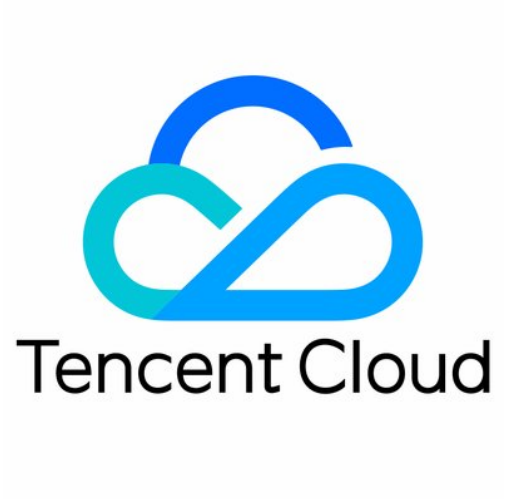
Basic Cloud Monitor

Best Practice

Product Documentation



Contents

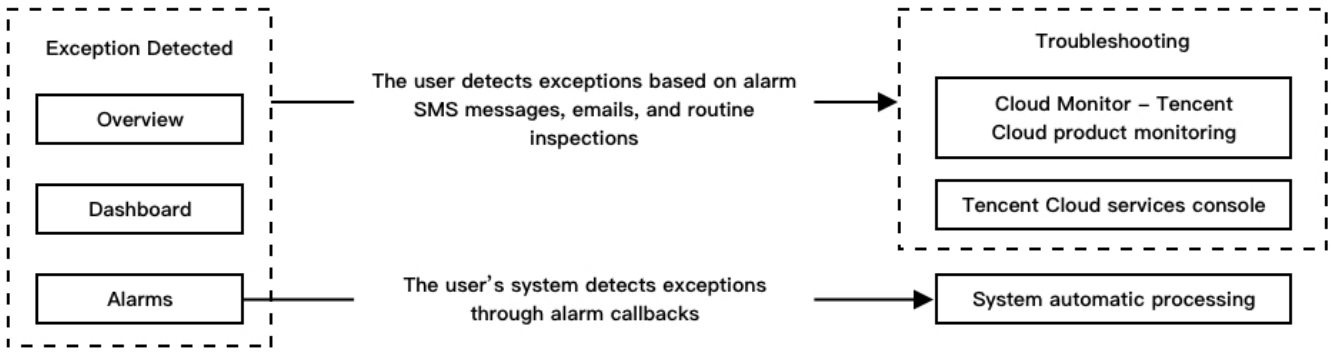
Best Practice
- Troubleshooting
- Mass monitoring scenarios
- Configuring CVM Metrics and Creating Alarms

Best Practice Troubleshooting

Last updated : 2020-07-27 10:23:34

Overview

Cloud Monitoring (CM) provides various methods to help you identify resource exceptions and multiple channels to notify you promptly.



Locating Exceptions

Detecting exceptions through alarms

Tencent Cloud uses monitoring and alarms to promptly detect an exception and notify you automatically. This helps keep you informed on exceptions in real time across all scenarios. You can log in to the Cloud Monitoring Console and configure alarm policies for resources. For more information, see Creating Alarm Policies.

If you have configured key performance metrics and events as alarm rules, you will be notified promptly in multiple ways via the alarm channel if an exception occurs.

Alarm policies configured with an alarm recipient group will be sent to you via SMS messages, emails, etc. Features such as repeated alarms and alarm aggregation are also supported to keep you informed while avoiding unnecessary notifications.

You can also configure the callback API feature in alarm channel to receive alarms promptly and process the alarm information.

Detecting exceptions through monitoring charts

You need to actively analyze the historical data and average trends of performance metrics to locate exceptions through monitoring charts. If an exception is difficult to locate using alarm rules or has not been configured with alarms, you can use monitoring charts to locate it during daily health check. Compared to alarms, monitoring charts allow you to query the global influence of resource exceptions. You can subscribe key resources to the Dashboard and configure monitoring charts to highlight exceptions in different scenarios.

For some instances, you can subscribe to details views to compare the trends of instance performance data on the Dashboard.

For resource clusters, you can subscribe to the aggregated data of a cluster to view the monitoring chart of the cluster on the Dashboard, and compare it with that of a single instance in this cluster. For more information, see Mass monitoring scenarios.

For exceptions detected through monitoring charts, you can use the sorting feature to locate specific resources related to an exception for further troubleshooting.

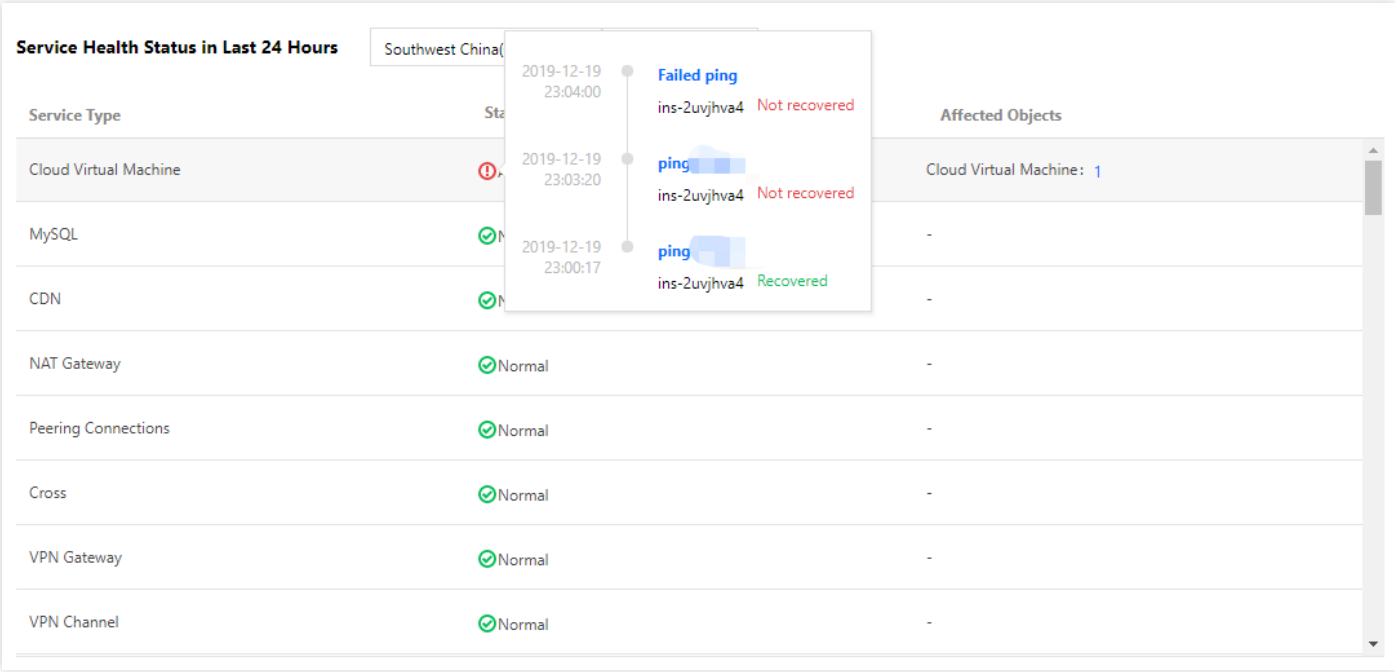
Troubleshooting

Locating exception objects on the monitoring overview page

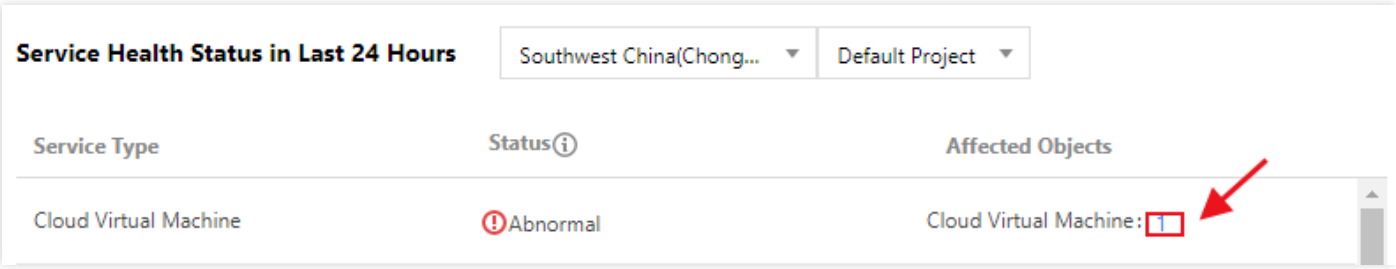
If you receive an alarm during daily health check, you can go to Monitoring Overview on the Cloud Monitoring Console.

1. Go to the overview page -> service health status module to view exceptions in each region and project.

You can browse recent exceptions by clicking on the status of each service.



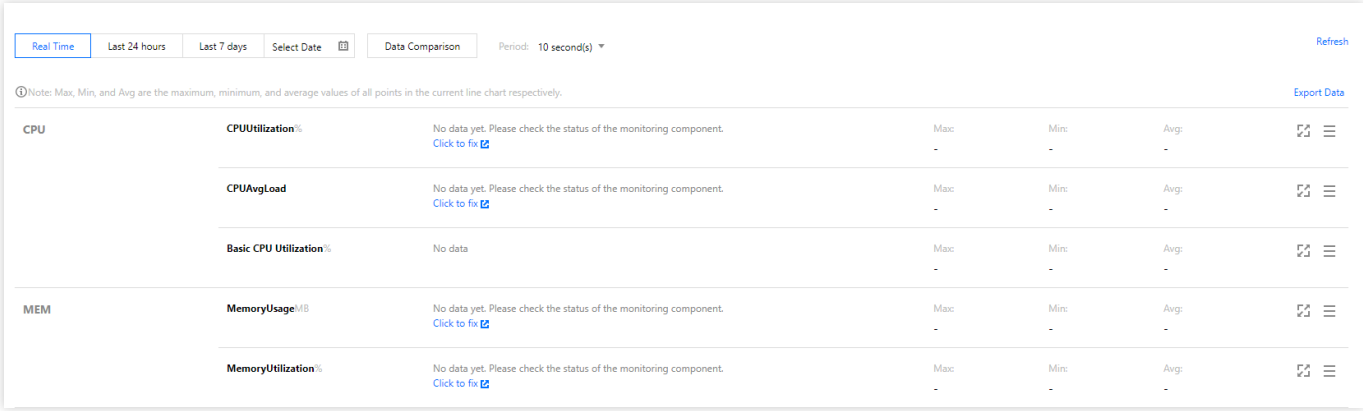
2. Click on the number of affected objects to go to the cloud product monitoring page.



Affected resource objects are automatically filtered out on the cloud product monitoring page.

3. Click on the ID of a specific object to go to the monitoring details page, where detailed information about its historical exceptions is provided.
   - The exception timeline allows you to view the current and historical information of the affected object. This helps you troubleshoot current exceptions based on historical alarms and status changes.
   - The monitoring data for resource performance allows you to compare the current and historical data of the same metric year over year and month over month, or compare data changes of

different metrics within the same period for troubleshooting.



Mass monitoring scenarios

Last updated : 2020-03-04 11:16:01

Overview

As your business continues to develop, your need for underlying resources will also increase. With more and more basic resources, the efficiency of daily monitoring becomes a bottleneck in OPS. Tencent Cloud Cloud Monitoring (CM) provides a solution for large-scale resource monitoring scenarios to customers who have a large number of resources.

Directions

Performance view for large-scale resource monitoring

With a large number of resources, it is impossible to view the metric data of all cloud resources one by one. Even if you do, you still cannot compare the data in a global way, nor detect exceptions. There are two key points when monitoring a large number of resources:

- Aggregation: The performance data of a batch of resources is aggregated. With aggregated data, you can easily understand the overall resource operation performance.
- Sorting: The data of a batch of resources is sorted by metric, allowing you to quickly identify abnormal data and corresponding resource objects.

Creating an aggregation monitoring view for large-scale resources

Using Cloud Virtual Machine (CVM) as an example:

1. CVM resources are classified and managed by service and cluster in projects. The resources of different services or clusters reside in different projects.

2. Log in to Cloud Monitoring Console.

3. In the left sidebar, click **Dashboard** to access the dashboard management page.

4. In the upper-left corner of the page, click **Add Monitoring Dashboard** to add a dashboard.

5. Click **add Monitoring Chart**, and in the pop-up configuration box, configure the monitoring item.

6. After the configuration is completed, click **OK** to complete the creation.
   - You can create multiple charts with multiple metrics in batches to avoid repeatedly selecting monitoring items.
   - You can create charts in batches in the order of objects in the list to avoid repeatedly configuring new charts when the number of resources to be monitored exceeds the content limit of a chart.
   - You can filter and search for resources, select all resources with one click, or select multiple resources by pressing **Shift**. The user-friendly batch operations facilitate the batch selection of resources, improving configuration efficiency.

7. Sum up the data of all servers to calculate the total bandwidth used by a service or cluster according to bandwidth-related metrics.
   Calculate the `Avg`, `Max`, and `Min` values of the monitoring data of all servers according to performance metrics, such as the CPU utilization, and display them in one chart. You can then obtain the average, maximum, and minimum CPU utilization of a service or cluster.

8. **Detect abnormal data in an aggregation view**. According to the overall trend of resource aggregation curves and their comparisons, you can understand the overall trends and exceptions in the performance data of resources.
   For example, you can determine whether the current bandwidth is abnormal by comparing the inbound and outbound bandwidth curves as well as the overall trend of bandwidth curves. You can also determine the overall status of resources and whether abnormal resources exist by comparing the average, maximum, and minimum CPU utilization.

9. **Locate a specific abnormal object.**

0. Click the curve at a specific time point to show a list of corresponding instances sorted by performance. You can change the sorting order and metrics, or switch the data displayed in the list by clicking different points in the curve.

xi. Hover over an instance in the sorted list. The monitoring data curve corresponding to this instance is highlighted in the curve above. Compare and analyze the monitoring curve of this instance and the overall aggregated data curve to further determine the current and historical exceptions of the instance.

xii. After confirming the specific abnormal object via the previous two steps, click the name of the abnorml object in the list to open the monitoring details page for further troubleshooting.

So far, you have completed the processes of creating a monitoring view, viewing the monitoring view, detecting an exception, and locating the exception. The chart and the sorting list allow you to intuitively view the running status of all resources, locate the specific abnormal object, and analyze the trend of an exception. This provides an effective solution to solve inefficiency in large-scale resource monitoring and difficulty in detecting exceptions.

> Currently, a maximum of 12 CVM instances can be added to each chart on the dashboard. If this does not meet your needs, you can submit a ticket to raise the limit.

Creating a details monitoring view for large-scale resources

In addition to aggregation views, you can also use a details view to detect and locate exceptions in large-scale resources.

Details view: The curves of all instances are displayed in the same chart.
Aggregation view: The curves of all instances are computed and aggregated into one or more curves by using a custom statistical method.

1. **Create a details view.**
   Creating a details view Creating a details view is similar to creating an aggregation view. When creating a details view, you do not need to select the statistical method.

2. **Detect exceptions in a details view.**
   - The more resources are in the same service or cluster, the denser the curves are in the chart. The overall trends and densities of curves in the chart indicate the overall trends and distributions of resource performance data.
   - If some curves deviate from the rest, the performance data of the corresponding instances is abnormal.

3. **Locate a specific abnormal object.**
   You can also use a details view in conjunction with a chart and a sorted list to locate a specific abnormal object. The overall process is similar to that for an aggregation view. For more information, see the sixth item for aggregation views above.

> Currently, a maximum of 12 CVM instances can be added to each chart on the dashboard. If this cannot meet your needs, you can submit a ticket to raise the limit.

Configuring alarm policies for large-scale resources

1. CVM resources are classified and managed by service and cluster in the project. The resources of different services or clusters reside in different projects.
2. Log in to Cloud Monitor Console and choose **Alarm Configuration** to create alarm policies for resources. After the resources are grouped by project, you can create a default Alarm Policy for each project.
   The default alarm policy is automatically bound to all resources in the project. If resource changes occur, such as when new resources are added, project changes, or resources are terminated upon expiration, resource objects bound to the default policy will change accordingly by default, eliminating the need for complex manual maintenance.

Configuring CVM Metrics and Creating Alarms

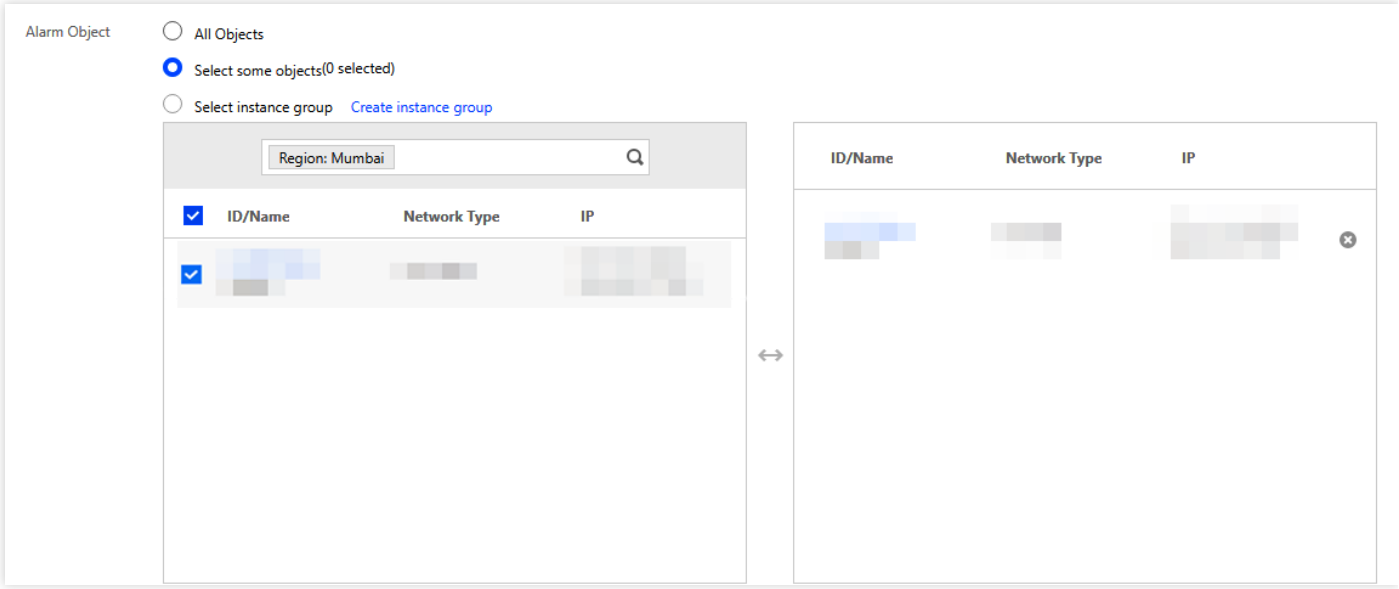
Last updated : 2020-07-27 10:23:34

Overview

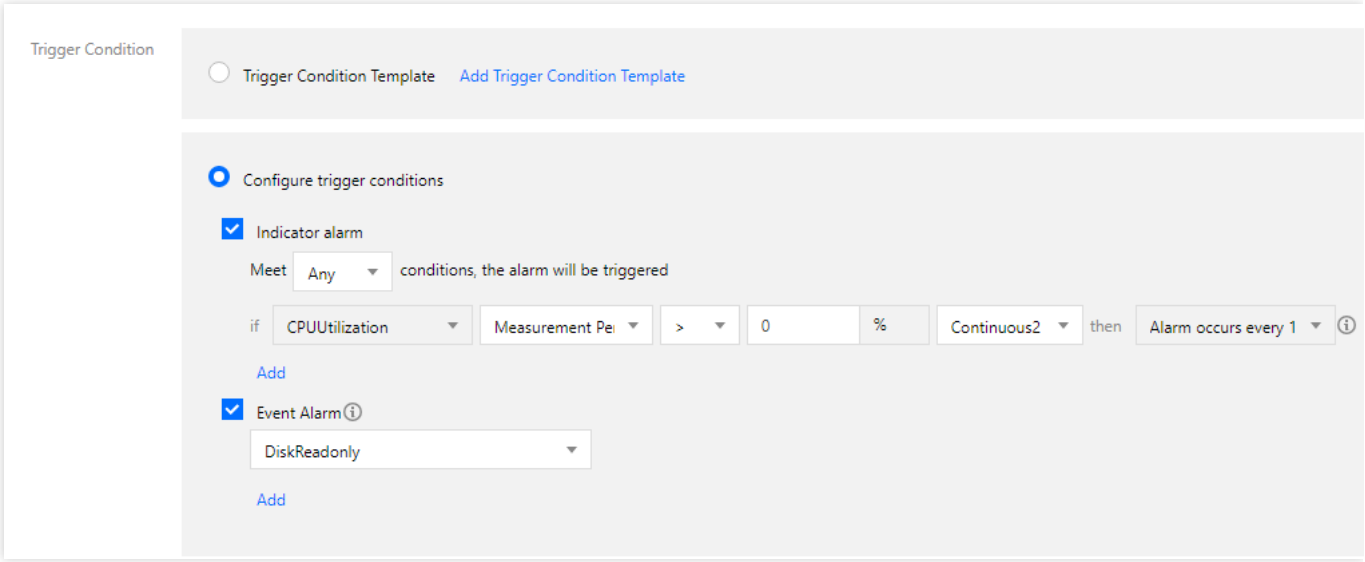
This example shows you how to configure an alarm. Assume you want to send an alarm via SMS to the number `12345678888` when the CPU utilization of CVM instance `ins-12345678` (in Guangzhou region) `exceeds 80%` for `two` consecutive 5-minute periods.

Directions

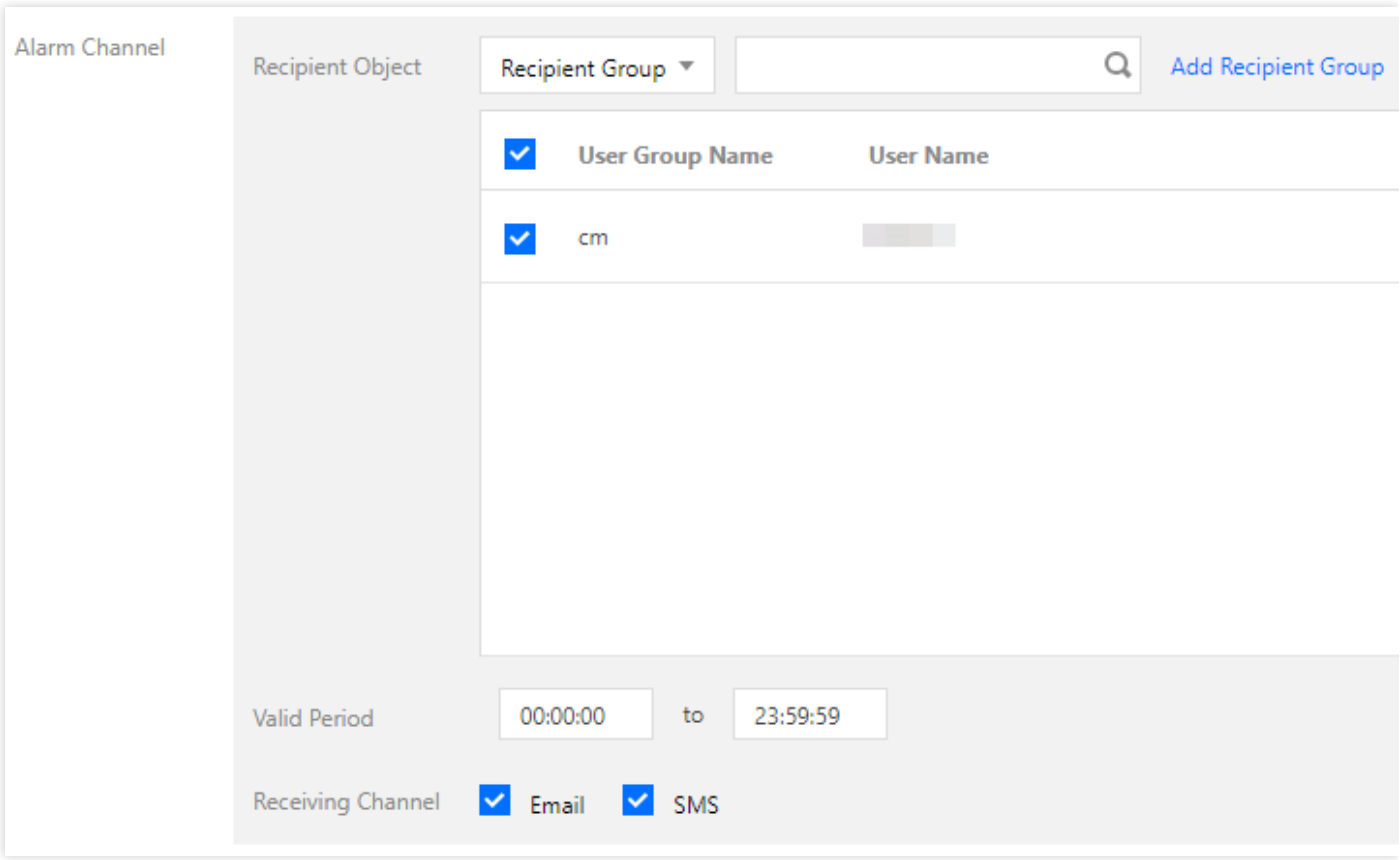
1. Log in to the Cloud Monitoring Console.
2. In the left sidebar, click **Alarm Configuration** -> **Alarm Policy**.
3. Click **Add** and configure the following items.
4. Configure the policy name and other items.
   - Policy Name: CPU alarm
   - Policy Type: Cloud Virtual Machine
5. Configure the alarm object. In the “Alarm Object” module, choose “Select some objects” and select the CVM instance.



6. Configure the trigger condition. In the “Trigger Conditions” module, configure the following conditions.
   - Select “Configure trigger conditions”
   - Select “Indicator alarm”: `CPU Utilization` `->` `80%` `5 minutes` `2 periods`
   - Alarm repetition period: `15 minutes`



7. Configure the alarm channel. Add an alarm recipient group (click **Add Recipient Group** to create one if you have not already done so).



8. Click **Complete** to complete the alarm configuration.
9. If the CPU utilization of the instance exceeds 80% for two consecutive 5-minute periods, the number `12345678888` will receive an alarm via SMS from Tencent Cloud.