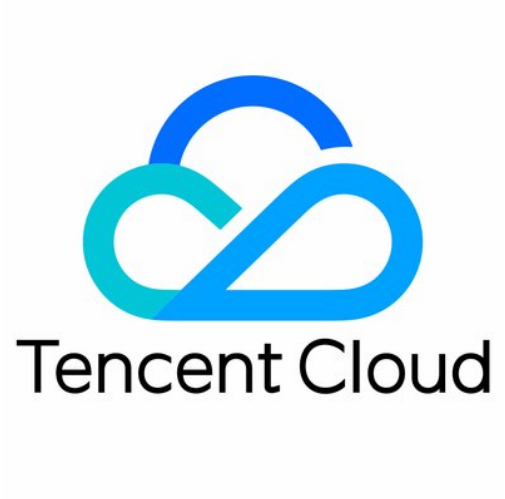
Cloud Load Balancer

Log Management

Product Documentation



Contents

Log Management
- Access Log Overview
- Viewing Operation Logs
- Configuring Access Logs
- Sampling Logs
- Configuring Health Check Logs
- Accessing Log Dashboard

Log Management
Access Log Overview

Last updated：2024-01-04 14:34:05

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	For more details on CLS available regions, see Available Regions.
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.
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

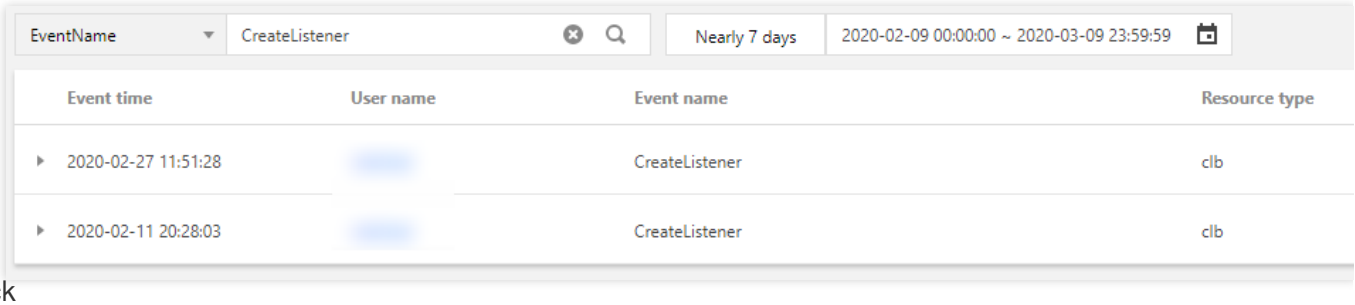
Viewing Operation Logs

Last updated：2024-01-04 14:34:05

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.

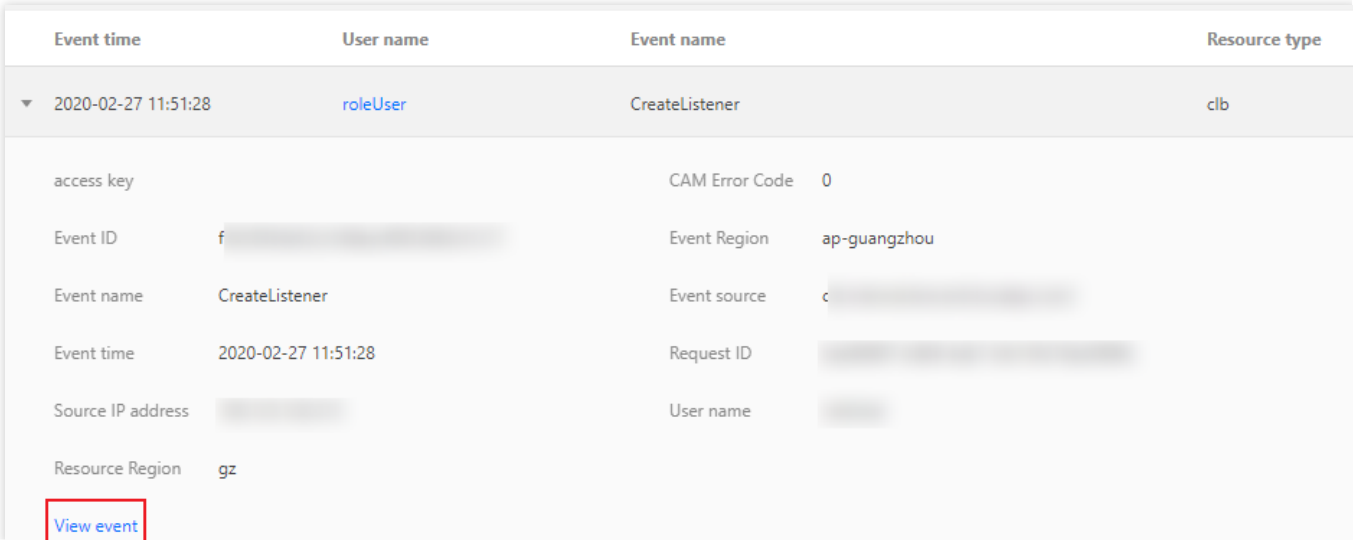
Directions

1. Log in to the CloudAudit console.
2. Click **Operation Record** on the left sidebar to enter the **Operation Record** page. You can also log in to the CLB Console and click **CloudAudit** in the top-right corner.
3. On the operation history page, 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. Click

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



Configuring Access Logs

Last updated：2024-01-04 14:34:05

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 services. In other words, service forwarding has a higher priority than log reporting.

Log storage and query: SLA is guaranteed 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).

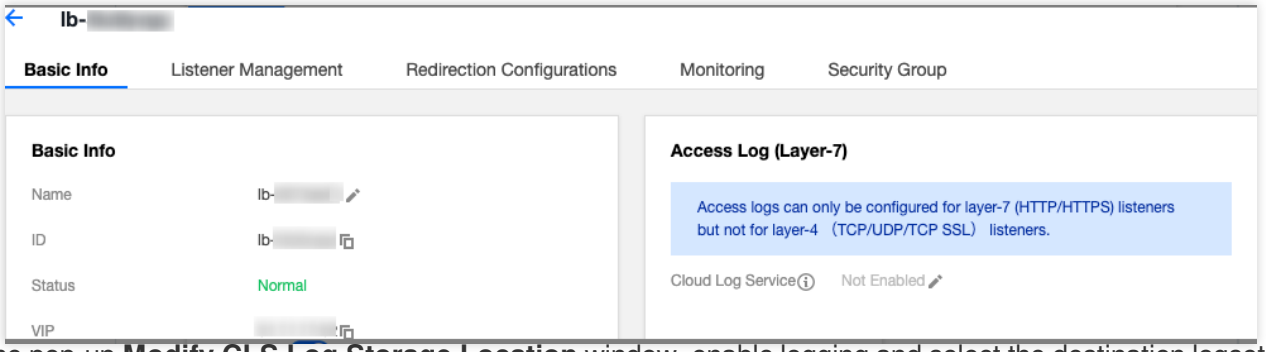
Storing CLB access logs to CLS is now free of charge. You only need to pay for the CLS service.

This feature is supported only in certain regions as displayed in the console.

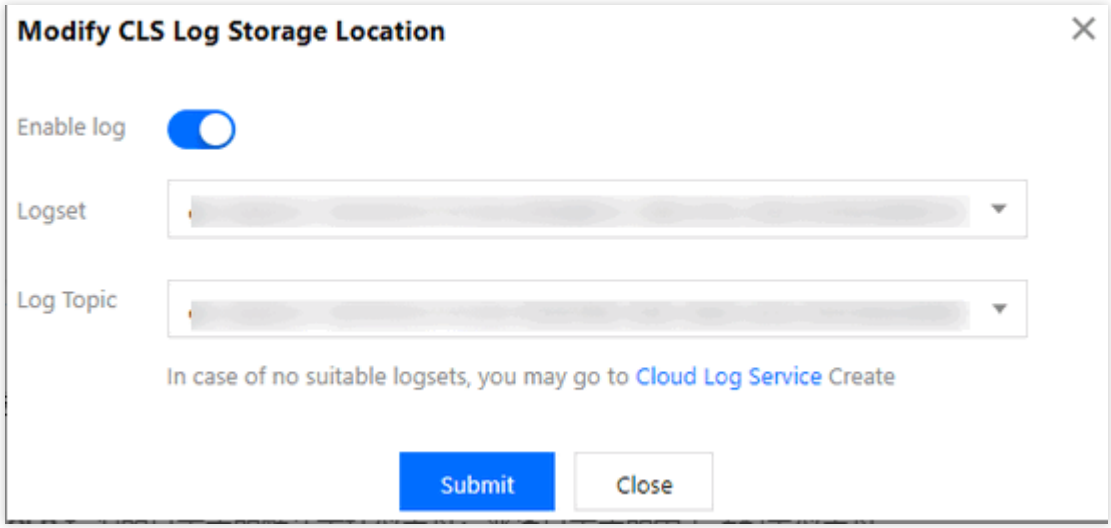
Method 1: Single-Instance Access Logging

Step 1. Enable access log storage in CLS

1. Log in to the CLB console, and click **Instance management** in the left sidebar.
2. On the **Instance management** page, click the ID of the target CLB instance.
3. Click the pencil icon in the **Access Log (Layer-7)** panel on the **Basic Info** tab.



4. In the pop-up **Modify CLS Log Storage Location** window, enable logging and select the destination logset and log topic for access log storage, and then click **Submit**. If you have not created a logset or log topic, create one and then select it as the storage location.



Note:

We recommend that you use a log topic marked with **CLB** in the clb_logset logset. The differences between a log topic marked with **CLB** and a common log topic are as follows:

CLB log topics can automatically create an index, while a common log topic requires manual index creation.

A dashboard is provided for CLB log topics by default, but needs to be manually configured for a common log topic.

5. Click the logset or log topic to go to the **Search Analysis** page in the CLS console.

6. (Optional) To disable access logging, click the pencil icon. In the **Modify CLS Log Storage Location** window, disable it and click **Submit**.

Step 2. Configure log topic indexes

Note:

If access logging is configured for a single instance, you must configure the index for the log topic. Otherwise, no logs can be found.

The recommended indexes are as follows:

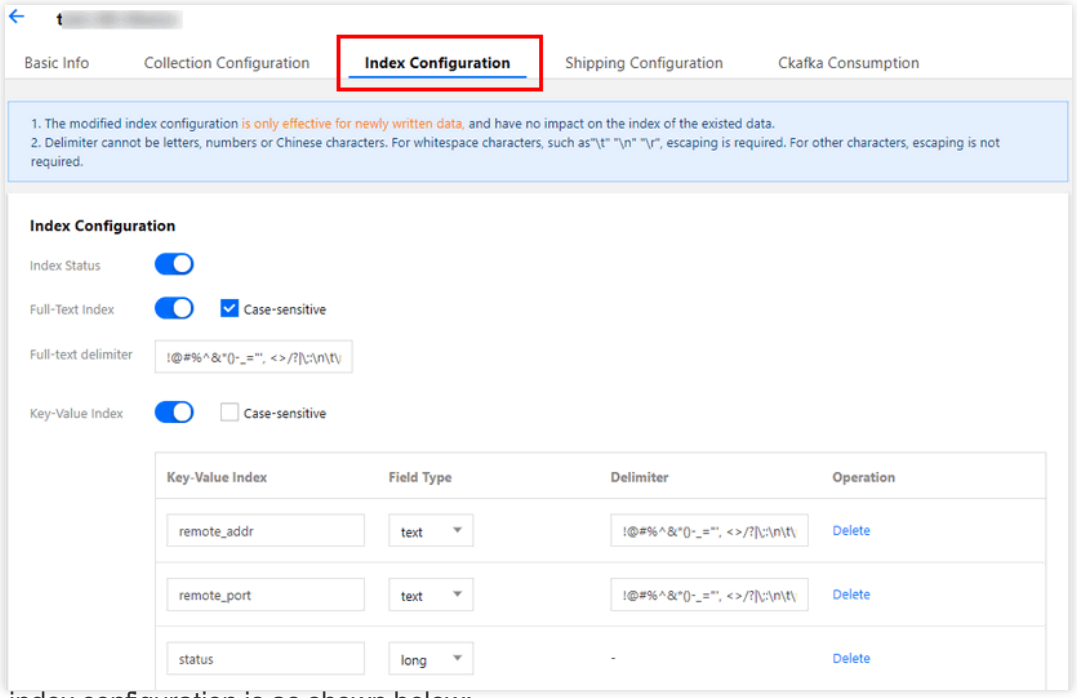
Key-value Index	Field Type	Delimiter
server_addr	text	Not required
server_name	text	Not required
http_host	text	Not required
status	long	-
vip_vpcid	long	-

The steps are as follows:

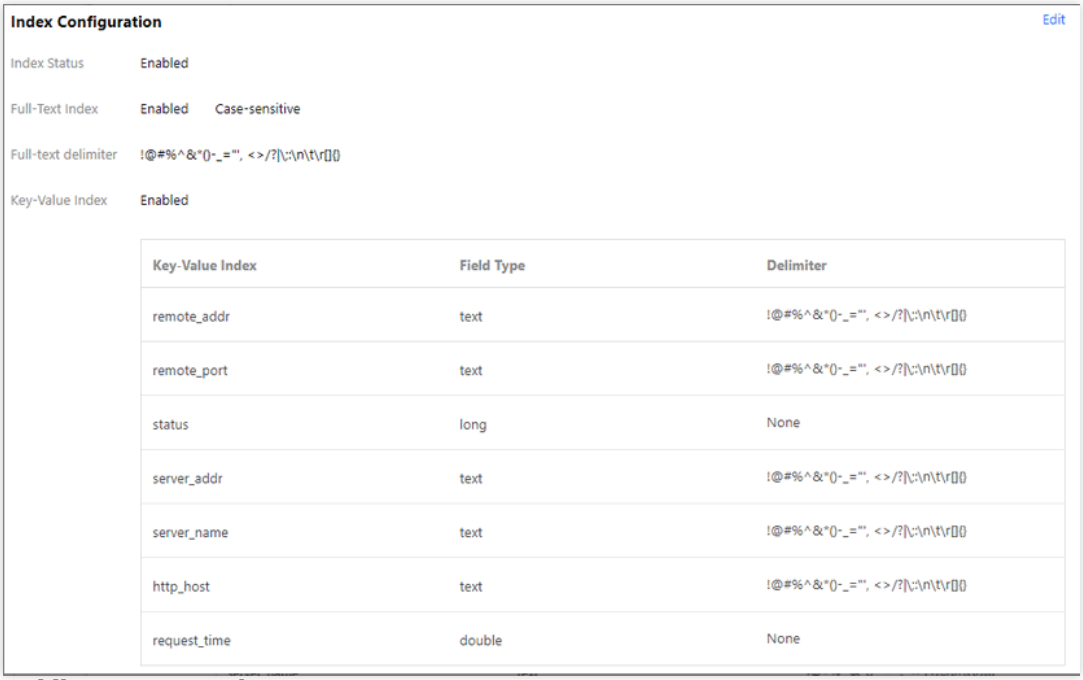
1. Log in to the CLS console, and click **Log Topic** in the left sidebar.

2. On the **Log Topic** page, click the ID of the target log topic.

3. On the log topic details page, click the **Index Configuration** tab, and click **Edit** in the top-right corner to add indexes. For more information about index configuration, see Configuring Index.

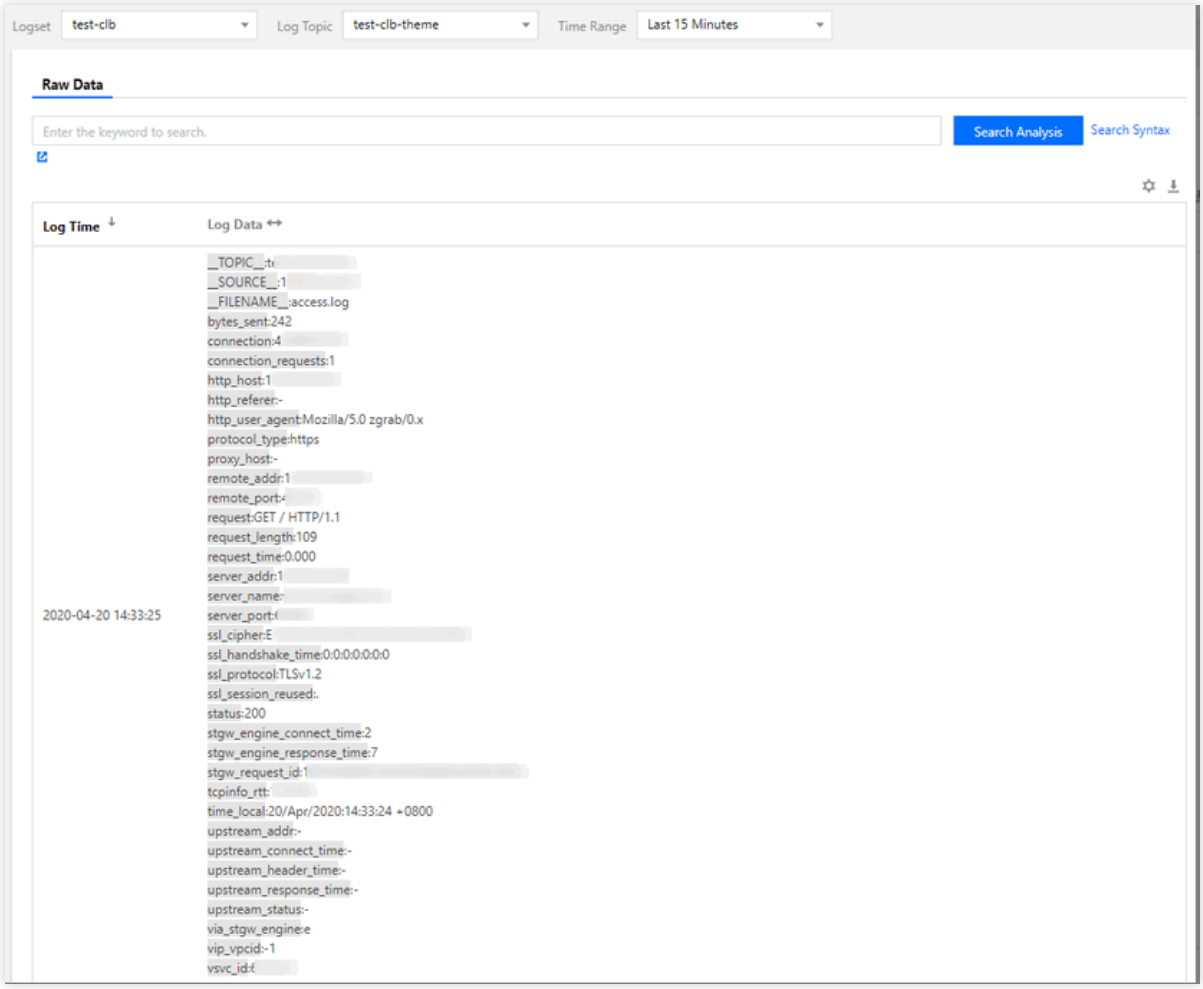


4. The index configuration is as shown below:



Step 3. View access logs

1. Log in to the CLS console, and click **Search Analysis** in the left sidebar.
2. 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 about the search syntax, see Legacy CLS Search Syntax.



Method 2: Batch Configure Access Logging

Step 1: Create a logset and log topic.

To configure access logs in CLS, you need to first create a logset and log topic.

If you have created a logset and log topic, skip to Step 2.

1. Log in to the CLB console and click **Access Logs** in the left sidebar.

2. On the **Access Logs** page, select a region for the logset, and then click **Create Logset** in the **Logset information** section.

3. In the pop-up **Create Logset** window, set the retention period and click **Save**.

Note:

You can create only a single logset named "clb_logset" in each region.

4. Click **Create Log Topic** in the **Log Topic** section of the **Access Logs** page.

5. In the pop-up window, specify the storage type and log retention period, select a CLB instance in the list on the left and add it to the list on the right, and then click **Save**.

Note:

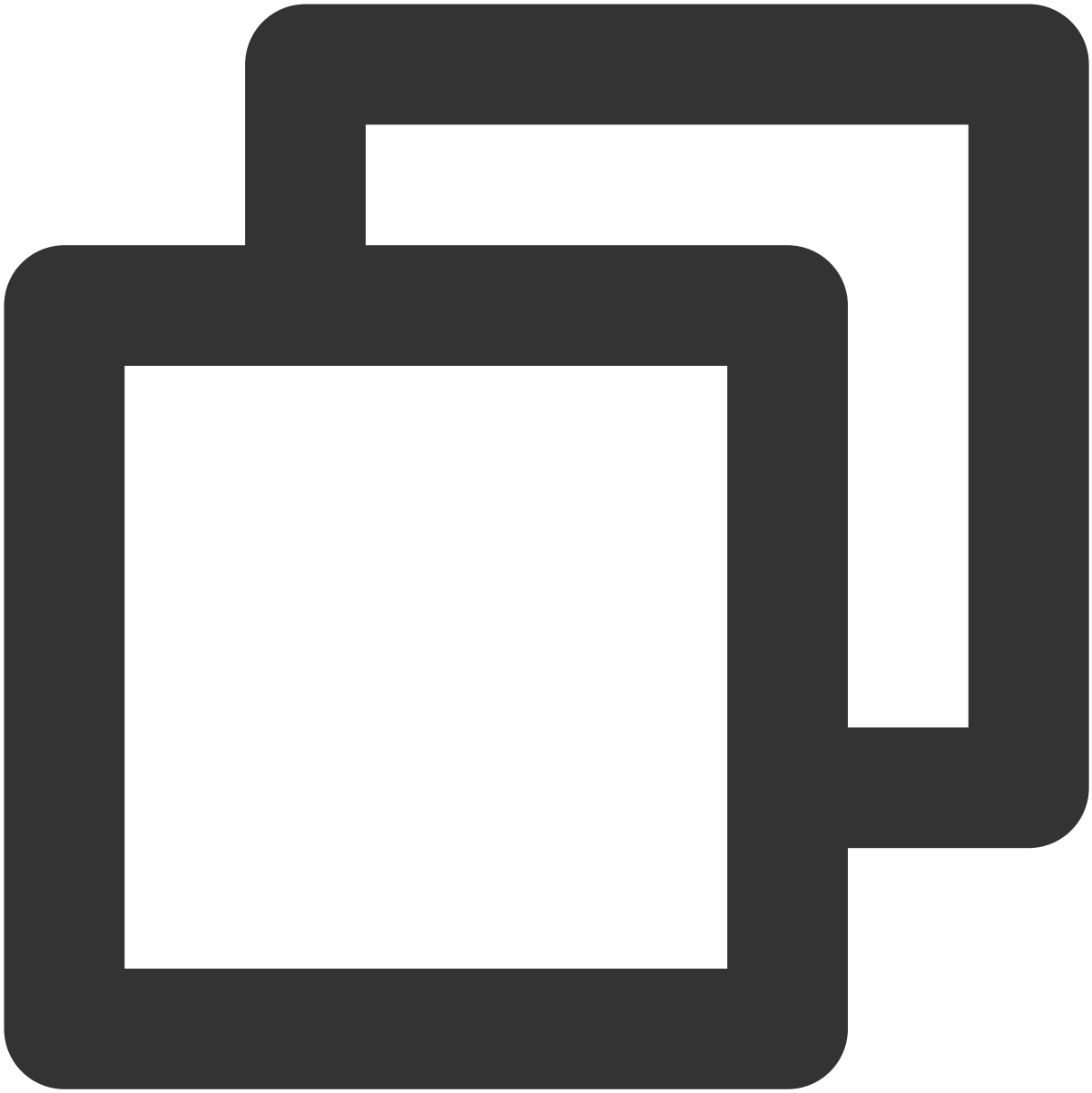
Supported storage types: STANDARD storage and IA storage. For more information, see Storage Class Overview.
Logs can be retained permanently or for a specified period of time.
When you create a log topic, you can add a CLB instance as needed. To add a CLB instance after a log topic is created, click **Manage** in the **Operation** column of the log topic in the list. Each CLB instance can be added to only one log topic.
A logset can contain multiple log topics. You can categorize CLB logs into various log topics which will be marked with **CLB** by default.
6. (Optional) To disable access logging, click **Disable**.

Step 2. View access logs

Without any manual configurations, CLB has been automatically configured with index search by access log valuable. You can directly query access logs through search and analysis.
1. Log in to the CLB console and click **Access Logs** in the left sidebar.
2. Click **Search** in the **Operation** column of the topic log topic to go to the **Search Analysis** page in the CLS console.
3. On the **Search Analysis** page, enter the search syntax in the input box, select a time range, and then click **Search Analysis** to search for access logs reported by CLB to CLS.
Note:
For more information about the search syntax, see Syntax Rules.

Log Format and Variable Description

Log format



```
[$stgw_request_id] [$time_local] [$protocol_type] [$server_addr:$server_port]  [$se
```

Field type

Currently, CLS supports the following three field types:

Name	Description
text	Text type.
long	Integer type (Int 64).

double	Floating point type (64 bit).

Log variable description

Variable Name	Description	Field Type
stgw_request_id	Request ID.	text
time_local	Access time and time zone. Example: `01/Jul/2019:11:11:00 +0800`, where `+0800` represents UTC+8.	text
protocol_type	Protocol type. Supported protocols: HTTP, HTTPS, SPDY, HTTP2, WS, and WSS.	text
server_addr	VIP of the CLB instance.	text
server_port	CLB VPort, that is, the listening port.	long
server_name	`server_name` value of a rule, that is, the domain name configured in a CLB listener.	text
remote_addr	Client IP address.	text
remote_port	Client port.	long
status	Status code returned by the CLB instance to the client.	long
upstream_addr	Address of the real server (RS).	text
upstream_status	Status code returned by the RS to the CLB instance.	text
proxy_host	Stream ID.	text
request	Request line.	text
request_length	Number of bytes of the request received from the client.	long
bytes_sent	Number of bytes sent to the client.	long
http_host	Request domain name, which is the value of the **Host** field in the HTTP header.	text
http_user_agent	`user_agent` field in the HTTP header.	text
http_referer	Source of the HTTP request.	text
http_x_forward_for	Content of `x-forward-for header` in the HTTP request.	text

request_time	Request processing time, which is duration from when the first byte is received from the client to when the last byte is sent to the client, that is, the total time consumed by the whole process in which the client request reaches the 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. Unit: seconds.	double
upstream_response_time	The time that an entire backend request process takes, starting from when the CLB instance connects with an RS to when the RS receives the request and responds. Unit: seconds.	double
upstream_connect_time	The time taken to establish a TCP connection with an RS, starting from when the CLB instance connects with the RS to when the CLB instance sends an HTTP request.	double
upstream_header_time	The time taken to receive an HTTP header from the RS, starting from when the CLB instance connects with the RS to when the HTTP response header is received from the RS.	double
tcpinfo_rtt	The round-trip time (RTT) of the TCP connection.	long
connection	Connection ID.	long
connection_requests	Number of requests in the connection	long
ssl_handshake_time	Time in microseconds taken by SSL handshake phases, in the format of `x:x:x:x:x:x:x` , with the time strings of different phases separated by colons (:). If the time of a phase is less than 1 ms, `0` is displayed. The first field indicates whether the SSL session is reused. The second field indicates the time taken by the entire handshake process. The third to seventh fields indicate the time taken by each SSL handshake phase. The third field indicates the time from when the CLB instance receives `client hello` to when the CLB instance sends `server hello done` . The fourth field indicates the time from when the CLB instance starts sending the server certificate to when the CLB instance finishes sending the server certificate. The fifth field indicates the time from when the CLB instance calculates the signature to when the CLB instance finishes sending `server key exchange` . The sixth field indicates the time from when the CLB instance starts receiving `client key exchange` to when the CLB instance	text

	finishes receiving `client key exchange`. The seventh field indicates the time from when the CLB instance receives `client key exchange` to when the CLB instance sends `server finished`.	
ssl_cipher	SSL cipher suite.	text
ssl_protocol	SSL protocol version.	text
vip_vpcid	ID of the VPC instance to which the CLB instance belongs. The `vip_vpcid` value of a public network CLB instance is `-1`.	long
request_method	Request method. Only POST and GET requests are supported.	text
uri	Uniform resource identifier.	text
server_protocol	Protocol used for CLB.	text

Default search log valuable

The following fields can be found in logsets with "CLB" by default:

Index Field	Description	Field Type
time_local	Access time and time zone. Example: `01/Jul/2019:11:11:00 +0800`, where `+0800` represents UTC+8.	text
protocol_type	Protocol type. Supported protocols: HTTP, HTTPS, SPDY, HTTP2, WS, and WSS.	text
server_addr	VIP of the CLB instance.	text
server_name	`server_name` value of a rule, that is, the domain name configured in a CLB listener.	text
remote_addr	Client IP address.	text
status	Status code returned by the CLB instance to the client.	long
upstream_addr	Address of the RS.	text
upstream_status	Status code returned by the RS to the CLB instance.	text
request_length	Number of bytes of the request received from the client.	long
bytes_sent	Number of bytes sent to the client.	long
http_host	Request domain name, which is the value of the **Host** field in the	text

	HTTP header.	
request_time	Request processing time, which is duration from when the first byte is received from the client to when the last byte is sent to the client, that is, the total time consumed by the whole process in which the client request reaches the 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.Unit: seconds.	double
upstream_response_time	The time that an entire backend request process takes, starting from when the CLB instance connects with an RS to when the RS receives the request and responds.Unit: seconds.	double

Sampling Logs

Last updated：2024-01-04 14:34:05

After you enable layer-7 access logging or health check logging, if the log volume is large, full log reporting may result in high log costs. Tencent Cloud Load Balancer (CLB) supports log collection through sampling to reduce the amount of reported data and reduce log costs.

Note:

You can configure to store CLB access logs and health check logs in Tencent Cloud Log Service (CLS) to achieve log search, analysis, visualization, and alarming. CLS is separately billed. For more information about the billing of CLS, see Product Pricing.

Prerequisites

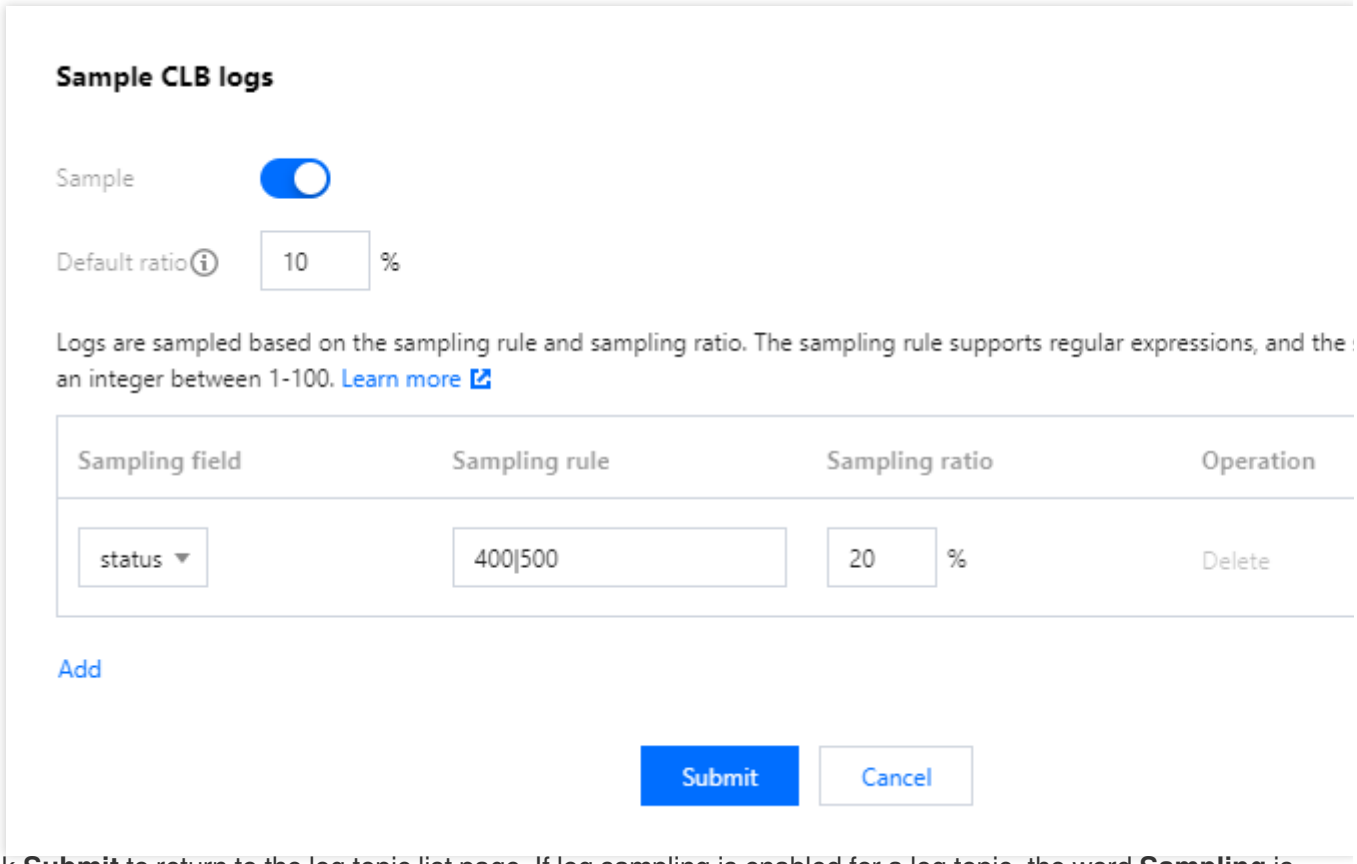
You have created the logset and log topics for access logs. For more information, see Configuring Access Logs.
You have created the logset and log topics for health check logs. For more information, see Configuring Health Check Logs.

Sampling Layer-7 Access Logs

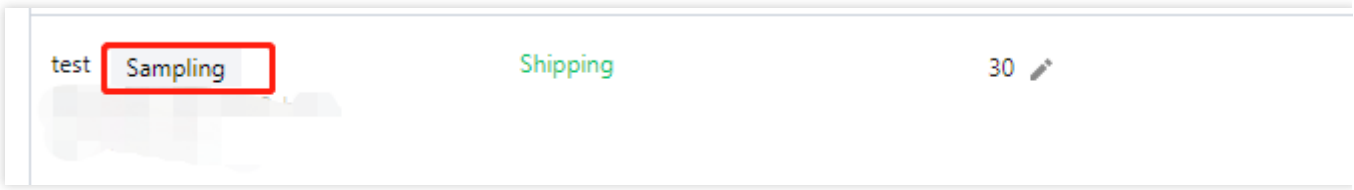
1. Log in to the CLB console and choose **Access logs** > **Log list** in the left sidebar.
2. In the top-left corner of the **Access logs** page, select your region. Find the target log topic in the log topic list and choose **More** > **Sample** in the **Operation** column.
3. In the **Sample CLB logs** pop-up window, turn on the sampling switch and configure the parameters as needed.

Parameter	Description
Sample	If the switch is turned on, log sampling is enabled. If the switch is turned off, full logs are collected.
Default ratio	If you configured the log sampling rule, logs that do not match the sampling rule are sampled based on the default sampling ratio. You can enter an integer from 1 to 100.
Sampling field	The **status** field is currently supported.
Sampling rule	Sampling rules support regular expressions. For example, if you want to sample logs whose status code is 400 or 500, you can set the sampling rule as to **400|500**.
Sampling ratio	Sampling ratio. You can enter an integer from 1 to 100.

Operation	You can delete the sampling rule.
Add	If the existing sampling rules do not meet your needs, you can add more sampling rules. At most five sampling rules can be configured for each log topic.



4. Click **Submit** to return to the log topic list page. If log sampling is enabled for a log topic, the word **Sampling** is displayed next to the topic name.



Sampling Health Check Logs

1. Log in to the CLB console and click **Health Check Logs** in the left sidebar.
2. Other steps are the same as those described in the Sampling Layer-7 Access Logs section.

References

Configuring Access Logs
Configuring Health Check Logs

Configuring Health Check Logs

Last updated：2024-01-04 14:34:05

CLB supports storing health check logs to CLS where you can view the logs, reporting at a minute granularity and querying online by multiple rules, helping you identify the causes of health check failures.

Note:

The feature is in a beta test. To try it out, submit a ticket.

Health check logging includes log reporting, storage and query:

Log reporting: Service forwarding has a higher priority than log reporting.

Log storage and query: SLA is guaranteed based on the storage service currently in use.

Restrictions

CLB layer-4 and layer-7 protocols can be used for storing health check logs to CLS.

Storing CLB health check logs to CLS is now free of charge. You only need to pay for the CLS service.

This feature is available only to CLB (formerly known as application CLB) instances.

This feature is supported only in certain regions as displayed in the console.

Step 1: Add a Role Permission

To add a role permission, make sure you have activated the CLS service.

1. Log in to the CLB console and click **Health Check Logs** in the left sidebar.
2. On the **Health Check Logs** page, click **Activate now**, and then click **Authorize and Activate** in the pop-up window.
3. Switch to the **Role Management** page in the CAM console, and click **Grant**.

Step 2: Create a Logset and Log Topic

To store health check logs to CLS, you need to first create a logset and log topic.

If you have created a logset and log topic, skip to Step 3.

1. Log in to the CLB console and click **Health Check Logs** in the left sidebar.
2. On the **Health Check Logs** page, select a region for the logset, and then click **Create Logset** in the **Logset information** section.
3. In the pop-up **Create Logset** window, set the retention period and click **Save**.
4. Click **Create Log Topic** in the **Log Topic** section of the **Health Check Logs** page.

5. In the pop-up window, specify the storage type and log retention period, select a CLB instance in the list on the left and add it to the list on the right, and then click **Save**.

Note:

Supported storage types: STANDARD storage and IA storage. For more information, see Storage Class Overview.

Logs can be retained permanently or for a specified period of time.

When you create a log topic, you can add a CLB instance as needed. To add a CLB instance after a log topic is created, click **Manage** in the **Operation** column of the log topic in the list. Each CLB instance can be added to only one log topic.

A logset can contain multiple log topics. You can categorize CLB logs into various log topics which will be marked with "CLB" by default.

6. (Optional) To disable health check logging, click **Disable**.

Step 3. View Health Check Logs

Without any manual configurations, CLB has been automatically configured with index search by health check log valuable. You can directly query health check logs through search and analysis.

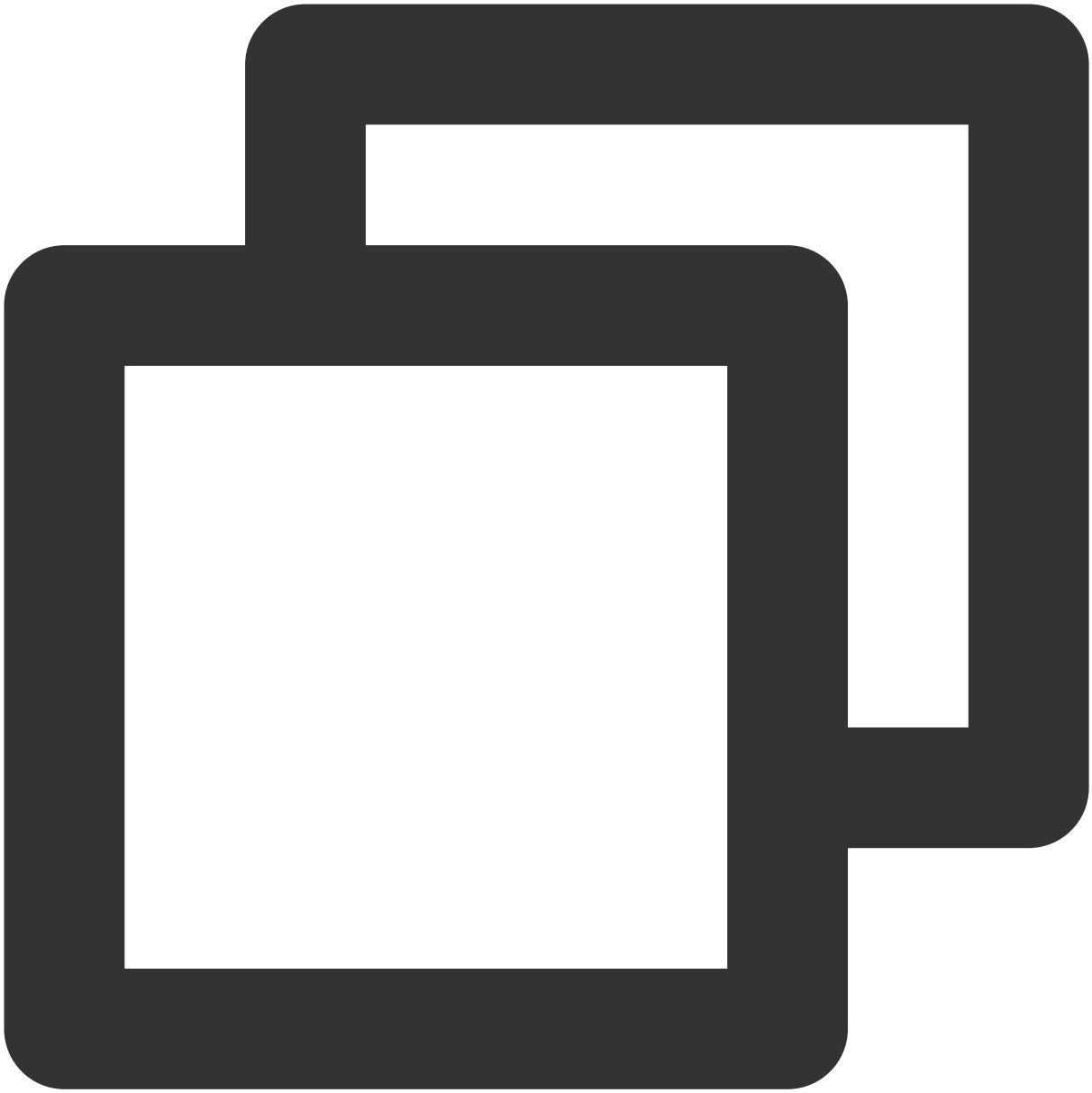
1. Log in to the CLB console and click **Health Check Logs** in the left sidebar.
2. On the **Health Check Logs** page, select the region of the logset you want to view. In the **Log Topic** section, click **Search** in the **Operation** column of the log topic you select to go to the CLS Console.
3. In the CLS console, click **Search Analysis** in the left sidebar.
4. On the **Search Analysis** page, enter the search syntax in the input box, select a time range, and then click **Search Analysis** to search for health check logs reported by CLB to CLS.

Note:

For more information about the search syntax, see Syntax Rules.

Health Check Log Format and Variable

Log format



```
[$protocol][$rsport][$rs_vpcid][$vport][$vpcid][$time][$vip][$rsip][$status][$domai
```

Log variable description

Variable Name	Description	Field Type
protocol	Protocol type. Supported protocols: HTTP, HTTPS, SPDY, HTTP2, WS, and WSS.	text
rsport	Port of the real server.	long

rs_vpcid	VPC ID of the real server. The `vip_vpcid` value of a public network CLB instance is `-1` .	long
vport	CLB VPort, that is, the listening port.	long
vpcId	VPC ID of the VIP of the CLB instance. The `vip_vpcid` value of a public network CLB instance is `-1` .	long
time	Access time and time zone. Example: `01/Jul/2019:11:11:00 +0800` , where `+0800` represents UTC+8.	text
vip	VIP of the CLB instance.	text
rsip	IP address of the real server.	text
status	Health status. Valid values: `true` : healthy `false` : unhealthy	text
domain	Domain name to be checked. This parameter is left empty if a layer-4 listener is used.	text
url	URL to be checked. This parameter is left empty if a layer-4 listener is used.	text

References

Getting Started in Five Minutes

Accessing Log Dashboard

Last updated：2024-01-04 14:34:05

By connecting CLB access logs to Cloud Log Service, you can check the access logs in a dashboard. The dashboard provides charts of multiple metrics, giving you a full picture of the load balancer.

Dashboard

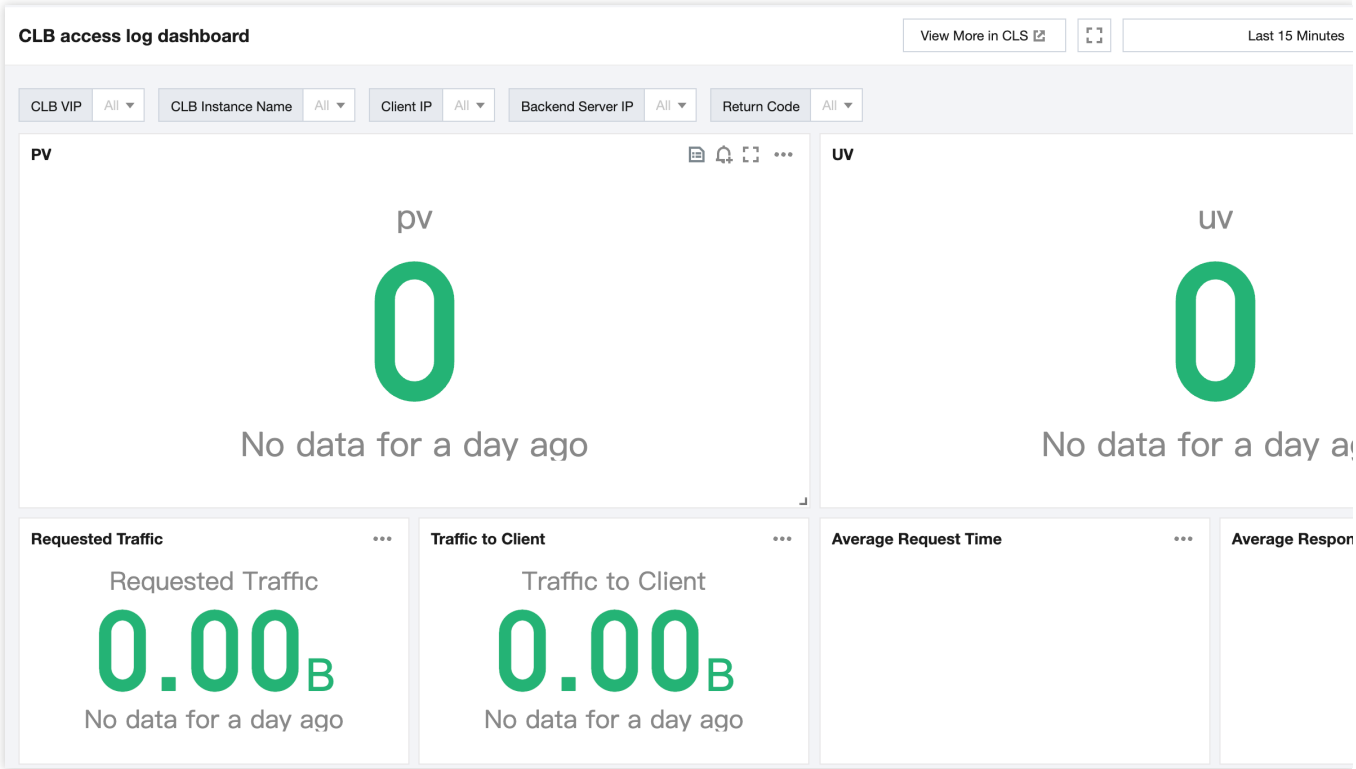
Each log topic has its own dashboard, which contains data of following metrics.
PV
UV
Outgoing request message traffic
Incoming response traffic
Average request time
Average response time
Backend status code distribution
Overall status code distribution
PV/UV trend
Outgoing/Incoming traffic trend
Average requests/responses per minute
P99, P95, P90, P50 access duration
Top requested instances
Top requested domain names

Preparations

Create logsets for CLB. See Creating Logsets and Log Topics.

Directions

1. Log in to the CLB console and select **Access Logs** on the left sidebar.
2. In the **Access Log Dashboard** page, select the region and log topic to see the dashboard of this log topic.



3. (Optional) In the upper corner of the **Access Log Dashboard** page, filter logs by the CLB VIP, client IP, backend server IP and status code.

See Also

For more information, see Configuring Access Logs.