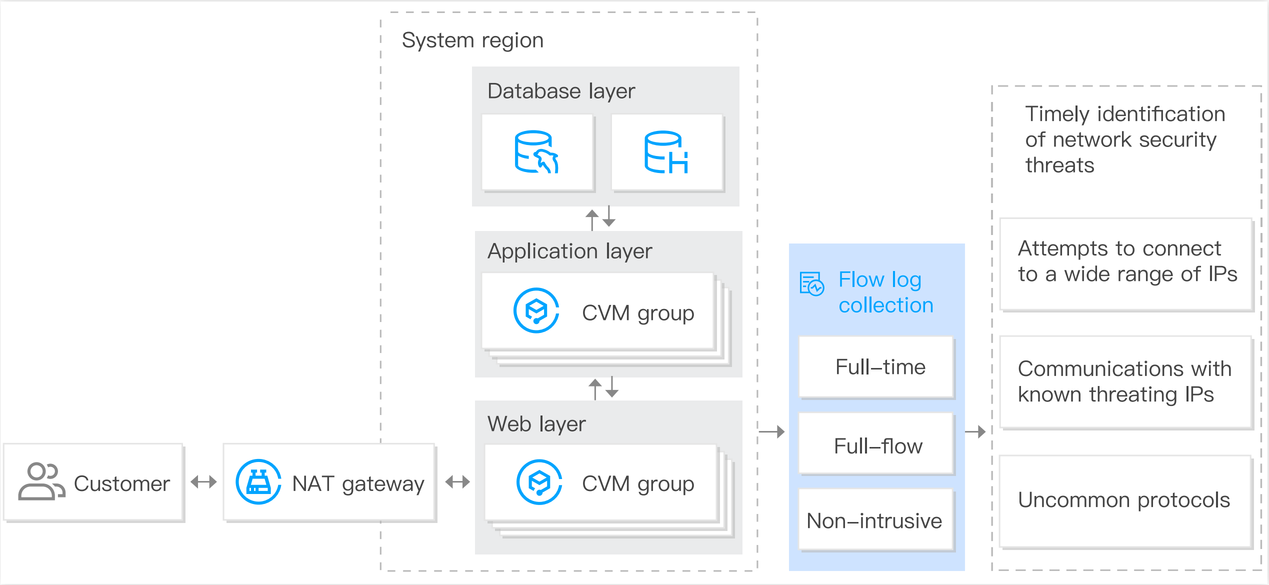
Communicate with an IP that is considered a known threat.

Identify an uncommonly used protocol.

Suggestions on Configuration:

Create flow logs to capture network traffic.

Deliver network logs to Cloud Log Service for query and analysis.


System region
Database layer
Application layer
CVM group
Web layer
CVM group
Customer
NAT gateway
Flow log collection
Full–time
Full–flow
Non–intrusive
Timely identification of network security threats
Attempts to connect to a wide range of IPs
Communications with known threating IPs
Uncommon protocols

Use Limits

Last updated：2024-01-10 16:10:45

Notes

Flow Logs (FL) supports the collection of flow logs of ENI, NAT Gateway, and cross-region CCN traffic only within the specified VPC range but not in the classic network.

Note:

The FL service for NAT Gateway and cross-region CCN traffic is currently in beta. To try it out, please submit a ticket.

The FL feature is available in all regions, but there are regional restrictions in the Cloud Log Service (CLS). Therefore, data in several regions may not be delivered to CLS. For more information, see Available Regions.

The configuration of a flow log cannot be modified after creation. For example, the 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.

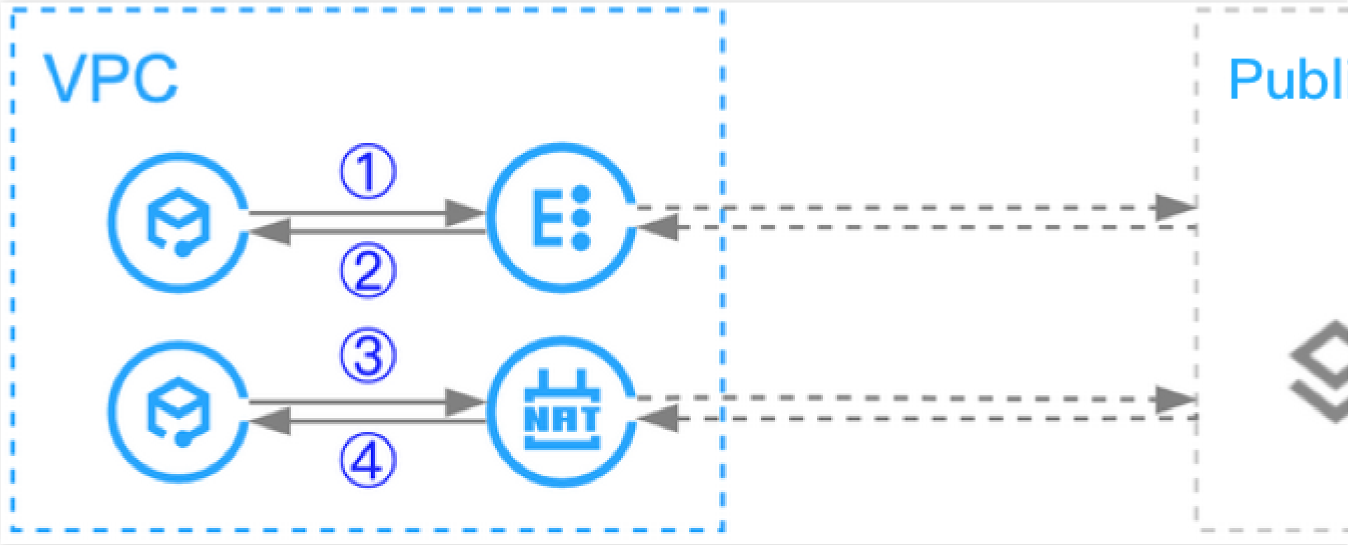
Only one flow log can be created for each ENI.

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.



Dashboard-Enabled Flow Log Types

Currently, advanced analysis dashboards can be created and viewed only for flow logs of the ENI type in the logset and log topic with the "Flowlog" flag.

Note:

In Topic Configuration, you can create the logset “flowlog_logset” and a log topic with the “Flowlog” flag.

Restricted Models

The Families and Models that support the FL feature: M6ce, M6p, SA3se, S4m, DA3, ITA3, I6t, I6, SA3, S5se, SA2, SK1, S4, S5, SN3ne, S3ne, S2ne, SA2a, S3ne, SW3a, SW3b, SW3ne, ITA3, IT5c, IT5, IT5c, IT3, I3, D3, DA2, D2, M6, MA2, M4, C6, IT3a, IT3b, IT3c, C4ne, CN3ne, C3ne, GI1, PNV4, GNV4v, GNV4, GT4, GI3X, GN7, and GN7vw.

The following models no longer support creating flow logs for data collection, and the existing flow logs on the models will not report data from July 25, 2022:

Standard: S3, SA1, S2, and S1

MEM optimized: M3, M2, and M1

Compute optimized: C4, CN3, C3, and C2

Batch compute: BC1 and BS1

High-performance computing cluster: HCCIC5 and HCCG5v

Relevant Products

Last updated：2024-01-10 16:10:45

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

Product	Relationship with Flow Logs
CVM	FL pinpoints the CVM which is the root cause of the problem quickly.
CLS	The flow logs can be published to CLS to meet the requirements of log auditing.
Security Group	Flow Logs quickly verifies whether the inaccessibility of a CVM is caused by the unreasonable settings for the security group.
Network ACL	FL quickly verifies whether the inaccessibility of a CVM is caused by the unreasonable settings for the ACL.
ENI	FL can collect and analyze the traffic data of ENI.
NAT Gateway	FL can collect and analyze the traffic data of NAT gateway.
CCN	FL can collect and analyze the cross-domain traffic data of CCN.