ALIBABA CLOUD

Alibaba Cloud

Server Load Balancer

Log management

Document Version: 20220420

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.View operation logs

The operation log feature of is used to record activities in within your Alibaba Cloud account. After you enable the feature, records are generated when you access or manage the CLB service.

Context

The operation log feature of is integrated with the event management feature of ActionTrail. ActionTrail is a service that monitors and records activities within your Alibaba Cloud account. Records are generated when you use the Alibaba Cloud Management Console, call APIs, or use SDKs to access or manage services on Alibaba Cloud.

Query logs

1.
2. In the left-side navigation pane, choose **Log Management > Operation Logs**.
3. On the **Operation Logs** page, perform the following operations to query logs:
   i. Select an event type.

Event type	Supported option
Read-Write Type	Valid values: **Write** and **Read**.
User Name	Enter an account type. For example, *root* specifies your Alibaba Cloud account.
Resource Type	Select a resource type.

   ii. Select a time period. You can query data collected in the last 90 days.
   iii. Click Q to query the logs.
4. Find the event that you want to manage and click the + icon.
5. View detailed information about the event.
   i. Click **Event Detail**.
   ii. The **Event Details** message displays the record in XML. You can click the icon to copy the record and save the record as needed. For example, you can save the record in local storage.

2.Health check logs

2.1. Store health check logs

You can view health check logs generated in the last three days on the **Health Check Logs** page. To view health check logs earlier than three days, you must download the complete health check logs and store them in an Object Storage Service (OSS) bucket.

Context

You can view the health check logs of backend servers by using the log management feature of Server Load Balancer (SLB). SLB retains health check logs only for the last three days. To store health check logs for longer, you can store them in an OSS bucket.

You can enable and disable the log storage feature at any time. After log storage is enabled, SLB creates a folder named *AliyunSLBHealthCheckLogs* in the selected bucket to store health check logs. Health check logs of SLB instances are generated on an hourly basis. The system automatically creates a subfolder whose name corresponds to the date of the stored health check log files. For example, a subfolder may be named *20170707*.

The log files generated each hour are named after the time at which they are generated. For example, a health check log file generated from 00:00 to 01:00 is named *01.txt*, and a health check log file generated from 01:00 to 02:00 is named *02.txt*.

> **Note** Health check logs are generated only when the health status of a backend server is abnormal. Health check logs are generated on an hourly basis. If no exceptions are detected on the backend server within an hour, no health check logs are generated for that hour.

Step 1: Create a bucket

1. On the OSS product page, click **Activate OSS**.
2. Log on to the OSS console.
3. Click **Create Bucket**.
4. In the **Create Bucket** panel, configure parameters and click **OK**.

> **Note** Make sure that the bucket and the SLB instance are in the same region.

Step 2: Authorize SLB to access OSS

After you create a bucket, you must authorize the `SLBLogDefaultRole` role to access OSS resources.

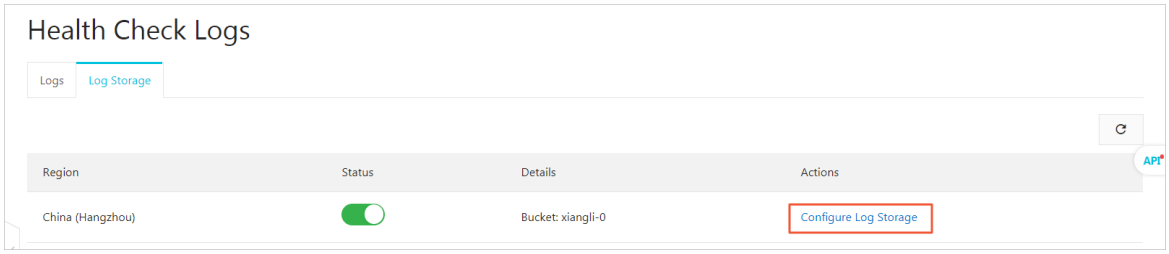
> **Notice** Authorization is required only when you configure log storage for the first time.

1. Log on to the SLB console.
2. In the left-side navigation pane, choose **Logs > Health Check Logs**.
3. On the **Health Check Logs** page, click the **Log Storage** tab.
4. Click **1. Activate OSS**.
5. After OSS is activated, click **Activate Now** in the **2. Authorize the required RAM role** section.

6. On the **Cloud Resource Access Authorization** page, read the authorization description and click **Confirm Authorization Policy**.
7. Log on to the Resource Access Management (RAM) console.
8. In the left-side navigation pane, click **RAM roles**, find the SLBLogDefaultRole role, and then click **Add Permissions** in the Actions column.
9. In the **Add Permissions** panel, set Select Policy to **System Policy**, select the **AliyunOSSFullAccess** policy from the list, and then click **OK**.
10. Click **Complete**.

Step 3: Configure log storage

1.
2.
3. In the left-side navigation pane, choose **Logs > Health Check Logs**.
4. On the **Health Check Logs** page, click the **Log Storage** tab.
5. Click **Configure Log Storage** corresponding to a region.



6. In the **Configure Log Storage** panel, select the bucket that you created and set Log Type to Health Check Log.
7. Click **OK**.
8. Turn on the switch in the **Status** column to enable log storage.

2.2. View health check logs

You can view health check logs generated in the last three days in the SLB console.

Procedure

1.
2.
3. In the left-side navigation pane, choose **Logs > Health Check Logs**.
4. On the **Health Check Logs** page, click the **Logs** tab.

> **Note** Health check logs are generated only when the health status of a backend server is abnormal. Health check logs are generated on an hourly basis. If no exception is detected on the backend server within an hour, no health check logs are generated for that hour.

- If the entry `SLB_instance_IP:port to Added_ECS_instance_IP:port abnormal; cause:XXX` is displayed in the health check log, the health status of the backend server is abnormal. Troubleshoot based on the detailed error message.

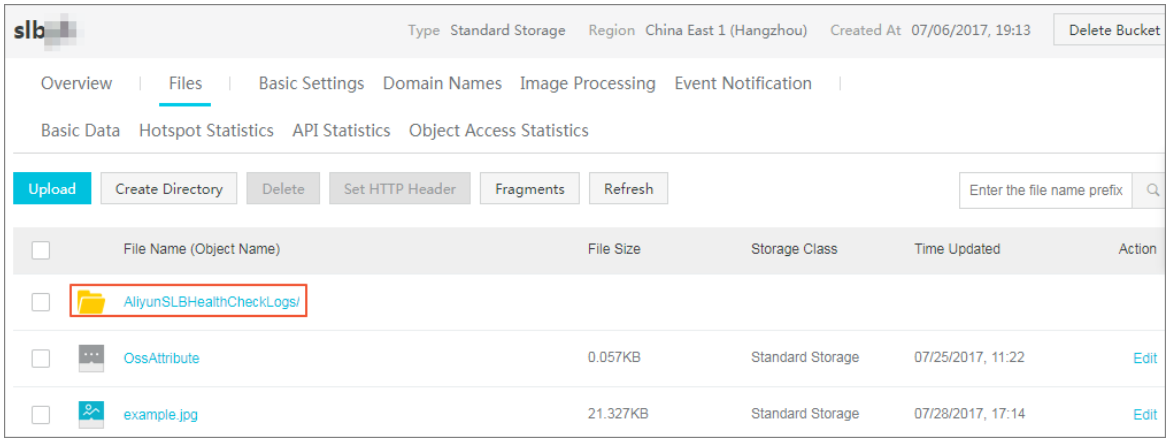
- If the entry `SLB_instance_IP:port to Added_ECS_instance_IP:port normal` is displayed in the health check log, the health status of the backend server becomes normal again.

2.3. Download health check logs

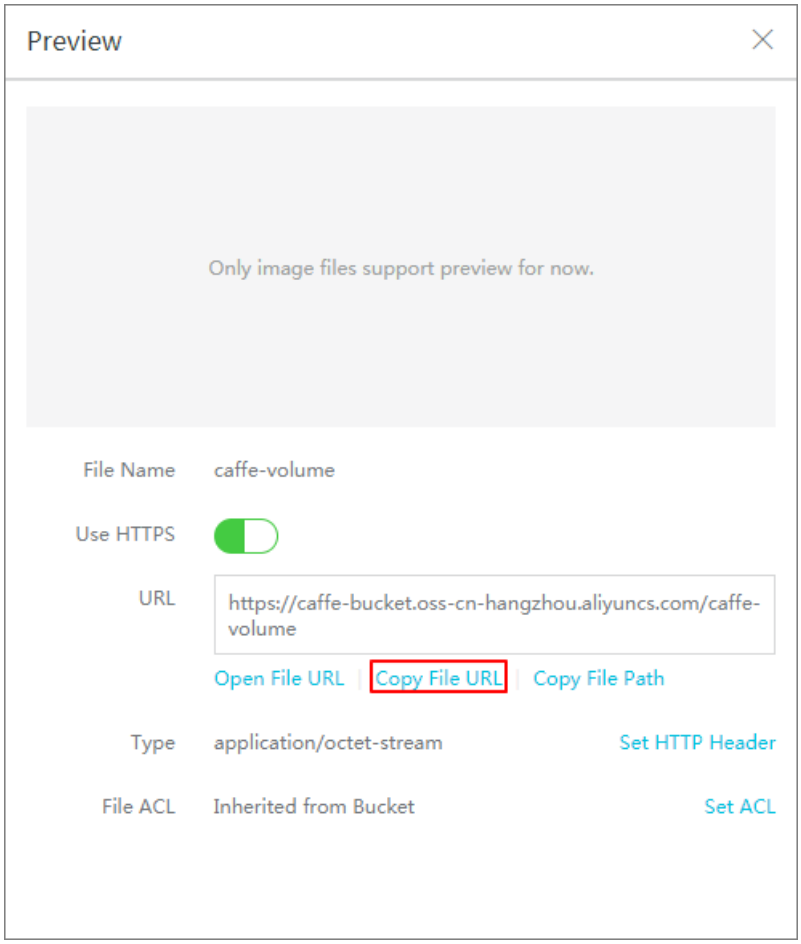
You can download health check logs of Server Load Balancer (SLB) instances in the Object Storage Service (OSS) console.

Procedure

1. Log on to the OSS console.
2. On the **Overview** page, click View Buckets in the Bucket Management section. On the Buckets page, click the name of the bucket where health check logs are stored. On the bucket management page, click **Files** in the left-side navigation pane.
3. On the **Files** page, click the *AliyunSLBHealthCheckLogs/* folder.



4. Click the folder of the heath log that you want to download.
5. Find the health log file and click **View Details** in the Actions column. In the panel that appears, click **Copy**.



6. Enter the copied URL in the browser to download the log.

3.Access logs

3.1. Overview of the access log feature

This topic provides an overview of the access log feature of Server Load Balancer (SLB). You can analyze access logs to better understand the activities and geographical distribution of client users and troubleshoot issues.

Overview

You can activate the access log feature of SLB to record detailed information of all requests sent to SLB instances, including the time when requests are sent, client IP addresses, latency, request URLs, and server responses. As an Internet access point, SLB distributes a large number of access requests. You can use access logs to analyze the activities and geographical distribution of client users and troubleshoot issues.

After you enable the access log feature of SLB, you can store access logs in the Logstores of Alibaba Cloud Log Service for log collection and analysis. You can disable the access log feature at any time.

No extra fee is charged for the access log feature of SLB. You only need to pay for Log Service.

> **Notice**
>
> - The access log feature can only be applied to Layer 7 SLB. This feature is available in all regions.
> - Make sure that the HTTP header value does not contain `||`. Otherwise, the exported logs may be misplaced.

Benefits

The access log feature of SLB has the following advantages:

- Easy to use

  This feature reduces log processing time for developers and O&M personnel so that they can focus on business development and technical research.

- Capable of dealing with large amounts of data

  SLB access logs contain a large amount of data that needs to be processed. Therefore, you must consider performance and cost for log processing. Log Service analyzes 100 million logs within one second. Compared with self-managed open source solutions, Log Service is faster and more cost-effective.

- Real-time

  Scenarios such as DevOps, monitoring, and alerting require real-time log data. Traditional methods cannot meet this requirement. For example, it is time-consuming to perform ETL operations and data analytics by using tools such as Hive. A significant amount of effort is spent on data integration. The access log feature of SLB, in conjunction with the powerful big data computing capabilities of Alibaba Cloud Log Service, can analyze and process real-time logs within seconds.

- Elastic

You can enable or disable the access log feature for selected SLB instances. You can set the storage period to a value ranging from 1 to 365 days. The capacity of a Logstore is scalable to meet business growth needs.

3.2. Configure access logs

You must authorize to access Log Service before access logs can be written to Log Service.

Prerequisites

- A Layer 7 CLB instance is created. For more information, see Create a CLB instance and Add an HTTP listener.
- Log Service is activated. For more information, see Activate Log Service.

Procedure

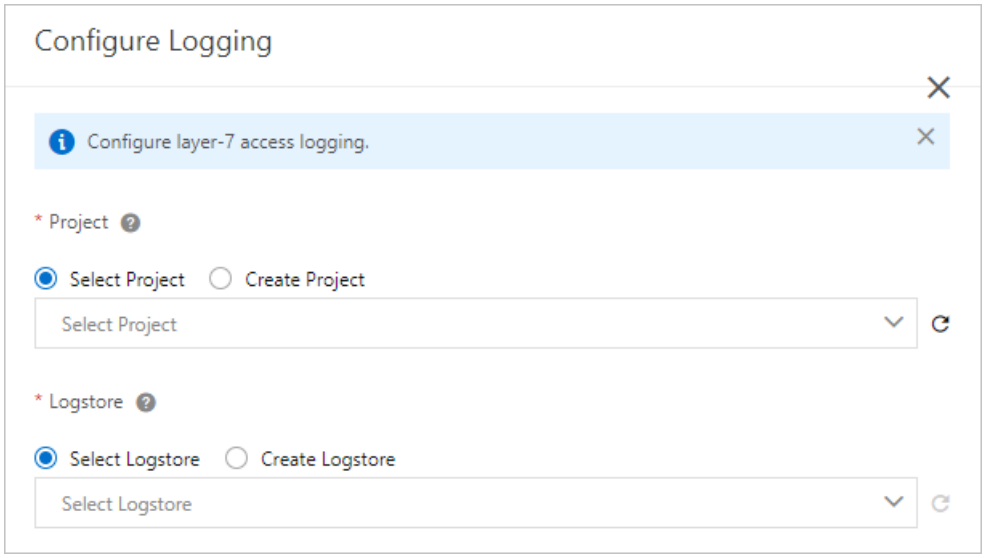
1.
2.
3. In the left-side navigation pane, choose **Logs > Access Logs**.
4. In the top navigation bar, select the region where the CLB instance is deployed.
5. Click **Authorize**. In the dialog box that appears, click **Confirm Authorization Policy** to authorize to write logs to Log Service.

   If you use a Resource Access Management (RAM) user, you must acquire the permissions from your Alibaba Cloud account. For more information, see Authorize a RAM user to use the access log feature.

   > **Note** You need only to perform the authorization once.

6. On the **Access Logs (Layer-7)** page, find the CLB instance that you want to manage and click **Configure Logging** in the **Actions** column.
7. In the **Configure Logging** panel, select a project and a Logstore.
   - **Project**: used to isolate and manage resources in Log Service.
   - **Logstore**: used to collect, store, and query log data.

   > **Note** Make sure that the name of the project is unique and the region of the project is the same as that of the CLB instance.



After access log is enabled, you can query and search for log data by using the fields listed in the following table.

Field	Description
slbid	The ID of the CLB instance.
__topic__	The topic of the log entry. The default topic is slb_layer7_access_log.
body_bytes_sent	The size of an HTTP response body. Unit: bytes.
client_ip	The client IP address.
host	By default, the value is retrieved from the request parameters. If the host is not specified in the request parameters, the system retrieves the value from the Host header. If this value cannot be retrieved from the request parameters or the Host header, the IP address of the backend server is used.
http_host	The Host header of an HTTP request.
http_referer	The Referer header of an HTTP request received by CLB.
http_user_agent	The Referer header of an HTTP request.
http_x_forwarded_for	The X-Forwarded-For header of an HTTP request.
http_x_real_ip	The client IP address.
read_request_time	The amount of time that CLB takes to process a request. Unit: milliseconds.
request_length	The combined size of the start line, headers, and body of an HTTP request.
request_method	The request method.

Field	Description
request_time	The amount of time from when CLB receives the first request to when CLB returns a response. Unit: seconds.
request_uri	The URI of a request received by CLB.
scheme	The request protocol. Valid values: HTTP and HTTPS.
server_protocol	The version of the HTTP protocol that is received by CLB. For example, HTTP/1.0 or HTTP/1.1.
slb_vport	The listening port of the CLB instance.
ssl_cipher	The cipher suite used to establish an SSL connection, for example, ECDHE-RSA-AES128-GCM-SHA256.
ssl_protocol	The protocol that is used to establish an SSL connection, for example, TLS 1.2.
status	The status of a response returned by CLB.
tcpinfo_rtt	The amount of time that is taken to establish a TCP connection. Unit: milliseconds.
time	The time when the log entry is generated.
upstream_addr	The IP address and port of the backend server.
upstream_response_time	The amount of time from when a connection is established to when the connection is closed. Unit: seconds.
upstream_status	The HTTP status code sent from a backend server to CLB.
vip_addr	The virtual IP address.
write_response_time	The amount of time taken to respond to a write request. Unit: milliseconds.

8. Click **OK**.

3.3. Authorize a RAM user to use the access log feature

This topic describes how to authorize a Resource Access Management (RAM) user to use the access log feature of with your Alibaba Cloud account. To use the access log feature, RAM users must acquire the required permissions.

Prerequisites

The access log feature is enabled for the Alibaba Cloud account. For more information, see Enable the access log management feature.

Procedure

1. Perform the following operations to create a policy:
   i. Log on to the RAM console with the Alibaba Cloud account.
   ii. In the left-side navigation pane, choose **Permissions > Policies**.
   iii. On the **Policies** page, click **Create Policy**.
   iv. On the **Create Policy** page, click the **JSON** tab.

   You can also create a policy on the Visual Editor Beta tab. For more information, see Create a custom policy on the Visual Editor Beta tab.
   v. On the JSON tab, enter the following code and click **Next Step**:

```
{
"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:QueryMetric*",
   "Resource": "*",
```

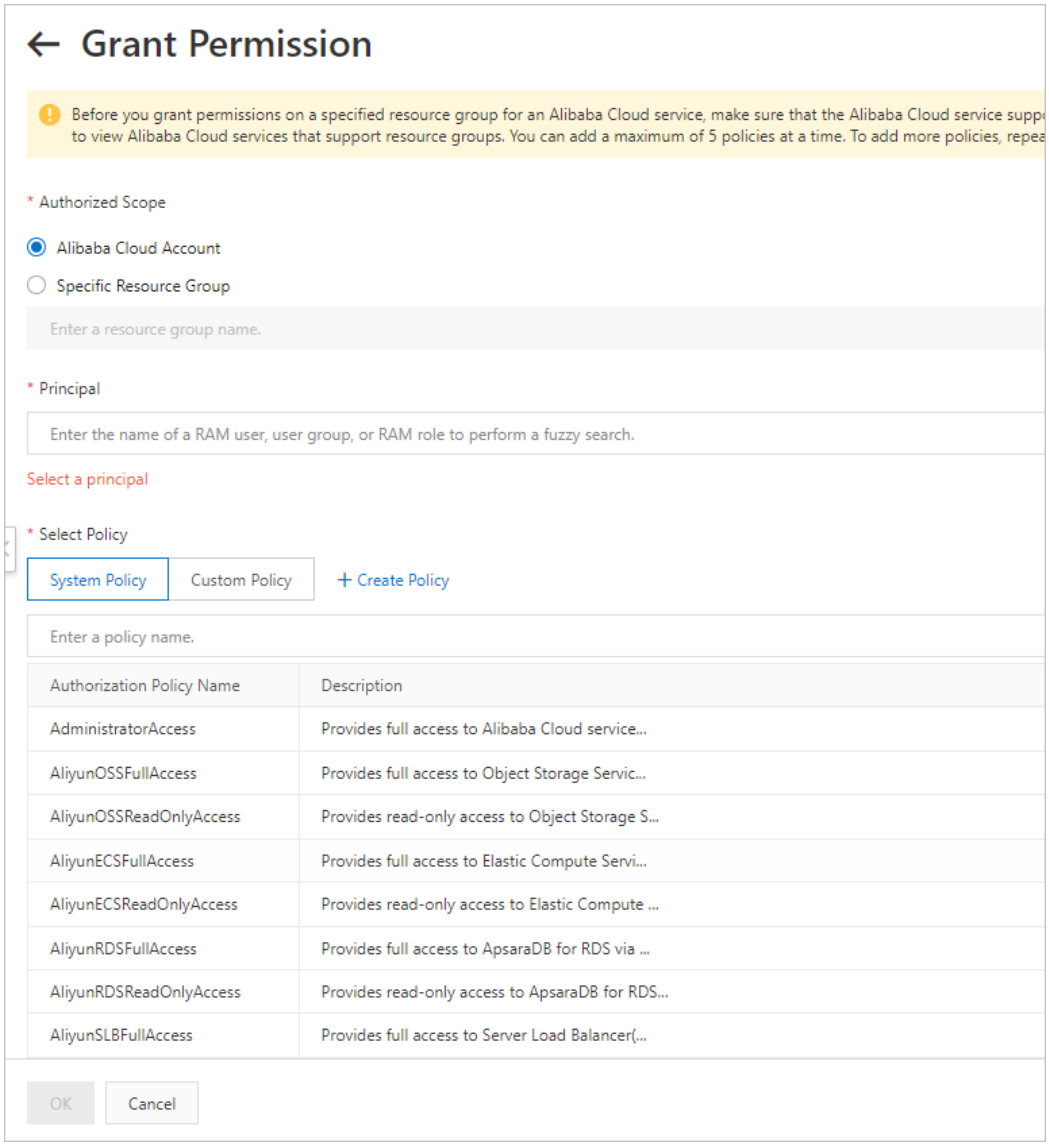
```
    "Effect": "Allow"
  },
  {
    "Action": [
      "slb:Describe*",
      "slb:DeleteAccessLogsDownloadAttribute",
      "slb:SetAccessLogsDownloadAttribute",
      "slb:DescribeAccessLogsDownloadAttribute"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "ram:Get*",
      "ram:ListRoles"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
],
"Version": "1"
}
```

vi. Specify the **Name** and **Note** parameters, and then click **OK**. For example, you can use the name **SlbAccessLogPolicySet**.

2. Perform the following operations to authorize a RAM user:

   i. In the left-side navigation pane of the RAM console, choose **Permissions > Grants** and click **Grant Permission**.

   ii. On the **Grant Permission** page, specify the **Authorized Scope** parameter.



- **Alibaba Cloud Account**: The permissions take effect on all resources in the current Alibaba Cloud account.
- **Specific Resource Group**: The permissions take effect on resources in a specified resource group.

iii. On the **Grant Permission** page specify **Principal**.

> **Note** You can attach a maximum of five policies to a RAM user at the same time. If you want to attach more than five policies to a RAM user, repeat the required operations.

iv. Select the policy that you want to attach to the RAM user from the **Authorization Policy Name** list and click **OK**.

v. Return to the **Grants** page and check whether the policy is attached to the RAM user. After the policy is attached to the RAM user, the RAM user can use the access log feature of .

3.4. Query access logs

This topic describes how to query logs through the Server Load Balancer (SLB) console and the Log Service console.

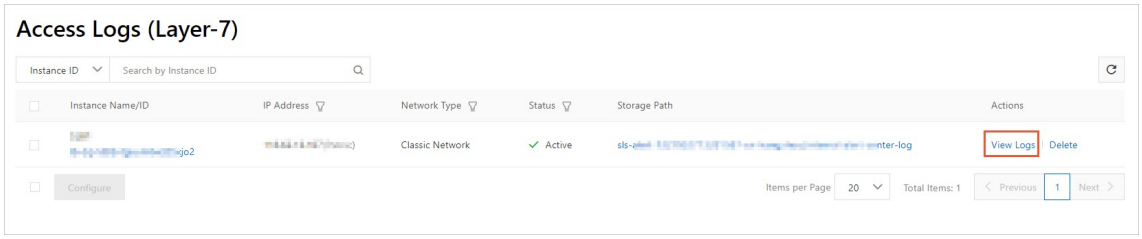
Procedure

1. Go to the log query page.

   You can go to the log query page from the SLB or Log Service console:

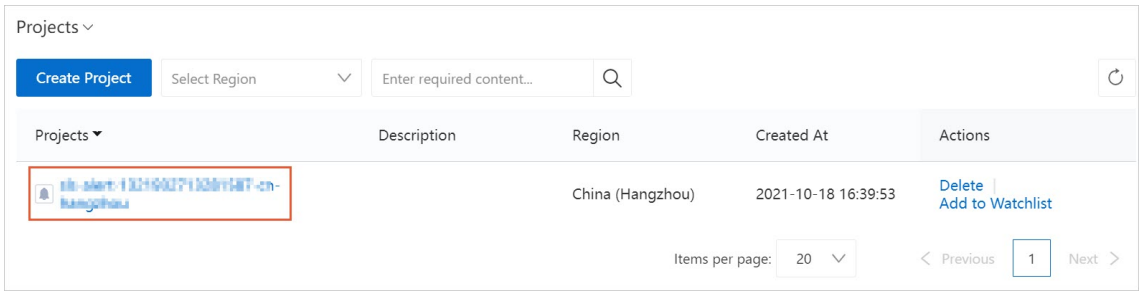
   - SLB console

     On the **Access Logs (Layer-7)** page, click **View Logs** in the **Actions** column.

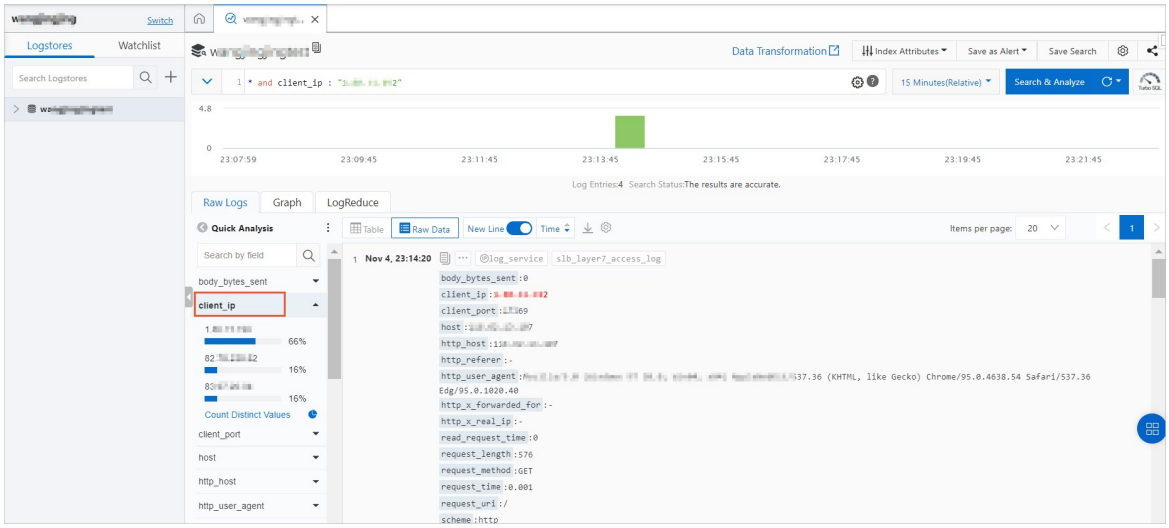
     

   - Log Service console

     On the **Logstores** page, click **Search** of the SLB Logstore entry.

2. Click the target log field to view detailed information.

3. Enter an SQL statement to query specific access logs.

   For example, enter the following SQL statement to query the top 20 clients that send the most access requests. It helps with the analysis of the sources of access requests and business decision-making.

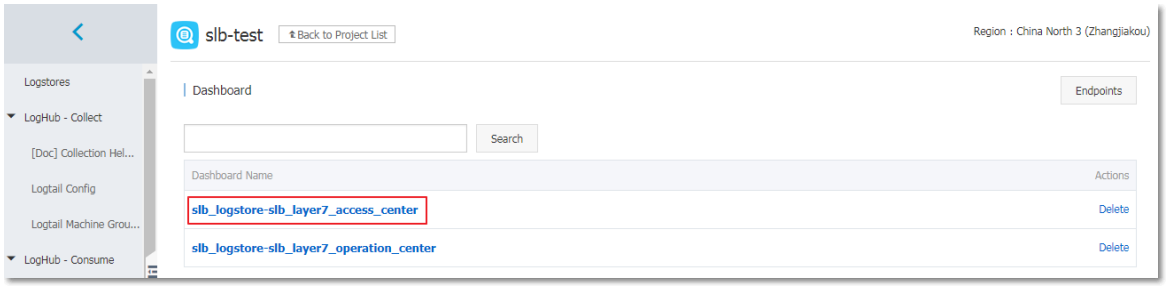
```
* | select ip_to_province(client_ip) as client_ip_province, count(*) as pv group by
    client_ip_province order by pv desc limit 50
```

3.5. Analyze access logs

This topic describes how to analyze access logs of Server Load Balancer (SLB) by using the dashboard of Log Service.

Procedure

1. Log on to the Log Service Console.
2. Click the Project of the SLB instance.
3. In the left-side navigation pane, choose **Search/Analytics > Dashboard**, and then click the name of the log.

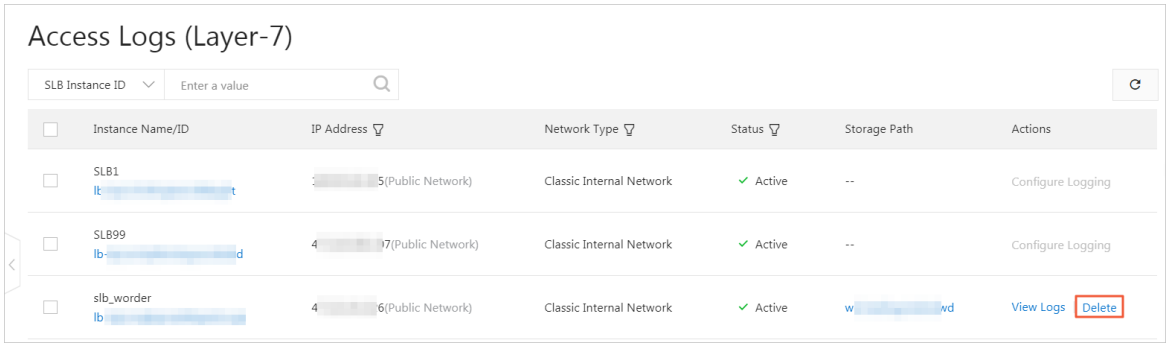


3.6. Disable access logs for an SLB instance

This topic describes how to disable access logs for a Server Load Balancer (SLB) instance. After you disable the access log feature, the access logs of the instance are no longer collected.

Procedure

1. Log on to the SLB console.
2. In the left-side navigation pane, choose **Logs > Access Logs**.
3. Select the region to which the target SLB instance belongs.
4. On the **Access Logs (Layer-7)** page, find the target instance and then click **Delete** in the **Actions** column.



5. In the displayed dialog box, click **OK**.