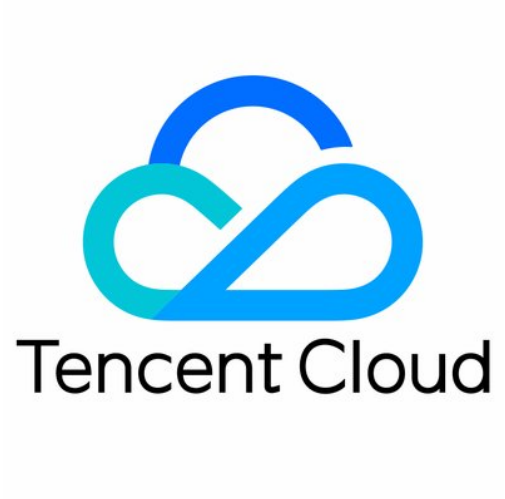
Cloud Load Balancer

Log Management

Product Documentation



Contents

Log Management
Access Log Overview

Last updated : 2020-10-26 16:14:09

CLB supports configuring access logs to collect and record the details of each client request, such as the request time, request path, client IP and port, return code, and response time. This feature can help you better understand client requests, troubleshoot issues, and analyze user behaviors.

Note :

- Only Layer-7 CLB supports configuring access logs.
- This feature is only available in regions listed below.

Storage Methods

- CLB access logs can be stored in Cloud Log Service (CLS): CLS is a one-stop log service platform that provides a variety of log services including log collection, storage, search, analysis, real-time export, and shipping. It assists you in implementing business operations, security monitoring, log audit, and log analysis.

Item	Storing Access Logs in CLS
Time granularity for log obtainment	Minute
Online search	Supported
Search syntax	Full-text search, key-value search, fuzzy keyword search, etc. For more information, please see Legacy CLS Search Syntax.
Supported regions	Guangzhou, Shanghai, Nanjing, Beijing, Chongqing, Chengdu, Hong Kong (China), Singapore, Mumbai, Silicon Valley, Toronto, Tokyo, and Frankfurt
Supported CLB type	Public network/private network CLB
Upstream and downstream links	CLS logs can be shipped to COS, and exported to CKafka for further processing.

Item	Storing Access Logs in CLS
Log retention	Tencent Cloud does not store access logs by default. The storage feature can be configured as needed.

Relevant Operations

- Storing Access Logs in CLS

Viewing Operation Logs

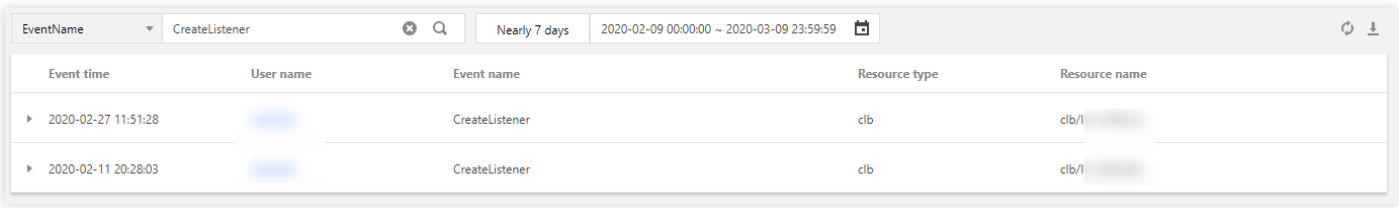
Last updated : 2020-05-12 16:18:57

You can query and download the operation history of CLB in the CloudAudit Console.

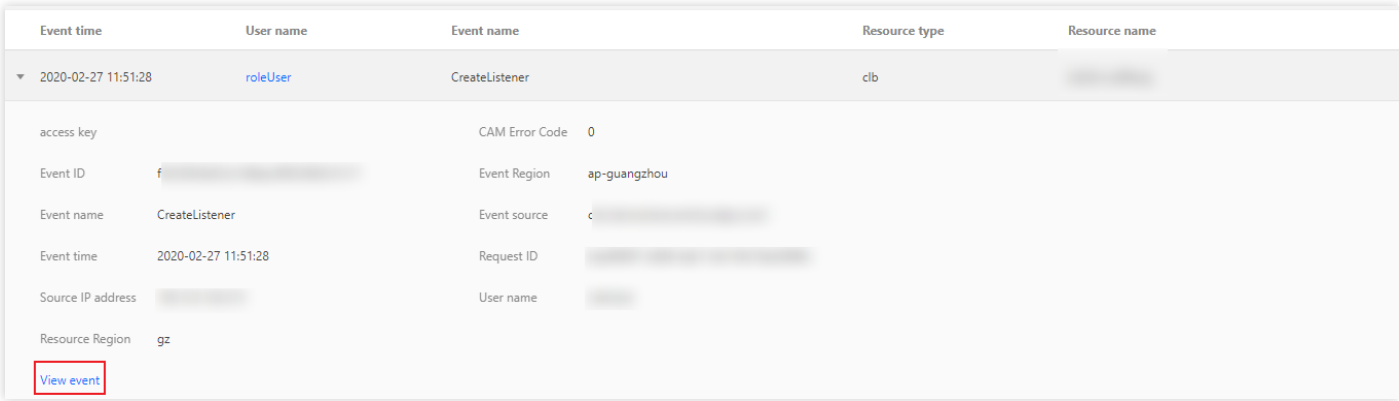
CloudAudit enables you to perform supervision, compliance check, operational review, and risk review for your Tencent Cloud account. It provides event history of your Tencent Cloud account activities, including operations performed through Tencent Cloud Console, APIs, command line tools, and other Tencent Cloud services, which simplifies security analysis, resource change tracking, and troubleshooting.

Directions

1. Log in to the CloudAudit Console.
2. On the left sidebar, click **Event History** to enter the event history page. You can also log in to the CLB Console and select in the top-right corner to enter the event history page.
3. On the event history page, you can query the operations by username, resource type, resource name, event source, event ID, etc. By default, only partial data will be displayed, and you can click **View More** at the bottom of the page to get more results.



4. You can click on the left of an operation to view its details such as access key, error code, and event ID. You can also click **View Event** to view the details of an event.



Storing Access Logs in CLS

Last updated : 2020-11-12 15:10:31

CLB supports configuring layer-7 (HTTP/HTTPS) access logs that can help you better understand client requests, troubleshoot issues, and analyze user behaviors. Currently, access logs can be stored in CLS, reported at a minute granularity, and searched online by multiple rules.

Access logs of CLB are mainly used to quickly locate and troubleshoot issues. The access logging feature includes log reporting, storage, and search:

- Log reporting provides best-effort service, that is, it prioritizes service forwarding over log reporting.
- Log storage and search provide SLA based on the storage service currently in use.

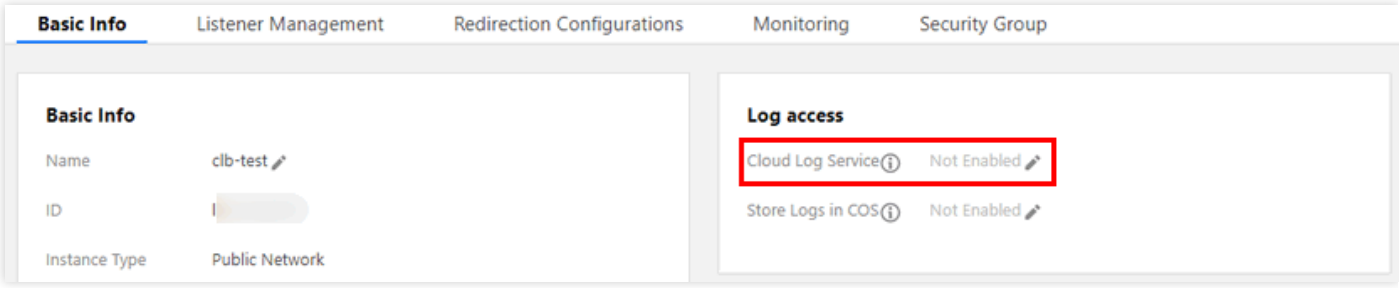
Note :

- Currently, access logs can be stored in CLS only for layer-7 protocols (HTTP/HTTPS) but not layer-4 protocols (TCP/UDP/TCP SSL).

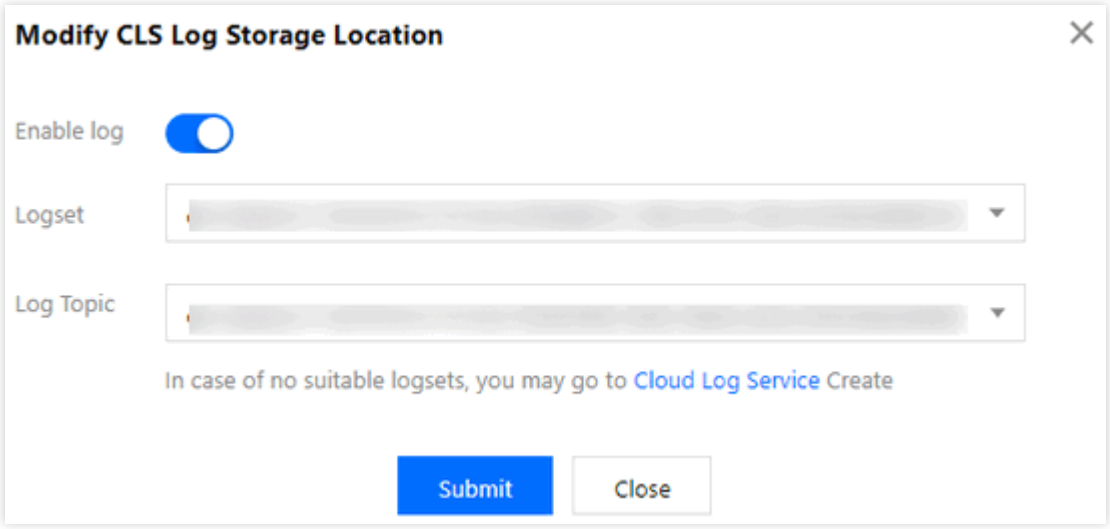
- The feature of storing CLB access logs in CLS is free of charge, and you only need to pay for CLS usage.
- Currently, access logs can be stored in CLS in the Guangzhou, Shanghai, Nanjing, Beijing, Chongqing, Chengdu, Hong Kong (China), Singapore, Mumbai, Silicon Valley, Toronto, and Frankfurt regions through the console or APIs.

Enabling Access Log Storage in CLS

1. Log in to the CLB Console.
2. Click the ID of the CLB instance to be configured to enter the "Basic Information" page.
3. In the "Log Access" module, edit "Cloud Log Service".



4. In the pop-up box, enable access logging and select the destination logset and log topic for access log storage. If you haven't created a logset or log topic yet, please create relevant resources and then select them as the storage location.



5. Click **Submit** and access logs will be collected into the corresponding topic.
6. Then, click the logset or log topic to redirect to the log search page in CLS.
7. (Optional) If you want to disable access logging, you can edit "Cloud Log Service" again to disable it and submit in the pop-up window.

Searching for Access Log

Step 1. Configure log topic indexes

> **Note :**
>
> The log topics must be configured with indexes; otherwise, no logs can be searched for.

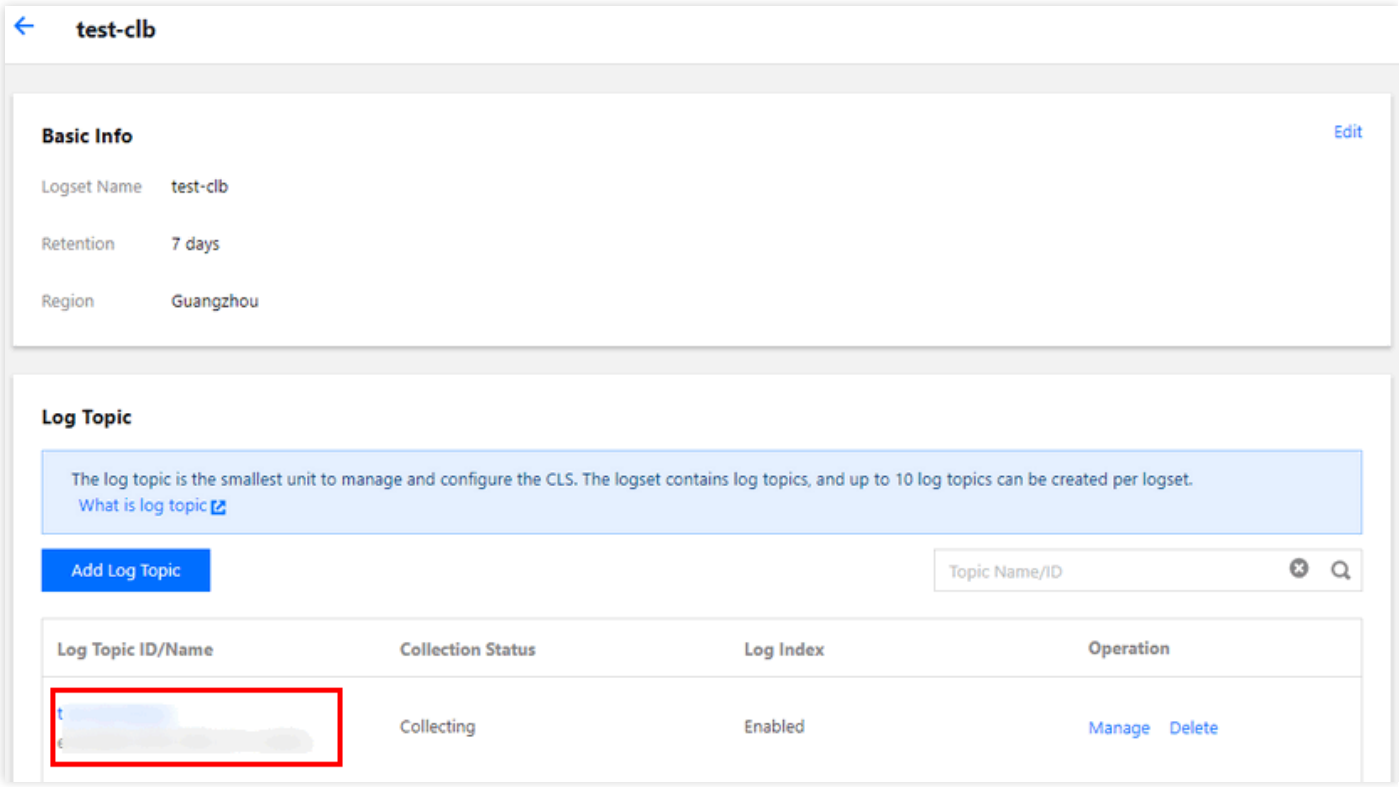
The recommended indexes are as follows:

Key-Value Index	Field Type	Delimiter
server_addr	text	No delimiter required
server_name	text	No delimiter required
http_host	text	No delimiter required
status	long	-

vip_vpcid	long	-

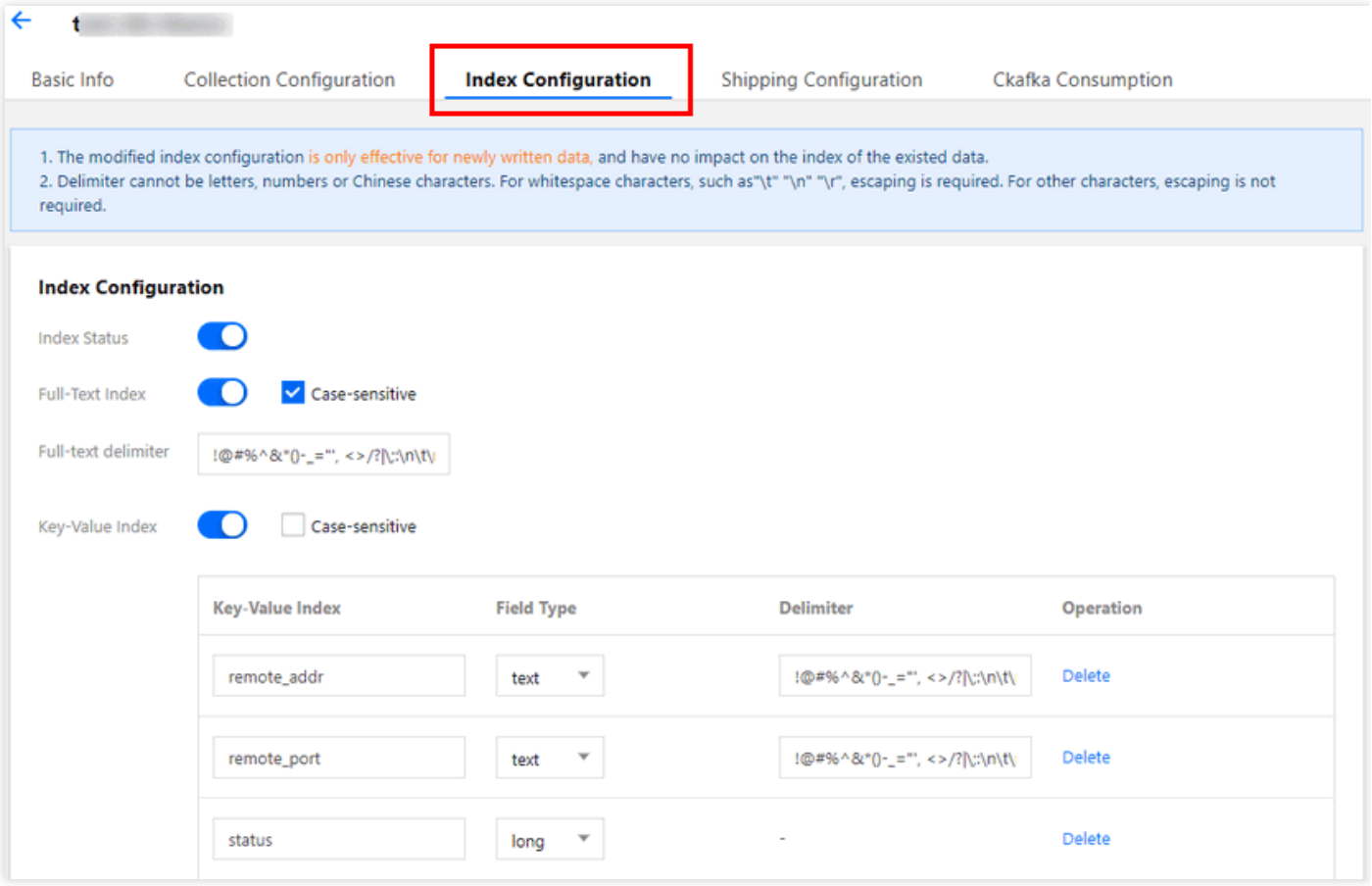
The steps are as follows:

1. Log in to the CLS Console.
2. On the left sidebar, click **Logset** to enter the "Logset Management" page.
3. Click a logset ID to enter the logset details page.
4. On the logset details page, click a log topic ID to enter the log topic details page.

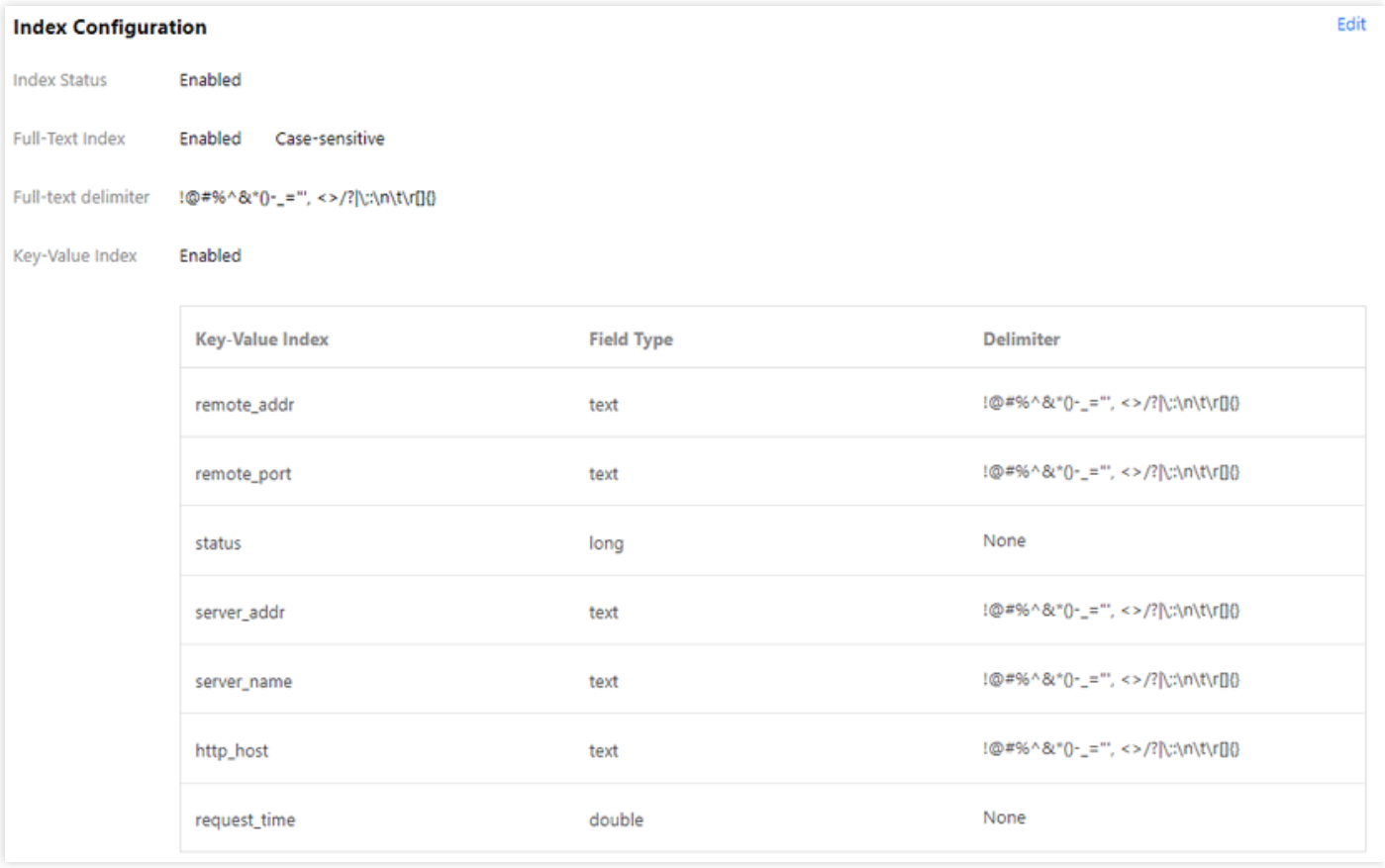


5. On the log topic details page, select the **Index Configuration** tab. You can select some variables from the log variables and configure the index fields as needed. For more information on how to

configure, please see Enabling Index.



6. The result of index configuration is as shown below:



Index Configuration Edit

Index Status: Enabled

Full-Text Index: Enabled Case-sensitive

Full-text delimiter: !@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}

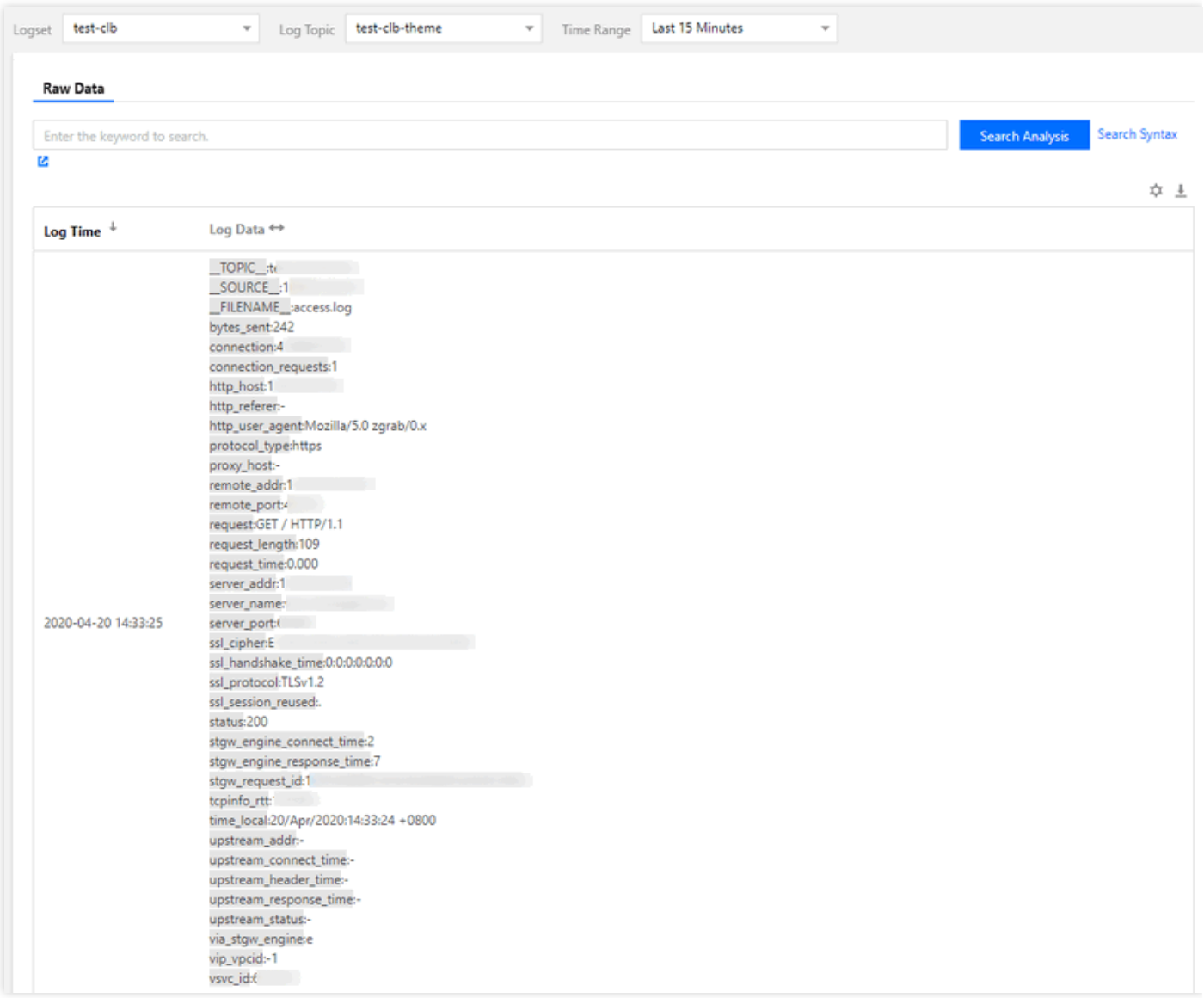
Key-Value Index: Enabled

Key-Value Index	Field Type	Delimiter
remote_addr	text	!@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}
remote_port	text	!@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}
status	long	None
server_addr	text	!@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}
server_name	text	!@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}
http_host	text	!@#%^&*()-_=''', <>/?|\;:\n\t\r[]{}
request_time	double	None

Step 2. Search for access logs

1. Log in to the CLS Console.
2. On the left sidebar, click **Search and Analysis** to enter the "Search Analysis" page.
3. On the "Search Analysis" page, select a logset, log topic, and time range, and click **Search Analysis** to search for the access logs reported by CLB to CLS. For more information on the search

syntax, please see Syntax and Rules.



Log Format and Variable Description

Log format

```
[$stgw_request_id] [$time_local] [$protocol_type] [$server_addr:$server_port] [$server_name] [$remote_addr:$remote_port] [$status] [$upstream_addr] [$upstream_status] [$proxy_host] [$request] [$request_length] [$bytes_sent] [$http_host] [$http_user_agent] [$http_referer] [$request_time] [$upstream_response_time] [$upstream_connect_time] [$upstream_header_time] [$tcpinfo_rtt] [$connection] [$connection_requests] [$ssl_handshake_time] [$ssl_cipher] [$ssl_protocol] [$vip_vpcid]
```

Field type

Currently, CLS supports the following three field types:

Name	Type Description
text	Text type
long	Integer type (Int 64)
double	Floating point type (64-bit)

Log variable description

Variable	Description	Field Type
stgw_request_id	Request ID.	text
time_local	Access time and time zone, such as "01/Jul/2019:11:11:00 +0800" where "+0800" represents UTC+8, i.e., Beijing time.	text
protocol_type	Protocol type (HTTP/HTTPS/SPDY/HTTP2/WS/WSS).	text
server_addr	Destination IP of request.	text
server_port	Destination port of request.	long
server_name	Rule's `server_name`, i.e., server name.	text
remote_addr	Client IP.	text
remote_port	Client port.	long
status	Status code returned to client.	long
upstream_addr	RS address.	text
upstream_status	Status code returned by RS to CLB.	text
proxy_host	Stream ID.	text
request	Request line.	text
request_length	Number of bytes of request received from client.	long
bytes_sent	Number of bytes sent to client.	long
http_host	Request domain name.	text

Variable	Description	Field Type
http_user_agent	`user_agent` field of the HTTP header.	text
http_referer	HTTP request source.	text
request_time	Request processing time. The timing begins when the first byte is received from the client and stops when the last byte is sent to the client, i.e., the total time the whole process takes, where the client request reaches a CLB instance, the CLB instance forwards the request to an RS, the RS responds and sends data to the CLB instance, and finally the CLB instance forwards the data to the client.	double
upstream_response_time	The time that an entire backend request process takes. The timing begins when a CLB instance connects with an RS and stops when the RS receives the request and responds.	double
upstream_connect_time	The time it takes to establish a TCP connection with an RS. The timing begins when a CLB instance connects with an RS and stops when it sends the HTTP request.	double
upstream_header_time	The time it takes to receive an HTTP header from the RS. The timing begins when a CLB instance connects with an RS and stops when the HTTP response header is received from the RS.	double
tcpinfo_rtt	TCP connection RTT.	long
connection	Connection ID.	long
connection_requests	Number of requests on connection.	long
ssl_handshake_time	The time that an SSL handshake takes.	double
ssl_cipher	SSL cipher suite.	text
ssl_protocol	SSL protocol version.	text
vip_vpcid	VPC ID of CLB instance VIP.	long

Storing Access Logs in COS

Last updated : 2020-08-03 11:16:21

⚠ Note :

The feature of storing access logs in COS will stop accepting new enablement requests after 00:00:00, May 15, 2020 (00:00:00, April 26, 2020 for the Guangzhou region) and will be officially disused after 00:00:00, June 30, 2020. For more information, please see Announcement on the Deactivation of the Feature of Storing CLB Access Logs in COS. Please use the upgraded feature of storing access logs in CLS.

CLB supports configuring layer-7 (HTTP/HTTPS) access logs that can help you better understand client requests, troubleshoot issues, and analyze access data. Currently, access logs can be stored in COS for download and analysis, and supported regions include Guangzhou, Shanghai, Beijing, Hong Kong (China), Shanghai Finance, and Shanghai Finance.

Access logs of CLB are mainly used to quickly locate and troubleshoot issues. The access logging feature includes log reporting, storage, and search:

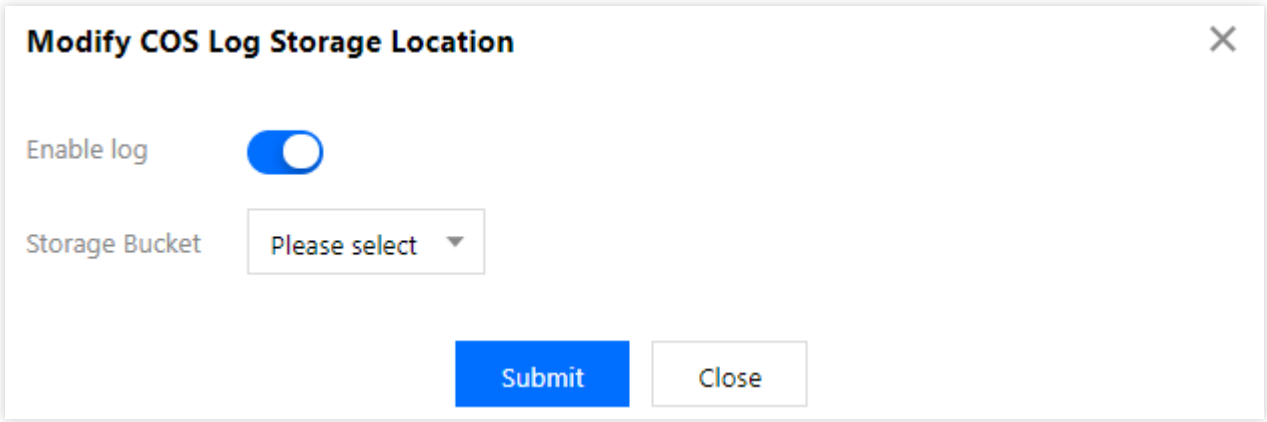
- Log reporting provides best-effort service, that is, it prioritizes service forwarding over log reporting.
- Log storage and search provide SLA based on the storage service currently in use.

ⓘ Note :

- Currently, log aggregation granularity is 1 hour, and log data transfer may have a delay.
- Currently, CLB supports storing and downloading access logs of public network layer-7 (HTTP/HTTPS) CLB instances but not layer-4 (TCP/UDP) or private network layer-7 CLB instances.
- The log service for CLB is free of charge. A free COS storage capacity of 50 GB is provided for individual users as specified in Free Tier. If you have a high number of logs, please clean them up in a timely manner.
- In the regions that support storing access logs in COS, if the access logging feature is not enabled, Tencent Cloud will retain the logs for three days by default; otherwise, the retention period will be subject to the COS configuration. Access log cannot be configured in other regions.

Enabling Access Log Storage in COS

1. Log in to the CLB Console.
2. On the "CLB Instance" list page, click the ID of the CLB instance to be configured to enter the "Basic Information" page.
3. In the "Access Log" module, edit "Store Logs in COS".
4. Enable access logging in the pop-up window and select a destination COS bucket. If you have not created any COS bucket yet, you can create a bucket and select it for log storage.



5. Click **Submit** and a folder named `lb-id` will be automatically created in the bucket for request logs.
6. Then, click the bucket address to enter the log download page.

Disabling Access Log Storage in COS

1. Log in to the CLB Console.
2. On the "CLB Instance" list page, click the ID of the CLB instance to be configured to enter the "Basic Information" page.
3. In the "Access Log" module, edit "Store Logs in COS".
4. In the pop-up box, disable access log and click **Submit**.
   The configuration result is as follows. Log storage in COS cannot be enabled again after it is disabled. For more information, please see Notice on the Deactivation of the Feature of Storing CLB Access Logs in COS.

Log Format and Variable Description

Log format

```
[$stgw_request_id] [$time_local] [$protocol_type] [$server_addr:$server_port] [$server_name] [$remote_addr:$remote_port] [$status] [$upstream_status] [$proxy_host] [$request] [$request_length]
```

```
[$bytes_sent] [$http_host] [$http_user_agent] [$http_referer]
[$request_time] [$upstream_response_time] [$upstream_connect_time] [$upstream_header_time] [$tcpi
nfo_rtt] [$connection] [$connection_requests] [$ssl_handshake_time] [$ssl_cipher] [$ssl_protocol]
[$ssl_session_reused]
```

Log variable description

Variable	Description
stgw_request_id	Request ID.
time_local	Access time and time zone, such as "01/Jul/2019:11:11:00 +0800" where "+0800" represents UTC+8, i.e., Beijing time.
protocol_type	Protocol type (HTTP/HTTPS/SPDY/HTTP2/WS/WSS).
server_addr:server_port	Destination IP and port of request.
server_name	Rule's `server_name` , i.e., server name.
remote_addr:remote_port	Client IP and port.
status	Status code returned by CLB to client.
upstream_status	Status code returned by RS to CLB instance.
proxy_host	Stream ID.
request	Request line.
request_length	Number of bytes of request received from client.
bytes_sent	Number of bytes sent to client.
http_host	Request domain name.
http_user_agent	`user_agent` field of the HTTP header.
http_referer	HTTP request source.
request_time	Request processing time. The timing begins when the first byte is received from the client and stops when the last byte is sent to the client, i.e., the total time the whole process takes, where the client request reaches a CLB instance, the CLB instance forwards the request to an RS, the RS responds and sends data to the CLB instance, and finally the CLB instance forwards the data to the client.

Variable	Description
upstream_response_time	The time that an entire backend request process takes. The timing begins when a CLB instance connects with an RS and stops when the RS receives the request and responds.
upstream_connect_time	The time it takes to establish a TCP connection with an RS. The timing begins when a CLB instance connects with an RS and stops when it sends the HTTP request.
upstream_header_time	The time it takes to receive an HTTP header from the RS. The timing begins when a CLB instance connects with an RS and stops when the HTTP response header is received from the RS.
tcpinfo_rtt	TCP connection RTT.
connection	Connection ID.
connection_requests	Number of connection requests.
ssl_handshake_time	The time that an SSL handshake takes.
ssl_cipher	SSL cipher suite.
ssl_protocol	SSL protocol version.
ssl_session_reused	SSL SESSION reuse.