Alibaba Cloud Server Load Balancer

Log management

Issue: 20190725

MORE THAN JUST CLOUD | C-J Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

- 1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
- 2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
- 3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
- 4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

- 5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
- 6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
A	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	• Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the cd / d C :/ windows command to enter the Windows system folder.
Italics	It is used for parameters and variables.	bae log list instanceid Instance_ID
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	ipconfig [-all -t]

Style	Description	Example
{} or {a b}	It indicates that it is a required value, and only one item can be selected.	<pre>swich {stand slave}</pre>

Contents

Legal disclaimer	I
Generic conventions	I
1 View operation logs	1
2 Manage health check logs	3
3 Authorize a RAM user to use access logs	
4 Configure access logs	14

1 View operation logs

You can view the logs of operations performed on SLB instances, HTTP listeners and server certificates in the past one month.

Context

The operation logs are recorded in ActionTrail. ActionTrail records the operations acted upon your Alibaba Cloud resources. You can query operation records and store the records to OSS.

Procedure

- 1. Log on to the SLB console.
- 2. In the left-side navigation pane, click Logs > Operation Log.
- 3. Click View Operation Logs.

- 4. On the History Search page, complete these steps to view operation logs:
 - a) Select Resource Type as a filter.
 - b) Select the SLB resource of which operation logs you want to view.

In this tutorial, LoadBalancer is selected.

Hist	ory Search							${old C}$ Refresh
Find	Find operations over the past 30 days in your cloud account involving resource creation, modification and deletion.							
Filter	Resource Type V	1	EventType Write	e v Time May	23, 2018 t	0 June 21, 2018	Search	
0	Event time	Metric	ame	Event Name	Resource Type	Resource Name		Error Code
•	Thursday, 21 June 20:	SLB		ConsoleSignin				
•	Thursday, 21 June 20	LoadBalancer		ConsoleSignin				
•	Thursday, 21 June 20:	ServerCertificate		ConsoleSignin				

c) Select an event type.

In this tutorial, All is selected.

- d) Select the time range to search.
- e) Click Search to view logs of operations performed on the selected resource.

Expand a record to view more detailed information.

His	story Search							\mathcal{C} Refresh	
Fir	Find operations over the past 30 days in your cloud account involving resource creation, modification and deletion.								
Filter	Resource Type V	adBalancer	EventType Write v	Time May 23, 2018	to	June 21, 2018	Search		
0	Event time	Username E	ivent Name	Resource Type	Resource Nam	e	Error Code		
•	Tuesday, 19 June 2018, 12.38.41 AM	root C	CreateDomainExtension	LoadBalancer	lb-1ud31bltkhv	vwjnwe3c5k0			
	Access key:				Event source:	slb-openapi-share.a	liyuncs.com		
	Region:	cn-hangzhou			Event Time:	Tuesday, 19 June 2	018, 12.38.41 AM		
	Error Code:				Request ID:	115E5A4E-4083-410	03-A301-8D62E2F1BF81		
	Event ID:	115E5A4E-4083-41	03-A301-8D62E2F1BF81	Sour	ce IP address:	61.149.173.169			
	Event Name:	CreateDomainExter	nsion		Username:	root			
	Related Resources (1)								
	LoadBalancer Ib-1ud31bltkhwwjnwe3c5k0						v	iew event	

2 Manage health check logs

You can view the health logs of Server Load Balancer (SLB) within three days on the Health Check Logs page. If you want to get health check logs generated three days or longer before, you can store the health check logs to OSS and download complete health check logs.

Store health check logs

You can view the health check logs of backend servers by using the health check log function of SLB. Currently, logs in the past three days are provided. If you want to view more logs, store the health check logs to OSS buckets.

You can enable and disable the storage function at any time. After the storage function is enabled, SLB will create a folder named *AliyunSLBH* ealthCheck

Logs in the selected bucket to store health check logs of SLB. Health check logs are generated on an hourly basis and the system will create a subfolder named after the date to store the log files generated in that day, for example, 20170707.

The log files generated in each hour of a day are named after the time when they are generated. For example, the file name of a log file generated between 00:00-01:00 is $01 \cdot txt$ and the file name of a log file generated between 01:00-02:00 is $02 \cdot txt$

Note:

Health check logs are generated only when backend servers are abnormal. If no failures occur to backend servers in an hour, no health check logs are generated in that hour.

To store health check logs, follow these steps:

- 1. Create a bucket
- 2. Authorize SLB to access OSS
- 3. Configure log storage

Step 1 Create a bucket

- 1. Open the OSS product page and click Buy Now to activate the OSS service.
- 2. Log on to the OSS console.

3. Click Create Bucket.

Object Storage	Basic Data			Get Started Developer Guide Download SDK More ▼
Overvie Create Bucket	() Data in the Overview page and Bucket Overview			
Bucket + 1 3	Storage Used Total Used 🗸	Internet Traffic This Inbound V	Requests This PUT ✓	13 buckets Create Bucket AccessKey
celcom-bigdata-dem cjitest-inti document-test	40.97 GB	251.54 MB Internet Traffic Last Month 2.21GB	632 Requests Last Month 8,995	0 alarm rules, 0 triggered, 0 alerts, 0 disabled Set Alarm Rule
 document-test1 ecsdoc-text 	Basic Settings			
example-company mytestbucket1234	Domain Names	Cross-Region Replication	Security Token Grant temporary access permissions to the sub-account	

4. In the Create Bucket dialog box, configure the bucket and click OK.

Note:

Make sure that the bucket and the SLB instance belong to the same region.

Step 2 Authorize SLB to access OSS

After creating a bucket, you must authorize the role (SLBLogDefa ultRole) to access OSS resources.

!) Notice:

The authorization is required only for the first time.

- 1. In the left-side navigation pane of the SLB console, click Logs > Health Check Logs.
- 2. Click 1. Activate OSS. if OSS has not been activated yet.
- 3. On the Health Check Logs page, click Authorize Now in the 2. Authorize the required RAM role. section.
- 4. Read the authorization description, and then click Confirm Authorization Policy.
- 5. Log on to the RAM console.
- 6. In the left-side navigation pane, click Roles, find the role named SLBLogDefaultRole, and then click Authorize.

7. In the Edit Role Authorization Policy dialog box, find the AliyunOSSFullAccess policy, click the policy, and then click OK.

Edit Role Authorization	Policy			X		
Roles added to this group have all the permissions of this group. A role cannot be added to the same group more than once.						
Search and Attach	Input and At	tach				
Available Authorizatio Names	on Policy					
	TypeQ					
AliyunOSSFullAccess		>				
		<				
-			Selected Authorization P Name	olicy		
			AliyunOSSFullAccess Provides full acce	Туре		
			ОК	Close		

After the authorization, click the role name of SLBLogDefaultRole, and then click the Role Authorization Policies tab to view the attached policy.

SLBLogDefaultRole			Edit Authorization Policy
Authorization Policy Name	Description	Туре	Actions
AliyunOSSFullAccess	Provides full access to Object Storage Service(OSS) via Management Console.	System	View Permissions Revoke Authorization

Step 3 Configure log storage

- 1. Log on to the SLB console.
- 2. In the left-side navigation pane, click Logs > Health Check Logs.
- 3. On the Health Check Logs page, click the Log Storage tab.

4. Find the target region and click Configure Log Storage.

Health Check Logs				
Logs Log Storage				
				G
Region	Status	Details	Actions	API
China (Hangzhou)		Bucket: xiangli-0	Configure Log Storage	

- 5. In the Configure Log Storage dialog box, select a bucket to store health check logs, and then click OK.
- 6. Turn on the status switch to enable log storage.

View health check logs

To view the health check logs generated in the past three days, follow these steps:

- 1. Log on to the SLB console.
- 2. In the left-side navigation pane, click Logs > Health Check Logs.
- 3. On the Health Check Logs page, click the Logs tab.



Health check logs are generated only when the health status of a backend server is abnormal. Health check logs are generated every one hour. If no failure occurs to backend servers in an hour, no health check logs are generated in that hour.

- The SLB_instan ce_IP : port to Added_ECS_ instance_I P : port abnormal ; cause : XXX log message indicates that the backend server is abnormal. Troubleshoot according to the detailed error message.
- The SLB_instan ce_IP : port to Added_ECS_ instance_I P : port normal log message indicates that the backend server becomes normal again.

	Health Check Logs						
	Logs Log Storage						
	() Note: Only log entries saved within the last	t three days are provided. To obtain mo	re log entries, go to LogStore				
	SLB Instance ID V Enter an SLB instance	e ID Q		G			
	Instance ID	Time	Details				
<	lb x	Apr 16, 2019, 15:07:54	[172.16.213.14]:443 to 172.16.32.254:80 abnormal; cause: check time out				

Download health check logs

You can download the completed health check logs stored in OSS buckets.

- 1. Log on to the OSS console.
- 2. On the Overview page, click the target bucket and then click Files.
- 3. On the Files page, click AliyunSLBH ealthCheck Logs /.

slb	Type Standard Storage	Region China Eas	st 1 (Hangzhou)	Created At 07/06/2017, 19:	13 Delete Bucket	
Overview Files Basic Settings De	omain Names Image	Processing Ever	nt Notification			
Basic Data Hotspot Statistics API Statistics Object Access Statistics						
Upload Create Directory Delete Set HTTI	P Header Fragments	Refresh		Enter th	e file name prefix Q	
File Name (Object Name)		File Size	Storage Clas	s Time Updated	Action	
AliyunSLBHealthCheckLogs/						
OssAttribute		0.057KB	Standard Sto	rage 07/25/2017, 11:2	2 Edit	
example.jpg		21.327KB	Standard Sto	rage 07/28/2017, 17:1	4 Edit	

4. Click the folder of the heath logs to download.

Preview \times Only image files support preview for now. caffe-volume File Name Use HTTPS URL https://caffe-bucket.oss-cn-hangzhou.aliyuncs.com/caffevolume Open File URL | Copy File URL | Copy File Path Туре application/octet-stream Set HTTP Header File ACL Inherited from Bucket Set ACL

5. Click Edit of the target folder. Then, click Copy File URL in the displayed page.

6. Enter the copied URL in the web browser to download the logs.

3 Authorize a RAM user to use access logs

Before a RAM user starts to use the access log function, the RAM user must be authorized by the corresponding Alibaba Cloud account.

Prerequisites

The account has enabled the access log function.

- 1. Log on to the RAM console by using the credentials of your account.
- 2. Click Roles to see whether the account has the AliyunLogArchiveRole.

If the account does not have this role, log on to the SLB console by using the credentials of the account, select Logs > Access Logs, click Authorize. In the displayed dialog box, click Confirm Authorization Policy.

Note:

This operation is required only at the first time.

Procedure

- 1. Create an authorization policy:
 - a) Log on to the RAM console by using the credentials of your account.
 - b) In the left-side navigation pane, click Policies, and then click Create Authorization Policy.

RAM	Policy Management		Create Authorization Policy	C Refresh
Dashboard Users	System Policy Custom Policy			
Groups	Policy Name or Description V Search K	eywords Search		
Roles	Authorization Policy Name	Description	Number of References	Actions
Settings	AdministratorAccess	Provides full access to Alibaba Cloud services and resources	7	View
	AliyunOSSFullAccess	Provides full access to Object Storage Service(OSS) via Mana	6	View

c) Click Blank Template.

Create Authorization Policy	×
Step 1: Select an Step 2: Edit p All Templates Enter keywords to dyn 	ermissions and Policy creation complete.
Blank Template	System AdministratorAccess Provides full access to
System AliyunOSSFullAccess Provides full access to	System AliyunOSSReadOnlyAccess Provides read-only acces
System AliyunECSFullAccess Provides full access to	System AliyunECSReadOnlyAccess Provides read-only acces
System AliyunRDSFullAccess Provides full access to	System AliyunRDSReadOnlyAccess Provides read-only acces

d) Enter a policy name, such as SlbAccessLogPolicySet, and then enter the following policy. Click Create Authorization Policy.

```
{
" Statement ":[
{
    " Action ":[
    " slb : Create *",
    " slb : List *"
    ],
    " Effect ": " Allow ",
    " Resource ": " acs : log :*:*: project /*"
},
{
    " Action ": [
    " log : Create *",
}
```

```
" log : List *"
    ],
" Effect ": " Allow ",
" Resource ": " acs : log :*:*: project /*"
 },
  {
     " Action ": [
        " log : Create *",
       " log : List *",
" log : Get *",
" log : Update *"
    ],
" Effect ": " Allow ",
" Resource ": " acs : log :*:*: project /*/ logstore /*"
 },
  {
    " Action ": [
" log : Create *",
       " log : List *",
" log : Get *",
" log : Update *"
    ],
" Effect ": " Allow ",
" Resource ": " acs : log :*:*: project /*/ dashboard /*"
 },
{
    " Action ": " cms : QueryMetri c *",
    " Resource ": "*",
" Effect ": " Allow "
 },
{
     " Action ": [
       " slb : Describe *",
" slb : DeleteAcce ssLogsDown loadAttrib ute ",
" slb : SetAccessL ogsDownloa dAttribute ",
" slb : DescribeAc cessLogsDo wnloadAttr ibute "
    ],
" Resource ": "*",
     " Effect ": " Allow "
 },
{
    " Action ": [
       " ram : Get *".
       " ram : ListRoles "
    J,
" Effect ": " Allow ",
    " Resource ": "*"
 }
],
" Version ": " 1 "
}
```

e) Click Close.

- 2. Attach the created policy to the RAM user:
 - a) In the left-side navigation pane, click Users.
 - b) Find the target RAM user (the user who uses the SLB access log function) and click Authorize.

RAM	User Management		Create User CRefresh
Dashboard	User Name V Search by User Name Search		
Groups	User Name/Display Name Description	Created At	Actions
Policies	zha zha	2017-11-01 11:26:17	Manage Authorize Delete Join Group

c) Search the created authorization policy and attach the policy to the RAM user.

Edit User-Level Authorization				×
Members added to this group added to the same group more	have all the re than once.	permissions	of this group. A member cannot b	e
Available Authorization Policy	Names			
	TypeQ			
SLB 👤		3		
AliyunSLBFullAccess Provides full acce	System	>		
AliyunSLBReadOnlyAccess Provides read-only	2 ^{System}		Selected Authorization Policy Na	me
SlbAccessLogPolicySet	Custom			Туре
]		
			OK	Close

d) Click OK.

Members added to this group added to the same group mor	have all the re than once	permissions	of this group. A member can	not be
Available Authorization Policy	Names			
	TypeQ			
SLB				
AliyunSLBFullAccess Provides full acce	System	>		
AliyunSLBReadOnlyAccess Provides read-only	System		Selected Authorization Polic	y Name
				Туре
			SlbAccessLogPolicySet	Custom

e) Go back to the user details page to check whether the policy has been attached to the target RAM user.

<	zhar				Edit Authorization Policy
User Details					
User Authorizatio	User-Level Authorization	Group-Level Authorization			
User Groups	Authorization Policy Name		Description	Туре	Actions
	SIbAccessLogPolicySet		-	Custom	View Permissions Revoke Authorization

4 Configure access logs

This topic describes how to configure access logs. By using Alibaba Cloud Log Service, you can analyze the access logs of a Server Load Balancer (SLB) instance to understand the behavior and geographical distribution of client users and troubleshoot problems.

What are access logs?

Access logs collect detailed information of all requests sent to an SLB instance, including the request time, client IP address, latency, request URL, and server response. As the entry of Internet access, SLB receives massive client requests. You can use access logs to analyze user behavior and geographical distribution, and troubleshoot problems.

After you enable the SLB access log feature, you can store access logs in the Logstore of Log Service to collect and analyze the access logs. You can also disable the access log feature at any time.

SLB access logs can be used free of charge. You only need to pay for fees incurred by the use of Log Service.



- Only Layer-7 SLB supports access logs and the access log function is available in all regions.
- Make sure that the HTTP header value does not contain ||. Otherwise, the exported logs may be misplaced.

Benefits

The following are benefits of SLB access logs:

· Easy to use

The access log function frees developers and maintenance staff from tedious and time-consuming log processing so that they can concentrate on business development and technical research.

Cost-effective

Access logs are typically massive. Processing access logs takes a lot of time and consumes a lot of resources. With Log Service, the processing of access logs is faster and cost-effective than self-built open-source solutions. Log Service can analyze one hundred million logs in one second.

· Real-time

Scenarios such as DevOps, monitoring, and alerting require real-time log data . Traditional data storage and analysis tools cannot meet this requirement. For example, it takes a long time to ETL data to Hive where a lot of time is spent on data integration. Powered by its powerful big data computing capability, Log Service can process and analyze access logs in seconds.

Flexible

You can enable or disable the SLB access log feature according to the instance specification. Additionally, you can set the storage period (1 to 365 days) as needed and the Logstore's capacity is scaleable to meet increasing service demands.

Configure access logs

Before you configure access logs, make sure that:

- A Layer-7 listener is added.
- Log Service is activated.

To configure access logs, complete these steps:

- 1. Log on to the SLB console.
- 2. In the left-side navigation pane, choose Logs > Access Logs.
- 3. Select a region.
- 4. Click Authorize, and then click Confirm Authorization Policy to authorize SLB to write logs to Log Service.

If you are a RAM user, you must obtain permissions from the corresponding account. For more information, see Authorize a RAM user to use access logs.



This step is required only at the first time.

5. On the Access Logs page, find the target SLB instance and click Configure Logging.

6. Select the LogProject and LogStore and then click OK.

If there is no available LogStore, click Log Service console to create log projects.

Note:

Make sure that the name of the LogProject is globally unique and the region of the LogProject is the same as that of the SLB instance.

LogProject	
Select	~
LogStore	
Select	~

Search and analyze access logs

After configuring SLB access logs, you can search and view logs by using the following indexing fields.

Field	Description
body_bytes_sent	The size of HTTP body (in byte) sent to the client.
client_ip	The client IP address.

Field	Description
host	The host header in the request.
http_user_agent	The received http_user_agent header in the request.
request_length	The length of the request including startline, HTTP header, and HTTP body.
request_method	The request method.
request_time	The interval of time from when SLB receives the first request to the time when SLB returns a response.
request_uri	The URL of the received request.
Slbid	The ID of the SLB instance.
status	The status of the SLB response.
Upstream_addr	The IP address and port number of the backend server.
upstream_response_time	The interval of time from when SLB establishes a connection with the backend server to the time when SLB receives the last byte of the response.
upstream_status	The response status code of the backend server received by SLB.

Search access logs

To search access logs, complete these steps:

- 1. Go to the log search page. You can navigate to the search page from the SLB console or the Log Service Console:
 - From the SLB console:

On the Access Logs page, click View Logs.

	Acce	ess Logs (Layer-7)					
	SLB In	stance ID 🗸 Enter a value	Q				C
		Instance Name/ID	IP Address ₽	Network Type 🙄	Status ਊ	Storage Path	Actions
		SLB1 Ik	5(Public Network)	Classic Internal Network	✓ Active		Configure Logging
<		SLB99 Ib-	4 17(Public Network)	Classic Internal Network	✓ Active		Configure Logging
		slb_worder lb	4 6(Public Network)	Classic Internal Network	✓ Active	w wd	View Logs Delete

• From the Log Service Console:

On the Logstores page, click Search of the target Logstore.

<	slb-test sack to Project List	Region : China North 3 (Zhangjiako
Logstores	Logstores	Learning Path Endpoints Create
 LogHub - Collect 	Enter a Londore name to Search Search	
[Doc] Collection Hel		Log Consumption Mode
Logtail Config	Logstore Name Data Import Monitor Log Collection Mode Wizard	Log
Logtail Machine Grou		Consumption Log Shipper LogSearch
 LogHub - Consume 	slb_logstore 🛢 🗠 Logtail Config (Manage) Diagnose More+	Preview MaxCompute OSS Search Modify Delete
[Doc] Consumption H		Total: 1 item(s), Per Page: 10 v item(s) « < 1 > »

- 2. Click the target log field to view detailed information.
- 3. Enter an SQL statement to query access logs.

For example, enter the following SQL statement to query the Top20 clients, which is used for analyzing the request source to assist business decision-making.

* | select ip_to_prov ince (client_ip) as client_ip_ province , count (*) as pv group by

	client_ip_	province	order	by	pv	desc	limit	50
₿ layer7log	(Belong to accesslogslb)			:	Share Ind	lex Attributes	Saved to Savedsearch	Saved to alarm
* select http_user	_agent, count(*) as pv group by http_us	er_agent order by pv desc limit 20		0	1hour	∨ 2018-02-0	09 09:58:20 ~ 2018-02-09	Search
60k								_
	أوحدكا وحدده	a Manan.						
09:58:40	10:09:30	10:20:30	10:	31:30	1	0:42:30	10:53:30	
Raw Data	Graph	http_user_ag	ent × v 🗧	Y pv	× v			IJ.
TS-HLIENT								
Mozil37.36								
Go-htt/1.1								
Mozil37.36						_		
axios/0.17.1								
Flink-ak/sk								
DalviCNDL)			_					
Mozil37.36								
Alicdimea2		alvik/1.6.0 (Linux; U; Android 4.4	4; 2014811 MIUI/V8	.2.1.0.KHJCNDL)			
Mozilscan		pv: 52686						

Analyze access logs

You can analyze access logs through the dashboard, which provides rich graphic information.

To analyze access logs, complete these steps:

- 1. In the Log Service console, click the project link of the SLB instance.
- 2. In the left-side navigation pane, choose LogSearch/Analytics Query > Dashboard, and then click the name of the access log.

<	slb-test tBack to Project List	Region : China North 3 (Zhangjiakou)
Logstores	Dashboard	Endpoints
 LogHub - Collect 	Curt.	
[Doc] Collection Hel	Search	
Logtail Config	Dashboard Name	Actions
Logtail Machine Grou	slb_logstore-slb_layer7_access_center	Delete
 LogHub - Consume 	slb_logstore-slb_layer7_operation_center	Delete

Disable the access log function

To disable the access log function, complete these steps:

- 1. Log on to the SLB console.
- 2. In the left-side navigation pane, choose Logs > Access Logs.
- 3. Select the region of the target SLB instance.

4. On the Access Logs page, find the target instance and click Delete.

	Access Logs (Layer-7)						
~	SLB In	stance ID 💛 Enter a value	Q				G
		Instance Name/ID	IP Address 🖓	Network Type 🟆	Status 🖓	Storage Path	Actions
		SLB1 It	5(Public Network)	Classic Internal Network	✓ Active		Configure Logging
		SLB99 Ib-	4 17(Public Network)	Classic Internal Network	✓ Active		Configure Logging
		slb_worder Ib	4 6(Public Network)	Classic Internal Network	✓ Active	w	View Logs Delete

5. In the displayed dialog box, click OK.