Cloud Log Service

Getting Started

Product Documentation

Contents

Getting Started
Getting Started Guide

Last updated：2024-01-20 16:38:07

Overview

Cloud Log Service (CLS) provides a one-stop log data solution. You can quickly and conveniently connect to it in five minutes to enjoy a full range of stable and reliable services from log collection, storage, and processing to search, analysis, consumption, shipping, dashboard generation, and alarming, with no need to care about resource issues such as scaling. It helps you improve the problem locating and metric monitoring efficiency in an all-around manner, making log Ops much easier.
This document describes how to use basic CLS features:
Collect log files from servers with LogListener
Search for and analyze logs
If you don't have proper resources to collect logs, you can use demos to quickly try out CLS's log search and analysis, dashboard, and alarming features free of charge without collecting logs.

Step 1. Activate the service

Log in to the Tencent Cloud CLS console. If CLS is not activated for your account, you will be prompted for activation. Just click **Activate**.

Step 2. Install LogListener

LogListener collects log files to CLS. The following describes how to install it in a Tencent Cloud CVM/Lighthouse instance.
LogListener also supports non-Tencent Cloud servers, TKE, and self-built K8s clusters.

Step 2.1. Get the key

Go to the CAM console, view/create and record the key, and make sure that the key is enabled.

Step 2.2. Install LogListener

1. On the Machine Group Management page, switch to the target CVM/LightHouse region in the top-left corner and click **Deploy Instances** in the top-right corner.

2. Select the target instance, enter the `SecretId` and `SecretKey` obtained in step 2.1 in **Enter a SecretId**, and enter **Machine label** (such as `test`, which is similar to an instance category for subsequent batch log collection from multiple machines).
3. After the installation is completed, click **Next**.
4. Add the instance with LogListener installed to a new machine group that requires log collection. Log files under the same path can be batch collected for instances in the same group. Enter the **Machine Group Name** and click **Join**.

Step 3. Create a log topic

A log topic is the basic unit for log data collection, storage, search, and analysis. It usually corresponds to a certain application/service (with a similar log structure). Log topics can be grouped by logset. A logset doesn't store any log data and is only used to facilitate log topic management.
1. On the Log Topic page, switch to the region in step 2.2 in the top-left corner and click **Create Log Topic**.
2. In the pop-up window, enter information and click **OK**.
Log Topic Name: `test` for example
Storage Class: STANDARD
Logset Operation: **Create Logset**
Logset Name: `test` for example

Step 4. Configure collection rules and indexes

1. On the Log Topic page, click the **Log Topic Name/ID** in step 3.
2. Select the **Collection Configuration** tab and click **Add** in the **LogListener Collection Configuration** area.
3. On the **Log Data Source** page, select ** Logs with Full Text in a Single Line**.
Note:
If you select **Logs with Full Text in a Single Line**, raw logs will be directly reported to CLS, and log fields won't be segmented or extracted. This is a simple way of extraction suitable for getting started with CLS, but it may prevent you from using features such as log search and analysis (for example, log search by field or statistical log analysis). In actual use, we recommend you select a proper log format to segment and extract log fields as instructed in Collection Overview.
For JSON logs, you can select **JSON Log File**.
4. Select the machine group created in step 2.2 and click **Next**.
5. Enter the **Collection Rule Name** and **Collection Path** (i.e., the path of the target log file) and click **Next**.
For example, if the absolute path of the target file is `/root/test.log`, then the **Directory Prefix** for **Collection Path** should be `/root`, and the file name should be `test.log`.
6. Set the index configuration and enable full-text index.

Note:

If **Extraction Mode** is not **Full text in a single line**, you can enable **Key-Value Index** and click **Auto Configure** to automatically configure the key-value index for the collected logs.

The modified index configuration takes effect only for newly written logs. Existing data won't be updated.

For more information on index configuration items, see Configuring Index.

Step 5. Search for and analyze logs

1. On the Search and Analysis page, select the log topic created in step 3 at the top to view the collected log data.
2. In the input box at the top, enter the target text as the search condition and click **Search and Analysis** to search for logs matching the condition.
3. Use the pipe symbol and SQL for statistical analysis of the found raw data.

For example, calculate the distribution of log sources.

Note:

For more information on the search and analysis syntax, see Overview and Syntax Rules.

`__SOURCE__` is a system preset field indicating the source IP of a log. After structuring a log and enabling statistics in **Key-Value Index** for log fields, you can perform statistical analysis on log fields, such as log count by URL.

Additional Information

Concepts: This document describes the basic concepts of CLS, including log topic, logset, index, and segment.

Collecting and Searching NGINX Access Logs: This document describes how to collect NGINX logs and use regex to segment and extract log fields.

Migrating Local Logs Searched by the grep Command to CLS: This document describes how to convert the grep command to the CLS search syntax to quickly understand CLS syntax rules.

Tencent Cloud Service Log Access: CLS has integrated some commonly used Tencent Cloud products to easily collect their logs.

Creating Processing Task: The data processing feature provides the capabilities to filter, cleanse, mask, enrich, and distribute raw logs.

Monitoring Alarm Overview: An alarm policy can be set for logs, for example, triggering an alarm when the number of error logs exceeds 10 within one minute.

Quickly Trying out CLS with Demo

Last updated：2024-05-21 16:43:33

Overview

If you want to quickly understand the various features of CLS but don't have the resources to try out the features, you can use the demos provided by CLS.

Note:

Demos are free of traffic and storage fees.

Demo Log	Description	Available Pre-built Dashboards
CLB	Contains the demo for CLB access logs and provides search, dashboard, and alarm template features	CLB access log dashboard
NGINX	Contains the demo for NGINX Ingress access logs and provides search, dashboard, and alarm template features	Nginx access dashboard Nginx monitoring dashboard
TKE	Contains the demo for TKE audit and event logs and provides search, dashboard, and alarm template features	TKE audit log_overview dashboard TKE audit log_node operation overview dashboard TKE audit log_K8S object operation overview dashboard TKE audit log_aggregated search dashboard TKE event log_overview dashboard TKE event log_aggregated search dashboard for exception events
CDN	Contains the demo for CDN Ingress access logs and provides search, dashboard, and alarm templates	CDN access log_quality monitoring analysis dashboard CDN access log_user action analysis dashboard
Flowlog	Contains the demo for ENI and CCN flow logs and provides search, dashboard, and alarm template features	ENI flow log_advanced analysis dashboard CCN flow log_advanced analysis dashboard
COS	Contains the demo for COS access logs and provides search, dashboard, and alarm template	COS access log analysis dashboard

	features	
WAF	Includes WAF access logs, providing search, dashboard, and alarm template features	WAF access log_access traffic analysis dashboard
CloudAudit	Includes CloudAudit logs, providing search, dashboard, and alert template features	CloudAudit audit log_event analysis dashboard
API Gateway	Includes API Gateway access logs, providing search, dashboard, and alert template features	API Gateway access log_API quality analysis dashboard

Using the Demo Log

Enabling the demo log

1. Log in to the CLS console.
2. In **Demo log Center** on the **Overview** page, find the target demo and click **Enable Demo**.
3. In the pop-up window, click **Confirm**.Resource initialization takes about 2 minutes.
4. After initialization, you can perform the following operations:

Click **Demo** > **Go to Search and Analysis** to view search and analysis details.

Click **Demo** > **View Dashboard** to view preset dashboards.

Click **Demo** > **View Alarm** to view monitoring alarm details.

Click **Demo** > **View Log Topic** to view log topic details.

Resetting the demo log

1. Log in to the CLS console.
2. In **Demo Log Center** on the **Overview** page, find the target demo and click **Demo** > **Reset Resources**. When a demo expires, you can enable it again by resetting it.

Disabling the demo log

1. Log in to the CLS console.
2. In **Demo Log Center** on the **Overview** page, find the target demo and click **Demo** > **Delete Resources**.
3. In the pop-up window, click **Confirm**. Demo log writing stops, and demo resources are deleted.