

**Cloud Eye**

# **Getting Started**

<b>Issue</b>	01
<b>Date</b>	2025-09-11



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Resource Monitoring.....1**

1.1 Quickly Building Server Monitoring Capabilities..... 1

1.2 Monitoring Large-scale Resources..... 7

**2 Visualization..... 12**

2.1 Creating Graphs on a Custom Dashboard..... 12

# 1 Cloud Resource Monitoring

[1.1 Quickly Building Server Monitoring Capabilities](#)

[1.2 Monitoring Large-scale Resources](#)

## 1.1 Quickly Building Server Monitoring Capabilities

### Scenarios

In the actual O&M process of cloud computing, server monitoring is of great importance. To better monitoring servers, you can install the Agent on cloud servers created from Huawei Cloud public images. Then, you can view visualized server monitoring data and configure alarms for key service metrics. This section uses an ECS as an example to describe how to set alarm rules for CPU usage.

### Procedure

Procedure	Description
<a href="#">Preparations</a>	Purchase an ECS. Check that the ECS is displayed in the server monitoring list on Cloud Eye.
<a href="#">Step 1: Install the Agent on the ECS</a>	Install the Agent on the ECS to report monitoring metrics.
<a href="#">Step 2: View ECS Monitoring Metrics</a>	View key metric data.
<a href="#">Step 3: Create an Alarm Rule to Monitor an ECS</a>	Set custom alarm rules for specific monitoring metrics.
<a href="#">Step 4: View Alarm Records</a>	When an alarm condition is met, Cloud Eye invokes SMN APIs to send notifications. You can also view the alarm information in alarm records.

Procedure	Description
<a href="#">Follow-up Operation: Masking Alarm Notifications</a>	Create a masking rule to mask alarm notifications if needed.

## Preparations

Purchase an ECS. Ensure that this ECS is displayed in the server monitoring list on Cloud Eye.

## Step 1: Install the Agent on the ECS

Both basic monitoring metrics and OS monitoring metrics of the ECS will be reported. Basic ECS monitoring metrics are collected every 5 minutes and reported by the ECS. OS monitoring metrics are reported only after the Agent is installed on the ECS. These metrics are reported by Cloud Eye every one minute and provide more accurate details. Moreover, the monitoring is more comprehensive, so you are advised to install the Agent on your ECSs.

The following describes how to install the Agent.

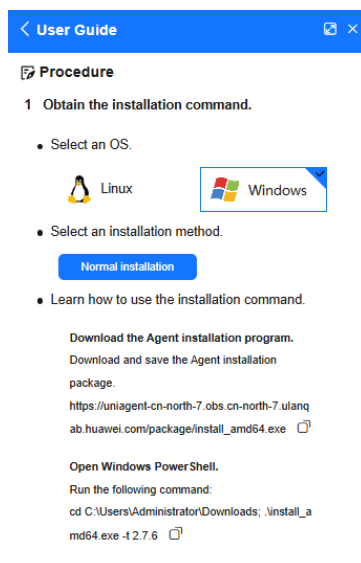
The Agent installation method depends on the OS.

## Installing the Agent on a Windows ECS

For a Windows ECS, you can only install the Agent manually. There are two methods for you to find the installation instructions.

- On the **Server Monitoring** page of the Cloud Eye console, locate an ECS and click **Install Manually** to view the instructions. Then, log in to the ECS and install the Agent.

**Figure 1-1** Agent installation guide



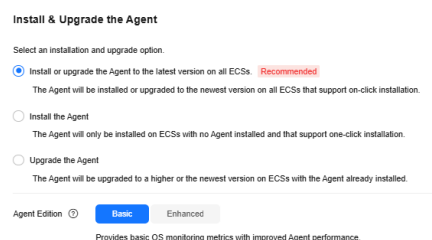
- Refer to the official document to [install the Agent](#).

## Installing the Agent on a Linux ECS

You can install the Agent on one or more Linux ECSs at a time.

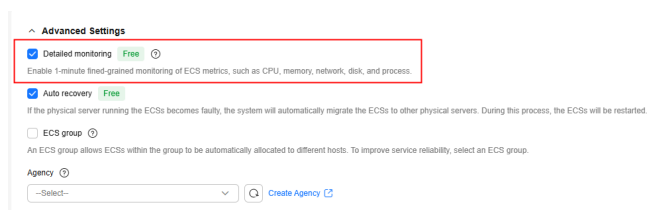
- For ECSs that support one-click installation, you can batch install the Agents for them on the console, which is more efficient.

**Figure 1-2** Installing and upgrading the Agent



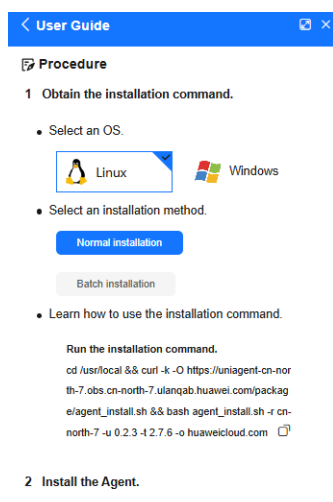
- For certain ECSs, you can enable Cloud Eye monitoring when you purchase them. The Agent will be installed automatically. For details, see [Purchasing and Using a Linux ECS](#).

**Figure 1-3** Enabling detailed monitoring



- For Linux ECSs that do not support one-click installation, you can manually install the Agents for them one by one or in batches. After you click **Install Manually** above the server list, the installation guide will be displayed.

**Figure 1-4** Agent installation guide



After the Agent is installed, you can view it in the server monitoring list. If the **Agent Status** of an ECS is **Running**, the Agent is installed for the ECS.

Figure 1-5 Viewing Agent status

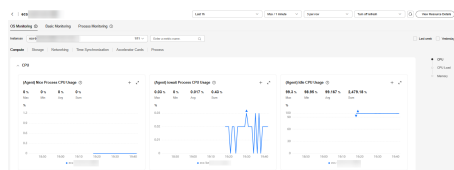


Search	IP Address	ECS ID	Agent Status	Agent ID	CPU%	Mem%	Swap%	OS	Instance Type	Tag	AZ	Private IP	Operation
	192.168.1.101	ECS-1	Running	2781	0.0%	0.0%	0.0%	Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.101	View Metric
	192.168.1.102	ECS-2	Running	2782	0.0%	0.0%	0.0%	Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.102	View Metric
	192.168.1.103	ECS-3	Stopped					Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.103	View Metric

## Step 2: View ECS Monitoring Metrics

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
5. Locate the target ECS and click **View Metric** in the **Operation** column to view the OS monitoring metrics, basic monitoring metrics, and process monitoring metrics.

Figure 1-6 OS monitoring



The OS monitoring and basic monitoring metrics are displayed on the metric details page. OS monitoring requires that the Agent be installed. If no OS monitoring metrics are displayed, install the Agent first.

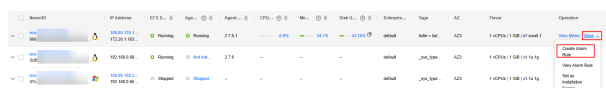
## Step 3: Create an Alarm Rule to Monitor an ECS

After purchasing an ECS, you can configure an alarm rule to monitor key service metrics of the ECS.

Cloud Eye provides a quick entry for creating alarm rules to monitor ECS or BMS metrics. This step describes how to set parameters for creating an alarm rule. For more information, see [Creating an Alarm Rule to Monitor a Server](#).

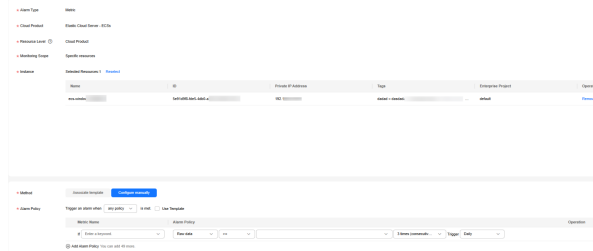
1. On the **Server Monitoring** page, locate an ECS and choose **More** > **Create Alarm Rule** in the **Operation** column.

Figure 1-7 Creating an alarm rule



Search	IP Address	ECS ID	Agent Status	Agent ID	CPU%	Mem%	Swap%	OS	Instance Type	Tag	AZ	Private IP	Operation
	192.168.1.101	ECS-1	Running	2781	0.0%	0.0%	0.0%	Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.101	View Metric
	192.168.1.102	ECS-2	Running	2782	0.0%	0.0%	0.0%	Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.102	View Metric
	192.168.1.103	ECS-3	Stopped					Linux	ecs.g5.xlarge	default	cn-north-1	192.168.1.103	View Metric

2. Set parameters. The alarm type, cloud product, resource level, monitoring scope, and monitored instance are preset.

**Figure 1-8** Creating an alarm rule to monitor a server**Table 1-1** Parameters for configuring an alarm rule for an ECS

Parameter	Example Value	Description
Alarm Type	Metric	Alarm type that the alarm rule applies to. The value cannot be changed.
Cloud Product	Elastic Cloud Server - ECSs	Name of the service for which the alarm rule is configured. The value cannot be changed.
Resource Level	Cloud product	A cloud product has many specific dimensions. If you set <b>Resource Level</b> to <b>Cloud product</b> , metrics across dimensions can be configured in the same alarm rule. If you set it to <b>Specific dimension</b> , only metrics of the specified dimension can be configured in the same alarm rule The value cannot be changed.
Monitoring Scope	Specific resources	Monitoring scope the alarm rule applies to.
Method	Configure manually	Select a rule triggering method.
Metric Name	ECSs - Process - ProcessIDs / (Agent)Process CPU Usage	Select a metric for triggering alarms.
Alarm Policy	If the metric value is greater than or equal to 80% for three consecutive times, an alarm is generated once every day.	Policy for triggering an alarm. <b>NOTE</b> If the alarm is not cleared after it is generated, an alarm is reported every day.
Alarm Severity	Major	Severity of alarms.

3. Configure alarm notifications. For details, see [Creating an Alarm Rule and Notifications](#).

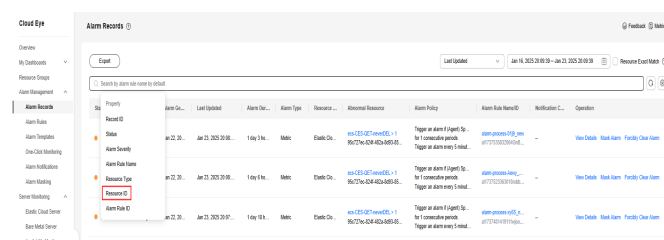
**Table 1-2** Parameters for configuring alarm notifications

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Select an alarm notification mode.
Recipient	Account contact	<ul style="list-style-type: none"><li>If you select <b>Topic subscriptions</b> for <b>Notified By</b>, select one or more notification recipients.</li><li>If <b>Recipient</b> is set to <b>Account contact</b>, notifications will be sent to the registered phone number and email address.</li></ul>
Notification Window	00:00–23:59	<ul style="list-style-type: none"><li>If <b>Notified By</b> is set to <b>Topic subscriptions</b>, you need to set the notification window.</li><li>Cloud Eye sends notifications only within the specified time period.</li></ul>
Trigger Condition	Generated alarm, Cleared alarm	This parameter is available when <b>Notified By</b> is set to <b>Topic subscriptions</b> or <b>Notification groups</b> . You can select <b>Generated alarm</b> , <b>Cleared alarm</b> , or both.

- After the configuration is complete, view the alarm rule in the alarm rule list.

## Step 4: View Alarm Records

After receiving an alarm notification, you can search for the alarm in the alarm records by resource ID.

**Figure 1-9** Viewing alarm records

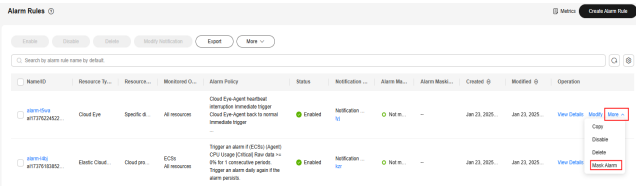
## Follow-up Operation: Masking Alarm Notifications

If you do not need to receive notifications after an alarm is triggered, you can mask the alarm using a masking rule. After the masking rule is applied, only alarm records are generated.

- Log in to the management console.
- Choose **Service List > Cloud Eye**.

- 3. In the navigation pane, choose **Alarm Management > Alarm Rules**.
- 4. On the **Alarm Rules** page, locate the row containing the alarm rule to be masked, click **More** in the **Operation** column, and select **Mask Alarm**. In the displayed **Create Alarm Masking** dialog box, configure **Alarm Masking Duration** and click **OK**.

Figure 1-10 Masking an alarm rule



Related Information

For details about parameters for creating an alarm rule, see [Creating an Alarm Rule and Notifications](#).

You can mask alarm notifications for a resource or some alarm policies of the resource. For details, see [Creating a Masking Rule](#).

Cloud Eye also provides the one-click monitoring for key monitoring metrics. For details, see [One-Click Monitoring](#).

1.2 Monitoring Large-scale Resources

Scenarios

For organizations or enterprises with a large number of resources, manual maintenance can lead to errors. Moreover, resources used in different production phases may need to manage separately. For instance, resources used for testing and production should be managed separately, with different configurations for alarm rules, notification methods, and recipients. Cloud Eye allows you to manage alarm rules and graphs by instance name, tag, and enterprise project, greatly simplifying O&M.

Procedure

Procedure	Description
<a href="#">Preparations</a>	Prepare required resources, with tags or enterprise projects set as needed.
<a href="#">Step 1: Create a Resource Group</a>	Group cloud resources.
<a href="#">Step 2: View the Group Resource Overview</a>	View resources in a resource group.

Procedure	Description
<a href="#">Step 3: Associate a Resource Group with an Alarm Template</a>	Batch create alarm rules by creating resource groups and associating them with alarm templates.
<a href="#">Step 4: View Alarm Rules for the Resource Group</a>	View alarm rules for all resources in a resource group.
<a href="#">Step 5: Create Alarm Masking</a>	Create a masking rule to mask alarm notifications if needed.

## Preparations

Before configuring a resource group, ensure that you have set tags and enterprise projects for your resources as needed.

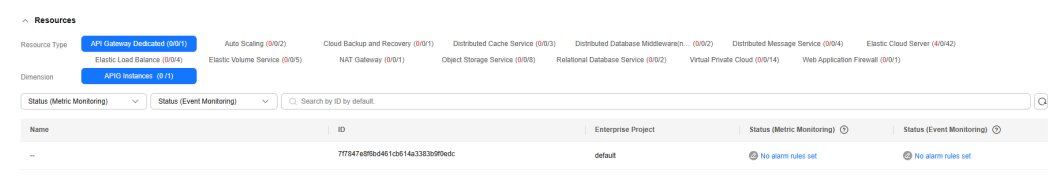
### Step 1: Create a Resource Group

Resources can be manually or automatically added to a resource group. If you select **Manually** for **Add Resources**, you can set **Resource Level** to **Cloud product** or **Specific dimension**. If **Automatically** is selected, you can match resources by instance name, enterprise project, tag, or multiple criteria. For more information, see [Creating a Resource Group](#).

### Step 2: View the Group Resource Overview

After the resource group is created, view its resource details.

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Choose **Service List > Cloud Eye**.
4. In the navigation pane, choose **Resource Groups**.
5. On the **Resource Groups** page, click the created resource group to view its resource details.
6. On the **Resource Overview** tab, you can view the basic information, matching rules, and resource details of the resource group.
  - a. In the **Resources** area, click a resource to view its graphs.
  - b. In the **Resources** area, select the **Status (Metric Monitoring)** and **Status (Event Monitoring)** filters, and search for resources by resource ID. Click **No alarm rules set** of a resource to go to the **Create Alarm Rule** page. Click **In Alarm** to go to the **Alarm Records** page and view the alarm results of the resource.



## Step 3: Associate a Resource Group with an Alarm Template

You can create a resource group and associate it with an alarm template to create alarm rules in batches, which improves alarm rule configuration efficiency.

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, choose **Resource Groups**.
5. On the **Resource Groups** page, locate the resource group and click **Associate Alarm Template** in the **Operation** column.
6. In the **Associate Alarm Template** dialog box, select an alarm template.

Figure 1-11 Associating an alarm template

The screenshot shows the 'Associate Alarm Template' dialog box. At the top, there is a warning message: 'After a resource group is associated with an alarm template, alarm rules are generated. If the template changes, the alarm policies for the alarm rules will be modified accordingly.' Below this, the 'Resource Groups' field is set to 'resource-group-6g4s02l'. The 'Template Name' field is 'alarmTemplate-as1toTuG' with a search icon and a 'Create Custom Template' link. The 'Alarm Notifications' toggle is turned on. There are three tabs: 'Notification policies' (selected), 'Notification groups', and 'Topic subscriptions'. Under 'Notification policies', there is a text description: 'You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy'. Below this, the 'Notification Policies' dropdown is set to '--Select--'. At the bottom, there are 'Cancel' and 'OK' buttons.

7. Configure alarm notifications. For details, see [Creating an Alarm Rule and Notifications](#).

Table 1-3 Parameters for configuring alarm notifications

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Select an alarm notification mode.
Recipient	Account contact	<ul style="list-style-type: none"><li>• If you select <b>Topic subscriptions</b> for <b>Notified By</b>, select one or more notification recipients.</li><li>• If <b>Recipient</b> is set to <b>Account contact</b>, notifications will be sent to the registered phone number and email address.</li></ul>
Notification Window	00:00–23:59	<ul style="list-style-type: none"><li>• If <b>Notified By</b> is set to <b>Topic subscriptions</b>, you need to set the notification window.</li><li>• Cloud Eye sends notifications only within the specified time period.</li></ul>

Parameter	Example Value	Description
Trigger Condition	Generated alarm, Cleared alarm, or both	This parameter is available when <b>Notified By</b> is set to <b>Topic subscriptions</b> or <b>Notification groups</b> . You can select <b>Generated alarm</b> , <b>Cleared alarm</b> , or both.

8. Select an enterprise project.

**Figure 1-12** Advanced settings



**Table 1-4** Configuring an enterprise project

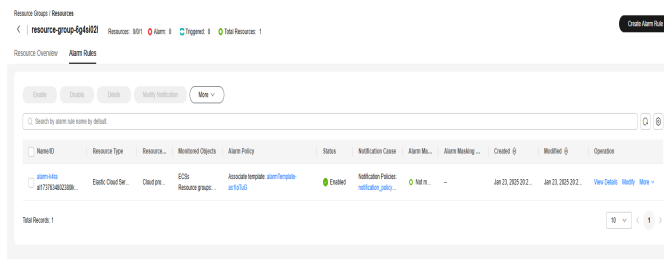
Parameter	Description
Enterprise Project	Enterprise project to which the alarm rule belongs. Only users with the enterprise project permissions can manage the alarm rule. To create an enterprise project, see <a href="#">Creating an Enterprise Project</a> .

9. Click **OK**.

## Step 4: View Alarm Rules for the Resource Group

After creating an alarm rule for a resource group, click the **Alarm Rules** tab in the upper left corner of the resource group details page to view the alarm rules created for all resources in the group.

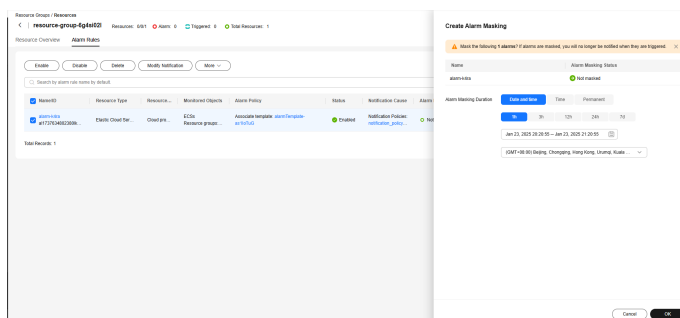
1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Choose **Service List > Cloud Eye**.
4. In the navigation pane, choose **Resource Groups**.
5. Click the name of the target resource group to go to the **Resources** tab page.
6. Click the **Alarm Rules** tab.
7. Locate an alarm rule, and click **View Details** in the **Operation** column to go to the **Alarm Records** page and view the alarm details of the resource.
8. In the **Operation** column of an alarm rule, click **Modify** to go to the **Modify Alarm Rule** page, and modify the alarm.



## Step 5: Create Alarm Masking

If you want to mask alarms for specified resources in a resource group, Cloud Eye allows you to quickly create a masking rule on the **Resources > Alarm Rules** page of the resource group.

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Choose **Service List > Cloud Eye**.
4. In the navigation pane, choose **Resource Groups**.
5. Click the name of the target resource group to go to the **Resources** tab page.
6. Click the **Alarm Rules** tab.
7. Locate the target alarm rule, and choose **More > Mask Alarm** in the **Operation** column. In the **Create Alarm Masking** dialog box, create an alarm masking rule. For details, see [Creating a Masking Rule](#).



# 2 Visualization

## 2.1 Creating Graphs on a Custom Dashboard

## 2.1 Creating Graphs on a Custom Dashboard

### Scenarios

In addition to the default dashboards, you can also create one with graphs of the desired type to display metric data. This section describes how to view the outband outgoing traffic rate of multiple ECSs on a custom dashboard. For more information, see [Custom Dashboards](#).

### Procedure

Procedure	Description
<a href="#">Preparations</a>	Ensure that you have required Cloud Eye permissions.
<a href="#">Step 1: Create a Dashboard</a>	Set the dashboard name and enterprise project to create a dashboard.
<a href="#">Step 2: Add a Graph</a>	Add graphs on the custom dashboard to monitor cloud services.
<a href="#">Step 3: View Graphs</a>	View the monitoring trend for selected metrics on the dashboard page.

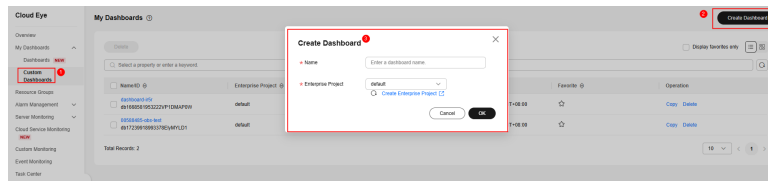
### Preparations

Ensure that you have obtained required Cloud Eye permissions and can create a custom dashboard.

### Step 1: Create a Dashboard

1. Log in to the management console.

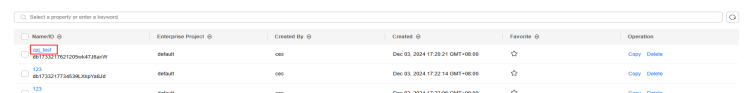
2. Choose **Service List > Cloud Eye**.
3. Choose **My Dashboards > Custom Dashboards**.
4. On the **My Dashboards** page, click **Create Dashboard**.



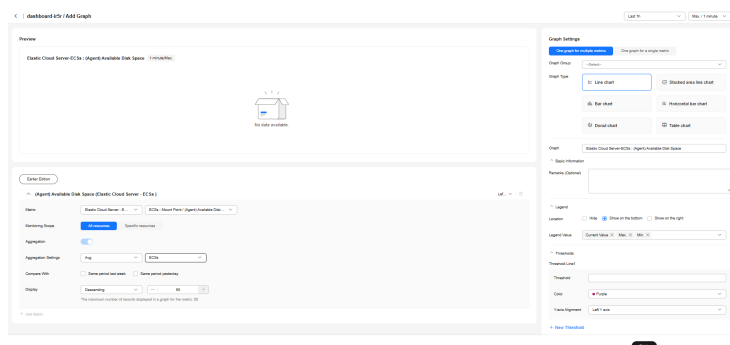
5. Enter a dashboard name, select an enterprise project, and click **OK**.

## Step 2: Add a Graph

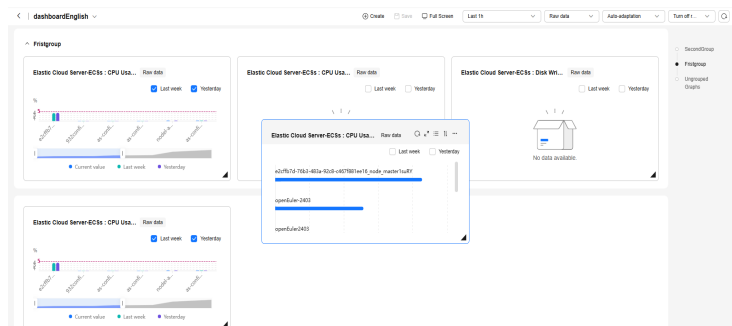
1. Log in to the management console.
2. Choose **Service List > Cloud Eye**.
3. Choose **My Dashboards > Custom Dashboards**.
4. Locate the dashboard for which you want to add a graph and click its name.



5. On the dashboard page, click **Create** to create a graph or graph group.
  - Graph: displays the trend or instantaneous values of selected metrics in different charts.
  - Graph group: Similar to a file directory, you can group graphs in a dashboard to different groups.
6. Click **Create Graph** and configure graph settings on the right of the page.
  - On the **Graph Settings** page, select **One graph for multiple metrics** and set **Graph Type** to **Line Chart**.
  - Set the legend position to **Show on the bottom** and **Legend Value** to **Current Value, Max., Min., Avg., and Sum**.
  - Set thresholds and threshold lines.
7. Select metrics in the lower part of the page.
  - **Metric:** Select **Elastic Cloud Server - ECSs > ECSs / Outband Outgoing Rate**.
  - **Monitoring Scope:** Select **All resources**.
  - **Aggregation Settings:** Select **Avg. > ECSs**.
  - **Display:** Select **Descending** and enter **50**.



- Click **Finish**. After the graph is created, you can drag it to a specified location or group.




#### NOTE

**Custom Dashboards** allows you to create graphs tailored to your O&M scenarios, helping you better manage cloud resources.

## Step 3: View Graphs

After adding a graph, you can view monitoring data in the default or custom time ranges.

- Log in to the management console.
- Choose **Service List > Cloud Eye**.
- Choose **My Dashboards > Custom Dashboards**.
- Click the name of the dashboard you created and view all graphs on it.
- Hover your mouse over a graph. In the upper right corner, click  to view monitoring details on an enlarged graph. Select a default time range or customize one to view the metrics.

**Figure 2-1** Viewing metric details

