ALIBABA CLOUD

Alibaba Cloud

CloudMonitor

Quick Start

Document Version: 20201023

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview 05
2.Dashboard 09
3.Application group 11
4.Host monitoring 13
5.Custom monitoring 15
6.Site monitoring 17
7.Cloud service monitoring 18
8.Alert service 20

1.Overview

CloudMonitor provides an overview of alerts, key events, and resource usage.

This allows you to check the resource usage and alerts of each cloud service in real time.

Alert overview

In the Alarm Overview section, CloudMonitor provides alert statistics, including the total number of alerts in the last seven days, the number of triggered alert rules, the number of alert rules with insufficient data, and the usage of text messages in the current month.

You can view more information about alert rules by clicking the number of alert rules that are triggered or with insufficient data.

Event overview

In the Event Overview section, CloudMonitor summarizes all the exceptions and O&M events in the last 24 hours. The following table lists the key events that are supported.

Alibaba Cloud service	Event
ECS or non-ECS hosts	Agent Stopped
ApsaraDB for RDS	Master/Slave Instance Switch
ApsaraDB for RDS	Instance Faults
ApsaraDB for MongoDB	Instance Faults
ApsaraDB for Redis	Master/Slave Instance Switch
ApsaraDB for Redis	Instance Faults

Resource usage overview

In the Resource Usage section, CloudMonitor displays the overall resource usage of each service under your account. For OSS, CDN, and Log Service, CloudMonitor displays the cumulative resource usage in the current month. For other services, CloudMonitor displays the resource usage in real time by using the 95th percentile.

Statistical method: the 95th percentile.

- A percentile is a measure used in statistics. It indicates the value lower than which a given percentage of observations in a group of observations in ascending order falls.
- The 95th percentile is the value lower than which 95% of observations in a group of observations in ascending order falls. For example, if the 95th percentile for the CPU usage of ECS instances is 34%, 95% of the ECS instances have a CPU usage of lower than 34%.

CloudMonitor uses the 95th percentile to measure the resource usage of most cloud services.

Resource metric description

Alibaba Cloud service	Metric	Statistical method	Statistical period	Statistical range
ECS or non-ECS hosts	CPU usage	95th percentile	Real-time	All instances
ECS or non-ECS hosts	Memory usage	95th percentile	Real-time	All instances
ECS or non-ECS hosts	Disk usage	95th percentile	Real-time	All instances
ECS or non-ECS hosts	Outbound bandwidth over Internet	95th percentile	Real-time	All instances
ApsaraDB for RDS	CPU usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	Input/Output operations per second (IOPS) usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	Connection usage	95th percentile	Real-time	All instances
ApsaraDB for RDS	Disk usage	95th percentile	Real-time	All instances
OSS	Total outbound traffic over Internet in the current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total number of PUT requests in the current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Total number of GET requests in the current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All buckets
OSS	Storage size	Sum	The sum of the storage occupied by all OSS buckets	All buckets

Alibaba Cloud service	Metric	Statistical method	Statistical period	Statistical range
CDN	Total traffic in the 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 percentile	Real-time	All domain names
CDN	Queries per second (QPS)	95th percentile	Real-time	All domain names
ApsaraDB for MongoDB	CPU usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Memory usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Connection usage	95th percentile	Real-time	All instances
ApsaraDB for MongoDB	Disk usage	95th percentile	Real-time	All instances
ApsaraDB for Memcache	Cache hit ratio	95th percentile	Real-time	All instances
ApsaraDB for Memcache	Cache usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	Memory usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	IOPS usage	95th percentile	Real-time	All instances
ApsaraDB for Redis	Connection usage	95th percentile	Real-time	All instances
EIP	Inbound bandwidth	95th percentile	Real-time	All instances
EIP	Outbound bandwidth	95th percentile	Real-time	All instances
Container Service	CPU usage	95th percentile	Real-time	All instances

Alibaba Cloud service	Metric	Statistical method	Statistical period	Statistical range
Container Service	Memory usage	95th percentile	Real-time	All instances
Container Service	Outbound traffic over Internet	95th percentile	Real-time	All instances
Log Service	Total inbound traffic in the 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 outbound traffic in the 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 number of requests in the current month	Sum	The cumulative value from 00:00 on the first day of the month to the current time	All projects
AnalyticDB for PostgreSQL	CPU usage	95th percentile	Real-time	All instances
AnalyticDB for PostgreSQL	Memory usage	95th percentile	Real-time	All instances
AnalyticDB for PostgreSQL	IOPS usage	95th percentile	Real-time	All instances
AnalyticDB for PostgreSQL	Connection usage	95th percentile	Real-time	All instances
AnalyticDB for PostgreSQL	Disk usage	95th percentile	Real-time	All instances

2.Dashboard

Cloud Monitor provides the dashboard feature. You can customize the monitoring data that a dashboard displays and view the monitoring data on the dashboard.

Scenario

On a dashboard, you can aggregate monitoring data of different instances that run the same workloads. These instances can belong to different services.

View monitoring data on a dashboard

You can use a dashboard to display the resource usage of Alibaba Cloud services.

> Note
> - Cloud Monitor provides a default dashboard that displays specific monitoring data for Elastic Compute Service (ECS).
> - You can add monitoring data of other Alibaba Cloud services to the dashboard.

Procedure

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Dashboard** > **Custom Dashboard**.
3. On the **Dashboards** page, select the dashboard that you want to view from the drop-down list. You can switch to another dashboard by selecting the dashboard from the drop-down list.

Create a dashboard

If the default dashboard for ECS cannot meet your requirements on service monitoring, you can create dashboards and add monitoring charts as needed.

Procedure

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Dashboard** > **Custom Dashboard**.
3. On the Dashboards page, click **Create Dashboard** in the upper-right corner.
4. In the Create Dashboard dialog box, enter a name for the dashboard and click **Create**. The Dashboards page displays the created dashboard. You can add monitoring charts to the dashboard as needed.

Add a monitoring chart

You can add monitoring charts for metrics of your Alibaba Cloud services and custom metrics.

If you use multiple Alibaba Cloud services, you can add monitoring charts for metrics of these services to a dashboard. Then, you can view the monitoring data of the services on the dashboard.

After you report custom monitoring data to Cloud Monitor by using the Cloud Monitor API, you can add monitoring charts for the custom metrics to a dashboard to display the monitoring data.

Procedure

For more information, see Add charts.

Delete a dashboard

> Notice
> - If you delete a dashboard, all monitoring charts that are added to the dashboard are deleted.
> - You cannot restore a dashboard after you delete it.
> - Exercise caution when you delete a dashboard.

Procedure

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Dashboard** > **Custom Dashboard**.
3. On the Dashboards page, click **Delete Dashboard** in the upper-right corner to delete the current dashboard.

Change the name of a dashboard

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Dashboard** > **Custom Dashboard**.
3. On the **Dashboards** page, move the pointer over the dashboard name and click **Edit** that appears. Enter a new name and click **OK**.

3.Application group

This topic describes the scenarios of using application groups, the features of application groups, and how to use application groups.

Scenarios

- **Manage resources from the business perspective**

  You can add resources in your account to different application groups based on the business type. Then, you can query monitoring data and alerts from the business perspective.

- **Perform routine inspection and detect faults**

  After you create application groups, you can use features such as group health check, faulty instance list, and dashboard to monitor resources in application groups. You can inspect resource usage in application groups on a routine basis, locate faulty resources, and identify root causes immediately after you receive alert notifications.

- **Improve resource usage**

  Application groups allow you to aggregate and display monitoring data from multiple dimensions. You can query monitoring data of an application group or a single instance to identify resources that are most frequently accessed.

Features

- Application groups allow you to manage your cloud resources in different services and regions from the business perspective.
- When you apply an alert rule to an application group, the alert rule is applied to all resources in the application group. This greatly improves the operations and maintenance (O&M) efficiency.
- You can find faulty instances by using the faulty instance list that is provided for each application group.
- You can customize and view monitoring charts on the dashboard of an application group.

Procedure

To create an application group, perform the following steps:

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the Application grouping tab of the Application Groups page, click **Create Group** in the upper-right corner. The **Create Group** panel appears.
4. In the **Basic Information** section, enter the application group name and select an alert group.
5. Optional. In the **MonitorAlert** section, select an alert template to initialize alert rules for the instances in the application group and set the **Muted** parameter. If you turn on **Initialize Agent Installation**, Cloud Monitor installs the Cloud Monitor agent on all instances in the application group.
6. In the **Event Monitor** section, select the **Subscribe Event notification** check box. When critical and warning events occur on the instances added to the application group, Cloud Monitor sends alert notifications.

7. In the **Add Instance dynamically** section, configure the rules for dynamically adding Elastic Compute Service (ECS) instances. All instances that match the rules are added to the application group. You can click **Add Product** to configure rules for dynamically adding ApsaraDB RDS and Server Load Balancer (SLB) instances. You can add instances of other Alibaba Cloud services to the application group after the application group is created.
8. Click **Create Group**. The application group is created.

4.Host monitoring

This topic describes the scenarios of using host monitoring, its features, and how to use host monitoring.

Context

Scenarios

- Monitor hosts in a hybrid cloud

  CloudMonitor uses the CloudMonitor agent to collect monitoring data from hosts. You can install the CloudMonitor agent on both Alibaba Cloud Elastic Compute Service (ECS) instances and non-ECS hosts to collect monitoring data from hosts in a hybrid cloud.

- Monitor hosts of an enterprise

  Host monitoring allows you to group hosts in different regions to an application group for business-based host management. In addition, host monitoring allows you to manage alert rules by application group. You can apply one alert rule to all hosts of an application group. This improves the O&M efficiency and overall management experience.

The following table lists the features supported by host monitoring.

Feature	Description
Diverse metrics	After you install the CloudMonitor agent, you can collect data of more than 30 metrics. For more information, see Metrics.
High collection frequency	Data of key metrics are collected every second. All metrics are reported at an interval of 15s. Therefore, the minimum interval between the data points in a monitoring chart is 15s.
Business-level process monitoring	Host monitoring collects statistical data of active processes, including the CPU usage, memory usage, and the number of opened files. This helps you obtain information about the resource allocation on hosts. For more information, see Process monitoring.
Application group-based management	You can manage hosts from different regions and configure alert rules by application group. This significantly reduces the cost of monitoring management.
Alert service	You can set alert rules for metrics and use multiple notification methods, including emails and DingTalk chatbots. For more information, see Alarm service.

Procedure

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Host Monitoring**.

   

3. On the **Instances** tab of the **Host Monitoring** page, install the CloudMonitor agent on target hosts.

   You can install the CloudMonitor agent on hosts in one of the following ways:

- Click **Aliyun ECS install** or **Not Aliyun ecs install** above the instance list. Select the host type, region, and operating system and follow the instructions in the console to install the CloudMonitor agent.
- Select multiple hosts on which you want to install the CloudMonitor agent and click **Batch Install**. You can view the installation status on the Instances tab.

> **Note** For more information about how to install the Java agent, see CloudMonitor Java agent overview. For more information about how to install the GoLang agent, see CloudMonitor GoLang agent overview.

After 3 minutes, find the target host and click **Monitoring Charts** in the **Actions** column to view the monitoring data of the host.

5.Custom monitoring

Custom monitoring allows you to customize metrics and alert rules. You can call the PutCustomMetric API operation to report business metrics about which you are concerned to CloudMonitor. Then, you can view monitoring data and create alert rules for these metrics in the CloudMonitor console. CloudMonitor sends alert notifications about abnormal metrics to you. This allows you to handle faults in a timely manner and ensures normal business operation.

Prerequisites

Monitoring data is reported to CloudMonitor. For more information, see Overview.

Context

Event monitoring and custom monitoring have the following differences:

- Event monitoring focuses on the data of non-continuous events.
- Custom monitoring focuses on periodically collected time series data.

View monitoring data on the Application Groups page

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab of the **Application Groups** page, click the name or ID of the application group that you want to view.
4. In the left-side navigation pane of the page that appears, click **Custom Monitoring**.
5. On the **Custom Monitoring** page, view monitoring data in monitoring charts.

Configure an alert rule on the Custom Monitoring page

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Custom Monitoring**.
3. Configure an alert rule.
   - On the **Time Series** tab of the Custom Monitoring page, configure an alert rule.
     a. On the **Time Series** tab of the Custom Monitoring page, select the application group and time series, and click Dimensions.
     b. In the **Dimensions** panel, find the dimension that you want to use and click **Setup Alarm Rule** in the **Operation** column.
     c. In the **Create/modify custom monitoring and alert rules** panel, configure the alert rule.
     d. Click **Confirm**.
     e. In the **Dimensions** panel, select the dimension that you want to use.
     f. Click **OK**.
   - On the **Alert Rules** tab of the Custom Monitoring page, configure an alert rule.
     a. Click the **Alert Rules** tab.
     b. On the **Alert Rules** tab, click **Create Alert Rule**.

c. In the **Create/modify custom monitoring and alert rules** panel, configure the alert rule.

d. Click **Confirm**.

Configure an alert rule on the Application Groups page

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab of the **Application Groups** page, click the name or ID of the application group that you want to configure.
4. In the left-side navigation pane of the page that appears, click **Custom Monitoring**.
5. On the Custom Monitoring page, find the metric for which you want to configure an alert rule and click **Setup Alarm Rule** in the **Operation** column.
6. On the **Create Alarm Rule** page, set relevant parameters.
7. Click **OK**.

6.Site monitoring

Site monitoring simulates accesses from users and monitors the availability, connectivity, and Domain Name System (DNS) resolution of sites. Site monitoring monitors the connectivity and response time of domain names, IP addresses, and ports and sends alert notifications based on monitoring results. This topic describes how to create a site monitoring task and view the monitoring data generated by a site monitoring task.

Create a site monitoring task

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **New Site Monitor > Site Manage**.
3. On the **Site Monitoring** page, click **New Monitoring Task** in the upper-right corner.
4. On the **New Task** page, set the parameters in the Set basic information, Select probe point, and Set alarm rules sections. For more information about how to set the parameters, see Create a site monitoring task.
5. Click **Create**.

View the monitoring data generated by a site monitoring task

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **New Site Monitor > Site Manage**.

   
3. On the **Site Monitoring** page, click the name of the target site monitoring task and view the monitoring data on the Monitoring overview page.

   

7.Cloud service monitoring

Cloud Monitor automatically monitors resources of each cloud service under your Alibaba Cloud account. You can view the monitoring data about resources of each cloud service in monitoring charts. You can also configure alert rules to monitor resources. When an alert is triggered based on the configured alert rules, Cloud Monitor sends an alert notification. This way, you are notified of performance or usage anomalies immediately after the anomalies occur.

Context

The monitoring data that is displayed on the monitoring page varies with cloud services. For example, you can view the instance list and monitoring charts on the monitoring page of Server Load Balancer (SLB). You can also configure alert rules on the monitoring page.

View monitoring data

On the monitoring page of a cloud service, you can view the running status, performance metrics, and usage metrics of resources.

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Cloud products**.
3. On the **Cloud products** page, click a cloud service.
4. On the monitoring page of the cloud service, click **Monitoring Charts** in the **Actions** column of a resource.On the page that appears, you can view the monitoring charts of the resource.

> **Note**
>
> You can view only the monitoring data that is generated in the last 30 days.

Configure alert rules

On the monitoring page of a cloud service, you can configure alert rules for resources. When an alert is triggered based on the configured alert rules, Cloud Monitor sends an alert notification to you.

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Cloud products**.
3. On the **Cloud products** page, click a cloud service.
4. Create an alert rule for the cloud service.
   - Create an alert rule on the **Alert Rules** page.
     a. On the monitoring page of the cloud service, find the resource for which you want to create an alert rule. Click **Alert Rules** in the **Actions** column.
     b. On the Threshold Value Alert tab of the **Alert Rules** page, click **Create Alert Rule**.
     c. On the **Create Alert Rule** page, configure the alert rule.
     d. Click **Confirm**.
   - Create an alert rule on the monitoring page of the cloud service.
     a. On the monitoring page of the cloud service, click **Create Alert Rule** in the upper-right corner.

b. On the **Create Alert Rule** page, configure the alert rule.

c. Click **Confirm**.

> **Note** For more information about how to configure an alert rule, see Create a threshold-triggered alert rule.

View alert rules

On the monitoring page of a cloud service, you can view all alert rules for resources.

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Cloud products**.
3. On the **Cloud products** page, click a cloud service.
4. On the monitoring page of the cloud service, click **Alert Rules** in the upper-right corner.

References

Appendix 1: Metrics

8.Alert service

You can customize alert rules to specify how the alert system checks the monitoring data and when it sends alert notifications. After you set alert rules for important metrics, you can receive alert notifications immediately after exceptions occur and handle the exceptions in a timely manner.

Context

- You can set the mute period for alert rules. During the mute period, the notification is not re-sent for an alert before the alert is cleared.
- By default, CloudMonitor adds your Alibaba Cloud account as an alert contact and automatically creates an alert group for the alert contact.

Procedure

1. Create an alert contact.
   i. Log on to the CloudMonitor console.
   ii. In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
   iii. On the **Alarm Contacts** page, click **Create Alarm Contact**.
   iv. In the **Set Alarm Contact** right-side pane, set the Name, Email ID, and DingTalk Robot parameters. Make sure that you specify the correct email address. Otherwise, you cannot receive alert notifications.
   v. Click **OK**.
2. Create an alert group.
   i. On the **Alarm Contacts** page, click the **Alarm Contact Group** tab.
   ii. On the **Alarm Contact Group** tab, click **Create Alarm Contact Group**.
   iii. In the **Create Alarm Contact Group** right-side pane, specify the alert group name and add alert contacts to the alert group.
   iv. Click **Confirm**.
3. Create an alert rule.
   i. In the left-side navigation pane, choose **Alarms > Alarm Rules**.
   ii. On the Threshold Value Alarm tab of the **Alarm Rules** page, click **Create Alarm Rule**.
   iii. On the **Create Alarm Rule** page, set the parameters in the Related Resource, Set Alarm Rules, and Notification Method sections.

   The following table describes the parameters for configuring an alert rule.

   iv. Click **Confirm**.