

Basic Cloud Monitor

FAQs

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

FAQs

General

Alarm Service

FAQ on Cloud Monitoring

CVM Agent

CVM Has No Monitoring Data

FAQs

General

Last updated : 2020-07-14 10:59:05

What is Cloud Monitor?

Cloud Monitor (CM) provides you with multi-dimensional statistics monitoring, intelligent data analysis, real-time fault alarms, and customizable report configurations for Tencent Cloud services so that you can oversee the health of your applications and cloud services. This document describes how to use APIs to perform CM operations such as pulling monitoring statistics. For more information, see [API Category](#). We recommend that you read [Overview](#) and [Monitoring Overview](#) before using CM APIs.

What is Custom Cloud Monitor?

Custom Cloud Monitor is an entry through which you can easily submit monitoring data. Tencent Cloud provides you with a wealth of use cases to help you decide which metrics to submit. You can then use Custom Cloud Monitor to configure and submit the metrics. The submitted data is processed by the powerful Tencent Cloud Custom Cloud Monitor backend and then retained for a period of time for free. During this period, you can generate graphs and charts such as single-instance graphs and multi-day trends. You can also aggregate data by dimension. Custom Cloud Monitor also supports alarms that help you detect exceptions promptly and monitor your applications in real time.

What is Basic Cloud Monitor?

Basic Cloud Monitor is the main entry for monitoring and managing all cloud services. You can use it to view comprehensive and detailed monitoring data. Basic Cloud Monitor monitors cloud services including CVM, Cloud Database, and CDN in real time, extracts key metrics and displays them as monitor icons, and supports custom alarm thresholds. It provides you with multi-dimensional data monitoring, intelligent data analysis, real-time fault alarms, and custom data report configurations for cloud services, giving you accurate information on the health of your applications and various cloud services in real time.

How do I purchase Cloud Monitor?

You do not have to purchase or enable Cloud Monitor. Instead, it is automatically enabled when you register your Tencent Cloud account. You can use the [Cloud Monitor console](#) to query the status of your cloud services and configure alarms after purchasing and configuring cloud services.

Do CDH instances support Cloud Monitor?

No.

How do I monitor the memory usage of CVM instances and TencentDB instances?

1. Log in to the [Cloud Monitor console](#).
2. Click **Cloud Virtual Machine** or **Cloud Database** under Cloud Product Monitoring to access the Cloud Product Monitoring page.
3. Click the monitoring icon of the target instance to query the memory usage of the instance, which can be a CVM or cloud database instance.

For more information on how to create an alarm for the memory usage of a CVM instance or a cloud database instance, see [Alarm Service](#).

How do I troubleshoot Cloud Monitor issues?

For more information on how to troubleshoot Cloud Monitor issues, see [Troubleshooting](#).

Alarm Service

Last updated : 2020-04-27 16:06:30

Why cannot I receive alarm notifications through some alarm channels?

- **Alarm notifications cannot be received via SMS:**
 - In the user list in the [CAM Console](#), click a username to access the user details page and check that the user's phone number has been verified.
 - In the [alarm policy](#) list, check whether the SMS channel is blocked in the corresponding alarm policy.
 - On the right of the [Monitoring Overview](#) page, check whether the free quota of SMS messages has been used up. For more information, please see [SMS Alarm Channel](#).
- **Alarm notifications cannot be received via email:**
 - In the user list in the [CAM Console](#), click a username to access the user details page and check that the user's email address has been verified.
 - In the [Alarm Policy](#) list, check whether the email channel is blocked in the corresponding alarm policy.

Why cannot some recipients in the alarm recipient group receive alarm notifications?

The alarm recipients' information for relevant alarm channels (SMS, and email) has not been verified. Please verify the information in the [CAM Console](#).

If a user is in multiple recipient groups that are all bound to an alarm policy, will the user receive multiple alarm notifications?

Yes. You can create a new recipient group based on your business needs to prevent individual users from receiving repeated alarm notifications.

When will an alarm notification expire? Why cannot an alarm notification be received if it has not been restored for a few days?

- Non-repeated alarm notifications: only one alarm notification will be received through each alarm channel.
- Default logic for repeated (once every 5 minutes, hour, or day) alarm notifications:
 - The alarm notification will be sent to you at the configured frequency within 24 hours after an alarm is triggered.
 - Following 24 hours after an alarm is triggered, the alarm notification will be sent once every day by default.

- Following 72 hours after an alarm is triggered, the alarm notification will be sent for the last time.

Will an alarm notification be received if the corresponding alarm is restored?

Yes. An alarm notification will be sent to the recipients after the corresponding alarm is restored.

Will a CVM instance be automatically associated with the default policy on the backend after a user disassociates it from the default policy on the alarm object association page?

No. After a user disassociates a CVM instance from the default policy, it will not be automatically associated again on the backend.

Can I restore an alarm by stopping and restarting it?

No. Stopping and restarting an alarm are only useful for disabling a no longer needed alarm policy and will not change the alarm status.

What is the default alarm policy?

There is only one default policy for each project in each policy type. The default policy will be automatically created after you purchase an instance, which can be modified but not deleted. Cloud Monitor will automatically create a default CVM alarm policy (alarms will be triggered when disks become read-only or ping becomes unreachable) and a default TencentDB policy (alarms will be triggered if the used disk capacity is greater than 90 MB or disk utilization exceeds 80% for 5 minutes).

Why cannot alarm notifications be received under the default alarm policy?

For the default alarm policy created by the system, you need to associate it with an alarm recipient group before alarm notifications can be received.

Which Tencent Cloud products support the default alarm policy?

Currently, the default alarm policy is only supported by CVM, TencentDB for MySQL, TencentDB for Redis, TencentDB for SQL Server, TencentDB for MongoDB, TencentDB for MariaDB, API Gateway, and Direct Connect. Other Tencent Cloud products will support the default alarm policy in the future. If you have any questions, please [submit a ticket](#) for assistance.

Why are alarm notifications still received after a CVM instance is disassociated?

Because the system's data monitoring has latency, it is normal to still receive alarm notifications for a short period of time after the alarm policy is disassociated from a CVM instance.

Where can I modify the alarm notification message template?

Currently, it cannot be modified.

Why cannot the configured alarm recipients be read in custom alarm monitoring?

Basic Tencent Cloud resource monitoring and custom monitoring use different sub-account permissions. A sub-account does not have permission to query information about other sub-accounts by default. After the Cloud Monitor root account grants the `QcloudMonitorFullAccess` permission to a sub-account, the configured alarm recipients of basic Tencent Cloud resources monitoring cannot be synced with the alarm recipients of custom monitoring. If the sub-account needs to read configured alarm recipients in custom monitoring, you need to log in to the [CAM Module](#) with the root account and grant the `QcloudCamReadOnlyAccess` permission to the sub-account.

How many alarm states are there and what do they mean?

Not restored: an alarm has not been processed or is being processed.

Restored: an alarm has been restored to its normal state.

Insufficient data: either the alarm policy that generated the alarm has been deleted, the CVM instance has migrated from one project to another, or no data is reported as Agent is not installed or has been uninstalled.

What alarm changes will occur if the CDN domain name alarm policy of project A is associated with the domain `a.com`, which is then migrated to project B?

The CDN domain name policy of project A will automatically be disassociated from the domain `a.com`. After disassociation, if the domain `a.com` is not associated with any other CDN domain name alarm policies, no alarm will be triggered. The automatic disassociation logic will be implemented once every day. The console data may have an update delay, which is normal.

FAQ on Cloud Monitoring

Last updated : 2019-09-26 19:35:59

1. Why is there no data in monitoring views?

1) There is no data in the monitoring views of all CVM metrics

It is likely that you have not installed the Monitor Agent. Please follow the instructions in [Install Monitoring Components](#) to install Monitor Agent.

Note:

- Only when all two processes in Monitor Agent are installed normally can the monitoring data be submitted.
- The "stargate" process monitors the "barad_agent" process and the "barad_agent" is responsible for collecting and submitting data.

Log in to Tencent Cloud Console, click "Cloud Products" - "Cloud Monitor" to enter the CVM list. If a CVM is with a yellow exclamation mark, it means that the Monitor Agent is not installed. You can click to export IP addresses of these CVMs based on the note on the top.

If you have installed Monitor Agent, but there is still no monitoring data, please check whether the CVM has just been created. If so, it is normal for certain latency of data submission. Generally, the data will be displayed in about 10 minutes. However, if the CVM has been created for a period of time, please check whether the CVM is shut down. The CVM in the shutdown status cannot submit data normally.

If you still cannot view the data, please check whether the CVM's private network DNS is set correctly. If the DNS is not set as required by Tencent Cloud, data cannot be submitted normally, thus leading to no monitoring data in the console. [Private network DNS configuration of basic network](#).

If the data still cannot be displayed normally, please submit a ticket and contact us for resolution.

2) There is no public network bandwidth data in CVM

When the CVM has no public network IP and hasn't been bound with a [Cloud Load Balancer](#), there is no public network bandwidth traffic in the CVM, so it will not generate public network bandwidth data.

2. Why does the monitoring view still indicate that a monitoring component has not been installed after installation?

If you see a yellow exclamation mark on the monitoring list page via "Cloud Monitor" - "Cloud Products Monitoring" - "Cloud Virtual Machine" and the Monitor Agent is found running normally when you log in to the CVM, it is probably attributed to the abnormal data submission due to network failure and the backend cannot detect Monitor Agent status of the CVM, so a yellow exclamation mark shows in the console. You may check whether the firewall is enabled. If the problem still persists, you can submit a ticket or contact customer service personnel for help.

CVM Agent

Last updated : 2019-12-31 10:33:30

What should I do if the CVM fails to download Agent?

If the private DNS configuration of the Cloud Virtual Machine (CVM) is incorrect, the Agent will fail to be downloaded and monitoring components will fail to report data. For more information on the private DNS configurations of Tencent Cloud CVMs, see [Private network access](#).

What is the installation directory for Agent?

- The Agent installation directory for Linux is `/usr/local/qcloud/stargate` or `/usr/local/qcloud/monitor`.
- The Agent installation directory for CoreOs is `/var/lib/qcloud/stargate` or `/var/lib/qcloud/monitor`.
- The Agent installation directory for Windows is `C:\Program Files\QCloud\Stargate` or `C:\Program Files\QCloud\Monitor`.

Why no prompt is displayed after I double-click the installer on Windows?

The installation on Windows is automatic. The installer automatically exits after installation. If you want to view the prompt during installation, run the installer in CLI mode.

Why can I only see the sgagent process after installation?

After the installation is complete, the sgagent process will start first, followed by the barad_agent process to be launched within 5 minutes. Before installation, check whether the disk partition where the installation directory resides is full, whether inode is full, whether the write permission has been granted, and whether the network is normal.

When can users view monitoring data at the frontend after installation?

If the network is normal, users can view the monitoring data at the frontend 5 minutes after the barad_agent process is started.

How can I uninstall Agent?

Run the uninstallation script in the `admin` sub-directory under the Agent installation directory to automatically uninstall Agent.

How can I restart Agent monitoring?

- For Windows
Choose **Server Manager** > **Service List** and select **QCloud BaradAgent Monitor** to stop and

then start Agent.

- For Linux

Access the `/usr/local/qcloud/monitor/barad/admin` directory, run the `stop.sh` script to stop Agent, and then run the `trystart.sh` script to start Agent.

What can cause the installation of monitoring components to fail?

- Modifying the DNS configuration can cause the backend server connection to fail.
- If the server is invaded and hackers tamper with PS files, information output will fail.

After installation, why does the monitoring view show that Agent has not been installed?

If you see a yellow exclamation mark (!) on the monitoring list page in **Cloud Monitor > Cloud Product Monitor > Cloud Virtual Machine**, log in to the CVM and check if Agent is running. If Agent is running properly, the reported failure may be caused by a network error, and the backend fails to detect the Agent status of the CVM, and a yellow exclamation mark (!) is displayed in the console. In this case, you can try enabling the firewall. If the problem persists, you can [Submit Ticket](#) or contact customer service for troubleshooting.

Why is there no monitoring data after Agent is installed?

Troubleshoot the problem by referring to [CVM has no monitoring data](#).

CVM Has No Monitoring Data

Last updated : 2020-04-14 15:58:01

How should I troubleshoot the problem where the CVM has no monitoring data?

The possible causes are as follows: Agent has not been installed, the user operates on the CVM through the console or command line, the CVM has a high load, or the private network DNS configuration for the CVM is incorrect. This document describes how to troubleshoot these problems.

Agent has not been installed

The CVM will have no monitoring data if you have not installed [Agent](#). Locate the exact causes through the following steps:

1. Check whether `barad_agent` has been installed.

If Agent has not been installed, your CVM cannot be monitored. You will not receive a notification if the CVM fails, which is highly risky. For more information on Agent, see [Installing CVM Agent](#).

The user operates on the CVM through the console or CLI

After the CVM is shut down, Agent on the instance goes offline and no data will be reported. When you perform CVM OPS such as restart, upgrade, reinstallation, or image creation in the CVM console or after logging in to the CVM, the reporting of CVM monitoring data may time out and Agent will be taken offline.

Troubleshooting: You can access the CVM details page and view operation logs to determine whether any relevant operations were performed on the CVM at that time.

The CVM has a high load

If the CVM CPU has a high load and the memory or bandwidth is used up, Agent may fail to report data.

Troubleshooting Method: You can log in to the CVM or check the monitoring view to determine whether the CPU, memory or bandwidth is fully utilized. If yes, expand the service as needed.

The DNS configuration in the CVM is incorrect

If the private DNS configuration in the CVM is incorrect, Agent may fail to report data.

Troubleshooting Method: For more information on private network DNS configuration, see [Private Network Access](#).

Troubleshooting methods for other problems

Using the Agent management tool for troubleshooting in Linux

1. Download the Agent management tool.

```
wget http://update2.agent.tencentyun.com/update/monitor_agent_admin && chmod +x monitor_agent_admin
```

2. Install Agent.

```
./monitor_agent_admin install
```

3. Run the following command to troubleshoot and fix the problem. If the problem persists, submit a ticket along with the tool output file **monitor_agent_admin-*.zip**. We will help you troubleshoot the problem.

```
sh ./monitor_agent_admin check
```

Other operations of the Agent management tool

- i. Download the Agent management tool.

```
wget http://update2.agent.tencentyun.com/update/monitor_agent_admin && chmod +x monitor_agent_admin
```

- ii. Install Agent.

```
./monitor_agent_admin install
```

- iii. Uninstall Agent.

```
./monitor_agent_admin uninstall
```

- iv. Reinstall Agent.

```
./monitor_agent_admin reinstall
```

4. Troubleshoot and fix the problem.

```
./monitor_agent_admin check
```

- vi. Restart Agent.

```
./monitor_agent_admin restart
```

Troubleshooting common problems in Windows

1. If Agent has been installed on your CVM, check whether barad_agent logs are rolled every minute in real time and reported successfully.

Log path in Windows: `C:\Program Files\QCloud\Monitor\Barad\logs\info.log`

Each log contains "nws send succ".

2. If the logs are not rolled, check whether Agent scheduling is normal (this usually occurs in Linux, and generally caused by system time change).

You can restart barad_agent and check whether the

`/usr/local/qcloud/monitor/barad/log/executor.log` log file contains any errors.

3. If reporting fails (nws send fail), locate the problem (such as timeout, CVM connection failure, or domain name resolution failure) based on the logs.

You can retrieve the reporting address from `nws_url` in the plugin.ini file under the etc directory.

4. If "nws send fail" does not appear during reporting, perform the following steps:

- i. Check whether the uuid file has been modified.

uuid file path:

In Linux: `/etc/uuid`

In Windows: `C:\windows\system32\drivers\etc\uuid`

The latest file named in uuid format in the `C:\windows\system32\drivers\etc\` directory

- ii. If the uuid file has not been modified, check the CVM timestamp.

In Linux, run the `/usr/sbin/ntpdate ntpupdate.tencentyun.com` command to check whether the time change is 50 seconds or less. If the time change exceeds 50 seconds, restart barad_agent.

```
/usr/sbin/ntpdate ntpupdate.tencentyun.com  
[14734]: adjust time server 10.142.25.101 offset 0.002232 sec
```

5. If the problem persists, [submit a ticket](#) to our customer service for troubleshooting.

