# Flow Logs

# Product Introduction

## Copyright Notice



## Trademark Notice



## Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

## Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

# Contents

# Product Introduction
# Overview

Last updated: 2025-03-28 18:11:12

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 Flow Logs with specified collection scopes (such as ENIs, NAT gateways, and cross-region traffic in Cloud Connect Networks) to collect incoming and outgoing traffic within that range. After creating flow logs, you can view and search for data in Tencent Cloud Log Service (CLS), as well as visualize log data in the advanced analysis dashboard.

> **Note**
> Currently, flow logs for NAT gateways and cross-region traffic in Cloud Connect Networks are in beta testing. If you are interested, please submit a ticket to request access.

# Strengths

Last updated: 2023-09-02 02:20:28

## No Performance Loss

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

## Secure service

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.

## Comprehensive and Continuous Traffic Monitoring

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.

## High Real-time Performance

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

## Effortless 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: 2023-09-04 14:54:15

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

Upon creating a Flow Log, the system automatically collects log flows within the specified scope (such as ENIs, NAT gateways, Direct Connect gateways, and cross-region traffic in Cloud Connect Network) and delivers the log data to Cloud Log Service (CLS). In CLS topics, each ENI has a unique log flow containing flow log records.

> **Note**
> Flow Logs for NAT gateways, cross-region traffic in Cloud Connect Network, and Direct Connect gateways are currently in beta testing. If you are interested, please submit a ticket.

## Flow Log Query

Flow Logs can be queried and consumed on the Cloud Log Service (CLS) platform. CLS supports billions of log data retrieval, allowing you to perform full-text search, multi-keyword search, cross-topic queries, and more, with results returned in seconds.

## Flow Log Storage

Flow Logs are deeply integrated with Cloud Log Service (CLS) to provide log data storage and management.

## Create a dashboard for multi-dimensional display of log data

In the dedicated logset "flowlog_logset", you can create dashboards for ENI-type flow logs, ultimately visualizing and analyzing flow log data through the dashboard. One log topic can create one dashboard.
The dashboard data display is shown in the following figure. For specific configurations, please refer to Advanced Analysis.

## Flow Log Records

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

## Flow Log records of CCN cross-region traffic

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 five-tuple consists of five elements: source IP address, source port, destination IP address, destination port, and transport layer protocol.
  - The source region refers to the region from which the cross-region traffic in Cloud Connect Network originates.
  - The destination region refers to the region where the Cloud Connect Network cross-region traffic arrives.
- **Capture Window**
  A continuous duration during which Cloud Log Service aggregates data before publishing flow log records. The capture window is approximately 1 minute, and the push time is about 5 minutes. Flow log records are space-separated strings in the following format, with no fixed field order:
  `version region-id ccn-id srcaddr dstaddr srcport dstport protocol srcregionid dstregionid packets bytes start end action log-status`

| Parameter | Data Type | Note |
| --- | --- | --- |
| version | text | Flow Log Version. |
| region-id | text | The region where logs are recorded. |
| ccn-id | text | For the unique identifier of the Cloud Connect Network, please contact us to confirm the CCN information. |
| srcaddr | text | Source IP Address. |
| dstaddr | text | Target IP. |
| srcport | text | Source port of the traffic. This field is only applicable to UDP/TCP protocols. For other protocols, this field will display as "-". |

| | | |
|---|---|---|
| dstport | long | Destination port of the traffic. This field is only applicable to UDP/TCP protocols. For other protocols, this field will display as "-". |
| protocol | long | The IANA protocol number for the traffic. For more information, refer to the assigned Internet Protocol numbers. |
| srcregionid | text | Traffic Source Region. |
| dstregionid | text | Traffic Destination Region. |
| packets | long | Number of data packets transmitted within the capture window. This field is displayed as "-" when the "log-status" is "NODATA". |
| bytes | long | The number of bytes transmitted within the capture window. When the "log-status" is "NODATA", this field is displayed as "-". |
| start | long | The timestamp of receiving the first packet in the current capture window, in Unix seconds format. If no packets are received within the capture window, the start time of the capture window is displayed. |
| end | long | The timestamp of the last packet received in the current capture window, in Unix seconds format. If no packets are received within the capture window, it displays the end time of the capture window. |
| action | text | Operations associated with traffic:<br>• ACCEPT: Cross-region traffic that is successfully forwarded through Cloud Connect Network.<br>• REJECT: Cross-region traffic that is blocked due to rate limiting. |
| log-status | text | Flow Log record status:<br>• OK: Indicates that the data has been successfully recorded to the specified target.<br>• NODATA: Indicates that there is no inbound or outbound network traffic in the capture window. In this case, the "packets" and "bytes" fields will display as "-1". |

### Other types of Flow Log records

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

- **Five-tuple**
  A set consisting of five elements: source IP address, source port, destination IP address, destination port, and transport layer protocol.
- **Capture Window**
  A continuous duration during which Cloud Log Service aggregates data before publishing flow log records. The capture window is approximately 5 minutes, and the data push time is about 5 minutes. Flow log records are space-separated strings in the following format, with no fixed field order:
  `version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status`

| Parameter | Note |
| --- | --- |
| version | Flow Log Version. |
| account-id | Account AppID for Flow Logs. |
| interface-id | ENI ID. |
| srcaddr | Source IP Address. |
| dstaddr | Target IP. |
| srcport | Source port of the traffic. When the traffic is using ICMP protocol, this field represents the ICMP ID. |
| dstport | The destination port of the traffic. For ICMP protocol traffic, this field represents the combination of ICMP type (upper 8 bits) and code (lower 8 bits). |
| protocol | The IANA protocol number for the traffic. For more information, refer to the assigned Internet Protocol numbers. |

| | |
|---|---|
| packets | Number of data packets transmitted within the capture window. |
| bytes | Capture the number of bytes transmitted within the window. |
| start | Capture window start time, using Unix seconds format. |
| end | Capture window end time, using Unix seconds format. |
| action | Operations associated with traffic:<br>• ACCEPT: Traffic allowed by security groups or network ACLs.<br>• REJECT: Traffic not permitted by security groups or network ACLs in the log records. |
| log-status | Flow Log record status:<br>• OK: Indicates that the data has been successfully recorded to the specified target.<br>• NODATA: Indicates that there is no inbound or outbound network traffic in the capture window. In this case, the "packets" and "bytes" fields will display as "-1".<br>• SKIPDATA: Indicates that some flow log records were skipped in the capture window. This may be due to internal capacity constraints or internal errors. |

## Sample

- If you allow SSH traffic (destination port 22, TCP protocol) to the ENI eni-lq6mkcis in account 1251762227, the flow log record would be as follows:

```
srcaddr:192.63.197.94 dstport:22 account-id:1251762227
start:1655104384 dstaddr:10.0.3.4 version:0001_0001 packets:2
protocol:6 bytes:108 action:ACCEPT srcport:58188 end:1655104384
log-status:OK interface-id:eni-lq6mkcis
```

- If you reject RDP traffic (target port 3389, TCP protocol) for the ENI eni-lq6mkcis in account 1251762227, the flow log record would be as follows:

```
srcaddr:192.63.197.94 dstport:3389 account-id:1251762227
start:1655104384 dstaddr:10.0.3.4 version:0001_0001 packets:2
protocol:6 bytes:108 action:REJECT srcport:58188 end:1655104384
log-status:OK interface-id:eni-lq6mkcis
```

- Flow Log Records for Security Group and Network ACL Rules
  - Security groups are stateful, allowing all traffic to respond accordingly.
  - Network ACLs are stateless, so traffic responses must adhere to the network ACL rules.

  For example, you use the `ping` command from your home computer (IP address `203.0.113.12`) to your instance (private IP address of the network interface `172.31.16.139`). Your security group inbound rules allow ICMP traffic, and outbound rules do not allow ICMP traffic. However, since security groups are stateful, they permit ping responses from your instance.
  Your network ACL allows inbound ICMP traffic but does not allow outbound ICMP traffic. Since network ACLs are stateless, the ping response is dropped and not transmitted to your home computer. In the Flow Logs, this is displayed as two flow log records:
  - Network ACL and Security Group both allow (thus reachable to your instance) ACCEPT records for initiating ping requests.
  - Network ACL rejects the response ping with a REJECT record.

```
srcaddr:203.0.113.12 dstport:0 account-id:1251762227
start:1432917027 dstaddr:172.31.16.139 version:0001_0001 packets:4
protocol:1 bytes:336 action:ACCEPT srcport:0 end:1432917142 log-
status:OK interface-id:eni-lq6mkcis
```

```
srcaddr:172.31.16.139 dstport:0 account-id:1251762227
start:1432917094 dstaddr:203.0.113.12 version:0001_0001 packets:4
protocol:1 bytes:336 action:REJECT srcport:0 end:1432917142 log-
status:OK interface-id:eni-lq6mkcis
```

  If your Network ACL allows outbound ICMP traffic, the Flow Log will display two ACCEPT records (one for initiating the ping and one for responding to the ping). If your security group denies inbound ICMP traffic, the Flow Log will display a REJECT record, as the traffic does not reach your instance.

# Scenarios

Last updated: 2023-09-02 02:23:23

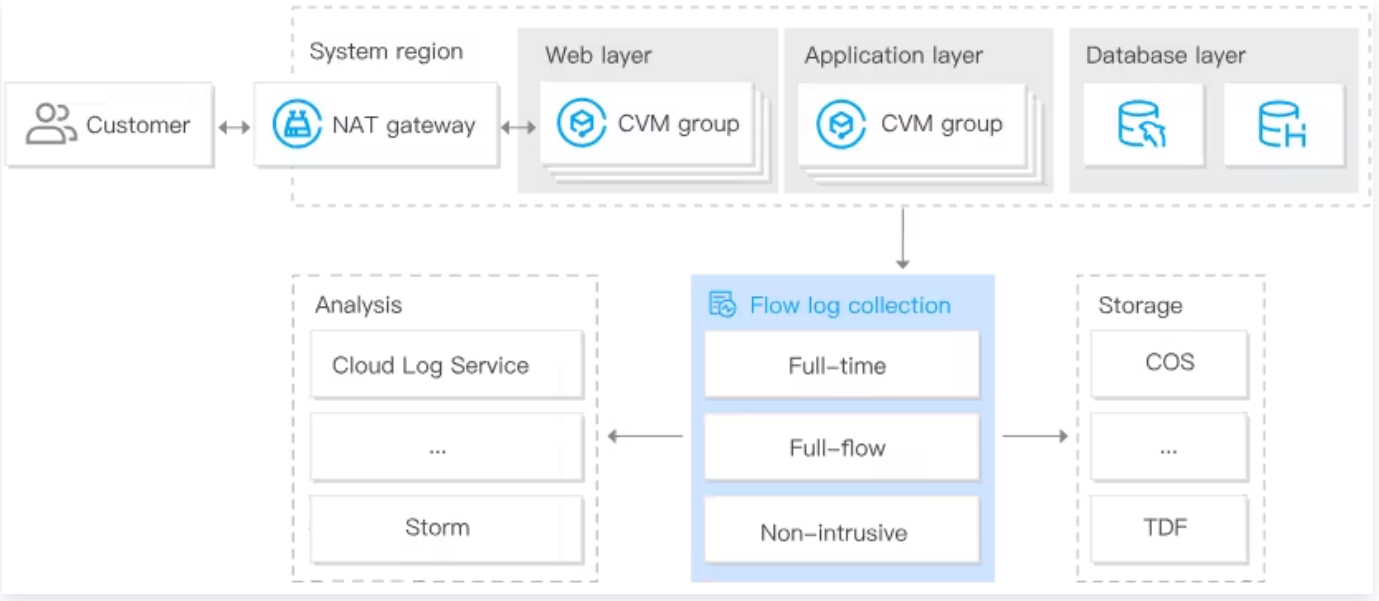
## Rapid Identification of Network Issues

Network quality is the cornerstone of business stability. Flow logs help preserve the fault scene, enabling you to quickly identify network issues, perform network traceback and forensics, and reduce network downtime. Key features include:

- Swiftly pinpoint the root cause of issues in Cloud Virtual Machines, such as broadcast storms or excessive bandwidth usage by Cloud Virtual Machines.
- Quickly determine if the inaccessibility of a Cloud Virtual Machine is due to improper security group or ACL configurations.

### Configuration Suggestions:

- Create a flow log to collect network interface card (NIC) traffic.
- Deliver network logs to Cloud Log Service for query and analysis.




## Rationally optimize network architecture

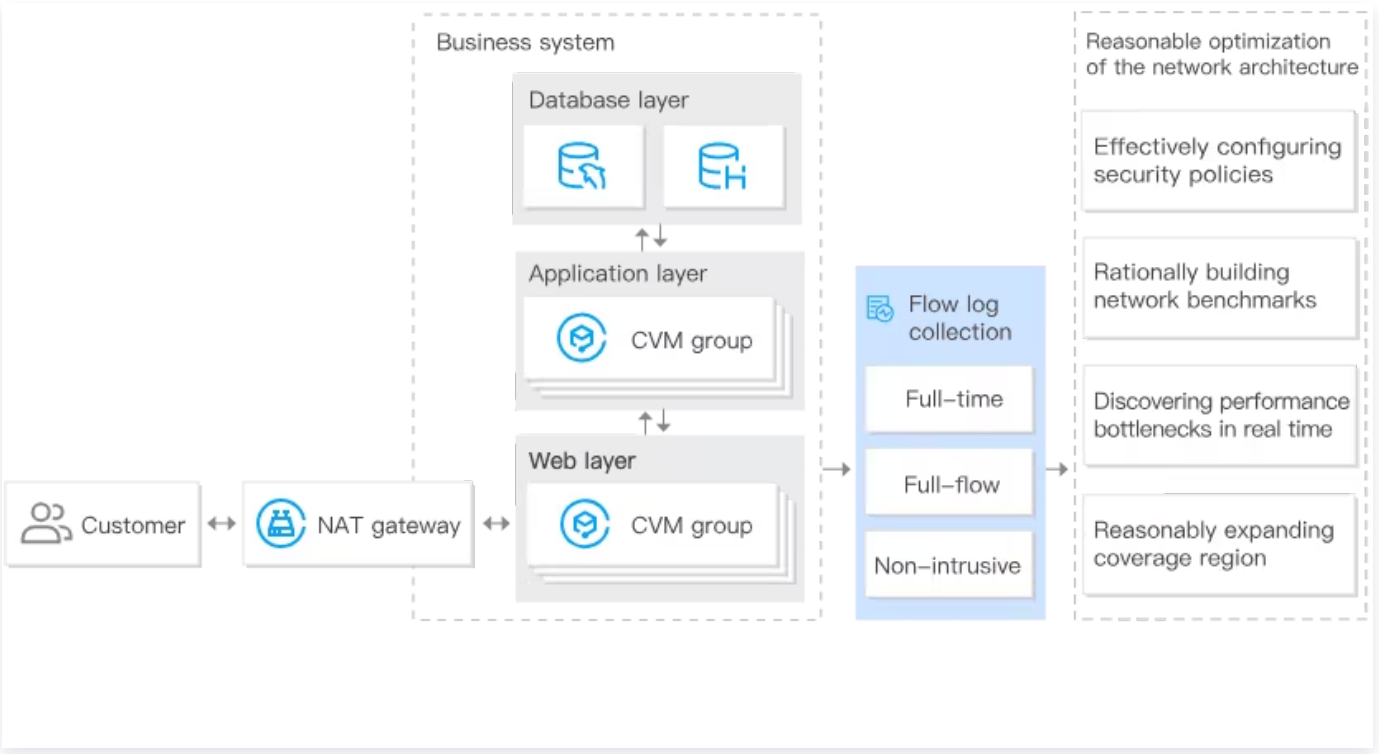
Flow logs can collect full-time, full-flow traffic from Elastic Network Interfaces (ENIs) across the entire network. By leveraging Big Data and visualization, flow logs empower you to enhance data-driven network operations capabilities and optimize network architecture rationally. Key features include:

- Analyze historical network data to establish a baseline for business network performance.
- Timely detect performance bottlenecks and make informed decisions on capacity expansion or traffic degradation.

- Analyze user access regions and strategically expand coverage areas.
- Analyze network traffic to optimize network security policies.

**Configuration Recommendations:**

- Create a flow log to collect network interface card (NIC) traffic.
- Deliver network logs to Cloud Log Service for query and analysis.



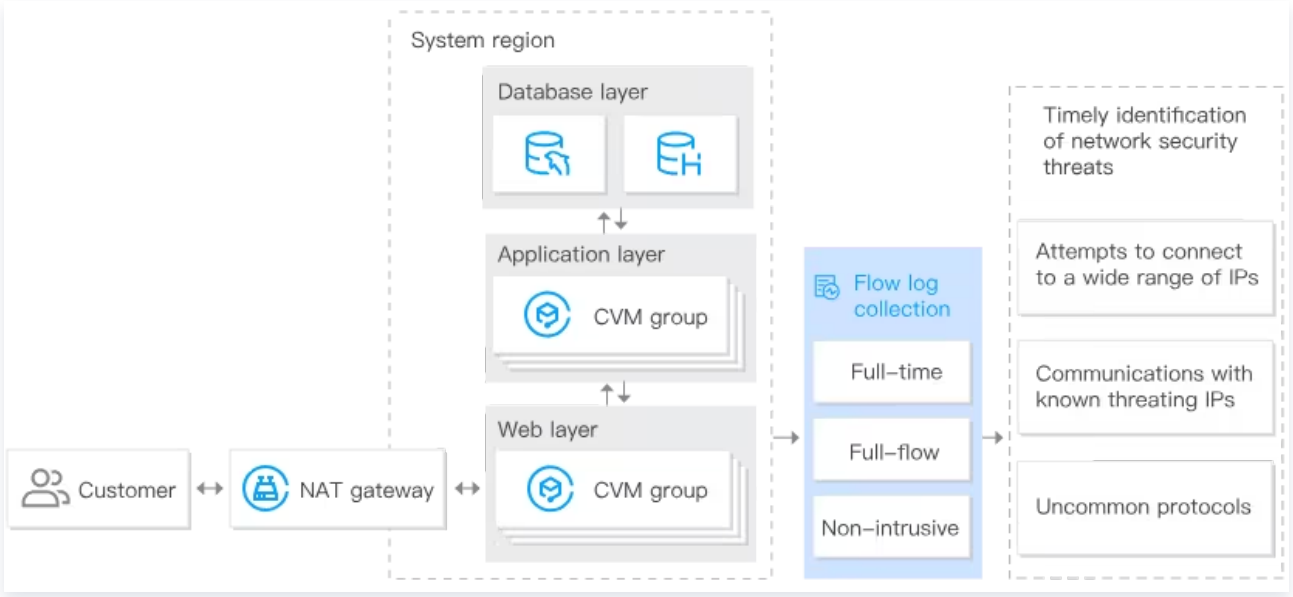

## Promptly Detect Network Security Threats

Traditional traffic inspection points can cause a decline in Cloud Virtual Machine performance. Flow logs adopt a full-time, full-flow, and non-intrusive collection method, helping you promptly detect network security threats without impacting Cloud Virtual Machine performance, thereby enhancing system security. Key features include:

- Attempting to connect to a wide range of IP addresses.
- Communicating with known threat IPs.
- Identify infrequently used protocols.

**Configuration Recommendations:**

- Create flow logs to collect network traffic.
- Deliver network logs to Cloud Log Service for query and analysis.



# Limits

Last updated: 2023-09-02 02:25:24

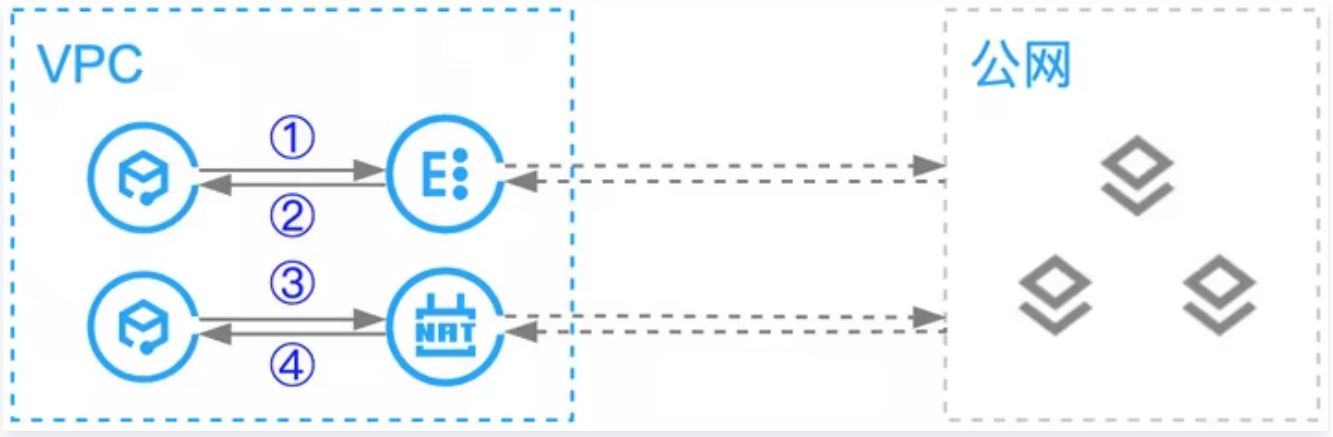
## Supports and Limits

- Network flow logs only support the collection of flow logs within the VPC range for ENI, NAT gateway, and cross-region CCN traffic, and do not support the collection of flow logs within the basic network range.

  > **Note**
  > Currently, the flow logs for NAT Gateway, cross-region CCN traffic, and Direct Connect Gateway are in beta testing. If needed, please submit a ticket.

- Flow log functionality is supported in all regions, but there are regional restrictions on the CLS side, which may prevent data from being delivered to CLS in some regions. For more information, please refer to the CLS available regions.
- Once a flow log is created, you cannot modify its configuration (such as changing the Cloud Log Service to which the flow log is delivered).
- IP traffic types not supported by flow logs:
  - Traffic generated by Windows instances for Windows license activation.
  - DHCP traffic.
- Only one flow log can be created for each Elastic Network Interface (ENI).
- When collecting network flow logs for the traffic on the Elastic Network Interface (ENI) of a Cloud Virtual Machine (CVM), the outbound traffic is collected before rate limiting, while the inbound traffic is collected after rate limiting.
  For example, when creating a network flow log for the ENI of a CVM:
  - When a Cloud Virtual Machine accesses the public network through Cloud Load Balance, the outbound traffic is collected at arrow 1, and the inbound traffic is collected at arrow 2.
  - When a Cloud Virtual Machine accesses the public network through a NAT gateway, the outbound traffic is collected at arrow 3, and the inbound traffic is collected at arrow

4.




## Flow log types with dashboard support

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 a logset "flowlog_logset" and log topics marked with "Flowlog".

## Model Restrictions

- Cloud Virtual Machine instance types that support flow log collection include: M6ce, M6p, SA3se, S4m, DA3, ITA3, I6t, I6, 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 will no longer support creating new flow logs for data collection, and existing flow logs will cease data reporting starting from July 25, 2022:
  - Standard: S3, SA1, S2, and S1
  - Memory-optimized: M3, M2, and M1
  - Compute: C4, CN3, C3, and C2
  - Batch Compute Models: BC1 and BS1
  - High-performance Compute Clusters: HCCIC5, HCCG5v

## Direct Connect Gateway Flow Log Regional Restrictions

Direct Connect Gateway Flow Logs are currently only supported in the following regions: Beijing, Shanghai, Guangzhou, Shenzhen, Nanjing, Hong Kong, Singapore, and Shanghai Finance.

# Relevant Products

Last updated: 2026-04-28 17:53:00

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

| Product name | Relationship with Flow Logs |
| --- | --- |
| Cloud Virtual Machine | Flow Logs can quickly pinpoint the root cause of issues in Cloud Virtual Machines |
| CLS Log Service | Flow Logs can be shipped to CLS Cloud Log Service, meeting log audit requirements |
| Security Group | Flow Logs can swiftly determine if the inaccessibility of Cloud Virtual Machines is due to improper security group configurations |
| Network ACL | Flow Logs can swiftly detect if the reason for Cloud Virtual Machine inaccessibility is due to improper network ACL settings |
| ENI | Flow Logs can collect and analyze traffic data at the granularity of Elastic Network Interfaces (ENI) |
| NAT Gateway | Flow Logs can collect and analyze traffic data at the granularity of NAT Gateways |
| Cloud Connect Network | Flow Logs can collect and analyze cross-domain traffic data at the granularity of Cloud Connect Network |