# Tencent Cloud Observability Platform FAQs

## Product Documentation

# Contents

# FAQs

# General

Last updated：2024-01-27 17:35:59

### No monitoring data available for a CVM

The possible causes are as follows:

The Agent is not installed or launched.

The reporting domains cannot be resolved.

The Agent failed to obtain the UUID.

The CVM instance is shut down or being restarted.

The CVM instance is under high load.

To troubleshoot, please see CVM Has No Monitoring Data.

### How do I create Tencent Cloud Observability Platform (TCOP) alarm policies?

1. Log in to the TCOP console.

2. Click **Alarm Configuration** > **Alarm Policy** to access the alarm policy configuration page.

3. Click **Create** to configure alarm policies.

For more information, see Creating Alarm Policy.

### How does TCOP pull monitoring data?

You can obtain the monitoring data of Tencent Cloud services through the API GetMonitorData.

For more information, see Using API to Pull Tencent Cloud Service Monitoring Data.

### How do I quickly create a TCOP dashboard?

See Quickly Creating a Dashboard

### No alarm is received

The possible causes are as follows:

The alarm policy has not been enabled.

The alarm SMS quota is insufficient.

The alarm notification channel has not been configured or verified.

No user has been added to the recipient group.

The alarm trigger conditions have not been met.

To troubleshoot, please see No Alarm Is Received.

### How do I create a recipient (group)?

Alarm recipients/ recipient groups determine who can receive alarm notifications. You can put people who pay attention to the same alarm in the same group. When the alarm is triggered, people in the group will receive the corresponding alarm notification. For more information, see Creating Recipient (Group).

### CVM is unreachable when pinged

If you receive a an alarm notification from CVM indicating that CVM is unreachable when pinged, you can refer to CVM Is Unreachable When Pinged to troubleshoot. If the alarm notification disturbs you, disable it as instructed in the “Disabling the alarm policy” section in the aforementioned documentation.
For more troubleshooting information, see CVM Is Unreachable When Pinged.

# Alarm Service

Last updated：2024-01-27 17:35:59

### Why can't I receive alarm notifications through some alarm channels?

**Alarm notifications cannot be received through SMS**:
In the user list in the CAM console, click a username to enter the user details page and check whether the user's mobile 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 tier of SMS messages has been used up. For more information, please see SMS Alarm Channel.
**Alarm notifications cannot be received through email**:
In the user list in the CAM console, click a username to enter the user details page and check whether 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 can't some recipients in the alarm recipient group receive alarm notifications?

Their 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 which 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 can't an alarm notification be received if it is not resolved for several days?

Non-repeated alarm notifications: only one alarm notification will be received through each alarm channel.
Default logic for repeated alarm notifications (once every 5 minutes, hour, or day):
The alarm notification will be sent to you at the configured frequency for 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.

### Will an alarm notification be received if the corresponding alarm is resolved?

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

### 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 resolve an alarm by disabling it?

No. The alarm switch is only used to disable 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 is automatically created after you purchase an instance, which can be modified but not deleted.
Tencent Cloud Observability Platform will automatically create a default CVM alarm policy (alarms will be triggered when disks become read-only or unreachable ping occurs) 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 can't 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 supported only 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 it 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?

The system's data monitoring has a certain 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 can't the configured alarm recipients be read in custom monitoring alarming?

Basic Tencent Cloud resource monitoring and custom monitoring use different sub-account permissions. A sub-account has no permission to query information of other sub-accounts by default. After the Tencent Cloud Observability Platform root account grants the `QcloudMonitorFullAccess` permission to a sub-account, alarm recipients configured in basic Tencent Cloud resource monitoring cannot be synced to 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 available in monitoring and what do they mean?

| Alarm Status | Description |
| --- | --- |
| Not resolved | An alarm has not been processed or is being processed. |
| Resolved | Normal status has been restored |
| Insufficient data | The alarm policy that triggered an alarm has been deleted.<br>The CVM instance has been migrated from one project to another.<br>No data is reported because Agents have not been installed or have been uninstalled. |
| Expired | The alarm policy has changed.<br>The latest triggering time of the alarm has not been updated for more than 24 hours. |

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

The CDN domain name policy of project A will be automatically disassociated from the domain name `a.com` . If the domain name `a.com` is not associated with any CDN domain name alarm policy, no alarm will be triggered. The automatic disassociation logic is implemented once every day, so it is normal if the data on the console is not up-to-date.

# Concepts

Last updated：2024-01-27 17:35:59

## What is Tencent Cloud Observability Platform?

Tencent Cloud Observability Platform (TCOP) 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 TCOP operations such as pulling monitoring statistics. For more information, see API Category. We recommend that you read Overview and Monitoring Overview before using TCOP APIs.

## What is Custom Tencent Cloud Observability Platform?

Custom Tencent Cloud Observability Platform 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 Tencent Cloud Observability Platform to configure and submit the metrics. The submitted data is processed by the powerful Tencent Cloud Custom Tencent Cloud Observability Platform 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 Tencent Cloud Observability Platform also supports alarms that help you detect exceptions promptly and monitor your applications in real time.

## What is Basic Tencent Cloud Observability Platform?

Basic Tencent Cloud Observability Platform is the main entry for monitoring and managing all cloud services. You can use it to view comprehensive and detailed monitoring data. Basic Tencent Cloud Observability Platform 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 Tencent Cloud Observability Platform?

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

## Do CDH instances support Tencent Cloud Observability Platform?

No.

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

1. Log in to the Tencent Cloud Observability Platform 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.

**Note：**

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 Tencent Cloud Observability Platform issues?

For more information on how to troubleshoot Tencent Cloud Observability Platform issues, see Troubleshooting.

# Monitoring Charts

Last updated：2024-01-27 17:35:59

## 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" - "Tencent Cloud Observability Platform" 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 "Tencent Cloud Observability Platform" - "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 Agents

Last updated：2024-01-27 17:35:59

### What do I do if there is no CVM monitoring data?

The possible causes are as follows:
The Agent is not installed or launched.
The reporting domains cannot be resolved.
The Agent failed to obtain the UUID.
The CVM instance is shut down or being restarted.
The CVM instance is under high load.
To troubleshoot, please see CVM Has No Monitoring Data.

### What do I do if the Agent cannot be downloaded to the CVM instance?

If the private DNS of the CVM is incorrectly configured, the Agent will fail to be downloaded and monitoring components will fail to report data. For more information about the private DNS configurations of CVMs, please see Private Network Access.

### What is the installation directory of the 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 I view the monitoring data in the frontend after the 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 the installation, why does the monitoring chart show that the Agent is not installed?

If you see a yellow exclamation mark (!) on the monitoring list page in **Tencent Cloud Observability Platform** > **Cloud Product Monitor** > **Cloud Virtual Machine**, log in to the CVM instance and check whether the Agent is running properly. If so, the reported failure may be caused by a network error, which stops the backend from detecting the Agent status of the CVM. In this case, you can enable the firewall. If the problem persists, submit a ticket to contact us for troubleshooting.

### Why is there no monitoring data after Agent is installed?

You can troubleshoot by referring to CVM Has No Monitoring Data.

# Dynamic Alarm Threshold

Last updated：2024-01-27 17:35:59

## What is the sensitivity of dynamic alarm thresholds?

The sensitivity of dynamic thresholds is the extent to which metrics can deviate from their acceptable ranges before alarms are triggered. It varies with your monitoring needs.

<escape>

| Sensitivity | Note |
| --- | --- |
| High | The tolerance of deviation is low, and you receive a relatively large amount of alarm notifications. |
| Medium | The tolerance of deviation is medium, and you receive a medium amount of alarm notifications. This is the default setting. |
| Low | The tolerance of deviation is high, and you receive a small amount of alarm notifications. |

**Note:**

On the product level, you can set the sensitivity of alarms to high, medium, or low, which corresponds to different backend configuration. Sensitivity is a hyperparameter, whose value is determined by the model through a continuous learning process and is inaccessible to users.

After a sensitivity level is selected, the allowed deviation, which is calculated dynamically, for metrics that fluctuate widely tends to be big, and that for metrics that change less dramatically tends to be small.

You can use the shading graph of dynamic alarm thresholds to determine which sensitivity level fits your needs, or accept the default setting (medium), which delivers satisfactory results in most application scenarios, especially on percentage and delay metrics.

## Can I create only 20 policies for dynamic alarm thresholds at most?

The free quota for dynamic alarm threshold policies is 20, and you can create up to 20 alarm objects (or dimension combinations) under each policy by default. To use additional dynamic threshold policies beyond the free quota, you can submit a ticket to purchase a package.

## What documents has Tencent Cloud published on dynamic alarm thresholds?

**Operation Guide Documentation**Dynamic Threshold Alarm OverviewUsing Dynamic Threshold Alarm**Best Practice Documentation**Best Practice > Dynamic Alarm Threshold

# CM Connection to Grafana

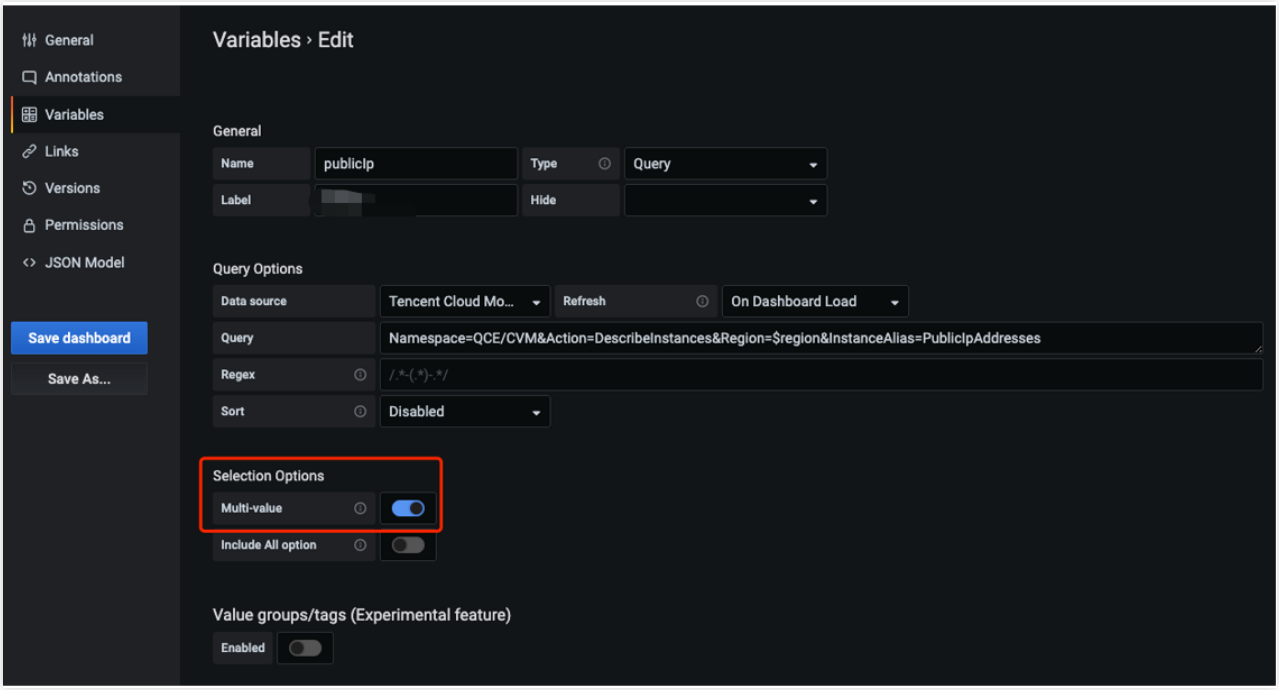
Last updated：2024-01-27 17:35:59

### Does the plugin support multi-region query in the same panel?

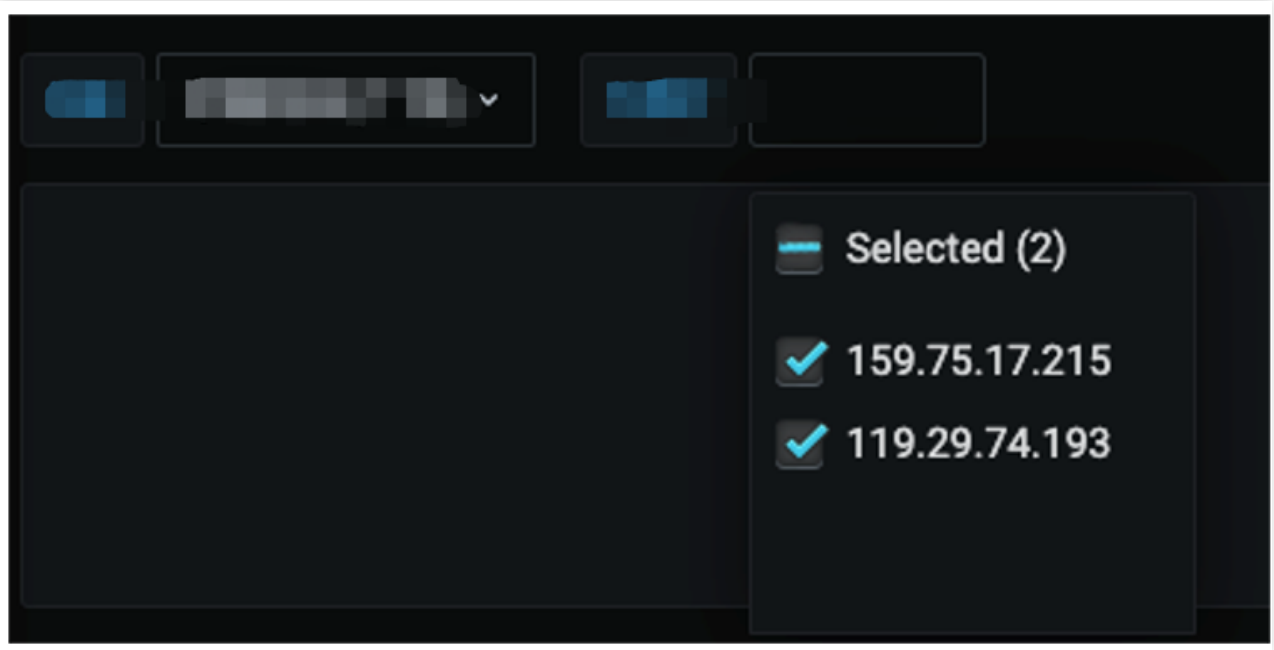
If the `region` template variable is used in the dashboard, only single-region query is supported. To compare instances in multiple regions, you can create multiple query targets in the same panel.

### Does the plugin support comparison of multiple instances in the same region?

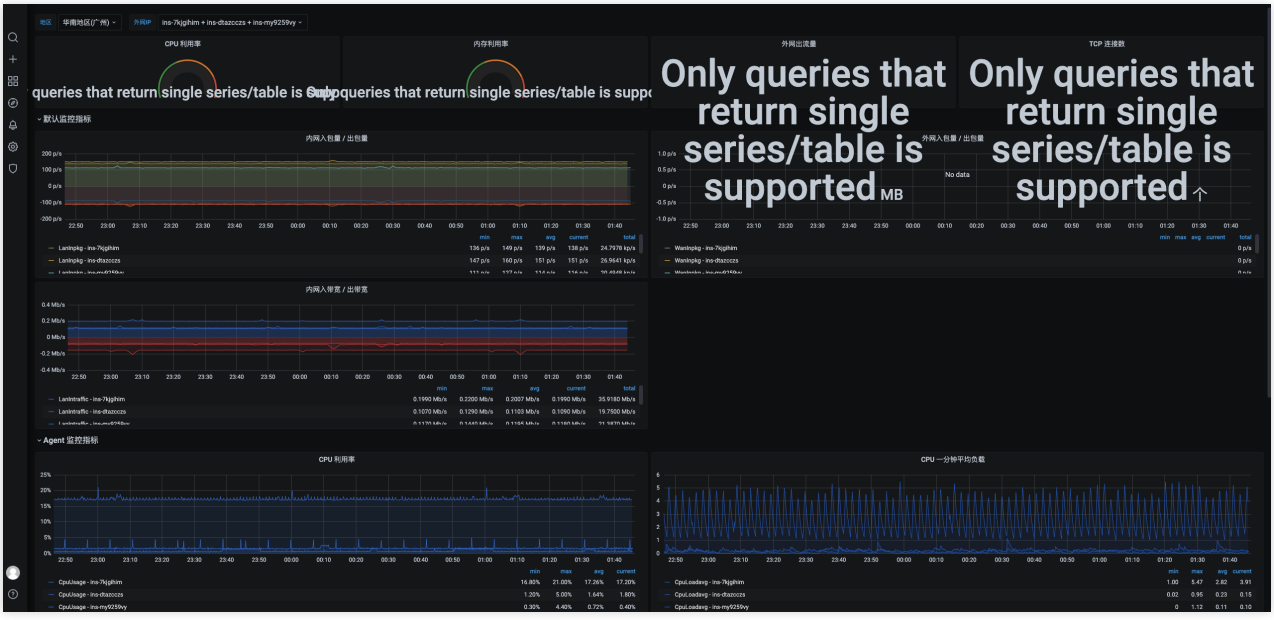
You can set `Multi-value` under `Selection Options` in the template variable to `true`.




You can select multiple instances from the drop-down list in the dashboard as shown below:




**When I compare multiple instances, why is the error `Only queries that return single series/table is supported` reported in the panel?**




Some panel types such as `dashboard` chart only support single-instance query. If you need to compare multiple instances, please use a line chart.

**The instance drop-down list in the template variable shows `InstanceId`. How do I make it show `InstanceName`?**

You can use `InstanceAlias=InstanceName` in the template variable or use the `display` attribute for splicing; for example:

1. `Namespace=QCE/CVM&Action=DescribeInstances&Region=$region&InstanceAlias=InstanceName`
2. `Namespace=QCE/CVM&Action=DescribeInstances&Region=$region&display=${InstanceId}-${InstanceName}`

**Note:**

If `InstanceAlias` and `display` appear at the same time, the drop-down list will only show the values of `display`.