Cloud Monitor

User Guide

User Guide

Product Introduction

Cloud Monitor is a monitoring service provided by Alibaba Cloud aiming at offering service availability, resource monitoring, and alarm management to Alibaba Cloud users. You do not need to build or develop the monitoring system by yourselve. The basic needs for monitoring can be achieved through simple setup.

Cloud Monitor offers the following functions.

Module	Capability	Main functions
Site Monitoring	Monitors the availability of user sites	The status of sites including http, ping, tcp, udp, dns, pop, smtp, ftp and their response time
Cloud Service Monitoring	Monitoring of cloud service	ECS’ s CPU and memory usage, system load, disk, disk read and write, incoming data volume and outgoing data volume, TCP, process count and status
Customized monitoring	Metric items defined by the monitoring users	The users report the metric data based on the user-defined metric items
Alarm	Alarm	Emails, messages, and TradeManager supported
Alarm contact management	Manages alarm contact and the alarm contact group	Sets alarm contact group and alarm contact

Product Brief

Overview

Definition

Cloud Monitor is a service that monitors Alibaba Cloud resources and Internet applications. Cloud Monitor can be used to collect metrics for Alibaba Cloud resources, detect Internet service availability, and set alarms for the metrics.

Customer benefits

Cloud Monitor can monitor ECS, RDS, Server Load Balancer and other types of Alibaba Cloud service resources. It can also monitor Internet application availability via common network protocols such as HTTP and ICMP. Cloud Monitor gives you a comprehensive understanding of the usage, performance and running status of Alibaba Cloud resources. The alarm service enables you to make quick responses to ensure that your applications run smoothly.

Product terminology

The following terms are the key concepts of Cloud Monitor.

Term	Description
Cloud service monitoring	This allows Alibaba Cloud service users to view performance indicators for various products. At present, it supports metric indicators for ECS, RDS, Server Load Balancer, OSS, and other main cloud products.
Customized monitoring	Based on your own business needs, you can create custom metric indicators and use scripts to report data. This satisfies your business-level monitoring needs.
Alarm service	This allows you to set alarm rules for the indicators of the three monitoring services described above. When metric data meets trigger conditions set by alarm rules, the service will send an alarm notification.
Metric item	You can set custom metric items or use the system’ s default metric data types. For example, HTTP monitoring in site monitoring has two default metric items: response time and status code. The ECS metric items include CPU usage and memory usage.
Dimension	Dimensions are used to locate metric item data. For instance, the metric item Disk IO has two dimensions: instance and disk name. These dimensions can locate the unique metric data. Currently, in customized monitoring, dimensions are represented by

	“field information”.
Alarm rule	An alarm rule is a condition. For example: “memory usage statistical period: 5 minutes; greater than or equal to 50% three times in a row” is a rule.
Channel silence	This refers to a condition under which an alarm will not be triggered again within a period of 24 hours when an indicator remains above the alarm threshold.
Alarm contact	The person who receives alarm notifications.
Alarm contact group	An alarm group is a group of one or more alarm contacts. During alarm setup, alarm notifications are sent to a specified alarm group. Based on the preset alarm method, the alarm system will send alarm notifications to members of the alarm group when an alarm is triggered.
Notification method	The method by which alarm notifications are sent to users. Methods include text message, TradeManager (Taobao), email, and MNS message queue push.

Application scenarios

Cloud Monitor provides an extensive array of application scenarios, which are explained using examples of different services below.

Cloud service monitoring

After you have bought and used an Alibaba Cloud service supported by Cloud Monitor, you can easily check the running status of your product as well as various metrics on the corresponding Cloud Service monitoring chart page. You can also set alarm rules for the metric items.

System monitoring

By monitoring ECS instance CPU usage, memory usage, outgoing public network traffic rate (bandwidth), and other basic indicators, you can use the instance properly and avoid service malfunction due to resource overuse.

Rapid exception handling

Cloud Monitor will send an alarm message when metric data reaches an alarm threshold based on

the alarm rules you set. This enables you to receive timely exception notifications and check the cause of the exception.

Rapid resizing

You can set alarm rules for various metric items such as bandwidth, connection count, and disk usage. This makes it easy for you to understand the current status of cloud services and resize as necessary once an alarm is triggered by an increase in service volume.

Site monitoring

At present, the site monitoring service supports monitoring eight protocols including HTTP, ICMP, TCP, UDP, DNS, POP3, SMTP, and FTP. This allows you to detect the availability, response time, and packet loss rate of your site. Therefore, you will get a complete picture of the availability of your site and rapidly handle any exceptions.

Customized monitoring

Customized monitoring is designed as a supplement to Cloud Service Monitoring. If Cloud Monitor does not provide your desired metric items, you can create a new metric item and report the acquired metric data to Cloud Monitor. Cloud Monitor will then display monitoring charts and raise alarms for the new metric item.

Product strengths

As a product of Alibaba Group’ s years of research efforts in the area of server monitoring, Cloud Monitor integrates the powerful data analysis capabilities of the Alibaba Cloud computing platform. Cloud Monitor provides Alibaba Cloud users with cloud service, site and customized monitoring capabilities to safeguard their products and businesses.

Seamless integration

Cloud Monitor does not have to be individually bought or activated. After registering an Alibaba Cloud account, you are automatically given access to the Cloud Monitor service. After buying and using Alibaba Cloud products, you can easily connect them with Cloud Monitor to view their operation status and set alarm rules.

Data visualization

Through Dashboard, Cloud Monitor provides a rich array of diagram presentation formats. It supports

full screen presentation and automatic data refresh. This can satisfy the metric data visualization needs in various scenarios.

Metric data processing

Cloud Monitor allows you to process metric data through Dashboard based on a combination of temporal and spatial dimensions.

Flexible alarms

Cloud Monitor also provides you with metric item alarm services. After setting reasonable alarm rules and notification methods for metric items, you will immediately receive an alarm notification when an exception occurs. This allows you to promptly discover and handle service exceptions, thereby increasing the availability of your products.

Overview page

Overview page

The **Overview** page provides an overview of cloud service resources in terms of usage and alarms. It keeps you informed about the resource usage and alarms related to each cloud service in real time.

Cloud service overview

The cloud service overview provides a resource usage overview and alarm overview for ECS, ApsaraDB for RDS, OSS, CDN, ApsaraDB for MongoDB, ApsaraDB for Memcache, Container Service, and Log Service.

The cloud service overview keeps you informed about the resource quantity, resource usage, and alarm status under your accounts.

Clicking the cloud service resource quantity brings you to the **Cloud Service Monitoring** instance list page for the corresponding product. Click an alarm rule status to enter the relevant alarm rule page.

Note: To collect the ECS instance CPU, memory, and disk usage data, you must install the Cloud Monitor plugin. For the plugin installation instructions, refer to ECS Monitoring Introduction.

Resource statistical methods

95th percentile

Percentile is a term used in statistics. To find a percentile, data values are arranged in ascending order, and the corresponding cumulative percentile is calculated. Thus, the data value corresponding to a certain percentile is called the percentile.

The 95th percentile is the value of the 95th percentile. Assuming that the 95th percentile for the CPU usage for all ECS instances is 34%. For all ECS instances, 95% of the instance CPU usage values are less than 34%.

The 95th percentile statistics for various resources show the resource consumption level for the majority of cloud services.

Resource indicator descriptions

Product name	Indicator name	Statistical method	Statistical period	Statistical range
ECS	CPU usage	95th Percent	Real-time	All instances
ECS	Memory usage	95th Percent	Real-time	All instances
ECS	Disk usage	95th Percent	Real-time	All instances
ECS	Outgoing Internet bandwidth	95th Percent	Real-time	All instances
ApsaraDB for RDS	CPU usage	95th Percent	Real-time	All instances
ApsaraDB for RDS	IOPS usage	95th Percent	Real-time	All instances
ApsaraDB for RDS	Connection usage	95th Percent	Real-time	All instances
ApsaraDB for RDS	Disk usage	95th Percent	Real-time	All instances
OSS	Total outgoing Internet traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total PUT requests for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets

OSS	Total GET requests for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
CDN	Total traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All domain names
CDN	Peak network bandwidth	95th Percent	Real-time	All instances
CDN	Cache hit rate	95th Percent	Real-time	All instances
ApsaraDB for MongoDB	CPU usage	95th Percent	Real-time	All instances
ApsaraDB for MongoDB	Memory usage	95th Percent	Real-time	All instances
ApsaraDB for MongoDB	IOPS usage	95th Percent	Real-time	All instances
ApsaraDB for MongoDB	Connection usage	95th Percent	Real-time	All instances
ApsaraDB for MongoDB	Disk usage	95th Percent	Real-time	All instances
ApsaraDB for Memcache	Cache hit rate	95th Percent	Real-time	All instances
ApsaraDB for Memcache	Cache used	95th Percent	Real-time	All instances
Container Service	CPU usage	95th Percent	Real-time	All instances
Container Service	Memory usage	95th Percent	Real-time	All instances
Container Service	Outgoing Internet traffic	95th Percent	Real-time	All instances
Log Service	Total incoming network traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All projects

Log Service	Total outgoing network traffic for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All projects
Log Service	Total requests for current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All projects

Site monitoring

Statistics are collected on the number of all sites created under your account and the current alarm status for all sites.

Click the number of monitored sites to go to the **Site Monitoring** page. Click the corresponding number of alarm rules to go to the **Alarm Rules** page.

Customized monitoring

Statistics are collected on the number of all custom metric items created under your account and the current alarm status for all metric items.

Click the number of metric items to go to the **Customized monitoring** page. Click the corresponding number of alarm rules to go to the **Alarm Rules** page.

Dashboard

Dashboard overview

With the launch of the dashboard function in Cloud Monitor, Alibaba Cloud provides you a one-stop metric visualization solution. It not only allows you to view detailed metrics for troubleshooting, but also gives you the big picture for a glimpse into all services.

Application scenario

The dashboard function supports customized multi-dimensional query and display of cloud product

metric data. The following are some types of typical application scenarios.

Display the metric data trend of multiple instances

For example, if one of your applications is deployed on multiple ECS instances, you can add metric data of these ECS instances to the same metric chart to view the change trend of the metric data of multiple machines. For example, the CPU usage of multiple ECS instances can be displayed in the time sequence in one chart.

Display the data comparison of multiple metric items

For example, a metric chart can display multiple metrics of an ECS instance, including CPU usage, memory usage, and disk usage.

Display the ordering of machine resource consumption

For example, if you have 20 machines, you can view the CPU usage of them in descending order in a table. This allows you to quickly know about resource consumption, use resources more rationally, and avoid unnecessary cost.

Display the real-time metric data distribution of multiple instances

For example, the CPU usage distribution of an ECS instance group can be displayed in a heat map, so that you can compare the CPU usage of each machine. You can click a color block to view the metric data trend of the corresponding machine in a specified period of time.

Display the aggregated data of a specified metric item of multiple instances

For example, you can view the average aggregation value of the CPU usage of multiple ECS instances in one chart, so as to know about the overall CPU usage and check whether the resource usage of each instance is balanced.

Full screen display

The dashboard supports full screen display and automatic refresh of data. You can add various product metrics to a dashboard to display them on the dashboard in full screen mode.

Manage monitoring dashboards

You can create, modify, delete dashboards, and view charts on them.

View monitoring dashboards

Application scenario

The dashboard function of Cloud Monitor supports custom display of metric data. You can view metric data in a monitoring dashboard across products and instances, and display instances of different products in a centralized manner.

Note:

Cloud Monitor initializes ECS monitoring dashboards for you and displays ECS metric data.

Data of one hour, three hours, and six hours can be automatically refreshed. Data of more than six hours cannot be automatically refreshed.

Monitoring dashboard parameter description

Select the time range: You can click the timeframe selection button at the top of the **monitoring dashboard** page to quickly select the timeframe for displaying metric data on the dashboard. The selected time range applies to all charts of the monitoring dashboard.

Automatic refresh: When you click the **Automatic refresh** button, the automatic refresh function is enabled, then you can select the time range of “one hour”, “three hours”, or “six hours” to refresh data every minute.

The unit of metric items is displayed in a bracket in the chart name.

Metric values of all charts for the same time frame are displayed as your move your mouse cursor.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

By default, the ECS global monitoring dashboard initialized by Cloud Monitor is displayed.

Click the monitoring dashboard name and select another monitoring dashboard from the

drop-down list.

Click **Full screen** in the top-right corner of the page to view the monitoring dashboard in full screen.

Create a monitoring dashboard

Application scenario

If your business is complicated, and the default ECS monitoring dashboards cannot satisfy your monitoring visualization requirements, you can create a new monitoring dashboard and customize the charts to be displayed.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

In the top-right corner of the page, click **Add View Group**.

Enter the name of the monitoring dashboard, and click **Create** to complete the creation.

The page is automatically redirected to the new monitoring dashboard page where you can add various metric charts as you like.

Switch monitoring dashboards

Application scenario

If you create multiple monitoring dashboards, you can view the monitoring charts of different dashboards by switching monitoring dashboards.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

Click the name of a monitoring dashboard in the top-left corner of the page.

All monitoring dashboards created by you are displayed in a drop-down list. You can switch to another dashboard by selecting the name of that dashboard.

Delete a monitoring dashboard

Application scenario

You can delete a monitoring dashboard if you do not need it as your business changes.

Note:

When you delete a monitoring dashboard, all metric charts added to the dashboard will all be deleted.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

In the top-right corner of the page, click the **Delete View Group** button to delete the dashboard.

Modify a monitoring dashboard

Application scenario

You can modify a monitoring dashboard if you need to change the name of it as the content of the monitoring dashboard changes.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

Hover your mouse over the name of monitoring dashboard, and the **Change name** option is

displayed on the right side. Click **Change name** to make it editable so that you can modify the name of the monitoring dashboard.

Add cloud product metrics

Application scenario

Cloud Monitor initializes the ECS monitoring dashboard of the user dimension. You can use the **Add cloud product metrics** function to view ECS data of other dimensions or other cloud product metric data.

Note:

By default, Cloud Monitor initializes the ECS monitoring dashboard for you. Seven metric charts are displayed, showing the CPU usage, inbound network speed, outbound network speed, system disk BPS, system disk IOPS, inbound network traffic, and outbound network traffic respectively.

Limit of line chart view: A line chart can display 10 lines at most.

Limit of area chart view: An area chart can display 10 areas at most.

Table data limit: The ordered results can be displayed for a maximum of 1,000 data entries.

Limit on heat map view: One heat map can display a maximum of 1,000 color blocks.

Parameter description

Product selection: Choose to view metric data of a specified cloud product.

Metric item: Name of a metric that you need to view, such as outbound network traffic and CPU usage.

Statistical method: Common statistical methods for metric items including maximum value, minimum value, and average value. That is, how metric data is aggregated within the statistical period.

Filter: It is similar to the SQL Where statements and is used to filter metric data source that meets the criteria.

Group By: It is similar to SQL Group By and is used to group metric data that have been filtered by defined dimensions.

User dimension: Group and aggregate metric data on the user account level. For example, if you want to view the average value of the overall memory usage of ECS instances A, B, and C, select **Memory usage** and **Average value** from metric items, select metric items A, B, and C as filter criteria, and set **Group By** to **User dimension**. User dimension is used to view the overall resource usage of multiple instances.

Instance dimension: Group and aggregate metric data on the instance level. For example, if you want to view the average value of the memory usage of an ECS instance, select **Memory usage** and **Average value** from metric items, select this instance as filter criteria, and set **Group By** to **Instance dimension**. Instance dimension is used to view the resource usage of a single instance. If you need to view the monitoring status of multiple instances simultaneously, select multiple instances as filter criteria, and set **Group By** to **Instance dimension**.

Chart views: A view can be displayed in line chart, area chart, heat map, pie chart and table.

Line chart: This chart displays metric data by time sequence. Multiple metric items can be added.

Area chart: It displays metric data by time sequence. Multiple metric items can be added.

Heat map: It displays the real-time data of metric items. It is used to display distribution and comparison of real-time metric data of a specific metric item of multiple instances. For example, a heat map can display the distribution of the CPU usage of multiple instances. Only one metric item can be added.

Pie chart: This chart displays the real-time metric data, and is usually used for data comparison. Multiple metric items can be added.

Table: It displays metric item value in descending order. For example, a table can display the CPU usage of all machines in an ECS group in descending order. Only one metric item can be added.

Operation procedure

Log on to the Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

Click the **Add cloud product metrics** button in the top-right corner of a monitoring dashboard to access the **Add** page.

Select the cloud product to view and the region of the instance.

a. Select the product instance.

b. Select the region of the instance.

Define the chart name and chart type.

a. Define the chart name. The default chart name generated is “product name + region”.

b. Select the chart type.

Select the type of metric data to view and the mode of viewing metric data.

a. Select the metric item to view.

b. Select the way metric data is aggregated, for example, by maximum value, minimum value or average value.

c. Select filter criteria.

d. Select the dimension for **Group By**.

Click the **Add** button and repeat Step 6 if you need to add more metric items.

Click **Publish** to generate a chart in Monitor Dashboard.

Drag the right border, bottom border or bottom right corner of a chart to resize its height and width (if needed).

Add business metric monitoring

Application scenario

By upgrading from custom monitoring to business metric monitoring, you can use the **Add Business Metric Monitoring** function on the data submitted through APIs or SDKs to Cloud Monitor for data processing and display in Dashboard.

With **Business Metric Monitoring**, metric data can be aggregated by time or space dimension. The time dimension can support the granularity of data aggregation down to a minimum of 1 minute. The space dimension controls the aggregation views with the **Group By** parameter.

Note:

When a chart is added, the data submitted in the last 60 minutes will be read. Therefore, if your data is submitted every other 60 minutes and more, no data will be shown during a preview.

Limit on line chart view: 1 line chart can display up to 15 lines.

Limit on area chart view: 1 area chart may display up to 15 areas.

Table data limit: The ordered results can be displayed for a maximum of 1,000 data entries.

Limit on heat map view: 1 heat map can display a maximum of 1,000 color blocks.

By default, metric data is aggregated at a 1-minute granularity. If your data is submitted once within less than 1 minute, when performing a query, you will only be able to get data submitted at a minimum granularity of 1 minute.

Parameter description

Chart title: the title of metric chart, displaying the name of metric item by default.

Metric name (required): you can customize name according to the meaning of a metric. It is a parameter for follow-up data query via APIs.

Metric item (required): the name of metric item for which data is submitted via APIs/SDKs.

Unit: the unit that is chosen according to the meaning of your metric.

Filter (optional): equivalent to the Where statement in SQL. If the filtering criteria is left blank, it means to process all the data.

Group By: equivalent to the Group By statement in SQL. The function can aggregate and group metric data by the space or other specified dimension. If no dimension is chosen for Group By, all the metric data will be aggregated using the aggregation methods.

Aggregation: aggregate the metric data within the aggregation period using the specific method. There are three aggregation methods available, including maximum, minimum and average values.

Chart views: a view can be displayed in line chart, area chart, heat map, pie chart and table.

Line chart: this chart displays metric data by time sequence.

Area chart: this chart displays metric data by time sequence.

Heat map: this map displays the real-time metric data, and is usually used to display distribution and comparison of metric data that is grouped by dimension and aggregated.

Pie chart: this chart displays the real-time metric data, and is usually used for data comparison.

Table: this table displays the real-time metric data.

Operation procedure

Log on to Cloud Monitor console.

Click the **Dashboard** option in the left menu to access the **Dashboard** page.

Click the **Add business metrics monitoring** button in the upper right corner of Monitor Dashboard.

Define the **Chart name**, **Metric name** and **Chart type**.

Choose the metric data you want to view and then define the processing method.

a. Select metric item and unit.

b. If you only want to view part of the data, select a filtering field.

c. If you want to aggregate the data grouped by dimension, choose the corresponding field in **Group By**.

d. Choose an aggregation method.

Click **Publish** to generate a chart in Monitor Dashboard.

Drag the right border, bottom border or bottom right corner of a chart to resize its height and width (if needed).

Best practices

This chapter describes how to use ECS instance groups to manage multiple ECS instances and use ECS instance groups in a dashboard to quickly create metric charts for each instance group.

How to use ECS instance groups

Log on to Cloud Monitor console.

Go to the ECS monitoring page.

Click **Create an instance group** at the top of the instance list.

Enter the group information and add instances to the group.

How to use ECS instance groups in a dashboard

Using ECS instance groups in a dashboard allows you to quickly add monitoring information so as to view the monitoring details of each instance in the group.

Log on to Cloud Monitor Dashboard.

Click **Add cloud product monitoring**.

Select **ECS group** from **Filter** and select **Instance dimensions** from **Group By** to add instances to a specified group and display the monitoring information of each instance in the group.

Click **Release** to add monitoring charts.

Glossary

These terminologies are the key concepts of Alibaba Cloud Monitor.

Metric item

You can set up or use the metric data type defaulted by the system. For example, **Http monitoring**, which belongs to site monitoring, has two items by default, namely, **http.responseTime** and **http.status**. The metric items of ECS include **CPU usage**, **Memory usage**, etc.

Metric point

One instance of metric item. For example, the http monitoring in connection with site, www.aliyun.com, actually includes two metric points which are **http.response** and **http.status**. There are 11 metric items concerning ECS Compute Clouds. Therefore, one Compute Cloud has 11 metric points by default.

Dimension

Locate the dimension of the metric data’ s position. In the example of the metric item **disk IO**, the unique monitoring position can be located via two dimensions, namely, instance and disk name. Currently in customized monitoring, dimension is represented by **Field information**.

Rule

Rule is a condition. For example, “the usage of CPU>=50%” is one rule. It is also a rule that 7 out of 10 ECS servers are available. (“The percentage of the available servers>=70%.”)

Event

In this version, **Event** is not shown and presented to the users. One event happens when the rules and conditions are fulfilled at one metric point. For example, when the usage of CPU reaches 60%, which fulfills the condition of the rule that “the usage of CPU>=50%”, one event occurs.

When many events meet the condition of one rule, a new event occurs. For example, there are two probe points of the site monitoring. But only one probe point detects the unavailability of target site. It does not meet the rule of “unavailability=2”, which will not lead to an “unavailable double-detection” event. Therefore, no alarm will be triggered. Only when two probe points detect the unavailability of one site, which will result in an “unavailable double-detection” event, the alarm will be triggered.

Event Level

In this version, **Event Level** is not shown and presented to the users. The classification can be done based on the degree of severity, that is, the methods of alarm from different categories are different.

There are two ways of classification by means of known and unknown approaches. With known approaches, the result can be achieved automatically. If using the unknown approach, there will be a need for manual handling.

Alarm

The event will trigger one **notifying gesture** informing the alarm contact and service in a specific form.

Alarm contact

The receiver of the alarm, including cellphone, TradeManager (Taobao) and emails.

Alarm group

One group of alarm contact may contain one or more than one **alarm contact**. During the alarm setup, the alarm notifications can be sent through **alarm contact group**. The alarm information corresponding to each metric point will be sent to the alarm group members when the threshold is exceeded according to the preset alarm methods.

The methods of alarm

Methods for notifying the users of exceptions, including text messages, TradeManager, emails, etc.

Cloud service monitoring

Overview

Cloud Service Monitoring is a service that Alibaba Cloud provides for users to monitor the indicators of various cloud products. After buying an instance of a related product, you have access to the relevant monitoring services.

At present, the following products are supported in Cloud Monitor. Click a product name to view the details.

- ECS
- RDS
- Server Load Balancer
- OSS
- EIP
- ApsaraDB for Memcache
- ApsaraDB for MongoDB
- ApsaraDB for Redis
- CDN
- Message Service
- Log Service
- Container Service

ECS Monitoring

Overview

Cloud Monitor monitors CPU usage, memory usage, disk usage, and other performance indicators for ECS, as well as the status of specified processes. In addition, it allows you to set alarm rules for ECS metric items.

Monitoring service

ECS metric indictors are divided into basic metric indicators and OS-level metric indicators. Basic

metric indicators are derived from the metric data directly collected by Alibaba Cloud. After buying an instance, you can log on to the console and view metric indicators without any additional operations. OS-level metric indicators require you to install plugins in the VM to collect relevant metric data.

Plugin installation guide

On the Cloud Monitor console, you can automatically install plugins. Or you can log on to the machine and install plugins manually.

Console plugin installation

Go to the ECS Monitoring Page.

Click the **Click to Install** button in the ECS instance list. Or after selecting instances, click the **Install ECS Monitoring** button at the bottom of the list.

Manual plugin installation

To learn how to manually install, uninstall, and view the status of plugins, refer to the Agent Operations Guide.

Metric item descriptions

ECS basic metric indicators

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
CPU usage	The percentage of ECS computing resources currently in use by programs	User and instance	Percentage	1 minute
Average rate of Internet inbound traffic	Incoming bits per second to the instance’ s public network card	User and instance	bps	1 minute
Average rate of intranet inbound traffic	Incoming bits per second to the instance’ s private network card	User and instance	bps	1 minute
Average rate of	Outgoing bits	User and	bps	1 minute

Internet outbound traffic	per second from the instance’ s public network card (the ECS public network outgoing bandwidth). This indicator is used for billing.	instance		
Average rate of intranet outbound traffic	Outgoing bits per second from the instance’ s private network card	User and instance	bps	1 minute
Total system disk read BPS	The space on the system disk read per second	User and instance	bps	1 minute
Total system disk write BPS	The space on the system disk written per second	User and instance	bps	1 minute
System disk read IOPS	The system disk reading speed	User and instance	Count/Second	1 minute
System disk write IOPS	The system disk writing speed	User and instance	Count/Second	1 minute
Internet inbound traffic	The volume of inbound Internet traffic to the ECS instance within the statistical period	User and instance	Bytes	1 minute
Intranet inbound traffic	The volume of inbound intranet traffic to the ECS instance within the statistical period	User and instance	Bytes	1 minute
Internet outbound traffic	The volume of outbound Internet traffic from the ECS instance within the statistical period	User and instance	Bytes	1 minute
Intranet outbound	The volume of outbound	User and instance	Bytes	1 minute

traffic	intranet traffic from the ECS instance within the statistical period			

After installing plugins, you can view the following metric indicators.

Metric item	Meaning	Dimension	Units	Minimum monitoring granularity
Disk IO read	The disk’s reading speed	User, instance, and disk	bps	1 minute
Disk IO write	The disk’s writing speed	User, instance, and disk	bps	1 minute
Disk usage	The percentage of the system’s virtual disk in use	User, instance, and disk	Percentage	1 minute
Average load	This is used in Linux; a server’s average load	User, instance, period		1 minute
Memory usage	The percentage of the application’s memory in use	User and instance	Percentage	1 minute
TCP connection count	Total number of TCP connections established by the server	User, instance, and status	Count	1 minute
System process count	Total number of processes running on the server	User and instance	Count	1 minute
Process count	Processes of interest in the running status will be counted when you add process monitoring.	User, instance, process	Count	1 minute

ECS group management

The ECS group function allows you to manage ECS instances by groups. If there are multiple ECS

instances, you can divide different ECS instances into different groups. ECS instances on a single machine can be divided into different groups. You can group ECS instances as needed. For instance, they can be grouped according to different applications.

Considerations

Instance group names must be unique.

Instance group names cannot be modified.

Create an instance group

Log on to **Cloud Monitor console**.

Go to the **ECS** page under **Cloud Service Monitoring**.

Click **New group of instances** at the top of the instance list.

Enter **Group name**, select the instances, and click **OK**.

Query an instance group

Log on to **Cloud Monitor console**.

Go to the **ECS** page under **Cloud Service Monitoring**.

From the instance group name drop-down list, select the instance group to view.

Delete an instance group

Log on to **Cloud Monitor console**.

Go to the **ECS** page under **Cloud Service Monitoring**.

From the instance group name drop-down list, select the instance group you want to delete.

Click the **Delete this group** button next to the instance group name, and click **Confirm to**

delete to delete the instance group.

Modify an instance group

Log on to Cloud Monitor console.

Go to the **ECS** page under **Cloud Service Monitoring**.

From the instance group name drop-down list, select the instance group you want to modify.

Click the **Edit instances within a group** button next to the instance group name to add or delete instances to or from the instance group.

Process monitoring

Process monitoring can monitor the status of specified processes.

Considerations

When adding a process, you do not need to enter its absolute path. Just enter a keyword related to the process to count processes that contain this keyword.

Add a process listener

Log on to Cloud Monitor console.

Go to the **ECS** page under **Cloud Service Monitoring**.

Click the instance name to go to the **Instance monitoring details** page.

On the **Process Count** metric chart, click **Add Process Monitor**. In the pop-up box, enter the name of the process you want to monitor.

Delete a process listener

Log on to Cloud Monitor console.

Go to the **ECS** page under **Cloud Service Monitoring**.

Click the instance name to go to the **Instance monitoring details** page.

On the **Process Count** metric chart, click **Add Process Monitor**. The pop-up box will show a list of previously added processes. Select the corresponding process name from the list and then click **Delete**.

View metric data

Log on to Cloud Monitor console.

Go to the **ECS** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Monitoring Chart** in the **Actions** column to access the **Instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by ECS.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **maximum**, **minimum**, and **sum** in **Statistical method**.

Average: the average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: the maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: the minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: the sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is the **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to Cloud Monitor console.

Go to the **ECS** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm rules** page.

Click **Create Alarm Rule** at the bottom of the **Alarm rules** page to create an alarm rule based on the entered parameters.

RDS monitoring

Overview

Cloud Monitor displays the RDS operation status based on four metric items: **Disk usage**, **IOPS usage**,

Connection usage, and **CPU usage**. After you buy RDS products, Cloud Monitor will automatically start monitoring the above four items without any additional operations.

Note:

RDS only provides monitoring and alarm services for primary and read-only instances.

By default, Cloud Monitor will create alarm rules for each primary instance and read-only instance. These rules set up the thresholds of **CPU usage**, **Connection usage**, **IOPS usage**, and **Disk usage** all to 80%. When metric data exceeds any of the above thresholds, a text message and email will be sent to the contact person for the Alibaba Cloud account.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
Disk usage	The percentage of disk space used by the RDS instance	Instance	Percentage	5 minutes
IOPS usage	The percentage of IO requests per second used by the RDS instance	Instance	Percentage	5 minutes
Connection usage	The connection count is the number of connections that application programs can establish with the RDS instance. Connection usage is the percentage of these connections currently in use.	Instance	Percentage	5 minutes
CPU usage	The percentage of CPU capacity consumed by the RDS instance (CPU	Instance	Percentage	5 minutes

	performance is determined by the database memory size.)			
Memory usage	The percentage of the RDS instance’ s memory in use. Currently, only MySQL databases support instance memory usage.	Instance	Percentage	5 minutes
Incoming network traffic	The instance’ s input traffic per second	Instance	Bps	5 minutes
Outgoing network traffic	The instance’ s output traffic per second	Instance	Bps	5 minutes

Note: The incoming and outgoing network traffic indicators only support MySQL and SQLServer databases.

View metric data

Log on to Cloud Monitor console.

Go to the **RDS** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by RDS.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the

alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceed the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

> **Average**: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.
>
> **Maximum**: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.
>
> **Minimum**: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.
>
> **Sum**: The sum of metric data within the statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

1. Log on to Cloud Monitor console.
2. Go to the **RDS** instance list under **Cloud Service Monitoring**.
3. Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm rules** page.

4. Click **Create Alarm Rule** at the bottom of the **Alarm rules** page to create an alarm rule based on the entered parameters.

Server Load Balancer monitoring

Cloud Monitor displays the status of Server Load Balancer based on seven metric items, including inbound traffic and outbound traffic. This helps you to monitor the operational status of instances and allows you to configure alarm rules for these metric items. After you create a Server Load Balancer instance, Cloud Monitor will automatically collect data on the metric items listed above.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
Inbound traffic	Traffic consumed by access to the Server Load Balancer from the Internet	Instance	Bps	1 minute
Outbound traffic	Traffic consumed by access to the Internet from the Server Load Balancer	Instance	Bps	1 minute
Incoming packet count	Number of request packets that the Server Load Balancer receives per second	Instance	Count per second	1 minute
Outgoing packet count	Number of request packets that the Server Load Balancer sends per second	Instance	Count per second	1 minute
New connection count	The number of first-time SYN_SENT statuses for TCP three-way	Instance	Count	1 minute

	handshakes in a statistical period			
Active connection count	The number of connections in the ESTABLISHED status in the current statistical period	Instance	Count	1 minute
Inactive connection count	The number of all TCP connections except connections in the ESTABLISHED status	Instance	Count	1 minute

Note: New connection count, active connection count, and inactive connection count all indicate the TCP connection requests from clients to the Server Load Balancer.

View metric data

1. Log on to Cloud Monitor console.
2. Go to the **Server Load Balancer** instance list under **Cloud Service Monitoring**.
3. Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.
4. Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: the monitoring indicators provided by Server Load Balancer.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: the average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: the maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: the minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: the sum of metric data within the statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to Cloud Monitor console.

Go to the **Server Load Balancer** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm rules** page.

Click **Create Alarm Rule** at the bottom of the **Alarm rules** page to create an alarm rule based on the entered parameters.

OSS monitoring

The OSS monitoring service provides you with metric data which describes basic system operation status, performance, and metering. It also provides a custom alarm service to help you track requests, analyze usage, collect statistics on business trends, and promptly discover and diagnose system problems.

Monitoring service

Metric item descriptions

OSS metric indicators are classified into groups including basic service indicators, performance indicators, and metering indicators. For details, refer to OSS Metric Indicator Reference Manual.

Note:

In order to maintain consistency with billing policies, the collection and presentation of metering indicators have the following special features:

- Metering indicator data are output by the hour. This means that resource metering information for each hour is combined into a single value that represents the overall metering condition for the hour.
- Metering indicator data have an output delay of nearly 30 minutes.
- The data time of metering indicator data refers to the start time of the relevant statistical period.
- The cutoff time of metering data acquisition is the end time of the last metering data statistical period of the current month. If no metering data are produced in the current month, the metering data acquisition cutoff is 00:00 on the first day of the current month.

  A maximum amount of metering indicator data is pushed for presentation. For precise metering data, refer to Consumption Records.

  For example, assume that you only use PutObject requests to upload data and perform this operation at an average of 10 times per minute. Then, in the hour between 2016-05-10 08:00:00 and 2016-05-10 09:00:00, the metering data value for your PUT requests will be 600 times (10*60 minutes), the data time will be 2016-05-10 08:00:00, this piece of data will be output at around 2016-05-10 09:30:00. If this piece of data is the last one since 2016-05-01 00:00:00, the metering data acquisition cutoff for the current month is 2016-05-10 09:00:00. If in May 2016, you have not produced any metering data, the metering data acquisition cutoff will be 2016-05-01 00:00:00.

Alarm service

Note:

OSS buckets must be globally unique. After deleting a bucket, if you create another bucket with the same name, the monitoring and alarms rules set for the deleted bucket will be applied to the new bucket with the same name.

Besides metering indicators and statistical indicators, alarms rules can be configured for other metric indicators and added to alarm monitoring. Also, multiple alarm rules may be configured for a single metric indicator.

User guide

For information about the alarm service, refer to Alarm Service Overview.

For instructions on how to use the OSS alarm service, refer to OSS Alarm Service User Guide.

CDN monitoring

Overview

Cloud Monitor displays the usage of CDN based on nine metric items, including **Queries Per Second (QPS)**, **Bytes Per Second (BPS)**, and **bytes hit rate**. After you add a CDN domain, Cloud Monitor automatically monitors the domain.

You can access the **CDN monitoring** page to view the metric data. You can configure alarm rules for metric items so that an alarm is generated when a data exception occurs.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
QPS	Total access requests in a specific time interval/Time interval	Instance	Quantity	5 minutes

Peak bandwidth BPS	The maximum network traffic per unit time	Instance	Bps	5 minutes
Hit rate	The probability that request bytes hit the cache in a specific time interval (Bytes = Number of requests x Traffic). The bytes hit rate directly reflects the back-to-source traffic.	Instance	Percentage	5 minutes
Internet outbound traffic	CDN Internet outbound traffic	Instance	Bytes	5 minutes
HTTP Return Code 4xx percentage	Percentage of HTTP Return Code 4xx in a specific time interval	Instance	Percentage	5 minutes
HTTP Return Code 5xx percentage	Percentage of HTTP Return Code 5xx in a specific time interval	Instance	Percentage	5 minutes

View metric data

1. Log on to Cloud Monitor console.
2. Go to the **CDN** instance list under **Cloud Service Monitoring**.
3. Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.
4. Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by CDN.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the

alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: the average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: the maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: the minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: the sum of metric data within the statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent.No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

1. Log on to Cloud Monitor console.
2. Go to the **CDN** instance list under **Cloud Service Monitoring**.
3. Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm Rules** page.
4. Click **Create Alarm Rule** at the bottom of the alarm rules page to create an alarm rule based

on the entered parameters.

EIP monitoring

Overview

Cloud Monitor provides four EIP metric items (**outbound traffic**, **inbound traffic**, **outgoing packet count**, and **incoming packet count**), to help you monitor the service status. You can set alarm rules for these metric items. After you buy the EIP service, Cloud Monitor will automatically collect data on the four metric items listed above.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
Inbound traffic	The volume of traffic per minute that passes through the EIP to an ECS instance	Instance	Bytes	1 minute
Outbound traffic	The volume of traffic per minute that passes through the EIP from an ECS instance	Instance	Bytes	1 minute
Incoming packet count	The number of packets per minute that pass through the EIP to an ECS instance	Instance	Count	1 minute
Outgoing packet count	The number of packets per minute that pass through the EIP from an ECS instance	Instance	Count	1 minute

View metric data

Log on to Cloud Monitor console.

Go to the **EIP** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by EIP.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceed the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within the statistical cycle. When the sum of the metric

data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to Cloud Monitor console.

Go to the **EIP** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the **Instance' s alarm rules** page.

Click **Create Alarm Rule** at the bottom of the **Alarm rules** page to create an alarm rule based on the entered parameters.

ApsaraDB for Memcache monitoring

Overview

Cloud Monitor provides seven ApsaraDB for Memcache metric items, including **used cache** and **read hit rate**, to help you monitor the status of the service. You can set alarm rules for these metric items. After you buy the Memcache service, Cloud Monitor will automatically collect data on the metric items listed above.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
Used cache	Amount of cache in use	Instance	Bytes	1 minute
Read hit rate	The probability that key values (KVs) are read successfully	Instance	Percentage	1 minute
QPS	Total times KVs are read per second	Instance	Count	1 minute
Record count	Total number of KVs in the current measurement period	Instance	Count	1 minute
Cache inbound bandwidth	Traffic generated during access to the cache	Instance	Bps	1 minute
Cache outbound bandwidth	Traffic generated during read operations on the cache	Instance	Bps	1 minute
Eviction	Number of KVs evicted per second	Instance	KVs per second	1 minute

Note:

- Metric data are saved for up to 31 days.
- You can view metric data for up to 14 consecutive days.

View metric data

Log on to **Cloud Monitor console**.

Go to the **ApsaraDB for Memcache Monitoring** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation**

column to access the **Instance monitoring details** page and view the various indicators.

Click a **Time Range** shortcut on the top of the page or use the specific selection function.

Click the **Zoom In** button in the top-right corner of the metric chart to enlarge the graph.

Alarm service

Cloud Monitor provides alarm services for all Memcache metric items. After setting an alarm rule for an important metric item, you will receive an alarm notification if the metric data exceeds the set threshold value. This allows for rapid troubleshooting and reduces the probability of faults.

Parameter description

Metric items: The monitoring indicators provided by ECS for Redis.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Consecutive times: Refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an individual alarm rule

Log on to Cloud Monitor console.

Go to the **ApsaraDB for Memcache Monitoring** instance list under **Cloud Service Monitoring** .

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.

Click the **Bell** button in the top-right corner of the metric chart to set an alarm for the corresponding metric item for this instance.

Batch set alarm rules

Log on to Cloud Monitor console.

Go to the **ApsaraDB for Memcache Monitoring** instance list under **Cloud Service Monitoring** .

Select the appropriate instance on the instance list page. Then, click **Set Alarm Rules** at the bottom of the page to add multiple alarm rules.

ApsaraDB for Redis monitoring

Overview

Cloud Monitor displays the status and usage of ApsaraDB for Redis based on various metric items, including **capacity usage** and **connection usage**. After you create a Redis instance, Cloud Monitor automatically starts monitoring the instance. You can access the **Cloud Monitor Redis** page to view the metric data. You can configure alarm rules for metric items so that an alarm is generated when a data exception occurs.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
Capacity used	The current Redis capacity used	Instance	Bytes	1 minute
Used connection count	The total number of client connections	Instance	Count	1 minute
Write speed	Network traffic generated per second during write operations on ApsaraDB for Redis	Instance	Bps	1 minute
Read speed	The network traffic generated per second during read operations on ApsaraDB for Redis	Instance	Bps	1 minute
Failed operation count	Number of failed operations on ApsaraDB for Redis	Instance	Count	1 minute
Capacity usage	Percentage of ApsaraDB for Redis capacity in use	Instance	Percentage	1 minute
Connection usage	Established connections as	Instance	Percentage	1 minute

	a percentage of total connections			
Write bandwidth usage	Percentage of bandwidth consumed by write operations	Instance	Percentage	1 minute
Read bandwidth usage	Percentage of bandwidth consumed by read operations	Instance	Percentage	1 minute

View metric data

Log on to Cloud Monitor console.

Go to the **ApsaraDB for Redis** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by ECS for Redis.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value

of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to **Cloud Monitor console**.

Go to the **ApsaraDB for Redis** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm Rules** page.

Click C**reate Alarm Rule** at the bottom of the **Alarm Rules** page to create an alarm rule based on the entered parameters.

ApsaraDB for MongoDB

Overview

Cloud Monitor provides many metric items for ApsaraDB for MongoDB, including **CPU usage** and **Memory usage**, to help you monitor the status of the service. You can set alarm rules for these metric items. After you buy the MongoDB service, Cloud Monitor will automatically collect data on the metric items listed above.

Monitoring service

Metric items

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
CPU usage	The percentage of the instance’s CPU in use	User, instance, and master/backup	Percentage	5 minutes
Memory usage	The percentage of the instance’s memory in use	User, instance, and master/backup	Percentage	5 minutes
Disk usage	The percentage of the instance’s disk in use	User, instance, and master/backup	Percentage	5 minutes
IOPS usage	The percentage of the instance’s IOPS in use	User, instance, and master/backup	Percentage	5 minutes
Connection usage	The connection count is the number of connections that application programs can establish with the MongoDB instance. Connection usage is the percentage of these connections currently in use.	User, instance, and master/backup	Percentage	5 minutes

Average SQL queries per second	The MongoDB instance’ s average number of SQL queries per second	User, instance, and master/backup	Count	5 minutes
Connections in use	The current number of connections that applications have established with the MongoDB instance.	User, instance, and master/backup	Count	5 minutes
Disk space used by instance	The disk space used by the instance itself	User, instance, and master/backup	Bytes	5 minutes
Disk space used by data	The disk space used by data	User, instance, and master/backup	Bytes	5 minutes
Disk space used by logs	The disk space used by logs	User, instance, and master/backup	Bytes	5 minutes
Intranet inbound traffic	The instance’ s inbound intranet traffic	User, instance, and master/backup	Bytes	5 minutes
Intranet outbound traffic	The instance’ s outbound intranet traffic	User, instance, and master/backup	Bytes	5 minutes
Request Qty	The total number of requests sent to the server	User, instance, and master/backup	Count	5 minutes
Insert operation count	The total number of insert commands received since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes
Query operation count	The total number of query commands received since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes

Update operation count	The total number of update commands received since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes
Delete operation count	The total number of delete operations executed since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes
Getmore operation count	The total number of getmore operations executed since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes
Command operation count	The total number of commands sent to the database since the last time MongoDB was started.	User, instance, and master/backup	Count	5 minutes

Note:

- Metric data are saved for up to 31 days.
- You can view metric data for up to 14 consecutive days.

View metric data

Log on to Cloud Monitor console.

Go to the **ApsaraDB for MongoDB** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page and view the various indicators.

Click the **Time Range** shortcut on the top of the page or use the specific selection function.

Up to 14 consecutive days of metric data can be viewed.

Click the **Zoom In** button in the top-right corner of the metric chart to enlarge the graph.

Alarm service

Parameter description

Metric items: The monitoring indicators provided by ECS for Redis.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Consecutive times: Refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU

usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an individual alarm rule

Log on to Cloud Monitor console.

Go to the **ApsaraDB for Memcache Monitoring** instance list under **Cloud Service Monitoring** .

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.

Click the **Bell** button in the top-right corner of the metric chart to set an alarm for the corresponding metric item for this instance.

Batch set alarm rules

Log on to Cloud Monitor console.

Go to the **ApsaraDB for Memcache Monitoring** instance list under **Cloud Service Monitoring** .

Select the appropriate instance on the **Instance list** page. Then, click **Set Alarm Rules** at the bottom of the page to add multiple alarm rules.

Message Service monitoring

Overview

Cloud Monitor displays the usage of Message Service queues based on the following three metric items: **DelayMessage**, **InactiveMessages**, and **ActiveMessages**. After you create a message queue for

the Message Service, Cloud Monitor automatically starts monitoring the queue. You can access the Cloud Monitor **Message Service** page to view the metric data. You can configure alarm rules for metric items so that an alarm is generated when a data exception occurs.

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
ActiveMessages	Total number of active messages in the queue	userId, region, bid, and queue	Count	5 minutes
InactiveMessages	Total number of inactive messages in the queue	userId, region, bid, and queue	Count	5 minutes
DelayMessage	Total number of delayed messages in the queue	userId, region, bid, and queue	Count	5 minutes

View metric data

Log on to Cloud Monitor console.

Go to the **Message Service** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation** column to access the **Instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by the Message Service.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the

alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: the sum of metric data within the statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to Cloud Monitor console.

Go to the **Message Service** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance' s **Alarm Rules** page.

Click **Create Alarm Rule** at the bottom of the alarm rules page to create an alarm rule based on the entered parameters.

ADS monitoring

Overview

Cloud Monitor displays the usage of ADS based on three metric items: **diskSize**, **diskUsed**, and **diskUsedPercent**. After you activate ADS, Cloud Monitor automatically starts monitoring the service. You can access the Cloud Monitor **ADS** page to view the metric data. You can configure alarm rules for metric items so that an alarm is generated when a data exception occurs.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
diskSize	Rated disk capacity	instanceId, tableSchema, and workerId	MB	1 minute
diskUsed	Disk capacity in use	instanceId, tableSchema, and workerId	MB	1 minute
diskUsedPercent	Percentage of disk space in use	instanceId, tableSchema, and workerId	Percentage	1 minute

View metric data

Log on to **Cloud Monitor console**.

Go to the **ADS** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation**

column to access the **Instance monitoring details** page.

Click the **Chart Size** button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by ADS.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a

5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Set an alarm rule

Log on to **Cloud Monitor console**.

Go to the **ADS** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance' s **Alarm Rules** page.

Click **Create Alarm Rule** at the bottom of the alarm rules page to create an alarm rule based on the entered parameters.

Log Service monitoring

Overview

Cloud Monitor displays the usage of the log service based on 11 metric items, including outbound traffic, inbound traffic, overall QPS, and log statistic methods. After you create a log service instance, Cloud Monitor automatically starts monitoring the service. You can access the Cloud Monitor **Log Service** page to view the metric data. You can configure alarm rules for metric items so that an alarm is generated when a data exception occurs.

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
LogInflowOutflow	Inbound traffic and outbound traffic per minute for the logStore	userId, Project, and Logstore	Bytes	1 minute

SumQPS	Total number of writes per minute to the logStore	userId, Project, and Logstore	Count	1 minute
LogMethodQPS	Number of writes per minute mapped to a specific method in the logStore	userId, Project, Logstore, and Method	Count	1 minute
LogCodeQPS	Number of writes per minute mapped to a specific status code in the logStore	userId, Project, Logstore, and Status	Count	1 minute
SuccessdByte	Number of successfully resolved bytes in the logStore	userId, Project, and Logstore	Bytes	10 minutes
SuccessdLines	Number of lines in successfully resolved logs in the logStore	userId, Project, and Logstore	Count	10 minutes
FailedLines	Number of lines in logs failed to be resolved in the logStore	userId, Project, and Logstore	Count	10 minutes
AlarmPV	Total number of ECS configuration errors in the logStore	userId, Project, and Logstore	Count	5 minutes
AlarmUv	Total number of ECS instances with incorrect configurations in the logStore	userId, Project, and Logstore	Count	5 minutes
AlarmIPCount	Number of errors incurred by a specific IP address in the logStore	userId, Project, Logstore, alarm_type, and source_ip	Count	5 minutes

View metric data

1. Log on to the CloudMonitor console.
2. Go to the “Log Service” instance list under “Cloud Service Monitoring”.
3. Click an instance name in the product instance list or click “Metric Chart” in the “Operation” column to access the instance monitoring details page.
4. Click the Chart Size button to switch to large chart display (optional).

Alarm service

Parameter description

Metric items: The monitoring indicators provided by the Log Service.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceed the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

> **Average**: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.
>
> **Maximum**: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.
>
> **Minimum**: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.
>
> **Sum**: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in

several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Note:

When you configure alarm rules, you can select a log method and a status code for QPS. If you do not select one, QPS will collect statistics on all log methods and status codes.

The method fields include **PostLogStoreLogs**, **GetLogtailConfig**, **PutData**, **GetCursorOrData**, **GetData**, **GetLogStoreHistogram**, **GetLogStoreLogs**, **ListLogStores**, and **ListLogStoreTopics**.

The status fields include 200, 400, 401, 403, 405, 500, and 502.

Set an alarm rule

Log on to **Cloud Monitor console**.

Go to the **Log Service** instance list under **Cloud Service Monitoring**.

Click **Alarm Rules** in instance list **Operations** to access the instance’ s **Alarm Rules** page.

Click **Create Alarm Rule** at the bottom of the **Alarm Rules** page to create an alarm rule based on the entered parameters.

Container Service monitoring

Overview

By monitoring seven indicators including Container Service CPU usage and memory usage, Cloud

Monitor informs you about Container Service usage. After you create a Container Service instance, Cloud Monitor automatically starts monitoring the service. You can access the Cloud Monitor **Container Service** page to view the metric data. You can configure alarm rules for metric items so that an alarm notification is generated in case of a data exception.

Monitoring service

Metric item descriptions

Metric item	Definition	Dimension	Units	Minimum monitoring granularity
containerCpuUtilization	The container CPU usage	User and container	Percentage	30 seconds
containerMemoryUtilization	The container memory usage	User and container	Percentage	30 seconds
containerMemoryAmount	The container memory usage amount	User and container	Bytes	30 seconds
containerInternetIn	The container’ s incoming traffic	User and container	Bytes	30 seconds
containerInternetOut	The container’ s outgoing traffic	User and container	Bytes	30 seconds
containerIORead	The container IO read speed	User and container	Bytes	30 seconds
containerIOWrite	The container IO write speed	User and container	Bytes	30 seconds

Note:

- Metric data are saved for up to 31 days.
- You can view metric data for up to 14 consecutive days.

View metric data

Log on to **Cloud Monitor console**.

Go to the **Container Service** instance list under **Cloud Service Monitoring**.

Click an instance name in the product instance list or click **Metric Chart** in the **Operation**

column to access the **Instance monitoring details** page and view the various indicators.

Click a **Time Range** shortcut on the top of the page or use the specific selection function. Up to 14 consecutive days of metric data can be viewed.

Click the **Zoom In** button in the top-right corner of the **Container Service Monitoring** page.

Alarm service

Set individual alarm rules: Click the **Bell** button in the top-right corner of the metric chart to set an alarm for the corresponding metric item for this instance.

Batch set alarm rules: Select the appropriate instance on the **Instance list** page. Then, click **Set Alarm Rules** at the bottom of the page to add multiple alarm rules.f the metric chart to enlarge the graph.

Quick Start

Custom Monitor

Custom monitoring Overview

Overview

Custom monitoring allows you to customize metric items and alarm rules. By using this feature, you can monitor concerned services and report collected monitoring data to Cloud Monitor, so that Cloud Monitor processes the data and generates alarms according to the result.

Note:

- Data can be stored for up to 30 days.
- The time span of queried data cannot exceed seven days.

Create custom metric items

You need to create custom metric items before reporting metric data through an interface based on the defined metric item field.

Note:

Currently, Cloud Monitor supports up to 10 custom metric items.

The metric data reporting service must be configured on Alibaba Cloud ECS.

Metric item names are not case sensitive. For example, if cpuUtilization is defined, defining CPUUtilization does not create a new metric item.

Parameter description

Metric item name: Metric data name a user reports, for example, **CPUUtilization**.

Metric data unit: It is not verified during data reporting and is only provided in order to facilitate the display or exchange of data. You can fill in the field based on actual conditions.

Reporting frequency: Metric data reporting cycle. The options are 1 minute, 5 minutes, and 15 minutes only.

Field information: It can be used to specify a unique metric item. For example, if the field information of the CPU metric item of ECS is an instance name, you must specify the instance name to locate a CPU message. If the field information of the ECS disk usage is an instance name and a mount point, you must specify both the instance name and the mount point for ECS disk usage to make sense.

Statistical period: You can notify Cloud Monitor of the frequency for aggregating the reported metric data.

Statistical method: It can be combined with the statistical period. If you select a 5 minute statistical period, then Cloud Monitor calculates the average, sum, maximum, and minimum values, and the sample count (how much data has been reported) of the data reported within a 5 minute period.

Operation procedure

Log on to Cloud Monitor console.

Go to the **Customized monitoring** page.

Click **Create metric items** in the top-right corner and enter related parameters.

Create alarm rules (optional)

Parameter description

Field: The value of the field defined when a metric item is created.

Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above statistical methods are needed for traffic-based indicators.

Trigger Alarm After Threshold Value Is Exceeded Several Times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Operation procedure

Log on to **Cloud Monitor console**.

Go to the **Customized monitoring** page.

Click **Alarm management** in the **Operation** column in the metric item list to access the page for creating metric item alarm rules.

Click **Alarm addition rule** at the bottom of the page to create alarm rules.

Upload metric data

You can use the API or SDK to upload metric data.

Note: The SDK supports Python Version 2.6 and Bash.

Upload data using the SDK

Parameter description

userid: The **Account ID** of a user.

Metric item name: The name filled in by the user when a metric item is created.

Metric item value: The metric data corresponding to a metric item.

Field information: The field information filled in by the user when a metric item is created and the value of the field information. This parameter is used to identify the dimension of data.

Procedure

Download the SDK.

Custom monitoring SDK (Python): cms_post.py

Custom monitoring SDK (Bash): cms_post.sh

Compile scripts.

a. In the user scripts, import cms_post and use the call cms_post method to push data to Cloud Monitor.

b. The post method transfers in four parameters, including **userid**, **metric item name**, **metric item value**, and **field information**. You need to add regular tasks only.

Regularly schedule scripts and upload data based on the upload cycle defined when metric items are created. You can use Crontab in Linux systems and quartz.net in Windows systems.

Supplemental Instructions: Add the corresponding interpreter at the beginning of your scripts. Generally the default interpreter is #!usr/bin/python. Add import cms_post in test.py. Then upload the metric data by calling cms_post.post(). Put the test.py file and the cms_post.py file in the same directory to avoid error during import.

Script example (Python+Linux environment)

```
#!/usr/bin/python
import cms_post

def get_mem_usage_percent():
try:
f = open('/proc/meminfo', 'r')
for line in f:
if line.startswith('MemTotal:'):
mem_total = int(line.split()[1])
```

```
elif line.startswith('MemFree:'):
mem_free = int(line.split()[1])
elif line.startswith('Buffers:'):
mem_buffer = int(line.split()[1])
elif line.startswith('Cached:'):
mem_cache = int(line.split()[1])
elif line.startswith('SwapTotal:'):
vmem_total = int(line.split()[1])
elif line.startswith('SwapFree:'):
vmem_free = int(line.split()[1])
else:
continue
f.close()
except:
return None
physical_percent = usage_percent(mem_total - (mem_free + mem_buffer + mem_cache), mem_total)
virtual_percent = 0
if vmem_total > 0:
virtual_percent = usage_percent((vmem_total - vmem_free), vmem_total)
return physical_percent
def usage_percent(use, total):
try:
ret = (float(use) / total) * 100
except ZeroDivisionError:
raise Exception("ERROR - zero division error")
return ret

MEMS_usage=get_mem_usage_percent()

if __name__ == '__main__':
cms_post.post("1058019241820815","MEMS_usage",MEMS_usage,"Percent","ecsinstanceId=i-28zdkoobp")
```

Upload data though the API

You can use the Cloud Monitor interface to upload your metric data.

Parameter description

MetricName: The metric item name you filled in when a metric item is created.

unit: The unit you filled in when a metric item is created.

dimensions: The field information you filled in when a metric item is created. Multiple dimensions are supported, which are separated by commas.

namespace: The parameter format is “ACS/CUSTOM/userId”. You can replace **userId** with your own account ID.

userId: Your Account ID.

timestamp: Data uploading time. Data can be uploaded either in long integer time format such as 1395556197448 or in ISO8601-based format using UTC time such as 2014-9-11T10:00:00Z. You must note that the corresponding Beijing time is 2014-09-11 18:00:00.

POST mode

You can submit multiple statistical data items at one time in a message body in JSON format. A sample message body is displayed as follows:

```
userId=123456&namespace=acs/custom/123456&metrics =
[{"metricName":"vm.cpu","timestamp":"1395556197448","value":80.0,"unit":"Percen
t","dimensions":{"instanceId":"vm_001"}}]
```

GET mode

You can submit multiple statistical data items at one time in a metrics field in JSON format.

```
http://open.cms.aliyun.com
/metrics/put?userId=123456&namespace=acs/custom/123456&metrics=[{"metricName":
"vm.cpu","timestamp":"1395556197448","value":80.0,"unit":"Percent","dimensions"
:{"instanceId":"vm_001"}},{"metricName":"vm.mem","timestamp":"1395556197448","v
alue":1280.0,"unit":"Megabytes","dimensions":{"instanceId":"vm_002"}}]
```

Response message

After receiving an HTTP request, Cloud Monitor directly returns an HTTP response whose status code is 200 if the request is processed successfully. The message body does not carry any content and you do not need to perform any operations based on the response. If the request failed to be processed, a message body in JSON format is returned, and meanwhile the status code of the HTTP response is not 200.

Error	Error description	HTTP status code
InternalServerError	Internal error or uncertain exceptions	500
InvalidParameterCombination	Parameter combination error	400
InvalidParameterValue	Parameter invalid or beyond the permitted range	400
MissingRequiredParameter	A required parameter is missing.	400

For example:

```
{"code":"InvalidParameterValue","msg":"the metricName is empty."}
```

Alarm rule

Alarm service overview

Overview

You can set alarm rules for probe points in site monitoring, instances in cloud service monitoring, and metric items in customized monitoring.

When you use the alarm function for the first time, you need to create an alarm contact, create an alarm contact group, and then set alarm rules for relevant services.

Site monitoring alarm rules

You can create alarm rules for probe points in site monitoring. The statistical cycle of alarm rules in site monitoring is the same as the detection cycle of probe points. That is, when the detection cycle of a probe point is five minutes, the statistical cycle of its alarm rule is also five minutes. The system monitors the data returned from the probe point every five minutes to check whether the actual value exceeds the threshold value.

Cloud service monitoring alarm rules

You can set alarm rules for instances in cloud service monitoring. Alarm rules can be set for metric items of each product.

Custom monitoring alarm rules

After creating a metric item, you can set alarm rules for the metric item settings, including response time, status code, and package loss rate of a probe point. The statistical cycle of an alarm rule is in consistent with that of the metric item.

The alarm service can be subscribed through SMS, email, TradeManager, or event. TradeManager can push alarm messages only through PC. If you have installed the Alibaba Cloud APP, you can receive

alarm notification from the Alibaba Cloud APP.

Note: The SMS quota for a new user is 1,000 by default. You can submit a ticket or contact Alibaba Cloud through TradeManager to apply for additional free alarm SMS quota.

Parameter description

Statistical cycle: The system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every one minute.

The statistical cycle refers to the interval time between two consecutive statistical operations, and the statistical method refers to the setting for exceeding threshold range. You can set **Average**, **Maximum**, **Minimum**, and **Sum** in **Statistical method**.

Field: Refers to the supplementary information of a dimension. Some indexes may have a dimension having a smaller granularity than instance, for example, the ECS disk usage. When setting alarm rules for an instance, you can select the disk information in the field.

Alarm After Threshold Value Exceeded for Several Times: Refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

Next, we will illustrate how calculations are done for various statistical methods when the CPU usage for ECS is over 80% in the case of a 15-minute statistical cycle.

Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. Only when the average value is over 80%, it exceeds the threshold.

Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold.

Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold.

Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The above

statistical methods are needed for traffic-based indexes.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80%for the second time within five minutes. An alarm is reported only if the CPU usage rate exceeds 80% for a third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is **Statistical cycle***(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

Alarm contact and alarm contact group

The contact and contact group information is a prerequisite for the alarm notification service. You need to create a contact and contact group and select a contact group for the alarm rule to receive the alarm notification.

Alarm contact management

You can manage the alarm contact function by creating, deleting or modifying the contact telephone, email, or other notification methods.

Create a contact

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click the **Create Contact** button on the right-top corner of the page, and complete the telephone, email, and other information.

A short message or email is sent to the mobile phone number or email address you fill in for verification purpose. This prevents that you cannot receive the alarm notification in time due to incorrect information.

Edit a contact

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click **Edit** in the **Operation** column in the contact list to edit the contact information.

Delete a contact

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click **Delete** in the **Operation** column in the contact list to delete the contact information.

After you delete a contact, no Cloud Monitor alarm notification is sent to the contact.

Alarm contact group management

An alarm group is a group of alarm contacts and may contain one or more alarm contacts. The same alarm contact can be added into multiple alarm contact groups. During the alarm rule setup, the alarm notifications can be sent through alarm contact group.

Create a contact group

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click the **Alarm contact group** menu on the top of the page to switch to the alarm contact group list.

Click **Create a contact group** on the right-top corner to access the **Create a Contact Group** page.

Fill in the group name and add desired contacts into the group.

Edit a contact group

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click the **Alarm contact group** menu on the top of the page to switch to the alarm contact group list.

Click **Edit** in the **Operation** column in the contact group list to modify contacts in the contact group.

Delete a contact group

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Click the **Alarm contact group** menu on the top of the page to switch to the alarm contact group list.

Click **Delete** in the **Operation** column in the contact group list to delete the contact group.

Batch add contacts to a contact group

Log on to Cloud Monitor console.

Go to the **Alarm contact** page.

Tick contacts to be added in the alarm contact list.

Click **Add to the alarm contact group** on the page bottom.

Select the contact group on the page prompted and click **Ok**.

Alarm rule management

The alarm rules of Cloud Service Monitoring are used as examples here. The alarm rules of site monitoring and customized monitoring are described in related sections.

Create alarm rules

Cloud Service Monitoring shows the instances you have bought. Click the **Alarm Rule** for an instance to enter the **Alarm Rule** page.

For first-time access, click **Here** to create an alarm rule. You may click the **New Alarm Rule** button at the top right corner to create a new alarm rule.

Cloud Monitor allows you to set alarm rules for metric items, so that an alarm is sent to the alarm contact once the conditions for an alarm rule are met.

Templates are supported for the ECS alarm rule settings. You may choose to use templates or create new templates on the **New Alarm Rule** page.

Modify an alarm rule

In the alarm rule list, click **Modify** next to an alarm rule to reset the alarm rule.

Delete an alarm rule

In the alarm rule list, click **Delete** after an alarm rule to delete the alarm rule.

Suspend an alarm rule

In the alarm rule list, click **Suspend** after an alarm rule to suspend the alarm rule. After an alarm rule is suspended, the alarm system no longer detects the data monitored according to the rule.

Create alarm rules in batches

You can adjust the quantity of instances displayed in the bottom right corner of the page. Up to 100 instances can be displayed on one page. After selecting the instances, click **set alarm rules in batches** to create alarm rules for up to 100 instances.

Enable, suspend, and delete alarm rules in batch

Click **View all rules** at the bottom of the instance list to access the **All alarm rules** page.

You can adjust the quantity of instances displayed in the bottom right corner of the page. Up to 100 instances can be displayed on one page. Select all these instances and click relevant operation (**Enable**, **Suspend**, or **Delete**) to process the instances.

View alarm history

Click **Alarm history** in the **Alarm rule list** to view alarm history of an alarm rule. You can view alarms in any consecutive three days in the last one month.

Event subscription service

Usage

Through event subscription, Cloud Monitor pushes alarms to a specified MNS queue, so you can connect to your service system by using alarm messages in the queue.

Note:

The frequency of pushing an alarm message to MNS is restricted by channel silence. If no status change occurs in 24 hours since an alarm is triggered, no more notifications are sent for another alarm triggered based on the same alarm rule.

Operation procedure

Activate MNS.

a. View the MNS product introduction and activation link.

b. For the MNS FAQs, click View.

Authorize Cloud Monitor.

After selecting **Event Subscriptions** on the console, you need to authorize Cloud Monitor the write permission to MNS Message Queue if you use the event subscription function for the first time.

Create an event subscription.

a. Click **Create Event** in the top-right corner to create an event to receive alarm rules.

b. To finish an event subscription, select the queue information for receiving alarm rules and the type of the alarms to be received.

Use alarm messages.

You can use the alarm messages through Message Service APIs, and view the delivery status through the MNS console.

a. Message Service API Documentation

b. Message Service Java SDK Documentation

Alarm message format

Alarm messages received in MNS are formatted as follows:

ECS alarm content

```
{
"message":{
"expression": "Average value > 80%", // Alarm rule description
"curValue":"85.65",
"unit": "%", //Unit
"levelDescription": "alarm triggered", //Alarm status, including "alarm triggered" and "alarm cleared".
"time": 1464257700000, // Time when an alarm is triggered
"metricProject": "acs_ecs", //Product name
"userId":"1078500464551219",
"dimensions": "ECS name=yapot_server_1, ECS instance ID=AY14051913564762762e, IP=182.92.79.214,
mountpoint=/mnt", //Monitoring dimensions
"evaluationCount": "1", //Number of retries
"period": "Five minutes", //Statistical period
"metricName": "Disk usage", // Metric name
"alertName":"AY14051913564762762e_98591490-9eb4-42a1-ba2a-3bdbe04196df"
},
"type":0
}
```

Server Load Balancer alarm content

```
{
"message":{
"expression": "maximum value > 2.0 Kb/s", // Alarm rule description
"curValue":"5",
"unit": "Kb/s", //Unit
"levelDescription": "alarm triggered", //Alarm status, including "alarm triggered" and "alarm cleared".
"time": 1451767500000, // Time when an alarm is triggered
"metricProject": "acs_slb", //Product name
"userId":"UserName", //
"dimensions": "instanceId=InstanceId, port=3306, vip=10.157.161.2", //Monitoring dimensions
"evaluationCount": "3", //Number of retries
"period": "15 minutes", //Statistical period
"metricName": "incoming data volume per second", // Metric name
"alertName":"14a850c9d49-cn-beijing-btc-a01_3306_3da5a7df-0821-4cce-93bf-dafe8ce56a68"
},
"type": 0 // A reserved field. 0 indicates a status alarm, including "triggered" and "cleared"; 1 indicates an exception
notification, with an alarm triggered at the occurrence of the exception and no status is logged.
}
```

RAM

Cloud Monitor RAM

Overview

Cloud Monitor supports RAM. This allows you to control the permissions for Cloud Service Monitoring metric data, alarm rule management, and contact and contact group management through sub-accounts.

Note:

At present, metric data queries are supported for the following cloud products:

- ECS
- RDS
- Server Load Balancer
- OSS
- CDN
- ApsaraDB for Memcache
- EIP
- ApsaraDB for Redis
- Message Service
- Log Service

Permission description

Considerations

In RAM system permissions, the Read-only Cloud Monitor access permission only authorizes sub-accounts to view metric data. If you want to authorize sub-accounts to apply alarm rules, refer to the **Alarm management** section below to learn how to modify or create new authorizations.

Authentication type

Besides basic sub-account permission control, RAM currently supports time, MFA, and IP authentication.

Resource description

At present, RAM does not support fine-grained resource descriptions. Only the “*” wildcard is used for resource authorization.

Operation description

Metric data

Data query actions are divided into two groups: product instance list display and Cloud Monitor metric data queries. When authorizing a sub-account to log on to the Cloud Monitor portal and view metric data, you must also grant the sub-account permissions for the corresponding product’s instance list and metric data query.

For metric data authorization, simply access the RAM product’s system authorization policy and select **Read-only Cloud Monitor access permission**.

Metric data query action: Query*.

Product instance list display actions are as follows.

Product name	Action
ECS	DescribeInstances
RDS	DescribeDBInstances
SLB	DescribeLoadBalancer*
OSS	ListBuckets
OCS	DescribeInstances
EIP	DescribeEipAddresses
ApsaraDB for Redis	DescribeInstances
MNS	ListQueue
CDN	DescribeUserDomains

Alarm management

At present, alarm management does not support fine-grained operations. After being granted the following permissions, a sub-account can add, delete, query, and modify alarm rules, contacts, and contact groups.

If you need to allow a sub-account to use alarm functions, add the following permissions.

```
{
"Version": "1",
"Statement": [
{
```

```
"Action": [
"cms:*"
],
"Resource": "*",
"Effect": "Allow"
}
]
}
```

Limits of use

Limits of use

You can create up to 200 metric points for site monitoring using an Alibaba Cloud account.

You can create up to 10 metric items for customized monitoring using an Alibaba Cloud account.

Each account can use up to 1,000 SMS messages per month after initialization.

CloudMonitor terms of service

Change history

Change history

Release date	Changes
July 11, 2015	New version of Cloud Monitor portal went live.

September 22, 2015	ECS supported panorama and ADS database monitoring.
December 14, 2015	Supported SLS log service monitoring and alarms.
December 29, 2015	Supported viewing of ECS basic metric data and added the event subscription function.
January 15, 2016	ECS process monitoring supported one-minute metric data collection and alarms.
January 19, 2016	Supported query of metric data using a sub-account.
May 5, 2016	Supported using the alarm function on the console with a sub-account.
May 15, 2016	Supported Container Service and alarms.
June 13, 2016	Supported OSS monitoring and alarms.
June 17, 2016	Released Dashboard Version 1.0, supporting instance metric data display of ECS and ApsaraDB for Memcache and multi-instance metric data aggregation.