

负载均衡

日志管理

产品文档



腾讯云

【版权声明】

©2013-2019 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

日志管理

访问日志概述

查看操作日志

配置访问日志到 CLS

配置访问日志到 COS

日志管理

访问日志概述

最近更新时间：2020-09-21 17:49:03

负载均衡的访问日志收集了每个客户端请求的详细信息，日志中记录了请求时间、请求路径、客户端 IP 和端口、返回码、响应时间等信息。访问日志可以帮助您了解客户端请求、辅助排查问题、分析梳理用户行为等。

说明：

- 仅七层负载均衡支持配置访问日志，四层负载均衡不支持配置访问日志。
- 当前仅部分地域支持配置访问日志，详情请参见下文。

存储方式

负载均衡的访问日志支持 [日志服务（CLS）](#)：日志服务是一站式日志服务平台，提供从日志采集、日志存储到日志检索分析、实时消费、日志投递等多项服务，协助用户通过日志来解决业务运营、安全监控、日志审计、日志分析等问题。

功能特性	配置访问日志到 CLS
获取日志的时间粒度	分钟级
在线检索	支持
检索语法	全文检索、键值检索、模糊关键字检索等，详情请参见 检索规则 。
支持地域	广州、上海、南京、北京、重庆、成都、中国香港、新加坡、孟买、硅谷、多伦多、东京、法兰克福。
支持类型	支持公网/内网负载均衡
上下游链路	CLS 日志支持投递到 COS，支持使用 CKafka 消费日志。
日志存储	腾讯云默认情况下不承诺存储访问日志，如有业务需要请自行配置访问日志到 CLS。

相关操作

- [配置访问日志到 CLS](#)

查看操作日志

最近更新时间：2020-04-01 18:35:18

您可以在 [云审计控制台](#) 查询、下载负载均衡的操作记录。

[云审计（CloudAudit）](#) 是一项支持对您的腾讯云账号进行监管、合规性检查、操作审核和风险审核的服务。

CloudAudit 提供腾讯云账号活动的事件历史记录，这些活动包括通过腾讯云管理控制台、API 服务、命令行工具和其他腾讯云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

操作步骤

1. 登录 [云审计控制台](#)。
2. 在左侧导航中，单击【操作记录】，进入操作记录页面。您也可以登录 [负载均衡控制台](#)，选择页面右上角的，即可快捷进入操作记录页面。
3. 在操作记录页面中，您可以根据用户名、资源类型、资源名称、事件源、事件 ID 等查询操作记录，默认情况下仅展示部分数据，可在页面下方单击【点击加载更多】来获取更多记录。

EventName	CreateListener	Nearly 7 days	2020-02-09 00:00:00 ~ 2020-03-09 23:59:59	
Event time	User name	Event name	Resource type	Resource name
▶ 2020-02-27 11:51:28		CreateListener	clb	clb/l
▶ 2020-02-11 20:28:03		CreateListener	clb	clb/l

4. 您如果想更进一步了解单个操作记录，单击该操作记录左侧的，即可查看操作记录的详情，包括访问密钥、错误码、事件 ID 等。同时，可以单击【查看事件】，进行了解事件的相关信息。

Event time	User name	Event name	Resource type	Resource name
▼ 2020-02-27 11:51:28	roleUser	CreateListener	clb	
access key		CAM Error Code	0	
Event ID	f	Event Region	ap-guangzhou	
Event name	CreateListener	Event source	c	
Event time	2020-02-27 11:51:28	Request ID		
Source IP address		User name		
Resource Region	gz			
View event				

配置访问日志到 CLS

最近更新时间：2020-11-12 15:07:39

负载均衡支持配置七层（HTTP/HTTPS）访问日志（Access Log），访问日志可以帮助您了解客户端请求、辅助排查问题、分析梳理用户行为等。当前访问日志支持存储到 CLS 中，支持分钟粒度的日志上报，在线多规则检索。

负载均衡的访问日志主要用于故障排查，帮助业务快速定位问题。访问日志功能包括日志上报、日志存储和查询：

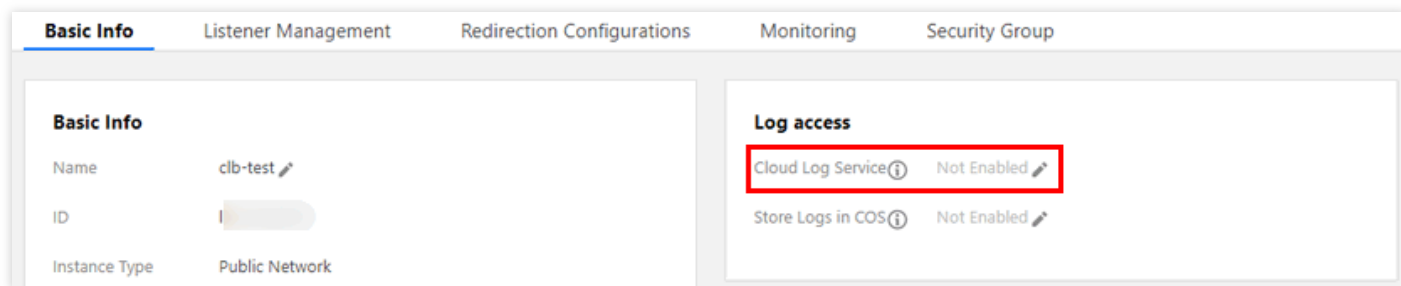
- 日志上报，提供尽力而为服务（Best-Effort Service），优先保障业务转发，再保障日志上报。
- 日志存储和查询，按当前使用的存储服务来提供服务保障 SLA。

说明：

- 当前负载均衡仅七层协议（HTTP/HTTPS）支持配置访问日志到 CLS，四层协议（TCP/UDP/TCP SSL）不支持配置访问日志到 CLS。
- 负载均衡配置访问日志到 CLS 的功能免费，用户仅需支付日志服务CLS的费用。
- 支持配置负载均衡访问日志到 CLS 的地域包括：广州、上海、南京、北京、重庆、成都、中国香港、新加坡、孟买、硅谷、多伦多、东京、法兰克福，可直接在控制台使用或通过 API 配置。

开启访问日志存入 CLS

1. 登录 [负载均衡控制台](#)。
2. 单击需进行配置的负载均衡 ID，进入“负载均衡基本信息”页面。
3. 在“日志访问”模块，编辑日志服务 CLS。



4. 在弹出框中，开启访问日志，并选择存储访问日志的日志集和日志主题。如您没有创建日志集或日志主题，请 [新建相关资源](#) 后，再选取具体的存储位置。

Modify CLS Log Storage Location

Enable log

Logset

Log Topic

In case of no suitable logsets, you may go to [Cloud Log Service Create](#)

Submit

Close

- 5. 单击【提交】，访问日志会被收集在对应的主题中。
- 6. 配置完成后单击日志集或日志主题将跳转到 CLS 的日志检索页面。
- 7. （可选）若想关闭访问日志，可再次编辑日志服务 CLS，在弹框中进行关闭并提交即可。

查询访问日志

步骤1：配置日志主题的索引

说明：

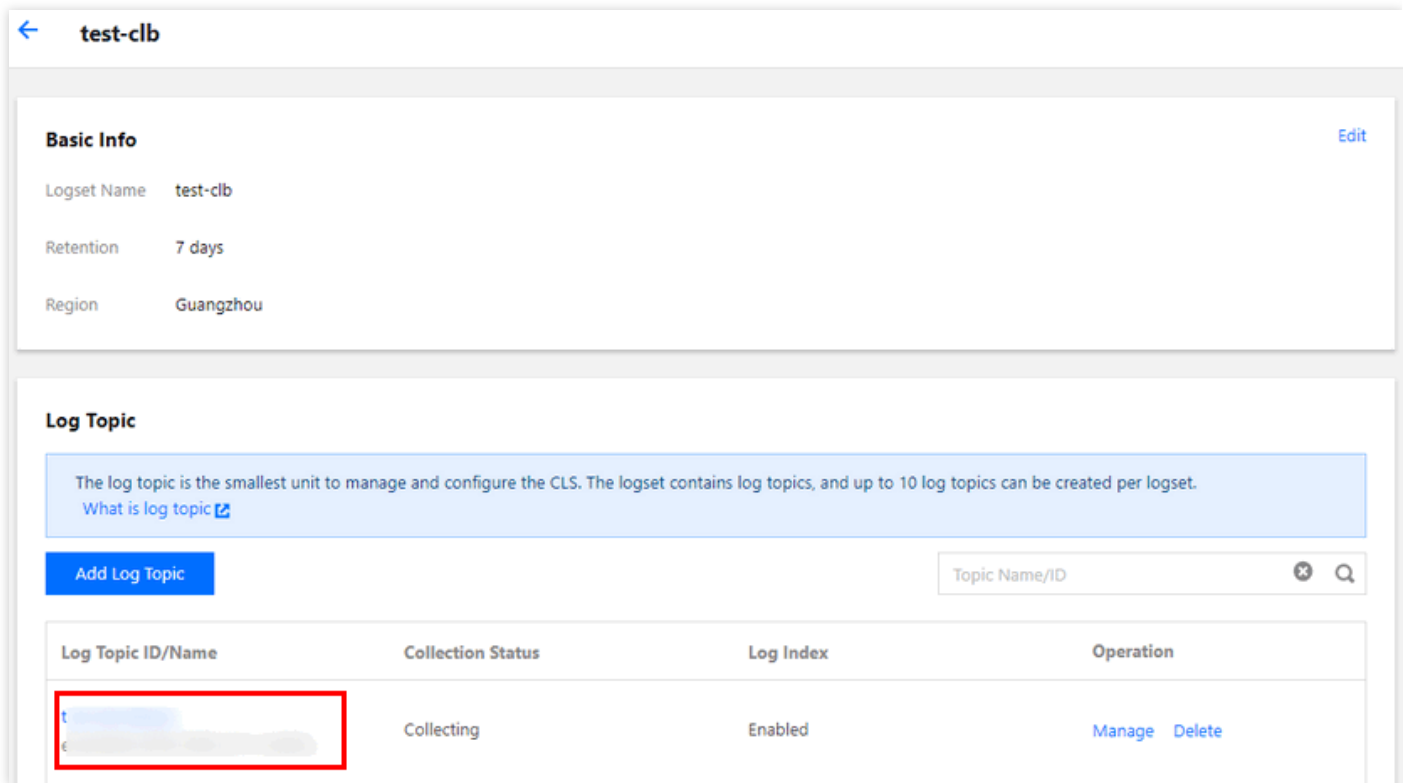
日志主题必须配置索引，否则检索不到日志。

建议配置的索引如下：

键值索引	字段类型	分词符
server_addr	text	无需配置分词符
server_name	text	无需配置分词符
http_host	text	无需配置分词符
status	long	-
vip_vpcid	long	-

具体操作如下：

1. 登录 [日志服务控制台](#)。
2. 在左侧导航中，选择【日志集管理】，进入“日志集管理”列表页。
3. 单击日志集 ID，进入日志集详情页。
4. 在日志集详情页，单击日志主题 ID，进入日志主题详情页。



5. 在日志主题详情页，选择【索引配置】选项卡，您可以在日志变量中选取部分变量，按需配置索引字段，配置说明请参见 [开启索引](#)。

← t

Basic InfoCollection ConfigurationIndex ConfigurationShipping ConfigurationKafka Consumption

1. The modified index configuration is only effective for newly written data, and have no impact on the index of the existed data.
2. Delimiter cannot be letters, numbers or Chinese characters. For whitespace characters, such as "\t" "\n" "\r", escaping is required. For other characters, escaping is not required.

Index Configuration

Index Status ☒

Full-Text Index ☒ ☒ Case-sensitive

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

Key-Value Index ☒ ☐ Case-sensitive

Key-Value Index	Field Type	Delimiter	Operation
remote_addr	text	<input <>="" ',="" ?\ ;:\n\t\""="" type="text" value="!@#%^&*()-_="/>	Delete
remote_port	text	<input <>="" ',="" ?\ ;:\n\t\""="" type="text" value="!@#%^&*()-_="/>	Delete
status	long	-	Delete

6. 索引配置完成后结果如下图所示。

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

步骤2：检索访问日志

1. 登录 [日志服务控制台](#)。
2. 在左侧导航中，选择【检索分析】，进入“检索分析”页面。
3. 在“检索分析 ”页面中，选择日志集、日志主题和时间范围，单击【检索分析】，即可检索 CLB 上报到 CLS 的访问日志。检索语法详情请参见 [语法与规则](#)。

Logset: test-clb Log Topic: test-clb-theme Time Range: Last 15 Minutes

Raw Data

Enter the keyword to search. [Search Analysis](#) [Search Syntax](#)

Log Time ↑	Log Data ↔
2020-04-20 14:33:25	<pre>_TOPIC__tr _SOURCE__1 _FILENAME__access.log bytes_sent:242 connection:4 connection_requests:1 http_host:1 http_referer:- http_user_agent:Mozilla/5.0 zgrab/0.x protocol_type:https proxy_host:- remote_addr:1 remote_port:4 request:GET / HTTP/1.1 request_length:109 request_time:0.000 server_addr:1 server_name: server_port: ssl_cipher:E ssl_handshake_time:0:0:0:0:0:0 ssl_protocol:TLSv1.2 ssl_session_reused: status:200 stgw_engine_connect_time:2 stgw_engine_response_time:7 stgw_request_id:1 tcpinfo_rtt: time_local:20/Apr/2020:14:33:24 +0800 upstream_addr:- upstream_connect_time:- upstream_header_time:- upstream_response_time:- upstream_status:- via_stgw_engine:e vip_vpcid:-1 vsvc_id:f</pre>

日志格式及变量说明

日志格式

```
[$stgw_request_id] [$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]
```

字段类型

目前日志服务支持如下三种字段类型：

名称	类型描述
text	文本类型
long	整型数值类型（Int 64）
double	浮点数数值类型（64 bit）

日志变量说明

变量名	说明	字段类型
stgw_request_id	请求 ID。	text
time_local	访问的时间与时区，例如，“01/Jul/2019:11:11:00 +0800”，最后的“+0800”表示所处时区为 UTC 之后的8小时，即为北京时间。	text
protocol_type	协议类型（HTTP/HTTPS/SPDY/HTTP2/WS/WSS）。	text
server_addr	请求的目的 IP。	text
server_port	请求的目的端口。	long
server_name	规则的 server_name，即服务器名称。	text
remote_addr	客户端 IP。	text
remote_port	客户端端口。	long
status	CLB 返回给客户端的状态码。	long
upstream_addr	RS 地址。	text
upstream_status	RS 返回给 CLB 的状态码。	text
proxy_host	stream ID。	text
request	请求行。	text
request_length	从客户端收到的请求字节数。	long
bytes_sent	发送到客户端的字节数。	long
http_host	请求域名。	text
http_user_agent	HTTP 协议头的 user_agent 字段。	text

变量名	说明	字段类型
http_referer	HTTP 请求来源。	text
request_time	请求处理时间：从收到客户端的第一个字节开始，直到给客户端发送的最后一个字节为止，包括客户端请求到 CLB、CLB 转发请求到 RS、RS 响应数据到 CLB、CLB 转发数据到客户端的总时间。	double
upstream_response_time	整个后端请求所花费时间：从开始 CONNECT RS 到从 RS 接收完应答的时间。	double
upstream_connect_time	和 RS 建立 TCP 连接所花费时间：从开始 CONNECT RS 到开始发送 HTTP 请求的时间。	double
upstream_header_time	从 RS 接收完 HTTP 头部所花费时间：从开始 CONNECT RS 到从 RS 接收完 HTTP 应答头部的时间。	double
tcpinfo_rtt	TCP 连接的 RTT。	long
connection	连接 ID。	long
connection_requests	连接上的请求个数。	long
ssl_handshake_time	SSL 握手所花费时间。	double
ssl_cipher	SSL 加密套件。	text
ssl_protocol	SSL 协议版本。	text
vip_vpcid	负载均衡 VIP 的所属私有网络 ID。	long

配置访问日志到 COS

最近更新时间：2020-07-02 18:05:37

⚠ 注意：

配置访问日志到 COS 将于2020-05-15 00:00:00关闭新增（其中广州地域将于2020-04-26 00:00:00关闭新增），所有地域将于2020-06-30 00:00:00正式下线该功能，详情请参见 [CLB 配置访问日志到 COS 功能下线公告](#)，请使用升级版功能：[配置访问日志到 CLS](#)。

负载均衡支持配置七层（HTTP/HTTPS）访问日志（Access Log），访问日志可以帮助您了解客户端请求、辅助排查问题、分析梳理访问数据等。当前访问日志支持存储到 COS 中下载分析，支持的地域包括广州、上海、北京、中国香港、上海金融和深圳金融。

负载均衡的访问日志主要用于故障排查，帮助业务快速定位问题。访问日志功能包括日志上报、日志存储和查询：

- 日志上报，提供尽力而为服务（Best-Effort Service），优先保障业务转发，再保障日志上报。
- 日志存储和查询，按当前使用的存储服务来提供服务保障 SLA。

📖 说明：

- 当前日志聚合粒度为1小时，日志数据的传输会有一定的延迟。
- 当前负载均衡仅支持公网七层（HTTP/HTTPS）日志的存储和下载，不支持四层（TCP/UDP）和内网七层日志的存储和下载。
- 负载均衡配置访问日志到 COS 的功能免费，用户仅需支付对象存储 COS 的费用，COS 面向所有新用户有一定量的免费额度，详情请参见 [免费额度](#)。
- 在支持配置访问日志到 COS 的地域中，若您不开启访问日志，腾讯云默认为您保留3天的日志；若您开启访问日志，存储时间则依 COS 存储而定。其他地域暂不支持配置访问日志。

开启访问日志存入 COS

1. 登录 [负载均衡控制台](#)。
2. 在“负载均衡”列表页面，单击想要配置的负载均衡 ID，进入“负载均衡基本信息”页面。
3. 在“访问日志”模块，编辑日志存入 COS。
4. 在弹出框中，开启访问日志，并选择相应 COS 中的存放 bucket。如您没有创建COS 的 bucket，请 [新建 bucket](#) 后，选取相应的存储位置。

- 5. 点击【提交】，请求日志会自动在 bucket 下，创建以 lb-id 为名称的文件夹进行存储。
- 6. 配置完成后，单击 bucket 地址可以直接跳转到日志下载页面。

关闭访问日志存入 COS

- 1. 登录 [负载均衡控制台](#)。
- 2. 在"负载均衡"列表页面，单击想要配置的负载均衡 ID，进入“负载均衡基本信息”页面。
- 3. 在“访问日志”模块，编辑日志存入 COS。
- 4. 在弹出框中，关闭访问日志， 点击【提交】 即可 。

关闭后将不支持再开启 COS 日志， 详见 [关于CLB配置访问日志到COS下线的公告](#)。

日志格式及变量说明

日志格式

```
[${stgw_request_id}] [${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}] [${upstream_header_time}] [${tcpinfo_rtt}] [${connection}] [${connection_requests}] [${ssl_handshake_time}] [${ssl_cipher}] [${ssl_protocol}] [${ssl_session_reused}]
```

日志变量说明

变量名	说明
stgw_request_id	请求 ID。
time_local	访问的时间与时区，例如“01/Jul/2019:11:11:00 +0800”，最后的“+0800”表示所处时区为 UTC 之后的8小时，即为北京时间。
protocol_type	协议类型（HTTP/HTTPS/SPDY/HTTP2/WS/WSS）。
server_addr:server_port	请求的目的 IP 和目的端口。

变量名	说明
server_name	规则的 server_name，即服务器名称。
remote_addr:remote_port	客户端 IP和客户端端口。
status	CLB 返回给客户端的状态码。
upstream_status	RS 返回给 CLB 的状态码。
proxy_host	stream ID。
request	请求行。
request_length	从客户端收到的请求字节数。
bytes_sent	发送到客户端的字节数。
http_host	请求域名。
http_user_agent	HTTP 协议头的 user_agent 字段。
http_referer	HTTP 请求来源。
request_time	请求处理时间：从收到客户端的第一个字节开始，直到给客户端发送的最后一个字节为止，包括客户端请求到 CLB、CLB 转发请求到 RS、RS 响应数据到 CLB、CLB 转发数据到客户端的总时间。
upstream_response_time	整个后端请求所花费时间：从开始 CONNECT RS 到从 RS 接收完应答的时间。
upstream_connect_time	和 RS 建立 TCP 连接所花费时间：从开始 CONNECT RS 到开始发送 HTTP 请求的时间。
upstream_header_time	从 RS 接收完 HTTP 头部所花费时间：从开始 CONNECT RS 到从 RS 接收完 HTTP 应答头部的时间。
tcpinfo_rtt	TCP 连接的 RTT。
connection	连接 ID。
connection_requests	连接上的请求个数。
ssl_handshake_time	SSL 握手所花费时间。
ssl_cipher	SSL 加密套件。
ssl_protocol	SSL 协议版本。

变量名	说明
ssl_session_reused	SSL SESSION 复用。