

Cloud Eye

Getting Started

Issue 01
Date 2024-01-12



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Monitoring Overview.....	1
2 Querying Metrics of a Cloud Service	3
3 Using Server Monitoring.....	5
4 Using Custom Monitoring.....	7
5 Using Event Monitoring.....	9
6 Using Resource Groups.....	11
7 Creating an Alarm Rule.....	12

1 Monitoring Overview

The **Monitoring Overview** page provides the following modules, helping you track the resource usage and alarms in real time.

Resource Overview

Displays the total number of monitored cloud service resources and alarms generated for these resources in the current account.

Alarm Statistics

Displays the alarm trend for the last seven days and the number of alarms of each severity.

After you click an alarm severity, the **Alarm Rules** page is displayed, showing all alarm rules of the severity.

NOTE

On the **Alarm Rules** page, click **View Resource** in the **Operation** column. On the displayed window, you can copy the resource ID and go to the corresponding cloud service console to search for the specific resource.

Server Monitoring

Displays the CPU usages of all monitored ECSs and a list of the top 5 ECSs, ranked by their CPU usage over the last 5 minutes.

Clicking an ECS takes you to the corresponding **Basic Monitoring** page.

Network Monitoring

Displays the outbound bandwidth and inbound bandwidth of the current EIP and bandwidth in the last 1 hour.

- Inbound bandwidth: indicates the network rate of inbound traffic.
- Outbound bandwidth: indicates the network rate of outbound traffic.

Storage Monitoring

Displays usages of all EVS disks in the last five minutes by listing the total read and write bandwidth in addition to the total quantity of read and write IOPS.

Full Screen

You can view various information, such as alarm statistics, event monitoring, and ECS monitoring on a full screen.

2 Querying Metrics of a Cloud Service

Cloud Eye provides multiple built-in metrics based on the characteristics of each service. After you enable one cloud service on the cloud platform, Cloud Eye automatically associates its built-in metrics. You can track the cloud service status by monitoring these metrics.

This topic describes how to view monitoring data of a cloud service resource.

NOTE

For services that support enterprise projects, the system displays, by default, the host list of the enterprise projects on which you have permissions.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring**, and select a cloud service.

The cloud service page is displayed.


4. Locate the row that contains the cloud service resource you want to monitor and click **View Graph** in the **Operation** column.

The detailed monitoring page is displayed.

You can view graphs based on raw data collected in the last **1h**, **3h**, **12h**, **1d**, and **7d**. In the upper right corner of the graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed. You can also enable **Auto Refresh** to view the real-time data refreshed every minute.


 **NOTE**

- Metric units can be changed between byte or byte/s and GB or GB/s on graphs. When you are changing the unit, if the maximum value of a metric is smaller than 10^5 , both the maximum value and the minimum value of this metric are 0. In addition, all data displayed on the graph is 0.
- If **Auto Refresh** is enabled, data is automatically refreshed every minute.
- You can search for a specific metric in the search box.
- Some cloud services allow you to view resource details. You can click **View Resource Details** in the upper part of the page to view details about monitored resources.

5. Hover your mouse over a graph and click  in the upper right corner. An enlarged graph of the metric is displayed, on which you can view the metric monitoring details for longer time ranges. In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. You can also view historical monitoring data for any period during the last six months by customizing the monitoring period in the upper right corner of the graph.

 **NOTE**

- If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data. For details about the rollup period, see [What Is Rollup?](#)
- If you select **7d** or **30d**, aggregated data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data.

6. In the upper right corner of the graph, click  to create alarm rules for the metric.
7. To export data, click **Export Data** on the **Cloud Service Monitoring** page, configure parameters as prompted, and click **Export**. For details, see [How Do I Export Collected Data?](#)

3 Using Server Monitoring

Server monitoring includes basic monitoring, process monitoring, and OS monitoring for servers.

- Basic monitoring provides Agent-free monitoring for basic ECS or BMS metrics.
- OS monitoring provides proactive and fine-grained OS monitoring for servers, and it requires the Agent (a plug-in) to be installed on all servers that will be monitored.
- Process monitoring provides monitoring of active processes on hosts.

NOTE

Agent access statement: After the Agent is installed, it collects and reports server monitoring data to the Cloud Eye service. When you update the Agent software package, Cloud Eye accesses the software package repository address to update the software. In addition to the preceding behaviors, the Agent does not access any other addresses.

Functions

- **Various Metrics**
Server monitoring provides more than 40 metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers.
- **Fine-grained Monitoring**
After the Agent is installed, the metrics collected by the Agent are reported every minute.
- **Process Monitoring**
CPU usage, memory usage, and number of opened files used by active processes are monitored to help you better understand the resource usages on ECSs and BMSs.

Using Server Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.

4. Select the target ECS or BMS and install the Agent on it.
 - a. Change the DNS server address of and add security group rules to the target ECS or BMS. For details, see [Modifying the DNS Server Address and Adding Security Group Rules \(Linux\)](#) or [Modifying the DNS Server Address and Adding Security Group Rules \(Windows\)](#).
 - b. Install the Agent. For details, see [Installing the Agent on a Linux Server](#) or [Installing and Configuring the Agent \(Windows\)](#).
5. After 5 minutes, check whether the Agent status is **Running**.
If yes, the Agent has been installed successfully.

On the right of the ECS, click **View Metric** in the **Operation** column to view the monitoring data.

4 Using Custom Monitoring


The **Custom Monitoring** page displays all custom metrics reported by users. You can use simple API requests to report collected monitoring data of those metrics to Cloud Eye for processing and display.

For details about how to add monitoring data, see [Adding Monitoring Data](#).

Viewing Custom Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. On the **Custom Monitoring** page, view the data reported by yourself through API requests, including custom services and metrics.
5. Locate the row that contains the target cloud service resource and click **View Metric** in the **Operation** column.

On the page displayed, you can view graphs based on raw data collected in **1h**, **3h**, and **12h**. In the upper right corner of each graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed.

6. If you want to view metric details, hover your mouse over a graph and click  in the upper right corner.

In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. To view historical monitoring data for any period during the last six months, customize the monitoring period by setting **Select Range** in the upper right corner.

In the upper left corner of the graph, click **Settings** to configure the rollup method.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. Locate the target cloud service resource and click **Create Alarm Rule** in the **Operation** column.

5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.

After you create the alarm rule, if the custom metric data reaches the threshold, Cloud Eye immediately notifies you through SMN that an exception has occurred.

5 Using Event Monitoring

You can query system events and custom events reported to Cloud Eye through the API. You can create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for you.

Events are key operations on cloud service resources that are stored and monitored by Cloud Eye. You can view events to see operations performed by specific users on specific resources, such as deleting or rebooting an ECS.

Event monitoring is enabled by default. You can view monitoring details about system events and custom events. For details about the supported system events, see [Events Supported by Event Monitoring](#).

Event monitoring provides an API for reporting custom events, which helps you collect and report abnormal events or important change events generated by services to Cloud Eye. For details about how to report custom events, see [Reporting Events](#).

The differences between monitoring of custom events and [custom monitoring](#) are as follows:

- Monitoring of custom events is used to report and query monitoring data for non-consecutive events, and generate alarms in these scenarios.
- Custom monitoring is used to report and query periodically and continuously collected monitoring data, and generate alarms in these scenarios.

Viewing Event Monitoring Graphs

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
On the page displayed, all system events and custom events of the last 24 hours are displayed by default.
4. Select an event and click **View Graph** in the **Operation** column.

Creating an Alarm Rule

1. Log in to the management console.

2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
4. In the event list, locate the event and click **Create Alarm Rule** in the **Operation** column.
5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.

After you create the alarm rule, if the metric data reaches the threshold, Cloud Eye immediately notifies you through SMN that an exception has occurred.

6 Using Resource Groups

Scenarios

- **Resource Management**
If you use multiple cloud services, you can add all related resources, such as ECSs, BMSs, EVS disks, elastic IP addresses, bandwidths, and databases to the same resource group for easier management and O&M.
- **Routine Inspection and Quick Fault Locating**
On the details page of a resource group, you can view the resource overview, unhealthy resources, alarm rules, and alarm records. This feature helps you view cloud resource usage and quickly locate faulty resources.

Functions

- Resource groups enable you to manage your cloud resources across products.
- The unhealthy resource list enables you to quickly locate faults.
- The alarm records help you track the overall service status.

Using Resource Groups

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Resource Groups**.
4. In the upper right corner, click **Create Resource Group**. On the page displayed, enter a group name as prompted.
5. Select the target cloud service resources.
6. Click **Create**.

For details about how to create and manage resource groups, see [Introduction to Resource Groups](#).

7 Creating an Alarm Rule

Scenarios

The alarm function provides the alarm service for monitoring data. By creating alarm rules, you define how the alarm system checks monitoring data and sends alarm notifications when metric data meets alarm policies.

After creating alarm rules for important metrics, you can timely know metric data exceptions and quickly rectify the faults.

Functions

- Alarm rules can be created for all monitoring items on Cloud Eye.
- Alarm rules can be created for all resources, resource groups, log monitoring, custom monitoring, event monitoring, and website monitoring.
- You can set validity periods of alarm rules, that is, customize the time when alarm rules take effect.
- Notifications can be sent by email, text message, or HTTP/HTTPS message.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**, and click **Create Alarm Rule** in the upper right corner.
4. On the **Create Alarm Rule** page, configure the parameters.
 - a. Set the alarm rule name and description.


Table 7-1 Name and Description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: alarm-b6a1

Parameter	Description
Description	(Optional) Provides supplementary information about the alarm rule.

- b. Select a monitored object and configure alarm content parameters.

Table 7-2 Alarm Content parameters

Parameter	Description	Example Value
Alarm Type	Specifies the alarm type to which the alarm rule applies. The value can be Metric or Event .	Metric
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server (ECS)
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitoring Scope	<p>The monitoring scope of an alarm rule can be All resources, Resource groups, or Specified resources.</p> <p>NOTE</p> <ul style="list-style-type: none"> If you select All resources, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources. If Resource groups is selected and any resource in the group meets the alarm policy, an alarm is triggered. If you select Specific resources, select one or more resources and click  to add them to the box on the right. 	All resources
Method	<p>There are three options: Associate template, Use existing template, and Configure manually.</p> <p>NOTE</p> <p>After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.</p>	Create manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A

Parameter	Description	Example Value
Alarm Policy	<p>Specifies the policy for triggering an alarm. If you set Resource Type to Custom Monitoring, or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods.</p> <p>If you set Resource Type is to Event Monitoring, the event that triggers the alarm is an instant event. For example, if event improper ECS running occurs, Cloud Eye triggers an alarm.</p> <p>NOTE A maximum of 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.</p>	N/A
Alarm Severity	Specifies the alarm severity, which can be Critical, Major, Minor, or Informational.	Major

c. Configure the alarm notification.

Figure 7-1 Alarm Notification parameters

Table 7-3 Alarm Notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.

Parameter	Description
Notification Object	<p>Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic.</p> <ul style="list-style-type: none"> • Account contact is the mobile number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.
Validity Period	<p>Cloud Eye sends notifications only within the notification window you specified.</p> <p>If Validity Period is set to 08:00-20:00, Cloud Eye sends notifications only within 08:00-20:00.</p>
Trigger Condition	<p>Specifies the condition for triggering the alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.</p>

d. Configure the **Enterprise Project** and **Tag**.

Figure 7-2 Advanced Settings

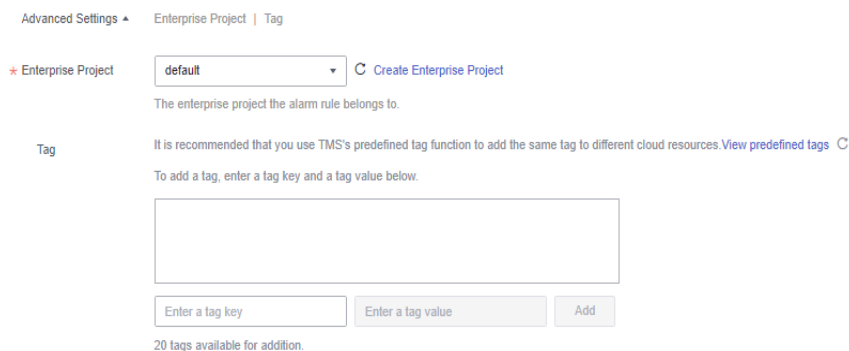


Table 7-4 Name and Description

Parameter	Description
Enterprise Project	<p>Specifies the enterprise project that the alarm rule belongs to. Only users who have all permissions for the enterprise project can view and manage the alarm rule. For details about how to create an enterprise project, see Creating an Enterprise Project.</p>

Parameter	Description
Tag	<p>A tag consists of a key-value pair. Tags can be used to categorize and search for your resources. You are advised to create predefined tags in TMS. For details, see Creating Predefined Tags.</p> <p>If your organization has configured tag policies for Cloud Eye, follow the policies when configure Tag for an alarm rule. If the tag configured does not comply with the tag policies, alarm rules may fail to be created. In this case, you can contact your administrator to learn more about the tag policies.</p> <ul style="list-style-type: none">• A key can contain up to 128 characters, and a value can contain up to 225 characters.• You can create up to 20 tags.

- e. Click **Create**.

After the alarm rule is created, if the metric data reaches the specified threshold, Cloud Eye immediately informs you that an exception has occurred.