Alibaba Cloud Server Load Balancer

Log management

Issue: 20190725

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.
	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 information, 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.	`swich {stand | slave}`

Contents

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

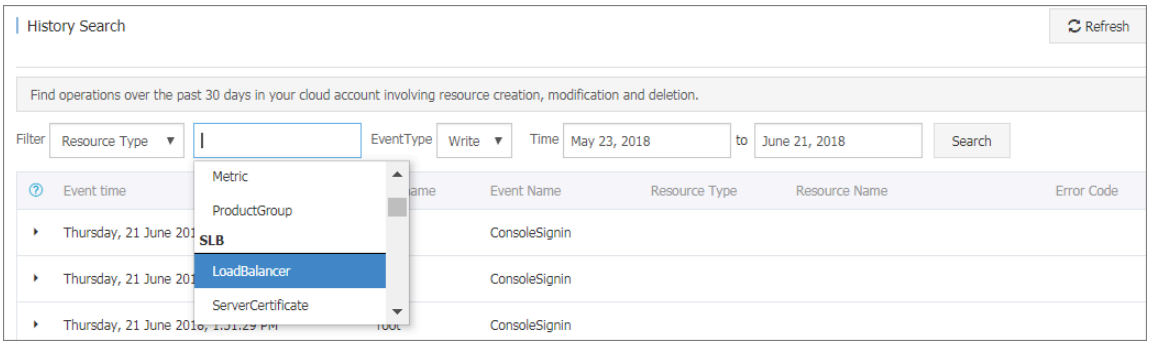
1. Log on to the SLB console.
2. In the left-side navigation pane, click Logs > Operation Log.
3. Click View Operation Logs.

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.



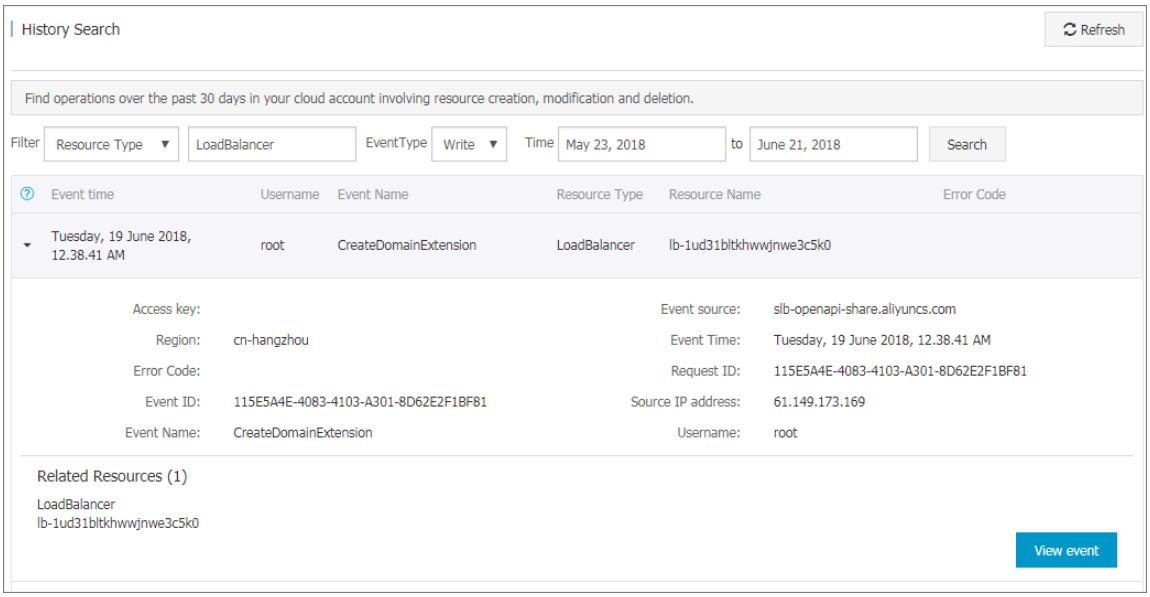
   c) Select an event type.

      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.



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 `AliyunSLBHealthCheckLogs` 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.txt` and the file name of a log file generated between 01:00-02:00 is `02.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.

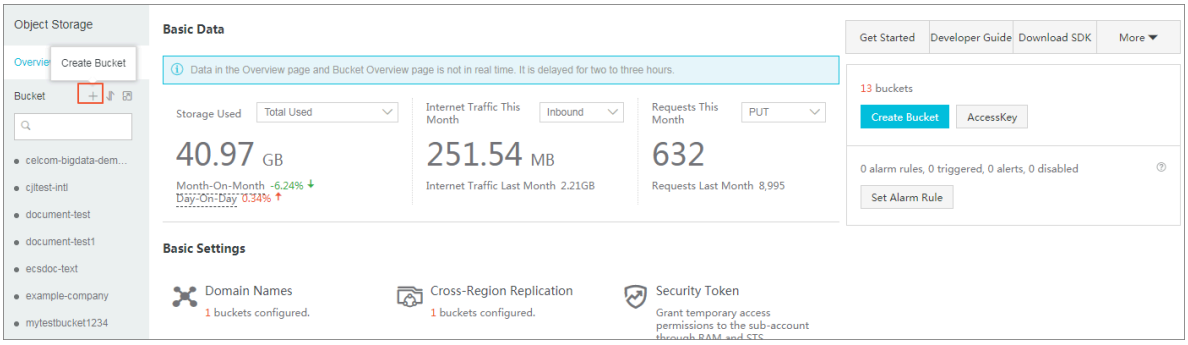
To store health check logs, follow these steps:

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.



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.

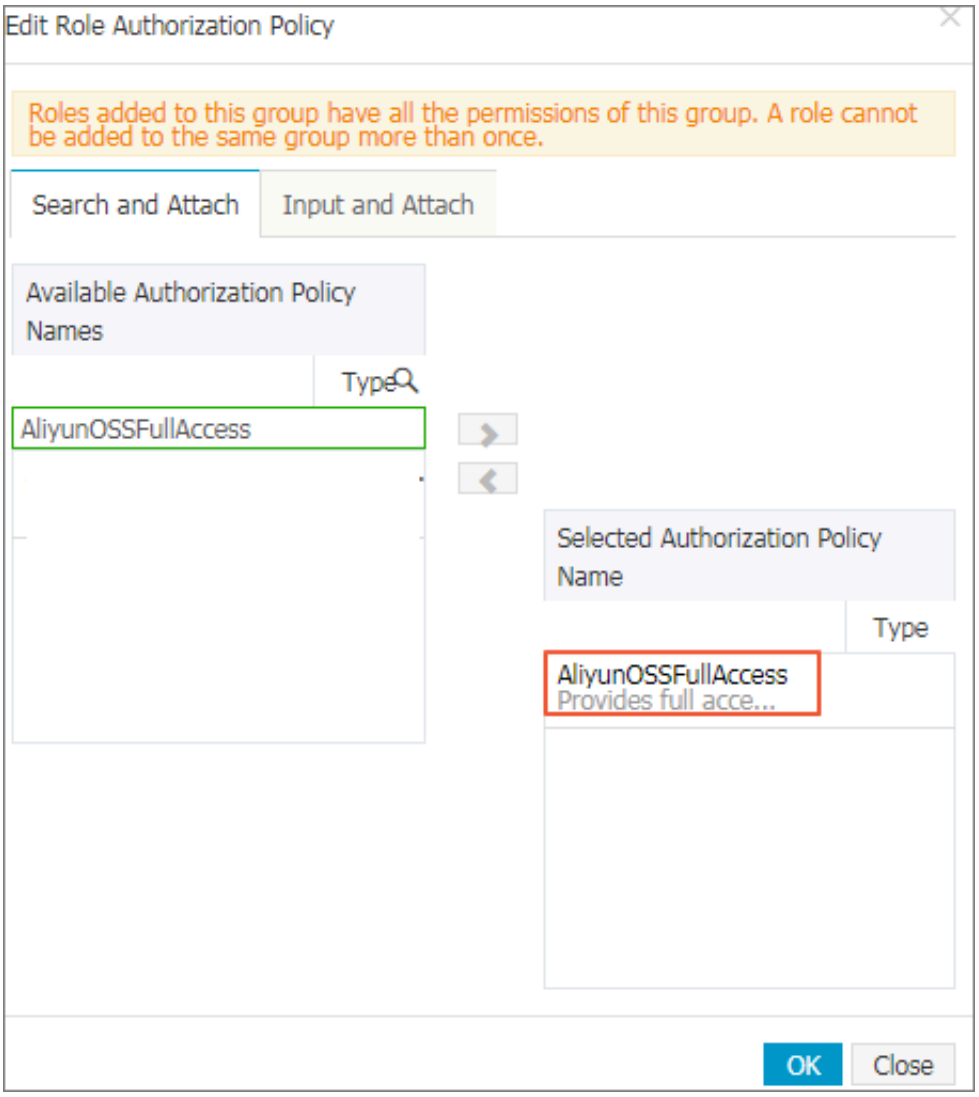
Step 2 Authorize SLB to access OSS

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

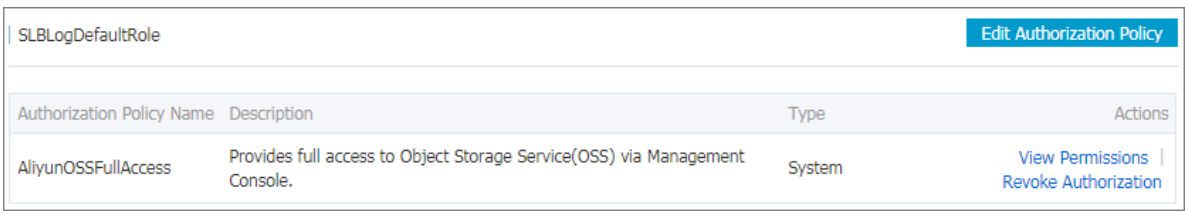
> **Notice:**
> The authorization is required only for the first time.

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.



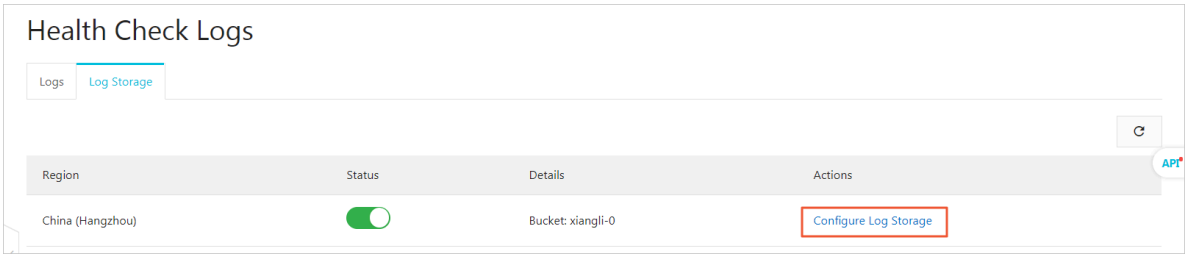
After the authorization, click the role name of SLBLogDefaultRole, and then click the Role Authorization Policies tab to view the attached policy.



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.



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.

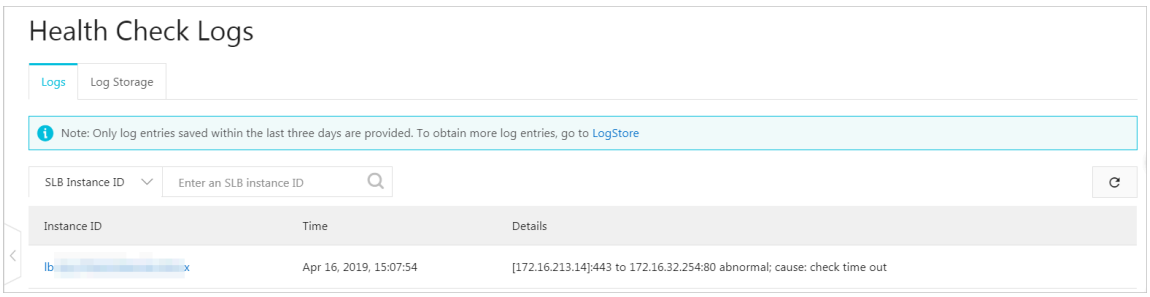
View health check logs

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.

> **Note:**
> 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.

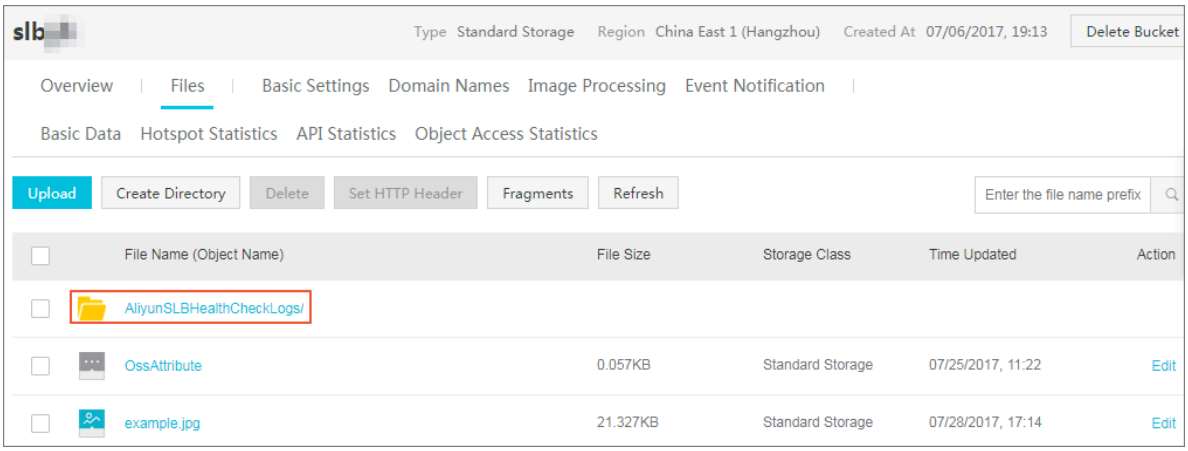
- The `SLB_instance_IP:port to Added_ECS_instance_IP:port abnormal; cause: XXX` log message indicates that the backend server is abnormal. Troubleshoot according to the detailed error message.
- The `SLB_instance_IP:port to Added_ECS_instance_IP:port normal` log message indicates that the backend server becomes normal again.



Download health check logs

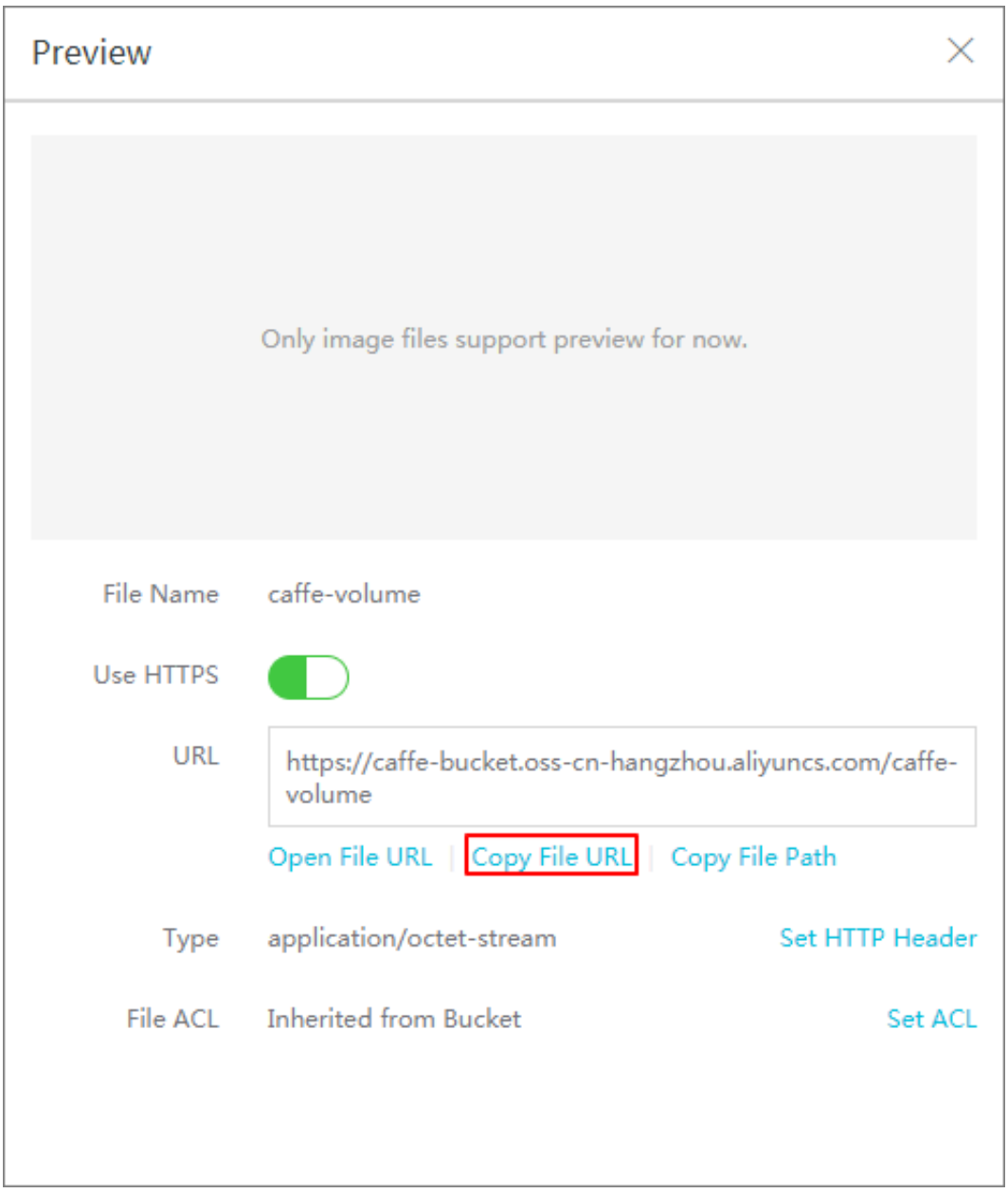
You can download the completed health check logs stored in OSS buckets.

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 /`.



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

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.

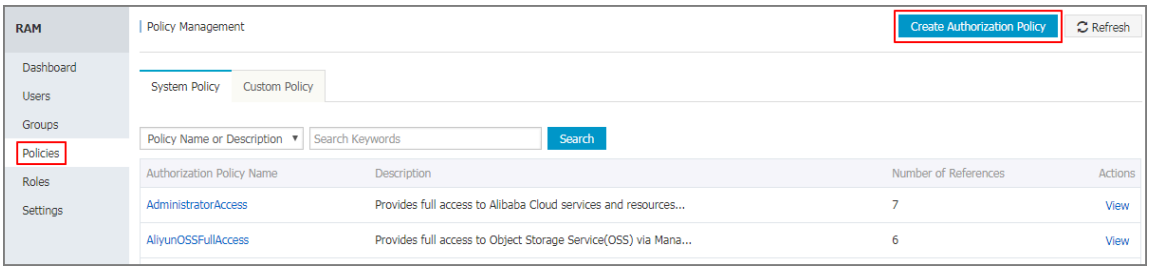
1. Log on to the RAM console by using the credentials of your account.
2. Click Roles to see whether the account has the AliyunLogArchiveRole.

   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.

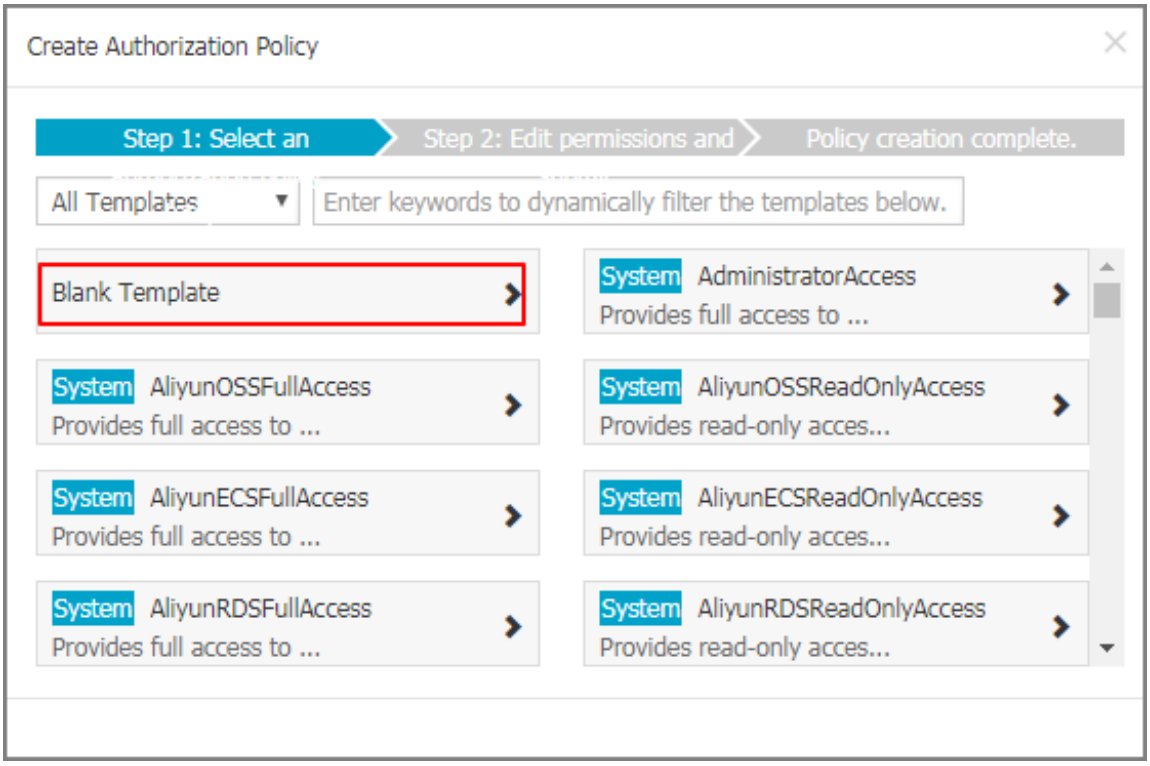
   > Note:
   > This operation is required only at the first time.

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.



   c) Click Blank Template.



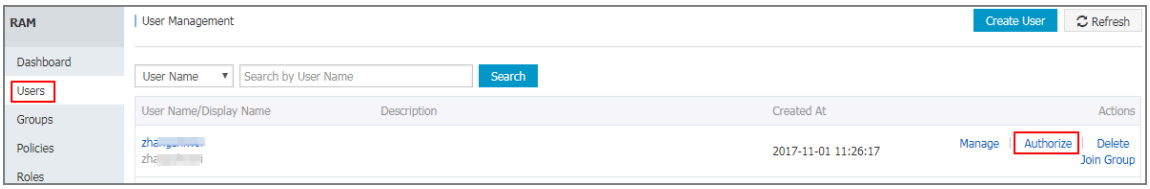
   d) Enter a policy name, such as SlbAccessLogPolicySet, and then enter the following policy. Click Create Authorization Policy.

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

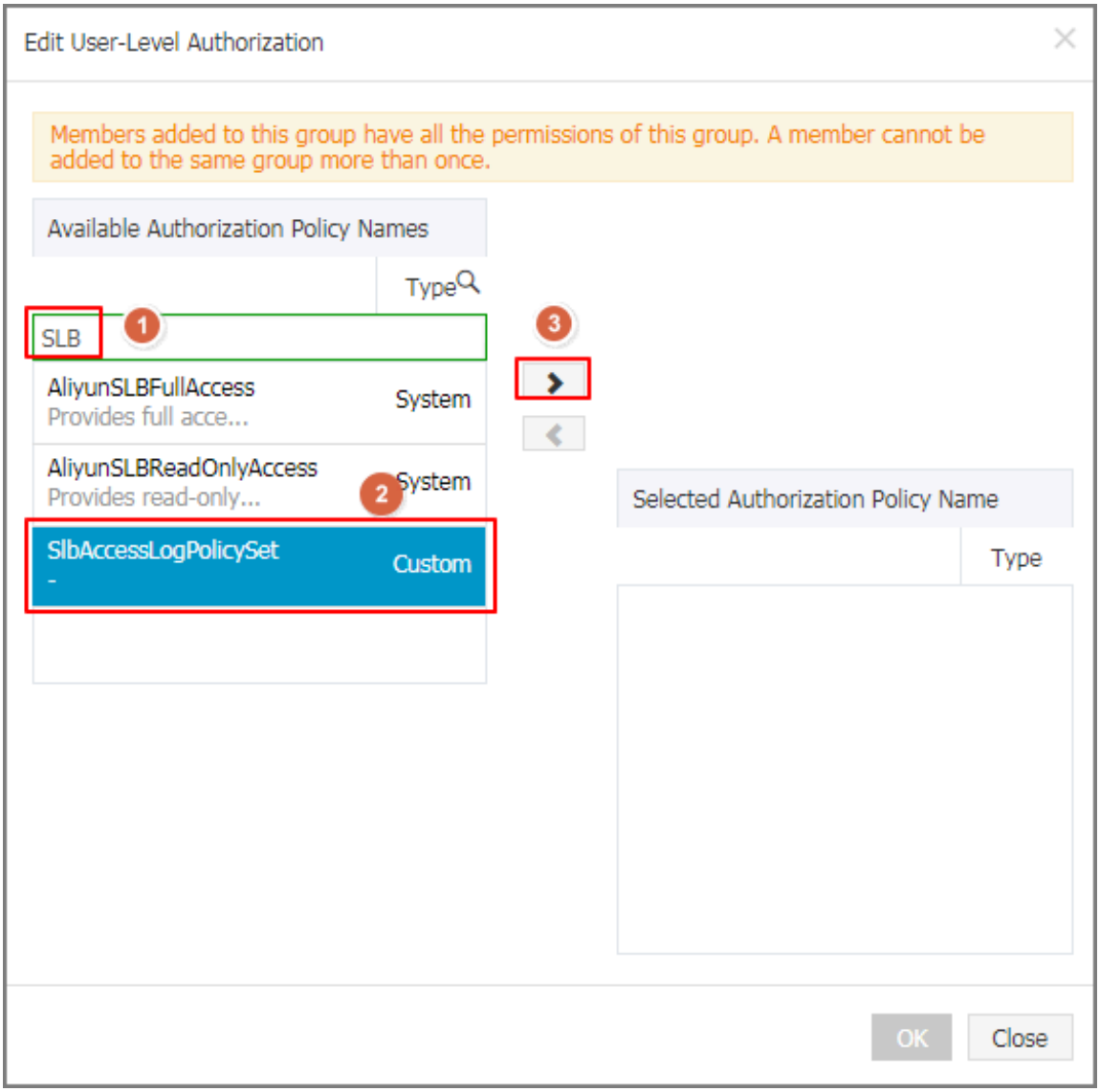
```
      " log : List *"
    ],
    " Effect ": " Allow ",
    " Resource ": " acs : log :*:*: project /*"
  },
  {
    " Action ": [
      " log : Create *",
      " log : List *",
      " log : Get *",
      " log : Update *"
    ],
    " Effect ": " Allow ",
    " Resource ": " acs : log :*:*: project /*/ 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 "
    ],
    " Effect ": " Allow ",
    " Resource ": "*"
  }
],
" Version ": " 1 "
}
```

e) Click Close.

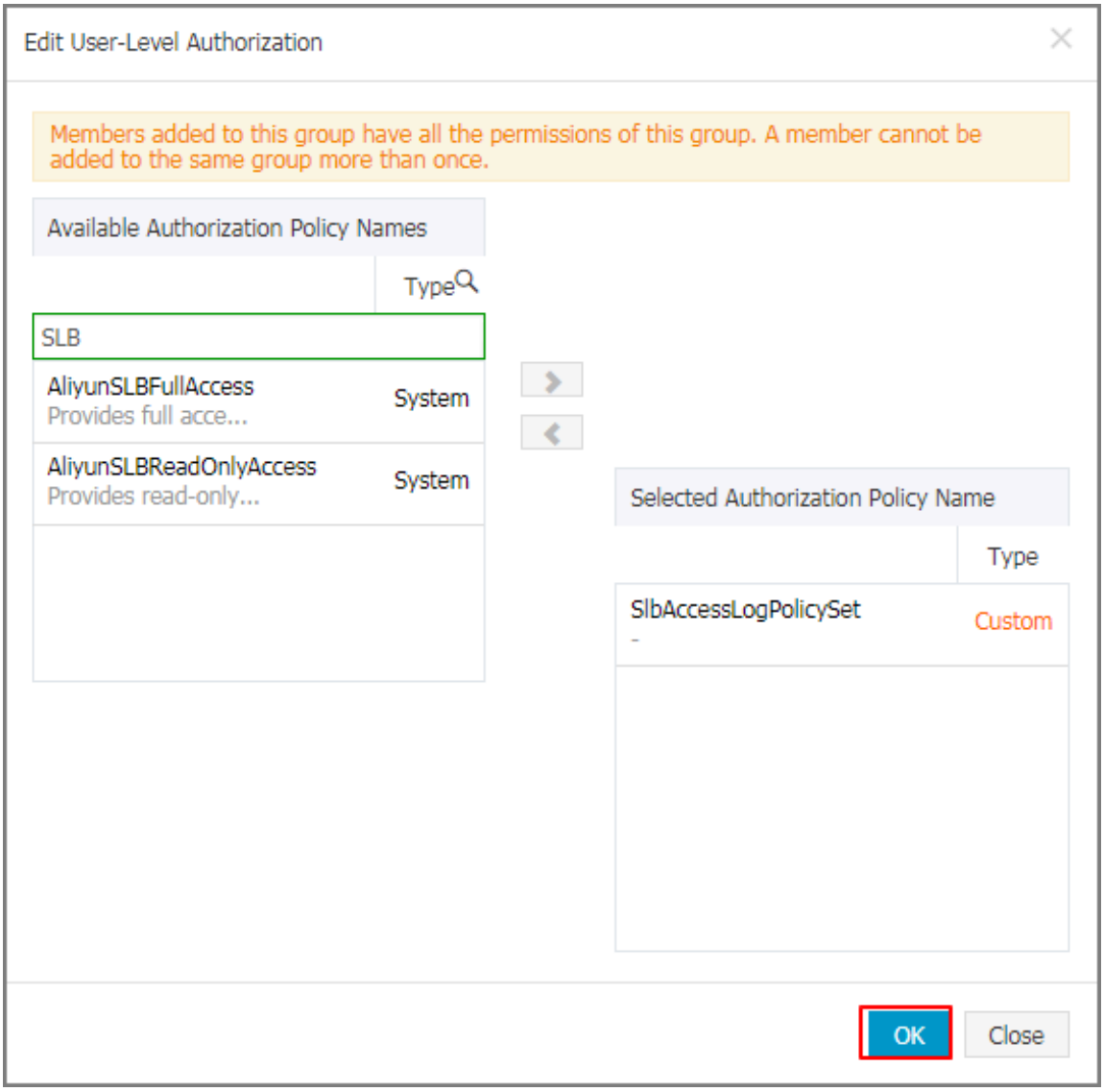
2. Attach the created policy to the RAM user:
   a) In the left-side navigation pane, click Users.
   b) Find the target RAM user (the user who uses the SLB access log function) and click Authorize.



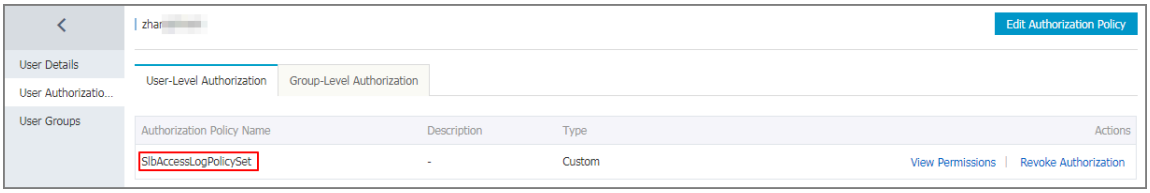
   c) Search the created authorization policy and attach the policy to the RAM user.



   d) Click OK.



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



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.

Note:

- 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.

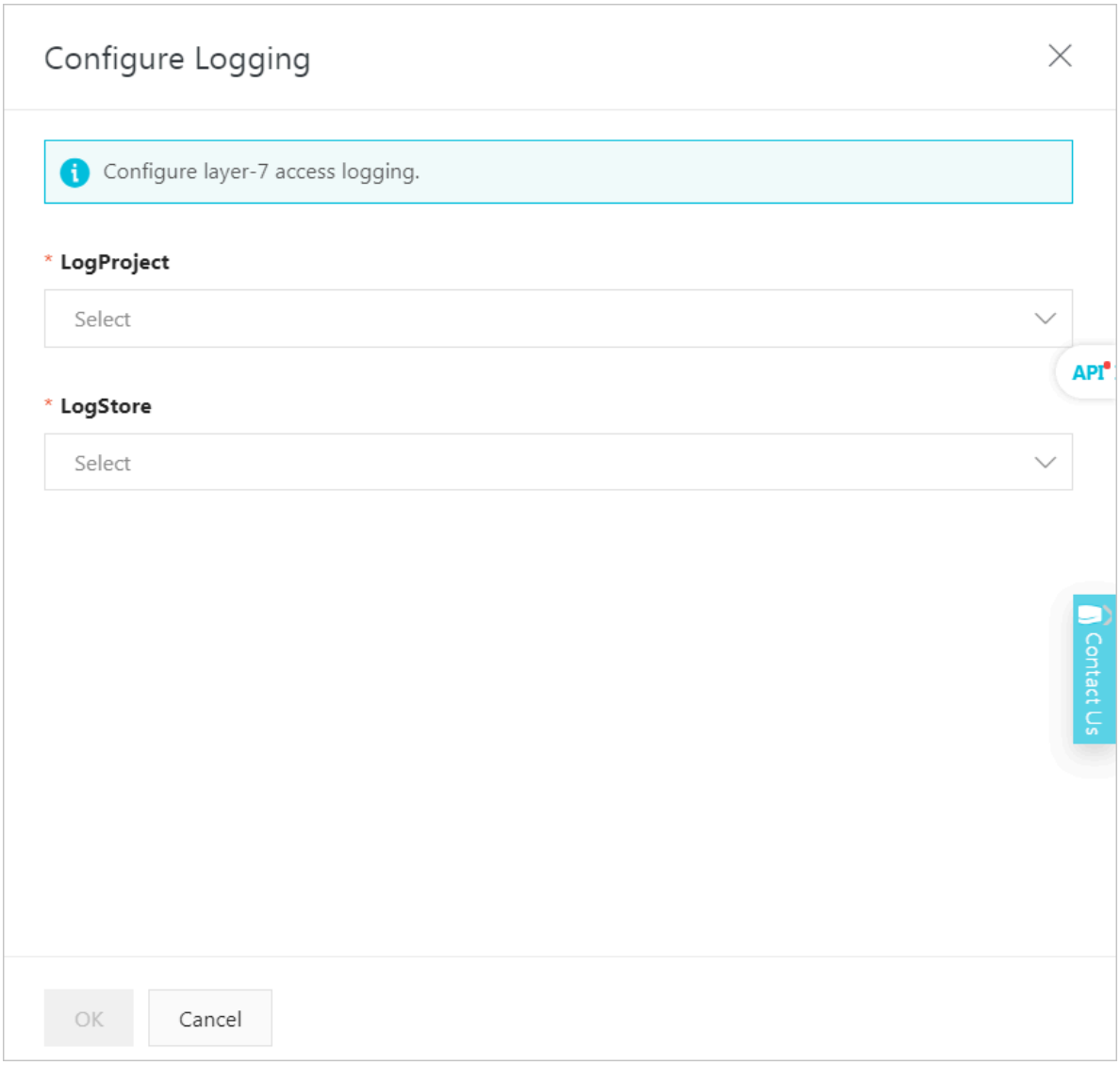
   > Note:
   > This step is required only at the first time.

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.



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.

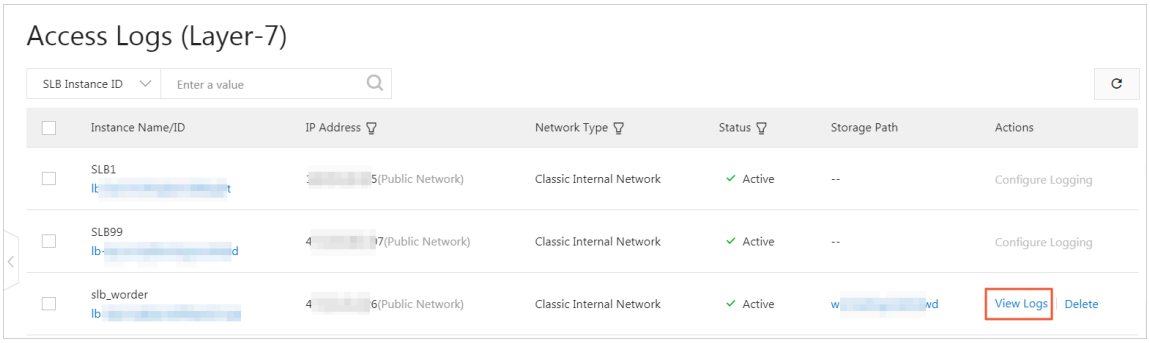
Search access logs

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:

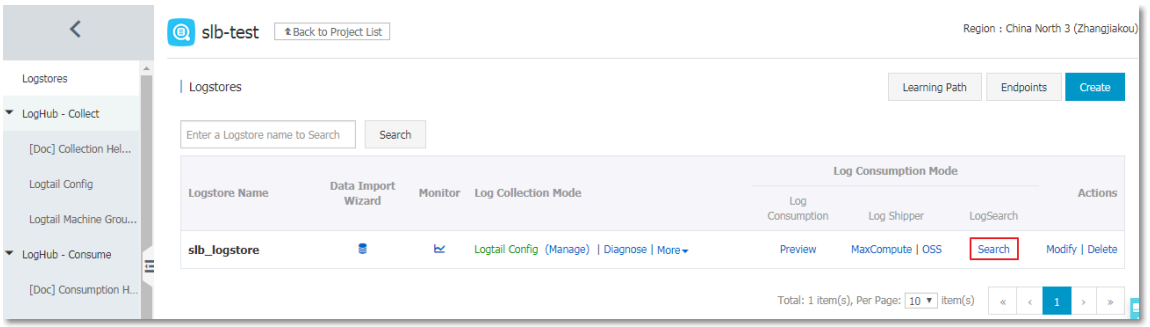
   - From the SLB console:

     On the Access Logs page, click View Logs.

   - From the Log Service Console:

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

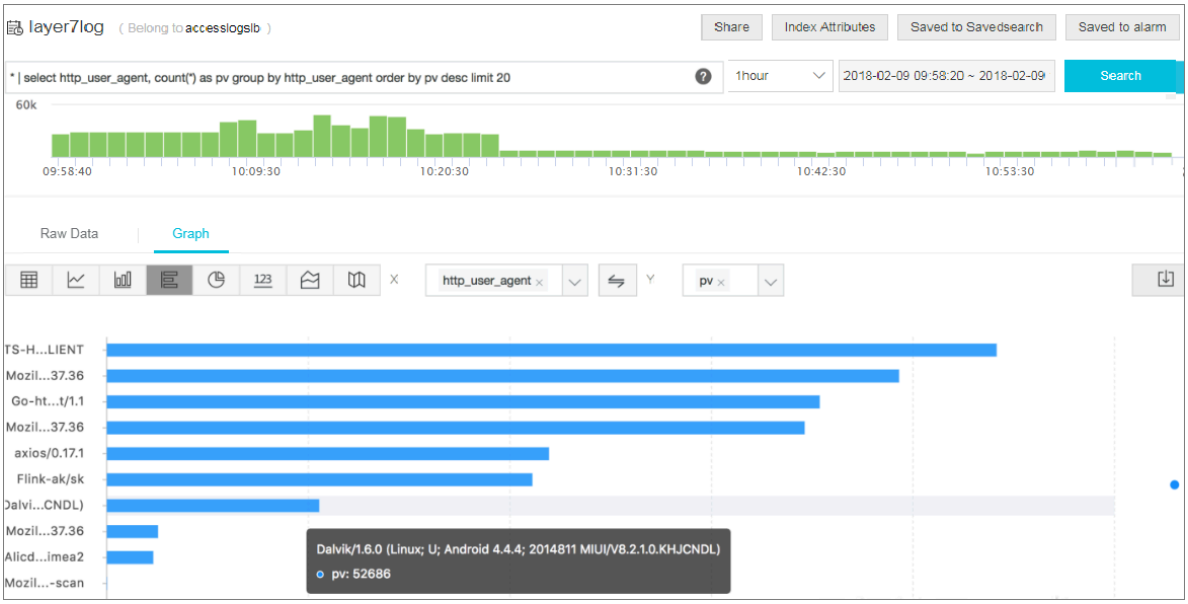
     

2. Click the target log field to view detailed information.
3. Enter an SQL statement to query access logs.

   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
```

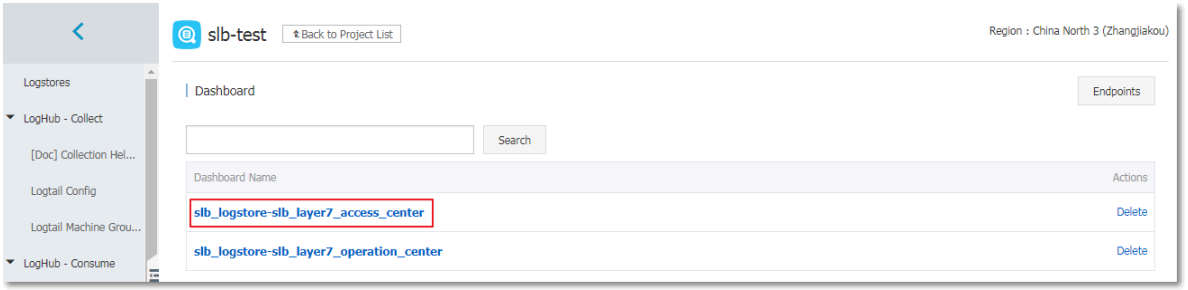


Analyze access logs

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.

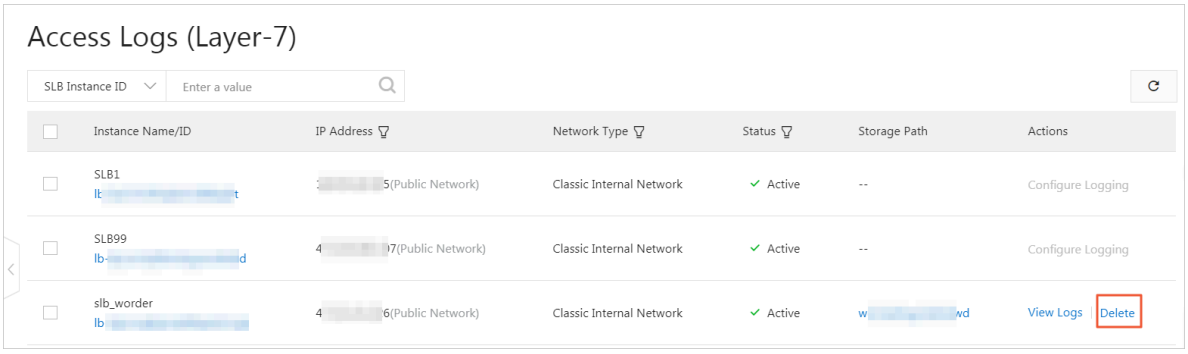


Disable the access log function

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.



5. In the displayed dialog box, click OK.