Cloud Load Balancer

Monitoring and Alarm

Product Documentation

Contents

Monitoring and Alarm
Monitoring Metric Descriptions

Last updated : 2020-05-26 14:11:12

Cloud Monitor collects raw data from the running CLB instances and displays the data entries in intuitive graphs. Statistics will be kept for one month by default. You can observe the operations of instances in the month to stay informed of the status of application services.

You can go to the Cloud Monitor Console to view CLB monitoring data. Click **Cloud Product Monitoring** >**Cloud Load Balancer** and then click the CLB instance ID to enter the monitoring details page. You can view monitoring data of the CLB instance and expand it to view the listener and real server monitoring information.

CLB Instance Level

Metric	Unit	Description
Inbound bandwidth	Mbps	Bandwidth used by the client to access CLB over the public network within a reference period.
Outbound bandwidth	Mbps	Bandwidth used by CLB to access the public network within a reference period.
Number of inbound packets	Packets/s	Number of request data packets received by CLB per second within a reference period.
Number of outbound packets	Packets/s	Number of data packets sent by CLB per second within a reference period.

Layer-4 Listener (TCP/UDP) Level

Layer-4 listeners allow you to view the monitoring metrics at three levels:

- Listener level
- Real server level
- Real server port level

Metric	Unit	Description

Metric	Unit	Description
Number of connections	-	Number of connections on the listener within a reference period.
Number of new connections	-	Number of newly established connections on the listener within a reference period.
Inbound bandwidth	Mbps	Bandwidth used by the client to access CLB over the public network within a reference period.
Outbound bandwidth	Mbps	Bandwidth used by CLB to access the public network within a reference period.
Number of inbound packets	Packets/s	Number of request data packets received by CLB per second within a reference period.
Number of outbound packets	Packets/s	Number of data packets sent by CLB per second within a reference period.

Layer-7 Listener (HTTP/HTTPS) Level

Layer-7 listeners allow you to view the monitoring metrics at five levels:

- Listener level
- Domain name level
- URL forwarding path level
- Real server level
- Real server port level

Metric	Unit	Description
Number of connections	-	Number of connections on the listener within a reference period.
Number of new connections	-	Number of newly established connections on the listener within a reference period.
Inbound bandwidth	Mbps	Bandwidth used by the client to access CLB over the public network within a reference period.
Outbound bandwidth	Mbps	Bandwidth used by CLB to access the public network within a reference period.

Metric	Unit	Description
Number of inbound packets	Packets/s	Number of request data packets received by CLB per second within a reference period.
Number of outbound packets	Packets/s	Number of data packets sent by CLB per second within a reference period.
Average response time	ms	Average response time of CLB within a reference period.
Maximum response time	ms	Maximum response time of CLB within a reference period.
Number of response timeouts	-	Number of CLB response timeouts within a reference period.
Requests per second	-	Number of CLB requests per second within a reference period, i.e., QPS.
2xx status code	-	Number of 2xx status codes returned by the real server within a reference period.
3xx status code	-	Number of 3xx status codes returned by the real server within a reference period.
4xx status code	-	Number of 4xx status codes returned by the real server within a reference period.
5xx status code	-	Number of 5xx status codes returned by the real server within a reference period.
404 status code	-	Number of 404 status codes returned by the real server within a reference period.
502 status code	-	Number of 502 status codes returned by the real server within a reference period.
3xx status code returned by CLB	-	Number of 3xx status codes returned by CLB within a reference period (sum of CLB and real server return codes).
4xx status code returned by CLB	-	Number of 4xx status codes returned by CLB within a reference period (sum of CLB and real server return codes).
5xx status code returned by CLB	-	Number of 5xx status codes returned by CLB within a reference period (sum of CLB and real server return codes).

Metric	Unit	Description
404 status code returned by CLB	-	Number of 404 status codes returned by CLB within a reference period (sum of CLB and real server return codes).
502 status code returned by CLB	-	Number of 502 status codes returned by CLB within a reference period (sum of CLB and real server return codes).

If you want to view the monitoring data of a CVM instance under a listener, please log in to the CLB Console, click the monitoring icon near the CLB instance ID, and then browse the performance data of each instance in the floating window.

Alarming Metric Descriptions

Last updated : 2020-05-26 14:08:28

Alarm Description

You can create alarms for specified instance metrics so that your CLB instance will send alarm information to target user groups when its running status meets a certain condition. By doing so, you can detect any exceptions in a timely manner and take appropriate actions to ensure system stability and reliability. For more information, please see Alarm Overview.
CLB alarm policies cover the following:

- Public network listener
- Private network listener
- Server port (other)
  - Listener level
  - Server port level
- Server port (private network Classic type)
- Layer-7 protocol monitoring

Public/Private Network Listeners

Currently, both public network CLB and private network CLB support alarming at the listener level with the following metrics:

Metric	Unit	Description
Inbound bandwidth	Mbps	Bandwidth used by the client to access CLB over the public network within a reference period.
Outbound bandwidth	Mbps	Bandwidth used by CLB to access the public network within a reference period.
Number of inbound packets	Packets/s	Number of request data packets received by CLB per second within a reference period.
Number of outbound packets	Packets/s	Number of data packets sent by CLB per second within a reference period.

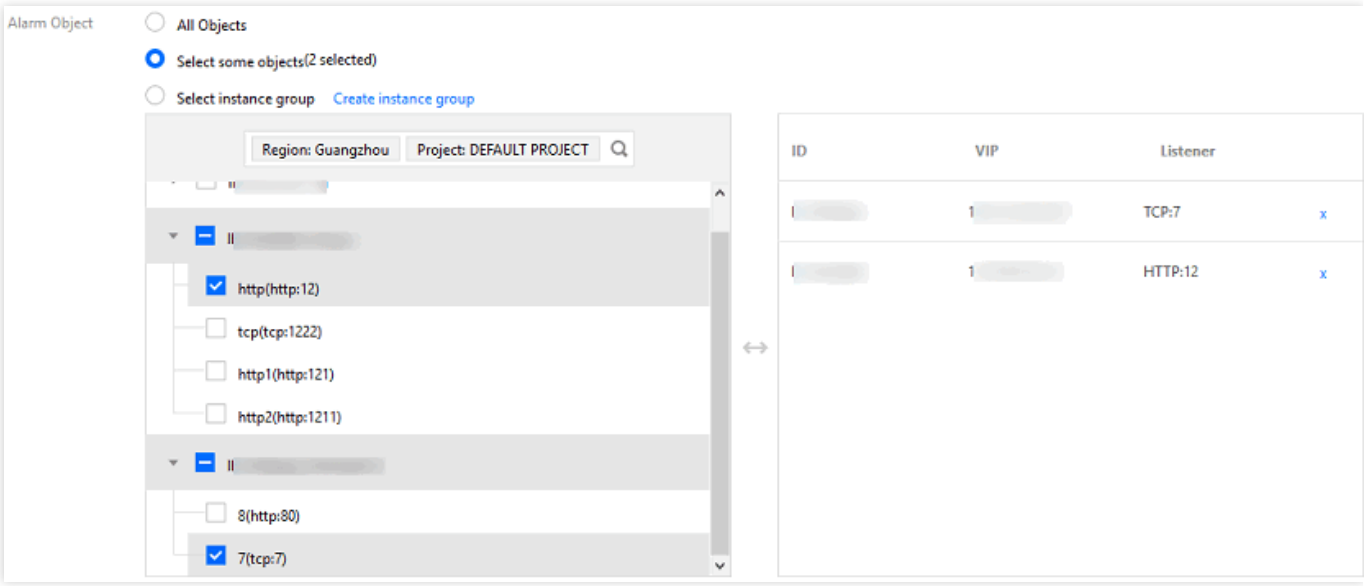
Server Port (Other)

All CLB instances except private network Classic ones support alarming at the following two level:

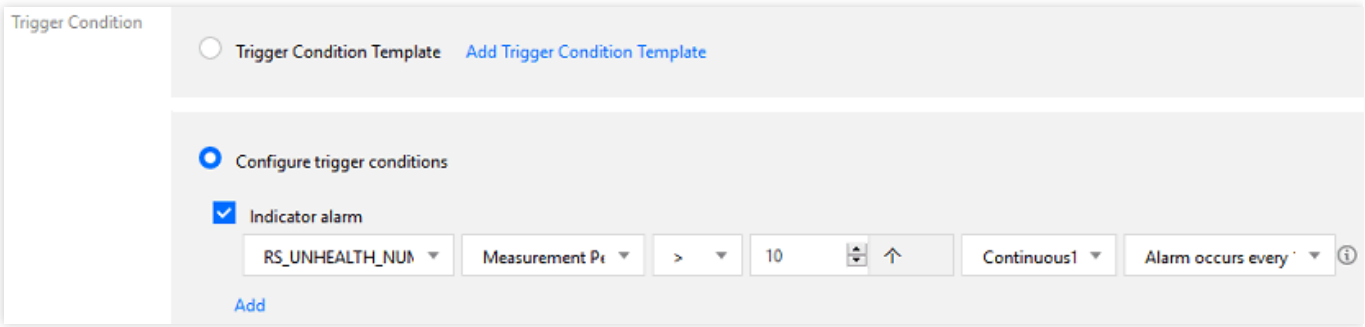
1. Listener level
   You can configure the number of exceptional real server ports of a listener for exception statistics of all bound server ports under the listener, which will trigger alarms based on the configured threshold. As shown below, the number of exceptional ports of all real servers under the selected listener is collected once every minute; if the number is greater than 10 per second for two consecutive reference period, it will trigger an alarm once per day.

   > To activate listener-level alarming, please submit a ticket for application.

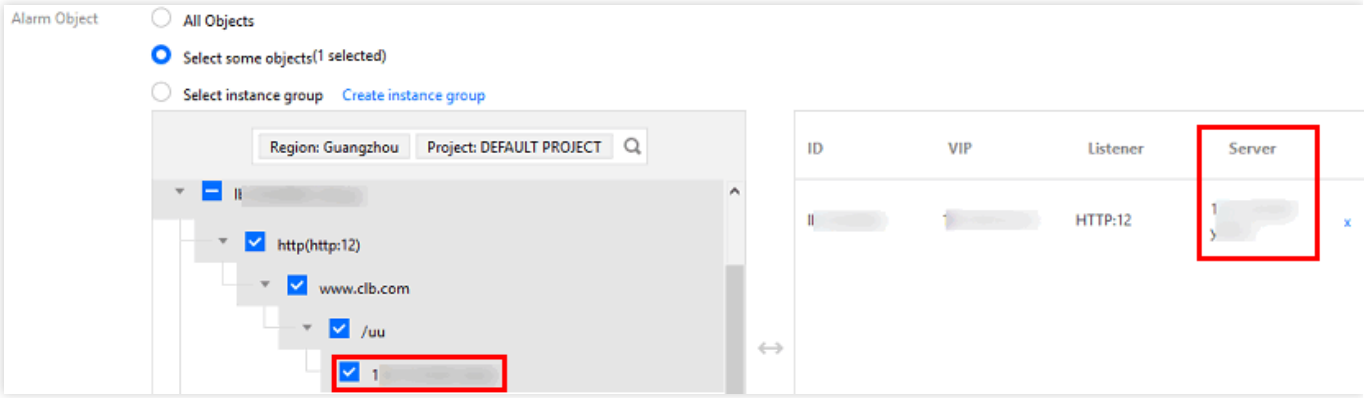
   - Configure alarm objects:



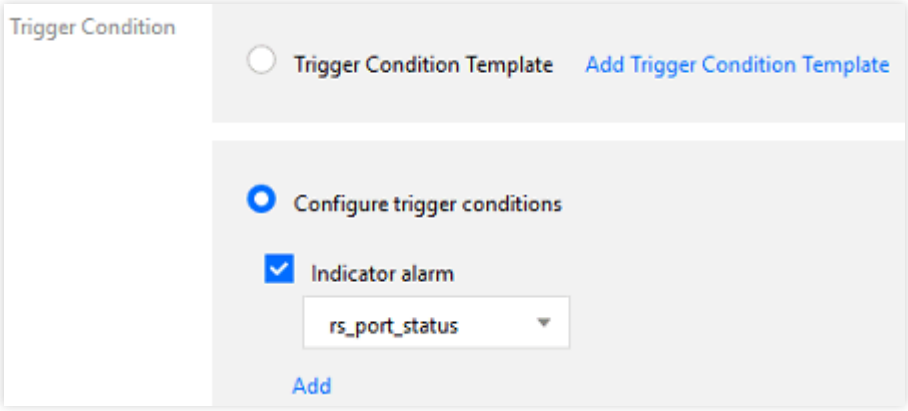
   - Configure trigger conditions:



2. Server port level
   You can configure exception alarms for a specified port of a real server bound to a listener, so that alarms will be sent whenever the port is exceptional.
   - Configure alarm objects:



   - Configure trigger conditions:



> - Real server port exception: it means that CLB finds the port of the real server unavailable; in some cases, network jitter can also trigger port exceptions.
> - Statistics at the listener level include port status of all real servers under the listener, from single alarm convergence to threshold alarming. To avoid the impact of network jitter, we recommend you to use listener-level alarming.

Server Port (Private Network Classic Type)

You can configure server port exception alarms for private network Classic CLB as instructed in "Server Port (Other) > Server port level".

You can configure exception alarms for a specified port of a real server bound to a listener, so that alarms will be sent whenever the port is exceptional.

Layer-7 Protocol Monitoring

You can configure unique monitoring metric alarm policies for all layer-7 (HTTP/HTTPS) listeners. The specific metrics are as follows:

Metric	Unit	Description
Inbound bandwidth	Mbps	Bandwidth used by the client to access CLB over the public network within a reference period.
Outbound bandwidth	Mbps	Bandwidth used by CLB to access the public network within a reference period.
Number of inbound packets	Packets/s	Number of request data packets received by CLB per second within a reference period.
Number of outbound packets	Packets/s	Number of data packets sent by CLB per second within a reference period.
Number of new connections	-	Number of new connections established per minute within a reference period.
Number of active connections	-	Number of active connections per minute within a reference period.
Average response time	ms	Average response time of CLB within a reference period.
Maximum response time	ms	Maximum response time of CLB within a reference period.
2xx status code	-	Number of 2xx status codes returned by the real server within a reference period.
3xx status code	-	Number of 3xx status codes returned by the real server within a reference period.
4xx status code	-	Number of 4xx status codes returned by the real server within a reference period.
5xx status code	-	Number of 5xx status codes returned by the real server within a reference period.

Metric	Unit	Description
404 status code	-	Number of 404 status codes returned by the real server within a reference period.
502 status code	-	Number of 502 status codes returned by the real server within a reference period.
3xx status code returned by CLB	-	Number of 3xx status codes returned by CLB within a reference period.
4xx status code returned by CLB	-	Number of 4xx status codes returned by CLB within a reference period.
5xx status code returned by CLB	-	Number of 5xx status codes returned by CLB within a reference period.
404 status code returned by CLB	-	Number of 404 status codes returned by CLB within a reference period.
502 status code returned by CLB	-	Number of 502 status codes returned by CLB within a reference period.

Obtaining Monitoring Data

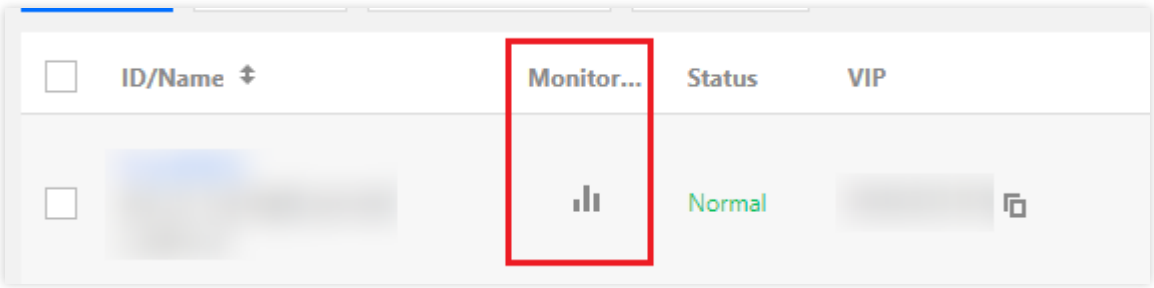
Last updated : 2020-09-10 15:20:53

Tencent Cloud Monitor collects and displays data for the CLB instance and the real server, helping you obtain CLB statistics, verify whether the system is running normally, and create alarms. For more information about Tencent Cloud Monitor, see the Basic Cloud Monitor documentation.

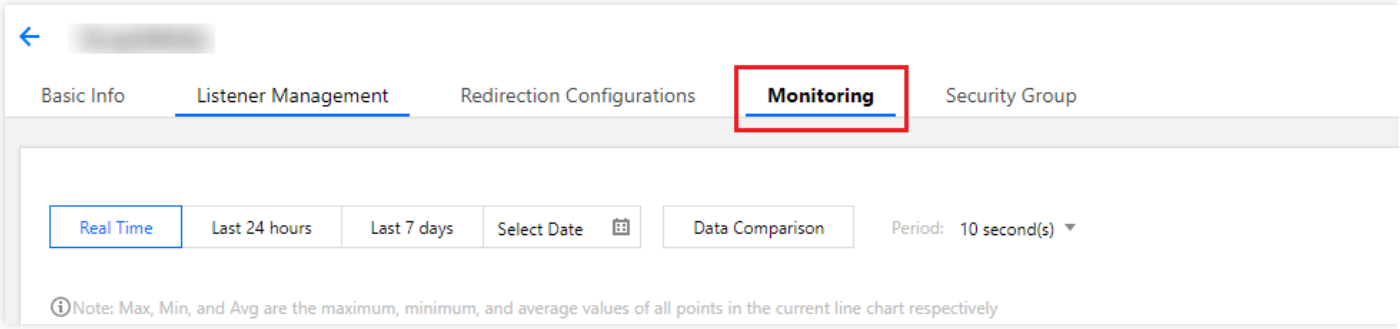
Tencent Cloud provides the Cloud Monitor feature for all users by default and does not require manual activation. You can use Cloud Monitor to collect the monitoring data of your CLB instances and view the data using the following methods.

CLB Console Method

1. Log in to the CLB console, click the monitoring icon next to the CLB instance ID, and then browse the performance data of the instance in the floating window.



2. Click the ID/Name of the CLB instance to access its details page. Click **Monitoring** to view its monitoring data.



Cloud Monitor Console Method

Log in to the Cloud Monitor console to view CLB monitoring data. Click **Cloud Load Balancer**(https://console.cloud.tencent.com/monitor/clb) on the left sidebar, and then click the ID/name of the CLB instance to access its monitoring details page. You can view the monitoring data of the CLB instance and expand its drop-down list to view the listener and real server monitoring information.

API Method

Use the `GetMonitorData` API to get the monitoring data of all products. For more information, see GetMonitorData, Public Network CLB Monitoring Metrics, Private Network CLB Monitoring Metrics (at the CLB Dimension), Private Network CLB Monitoring Metrics (at the Real Server Dimension), and CLB Layer-7 Data Monitoring Metrics.

Configuring Alarms

Last updated : 2020-05-14 17:34:42

You can create an alarm to trigger alarms and send alarm messages to a certain user group when a Tencent Cloud product meets the configured condition. The created alarm can periodically determine whether an alarm notification should be sent based on the difference between the monitored metric and the given threshold.

The specified users can take appropriate precautionary or remedial measures in a timely manner when the alarm is triggered. Therefore, properly created alarms can help you improve the robustness and reliability of your applications. For more information on alarms, please see Creating Alarm Policies.

You can create an alarm policy in the following steps:

1. Log in to the Cloud Monitor Console.
2. Click **Alarm Configuration** > **Alarm Policy** on the left sidebar to enter the alarm policy configuration page.
3. Click **Add** to configure an alarm policy.
4. Configure the basic items as shown below:
   - Policy Name: enter a policy name.
   - Remarks: add remarks to the policy.
   - Policy Type: select the monitoring metric.
   - Project: select a project as needed.
5. Configure alarm objects.
   - If you select "all objects", the alarm policy will be associated with all instances under the current account.
   - If you select "some objects", the alarm policy will be associated with the selected instances.
   - If you select "Instance group", the alarm policy will be associated with the selected instance group.
6. Set the alarm trigger. You can either choose a trigger condition template or configure trigger conditions.

- Trigger condition template
  Enable "Trigger Condition Template" and select a configured template from the drop-down list. For detailed configurations, please see Configuring Trigger Condition Templates. If a newly created template is not displayed, click **Refresh** on the right.
- Configure trigger condition
  An alarm trigger is a semantic condition consisting of metric, statistical period, comparison relationship, threshold, duration, and notification frequency.
  For example, if the specified metric is `inbound packets`, the statistical period is `1 minute`, the comparison relationship is `>`, the threshold is `100 packets/sec`, the duration is `2 periods`, and the notification frequency is `once per day`, then the number of inbound packets will be collected once every minute, and an alarm will be triggered once per day if the number of inbound packets of a CLB listener is over 100 packets/sec for two consecutive times.

7. Configure the alarm channel. Configure the recipient group, valid period, and receiving channel (email and object) as needed.

8. Configure the optional API callback as needed. Enter a URL accessible over the public network as the callback API address (domain name or IP[:port][/path]), and Cloud Monitor will push alarm messages to this address promptly.

9. After completing the configuration, click **Complete**.