ALIBABA CLOUD

# Alibaba Cloud

## CloudMonitor

## Quick Start

Document Version: 20220216

# 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

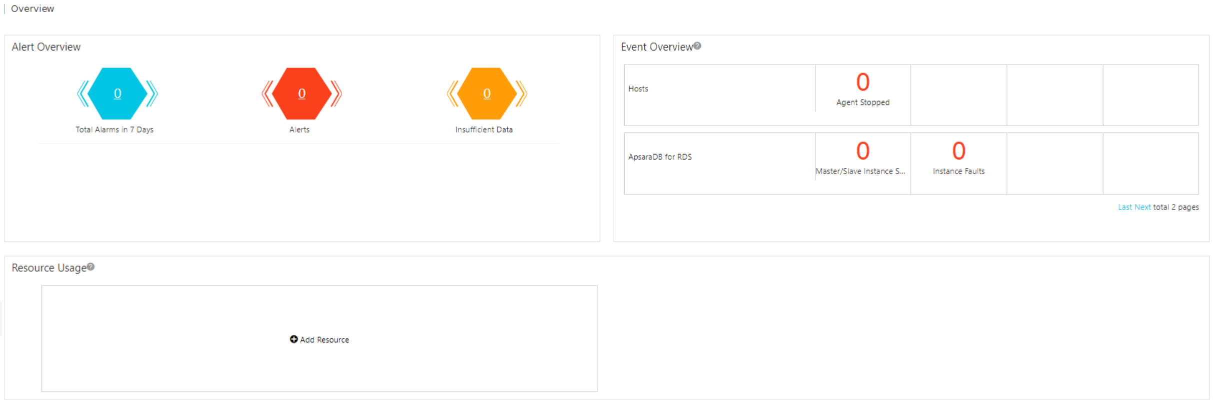
| Style | Description | Example |
|---|---|---|
| Danger | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. | Danger:<br>Resetting will result in the loss of user configuration data. |
| Warning | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. | Warning:<br>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:<br>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:<br>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`<br>*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

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

This allows you to check the resource usage and alerts of each Alibaba Cloud service in real time. The following figure shows the overview of CloudMonitor.



## Alert overview

In the Alert 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 this month.

- You can click Total Alarms in 7 Days to view the alert trend chart and alert history in the last seven days.
- You can click Alarms to view the details of alert rules in the **Alert** state.
- You can click Insufficient Data to view the details of alert rules in the **Insufficient Data** state.

## Event overview

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

| Alibaba Cloud service | Event |
|---|---|
| ECS or non-ECS hosts | Agent Stopped |
| ApsaraDB RDS | Master/Slave Instance Switch |
| ApsaraDB 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 Alibaba Cloud service within your account. CloudMonitor uses the 95th percentile to measure the resource usage of most Alibaba Cloud services.

The following table describes the statistical metrics of Alibaba Cloud services.

| Alibaba Cloud service | Metric | Statistical method | Statistical period | Statistical range |
|---|---|---|---|---|
| ECS or non-ECS hosts | CPU utilization | 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 RDS | CPU utilization | 95th percentile | Real-time | All instances |
| ApsaraDB RDS | Input/Output operations per second (IOPS) usage | 95th percentile | Real-time | All instances |
| ApsaraDB RDS | Connection usage | 95th percentile | Real-time | All instances |
| ApsaraDB 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 domains |
| CDN | Peak network bandwidth | 95th percentile | Real-time | All domains |
| CDN | Queries per second (QPS) | 95th percentile | Real-time | All domains |
| ApsaraDB for MongoDB | CPU utilization | 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 utilization | 95th percentile | Real-time | All instances |
| Container Service | Memory usage | 95th percentile | Real-time | All instances |

| Alibaba Cloud service | Metric | Statistical method | Statistical period | Statistical range |
|---|---|---|---|---|
| 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 |

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%.

# 2.Dashboard

If the default Elastic Compute Service (ECS) dashboard of CloudMonitor cannot meet your business needs, you can create a dashboard and add monitoring charts to view custom monitoring data.

## Create a dashboard

1. Log on to the CloudMonitor 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 dashboard name.
5. Click **Create**.

   You are redirected to the newly created dashboard. You can then add monitoring charts to the dashboard as needed. For more information, see Add a monitoring chart.

## Add a monitoring chart

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Dashboard > Custom Dashboard**.
3. Select a dashboard from the **Dashboards** drop-down list.
4. In the upper-right corner, click **Add View**.
5. In the **Add View** panel, select a chart type and metrics.

| Parameter | Description |
|---|---|
| **Chart Type** | Supported types include line charts, area charts, tables, heat maps, and pie charts. |
| **Select Metrics** | You can select cloud service metrics, log monitoring metrics, or custom metrics.<br>○ Dashboards: the metrics of Alibaba Cloud services. For more information, see Cloud service monitoring.<br>○ Custom: the metrics that you add by using the custom monitoring feature. For more information, see Report monitoring data. |

6. Click **Save**.

## View monitoring charts

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Dashboard > Custom Dashboard**.
3. Select a dashboard from the **Dashboards** drop-down list.
4. Select the time range to display monitoring data on the monitoring charts.

> **Note** You can query only the monitoring data of the last 30 days.

5. View the monitoring charts.
   - Click **Full Screen** in the upper-right corner. You can view all the monitoring charts on the dashboard in full-screen mode.
   - Click **Refresh** in the upper-right corner. You can refresh all monitoring charts on the dashboard in real time.

# 3.Create an application group

The application group feature allows you to manage resources from different services and regions by group. You can create application groups based on your business requirements. You can add resources such as servers and databases related to the same business to an application group, and manage alert rules by application group.

## Context

The following table describes the methods of creating application groups and the Alibaba Cloud services that are supported by each creation method.

| Creation method | Description | Supported Alibaba Cloud service |
|---|---|---|
| **Create a standard application group** | You can create a standard application group to manage existing instances based on your business requirements. | Supported Alibaba Cloud services |
| **Create an application group based on smart tag synchronization** | If tags are attached to your instances, you can specify a tag-based matching rule to create an application group. All instances that match the rule are automatically added to the application group for you to manage. If an existing instance has a tag that is specified in the matching rule, an application group is automatically created for the tag. If a newly created instance has a tag that is specified in the matching rule, an application group is also automatically created for the tag. Up to 3,000 instances can match a rule at a time.<br>For more information about how to create and attach tags in Resource Management, see Add a custom tag. | • Elastic Compute Service (ECS)<br>• ApsaraDB for Redis (standard architecture)<br>• ApsaraDB for Redis (cluster architecture)<br>• ApsaraDB for Redis (read/write splitting architecture)<br>• ApsaraDB for MongoDB (replica set architecture)<br>• ApsaraDB for MongoDB (sharded cluster architecture)<br>• ApsaraDB for MongoDB (standalone instance architecture)<br>• ApsaraDB RDS<br>• ApsaraDB RDS for PostgreSQL<br>• Server Load Balancer (SLB)<br>• Elasticsearch<br>• PolarDB for MySQL<br>• AnalyticDB for PostgreSQL<br>• AnalyticDB for MySQL V3.0<br>• Function Compute<br>• E-MapReduce<br>• Anti-DDoS Pro<br>• Alibaba Cloud CDN<br>• Express Connect<br>• Elastic IP Address (EIP)<br>• EIP Bandwidth Plan<br>• NAT Gateway |

| Creation method | Description | Supported Alibaba Cloud service |
|---|---|---|
| **Create an application group based on a smart instance rule** | You can specify an instance name-based matching rule to create an application group. All instances that match the rule are automatically added to the application group for you to manage. | - Elastic Compute Service (ECS)<br>- ApsaraDB RDS<br>- Server Load Balancer (SLB)<br>- ApsaraDB for Redis (standard architecture)<br>- ApsaraDB for Redis (cluster architecture)<br>- ApsaraDB for Redis (read/write splitting architecture)<br>- PolarDB for MySQL<br>- ApsaraDB for MongoDB (replica set architecture)<br>- ApsaraDB for MongoDB (sharded cluster architecture)<br>- ApsaraDB for MongoDB (standalone instance architecture) |
| **Create an application group from a resource group** | If you have specified a resource group, you can create an application group from the resource group. All instances in the resource group are added to the application group for you to manage.<br>For more information about how to create resource groups in Resource Management, see Create a resource group. | - Elastic Compute Service (ECS)<br>- ApsaraDB RDS<br>- Server Load Balancer (SLB)<br>- Elastic IP Address (EIP)<br>- Anti-DDoS Pro<br>- Alibaba Cloud CDN<br>- EIP Bandwidth Plan<br>- PolarDB for MySQL<br>- ApsaraDB for Redis (standard architecture)<br>- ApsaraDB for Redis (cluster architecture)<br>- ApsaraDB for Redis (read/write splitting architecture)<br>- ApsaraDB for MongoDB (replica set architecture)<br>- ApsaraDB for MongoDB (sharded cluster architecture)<br>- ApsaraDB for MongoDB (standalone instance architecture)<br>- Web Application Firewall (WAF) |

## Create a standard application group

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab, click **Create Group** in the upper-right corner.

4. In the **Create Group** panel, set the **Creation method** parameter to **Standard Group creation** and set other parameters.

| Parameter | Description |
|---|---|
| **Basic Information** | Set the Application Group Name and Contact Group parameters.<br>○ **Application Group Name**: the name of the application group.<br>○ **Contact Group**: the contact group to which alert notifications are sent. You can select an existing contact group or create a contact group. |
| **MonitorAlert** | Set the Select Template and Muted parameters.<br>○ **Select Template**: the alert template used to initialize alert rules of the application group.<br>For more information about how to create an alert template, see Create an alert template.<br>○ **Muted**: the interval of resending the notification for an alert before the alert is cleared. The minimum value is 5 minutes, and the maximum value is 24 hours. |
| **Initialize Agent Installation** | After you turn on **Initialize Agent Installation**, CloudMonitor automatically installs the CloudMonitor agent on the instances in the application group to collect monitoring data from the instances. |
| **Event Monitor** | If you select **Subscribe Event notification**, CloudMonitor automatically sends alert notifications to you when critical or warning events occur on the instances added to the application group. |

5. Click **Create Group**.
6. On the **Application grouping** tab, select **Custom** from the drop-down list to view the created application group.

## Create an application group based on smart tag synchronization

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab, click **Create Group** in the upper-right corner.
4. In the **Create Group** panel, set the **Creation method** parameter to **Smart tag synchronization creation** and set other parameters.

| Parameter | Description |
|---|---|
| **Basic Information** | Set the Application Group Name and Contact Group parameters.<br>○ **Application Group Name**: CloudMonitor automatically generates a name for the application group.<br>○ **Contact Group**: the contact group to which alert notifications are sent. You can select an existing contact group or create a contact group. |

| Parameter | Description |
|---|---|
| **MonitorAlert** | Select an alert template. You can initialize alert rules of the application group by using the alert template.<br>For more information about how to create an alert template, see Create an alert template. |
| **Region** | The region where the application group resides. |
| **Match Rule** | You can specify a dynamic matching rule based on a resource tag to automatically add instances.<br>- **Resource Tag Key**: the tag key of the instance.<br>**Note** A custom tag key must be one of the existing tag keys of a resource. Otherwise, you cannot create an application group.<br>- **Tag Value**: the tag value of the instance. Instances whose tag values **contain**, **start with**, **end with**, **do not contain**, or **equal to** the value you specify are automatically added to the application group. If you set the Tag Value parameter to **All**, all instances with the specified tag are added to the application group. A newly created instance that matches the rule is also added to the application group. |
| **Initialize Agent Installation** | After you turn on **Initialize Agent Installation**, CloudMonitor automatically installs the CloudMonitor agent on the instances in the application group to collect monitoring data from the instances. |
| **Event Monitor** | If you select **Subscribe Event notification**, CloudMonitor automatically sends alert notifications to you when critical or warning events occur on the instances added to the application group. |

5. Click **Add**.
6. On the **Application grouping** tab, select **Resource tags** from the drop-down list to view the created application group.

## Create an application group based on a smart instance rule

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab, click **Create Group** in the upper-right corner.
4. In the **Create Group** panel, set the **Creation method** parameter to **Smart Instance Rule Creation** and set other parameters.

| Parameter | Description |
|---|---|
| **Basic Information** | Set the Application Group Name and Contact Group parameters.<br>- **Application Group Name**: the name of the application group.<br>- **Contact Group**: the contact group to which alert notifications are sent. You can select an existing contact group or create a contact group. |

| Parameter | Description |
|---|---|
| **MonitorAlert** | Set the Select Template and Muted parameters.<br>○ **Select Template**: the alert template used to initialize alert rules of the application group.<br>For more information about how to create an alert template, see Create an alert template.<br>○ **Muted**: the interval of resending the notification for an alert before the alert is cleared. The minimum value is 5 minutes, and the maximum value is 24 hours. |
| **Add Instance dynamically** | Specify the matching rule so that CloudMonitor automatically adds instances to the application group based on the names of the instances. |
| **Initialize Agent Installation** | After you turn on **Initialize Agent Installation**, CloudMonitor automatically installs the CloudMonitor agent on the instances in the application group to collect monitoring data from the instances. |
| **Event Monitor** | If you select **Subscribe Event notification**, CloudMonitor automatically sends alert notifications to you when critical or warning events occur on the instances added to the application group. |

5. Click **Create Group**.
6. On the **Application grouping** tab, select **Custom** from the drop-down list to view the created application group.

## Create an application group from a resource group

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the **Application grouping** tab, click **Create Group** in the upper-right corner.
4. In the **Create Group** panel, set the **Creation method** parameter to **Resource group creation** and set other parameters.

| Parameter | Description |
|---|---|
| **Basic Information** | Set the Resource group creation and Contact Group parameters.<br>○ **Resource group creation**: Select a resource group that was created in the Resource Management console.<br>○ **Contact Group**: the contact group to which alert notifications are sent. You can select an existing contact group or create a contact group. |
| **Initialize Agent Installation** | After you turn on **Initialize Agent Installation**, CloudMonitor automatically installs the CloudMonitor agent on the instances in the application group to collect monitoring data from the instances. |
| **Event Monitor** | If you select **Subscribe Event notification**, CloudMonitor automatically sends alert notifications to you when critical or warning events occur on the instances added to the application group. |

5. Click **Add**.
6. On the **Application grouping** tab, select **Resource group** from the drop-down list to view the created application group.

# 4.Host monitoring

Host monitoring collects multiple monitoring data of operating system metrics from your hosts by using the Cloud Monitor agents installed on your hosts.

## Context

Scenarios

- Monitor hosts in a hybrid cloud

  Cloud Monitor collects monitoring data from your hosts by using the Cloud Monitor agents installed on your hosts. You can install the Cloud Monitor 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.

## Install Cloud Monitor agents

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, select the ECS instances on which you want to install or update the CloudMonitor agent for C++ and click **Batch Install**.

   The process requires about 5 minutes to complete. When the agent status changes from **Installing** to **Running**, the installation or update succeeds.

   > **Note** If you turn on **New Purchase ECS Automatically Installs Cloud Monitor**, the CloudMonitor agent for C++ is automatically installed on new ECS instances. Otherwise, you must manually install the CloudMonitor agent for C++.

## View monitoring charts

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Host Monitoring**.
3. On the **Instances** tab of the **Host Monitoring** page, click the instance name of the host or click **Monitoring Charts** in the **Actions** column.
4. On the **instance details** page, you can view the monitoring charts of the key metrics of your host.

## Configure an alert rule

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Host Monitoring**.
3. On the **Host Monitoring** page, click the **Alert Rules** tab.
4. On the **Alert Rules** tab, click **Create Alert Rule** in the upper-right corner.
5. On the **Create Alert Rule** page, set the parameters.

For more information about how to set the parameters, see Create a threshold-triggered alert rule.

6. Click **Confirm**.

# 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, click the name or ID of the application group that you want to manage.
4. In the left-side navigation pane of the page that appears, click **Custom Monitoring**.
5. On the **Time Series** tab of the **Custom Monitoring** page, select the time series and click **Dimensions**.
6. In the **Dimensions** panel, select the dimension that you want to use and click **OK**.
7. View monitoring data of the metric.

## Configure an alert rule on the Custom Monitoring page

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Custom Monitoring**.
3. On the **Custom Monitoring** page, click the **Alert Rules** tab.
4. On the **Alert Rules** tab, click **Create Alert Rule**.
5. In the **Create/Modify Custom Monitoring And Alert Rules** panel, configure the parameters for the alert rule on a custom metric. The following table describes the parameters.

| Parameter | Description |
|---|---|
| **Rule Name** | The name of the alert rule. |
| **Application Groups** | The ID of the application group to which the alert rule belongs.<br>By default, the Application Groups parameter is set to Does not belong to any group. You can select an application group based on your business requirements. For more information about how to create an application group, see 创建应用分组. |

| Parameter | Description |
|---|---|
| **Monitor Metric** | The name of the custom metric. |
| **Dimension** | The resources for which you want to query the monitoring data.<br>Format: a set of key-value pairs. Example: `instanceId:i-uf6j91r34rnwawoo****` and `userId:100931896542****` . |
| **Alert Type** | The notification method. In this example, the Email + DingTalk option is specified. |
| **Rule Description** | The conditions. If the metric meets the conditions, the alert rule is triggered. |
| **Contact Group** | The alert group. For more information, see Create an alert contact or alert group.<br>○ If you set the **Application Groups** parameter to **Does not belong to any group**, you can select an alert group. If the alert rule is triggered, the alert contacts of the alert group receive alert notifications.<br>○ If you specify an application group for the **Application Groups** parameter, you can select an alert group. If the alert rule is triggered, the alert contacts of the alert group receive alert notifications. The alert group of the application group remains unchanged. The alert contacts of the alert group do not receive alert notifications. |
| **Triggered when threshold is exceeded for** | The number of consecutive times the threshold value is exceeded. If the number of times exceeds the limit that you specify, the alert contacts of the alert group receive alert notifications. Valid values: 1, 3, 5, 10, 15, and 30. |
| **Channel Silence Cycle** | The interval at which CloudMonitor sends alert notifications until the alert that is triggered based on the alert rule is cleared. Valid values: 5miniute, 10minute, 15minute, 30minute, 60minute, 3hour, 6hour, 12hour, and 24hour.<br>An alert is triggered if the conditions of an alert rule are met. CloudMonitor does not resend an alert notification if the alert is triggered again within the mute period. CloudMonitor resends alert notifications if the alert is not cleared when the mute period elapses. |
| **Effective Time** | The period within which the alert rule is valid. CloudMonitor monitors the resources that you specify and triggers alerts based on the metric only within the period. |
| **Alert Callback** | The callback URL that can be accessed over the Internet. CloudMonitor sends a POST request to push an alert to the callback URL that you specify. Only HTTP requests are supported. For more information about how to configure alert callbacks, see Use the alert callback feature to send notifications about threshold-triggered alerts. |

6. Click **Confirm**.

## Configure an alert rule on the Application Groups page

1. Log on to the CloudMonitor 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 manage.
4. In the left-side navigation pane of the page that appears, click **Custom Monitoring**.
5. On the **Custom Monitoring** page, click the **Alert Rules** tab.
6. On the **Alert Rules** tab, click **Create Alert Rule**.
7. In the **Create/Modify Custom Monitoring And Alert Rules** panel, configure the parameters for the alert rule on a custom metric.
8. Click **Confirm**.

# 6.Create and view a site monitoring task

The site monitoring feature is used to simulate user access and monitor the availability, connectivity, and Domain Name System (DNS) resolution of sites. The feature allows you to monitor the connectivity and response time of domains, IP addresses, and ports and send alert notifications based on monitoring results. This topic describes how to create a site monitoring task and view the monitoring data that is 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, click **SiteMonitor**.
3. On the **Monitoring task** tab, click **Create task**.
4. In the **Task settings** step of the New Task panel, select a protocol and configure the basic information about the protocol.

| Parameter | Description |
|---|---|
| Monitor Type | The protocol that is used by the site monitoring task. Valid values: HTTP(S), PING, TCP, UDP, DNS, SMTP, POP3, and FTP. |
| **Task Name** | The name of the site monitoring task. The name must be 4 to 100 characters in length, and can contain letters, digits, and underscores (_). |
| **IP Probe Type** | The type of the IP address that is used by the site monitoring task. Valid values: IPV4 and IPV6. |
| **Monitor Domain Name** | The address of the site that you want to monitor. Valid values:<br>○ **Enter the task address manually**: Enter the address of the site that you want to monitor. You can enter multiple addresses at a time. Separate multiple addresses with line feeds. After you configure a site monitoring task, CloudMonitor generates a sub-task for each site address that you specify.<br>○ **Import from Cloud Resolution Domain Name**: Select the domain name of the site that you want to monitor from Alibaba Cloud DNS. For more information about how to create a DNS domain name, see Add an A record to a website domain. |
| **Frequency** | The frequency at which the site monitor task sends detection requests to the monitored site. Valid values: 1Minute, 5Minute, 15Minute, 30Minute, and 60Minute. For example, if you select 1Minute, a detection point in a region sends a detection request to the monitored site every minute. |
| Advanced setting | The parameters in this section vary based on the protocol that you specify. For more information, see Description. |

5. Click **Next**.
6. Select detection points.

**Probe points advanced options**: allows you to customize detection points by specifying the carrier and region.

7. Click **Next**.
8. 
9. Click **Finish**.

## View a site monitoring task

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **SiteMonitor**.
3. On the **Site monitoring list** page, you can view the total number of site monitoring tasks, the number of site monitoring tasks for which the Availability Rate alert rule is triggered, and the number of site monitoring tasks for which the Response Time alert rule is triggered. You can also view the quota usage of the number of site monitoring tasks allowed.
4. On the **Monitoring task** tab, click the name of the site monitoring task whose data you want to view, or the 📈 icon in the **Actions** column of the site monitoring task.
5. You can view data related to the site monitoring task on the Overview, Monitoring analysis, and Alarm rules pages.
    - On the **Overview** page, you can view data displayed in the **Monitoring overview**, **Alert Rule**, **Detection results(Last 6 hours detection results)**, and **Availability response time analysis statistics (average)** sections. You can also view detected errors in the Detection results(Last 6 hours detection results) section.
    - On the **Monitoring analysis** page, you can view data displayed on the **Overall detection mission analysis**, **Geographical detection analysis**, **Operator Detection Analysis**, and **Detection error analysis** tabs.
    - On the **Alarm rules** page, you can view the alert rules of the site monitoring task, and modify, delete, disable, or enable the alert rules for the site monitoring task.

# 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.Alerting service

You can use alert rules to specify how CloudMonitor checks the monitoring data and when CloudMonitor sends alert notifications. After you configure alert rules based on important metrics, you can receive alert notifications immediately after exceptions occur and handle the exceptions at the earliest opportunity.

## Context

- You can specify a mute period such as 24 hours for an alert rule. To prevent an excessive number of alerts from being sent in a short period of time, CloudMonitor sends only one alert notification within the mute period if the alert rule is not triggered as expected.
- By default, CloudMonitor automatically creates an alert group and adds your Alibaba Cloud account as an alert contact to the alert group.

## Create an alert contact

You can add an alert contact to multiple alert groups.

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
3. On the **Alert Contacts** tab, click **Create Alert Contact**.
4. In the **Set Alert Contact** panel,enter the name, email address, and DingTalk chatbot of the alert contact, and retain the default value **Automatic** for the **Alert Notification Information Language** parameter.

   > **Note** **Automatic** indicates that Cloud Monitor automatically selects the language of alert notifications based on the language that you use to create your Alibaba Cloud account.

5. Verify the parameters and then click **OK**.
6. Optional. Activate the email address and phone number of the alert contact.

   By default, the email address and phone number of the alert contact are in the **Pending Activation** state. After the alert contact receives an email and text message that contain the activation links, the alert contact must activate the email address and phone number within 24 hours. Otherwise, the alert contact cannot receive alert notifications. After the email address and phone number are activated, they are displayed in the alert contact list.

## Create an alert group

An alert group is a group of one or more alert contacts.

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
3. Click the **Alert Contact Group** tab.
4. On the **Alert Contact Group** tab, click **Create Alert Contact Group**.
5. In the **Create Alert Contact Group** panel, specify the alert group name and add alert contacts to the alert group.
6. Click **Confirm**.

## Add multiple alert contacts to an alert group at a time

1. 
2. 
3. On the **Alert Contacts** tab, select multiple alert contacts.
4. Click **Add to a contact group**.
5. In the **Confirm** dialog box, select the alert group.
6. Click **OK**.

## Create a static threshold-triggered alert rule

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Alerts > Alert Rules**.
3. On the **Threshold Value Alert** tab, click **Create Alert Rule**.
4. On the **Create Alert Rule** page, set the **Threshold type** parameter to **Static threshold** and set the parameters that are described in the following table.

| Parameter | Description |
|---|---|
| **Product** | The name of the service monitored by CloudMonitor. Example: RDS-DB. |
| **Resource Range** | The resources to which the alert rule applies. Valid values:<br>○ **All Resources**: indicates that the alert rule applies to all resources included in the specified cloud service of the Alibaba Cloud account.<br>○ **Instance**: indicates that the alert rule applies only to the specified resource included in the specified cloud service of the Alibaba Cloud account. |
| **Alert Rule** | The name of the alert rule. |
| **Rule Description** | The content of the alert rule. This parameter defines the conditions that trigger an alert. |
| **Mute for** | The interval of resending the notification for an alert before the alert is cleared.<br>An alert is triggered when the conditions of an alert rule are met. CloudMonitor does not resend an alert notification when the alert is triggered again within the mute period. CloudMonitor starts to resend alert notifications if the alert is not cleared after the mute period ends. |
| **Effective Period** | The period during which the alert rule is effective. CloudMonitor monitors the metrics and generates alerts only if the alert rule is effective. |
| **Notification Contact** | The alert groups to which alert notifications are sent. |
| **Notification Methods** | Email + DingTalk |

| Parameter | Description |
|---|---|
| **Auto Scaling** | If you select **Auto Scaling**, the specified scaling rule is triggered if an alert is generated. You must set the **Region**, **ESS Group**, and **ESS Rule** parameters.<br>○ For more information about how to create a scaling group, see Create a scaling group.<br>○ For more information about how to create a scaling rule, see Create a scaling rule. |
| **Log Service** | If you select **Log Service**, the alert message is written to Log Service if an alert is generated. You must set the **Region**, **Project**, and **Logstore** parameters.<br>For more information about how to create a project and a Logstore, see Getting Started. |
| **Email Remark** | Optional. The custom remarks that you want to include in the alert notification email. |
| **HTTP WebHook** | The callback URL that can be accessed over the Internet. CloudMonitor sends a POST request to push an alert to the specified callback URL. Only HTTP requests are supported. For more information about how to configure alert callbacks, see Use the alert callback feature to send notifications about threshold-triggered alerts. |

5. Click **Confirm**.

## Create a dynamic threshold-triggered alert rule

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Alerts** > **Alert Rules**.
3. On the **Threshold Value Alert** tab, click **Create Alert Rule**.
4. On the **Create Alert Rule** page, set the **Threshold type** parameter to **Dynamic threshold** and set the parameters that are described in the following table.

| Parameter | Description |
|---|---|
| **Product** | The name of the service monitored by CloudMonitor. |
| **Resource Range** | The resources to which the alert rule applies. A dynamic threshold-triggered alert rule applies only to a single resource. |
| **Alert Rule** | The name of the alert rule. |
| **Rule Description** | The content of the alert rule. This parameter defines the conditions that trigger an alert. |
| **Alert sensitivity** | The sensitivity level of the alert. Default value: Low. Valid values: Low, In, and High.<br>The higher the alert sensitivity level is, the more frequently the alert is generated. |

| Parameter | Description |
|---|---|
| **Historical data used by default (days)** | The number of days of the historical monitoring data that CloudMonitor uses to calculate the dynamic thresholds. Unit: days. Valid values: 3 to 14. Default value: 14.<br>For example, you can set this parameter to **14**. Before you create a dynamic threshold-triggered alert rule, make sure that the metric to be monitored has monitoring data within the last 14 days. If no monitoring data is available in one of the last 14 days, the calculation fails, and CloudMonitor does not send an alert notification to you.<br>**Note** To change the default value of the **Historical data used by default (days)** parameter, click **Alarm configuration**. |
| **Mute for** | The interval of resending the notification for an alert before the alert is cleared.<br>An alert is triggered when the conditions of an alert rule are met. CloudMonitor does not resend an alert notification when the alert is triggered again within the mute period. CloudMonitor starts to resend alert notifications if the alert is not cleared after the mute period ends. |
| **Effective Period** | The period during which the alert rule is effective. CloudMonitor monitors the metrics and generates alerts only if the alert rule is effective. |
| **Notification Contact** | The alert groups to which alert notifications are sent. |
| **Notification Methods** | Email + DingTalk |
| **Auto Scaling** | If you select **Auto Scaling**, the specified scaling rule is triggered if an alert is generated. You must set the **Region**, **ESS Group**, and **ESS Rule** parameters.<br>○ For more information about how to create a scaling group, see Create a scaling group.<br>○ For more information about how to create a scaling rule, see Create a scaling rule. |
| **Log Service** | If you select **Log Service**, the alert message is written to Log Service if an alert is generated. You must set the **Region**, **Project**, and **Logstore** parameters.<br>For more information about how to create a project and a Logstore, see Getting Started. |
| **Email Remark** | Optional. The custom remarks that you want to include in the alert notification email. |
| **HTTP WebHook** | The callback URL that can be accessed over the Internet. CloudMonitor sends a POST request to push an alert to the specified callback URL. Only HTTP requests are supported. For more information about how to configure alert callbacks, see Use the alert callback feature to send notifications about threshold-triggered alerts. |

5. Click **Confirm**.

# 9.Container monitoring

Cloud Monitor provides the container monitoring feature. This feature provides an overview of Container Service for Kubernetes (ACK) clusters and monitoring data of nodes, namespaces, and workloads of ACK clusters. This feature allows you to track the status of ACK clusters. This feature also allows you to configure alert rules for ACK clusters, nodes, and pods. When an alert is triggered, Cloud Monitor sends an alert notification. This way, you are immediately notified of exceptions and can handle the exceptions as early as possible.

## Prerequisites

ACK is activated and a cluster is created. For more information, see Quick start for first-time users.

## Context

Before Cloud Monitor can monitor ACK clusters, you must update the metrics-server component of the clusters to V0.3.8 or later. For more information, see Install the metrics-server component.

## Cluster overview

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Container Service Monitoring**.
3. On the **Container Service Monitoring** page, find the cluster that you want to view and click the cluster name or **View the Detail**.
4. The **Cluster overview** page appears. You can view the basic information and monitoring data of the cluster.
    - On the **Overview** tab, you can view the status of pods and nodes. You can also view the CPU utilization and memory usage of top pods and nodes.
    - On the **Cluster Monitoring Chart** tab, you can view the monitoring charts of all metrics of the cluster in the specified time range.

## Node monitoring data

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Container Service Monitoring**.
3. On the **Container Service Monitoring** page, find the cluster that you want to view and click the cluster name or **View the Detail**.
4. In the left-side navigation pane, click **Node**.
5. On the **Node** page, find the node that you want to view and click the node ID or **View the Detail**.
6. On the **Monitoring Charts** tab, you can view the monitoring charts of all metrics of the node in the specified time range.

## Namespace monitoring data

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Container Service Monitoring**.
3. On the **Container Service Monitoring** page, find the cluster that you want to view and click the cluster name or **View the Detail**.

4. In the left-side navigation pane, click **Namespace**.
5. On the **Namespace** page, find the namespace that you want to view and click the namespace name or **View the Detail**.
6. On the **Monitoring Charts** tab, you can view the status of pods and the monitoring charts of CPU utilization and memory usage of top pods in the specified time range.

## Workload monitoring data

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Container Service Monitoring**.
3. On the **Container Service Monitoring** page, find the cluster that you want to view and click the cluster name or **View the Detail**.
4. In the left-side navigation pane, click **Workload**.
5. On the **Workload** page, you can view the monitoring charts of applications and pods. You can also view the CPU utilization and memory usage of top pods.
   - On the **Stateless**, **Stateful**, **Daemon set**, **Scheduled Tasks**, or **Task** tab, find the application that you want to view. Then, click the application name or click **View the Detail** in the **Actions** column. On the page that appears, you can view the monitoring chart, the list of pods, and the hot spots of pods of the application.
   - On the **Container Group** tab, find the pod that you want to view. Then, click the pod name or click **View the Detail** in the **Actions** column. On the page that appears, you can view the monitoring charts of all pods in the workload.
6. On the **Stateless** tab of the **Workload** page, find the workload that you want to view and click the workload name or **View the Detail**.

   You can view the CPU utilization and memory usage of workloads on the **Stateless**, **Stateful**, **Daemon set**, **Scheduled Tasks**, **Task**, and **Container Group** tabs.
7. On the **Deployment Application**, **Container group list**, and **Container group hotspot** tabs, you can view the basic information and monitoring charts of the workload.

## Create an alert rule

1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, click **Container Service Monitoring**.
3. On the **Container Service Monitoring** page, find the cluster for which you want to create an alert rule and click **View Alert Rules** in the **Actions** column.
4. On the **Alert Rules** page, click **Create Alert Rule**.
5. In the **Create Alert Rule** panel, configure the parameters.

| Parameter | Description |
|---|---|
| **Resource Range** | The resources to which the alert rule is applied. Valid values:<br>○ **Cluster**: The alert rule is applied to the cluster.<br>○ **Node**: The alert rule is applied to all nodes or specified nodes in the cluster.<br>○ **Container Group (pod)**: The alert rule is applied to all pods or specified pods in the specified application under the specified namespace of the cluster. |

| Parameter | Description |
|---|---|
| **Rule Description** | The content of the alert rule. The parameters in this section specify the conditions that trigger an alert. |
| **Effective Time** | The interval of re-sending the notification for an alert before the alert is cleared. |
| **Effective Time** | The time period during which the alert rule is effective. Cloud Monitor checks whether the monitoring data meets the alert rule only during the effective period. |
| **HTTP Callback** | Cloud Monitor sends a POST request to push an alert message to the specified callback URL. Only HTTP requests are supported.<br>**Note** We recommend that you specify a callback URL that can be accessed over the Internet. |
| **Alert Contact Group** | The alert group that receives alert notifications. |

6. Click **OK**.