Flow Logs
Operation Guide

Contents

Operation Guide
Operation Overview

Last updated: 2023-09-02 02:31:18

While using Flow Logs, you may encounter issues such as creating and deleting flow logs, creating log sets and log topics, viewing flow log records, topic configuration, and advanced analysis. This article provides an overview of common operations for using Flow Logs and related products for your reference.

Common Operations

- Authorize Flow Log Access to CLS
- Create Logset and Log Topic
- Create Flow Log
- Modify Flow Log
- View Flow Log Records
- Delete Flow Log
- Topic Configuration
- Advanced Analysis Dashboard

Authorizing FL to Access CLS

Last updated: 2023-09-02 02:31:41

The Flow Log feature requires reporting collected log data to Cloud Log Service (CLS), so it is necessary to grant Flow Log read and write permissions to access CLS; otherwise, log data cannot be queried in CLS. This guide will help you configure the resource access permissions for Flow Log to access CLS.

Instructions

1. Log in to the Cloud Access Management console.
2. Click **Roles** to enter the Role Management interface.
3. Click **Create Role** and select the role carrier as **Tencent Cloud Account**.
4. In the **Enter Role Carrier Information** interface, select **Other Primary Account** and enter the Flow Log public account **91000000202**, then click **Next**.
5. In the **Configure Role Policy** interface, enter **Cloud Log Service** for search, select **QcloudCLSFullAccess** to grant Flow Log public account read and write access to CLS, and click **Next**.
6. In the **Review** interface, enter the role name "FlowLogClsRole".
7. Click **Complete**, the role is successfully created and authorized as shown in the following image.

Creating Logsets and Log Topics

Last updated: 2023-09-02 02:34:27

You need to create logsets and log topics to store and view the flow logs.

- Logset: Specifies the storage collection for flow logs within Cloud Log Service.
- Log Topic: Specifies the smallest dimension for log storage, used to distinguish different types of logs, such as Accept logs, etc.

> **Note**
> This document describes how to create logsets and log topics that are not marked with `Flowlog`. These logsets and log topics cannot be used to create and use the advanced analysis dashboards.

Instructions

1. Log in to the Cloud Log Service Console, click **Log Topics** in the left sidebar to access the log topic management page.
2. At the top of the page, select the appropriate region and click **Create Log Topic**.
3. In the pop-up **Create Log Topic** window, enter the log topic name, partition count, and other information, then click **Confirm**.
   - Log Topic Name: For example, nginx.
   - Storage types: By default, STANDARD storage is used. For more information on storage types, see Storage Class Overview.
   - The log retention period is set to 30 days by default, and can be selected from a range of 1 to 3,600 days.
   - Logset Operations:
     - Select an existing logset: Choose the target logset from the drop-down menu. The log retention period will be the same as the logset retention period.
     - Create Logset: Logset Name, for example, cls_test.
   - Partition Count: By default, one partition is created. For more information on topic partitions, please refer to Topic Partition Introduction.
   - Partition Auto-Split: Enabled by default.
   - Maximum number of partitions: You can customize the number of partitions, with a maximum limit of 50 partitions.

> **Note**
> - After the auto-split feature is enabled, the partition will be automatically split

up to 50 partitions based on the actual write capacity when the write requests or write traffic of the partition always exceed the capability.

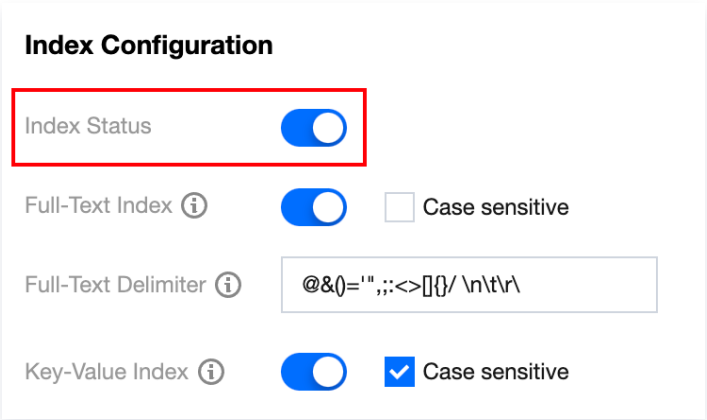
- If the number of partitions in a log topic reaches the maximum value set, Cloud Log Service will no longer trigger auto-splitting, and the excess portion will be rejected, returning a request limit exceeded error code.

4. In the details page of the created log topic, select the **Index Configuration** tab and click **Edit** in the upper right corner.

5. Enable indexing and click **Confirm** to view and search flow logs.

Note

- You do not need to install agents or be concerned about the server group status.
- If you have no need to import flow logs into services like COS, you don't need to worry about log shipping tasks.



Managing Logs
Create flow logs

Last updated: 2023-09-02 02:39:23

This document describes how to create a flow log policy to collect flow logs of ENIs, NAT gateway and CCN cross-region connections.

> **Note**
> NAT Gateway and CCN cross-region traffic logs are currently in beta testing. To use them, please submit a ticket.

Preparations

- Since flow log data is written to Cloud Log Service (CLS), ensure that you have completed the authorization for CLS to view log data. For more information, please refer to Authorizing Flow Logs to Access CLS.
- A logset and log topic have been created:
  - To use the advanced analysis dashboard feature, you must select the "flowlog_logset" logset marked with "Flowlog" and its corresponding log topics. Please refer to the Topic Configuration page for creation in advance.
  - If you do not intend to use the advanced analysis dashboard feature, you can choose any log set and log topic. You can create a log set and log topic without the "Flowlog" identifier in the CLS console, or you can create a log set and log topic with the "Flowlog" identifier on the **Topic Configuration** page in the flow log console.

Instructions

Creates a flow log

1. Log in to the Virtual Private Cloud console and select **Flow Logs** > **Log List** in the left sidebar.
2. On the **Flow Logs** page, select a region in the top-left corner, then click **+Create**. In the **Create Flow Log** dialog box, configure the following parameters:

Parameter	Description
Name	The name of the flow log.

Collection range	This specifies the collection range of the flow log. ENI, NAT gateway and CCN are supported.
VPCs	Collect flow logs for all Virtual Private Clouds.
Subnets	The subnet where the flow logs are collected.
Collection type	Select the type of traffic to be collected by the flow log: all traffic, or the traffic rejected or accepted by security groups or ACL.
Logset	This specifies the storage location in CLS for the flow log.
Log Topic	This specifies the minimum dimension of log storage, which is used to distinguish log types, such as “Accept” log.
Tag Key	(Optional) It is used for locating and managing flow logs. You can create a tag key or select an existing one.
Tag Value	(Optional) You can create a tag value, select an existing one, or just leave it empty.

3. Click **OK**.

> **Note**
> - Upon creating a flow log for the first time, you need to wait for several minutes (e.g., five minutes for the capture window and five minutes for data publishing for ENI flow logs) before you can view the flow log in Cloud Log Service.
> - Flow logs are currently free of charge, but data storage in Cloud Log Service is subject to standard fees for Cloud Log Service.

Viewing log information

1. After creating a flow log for about 10 minutes, click **View** on the right side of the target flow log, and the system will redirect you to the **Search Analysis** interface of Cloud Log Service.
2. On the **Search and Analysis** interface, you can select the region, logset, log topic, time, or customize filter conditions. Click **Search and Analysis** to quickly query log information under specified conditions.

> **Note**
> Click **Index Configuration** and ensure that the **Index Status** is set to **Enabled**, as log data collected when indexing is disabled cannot be searched.

Modify flow log

Last updated: 2023-09-02 02:47:27

After creation, the flow log only supports modification of the log name and tags.

Modify flow log name

1. Log in to the Virtual Private Cloud console and select **Flow Logs** > **Log List** in the left sidebar.
2. Click the edit icon next to the name, enter the new name, and click **Save** to confirm.

Modify flow log tags

Configuring tags for flow logs enables quick search and management of the logs.

1. Log in to the Virtual Private Cloud console and select **Flow Logs** > **Log List** in the left sidebar.
2. Click **Edit Tags** on the right side of the flow log you want to modify.
3. In the pop-up "**Edit Tags**" dialog box, you can **add** or **delete** tag resources. If no suitable tags are available, click **Tag Management** to create a new one.
4. Click **OK** to complete the tag modification.

Viewing Flow Log Records

Last updated: 2023-09-02 02:50:15

You can view flow logs in Cloud Log Service to quickly pinpoint business issues. You can select multiple log topics within the same log set for cross-topic queries. For specific operations, please refer to Log Retrieval.

Note

- For flow log field descriptions, see Flow Log Record.
- As flow log data needs to be written to Cloud Log Service (CLS), ensure that you have granted the necessary permissions for flow logs to access CLS; otherwise, you will not be able to query log data in CLS. For more information, see Authorizing Flow Logs to Access CLS.

Delete Flow Logs

Last updated: 2023-09-02 02:53:07

If you no longer require Flow Logs to collect traffic records, you can delete them. Upon deletion, the collection of Flow Logs will cease, but the stored log data will not be removed.

Instructions

1. Log in to the Virtual Private Cloud console and select **Flow Logs** > **Log List** in the left sidebar.
2. Select the Flow Log you wish to delete, click **Delete**, and then click **Confirm** to complete the operation.

Advanced Analysis Dashboard

Last updated: 2023-09-02 02:58:36

Advanced analytics provides a clear and intuitive display of log records through dashboards, enabling quick and efficient business issue identification and improved operational efficiency. You can create and view dashboard analysis data for Elastic Network Interface flow logs under the "flowlog_logset" logset.

Preparations

Ensure that the logset **flowlog_logset** and its log topics have been created in the theme configuration. After creating a log topic in **Theme Configuration**, the system will automatically create a corresponding dashboard for the log topic. Dashboard data can be directly viewed in the advanced analytics interface View Dashboard Data.

View Dashboard Data

1. Log in to the Virtual Private Cloud console, and select **Flow Logs** > **Advanced Analytics** in the left sidebar.
2. Select the region, log topic and query period. The log record based on the specified conditions will be displayed.

Creating a Dashboard

If the dashboard has been deleted in CLS, or the system failed to create the dashboard, you can refer to this section to recreate the dashboard.

1. Log in to the Virtual Private Cloud console, and select **Flow Logs** > **Advanced Analytics** in the left sidebar.
2. Navigate to the **Access Log Dashboard** interface, select the region and log topic, then click **Create**.