

Cloud Monitor

Quick Start

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

Quick Start

Monitoring Overview

Dashboard Creation

Instance Group

Alarm Service

Tencent Cloud Product Monitoring

Traffic Monitoring

Quick Start

Monitoring Overview

Last updated : 2020-05-08 18:24:18

This document describes how to quickly view Tencent Cloud product monitoring information in [Cloud Monitoring Console](#).

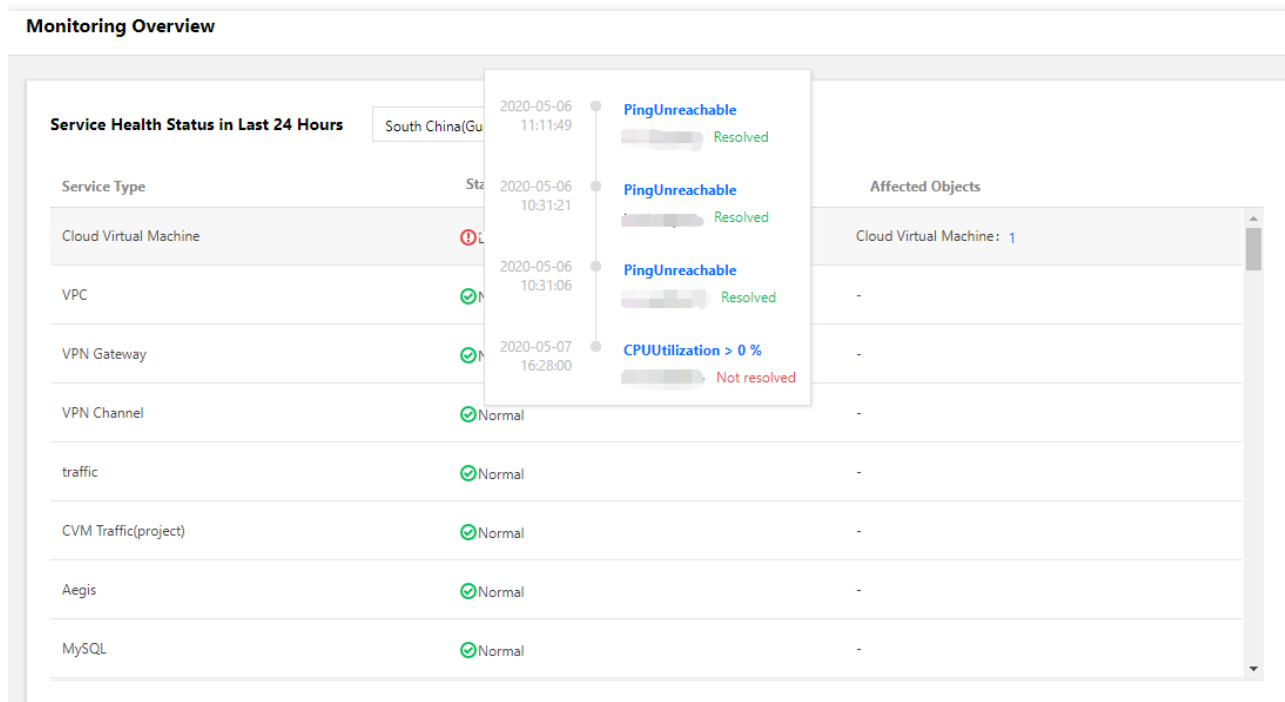
Feature Overview

Monitor Overview displays an overview of Tencent Cloud product monitoring and alarms, allowing you to view the health status of your Tencent Cloud products in real time and ensure their normal operations.

Product Overview

Tencent Cloud product overview displays an overview of the monitored health status of all Tencent Cloud products in the last 24 hours, keeping you informed on the status of all your cloud resources.

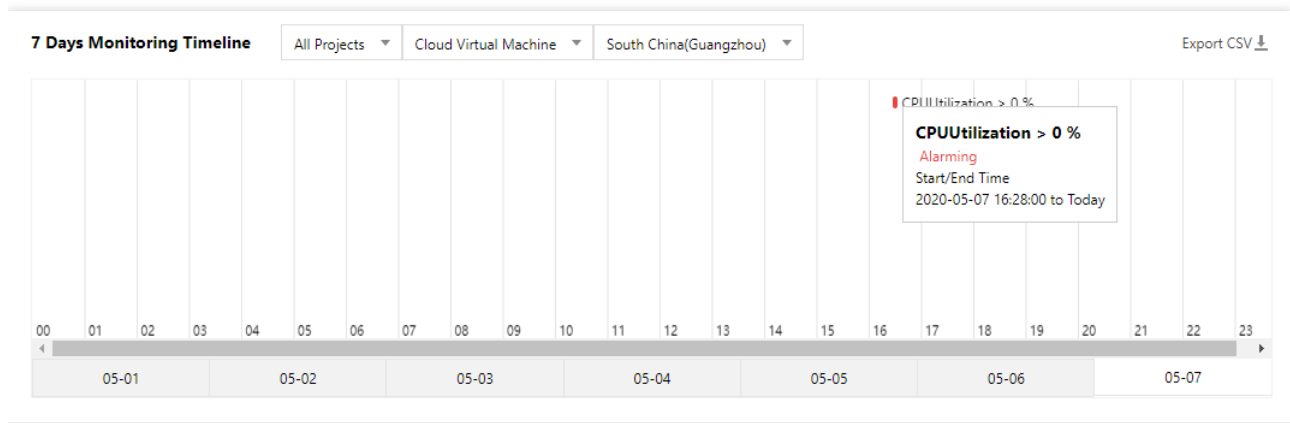
If there is an exception in the chart, you can hover over the exception icon to view its causes.



Alarm Overview

Alarm overview displays the statistics and SMS usage of monitored objects in the last 7 days, allowing you to easily view alarms and quickly troubleshoot exceptions.

If there is a red bar in the chart, you can hover over it to view the exception.



For more information on monitoring statistics, please see [Monitoring Statistics](#).

Dashboard Creation

Last updated : 2021-06-08 16:15:21

This document describes how to quickly create a dashboard.

Overview

Dashboards provide users with a custom monitoring dashboard service, which allows them to customize basic metrics and monitoring metrics across products and instances in order to display the resources of a business or cluster in one place.

Preparations

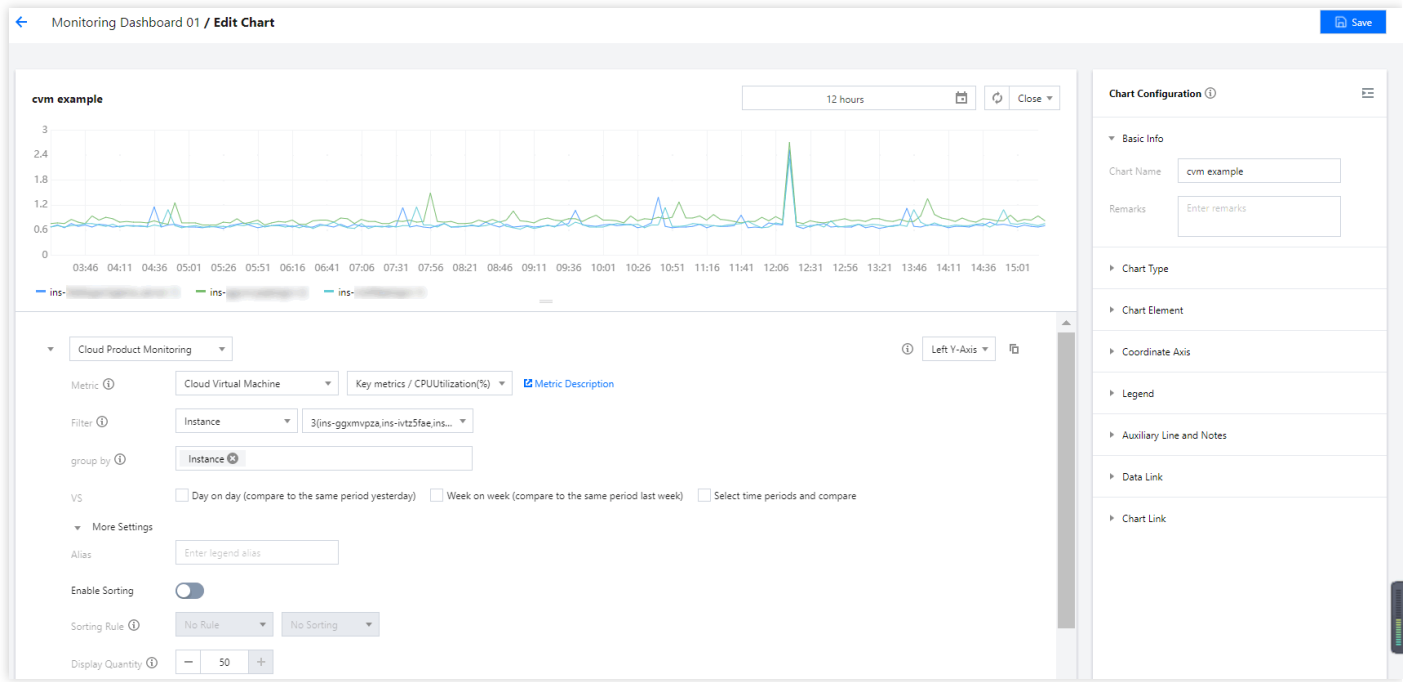
1. Log in to the [Cloud Monitor console](#).
2. In the left sidebar, click **Dashboard > Dashboard List**.

Step 1: Create a Dashboard

On the **Dashboard List** page, click **Create Dashboard** in the upper-left corner.

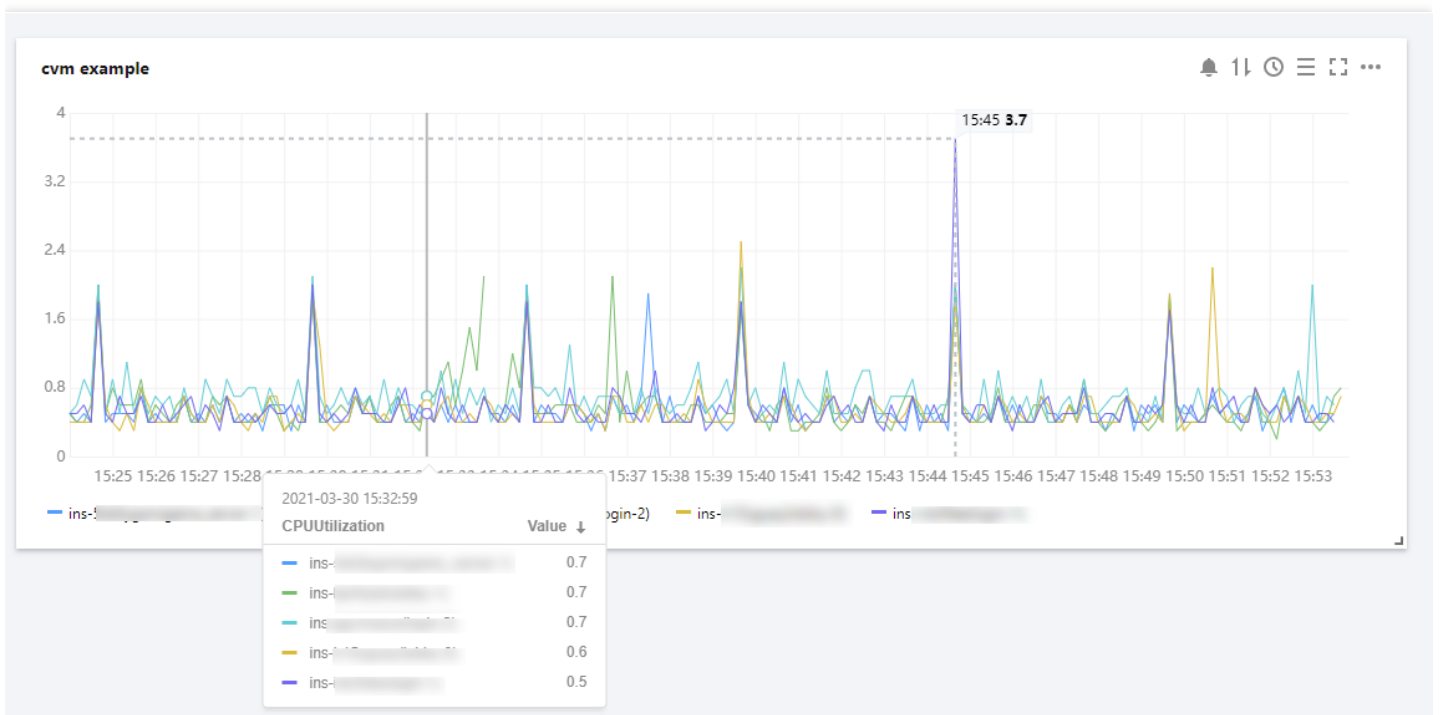
Step 2: Create a Monitoring Chart

1. On the **New Dashboard** page, click **Create Chart**.
2. Set the metric information from below the chart and customize a chart name on the right of the chart. After this, click **Save** in the upper-right corner. For more information, please see [Step 1: Create a metric](#).



Step 3: View the Monitoring Chart

After creating the monitoring chart, you can view it on the dashboard management page.



Note :

For more information about dashboard settings, please see [Dashboard](#) in the operation guide.

Instance Group

Last updated : 2022-08-25 18:07:30

Feature Overview

You can group cross-region and cross-project group instances of a Tencent Cloud product for unified management. When creating a large number of instances, you can create instance groups as needed. By managing instance groups, you can better manage instances, configure alarm policies, and improve Ops efficiency.

Use Cases

- Alarm policies can be set for cross-instance and cross-region projects of the same product in a unified manner.
- You can manage various resources under your Tencent Cloud account by service category.

Notes

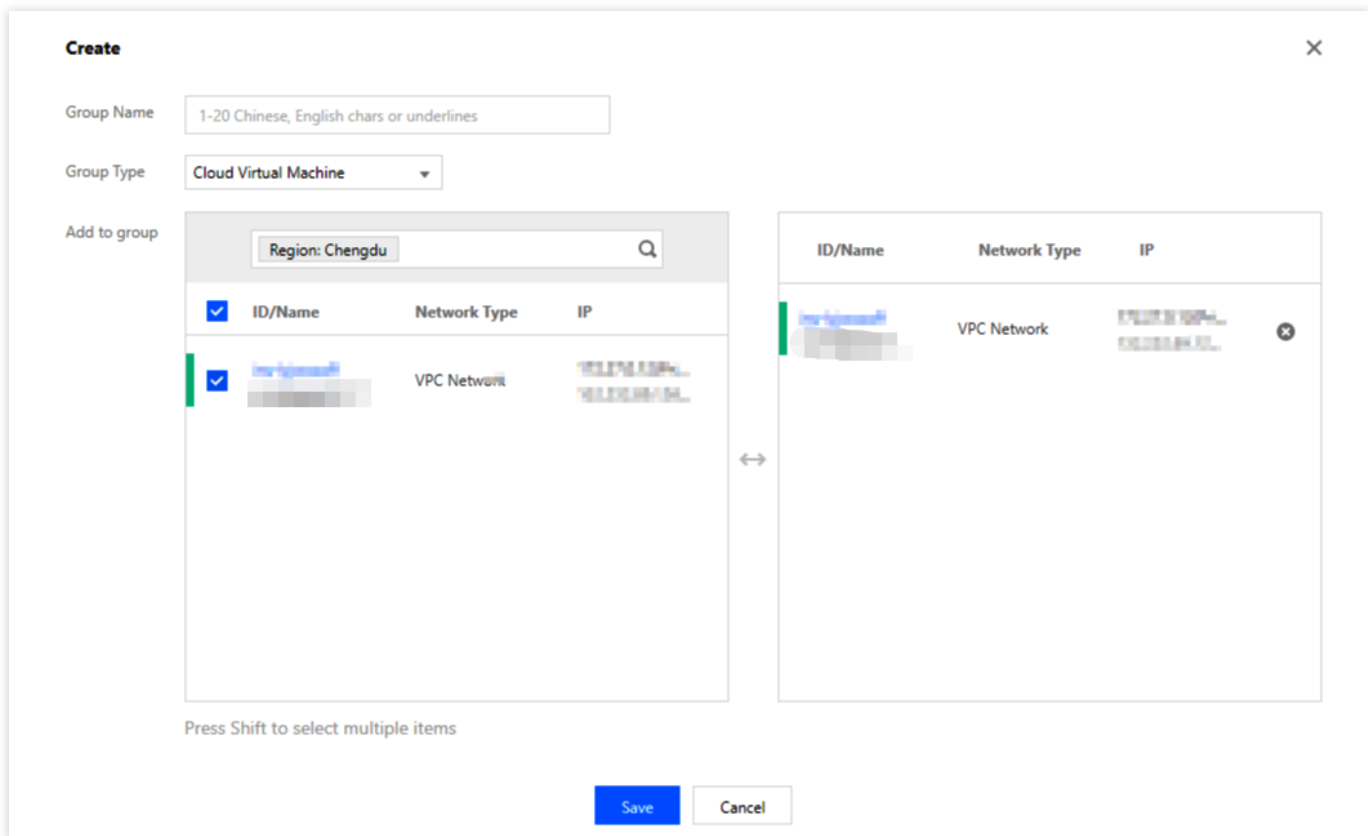
- Each instance group can contain up to 2,000 instances, and a maximum of 200 instances can be added to an instance group at a time.
- By grouping instances, you can manage cross-region and cross-project group Tencent Cloud products in a unified manner and configure alarm policies to avoid repeated operations and improve Ops efficiency.

Directions

Creating an instance group

1. Log in to the [CM console](#).
2. On the left sidebar, click **Instance Group** to enter the **Instance Group** page.
3. Click **Create** and configure the following fields:
 - Group Name: Enter the instance group name.
 - Group Type: Select an option as needed.

- Add to Group: Select instances to be added to the group.



4. Click **Save**.

Editing an instance group

Note :

- If an instance group has been bound to an alarm policy, the instances added to it will be automatically bound to the alarm policy.
- If an instance group has been bound to an alarm policy, the instances removed from it will be unbound from the alarm policy.

1. Log in to the [CM console](#).
2. On the left sidebar, click **Instance Group** to enter the **Instance Group** page.
3. Select the name of the target instance group to enter the instance management page. You can create or delete instances in the instance group on this page.

Adding an instance

1. Click **Add**.


2. In the pop-up window, select the target instance.
3. Click **OK**.



Removing an instance

1. Select the target instance and click **Remove**.
2. In the pop-up window, click **Remove**.

Deleting an instance group

1. Log in to the [CM console](#).
2. On the left sidebar, click **Instance Group** to enter the **Instance Group** page.
3. Find the target instance group and click **Delete** in the **Operation** column on the right.

Bound Alarm Policies	Last Modified 	Operation
0count	100010380631 2019/12/25 17:13:00	Replication Delete

Lines per page 20  

4. In the pop-up window, click **Confirm**.

Note :

When an instance group bound to an alarm policy is deleted, the alarm policy will become invalid.

Copying an instance group

1. Log in to the [CM console](#).
2. On the left sidebar, click **Instance Group** to enter the **Instance Group** page.

3. Find the target instance group and click **Copy** in the **Operation** column on the right.

Bound Alarm Policies	Last Modified ↑	Operation
0count	100010380631 2019/12/25 17:13:00	Replication Delete

4. In the pop-up window, click **Copy**.

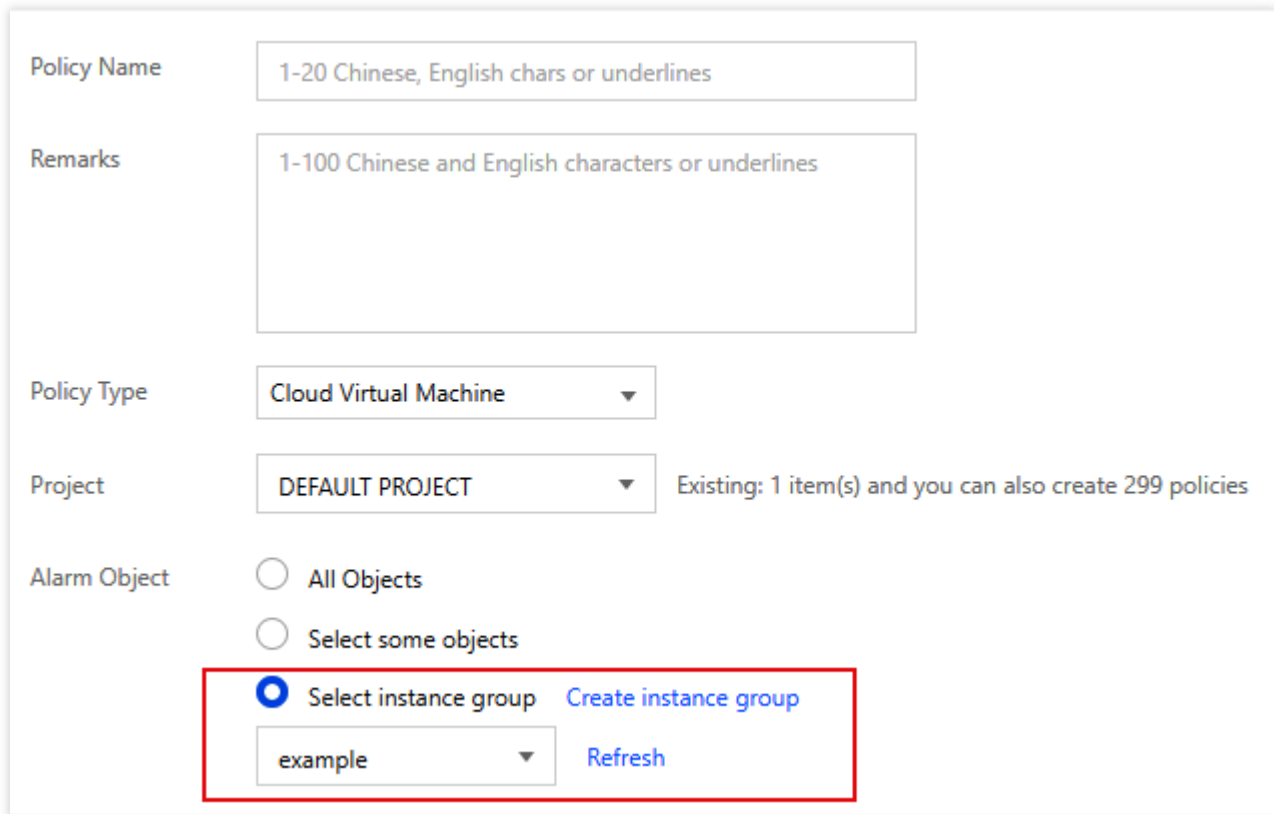
Note :

When an instance group is copied, only instances in the group will be copied. If the copied instance group is bound to an alarm policy, the binding relationship will not be copied.

Binding an instance group to an alarm policy

1. Log in to the [CM console](#).
2. On the left sidebar, click **Alarm Configuration** > **Alarm Policy** to enter the alarm policy management page.
3. Click **Create** to enter the **Create Policy** page.

4. Find the **Alarm Object** configuration item and select **Instance Group**.



Policy Name

Remarks

Policy Type

Project Existing: 1 item(s) and you can also create 299 policies

Alarm Object

- All Objects
- Select some objects
- Select instance group [Create instance group](#)

[Refresh](#)

5. Complete settings of other configuration items on the page.

Alarm Service

Last updated : 2021-06-08 16:15:54

This document describes the features and operation processes of the alarm management module.

Feature Overview

Alarms are provided for monitoring metrics. You can create alarms to stay informed on status changes of certain metrics. The specific metrics will be monitored during a certain period of time, and alarms will be sent through channels such as WeChat and SMS at specified intervals based on the specified threshold.

Use Cases

To prevent the normal operation of your system from being affected when a monitoring metric of your CVM instance reaches a certain value, you can configure alarm rules for these metrics. The alarm system can then automatically check the monitoring data and send alarm notifications to the admin when the monitoring data meets the configured conditions, which will help you stay informed of business exceptions and quickly solve them.

Directions

Creating an alarm

Step 1. Create an alarm contact

1. Log in to the [CAM Console](#).
2. On the left sidebar, select **Users > User List > Create User** to access the sub-user creation page.
3. Select **Custom Create > Receive messages only**.
4. Enter the user information and click **Done**.

For more information on how to manage users, please see [User Group Management](#).

Step 2. Create an Alarm Recipient Group

1. Log in to the [CAM Console](#).
2. On the left sidebar, select **User Groups > Create User Group** to access the user group creation page.

3. Enter the user group name and click **Next**.
4. Select the associated policy. You can also choose to leave the associated policy empty. Once you are done, select **Next > Done** to create the user group.
5. In the user group list, find the user group you just created. In the "Operation" column on the right, click **Add User** and select the target users.
6. After adding the users, click **OK**.

- For more information on how to create user groups, please see [Creating User Groups](#).
- Basic cloud resource monitoring and custom monitoring have different sub-account permissions. A sub-account has no permission to query information about other sub-accounts by default. You can grant the relevant query permission if needed.
 - If a sub-account needs permission to view user groups for basic Tencent Cloud services monitoring, you need to log in to the [CAM Console](#) with the root account and grant the `QcloudMonitorFullAccess` permission to the sub-account (if only this permission is granted, the alarm recipients for services monitoring will not be synced with that for custom monitoring).
 - If a sub-account needs permission to view user groups for custom monitoring, you need to log in to the [CAM module](#) with the root account and grant the `QcloudCamReadOnlyAccess` permission to the sub-account.

Step 3. Create an alarm policy

1. Log in to the [Cloud Monitoring Console](#).
2. On the left sidebar, select **Alarm Configuration > Alarm Policy** to access the alarm policy configuration page.
3. Click **Add** to configure an alarm policy.
 - Configure basic settings such as policy name, remarks, policy type, and project.
 - Set alarm objects.
 - Set alarm trigger conditions.
 - Set alarm channels.
4. After the above configurations, click **Complete**.

For more information on alarm settings, please see [Creating Alarms](#).

Viewing an alarm

1. Log in to the [Cloud Monitoring Console](#).
2. On the left sidebar, click **Monitor Overview** to access the monitoring overview page and view alarms.

Tencent Cloud Product Monitoring

Last updated : 2020-05-08 18:24:19

This document describes the features and operations of Tencent CM.

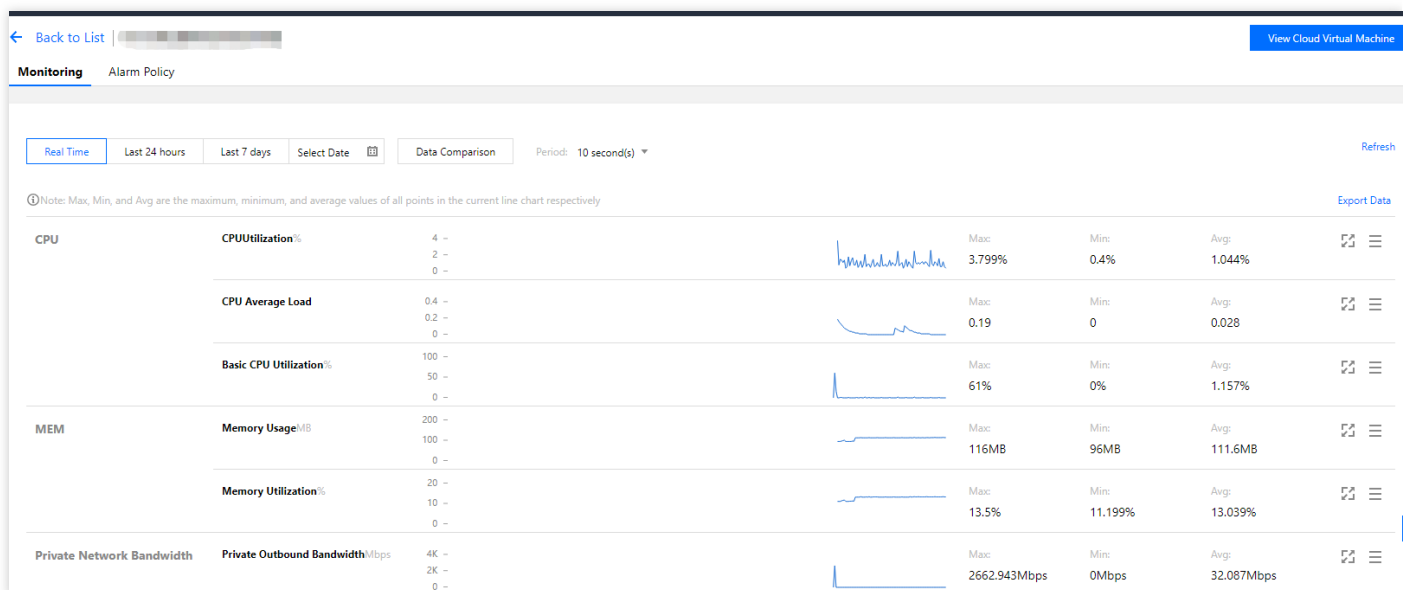
Feature Overview

Cloud Monitor is a platform that displays the performance metrics of all Tencent Cloud products. You can view the list of cloud resources and their corresponding monitoring metrics as well as alarm details under your account.

Compared with the service console that only displays the monitoring data, Cloud Monitor also displays the health status and alarm data of instances. You can quickly locate unhealthy instances, analyze cloud resource usage based on the specific data, and troubleshoot problems based on information about exceptions.

Directions

1. Log in to the [Cloud Monitoring Console](#).
2. On the left sidebar, select **Cloud Product Monitoring** > **Cloud Virtual Machine** to enter the CVM monitoring list page.
3. Find the CVM instance you want to monitor and click its name to enter the monitoring page.



Tencent Cloud services that support Cloud Monitor

For more information on Tencent Cloud services that support Cloud Monitor, please see [Overview](#).

Traffic Monitoring

Last updated : 2020-07-31 10:57:04

Overview

In order to prevent access traffic surges from affecting your business, you need to monitor the public network outbound bandwidth of CVM in real time. This document describes the traffic monitoring feature and how to use it.

Directions

Note :

Traffic monitoring displays the aggregated data of the public network outbound bandwidth of all CVM instances. Currently, data cannot be filtered by instance or region. If you want to view the public network outbound bandwidth monitoring data of individual instances, please see [Tencent Cloud Product Monitoring](#).

1. Log in to the [Cloud Monitor Console](#).
2. Click **Data Usage Monitoring** on the left sidebar to access the traffic monitoring page.

The real-time traffic monitoring data is displayed by default, and you can view the public network outbound bandwidth monitoring data in real time, in the last 24 hours, in the last 7 days, and using a custom time period. You can also move your cursor in the monitoring chart to view the monitoring data of a certain moment.

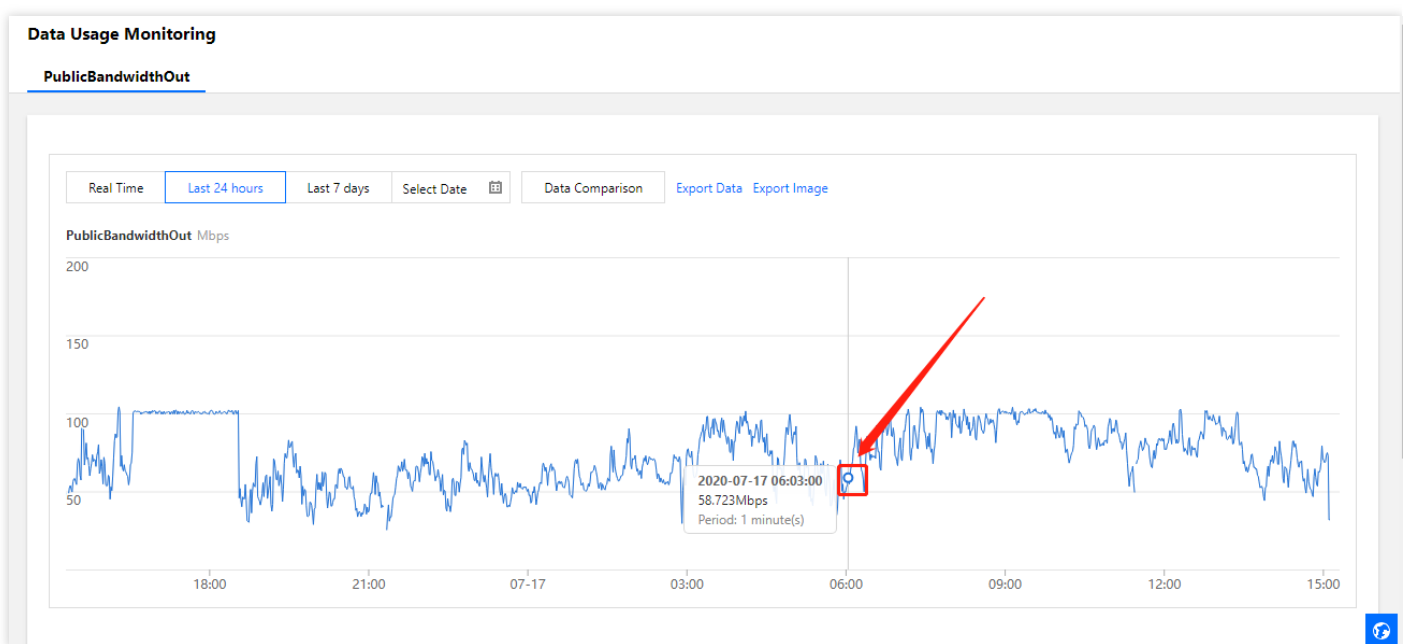


Table showing the correspondence between the time range and the monitoring data granularity:

Time Range	Granularity
< 1 day	1 minute
2-3 days	5 minutes
3-62 days	1 hour
>= 62 days	1 day

Data Comparison

Traffic monitoring supports monitoring data comparison. If you select **real time** or **last 24 hours**, the comparison will be made against the data at the same time yesterday by default. If you select **last 7 days**, the comparison will be made against the data at the same time last week by default. You can also customize the start time to be compared with the monitoring data in real-time, in the last 24 hours, or in the last 7 days, as shown below.



Note :

For more information on bill-by-bandwidth rules, please see [Public Network Billing](#).