Basic Cloud Monitor
Operation Guide
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

Operation Guide
  Cloud Monitoring Overview
    Key Exceptions
    Monitoring Statistics
    Customize Monitoring View
Get Monitor View
  Getting the Monitoring Data of Specified Metrics
Dashboard
  What Is a Dashboard?
  List
    Default Dashboard
    Deleting a Dashboard
    Copying a Dashboard
Dashboard
  Creating a Dashboard
  Viewing a Dashboard
  Adding a Dashboard to Favorites
  Sharing a Dashboard
  Basic Configuration
  Template Variables
  Link Management
  JSON
Monitoring Charts
  Creating a Chart
    Step 1: Create a metric
    Step 2: Configure the chart
  Use Cases of Different Chart Types
    Line Charts
    Bar Charts
    Dashboard
    Pie Charts
    Numbers
  Deleting a Chart
  Viewing a Chart
  Creating a Chart Group
  Sharing a Chart
  Copying a Chart
  Exporting Data
Alarm Service
  Configuring Alarm Policies
Configuring Alarm Policies
Configuring trigger condition templates
Alarm Receiver
  Binding and Unbinding Objects
  Creating Alarm Recipient Groups
Alarm type, channel, and quota
  Alarm Type, Channel
  SMS Channel
Alarm Callback
  Receiving Alarm Notifications through a WeCom Group
View Alarm
  Start and stop alarms
  Custom Message
Event Center
  Event center overview
  Product Event
  Product Event List
  Platform Event
Installing CVM Agents
Cloud Access Management (CAM)
The monitoring overview module is an entry through which you can view the overall monitoring information of Tencent Cloud services. In particular, you can view the information of the following key exceptions.

CVM is unreachable when pinged

The number of alarm records in the last month whose policy type is "CVM", alarm status is "Uncleared", and alarm type is "Unreachable" are displayed. Uncleared CVM alarms are generally important and may affect the normal operation of your business.

To troubleshoot the problem of CVM being unreachable when pinged, see CVM Is Unreachable When Pinged.

CVM disk is read-only

The number of alarm records in the last month whose policy type is "CVM", alarm status is "Uncleared", and alarm type is "Disk Read-Only" are displayed. If your CVM instance has any services for which data needs to be written but your CVM disk is read-only, this problem may affect the normal operation of your business.

To troubleshoot the problem of your CVM disk being read-only, see CVM Disk Is Read-Only.
Monitoring Statistics

Last updated : 2020-05-13 15:18:58

The monitoring overview module is an entry through which you can view the overall monitoring information of Tencent Cloud services. It displays the statistics of monitored objects in the last 7 days, which mainly consist of the following:

Number of unresolved alarms

It displays the number of unresolved alarms in the last month, which are grouped by alarm policy type.

CVM load statistics in the last 7 days

This section displays the CVM load statistics in the last 7 days, which are calculated based on the CPU utilization of each CVM instance. If the utilization exceeds 80%, the CVM has a high load. If below 10%, the load is low. Otherwise, the load is normal.

The figure shows the numbers of CVM instances with high, medium, and low load in the last 7 days. The Cloud Monitor backend collects the numbers of instances with high and low load once every day, and displays the statistics as curves.

CVM high load details in the last 7 days

This section displays the CVM high load statistics in the last 7 days, which are calculated based on the CPU utilization of each CVM instance. If the utilization exceeds 80%, the CVM has a high load.

- High load duration: total duration when the instance had a high load in the last 7 days.
- Number of high load occurrences: total number of times that the instance entered high load status in the last 7 days.

These statistics helps you quickly view and troubleshoot CVM exceptions, ensuring the normal operation of your business.

Public network bandwidth statistics in the last hour

This section displays the overall public network bandwidth data of all CVM instances (excluding public network bandwidth generated by other products) under your account in the last hour. These statistics helps you quickly view the status of the server cluster that provides external services, and estimate the corresponding network fee.

To view more public network bandwidth statistics, go to the Data Usage Monitoring page in the Cloud Monitoring Console.
Customize Monitoring View

Monitor Overview allows you to access the overall monitoring information of your cloud products. The Custom Monitoring View helps users quickly understand the pre-defined key metrics and is the most important feature on the monitoring overview page.

You can choose to add the core metrics (such as CPU utilization, etc.) and choose the monitored objects to be displayed on the view. You can also click on the view to show/hide the data of some monitored objects. Tencent Cloud's Cloud Monitor helps you aggregate the data of all monitored objects you have chosen on the same chart, so that you can directly view the key metrics for core services each time you visit the overview page, greatly reducing your inspection costs.

- Only filtering for CVM and cloud database metrics is supported currently, and more metrics and products will be available in the future.
- A maximum of 3 metrics can be added, with no more than 6 objects added for each metric.

Creating a Custom Monitoring View

1) Log in to the Tencent Cloud Console, select "Cloud Monitoring" - "Monitoring Overview" tab.
2) In the column of "My Monitored Metrics", click the "Add Metrics to Be Monitored" button to select the product type and metrics to be monitored, and corresponding region and monitored objects.
3) The selected metrics and all objects will appear in the view. Users can click the "Select Object" button to re-select the objects to be monitored, or click the object name below the chart to show or hide some of the object data. You can also select different periods to view the monitoring data.

Modifying Displayed Objects

Users can modify the object data displayed in the chart by clicking the "Add Metrics to Be Monitored" button, the "Select Object" button, or the object name below the chart.
Get Monitor View

Getting the Monitoring Data of Specified Metrics

Last updated: 2020-05-13 15:18:59

Cloud Monitor allows you to get the specified metric data at a specific point in time of a monitored object by the following methods:

Getting the specified metric data in the console

1. Log in to the Tencent Cloud Console and enter the console of the product whose monitoring data you want to view.
2. Select the object to be monitored and click its ID to enter its monitoring details page, or click the monitoring icon in the object list to view its data in the floating window.
3. Find the specified metric on the monitoring page or in the floating window.
4. Use the time selector and granularity selector to adjust the content displayed in the chart to view the specified metric data at the specific point in time of this monitored object.

Getting the specified metric data through API

For more information, please see the GetMonitorData API.
Dashboard

What Is a Dashboard?

Last updated : 2020-10-30 12:03:12

Dashboards are smart monitoring panels provided by Cloud Monitor that allow you to monitor the metric data of Tencent Cloud services. Dashboards also provide visualization and analysis features.

You can create dashboards for Tencent Cloud service metrics. The dashboards will automatically display monitoring data in intuitive and elegant charts, helping you analyze metrics through trends and exceptional values.

Feature Overview

- Flexible chart configuration, supporting visualized charts in customizable layouts.
- Displaying multiple instances or multiple metrics of the same instance in a single chart, facilitating the monitoring of key metrics of instances during troubleshooting.
- Template variables, custom links, legend sorting, and other features to assist you in the overall coupling analysis of the metrics data.
- Instant sharing of monitoring charts or monitoring dashboards to facilitate efficient and collaborative troubleshooting.

Use Cases
Common scenarios:

- When you receive a metric alarm, you can use dashboards to analyze the cause of the alarm.
- After a new feature is released, you can use dashboards to check for resource exceptions.
- Through real-time metric display, you can optimize performance during business peaks.
- You can view the loads on dashboards to determine whether resource scaling is needed.

Advantages:

- Ready-to-use dashboards reduce the costs of human resources and time for OPS personnel when building open-source visualization software such as Grafana.
- This feature meets the demand for the visualization of metric data in various monitoring scenarios, helping you analyze metric data and troubleshoot efficiently.

Use Limits

<table>
<thead>
<tr>
<th>Category</th>
<th>Upper Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of custom dashboards</td>
<td>20</td>
</tr>
<tr>
<td>Number of charts on each dashboard</td>
<td>20</td>
</tr>
<tr>
<td>Number of instances that can be bound with each chart</td>
<td>12</td>
</tr>
</tbody>
</table>
List

Default Dashboard

Last updated: 2020-10-30 14:21:24

This document describes how to configure the default dashboard.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, hover over the name of the target dashboard and click Set as “Default Dashboard”.

After specifying the default dashboard, you can click Default Dashboard in the menu bar on the left to access the dashboard instantly.

⚠️ Note:

For custom dashboards, only one default dashboard can be specified. If you specify the default dashboard repeatedly, the previous default dashboard will be overwritten.
Deleting a Dashboard

This document describes how to delete a dashboard.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. Both individual deletion and batch deletion are supported, as described below:

   - **Individual deletion**
     
     Find the dashboard that you want to delete in the dashboard list, click **Delete** under the “Operation” column, and then confirm the deletion in the window that appears.

   - **Batch deletion**
     
     i. Select all or multiple dashboards that you want to delete in the dashboard list, and click **Delete** above the list.
     
     ii. Click **Delete** in the window that appears.
Copying a Dashboard

This document describes how to copy a dashboard.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard that you want to copy and click Copy under the “Operation” column.
4. In the window that appears, rename the dashboard and click Save.
Dashboard
Creating a Dashboard

Last updated: 2020-10-30 12:03:12

You must create a dashboard before you can create a monitoring chart. This document describes how to create a dashboard.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the upper-left corner of the dashboard list page, click Create to go to the management page for creating a dashboard.
4. Click the dashboard area , enter a dashboard name, and click OK to quickly create a dashboard.

⚠️ Note:
To edit the dashboard name or configure a dashboard (including template variables, link management, and JSON configuration), see Configuring a Dashboard.
Viewing a Dashboard

Last updated: 2020-10-30 12:03:12

Using the dashboard feature, you can switch between Recent Dashboards, Favorite Dashboards, and Custom Dashboards. This document describes how to view dashboards after creating them.

Preparations

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.

Viewing a Dashboard in the Full Screen Mode

1. In the dashboard list, find the dashboard that you want to view, and click the dashboard name to go to the dashboard management page.

2. Click the full screen mode icon to view the dashboard in the full screen mode.

Exiting the Full Screen Mode

You can press Esc or click the close icon in the upper-right corner to exit the full screen mode.
Switching Dashboards

1. In the dashboard list, click any dashboard name to go to the dashboard management page.

2. As shown in the figure below, click in the dashboard area to switch between Recent Dashboards, Favorite Dashboards, and Custom Dashboards.
   - Recent Dashboards: displays the most recent three dashboards you have accessed.
   - Favorite Dashboards: displays all the dashboards you have added to Favorites.
   - Custom Dashboards: displays all the dashboards you have customized.

![Dashboard Switching Figure]

Note:
To add a dashboard to Favorites, see Adding a Dashboard to Favorites.

Adjusting the Time Span and Refreshing Frequency of a Dashboard

By default, dashboards display the data of the last 12 hours, and monitoring data is refreshed in real time.

- You can adjust the time span and granularity for all charts on the current dashboard by using the time selector in the upper-right corner of the dashboard. In this way, you can review historical monitoring data and perform
In the upper-right corner of the dashboard, you can click the refresh button to refresh the dashboard or select a time interval from the drop-down list to adjust the refreshing frequency.
Adding a Dashboard to Favorites

This document describes how to add a dashboard to Favorites.

Directions

After adding dashboards to Favorites, you can quickly switch between the dashboards in Favorites by following the directions under “Switching Dashboards” in Viewing Dashboards and perform troubleshooting. You can quickly filter the dashboards in Favorites by following the directions in Viewing Dashboards.

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard that you want to add to Favorites, and click the dashboard name to go to the dashboard management page.
4. Click , as shown in the figure below. If the “Added to Favorites successfully” message appears, the dashboard has been successfully added to Favorites.
Sharing a Dashboard

Last updated: 2020-10-30 12:03:13

This document describes how to share a dashboard.

Directions

Users can share their dashboards with others. To access a shared link, users must have a Tencent Cloud account under the same root account and Cloud Monitor access permissions.

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard that you want to share, and click the dashboard name to go to the dashboard management page.
4. Click . In the window that appears, configure the sharing conditions and copy the sharing link to share it with other accounts. The description of the option is as follows:
   - **Time**: you can determine whether to synchronously share the currently selected time in the time filter with others.

   ![Image of sharing dashboard](image)

   **Note**: To configure the template variable selector, see Template Variables.
This document describes the directions for configuring the basic dashboard settings.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the upper-left corner of the dashboard list page, click Create to go to the management page for creating a dashboard.
4. Click > Basic Configuration.
5. Click Basic Configuration, and you can specify the dashboard name and the dashboard remarks.
This document describes how to configure and use template variables.

Configuring Template Variables

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the upper-left corner of the dashboard list page, click Create to go to the management page for creating a dashboard.
4. Click   > Template Variables.
5. Click Template Variables. You can customize dashboard filter conditions and use template variables on the dashboard management page. For more information, see Using Template Variables. Currently, filtering by the labels of CVM - basic monitoring, storage monitoring, and TencentDB for MySQL primary/standby server monitoring is supported.
6. Create template variables. Click Create. After configuring the template variables, click OK.

Editing and Deleting Template Variables
You can delete and edit template variables in the template variable list.

### Using Template Variables

1. Log in to the [Cloud Monitor console](https://console.cloud.tencent.com).
2. In the left sidebar, click **Dashboard** > **Dashboard List** to go to the dashboard list page.
3. Find the dashboard where the template variables you want to view are located and click the corresponding dashboard name.
4. After creating a template variable, you can use it as a quick selector of dashboards and monitoring charts.
   - Using it in dashboards: on the dashboard management page, you can use template variables to filter the displayed data of the dashboard.

   ![Dashboard Management Page](image)

   - Using it in monitoring charts: on the chart editing page, you can select labels to quickly group and aggregate instance data for display.

   ![Chart Editing Page](image)
**Note:**

If you need to edit a monitoring chart, please see [Editing Metrics](#).
Link Management

This document describes how to configure and use a link.

Configuring a Link

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the upper-left corner of the dashboard list, click Create to go to the management page for creating a dashboard.
4. Click Link Management. 
5. Click Link Management > Create to customize a quick dashboard redirection link. The link management settings include the link name, type, link target, and parameter, as described below:
   - Link name: enter a custom link name.
   - Type
     - Custom link: supports all links.
     - Other dashboards: link to other dashboards.
   - Link target: indicates the link address or link dashboard.
   - Parameter
     - Time: indicates whether to synchronize the dashboard time when redirecting to the link page.
   - Opening mode
     - New tab: opens a link with a new label.
Current page: opens a link with the current label.

Using a Link

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. Find the dashboard for which you have configured a link and click the corresponding dashboard name.
4. On the dashboard management page, you can quickly redirect to your custom link to perform troubleshooting or compare monitoring data.
This document describes the directions and notes for using JSON.

Viewing and Copying the JSON Template

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the upper-left corner of the dashboard list page, click Create to go to the management page for creating a dashboard.
4. Click 🌐 > JSON.
5. Click JSON and copy the JSON template to deploy the JSON format to your self-built system. Then, you can view the corresponding dashboard in your system.

The JSON template contains fields such as the dashboard attribute, template variable, and dashboard query. For the description of these fields, see the following section.
Description of JSON Fields

```json
{
    "Description": "",
    "Refresh": "close",
    "Title": "JSONTEST",
    "UUID": "jdq4joy56is4w60q",
    "Version": 1,
    "Templating": [],
    "Links": [],
    "Panels": [],
    "Time": {
        "From": "now-12h",
        "To": "now"
    }
}
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the current dashboard</td>
</tr>
<tr>
<td>Refresh</td>
<td>Interval for automatic refreshing</td>
</tr>
<tr>
<td>Title</td>
<td>Name of the current dashboard</td>
</tr>
<tr>
<td>UUID</td>
<td>Unique dashboard ID</td>
</tr>
<tr>
<td>Version</td>
<td>Dashboard version, which increases every time you save the dashboard</td>
</tr>
<tr>
<td>Templating</td>
<td>Dashboard template variable. For more information, see Templating</td>
</tr>
<tr>
<td>Link</td>
<td>Dashboard link. For more information, see Link</td>
</tr>
<tr>
<td>Panels</td>
<td>Chart configuration. See Panels</td>
</tr>
<tr>
<td>Time</td>
<td>Dashboard time range</td>
</tr>
</tbody>
</table>

**Templating**

```
"Templating": [ // Template variable
{
    "Label": "cvm instance name", // Template variable alias
    "Multi": true, // Multiple or not
    "Name": "cvm", // Label
    "Selected": [], // Template variable value
    "Type": "monitor", // Template variable type
    "TemplatingType": "basics", // Label type: basic monitoring or custom monitoring
    "TemplatingType": '123', // Variable ID
}
```

©2013-2019 Tencent Cloud. All rights reserved.
"Links": [  // Dashboard link
  {
    "IncludeVars": true,  // Whether the link parameters carry template variables
    "KeepTime": true,  // Whether the link parameters carry time variables
    "TargetBlank": true,  // Whether to open a new tab
    "Title": "xxx",  // Link name
    "Type": "other",  // Link type: custom link or redirection link to another dashboard
    "Url": "/monitor/dashboard2/dashboards/d/0hh64oj49rru3ctk/dashboard2-0yan-shi-an-li-xia-zuan-lian-jie",  // Link address
    "ID": 0  // ID
  }
]

"Panels": [  // Panel configuration
  {
    "Collapsed": false,  // Whether to collapse the chart group
    "Datasource": null,  // Data source
    "GridPos": {  // Chart position
      "H": 1,
      "W": 6,
      "X": 0,
      "Y": 0
    },
    "ID": 1595472129140,  // Chart ID
    "Panels": [],  // Panel is a field for the chart group, which stores sub-panels
    "Title": "Default chart group",  // Title
    "Type": "row"  // Chart type
  },
  {
    "DataLinks": [],  // Data link for the chart configuration
    "Description": "",  // Chart description
    "GridPos": {
      "H": 5,
      "W": 6,
      "X": 0,
      "Y": 1
    },
    "ID": 1595471392817,
    "Links": [],  // Chart link
    "Settings": {  // Chart visualization configuration
      "aliasColors": {},
      "bars": false
    }
  }
]
"dashLength": 10,
"dashes": false,
"datasource": null,
"decimals": 2, // Legend precision
"fieldConfig": {
  "defaults": {
    "custom": {}
  },
  "overrides": []
},
"fill": "0.8", // Chart fill opacity
"fillGradient": 0,
"gridPos": {
  "h": 8,
  "w": 12,
  "x": 0,
  "y": 0
},
"hiddenSeries": false,
"id": "1595471392817", // Chart panel ID
"legend": {
  // Legend settings
  "alignAsTable": [ // Whether to display legends as tables
    "1"
  ],
  "avg": [ // Whether to display the average value. **'1'**: true. **'0'**: false.
    "1"
  ],
  "current": [ // Whether to display the latest value. **'1'**: true. **'0'**: false.
    "1"
  ],
  "max": [ // Whether to display the maximum value. **'1'**: true. **'0'**: false.
    "1"
  ],
  "min": [ // Whether to display the minimum value. **'1'**: true. **'0'**: false.
    "1"
  ],
  "rightSide": [ // Whether to place on the right side. **'1'**: true. **'0'**: false.
    "1"
  ],
  "show": [ // Whether to display legends. **'1'**: true. **'0'**: false.
    "1"
  ],
  "total": [ // Whether to display accumulative values. **'1'**: true. **'0'**: false.
    "1"
  ],
  "values": false
},
"lines": [ // Whether to display curves. **'1'**: true. **'0'**: false.
  "1"
],
"linesType": true, // Whether to display smooth curves. **'1'**: true. **'0'**: false.
"linewidth": "2", // Curve width
"markline": { // Mark settings
  "marklineMax": 
}
"max": []// Whether to display peak values. **1**: true. **0**: false.
"1"
],

"nullPointMode": "1",// Display mode of null values. 0: link to null data. 1: do not fill. 2: automatically fill with 0.
"options": {
"dataLinks": []// datalinks array
},

"percentage": false,
"pointradius": 2,
"points": false,
"renderer": "flot",
"seriesOverrides": [],
"spaceLength": 10,
"stack": []// Whether to allow stacked display. **1**: true. **0**: false.
"1"
],

"steppedLine": false,
"targets": [
{
"refId": "A",
"scenarioId": "random_walk"
}
],

"thresholds": [],
"timeFrom": null,
"timeRegions": [],
"timeShift": null,
"title": "New chart",
"tooltip": {
"shared": true,
"sort": 0,
"value_type": "individual"
},

"type": "graph",
"xaxis": {
"buckets": null,
"mode": "time",
"name": null,
"show": true,
"values": []
},

"yaxes": [
{
"decimals": 2,// Left y-axis precision
"format": ".%",// Left y-axis label unit
"label": null,
"logBase": 1,
"max": 2,// Maximum value of the left y-axis coordinate
"min": 0,// Minimum value of the left y-axis coordinate
"show": []// Whether to display the left y-axis. **1**: true. **0**: false.
"1"}


] } 

{ "decimals": 2, "format": "", "label": null, "logBase": 1, "max": null, "min": null, "show": [ 1 ] }, "yaxis": { "align": false, "alignLevel": null } }, "Targets": [ // Metric configuration { "Aggregate": "", // Statistical mode "CompareLastWeek": false, // Compare with last week "CompareYesterday": false, // Compare with yesterday "Conditions": [ // Filtering conditions { "Dimension": [ "{InstanceId":"ins-19827u5b"}, "{InstanceId":"ins-xxooxxoo"}, "{InstanceId":"ins-19719mfp"} "Region": "ap-guangzhou", "Type": "normal" } ], "ConfigId": "cvm", "Datasource": "DS_QCEMetric", // Product type "DimensionKey": [ "InstanceId" ], "GroupBy": [ // groupby "InstanceId" ], "MetricNames": [ // Metric name "BaseCpuUsage" ], "Namespace": "QCE/CVM", // Namespace "Period": 60 // Granularity }, }, "Title": "single metric - default configuration", // Chart name "Type": "graph" // Chart type 

]
Monitoring Charts
Creating a Chart
Step 1: Create a metric

Last updated: 2020-10-30 12:03:13

This document describes how to add and edit metrics when creating a monitoring chart.

Adding Metrics

1. Log in to the Cloud Monitor console and click **Dashboard** > **Default Dashboard** on the left sidebar.
2. Switch to the dashboard that you want to operate to go to the dashboard management page.
3. Click **Create a Chart** to go to the chart editing page. Configure the metric information as follows:
   - **Select Monitoring Type**: supports basic monitoring and custom monitoring metrics.
   - **Metric**: select the product type and metric.
   - **Filter**: click “Select a variable” and select a filter condition. Data that meets the condition will be displayed in the chart. If you add multiple filter conditions, only data that meets all the conditions (by running the logical AND operation) will be displayed in the chart.
   - **group by**: similar to the Group by feature of SQL, this feature can group data based on specified labels and then aggregate data according to aggregation algorithms. If you do not select a label, you can customize the metric statistical method for the statistical period, which can be avg, max, min, or sum.
   - **Compare**: day-over-day (compare with the same period yesterday), week-over-week (compare with the same period last week), and custom time comparisons are supported. If you select all the comparison options, the chart will display the day-over-day and week-over-week monitoring curves for the selected instance, making it easier for you to compare the data.
   - **Alias**: you can configure the aliases of all instances with one click. To configure different aliases for different instances, you can create multiple metrics and enter an alias under each metric.
- **Left Y-Axis, Right Y-Axis**: you can adjust the position of the Y-axis, which can be on the left or on the right.

![Chart Image]

4. After configuring the preceding settings, click > **OK**.

**Creating multiple metrics and copying metrics**

You can click **Add a Metric** or **** to display multiple metrics in the same chart for cross-instance metric data comparison.

**Sorting metrics**

You can click the **icon to adjust the sorting of metrics.**

**Editing Metrics**

1. Log in to the Cloud Monitor console and click **Dashboard > Default Dashboard** on the left sidebar.
2. Switch to the dashboard that you want to operate to go to the dashboard management page.
3. Find the monitoring chart that you want to edit and click ****.
4. In the window that appears, click **Edit** to go to the chart editing page.

**Deleting Metrics**

1. Log in to the Cloud Monitor console and click **Dashboard > Default Dashboard** on the left sidebar.
2. Switch to the dashboard that you want to operate to go to the dashboard management page.
3. Find the monitoring chart that you want to edit and click ****.
4. In the window that appears, click **Edit** to go to the chart editing page. Click **** to delete the metric.
Step 2: Configure the chart

Last updated : 2020-10-30 12:03:13

This document describes how to configure a chart when creating a monitoring chart.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. Find the dashboard for which you want to create charts, and click the dashboard name to go to the dashboard management page.
4. Click Dashboard > Create a Chart to go to the chart editing page and configure the settings as follows:
   - Basic info: includes the chart name and chart notes.
   - Chart type: can be a line chart, a bar chart, a dashboard, a pie chart, or a numerical chart. More chart types will be available in the future. For different chart types, the chart elements, thresholds, and legend configurations are different. For more information, see Use Cases of Different Chart Types.

   - Data link: defines whether to display a link when you double-click the chart. After adding a data link, you can click a certain period in the chart to be redirected to the custom link.

   Chart link: defines the chart redirection link. After adding a chart link, you can click in the chart to be redirected to the custom link, as shown in the figure below:

   - Chart link: defines the chart redirection link. After adding a chart link, you can click in the chart to be redirected to the custom link, as shown in the figure below:
5. After configuring the settings, click .

**List of units**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No unit displayed</td>
</tr>
<tr>
<td>%</td>
<td>Percentage</td>
</tr>
<tr>
<td>s</td>
<td>Second</td>
</tr>
<tr>
<td>us</td>
<td>Microsecond</td>
</tr>
<tr>
<td>ms</td>
<td>Millisecond</td>
</tr>
<tr>
<td>Count</td>
<td>Total number of times</td>
</tr>
<tr>
<td>Count/s</td>
<td>Times per second</td>
</tr>
<tr>
<td>Bytes</td>
<td>Bytes</td>
</tr>
<tr>
<td>KBytes</td>
<td>Kilobytes</td>
</tr>
<tr>
<td>MBytes</td>
<td>Megabytes</td>
</tr>
<tr>
<td>GBytes</td>
<td>Gigabytes</td>
</tr>
<tr>
<td>TBytes</td>
<td>Terabytes</td>
</tr>
<tr>
<td>KiBytes</td>
<td>Kilobytes (in the 1024 system)</td>
</tr>
<tr>
<td>MiBytes</td>
<td>Megabytes (in the 1024 system)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>GiBytes</td>
<td>Gigabytes (in the 1024 system)</td>
</tr>
<tr>
<td>TiBytes</td>
<td>Terabytes (in the 1024 system)</td>
</tr>
<tr>
<td>Bits</td>
<td>Bits</td>
</tr>
<tr>
<td>KBits</td>
<td>Kilobits</td>
</tr>
<tr>
<td>GBits</td>
<td>Gigabits (in the 1024 system)</td>
</tr>
<tr>
<td>TBits</td>
<td>Terabits (in the 1024 system)</td>
</tr>
<tr>
<td>KiBits</td>
<td>Kilobits (in the 1024 system)</td>
</tr>
<tr>
<td>MiBits</td>
<td>Megabits (in the 1024 system)</td>
</tr>
<tr>
<td>GiBits</td>
<td>Gigabits (in the 1024 system)</td>
</tr>
<tr>
<td>TiBits</td>
<td>Terabits (in the 1024 system)</td>
</tr>
<tr>
<td>Bytes/s</td>
<td>Bytes per second</td>
</tr>
<tr>
<td>KBytes/s</td>
<td>Kilobytes per second</td>
</tr>
<tr>
<td>MBytes/s</td>
<td>Megabytes per second</td>
</tr>
<tr>
<td>GBytes/s</td>
<td>Gigabytes per second</td>
</tr>
<tr>
<td>TBytes/s</td>
<td>Terabytes per second</td>
</tr>
<tr>
<td>KiBytes/s</td>
<td>Kilobytes per second (in the 1024 system)</td>
</tr>
<tr>
<td>MiBytes/s</td>
<td>Megabytes per second (in the 1024 system)</td>
</tr>
<tr>
<td>GiBytes/s</td>
<td>Gigabytes per second (in the 1024 system)</td>
</tr>
<tr>
<td>TiBytes/s</td>
<td>Terabytes per second (in the 1024 system)</td>
</tr>
<tr>
<td>Bit/s</td>
<td>Bits per second</td>
</tr>
<tr>
<td>KBit/s</td>
<td>Kilobits per second</td>
</tr>
<tr>
<td>MBit/s</td>
<td>Megabits per second</td>
</tr>
<tr>
<td>GBit/s</td>
<td>Gigabits per second</td>
</tr>
<tr>
<td>TBit/s</td>
<td>Terabits per second</td>
</tr>
<tr>
<td>KiBit/s</td>
<td>Kilobits per second (in the 1024 system)</td>
</tr>
<tr>
<td>MiBit/s</td>
<td>Megabits per second (in the 1024 system)</td>
</tr>
<tr>
<td>GiBit/s</td>
<td>Gigabits per second (in the 1024 system)</td>
</tr>
<tr>
<td>TiBit/s</td>
<td>Terabits per second (in the 1024 system)</td>
</tr>
</tbody>
</table>
Use Cases of Different Chart Types

Line Charts

Last updated: 2020-10-30 12:03:14

This document describes the use cases and the operations directions of line charts.

Use Cases

**Line chart**: is used to display the trends of metrics or the comparisons between the same or different metrics.

*Configuration effects of multiple types of line charts:*

![Line Chart Examples](image)

**Directions**

1. Log in to the Cloud Monitor console and click **Dashboard > Default Dashboard** on the left sidebar.

2. Click **Create a Chart** to go to the chart editing page.

3. In the chart configuration module, select “Line Chart” as the chart type.

**Chart element configuration**

- **Point**: indicates whether to display chart data as points.
- **Line**: is the default display pattern, which can be customized to display the chart data as lines.
- **Bar**: indicates whether to display the chart data as bars.
- **Line Type**: indicates the type of the line displayed, which can be a broken line or a smooth line.
• **Line Width**: you can adjust the line width in the charts.

• **Fill**: you can determine whether to fill the areas formed between a line and the X and Y axes. 0 indicates no filling. 1 to 10 indicate the depth of color for filling the areas, with a greater value indicating a deeper color.

• **Stack**: you can determine whether to stack instance data, that is, whether to calculate the sum of data. To achieve the stack effect, at least two instances are needed.

• **Null Values**: you can determine how null values appear in charts. There are three possible values: not filling, automatic filling with 0, and linking null values.

### Coordinate Axis Configuration

You can determine the displayed content and the display position of the Y axis, which can be left, right, or both. The settings are described as follows:

- **Show**: indicates whether to show the Y axis.
- **Unit**: indicates the display unit of the Y axis. For more information, see [List of Units](#).
- **Min**: indicates the starting value of the Y axis.
- **Max**: indicates the ending value of the Y axis.
- **Precision**: indicates the number of decimal places to be retained for the Y axis. 0: do no retain any decimals. 1: retain one decimal place.

### Legend Configuration

You can determine the display position of legends by configuring the following settings:

- **Show**: indicates whether to show legends in charts.
- **Table Type**: can be the maximum value, the minimum value, the average value, or the current value. After you select a table type, the data will be sorted by this type.
- **Put on the Right**: indicates whether to place the instances, the maximum value, the minimum value, the average value, and the current value on the right side of charts. By default, they are placed below charts.
- **Max, Min, Avg, Sum, and Current Value**: indicates whether to display the maximum value, the minimum value, the average value, the sum, and the current value below charts.
- **Precision**: indicates the number of decimal places to be retained for the maximum value, the minimum value, the average value, the sum, and the current value. 0: do no retain any decimals. 1: retain one decimal place.

### Auxiliary Line and Notes

You can determine whether to display the auxiliary line and the notes of the maximum value. By default, they are displayed.

4. After completing the configuration, click **Save** in the upper-right corner.
Bar Charts

Last updated: 2020-10-30 12:03:14

This document describes the use cases and operations directions of bar charts.

Use Cases

**Bar chart**: is applicable to the comparison between metrics in each statistical period.

**Configuration effects of bar charts**: 

Directions

1. Log in to the Cloud Monitor console and click **Dashboard** > **Default Dashboard** on the left sidebar.

2. Click **Create a Chart** to go to the chart editing page.

3. In the chart configuration section, select “Bar Chart” as the chart type.

4. (Optional) Under “Chart Elements,” you can specify whether to display units. For more information on the meanings of units, see **List of Units**.

5. After the configuration is completed, click **Save** in the upper-right corner.
Dashboard

Last updated: 2020-10-30 12:03:14

This document describes the use cases of and the operations directions for dashboards.

Use Cases

Dashboard: is applicable to percentage metrics such as the CPU utilization, memory usage, and disk utilization.

Dashboard configuration effects:

Directions

1. Log in to the Cloud Monitor console and click Dashboard > Default Dashboard on the left sidebar.

2. Click Create Chart to go to the chart editing page.
3. In the chart configuration module, select dashboard as the chart type.
4. Configure the dashboard information.

Chart elements

- **Statistical mode**: indicates the metric statistical mode, which can be the current value, the minimum value, the maximum value, the average value, and the sum.
- **Unit**: indicates whether to display the unit of the statistical value. For more information on the meanings of different units, see List of Units.
- **Precision**: indicates the number of decimal places to be retained for the metric statistical value. 0: do not retain decimals. 1: retain one decimal place.

Threshold
- **Threshold**: indicates the thresholds for colors. Format: ,. For example, if you enter "50,80" in this field, it means that the displayed color of the metric will be green when the metric value is less than 50, orange if the metric value is equal to or greater than 50 but less than 80, and red if the metric value is equal to or greater than 80.

- **Color**: indicates the color sequence. For example, set the "Threshold" field to "50,80".  

**Non-reverse cases:**
- If the metric value is less than 50, display **green**.
- If the metric value is equal to or greater than 50 but less than 80, display **orange**.
- If the metric value is equal to or greater than 80, display **red**.

**Reverse cases:**
- If the metric value is less than 50, display **red**.
- If the metric value is equal to or greater than 50 but less than 80, display **orange**.
- If the metric value is equal to or greater than 80, display **green**.

- **Min, Max**: indicates the minimum and maximum values displayed on the dashboard.

- **Show Threshold**: indicates whether to display the threshold for each color on the dashboard.
Pie Charts

Last updated: 2020-10-30 14:21:24

This document describes the use cases and operations directions of pie charts.

Use Cases

Pie chart: can clearly show the proportion of each instance regarding the same metric. Pie charts can be used when you want to view the proportion of each instance regarding the same metric without requiring an elaborate display of data.

Configuration effects of pie charts:

Directions

1. Log in to the Cloud Monitor console and click Dashboard > Default Dashboard on the left sidebar.

2. Click > Create a Chart to go to the chart editing page.

3. In the chart configuration module, select “Pie Chart” as the chart type.

4. Configure the pie chart information as follows:

Chart elements

- **Pie type**: indicates the pie chart display mode, which can be the doughnut chart mode or the pie chart mode.
- **Statistical mode**: indicates the metric statistical mode, which can be the current value, the minimum value, the maximum value, the average value, or the sum.
- **Sort by**: indicates the mode in which the proportions of different instances in the metric data are sorted. The value can be default (automatic sorting by the system), ascending, or descending.
- **Unit**: indicates whether to display the unit of the statistical value. For more information on the meanings of different units, see “List of Units” in Step 2: Configure the chart.
- **Gap width**: indicates whether a gap is required between sections in a pie chart. The value can be no gap or 1px to 5px. A greater value indicates a larger gap.
- **Precision**: indicates the number of decimal places to be retained for the metric statistical value. 0: do not retain any decimals. 1: retain one decimal place.
- **Merge**: indicates whether to merge the numerical metric values of different instances. For example, if you enter 3, the numerical metric values of instances numbered later than 3 will be merged. In the following figure, **Merge** is set to 3 as an example, which means that the data of instances ④ and ⑤ are merged as other data.

**Legend configuration**

You can specify the display positions of legends.
- **Show**: indicates whether to show legends in charts.
- **Table Type**: can be the maximum value, the minimum value, the average value, or the current value. After you select a table type, the data will be sorted by this type.
- **Put on the Right**: indicates whether to place the instances, the maximum value, the minimum value, the average value, and the current value on the right side of charts. By default, they are placed below charts.
- **Max, Min, Avg, Sum, and Current Value**: indicates whether to display the maximum value, the minimum value, the average value, the sum, and the current value below charts.
- **Precision**: indicates the number of decimal places to be retained for the maximum value, the minimum value, the average value, the sum, and the current value. 0: do not retain any decimals. 1: retain one decimal place.
Numbers

Last updated: 2020-10-30 12:04:22

This document describes the use cases and the operations directions of numerical charts.

Use Cases

**Numerical chart**: is applicable to metric values within a period of time. Examples include TCP links, public network outbound packets, and private network inbound packets.

**Configuration effects of numerical charts**:

![Numerical chart example](image)

Directions

1. Log in to the Cloud Monitor console and click **Default Dashboard**.
2. Click **Create a Chart**.
3. In the chart configuration module, select “Numerical” as the chart type.
4. Configure the numerical chart information.

**Chart elements**

- **Statistical Mode**: indicates the metric statistical mode, which can be the current value, the minimum value, the maximum value, the average value, or the sum.
- **Unit**: indicates whether to display the unit of the statistical value. For more information on the meanings of different units, see **List of Units**.
- **Hide Curve**: indicates whether to hide curves.
• **Precision**: indicates the number of decimal places to be retained for the metric statistical value. 0: do not retain decimals. 1: retain one decimal place.

**Threshold**

• **Threshold**: indicates the threshold for colors. Format: \(<\text{Numerical value},\text{Numerical value}>\). For example, if you enter \(50,80\), it means that the displayed color of the metric will be green if the metric value is less than 50, orange if the metric value is equal to or greater than 50 but less than 80, and red if the metric value is equal to or greater than 80.

• **Color**: indicates the color sequence. For example, set the “Threshold” field to \(50,80\).

  **Non-reverse cases:**
  - If the metric value is less than 50, display **green**.
  - If the metric value is equal to or greater than 50 but less than 80, display **orange**.
  - If the metric value is equal to or greater than 80, display **red**.

  **Reverse cases:**
  - If the metric value is less than 50, display **red**.
  - If the metric value is equal to or greater than 50 but less than 80, display **orange**.
  - If the metric value is equal to or greater than 80, display **green**.
Deleting a Chart
Last updated: 2020-10-30 12:03:14

This document describes how to delete a monitoring chart.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard from which you want to delete a chart, and click the dashboard name to go to the dashboard management page.
4. Find the chart that you want to delete, and click ••• > Delete.
5. Click Delete Now in the window that appears.
Viewing a Chart

This document describes how to view a monitoring chart.

Preparations

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click **Dashboard > Dashboard List** to go to the dashboard list page.
3. In the dashboard list, find the dashboard that you want to view, and click the dashboard name to go to the dashboard management page.

Viewing Charts in the Full Screen Mode

Click the “Full-Screen Chart” icon in the upper-right corner of the chart to view it in the full-screen mode.

You can press **ESC** or click the icon in the upper-right corner to exit the full screen mode.

Chart Scaling and Moving

- Chart scaling: you can scale a chart by hovering over the lower-right corner of the chart until a straight-angle icon appears, as shown in the figure below:

![Chart Scaling Example](image-url)

- Chart moving: you can move a chart by hovering over the name of the chart until a movement icon appears, as shown in the figure below:
Viewing the Monitoring Data of a Period

You can view the monitoring data of a period by hovering over the monitoring chart, as shown in the figure below:

Viewing Data by Using the Variable Selector

If you have many instances, you can define a template variable to dynamically switch labels so that you can view the monitoring data of different instances in the same monitoring chart.
Adjusting the Time Span of Charts to View Monitoring Data

By default, dashboards display the data of the last 12 hours.

You can adjust the time span and granularity for all charts in the current dashboard by using the time selector in the upper-right corner of the dashboard. In this way, you can review historical monitoring data and perform

**Note:**

To create a template variable, see Configuring a Dashboard.
troubleshooting.

### Time Periods and Corresponding Chart Granularities

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Default Statistical Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=1h</td>
<td>1min</td>
</tr>
<tr>
<td>(1h,12h]</td>
<td>1min</td>
</tr>
<tr>
<td>(12h,3d]</td>
<td>5min</td>
</tr>
<tr>
<td>(3d,30d]</td>
<td>1h</td>
</tr>
<tr>
<td>(30d,186d]</td>
<td>1d</td>
</tr>
</tbody>
</table>
Creating a Chart Group

This document describes how to create a chart group and associate and remove charts.

Creating a Chart Group

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard List to go to the dashboard list page.
3. Find the dashboard for which you want to create charts, and click the dashboard name to go to the dashboard management page.
4. Click ➤ Create a Chart Group to create a chart group. As shown in the figure below, you can rename or delete the chart group by hovering over the chart group and clicking the corresponding icon.

![Create a Chart Group](image)

Associating a Chart with a Chart Group

Move a chart to the area below the chart group, click ➤ , and confirm the association to finish associating the chart with the chart group.
Removing a Chart from a Chart Group

Move a chart to the area above the chart group, click δ, and confirm the removal to finishing removing the chart from the chart group.
Sharing a Chart

Last updated: 2020-10-30 12:03:14

This document describes how to share a monitoring chart.

Directions

Users can share their monitoring charts with others. To access a shared link, users must have a Tencent Cloud account under the same root account and Cloud Monitor access permissions.

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard that you want to share, and click the dashboard name to go to the dashboard management page.
4. Find the chart that you want to share, and click ⋯ > Share. In the window that appears, configure the sharing conditions and copy the sharing link to share the chart with other accounts.
   - **Time**: you can determine whether to synchronously share the currently selected time in the time filter with others.

1 Note:

To configure sub-account access permissions, see Cloud Access Management (CAM).

Note:

To configure the template variable selector, see Template Variables.
Copying a Chart

Last updated : 2020-10-30 12:03:14

This document describes how to copy a monitoring chart.

Feature Overview

By using the monitoring chart copying feature, you can quickly deploy a monitoring chart to the current dashboard or to the other dashboards.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard from which you want to copy a chart, and click the dashboard name to go to the dashboard management page.
4. Find the chart from which you want to export data, and click more options > Copy to copy the chart to the current dashboard or clipboard, as described below:

- Copy to the current dashboard: click To the current dashboard to copy the chart to the current dashboard.
- Copy to the clipboard: click To the clipboard, and later, when creating a monitoring chart under any dashboard, directly paste the copied chart.
Exporting Data

This document describes how to export the detailed data of monitoring charts.

Directions

1. Log in to the Cloud Monitor console.
2. In the left sidebar, click Dashboard > Dashboard List to go to the dashboard list page.
3. In the dashboard list, find the dashboard from which you want to export chart data, and click the dashboard name to go to the dashboard management page.
4. Find the chart from which you want to export data, and click ⃘ > Data Export. Then, the detailed monitoring data of the chart will be exported.
Alarm Service
Configuring Alarm Policies

This document describes how to create and delete alarm policies and set the default alarm policy.

Use Cases

You can set threshold alarms for the performance consumption metrics of the Tencent Cloud service resources supported by Cloud Monitor. You can also set event alarms for the service status of Tencent Cloud service instances or the underlying platform infrastructure. This way, when an exception occurs, you will promptly receive notifications, which will allow you to take appropriate measures. An alarm policy consists of five required parameters: name, policy type, alarm trigger condition, alarm object, and alarm channel. You can create alarm policies by following the directions below:

Directions

Creating an alarm policy

1. Log in to the Cloud Monitor console.
2. Choose Alarm Configuration > Alarm Policy to access the alarm policy configuration page.
3. Click Add and configure a new alarm policy, as shown below:
### Basic Cloud Monitor

©2013-2019 Tencent Cloud. All rights reserved.

Press Shift to select multiple items

<table>
<thead>
<tr>
<th>Trigger condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Condition Template</td>
</tr>
</tbody>
</table>

#### Configure trigger conditions

- **Indicator alarm**
  - Alarm is triggered when any conditions are met.
  - Example:
    ```
    if CPUUtilization > Statistical Per > 80% Last for 15min then Alarm once even
    ```
  - Add:
    - Event Alarm:
      - DiskReadOnly
    - Add:

#### Alarm Channel

- **Recipient Object**
  - Recipient:
    - Add Recipients
  - User Name, Mobile number, Email

- **Valid Period**
  - 00:00:00 to 23:59:59

- **Receiving Channel**: Email, SMS

- **Language**: English

#### Advanced Features

- **Auto Scaling**: After enabling auto scaling policy, the auto scaling can be triggered when the alarm condition is reached.

- **Port Callback (optional)**
  - Input the URL that can be accessed by the public network as the callback API address (domain name or IP:port/path), and the cloud monitor will push the alarm information to this address in time.

   ```
   The callback domain name takes effect after verification. Please return the following code in the Response Body:
   4q3fjthjyq
   ```

---

<table>
<thead>
<tr>
<th>Configuration Type</th>
<th>Configuration Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic configurations</td>
<td>Policy names</td>
<td>Custom policy names</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>Notes on custom policies</td>
</tr>
<tr>
<td></td>
<td>Policy types</td>
<td>Select the desired policy type for monitoring Tencent Cloud services.</td>
</tr>
</tbody>
</table>
|                    | Projects | This configuration item has two functions: 
  - It manages alarm policies. After setting a project, you can quickly locate the alarm policies of a project in the alarm policy list. |
- It manages instances. Choose a project based on your needs. Then, in **Alarm Object**, you can quickly select instances under the project. You can assign Tencent Cloud services to each project based on your business types. If you want to create a project, see [Project Management](#). After creating a project, you can use the console of each Tencent Cloud service to assign projects to resources. Some Tencent Cloud services such as TencentDB for MySQL do not support project assignment. In that case, you can refer to [Specifying Projects for Instances](#) to assign projects to the corresponding instances. If you do not have project permissions, see [Cloud Access Management (CAM)](#) to obtain permissions.

**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.

**Alarm trigger conditions**
- An alarm trigger condition is a semantic condition consisting of metric, comparison, threshold, measurement period, and duration. For example, if the metric is CPU utilization, the comparison is `>`, the threshold is `80%`, the measurement period is `5 minutes`, and the duration is `2 periods`, then data on the CPU utilization of a CVM will be collected once every 5 minutes, and an alarm will be triggered if the CPU utilization exceeds 80% for three consecutive periods.
- Alarm frequency: you can set a repeated notification policy for each alarm rule. This way, an alarm notification will be sent repeatedly at a specified frequency when an alarm is triggered. Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, at an exponentially increasing interval, and other frequency options.
  - An exponentially increasing interval means that a notification is sent when an alarm is triggered the first time, second time, fourth time, eighth time, and so on. In other words, the alarm notification will be sent less and less frequently as time goes on to reduce the disturbance caused by repeated notifications.
  - Default logic for repeated alarm notifications: the alarm notification will be sent to you at the configured frequency within 24 hours after an alarm is triggered. After 24 hours, the alarm notification will be sent once every day by default.

**Configuring trigger conditions (metric alarms)**

**Configuring trigger conditions (event alarms)**
You can create event alarms so that when the Tencent Cloud service resources or the underlying infrastructure services encounter any errors, you will promptly receive notifications and can then take measures accordingly. For more information, see [Event Center](#).

**Trigger condition templates**
Enable "Trigger Condition Template" and select a configured template from the drop-down list. For detailed configurations, see [Configuring trigger condition templates](#). If the created template is not displayed, click **Refresh** on the right.
### Alarm channels

<table>
<thead>
<tr>
<th>Receiving objects</th>
<th>You can configure the receiving group or recipient as needed. If you do not have the permission to bind the receiving object, refer to <a href="https://cloud.tencent.com/document/product/598">Cloud Access Management (CAM)</a> to obtain permissions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective periods</td>
<td>You can set custom effective periods for alarm notifications. By default, the effective period is all day (00:00:00 - 23:59:59).</td>
</tr>
</tbody>
</table>
| Receiving channels | Email and SMS are supported.  
  - Before configuring the email/SMS receiving channel, go to the [Cloud Access Management](https://cloud.tencent.com/document/product/598) console to check whether your email and SMS have been verified. If they have not been verified, you will not be able to receive alarm notifications. For each alarm type, each user has a monthly quota of 1,000 free text messages per month. After this quota is exceeded, you will not be able to receive SMS alarm notifications. You can refer to [SMS Channel](https://cloud.tencent.com/document/product/375) to purchase a higher SMS quota. |

### API callbacks

| - | Your system can directly receive Tencent Cloud alarm notifications through the callback API. For more information, see [Callback API](https://cloud.tencent.com/document/product/598). |

4. After configuring the above information, click **Save**. The alarm policy has been created successfully.

**Note:**

CVM alarms can be sent normally only after the monitoring **Agent** has been installed on CVM instances and reports monitoring metric data. On the Cloud Monitor page, you can view CVM instances that do not have Agent installed and download the IP address list.

### Deleting an alarm policy

**Note:**

The **Enabled/Instances** field in the alarm policy list displays the number of **alarm objects** associated with the alarm policy. If the value is not 0, the policy cannot be deleted. Only when all alarm objects are disassociated can the policy be deleted.

**Case 1: the alarm policy is not associated with instances.**
Click **Delete** in the alarm policy list.

### Case 2: the alarm policy is associated with instances.

1. On the alarm policy list, click the name of the alarm policy you want to delete to go to the alarm policy management page.
2. In the **Alarm Object** module, click **Disassociate All** and confirm the disassociation in the pop-up window. If instances are deployed in multiple regions, you need to repeat this step until all instances in all regions have been disassociated.

3. After all instances are disassociated from the policy, return to the alarm policy list page and click **Delete**.

### Default alarm policy

Currently, the default alarm policy is only supported for: CVM-basic monitoring, TencentDB for MongoDB, TencentDB for MySQL-CVM monitoring, TencentDB for Redis, TencentDB for CynosDB-MySQL, TencentDB for CynosDB-PostgreSQL, Messaging Service CKafka-Instance, and Elasticsearch.

- When you successfully purchase a Tencent Cloud service that supports the default policy for the first time, Cloud Monitor will automatically create the default alarm policy for you. For more information on the metrics/events supported by the default policy or alarm rules, see the default policy of Tencent Cloud services.
- You can also manually create an alarm policy and set it as the default alarm policy. After the default policy is set, newly purchased instances will be automatically associated with the default policy without requiring
The default alarm policy cannot be deleted.

The default policy of Tencent Cloud services is as follows:

<table>
<thead>
<tr>
<th>Tencent Cloud Service</th>
<th>Alarm Type</th>
<th>Metric/Event Name</th>
<th>Alarm Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVM</strong></td>
<td><strong>Metric alarms</strong></td>
<td><strong>CPU utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;95%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Memory utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;95%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;95%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Public bandwidth utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;95%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td><strong>Event alarm</strong></td>
<td><strong>Disk read-only</strong></td>
<td>-</td>
</tr>
<tr>
<td><strong>TencentDB for MySQL-CVM monitoring</strong></td>
<td><strong>Metric alarms</strong></td>
<td><strong>Disk utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CPU utilization</strong></td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td>Service</td>
<td>Event alarms</td>
<td>Metric alarms</td>
<td>Alarm Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TencentDB for MongoDB</td>
<td>Memory OOM</td>
<td>Disk usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td>TencentDB for Redis-CKV version/community version</td>
<td></td>
<td>Capacity usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td>TencentDB for CynosDB-MySQL</td>
<td>Event alarms</td>
<td>Memory OOM</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Instance read-only (disk capacity limit exceeded)</td>
<td></td>
</tr>
<tr>
<td>TencentDB for CynosDB-PostgreSQL</td>
<td>Event alarms</td>
<td>Insufficient memory</td>
<td>-</td>
</tr>
<tr>
<td>Message Queue CKafka-Instance</td>
<td>Metric alarm</td>
<td>Disk usage percentage</td>
<td>The measurement period is 1 minute; the threshold is &gt;85%; the duration is 5 periods</td>
</tr>
<tr>
<td>Elasticsearch service</td>
<td>Metric alarms</td>
<td>Avg disk usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;80%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg CPU usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;90%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg JVM memory usage</td>
<td>The measurement period is 1 minute; the threshold is &gt;85%; the duration is 5 periods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluster health</td>
<td>The measurement period is 1 minute; the threshold is &gt;=1; the duration is 5 periods</td>
</tr>
</tbody>
</table>
Configuring trigger condition templates

Overview

You can set an alarm rule for a specific Tencent Cloud product through a trigger template and then reuse the alarm rule to set alarm policies for other products, eliminating the need to set the same alarm rule repeatedly. When using a trigger template to set triggers for an alarm policy, you can edit the template and then apply it to the corresponding alarm policy group. This allows you to quickly modify alarm policies and rules in a unified manner, improving OPS efficiency. This document describes how to configure a trigger template.

Notes

An alarm trigger is a semantic condition consisting of metric, comparison, threshold, statistical period, and duration. For example, if the metric is CPU utilization, the comparison is $>$ , the threshold is 80% , the statistical period is 5 minutes , and the duration is 2 periods , then data on CPU utilization of a CVM will be collected once every 5 minutes, and an alarm will be triggered if the CPU utilization exceeds 80% for three consecutive periods.

You can set a repeated notification policy for each alarm rule, so an alarm notification will be sent repeatedly at specified frequency when an alarm is triggered.

Frequency options: never repeat, every 5 minutes, every 10 minutes, and other frequencies that increase exponentially.

Exponential increase means that when an alarm is triggered for the first time, second time, fourth time, eighth time, ..., or 2 to the power of Nth time, alarm notifications will be sent. In other words, the alarm notification will be sent less and less frequently with longer time interval in between, reducing the disturbance caused by repeated notifications.

The default logic for repeated alarm notifications is as follows:

- The alarm notification will be sent to you at the configured frequency for 24 hours after an alarm is triggered.
- Then, the alarm notification will be sent once every day by default.
- The alarm notification will be sent for the last time 72 hours after the alarm is triggered and then will no longer be sent.

- A trigger template is used to set triggers for one specific Tencent Cloud product.
- After a trigger template is modified, the corresponding alarm policy that has already been applied will be synced to the latest trigger.

Directions
Creating a trigger condition template

1. Log in to the Cloud Monitor Console.
2. On the left sidebar, click Trigger Condition Template to enter the trigger template list page.
3. Click Create. In the pop-up window, configure the following items:
   - Template Name: enter a template name.
   - Remarks: enter template remarks.
   - Policy Type: select a monitored service, such as CVM.
   - Use preset trigger conditions: select this option to enable preset trigger conditions for the corresponding monitored product.
   - Trigger condition: this includes indicator alarm and event alarm. You can click "Add" to set multiple alarms.
4. Click Save.

Editing a trigger condition template

1. Log in to the Cloud Monitor Console.
2. On the left sidebar, click Trigger Condition Template to enter the trigger template list page.
3. Click the name of the template to be edited to enter the details page.
4. Click **Edit** to modify alarm trigger conditions.

![Image of Basic Cloud Monitor page](image-url)
5. Modify trigger conditions as needed.

![Modify trigger conditions](image)

The alarm trigger condition template has been associated with 0 policies. Any modification on it will be applied to all associated alarm policies.

After a trigger template associated with alarm policies is edited, the modification will apply to all associated alarm policies.

**Deleting a trigger condition template**

1. Log in to the Cloud Monitor Console.
2. On the left sidebar, click **Trigger Condition Template** to enter the trigger template list page.
3. Find the template to be deleted and click **Delete** in the column on the right.

![Trigger template list](image)

4. Click **Delete** in the pop-up dialog box.

After a trigger template associated with alarm policies is deleted, all alarm policies associated with the template will become invalid.
Copying a trigger condition template

1. Log in to the Cloud Monitor Console.
2. On the left sidebar, click Trigger Condition Template to enter the trigger template list page.
3. Find the template to be copied and click Copy in the column on the right.

When a trigger template is copied, only its trigger conditions and rules will be copied. If the trigger template is associated with alarm policies, the relationship will not be copied.
Alarm Receiver

Binding and Unbinding Objects

Last updated: 2020-07-14 10:15:23

Introduction

After you create an alarm policy, you need to bind certain alarm objects to the policy to specify which instance objects will trigger alarms when the alarm conditions are met.

Directions

**Binding objects**

1. Log in to the Cloud Monitoring Console.
2. Click **Alarm Configuration** > **Alarm Policy** to access the **Alarm Policy** page.
3. Find the policy with which you want to bind objects and click the alarm policy name to access its details page.
4. In the **Alarm Object** section, click **Add Object** after selecting the desired region and then select a corresponding product instance to bind an object to the policy.

![Alarm Object Table]

**Unbinding objects**

1. Log in to the Cloud Monitoring Console.
2. Click **Alarm Configuration** > **Alarm Policy** to access the **Alarm Policy** page.
3. Find the policy with which you want to bind objects and click the alarm policy name to access its details page.
4. In the **Alarm Object** section, select the instance for which you want to remove a bound object. At the top of the **Alarm Object** section, click **Disassociate** to unbind the object from the alarm policy.
5. You can also click **Disassociate All** to unbind all objects from the alarm policy.
Creating Alarm Recipient Groups

Operation Scenarios

Alarm recipient groups determine who can receive alarm notifications. You can put people related to the same alarm in the same group. When the alarm is triggered, people in the group will receive the corresponding alarm notification. The following describes how to add an alarm recipient group for an alarm policy.

Directions

Adding an alarm recipient group

1. Log in to the Cloud Monitoring Console.

2. In the left sidebar, choose Alarm Configuration > Alarm Policy to access the alarm policy management page.

3. Find the policy to which you want to add a recipient group and click on its name to access the details page.

4. Scroll down, find the Alarm Recipient Object configuration item, and click Edit. The alarm recipient configuration box will pop up.
5. Click **Add Recipient Group** and the user group module in the CAM Console will be displayed on a new page. For more information on how to create a user group, please see User Group Management. For more information on how to create a new user, please see Creating a Custom Sub-user.

6. After creating the user and user group, return to and refresh the alarm policy page of Cloud Monitoring. In the alarm recipient group module, select the user group you just created.

7. You can select receipt channels as needed.

8. After completing the configuration, click **Save** to add the user group to the alarm policy. The user group can then receive alarm notifications sent by the alarm policy.

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.

Managing alarm receipt methods

- Currently, alarm notifications can be sent via email, SMS, and WeChat. You can modify users' phone numbers, email addresses, and WeChat accounts in the CAM Console and decide how they will receive alarm notifications. For more information on how to modify user information, please see Creating a Custom Sub-user. You can set alarm notifications to be received via WeChat.

Unsubscribing from an alarm

If you do not want a user to receive alarm notifications for a particular policy, you can cancel the user's alarm subscription by the two following ways:

- In the Cloud Monitoring Console, disassociate the alarm recipient group of the target user from the corresponding policy.
- In the CAM Console, delete the corresponding user group or user.
Alarms Types

There are four types of Tencent Cloud Monitor alarms, including basic monitor alarm, cloud automated testing alarm, custom message alarm and custom monitor alarm

<table>
<thead>
<tr>
<th>Alarm Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic monitor alarm</td>
<td>Alarms regarding the basic monitoring metrics supported by Tencent Cloud, such as CVM CPU utilization, disk utilization and so on.</td>
</tr>
<tr>
<td>Cloud automated testing alarm</td>
<td>Alarms created by the automated testing tasks that were configured by users in the Cloud Automated Testing console.</td>
</tr>
<tr>
<td>Custom message alarm</td>
<td>Alarms created by the Cloud Monitor Custom Message service that is used by users.</td>
</tr>
<tr>
<td>Custom monitor alarm</td>
<td>Alarms created by the Cloud Monitor Custom Monitor service that is used by users.</td>
</tr>
</tbody>
</table>

Alarm Channel

Currently, Tencent Cloud supports sending alarm messages via SMS and email.

All alarms are sent via these two channels by default. If you just want to receive alarms from one channel, you can go to the Tencent Cloud console and check if your email/mobile phone has been correctly configured and verified.
SMS Channel

Last updated: 2020-02-24 19:54:01

SMS Quota

Currently, Tencent Cloud SMS alarm channel has quota limit. The quota system consists of a free quota and an additional quota that you purchase.

When the monthly free SMS quota is used up, the system will send you an alarm notification, which will no longer be sent through the SMS channel for the rest of the month, but the email channel is not affected.

You can purchase an additional SMS quota if the free quota does not meet your needs.

Quota Types

<table>
<thead>
<tr>
<th>Quota Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Quota</td>
<td>A certain amount of free SMS quota is available, allowing you to receive alarm notifications through the SMS channel</td>
</tr>
<tr>
<td>Additional Quota</td>
<td>You can purchase an additional SMS quota if the free quota does not meet your needs</td>
</tr>
</tbody>
</table>

Free quota details

<table>
<thead>
<tr>
<th>Alarm Type</th>
<th>Free Quota</th>
<th>Free Quota Granting Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Alarm</td>
<td>1,000 messages/month</td>
<td>The free quota is reset to 1,000 on the first day of each month, regardless of the remaining quota in the previous month</td>
</tr>
<tr>
<td>Cloud automated testing alarm</td>
<td>1,000 messages/month</td>
<td>The free quota is reset to 1,000 on the first day of each month, regardless of the remaining quota in the previous month</td>
</tr>
<tr>
<td>Custom message alarm</td>
<td>1,000 messages/month</td>
<td>The free quota is reset to 1,000 on the first day of each month, regardless of the remaining quota in the previous month</td>
</tr>
<tr>
<td>Custom monitoring alarm</td>
<td>1,000 messages/month</td>
<td>The free quota is reset to 1,000 on the first day of each month, regardless of the remaining quota in the previous month</td>
</tr>
</tbody>
</table>

Additional quota details

Billing methods of additional quotas
Additional quotas for different alarm types are calculated separately, so you need to purchase separate quotas for basic alarms, cloud automated testing alarms, custom message alarms, and custom monitoring alarms.

Currently, additional quotas are not available for custom message alarms or custom monitoring alarms.

<table>
<thead>
<tr>
<th>Additional quota to be purchased</th>
<th>Additional quota price</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 100 messages</td>
<td>0.055</td>
</tr>
<tr>
<td>≥ 100 messages and &lt; 500 messages</td>
<td>0.052</td>
</tr>
<tr>
<td>≥ 500 messages and &lt; 1,000 messages</td>
<td>0.050</td>
</tr>
<tr>
<td>≥ 1,000 messages</td>
<td>0.045</td>
</tr>
</tbody>
</table>

- Deduction rule: When sending alarm messages, the system uses the free quota first, and then the additional quota if free quota is used up.
- Quota validity: An alarm quota is permanently valid. You can use a purchased quota at any time.

**Purchase Channels**

Log in to [Cloud Monitoring Console](#). On the [Monitoring Overview](#) page, you can view the SMS utilization. Click **Purchase SMS** to purchase an additional SMS quota.

**Quota counting rules**

1. The quotas for each alarm type are counted separately. Each developer has a certain free SMS quota for each alarm type every month. When the free SMS quota for an alarm type is used up, it does not affect the SMS message sending of other alarm types.
2. The quantity deducted from an SMS quota is determined by the actual number of received messages. For example, if you configure 10 recipients to receive a certain alarm message (a total of 10 messages will be sent to 10 recipients when the alarm is triggered), 10 messages will be deducted from the corresponding SMS quota.

   Assume that you are using the repeated alarm notification feature, a recipient group of 10 recipients is configured for a certain alarm, and the alarm is configured to be sent repeatedly every hour. If the alarm lasts for 24 hours, 240 messages (10 x 24) will be deducted from the SMS quota. Note that repeated alarm notification increases SMS quota consumption.

3. When sending alarm messages, the system uses your free quota first, and then the additional quota if the free quota is used up.
Alarm Callback

Last updated : 2020-09-21 14:18:25

By using API callbacks, your WeCom group or self-built system can directly receive alarm notifications from Cloud Monitor. API callbacks can push alarm information to URLs that are accessible over the public network through HTTP POST requests. You can take further actions based on the alarm information pushed by API callbacks. If you need to receive alarm notifications through a WeCom group, see Receiving Alarm Notifications through a WeCom Group.

Note:

- After you save the callback URL, the system will automatically verify your URL once. The timeout threshold for this verification is 5 seconds. When an alarm policy created by the user is triggered or the alarm is resolved, the alarm messages will be pushed through the API callbacks. An alarm message can be pushed up to three times, and the timeout threshold for each request is 5 seconds.
- When an alarm policy created by the user is triggered or the alarm is resolved, the alarm messages will be pushed through the API callbacks. API callbacks also support repeated alarms.

Directions

1. Go to the Cloud Monitor Console > Alarm Policy.
2. Select an alarm policy to enter its alarm policy management page.
3. In the API callback section, enter an alarm callback URL that is accessible over the public network.

4. If the HTTP response returns code 200, the verification is successful. After the callback URL is successfully verified, Cloud Monitor will push the alarm messages through the HTTP POST requests to the URL of your system. You can further process the pushed alarm information by referring to Alarm Callback Parameters.

**Alarm Callback Parameters**

When an alarm rule is triggered, Cloud Monitor will send alarm messages to the URL of your system. The API callback sends data in the JSON format through the HTTP POST requests. You can further process the alarm information by referring to the following parameter descriptions.
Metric alarms

Sample metric alarm parameters

```json
{
"sessionId": "xxxxxxxxx",
"alarmStatus": 1, // 1: alerted, 0: resolved
"alarmType": "metric", // Alarm type ("metric": metric alarm, "event": event alarm)
"alarmObjInfo": {
"region": "gz", // This field will not be returned for products that are not region-specific
"namespace": "qce/cvm", // Product namespace
"dimensions": {}, // The value of the `dimensions` field varies by product
"unInstanceId": "ins-o9p3rg3m",
"objId": "xxxxxxxxxxxxxx"
}
},
"alarmPolicyInfo": {
"policyId": "policy-n4exeh88", // ID of the alarm policy group
"policyType": "cvm_device", // Name of the alarm policy type
"policyName": "test", // Name of the alarm policy group
"policyTypeCName": "CVM - basic monitoring", // Displayed name of the alarm policy type
"conditions": {
"metricName": "cpu_usage", // Metric name
"metricShowName": "CPU utilization", // Displayed metric name
"calcType": ">", // Comparison method (this field will not be returned for metrics without a threshold)
"calcValue": "90", // Alarm threshold (this field will not be returned for metrics without a threshold)
"currentValue": "100", // Current alarm value (this field will not be returned for metrics without a threshold)
"unit": "/", // Unit (this field will not be returned for metrics without a threshold)
"period": "60", // Statistical period in seconds (this field will not be returned for metrics without a threshold)
"periodNum": "1", // Duration (this field will not be returned for metrics without a threshold)
"alarmNotifyType": "continuousAlarm", // Whether repeated alarms are supported ("singleAlarm": non-repeated alarm; "exponentialAlarm": exponential alarm; "continuousAlarm": persistent alarm. This field will not be returned for metrics without a threshold)
"alarmNotifyPeriod": 300 // Frequency of the repeated alarms in seconds (this field will not be returned for metrics without a threshold)
}
},
"firstOccurTime": "2017-03-09 07:00:00", // Time when the alarm is triggered for the first time
"durationTime": 500, // Alarm duration in seconds (if the alarm is unresolved, this value will be the duration from the time when the alarm is triggered for the first time to the time when the current alarm is sent)
"recoverTime": 0 // The time it takes to resolve the alarm in seconds (if the alarm is unresolved, the value of this parameter will be 0)
}
```

Sample metric alarm dimensions

**CVM**

```json
"dimensions": {
"unInstanceId": "ins-xxxxxxxxx",
"objId": "94f1133c-46cf-4c61-a4c1-d928183aba47", // Instance dimension bound to the backend
```
"objName": "172.21.30.15#588789" // Instance information returned in the alarm SMS message
}

CLB - public network listener

"dimensions": {
"protocol": "https",
"vip": "118.25.31.161",
"vport": 443,
"objId": "118.25.31.161#443#https", // Instance dimension bound to the backend
"objName": "CAuthCenteH5 | Classic network | 118.25.31.161(https:443)" // Instance information returned in the alarm SMS message
}

CLB - private network listener

"dimensions": {
"protocol": "",
"vip":",
"vpcId": 123,
"vport": "",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

CLB - public network server port

"dimensions": {
"domain": "",
"unLoadBalancerId": "",
"protocol": "",
"lanIp": "",
"port": "",
"url": "",
"vip": "",
"vpcId": 123,
"loadBalancerPort": "",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

CLB - private network server port

"dimensions": {
"protocol": "",
"lanIp": "",
"port": "",
"vip": "",
"vpcId": 123,
"loadBalancerPort": "",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

TencentDB for MySQL - primary monitoring

"dimensions": {
  "uInstanceId": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}

TencentDB for MySQL - secondary monitoring

"dimensions": {
  "uInstanceId": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}

TencentDB for Redis

"dimensions": {
  "redis_uuid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}

Direct Connect - connection

"dimensions": {
  "directconnectid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}

Direct Connect - dedicated tunnel

"dimensions": {
  "directconnectconidd": "dcx-jizf8heu",
  "objId": "dcx-jizf8heu", // Instance dimension bound to the backend
  "objName": "dcx-jizf8heu" // Instance information returned in the alarm SMS message
}

VPC - direct connect gateway

"dimensions": {
  "directconnectgatewayid": "dcg-8wo1p2ve",
  "objId": "dcg-8wo1p2ve", // Instance dimension bound to the backend
  "objName": "dcg-8wo1p2ve" // Instance information returned in the alarm SMS message
}
Direct Connect - dedicated tunnel

```
"dimensions": {
  "directconnectconnid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

VPC - NAT gateway

```
"dimensions": {
  "uniq_nat_id": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

VPC - VPN tunnel

```
"dimensions": {
  "vpnconnid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

VPC - peering connection

```
"dimensions": {
  "peeringconnectionid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

** VPC - cross-region interconnection over the classic network**

```
"dimensions": {
  "peeringconnectionid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

VPC - direct connect gateway

```
"dimensions": {
  "directconnectgatewayid": "xxx",
  "objId": "xxx", // Instance dimension bound to the backend
  "objName": "xxx" // Instance information returned in the alarm SMS message
}
```

VPC - VPN gateway
"dimensions": { 
"appid": 12345,
"vip": "10.0.0.0",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

VPC - network detection

"dimensions": { 
"appid": 12345,
"netdetectid": "xxx",
"vpcid": "xxx",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

VPC - shared bandwidth package

"dimensions": { 
"__region__": "xxx",
"appid": 12345,
"netgroup": "xxx",
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx" // Instance information returned in the alarm SMS message
}

Event alarms

Sample event alarm parameters

```
{
  "sessionId": "vuRH4Z1xBJSMNJHvNZhlsG9HY",
  "alarmStatus": "1", // 1: alerted, 0: resolved
  "alarmType": "event", // Alarm type ("metric": metric alarm, "event": event alarm)
  "alarmObjInfo": {
    "region": "gz", // This field will not be returned for products that are not region-specific
    "dimensions": { // The value of the 'dimensions' field varies by product
      "unInstanceId": "ins-pftdvqa2",
      "objDetail": { // Details of the event alarm object
        "deviceLanIp": "172.21.0.17",
        "deviceWanIp": "118.89.233.99",
        "uniqVpcId": "vpc-ilrwkcbw"
      }
    }
  },
  "alarmPolicyInfo": {
    "policyId": "policy-n4exeh88", // ID of the alarm policy group
    "policyType": "cvm_device", // Name of the alarm policy type
    "policyName": "teset", // Name of the alarm policy group
    "conditions": {
```
"productName":"cvm", // Name of the product type
"productShowName":"CVM", // Displayed name of the product type
"eventName":"ping_unreachable", // Event name
"eventShowName":"ping unreachable", // Event name
"alarmNotifyType":"singleAlarm", // Whether repeated alarms are supported ("singleAlarm": non-repeated alarm; "exponentialAlarm": exponential alarm; "continuousAlarm": persistent alarm. This field will not be returned for metrics without a threshold)
"alarmNotifyPeriod":"0" // Frequency of the repeated alarms in seconds (this field will not be returned for metrics without a threshold)
},
"policyTypeCName":"CVM - basic monitoring" // Displayed name of the alarm policy type
},
"firstOccurTime":"2018-06-15 16:32:06", // Time when the alarm is triggered for the first time
"recoverTime":0 // The time it takes to resolve the alarm in seconds (if the alarm is unresolved or does not have a resolved state, the value of this parameter will be 0)
}

Sample event alarm dimensions

CVM

"dimensions":{
"unInstanceId":"ins-pftdvqa2",
"objDetail":{ // Details of the event alarm object
"deviceLanIp":"172.21.0.17",
"deviceWanIp":"118.89.233.99",
"uniqVpcId":"vpc-ilrwkcbw"
}
}

TencentDB for MySQL

"dimensions": {
"deviceName": "production-xd_item_center-0-offline-6035",
"objDetail": { 
"IP": "10.80.17.217"
},
"unInstanceId": "cdb-bwieva60"
}

VPC - peering connection

"dimensions":{
"unInstanceId":"pcx-142mpvfc",
"objDetail":{ // Details of the event alarm object
"PeeringConnectionName":"test-VPC1 <-> test-VPC3",
"QosBandwidth":"100Mps",
"VpcName":"test-VPC1",
"VpcId":"vpc-5xl9j9q8"
}
}
VPC - VPN gateway

```
"dimensions":{
  "unInstanceId":"vpngw-i0s10nr1",
  "objDetail": { // Details of the event alarm object
    "VpnGatewayName":"vpn---fran",
    "InternetMaxBandwidthOut":"5Mps",
    "VpcName":"vy-vpn2",
    "VpcId":"vpc-709l0i0x"
  }
}
```

CLB - VIP blocking

```
"dimensions":{
  "unInstanceId":"clb-test",
  "objDetail": { // Details of the event alarm object
    "vip":"127.0.0.1"
  }
}
```

Direct Connect - connection

```
"dimensions":{
  "objDetail":{
    "ar":"Guangzhou Science City",
    "bandwidth":"10000",
    "circuitNumber":"Huaxinyuan 0601-H0x-PL0x-x",
    "dcType":"Bare fiber"
  },
  "unInstanceId":"dc-j0cp3tgr"
}
```

Direct Connect - dedicated tunnel

```
"dimensions":{
  "objDetail":{
    "connLocalIp":"169.254.65.133",
    "connPeerIp":"169.254.65.134"
  },
  "unInstanceId":"dcx-881ekns2"
}
```
Receiving Alarm Notifications through a WeCom Group

This document describes how to receive alarm notifications through a WeCom group.

Use Limits

Regarding sending WeCom group messages, the number of messages sent by each bot cannot exceed 20 per minute. If you have many alarm policies, we recommend that you create multiple bots and associate alarm policies with different bots. Otherwise, multiple alarm policies may trigger alarms simultaneously, and you may fail to receive some alarm notifications as a result.

Note:

After you successfully create WeCom bots and configure the callback address, Cloud Monitor will automatically push the alarm messages to the WeCom bots. This way, you can receive alarm notifications through a WeCom group.

Step 1: Add a Bot on WeCom

WeCom for PC

1. On WeCom for PC, find the target WeCom group for receiving alarm notifications.
2. Right-click the WeCom group. In the window that appears, click Add Group Bot.
3. In the window that appears, click Create a Bot.
4. In the window that appears, enter a custom bot name and click Add.
5. Copy the webhook address and configure the API callback by following Step 2.

WeCom for Web
1. On WebCom for Web, open the target WeCom group for receiving alarm notifications.
2. Click the group settings icon in the upper-right corner.
3. On the group settings page, choose **Group Bots > Add a Bot**.
4. On the management page for adding bots, enter a custom name for the new bot.
5. Click **Add**, copy the webhook address, and configure the API callback by following Step 2.

Step 2: Configure the Alarm API Callback

Go to **Cloud Monitor Console - Create Alarm Policy**, enter the webhook address, and click **Complete**. For more information on how to create alarm policies, see **Creating Alarm Policies**.
After the configuration is completed successfully, when an alarm policy is triggered or the alarm is resolved, you will receive alarm notifications sent by group bots through the WeCom group, as shown in the following figure:
Callback example 207 9-7 15:37:19

Dear User,
A Cloud Monitoring threshold alarm under your account (ID: [redacted], alias: [redacted]) has been triggered.

Alarm Details
Alarm Information: Cloud Virtual Machine | CPUUtilization > 80%
Current Data: 85%
Alarm Object: [redacted]
Project | Region: default project | guangzhou
Alarm Policy: test111
Triggered Time: 2020-09-07 15:37:00 (UTC+08:00)
Alarm details are available on Cloud Monitor Console.
View Alarm

Last updated : 2019-12-14 14:20:31

You can view all the alarms occurring within a certain period via the Tencent Cloud's Cloud Monitoring Console. There are three types of alarms((Viewing Custom Monitoring alarms is not available in Monitoring Console)):

- Basic alarms: Alarms sent by pre-defined alarm metrics of each product
- Cloud Automated Testing alarms: Alarms sent by Cloud Automated Testing
- Custom Monitoring alarms: Alarms sent by Custom Monitoring

1) Log in to Tencent Cloud Console, click "Cloud Monitoring" - "My Alarms" tab, and then click "Alarm List" menu.

2) The details of basic alarms, Cloud Automated Testing alarms, and Custom Monitoring alarms will be displayed on the right side. Users can easily acquire the operation status of services within a certain period.

3) Click the time picker in the upper left corner to adjust the alarm time to be displayed.
Start and stop alarms

Operation Scenarios

You can use the alarm on-off feature to enable or disable an alarm policy as needed. This allows you disable unwanted alarm messages. You can also quickly enable the disabled alarm policy again when needed.

Steps

1. Log in to the Cloud Monitoring console.
2. In the left sidebar, click Alarm Configuration > Alarm Policy to access the management page.
3. Find the target policy. Click the toggle in the Alarm On-Off column to enable or disable alarms for the policy.
Custom Message

Overview

Cloud Monitor provides a complete set of monitoring capabilities such as monitoring data collection, data computation and aggregation, visualized data display, alarm convergence, alarm distribution, alarm notification, etc. The custom notification feature of Cloud Monitor now provides alarm channel as an independent application to help you implement alarm distribution and notification for your own businesses and self-built monitoring system in different monitoring and alarm scenarios. You can thus quickly build alarm notification push channels.

Features

Custom notification provides the following features for business alarm scenarios:

- **Alarm distribution**: you can push alarm notifications of different modules and resources to the corresponding notification policies by configuring and managing such policies.
- **Alarm subscription**: you can configure recipient groups for notification policies to implement subscription to corresponding alarm notifications.
- **Alarm channel**: you can configure alarm channels for notification policies, so recipients in the alarm recipient group can receive notifications pushed via corresponding channels.
- **Alarm history view and search**: you can view previously pushed alarm notifications under a notification policy and search for alarm content by keywords.

Scenarios

- **Custom business alarm push**: alarms can be pushed to corresponding recipients through specific alarm channels in a self-built monitoring system.
- **Prompt delivery of important service information**: notifications about specific service status and exceptions will be pushed to developers promptly, with no need to configure monitoring, log system integration, and alarm policies.

Principle and call methods

Cloud Monitor custom notifications uses a **notification policy** with a globally unique ID as the hub for receiving and distributing alarm notifications. An alarm notification can be distributed to a notification policy by specifying its ID, and then the policy will send the notification to recipients based on the configured subscription and alarm channel.
Cloud Monitor custom notification supports two call methods to provide the alarm channel service.

- **API**: the API for sending custom notifications can be called to push an alarm notification to the corresponding notification policy by passing in the specified policy ID and alarm content.
- **Agent**: on a CVM instance where Cloud Monitor Agent has been installed, you can directly use the provided command line tool `cagent_tools` to run relevant commands to specify the policy ID and content and send them when an alarm is triggered.

### Operation Guide

#### Creating and managing notification policy

You can create, configure, edit, and delete a notification policy.

1. Log in to the [Cloud Monitoring Console](https://console.cloud.tencent.com).
2. On the left sidebar, click **Alarm Configuration > Custom Notifications** to enter the custom notification page.
3. (Optional) Click **Add Notification Policy**, enter the policy name, select the recipient group, check the corresponding alarm channel, and click **Complete** to complete policy creation.
4. (Optional) Click **Edit** in the "Operation" column of the specified notification policy, modify the policy name, recipient group, and alarm channel, and click **Complete** to complete policy modification.
5. (Optional) Click **Delete** in the "Operation" column of the specified notification policy and click **OK** in the pop-up box to delete the policy.

#### Pushing alarm notification through call

You can call the relevant API or use the agent command line tool to send notifications to the custom notification service.

1. Enter the [Custom Notifications](https://console.cloud.tencent.com) page in Cloud Monitoring Console to get the ID of the specified policy for alarm distribution.
2. (Optional) **Method 1**: call the API for sending custom notifications to pass in the specified policy ID and alarm content to the corresponding notification policy.
3. (Optional) **Method 2**: use the command line tool `cagent_tools` provided by Agent to run relevant commands to specify the policy ID and content and push the alarm notification to the corresponding notification policy.

> **cagent_tools** is applicable only to CVM instances created with system images in Tencent Cloud.

#### Example 1. Using `cagent_tools` on Linux

1. Install Agent on Linux. For more information on installation, please see [Installing Agent](https://console.cloud.tencent.com).
2. Run the following command to view the tool's help information:

```
cagent_tools
```
The result is as shown below:

3. Run the following command to specify the policy ID and alarm content to be pushed:

```
cagent_tools alarm "$alarm content" cm-xxxxxxxx (policy ID)
```

Currently, only the UTF-8 encoding format is supported for alarm content in Chinese.
The maximum length of an alarm notification is 256 bytes, and the excessive part will be truncated.
If an alarm notification is sent successfully, "send alarm OK!" will be displayed on the command line, and the return code will be 0. If an alarm notification fails to be sent, the relevant error will be displayed on the command line, and the return code will not be 0.

4. Below are use cases.

   PHP sample:

   ```
   $link = mysql_connect('192.168.0.2', 'mysql_user', 'mysql_password');
   if (!$link) {
     //alarm content
     $alarmContent = "Connection failed ";
     $cmd = "cagent_tools alarm $alarmContent cm-xxxxxxxx(policyId)";
     system($cmd);
     die('Could not connect: ' . mysql_error());
   }
   ```

   Shell sample:

   ```
   #!/bin/sh
   PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:$PATH
   CAGENT_CMD = /usr/bin/cagent_tools
   cnt=$(ps -ef | grep mysql | grep -v grep | wc -l)
   if [ $cnt -eq 0 ]; then
   ```
Example 2. Using cagent_tools on Windows

1. Install Agent on Windows. For more information on installation, please see Installing Agent.

2. Run the following command on the command line to view the tool's help information:

   ```
cagent_tools
   ```

   The result is as shown below:

   ![Command Line Output]

3. Run the following command to specify the policy ID and alarm content to be pushed:

   ```
cagent_tools alarm "$alarm content" cm-xxxxxxxx (policy Id)
   ```
4. Below are use cases.
   - **DOS sample:**
     ```
     @echo off
     set service_name=StargateSvc
     sc query %service_name% > nul
     if not %errorlevel% == 0 (cagent_tools alarm "service %service_name% didn't exist" cm-xxxxxxxx(policyId))
     ```
   
   - Currently, both UTF-8 and GBK encoding formats are supported for alarm content in Chinese.
   - The maximum length of an alarm notification is 256 bytes, and the excessive part will be truncated.
   - If an alarm notification is sent successfully, "send alarm OK!" will be displayed on the command line, and the return code will be 0. If an alarm notification fails to be sent, the relevant error will be displayed on the command line, and the return code will not be 0.

**Viewing and searching for alarm history**

1. Log in to the Cloud Monitoring Console.
2. On the left sidebar, click **Alarm Configuration > Custom Notifications** to enter the custom notification page.
3. Click on the number of alarms triggered in the last 24 hours under the specified policy as shown below:

![Image of Basic Cloud Monitor interface]

4. A floating window will pop up to display the content, time, and call method of all alarm notifications sent by the policy.

![Image of Alarm Records]

5. (Optional) You can enter alarm notification content keywords or the private IP of the CVM that calls `cagent_tools` in the search box on the top-right corner to search for corresponding alarms.
## Event Overview

An event is an information carrier, which describes a change to a specific object at a specific time. An event is associated with a unique moment and a unique object. For example, an event occurs when the status of a computer changes from running to shutdown, when a program starts or stops running, or when a power failure occurs in an office building. An event records the moment when an object changes between different states.

The monitoring service helps find, locate, and solve problems to ensure the overall stability and performance of the system and services. **Information and data** are core drivers for OPS and monitoring.

As the main information source for monitoring, metric describes the value and trend of an object's specific variable over time in a threshold-like, periodic, and persistent manner. It shows the usage of resources and environment, while reflecting their health status. For example, the metric can show the CPU utilization of a Cloud Virtual Machine (CVM) instance and the number of slow query log of a database instance. The metric covers most scenarios where problems are detected during monitoring. However, using metric as the only information source for monitoring has the following disadvantages:

- Information transmission delay. The threshold for a metric may or may not change after an event occurs for a time period.
- The accuracy and clarity of the transmitted information are low. It is difficult to determine and locate the real event or the cause of the problem by analyzing changes in threshold alone.
- Information carrier has limited forms. Metric is recorded in the form of threshold, and supplementary and incidental information cannot be provided as text.

Using event as a carrier of monitoring information can describe the running status of **resources** and **underlying infrastructure and services** in a more accurate and direct manner. This helps discover, locate, and solve problems more efficiently.

**Advantage:** events are result-oriented and can improve information accuracy, reduce delay, transmit more information, and enrich the dimension of monitoring information.

### Event Center Overview

As the event information hub of Tencent Cloud, the Cloud Monitor (CM) Event Center packages important event information in the lifecycle and operation of Tencent Cloud **resources** and **underlying infrastructure and services** into a product, which constructs a complete event consumption channel and process to help customers with monitoring and OPS on the cloud.

The packaged event information provided by the Event Center is obtained from Tencent Cloud product modules and underlying infrastructure services. It is then aggregated, analyzed, condensed, and ultimately presented.
Information sources are system logs and monitoring items under each module, which ensure the accuracy and value of the information passed on to customers.

**Event Types**

Based on information sources, causes, characteristics, and forms, events are categorized by the event center as product events and platform events, which are carried by two independent product pages and consumption processes.

- **Product Event**: product events are generated by resource instances and products (such as CVM instances) that are purchased and used by customers in Tencent Cloud. These events are directly or indirectly triggered by customers during use. They belong to specific resource instances. Customers can control and manage them. Resource instances affected by and associated with events can be explicitly determined.

- **Platform Event**: platform events are generated by the underlying infrastructure and services that support Tencent Cloud products, such as Virtual Machine Manager (VMM) that supports CVM at the virtualization layer and the underlying physical machines, networks, and storage modules. These events are generated or caused by the infrastructure and services of Tencent Cloud rather than customers. They belong to services. Customers cannot control platform events, which can only be managed by Tencent Cloud. Services or product modules affected by and associated with platform events can be determined, but the affected and associated resource instances cannot always be determined.

### Event comparison

<table>
<thead>
<tr>
<th>Item</th>
<th>Product Event</th>
<th>Platform Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event source</td>
<td>Resource instances and products that are purchased and used by customers in Tencent Cloud</td>
<td>Underlying infrastructure and services of Tencent Cloud</td>
</tr>
</tbody>
</table>

- Triggered by user behavior
- Resource Dimension
- Can be managed by customers
- Can determine affected resources
- Caused by Tencent Cloud’s underlying infrastructure devices and services
- Service Dimension
- Cannot be managed by customers, must be processed by Tencent Cloud
- Can determine affected services, but not always affected resources
<table>
<thead>
<tr>
<th>Event cause</th>
<th>Directly or indirectly triggered by customers during use</th>
<th>Generated or caused by the infrastructure and services of Tencent Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event dimension</td>
<td>Resource instance</td>
<td>Underlying service</td>
</tr>
<tr>
<td>Event processing</td>
<td>Can be controlled and managed by customers</td>
<td>Cannot be controlled by customers and must be managed by Tencent Cloud</td>
</tr>
<tr>
<td>Event object granularity</td>
<td>Resource instances affected by and associated with events can be explicitly determined</td>
<td>Services or product modules affected by and associated with events can be determined, but the affected and associated resource instances cannot always be determined</td>
</tr>
<tr>
<td>Event subscription</td>
<td>The entry is in <strong>Alarm Configuration</strong> &gt; <strong>Alarm Policy</strong>, and resource instances need to be bound</td>
<td>The entry is in <strong>Alarm Configuration</strong> &gt; <strong>Platform Event Subscription</strong></td>
</tr>
</tbody>
</table>

**Event Center Use Case**

Based on event information, the Event Center plans and provides comprehensive event consumption channels and capabilities.

- Display and tracing: records all event information related to the account. In the console, you can view, filter, search for, and trace event information.
- Alarm and notification: configures alarms for or subscriptions to monitored events and resources to promptly notify responsible personnel.
• Data pull by API: uses APIs to pull event information and connects it to Tencent’s monitoring system.
• Automation: uses events as sources to trigger associated calls to support automatic OPS.

Value

• Event Center provides a wider range of resource monitoring information to offer comprehensive data support for monitoring and OPS.
• Event Center provides event information consumption channels to tap into the value of monitoring data.
• Event Center converges determination logic to efficiently and directly locate the affected resources and their causes.
• Event information can be traced and reviewed to understand important event changes in resources and platform lifecycles.
• Events can be used as triggers to automatically respond to specific resource and environment changes.
# Event Definition

Product event records changes in instance resources and products you have purchased and used on the cloud.

Product event is directly or indirectly triggered by you during use and belongs to specific resource instance. You can control and manage the event, and determine resource instances affected by and associated with it.

Each product event record consists of the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time when an event record is generated, accurate to the second.</td>
</tr>
<tr>
<td>Event</td>
<td>Event name.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Events are divided into <code>exception</code> and <code>status change</code> based on their impact on resources and instances.</td>
</tr>
<tr>
<td>Product</td>
<td>Product type of resources associated with an event.</td>
</tr>
<tr>
<td>Associated Resource</td>
<td>Resource instance uniquely associated with an event.</td>
</tr>
<tr>
<td>Status</td>
<td>The triggered and recovered status of a recoverable exception of a specific resource.</td>
</tr>
<tr>
<td>Region (if applicable)</td>
<td>The region where a resource resides.</td>
</tr>
<tr>
<td>Project (if applicable)</td>
<td>The project to which a resource belongs.</td>
</tr>
<tr>
<td>Additional Information (if applicable)</td>
<td>Supplementary information for an event, which can include zero to multiple fields based on actual scenarios.</td>
</tr>
</tbody>
</table>

A recoverable exception is associated with two event records: triggered and recovered. To better locate and understand resource status through the console, the two associated event records are displayed together and the status of the exception of the specific resource is updated through `status`. The two event records are differentiated by start time and update time.

## Features

In addition to getting and storing resource instance events, the product event module provides a comprehensive event information consumption channel to drive monitoring and OPS.

The product event module provides the following features based on use cases such as display and tracing, alarm notification, data pull by API, and automated operation triggering:
• **Event overview**: displays the statistical data of key events filtered by current conditions. The *unresolved exception* and *unalarmed exception* dimensions are provided to help you quickly understand exceptions. You can click the corresponding number to load relevant event information.

• **Global event filtering**: allows you to filter events by attributes such as time span, product type to which an event belongs, event, event status, event type, alarm configuration status, project, etc. Multiple attributes can be selected for filtering. When multiple options of one attribute are used, the "OR" operation will be performed. When multiple attributes are used, the "AND" operation will be performed.

• **Searching for resource-associated events**: allows you to search for resource object IDs and multiple resource attributes in object details to get resource-associated events.

• **Viewing event alarm and setting quick configuration**: displays configured alarm policies for specific resources and event rules. In addition to creating and configuring event alarms on the alarm policy page, you can set quick configuration for specific resources and events. When you click the entry for creating and configuring specific product event records, resource instances and related event rules will be loaded to the alarm policy configuration page.

APIs for pulling data and the automated triggering capability will be publicly available in the near future.

**Scenarios**

• **Locating problems through alarm messages**: if alarm policies are configured for resources, event rules can be incorporated into alarm policies. When an event triggers the alarm, an alarm message will be promptly sent to the recipient through an alarm channel.

• **Routine inspection**: you can browse the product event overview, check the health status of product resource instances in real time, and promptly view unresolved and unalarmed exceptions.

• **Exception tracing**: detailed event information records are provided to help you locate resources that have exceptions, and information on associated events can be traced.

• **Automated operation triggering**: you can configure automated triggering rules based on specific resource instance events to implement auto-recovery and automated scheduling, improving monitoring and OPS efficiency.

**Use Limits**

• You can only view event information in the last 6 months.

• Event alarm messages are included in the message quota.

• The maximum number of event alarms can be configured for an account (including alarm policies of event rules) equals to the maximum number of alarm policies allowed.

**Operation Guide**

**Filtering events**
You can use global event filtering to get information on events with a specified attribute combination.

1. Log in to the Cloud Monitor Console.
2. Click Event Center > Product Event on the left sidebar to enter the product event page.
3. Click the global filtering search box in the top-right corner, modify the default filtering items (Product Type and Event Name) and confirm. Alternatively, add custom filtering items (Region, Event Status, Event Type, Alarm Configuration Status and Project) and click to complete filtering. You can use the time filtering box in the top-left corner to customize the time range and view events updated within the time range.
4. Scroll up or down on the event list page or select a specific page to view results.

Searching for resources-associated events

You can view information of events associated with specific resources.

1. Log in to the Cloud Monitor Console.
2. Click Event Center > Product Event on the left sidebar to enter the product event page.
3. Click the global filtering search box in the top-right corner, select Affected Object, enter the resource object ID, and press Enter.
4. (Optional) You can search for associated events by resource object attributes. Click the corresponding product in the Type column. Attributes supported by the product will be displayed in the global filtering search box. For example, Cluster ID and Namespace are added for TKE. Press Enter to confirm.
5. Scroll up or down on the event list page or select a specific page to view results.

Viewing event overview

The product event overview page allows you to quickly understand the overall status of resource instances and provides a shortcut entry to view key event information.

1. Log in to the Cloud Monitor Console.
2. Click Event Center > Product Event on the left sidebar to enter the product event page.
3. View event data that meets the current filter conditions in event overview, including exception and status change categories. For exception, the system also counts the number of unresolved and unalarmed events. The number in event overview changes by filter conditions and search criteria.
4. When you click the number corresponding to an overview item, the color of the overview item turns dark and the corresponding event information will be loaded in the list. Click the overview item again to return to the previous status.

Configuring event alarms

You can configure the recipients of alarm policies based on event information.

Creating an alarm policy

This procedure is the same as the existing procedure of configuring a new alarm policy. Select the corresponding rule item from the new event alarm items.

Quick configuration

1. Log in to the Cloud Monitor Console.
2. Click Event Center > Product Event on the left sidebar to enter the product event page.
3. Find the event to be configured. In the **Alarm Configuration** column, click **Add Configuration** to be redirected to the page for creating alarm policies. Enter the corresponding event rule and associated resource instance, modify the policy as needed, and then submit.

4. View alarm records in **Alarm History**.

### Supported Products

Currently, product event supports the following products and more will be supported soon. For more information, please see [Product Event List](#).

- Cloud Virtual Machine (CVM)
- Cloud Load Balancer (CLB)
- VPN Gateway
- Tencent Kubernetes Engine (TKE)
- TencentDB for MySQL
- TencentDB for MongoDB
- Direct Connect (Connection, Dedicated Tunnel)
The event center of Cloud Monitor (CM) currently provides the following monitoring information for product events:

## Cloud Virtual Machine

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
</table>
| Kernel failure | GuestCoreError   | Exception  | CVM instance | No          | An OS kernel bug or driver issue causes a fatal error in the OS kernel     | 1. Check whether any kernel driver modules are loaded into the system other than those provided by the kernel. Try not to load these modules and observe the operating status of the system.  
2. View released bug reports of the kernel and OS, and try to upgrade the kernel.  
3. By default, kdump is enabled for CVM. When a panic occurs, system memory dump information will be generated in the /var/crash directory. You can analyze it with the crash tool |
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOM</td>
<td>GuestOom</td>
<td>Exception</td>
<td>CVM instance</td>
<td>No</td>
<td>System memory usage is overloaded</td>
<td>1. Check whether the memory capacity configured in the current system meets business requirements. If additional capacity is required, we recommend upgrading the CVM memory configuration. 2. View processes that are killed during OOM based on system logs such as dmesg and /var/log/messages to check whether the memory used by processes is as expected. Use tools such as valgrind to analyze whether memory leakage occurs</td>
</tr>
<tr>
<td>Event Name</td>
<td>Event Parameter</td>
<td>Event Type</td>
<td>Dimension</td>
<td>Recoverable</td>
<td>Description</td>
<td>Troubleshooting Methods</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ping failure    | PingUnreachable | Exception  | CVM instance | Yes         | The network of the CVM instance is not pingable                             | 1. Check whether the running status of the CVM instance is normal. If any exceptions occur (for example, the system crashes), force restart the CVM instance in the console to restore it.  
2. If the CVM instance is running normally, check the CVM network configuration. This includes the internal network service configuration, firewall configuration, and security group configuration |
| Read-only disk  | DiskRead only   | Exception  | CVM instance | Yes         | Data cannot be written into the disk                                       | 1. Check whether the disk is full.  
2. In Linux, run the `df -i` command to check whether inode is used up.  
3. Check whether the file system is damaged |
<p>| Server restart  | GuestReboot     | Status change | CVM instance | Yes         | The CVM instance restarts                                                    | This event is triggered when the CVM restarts. Check whether the status change is as expected based on actual scenarios |</p>
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet loss occurs when the public network outbound bandwidth exceeds the limit</td>
<td>PacketDroppedByQoS WanOutBandwidth</td>
<td>Exception</td>
<td>CVM instance</td>
<td>Yes</td>
<td>The public network outbound bandwidth of the CVM instance exceeds the upper limit, causing packet loss. Packet loss caused by bandwidth glitches is not reflected on the bandwidth view because the minimum granularity for bandwidth statistics is 10 (total traffic in 10 seconds/10 seconds). If the constant bandwidth is not exceeded by much, it can be ignored</td>
<td>Increase the upper limit of the public network bandwidth. If the maximum purchase limit has been reached, you can reduce the bandwidth consumption of the server through load balancing and other means</td>
</tr>
<tr>
<td>CVM nvme device error</td>
<td>NvmeError</td>
<td>Exception</td>
<td>CVM instance</td>
<td>No</td>
<td>CVM nvme disk failure</td>
<td>1. Isolate the read/write of the disk and unmount the corresponding directory 2. Submit a ticket and wait for the technical personnel to replace the disk 3. After the disk is replaced, format the new disk before use</td>
</tr>
</tbody>
</table>
## Cloud Load Balancer

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked public IP</td>
<td>VipBlockInfo</td>
<td>Exception</td>
<td>CLB instance</td>
<td>Yes</td>
<td>CLB public IP under attack is blocked after an exception is detected by the security system</td>
<td>Submit a ticket to query causes and solutions</td>
</tr>
<tr>
<td>Server port status has an</td>
<td>RsPortStatusChange</td>
<td>Exception</td>
<td>Real server port</td>
<td>Yes</td>
<td>An exception is found at the real server port of the public network CLB instance during health check</td>
<td>View the service status of the real server port</td>
</tr>
</tbody>
</table>

## VPN Gateway

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
### Event Name
Packet loss occurs when the public network outbound bandwidth exceeds the limit

### Event Parameter
PacketDroppedByQoSWanOutBandwidth

### Event Type
Exception

### Dimension
VPN Gateway instance

### Recoverable
Yes

### Description
The public network outbound bandwidth of a VPN gateway instance exceeds the upper limit, causing packet loss. Packet loss caused by bandwidth glitches is not reflected on the bandwidth view because the minimum granularity for bandwidth statistics is 10 (total traffic in 10 seconds/10 seconds). If the constant bandwidth is not exceeded by much, it can be ignored.

### Troubleshooting Methods
Increase the upper limit for public network bandwidth

### Event Name
Packet loss occurs when the number of connections exceeds the limit

### Event Parameter
PacketDroppedByQoSConnectionSession

### Event Type
Exception

### Dimension
VPN Gateway instance

### Recoverable
Yes

### Description
The number of connections to the VPN Gateway instance exceeds the limit, causing packet loss.

### Troubleshooting Methods
Submit a ticket to contact us

---

**TKE**
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node exception</td>
<td>NodeNotReady</td>
<td>Exception</td>
<td>Node</td>
<td>Yes</td>
<td>A node exception may be caused by network disconnection, node kubelet exception, container OOM and more. If the node exception lasts for a long time, Kubernetes will drain containers on the node</td>
<td>1. Check on the CVM monitoring page whether the node is running. 2. Log in to the CVM to check whether kubelet is running normally. 3. Log in to the CVM to check whether docker is running normally</td>
</tr>
<tr>
<td>Node disk capacity will run out soon</td>
<td>NodeHasDiskPressure</td>
<td>Exception</td>
<td>Node</td>
<td>Yes</td>
<td>The disk (cbs or root) capacity used for container and image storage on the node will run out soon. NodeOutOfDisk will be triggered after the capacity runs out, and new containers cannot be scheduled to this node</td>
<td>Clean up the disk or container images no longer in use</td>
</tr>
<tr>
<td>Node disk capacity has run out</td>
<td>NodeOutOfDisk</td>
<td>Exception</td>
<td>Node</td>
<td>Yes</td>
<td>The disk (cbs or root) capacity used for container and image storage on the node has run out, and new containers cannot be scheduled to this node</td>
<td>Clean up the disk or container images no longer in use</td>
</tr>
<tr>
<td>Event Name</td>
<td>Event Parameter</td>
<td>Event Type</td>
<td>Dimension</td>
<td>Recoverable</td>
<td>Description</td>
<td>Troubleshooting Methods</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Node memory will run out soon</td>
<td>NodeHasInsufficientMemory</td>
<td>Exception</td>
<td>Node</td>
<td>Yes</td>
<td>Node memory utilization is high</td>
<td>Expand the node or schedule containers to other nodes</td>
</tr>
<tr>
<td>Node OOM</td>
<td>SystemOOM</td>
<td>Exception</td>
<td>Node</td>
<td>No</td>
<td>OOM occurs on the node due to high memory utilization</td>
<td>Check the causes of OOM on the node by querying monitoring data, syslog, demsg, and more</td>
</tr>
<tr>
<td>Node network unreachable</td>
<td>NodeNetworkUnavailable</td>
<td>Exception</td>
<td>Node</td>
<td>No</td>
<td>The network on the node is not configured properly. Normally, this problem will not occur in clusters created through the console or Tencent Cloud API</td>
<td>Submit a ticket to contact us</td>
</tr>
<tr>
<td>Insufficient inodes on the node</td>
<td>NodeInodePressure</td>
<td>Exception</td>
<td>Node</td>
<td>No</td>
<td>New containers cannot be created due to insufficient inodes on the node</td>
<td>Check the remaining inodes on the node. Try to clean up container images no longer in use to free up Inode space</td>
</tr>
</tbody>
</table>

**TencentDB for MySQL**

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOM</td>
<td>OutOfMemory</td>
<td>Exception</td>
<td>TencentDB for MySQL instance</td>
<td>Yes</td>
<td>Database memory usage is overloaded</td>
<td>Check whether the memory capacity configured in the database meets business requirements. If additional capacity is required, we recommend upgrading the MySQL memory configuration</td>
</tr>
<tr>
<td>Primary-secondary switch</td>
<td>PrimarySwitch</td>
<td>Exception</td>
<td>TencentDB for MySQL instance</td>
<td>No</td>
<td>This event can be triggered when a physical machine fails. Check whether the instance status is normal</td>
<td></td>
</tr>
<tr>
<td>Read-only instance removal</td>
<td>RORemoval</td>
<td>Exception</td>
<td>TencentDB for MySQL instance</td>
<td>Yes</td>
<td>A read-only instance fails or exceeds the latency threshold</td>
<td>If the read-only group contains only one instance, switch the read traffic after the read-only instance is removed to avoid a single point of failure. We recommend purchasing at least two read-only instances for the group</td>
</tr>
<tr>
<td>Instance migration caused by server failure</td>
<td>ServerfailureInstancerMigration</td>
<td>Exception</td>
<td>TencentDB for MySQL instance</td>
<td>No</td>
<td>Server failure results in instance migration</td>
<td>The migration time is subject to the maintenance window. Please change the time promptly if needed. The new migration time will be subject to the new maintenance window</td>
</tr>
</tbody>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
# TencentDB for MongoDB

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient oplog backup</td>
<td>oplogInsuffici</td>
<td>Exception</td>
<td>TencentDB for MongoDB instance</td>
<td>No</td>
<td>When TencentDB for MongoDB backs up data, it cannot read the full oplog from the last backup to the current backup. This affects database rollback to any time point in the last 7 days.</td>
<td>We recommend adjusting the size or backup frequency of the TencentDB for MongoDB oplog in the MongoDB console. If you do not need this event notification, disable it on the backup interface of the MongoDB console.</td>
</tr>
<tr>
<td>The number of connections exceeds the limit</td>
<td>connection</td>
<td>Exception</td>
<td>TencentDB for MongoDB instance</td>
<td>Yes</td>
<td>The number of connections to the instance exceeds the limit.</td>
<td>Check whether the maximum number of connections configured for the TencentDB for MongoDB instance meets business requirements. If additional connections are required, we recommend upgrading the instance configuration.</td>
</tr>
<tr>
<td>Primary-secondary switch</td>
<td>primarywitch</td>
<td>Exception</td>
<td>TencentDB for MongoDB instance</td>
<td>Yes</td>
<td>This event can be triggered when a physical machine fails. Check whether the instance status is normal.</td>
<td></td>
</tr>
</tbody>
</table>
### Direct Connect (Connection, Dedicated Tunnel)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection downtime</td>
<td>DirectConnect</td>
<td>Exception</td>
<td>Connection</td>
<td>Yes</td>
<td>Physical link of the connection is interrupted or has an exception</td>
<td>1. Check whether the physical link has an exception or is interrupted (for example, the fiber cable is cut off, the line is unplugged, etc.) 2. Check whether the receiving port and optical/electrical modules are normal 3. Check whether the network device port is turned off</td>
</tr>
</tbody>
</table>

The disk capacity has run out

- **instanceOutOfDisk** Exception
- **TencentDB for MongoDB instance** Yes
- The disk capacity is full and the instance becomes read-only
- Clean up the disk

Instance rollback

- **instanceRollback** Exception
- **TencentDB for MongoDB instance** Yes
- Instance data rollback
- This event may be triggered if the primary node fails and a primary-secondary switch occurs when some data on the primary node has not been synced to the secondary node. Check whether the instance status is normal
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Parameter</th>
<th>Event Type</th>
<th>Dimension</th>
<th>Recoverable</th>
<th>Description</th>
<th>Troubleshooting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated tunnel downtime</td>
<td>DirectConnectTunnelDown</td>
<td>Exception</td>
<td></td>
<td>Yes</td>
<td>Physical link of the connection is interrupted or has an exception</td>
<td>1. Check whether the physical link has an exception or is interrupted (for example, the fiber cable is cut off, the line is unplugged, etc.) 2. Check whether the receiving port and optical/electrical modules are normal 3. Check whether the network device port is turned off</td>
</tr>
<tr>
<td>Dedicated tunnel BGP session downtime</td>
<td>DirectConnectTunnelBGPSessionDown</td>
<td>Exception</td>
<td></td>
<td>Yes</td>
<td>The dedicated tunnel BGP session is interrupted</td>
<td>1. Check whether the BGP process of the network device is normal 2. Check whether the dedicated tunnel is normal 3. Check whether the physical line is normal</td>
</tr>
<tr>
<td>Alarm for exceeded number of BGP tunnel routes</td>
<td>DirectConnectTunnelRouteTableOverload</td>
<td>Exception</td>
<td></td>
<td>No</td>
<td>The number of BGP session routes in a dedicated tunnel exceeds 80% of the threshold</td>
<td>1. Check whether routes published by the BGP session of the dedicated tunnel have reached 80% of the maximum, which is 100 by default. For more information, see Use Limits)</td>
</tr>
<tr>
<td>Dedicated tunnel BFD detection downtime</td>
<td>DirectConnectTunnelBFDDown</td>
<td>Exception</td>
<td></td>
<td>Yes</td>
<td>The dedicated tunnel BFD detection is interrupted</td>
<td>1. Check whether the dedicated tunnel is normal 2. Check whether the physical line is normal</td>
</tr>
</tbody>
</table>
Event Definition

Platform events record changes in the underlying infrastructure and services of Tencent Cloud. These events are generated or caused by Tencent Cloud infrastructure and services. Customers cannot control these events, which instead can only be managed by Tencent Cloud.

Each platform event record consists of the following attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>The product+event name supported by the underlying infrastructure and services that caused the event</td>
</tr>
<tr>
<td>Time</td>
<td>The time when an event record is generated, accurate to second</td>
</tr>
<tr>
<td>Event Type</td>
<td>Event types are divided into problems, changes, operational announcements, and other subscriptions based on the causes and impacts of the event. <strong>Problem-type platform events</strong> are supported. Other subscription events, which are not generated by Tencent Cloud but affect underlying infrastructure, are external events for customers</td>
</tr>
<tr>
<td>Associated Resource</td>
<td>The resources associated with the infrastructure and services affected by events. Multiple resource instances of a single account may be affected</td>
</tr>
<tr>
<td>Status</td>
<td>The status indicates the event triggering and restoration status of a problem-type platform event, the event start and end status of a change-type platform event, or no status for an announcement-type event</td>
</tr>
<tr>
<td>Region (if applicable)</td>
<td>The region of the underlying infrastructure and services affected by platform events</td>
</tr>
</tbody>
</table>

Two consecutive event records are associated with an event that has a status. To better locate and understand the status of infrastructures and services in the console, the two associated event records are displayed together and the progress of a specific platform event is updated according to the **Status** attribute. The triggering and restoration event records differ by their start times and update times.

Features

The platform event module retrieves and records events generated by the platform infrastructure and underlying services, and provides the following features to support display rewind, alarm notification, data pull through APIs, and automated operation triggering:
Filtering Events: allows users to filter events by attributes, such as time span, event type, event, event status, status, and region. Multiple attributes can be selected for filtering. When multiple options of one attribute are used, the OR operation applies. When multiple attributes are used, the AND operation applies.

Searching for object-associated events: allows users to search for associated platform events by the IDs of affected objects.

Subscribing to platform events: allows users to subscribe to and promptly obtain information about platform events of specific infrastructure and services.

The progress of platform event processing is updated in real time. Event pull via APIs and automated operation triggering capacities are supported and will be publicly available in the future.

Scenarios

Planning resource changes and troubleshooting method through alarm triggering: You can subscribe to platform events associated with specific products to promptly learn about platform problems and information changes, thus quickly planning for resource changes and tracking the troubleshooting progress.

Rewinding to locate exceptions: You can refer to the processing records of platform events to locate events and determine their causes by working backward.

Automated operation triggering: The event sources of automated triggering rules support platform events, allowing you to implement self-recovery and automated scheduling to improve the efficiency of monitoring and OPS.

Use Limits

- You can only view event information from the past 6 months.
- Event alarm messages are counted into the message quota.

Operation Instructions

Filtering Events

Use the global event filtering capability to query information about platform events that match a specified attribute combination.

1. Log in to Cloud Monitoring Console.
2. In the left sidebar, click Event Center > Platform Event to access the platform event page.
3. Click the global filtering search box in the upper-right corner, modify default filtering items Product Type and Event Name, and confirm. Alternatively, customize filtering items such as Region and Event Status, and click to complete filtering. By using the time filtering box in the upper-left corner, you can customize the time range filter to display events updated within the specified time range.
4. Use the scroll bar to scroll up and down the event list page or select a specific page to jump to.
Searching for events associated with affected objects

View the information about events associated with specific affected objects.

1. Log in to Cloud Monitoring Console.
2. In the left sidebar, click Event Center > Platform Event to access the platform event page.
3. Click the global filtering search box in the upper-right corner, select Affected Object, enter the resource object ID, and press Enter.
4. Use the scroll bar to scroll up and down the event list page or select a specific page to jump to.

Subscribing to platform events

Subscribe to the recipient of information about the platform event associated with a specific product.

1. Log in to Cloud Monitoring Console.
2. In the left sidebar, choose Alarm Configuration > Platform Event Subscription to access the platform event subscription page.
3. Hover over a subscription item, click Subscription Management, select a message reception mode and a recipient, and then click OK.
4. View the latest reception modes and recipients in the subscription item list.
5. View alarm records in Alarm List.

Supported Events

The following events are currently supported and other associated products will be gradually supported.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event</th>
<th>Cause</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Cloud Virtual Machine (CVM) storage</td>
<td>Caused by the CVM infrastructure storage module</td>
<td>The I/O performance of the CVM instance deteriorates and data read-write exceptions occur</td>
</tr>
<tr>
<td>Problem</td>
<td>CVM network connection</td>
<td>Caused by the CVM infrastructure network</td>
<td>The speed of the CVM instance network slows down or the network is disconnected</td>
</tr>
<tr>
<td>Problem</td>
<td>CVM running exception</td>
<td>Caused by CVM infrastructure</td>
<td>The CVM instance bears a high load or crashes, causing services to be unavailable</td>
</tr>
</tbody>
</table>

Troubleshooting suggestion: Tencent Cloud will fix the problem. You can authorize the affected resources according to the alarm information, or wait for Tencent Cloud to solve the problem. For more information, see the documentation about service scheduling and migration.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event</th>
<th>Cause</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other subscription</td>
<td>ISP network jitter</td>
<td>Caused by ISP network problems</td>
<td>The latency to access Tencent Cloud via a public network increases or the network is disconnected</td>
</tr>
</tbody>
</table>
Installing CVM Agents

To use Cloud Monitor to view CVM metric data and generate alarms, install the monitoring component Agent on the CVM instance to collect metric data.

- To ensure the normal reporting of the monitoring data, TCP dport 80 in the CVM instance must be opened to the Internet. Agent reports data without relying on security groups or the network ACL. Therefore, you do not need to open TCP dport 80 of the security groups or the network ACL.
- To run the following command to obtain the Agent installer, you must first log in to the CVM instance.

Installing Agent on a Linux CVM Instance

Log in to the CVM instance to download the Agent installer. You can download the Agent installer only by using a private IP address of Tencent Cloud. Therefore, please ensure that the DNS of your CVM instance is a private network DNS. Otherwise, the resolution of the URL for downloading the Agent installer will fail.

Installation directions

1. Log in to a Linux CVM instance and run the following commands to install Agent:

   `chmod +x linux_stargate_installer` // Grant the permission to run the Agent installation script.
   `./linux_stargate_installer` // Install Agent.

2. Perform steps 3 and 4 to check whether the Agent installer has been executed correctly.

3. Run the following command to check whether Agent has been added to scheduled tasks.

   `crontab -l | grep stargate`

   If the following command output is returned, Agent has been added to scheduled tasks. If no prompt appears, the installation has failed.

4. Run the following commands to check whether Agent-related processes have been launched.

   `ps ax | grep sgagent`
   `ps ax | grep barad_agent`

   If the following command output is returned, the Agent-related processes have been properly launched and Agent has been successfully installed.
Other operations

Run the following command to access the Agent installation directory.

```
  cd /usr/local/qcloud/stargate/admin
```

- Uninstall Agent: no output is returned after the uninstallation command is executed. You can run the `crontab -l | grep stargate` command to check whether there are any scheduled tasks. If there are no scheduled tasks, the uninstallation has been successfully completed.

```
  ./uninstall.sh
```

- Restart Agent: if `stargate agent run succ` appears, Agent has successfully restarted.

```
  ./restart.sh
```

- Stop Agent: no output is returned after the stop command is executed. You can run the `ps ax | grep sgagent` command to check whether any Agent-related processes are running. If there are no Agent-related processes running, Agent has successfully stopped running.

```
  ./stop.sh
```

Installing Agent on a Windows CVM Instance

Log in to the CVM instance to download the Agent installer. You can download the Agent installer only by using a private IP address of Tencent Cloud. Therefore, please ensure that the DNS of your CVM instance is a private network DNS. Otherwise, the resolution of the URL for downloading the Agent installer will fail.

**Installation directions**

1. **Log in to a Windows instance**, copy the download URL `http://update2.agent.tencentyun.com/update/windows-stargate-installer.exe`, and paste it in the address bar of your browser to download the `windows-stargate-installer.exe` installer.

2. Run the installer to automatically install Agent.

   If the installation is successful, the following will appear:
i. Run the service, and you will see that the QCloud BaradAgent Monitor and QCloud Stargate Manager services are running.

![Image of Services (Local) showing QCloud BaradAgent Monitor and QCloud Stargate Manager services running]

ii. Run the task manager, and you will see the BaradAgent and sgagent processes.

![Image of Task Manager showing BaradAgent and sgagent processes]

Other operations

Uninstall Agent: run the following commands. After "[SC] DeleteService succeeds" appears, restart the CVM instance.
sc.exe delete "BaradAgentSvc"
sc.exe delete "StargateSvc"

FAQs

- If you cannot download the Agent installer or encounter other problems, see FAQs for CVM Agent.
- You can also submit a ticket to contact us for assistance.
Cloud Access Management (CAM)

Last updated: 2020-07-28 15:10:59

Cloud Monitor (CM) allows a root account to grant a sub-account access permissions via Cloud Access Management (CAM). This document describes how to manage access permissions for a sub-account.

Feature Overview

By default, a root account is the resource owner and has full access to all resources in the account. A sub-account has no access to any resources. The root account must grant a sub-account access permissions for it to access resources. You can use your root account to log in to the CAM console and grant a sub-account access permissions. For more information, see Authorization Management.

CM policies depend on the policies of other Tencent Cloud services. When you grant CM permissions to a sub-account, the corresponding cloud service permissions must also be granted for CM permissions to take effect.

**Note:**
- Permissions: allow or deny operations to access specific resources under certain conditions.
- Policies: syntax rules used to define and describe one or more permissions.

Common Permission Configuration

**Note:**
Below takes CVM permission configuration as an example. For more information on how to grant permissions for other Tencent Cloud services, see the following scenarios and CM-related Tencent Cloud service policies.
Enable the corresponding Tencent Cloud service permissions.

### Common permissions

<table>
<thead>
<tr>
<th>Permission Type</th>
<th>Permission Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM permission</td>
<td>QcloudMonitorFullAccess and QcloudMonitorReadonlyAccess</td>
</tr>
<tr>
<td>CVM permission</td>
<td>QcloudCVMReadOnlyAccess or QcloudCVMFullAccess</td>
</tr>
</tbody>
</table>

### Features and permissions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Operation Permissions</th>
<th>Access Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tencent Cloud Service</td>
<td>Policy</td>
<td>Permission Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cloud Virtual Machine (CVM)</td>
<td>QcloudCVMFullAccess</td>
<td>Full access permissions for CVMs, including monitoring permissions for CVM, CLB and VPC</td>
</tr>
<tr>
<td></td>
<td>QcloudCVMReadOnlyAccess</td>
<td>Read-only permissions for CVM resources</td>
</tr>
<tr>
<td>TencentDB for MySQL</td>
<td>QcloudCDBFullAccess</td>
<td>Full access permissions for TencentDB for MySQL instances, including</td>
</tr>
</tbody>
</table>

**CM-related Tencent Cloud service policies**

**Note:**
Provided that CM permissions have been properly granted, Tencent Cloud service resources can be accessed after the read-only permission is granted. The following table lists permissions for some Tencent Cloud services. For more information on permissions for other Tencent Cloud services, see CAM-Enabled Products.
<table>
<thead>
<tr>
<th>Tencent Cloud for MongoDB</th>
<th>TencentDB for MongoDB</th>
<th>QcloudMongoDBFullAccess</th>
<th>Full access permissions for TencentDB for MongoDB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>QcloudMongoDBReadOnlyAccess</td>
<td>Read-only permissions for TencentDB for MongoDB</td>
</tr>
<tr>
<td>TencentDB for Redis</td>
<td></td>
<td>QcloudRedisFullAccess</td>
<td>Full access permissions for TencentDB for Redis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QcloudRedisReadOnlyAccess</td>
<td>Read-only permissions for TencentDB for Redis</td>
</tr>
<tr>
<td>Tencent Cloud TcaplusDB</td>
<td></td>
<td>QcloudTcaplusDBFullAccess</td>
<td>Full access permissions for TencentDB for TcaplusDB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QcloudTcaplusDBReadOnlyAccess</td>
<td>Read-only permissions for TencentDB for TcaplusDB</td>
</tr>
<tr>
<td>Elasticsearch Service</td>
<td></td>
<td>QcloudElasticsearchServiceFullAccess</td>
<td>Full access permissions for Elasticsearch Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QcloudElasticsearchServiceReadOnlyAccess</td>
<td>Read-only permissions for Elasticsearch Service</td>
</tr>
<tr>
<td>VPC</td>
<td></td>
<td>QcloudVPCFullAccess</td>
<td>Full access permissions for VPC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QcloudVPCReadOnlyAccess</td>
<td>Read-only permissions for VPC</td>
</tr>
<tr>
<td>Direct Connect (DC)</td>
<td></td>
<td>QcloudDCFullAccess</td>
<td>Full access permissions for DC</td>
</tr>
<tr>
<td>Cloud Message Queue (CMQ)</td>
<td></td>
<td>QcloudCmqQueueFullAccess</td>
<td>Full access permissions for CMQ, including permissions for queues and Cloud Monitor</td>
</tr>
<tr>
<td>Message Queue CKafka</td>
<td></td>
<td>QcloudCKafkaFullAccess</td>
<td>Full access permissions for Message Queue CKafka</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QcloudCKafkaReadOnlyAccess</td>
<td>Read-only permissions for Message Queue CKafka</td>
</tr>
<tr>
<td>Cloud Object Storage (COS)</td>
<td>QcloudCOSFullAccess</td>
<td>Full access permissions for COS</td>
<td>Access Management</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------</td>
<td>---------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>QcloudCOSReadOnlyAccess</td>
<td>Read-only permissions for COS</td>
<td></td>
</tr>
<tr>
<td>Cloud Load Balancer (CLB)</td>
<td>QcloudCLBFullAccess</td>
<td>Full access permissions for CLB</td>
<td>Access Management</td>
</tr>
<tr>
<td></td>
<td>QcloudCLBReadOnlyAccess</td>
<td>Read-only permissions for CLB</td>
<td></td>
</tr>
<tr>
<td>Cloud File Storage (CFS)</td>
<td>QcloudCFSFullAccess</td>
<td>Full access permissions for CFS</td>
<td>Access Management</td>
</tr>
<tr>
<td></td>
<td>QcloudCFSReadOnlyAccess</td>
<td>Read-only permissions for CFS</td>
<td></td>
</tr>
</tbody>
</table>