Cloud Eye

User Guide

Issue 15

Date 2023-11-01

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 Overview

Overview consists of **Resource Monitoring** and **Website Monitoring**. You can learn about resource alarms of each cloud service and website response in real time.

Resource Monitoring

Resource Monitoring displays real-time alarms of each resource group and cloud service. You can view resource alarms in different dimensions to efficiently manage resources.

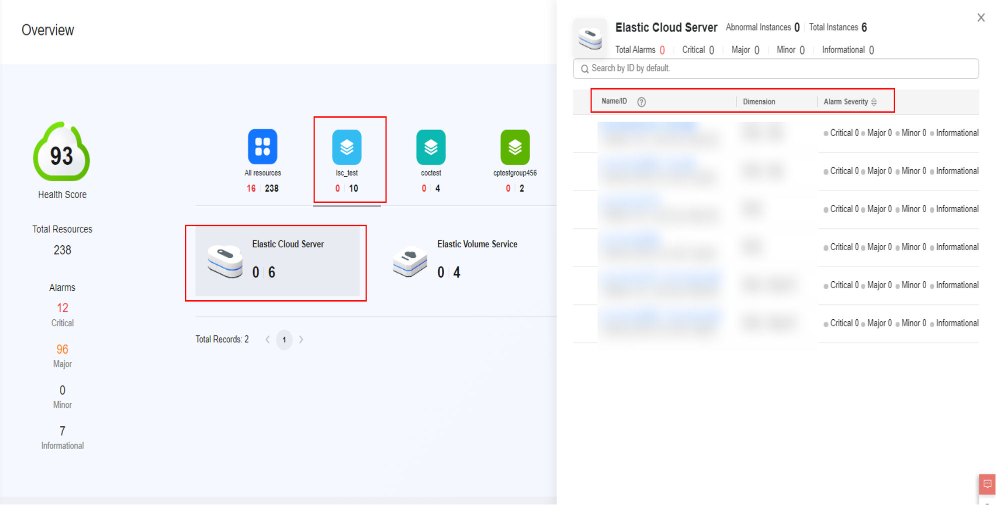
The following describes how you can use **Resource Monitoring**.

- On the left of **Resource Monitoring**, you can view the health score of all resources, total number of resources, and total number of resources with alarms are displayed. You can also view the number of resources of different alarm severities.

  NOTE

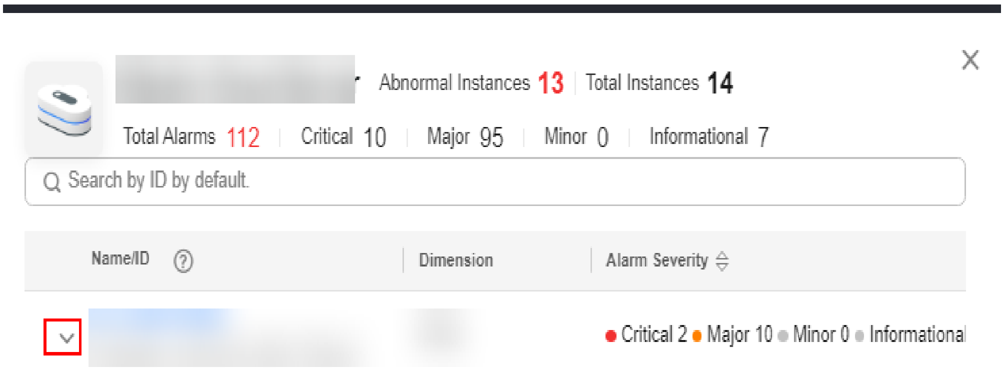
  Health score = Number of resources that have no alarms generated/Total resources

- You can select a resource group to view resources added to it. You can click a service name to view the name, dimension, and alarms of each resource.



Name/ID	Dimension	Alarm Severity
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational
[redacted]	[redacted]	Critical 0 Major 0 Minor 0 Informational

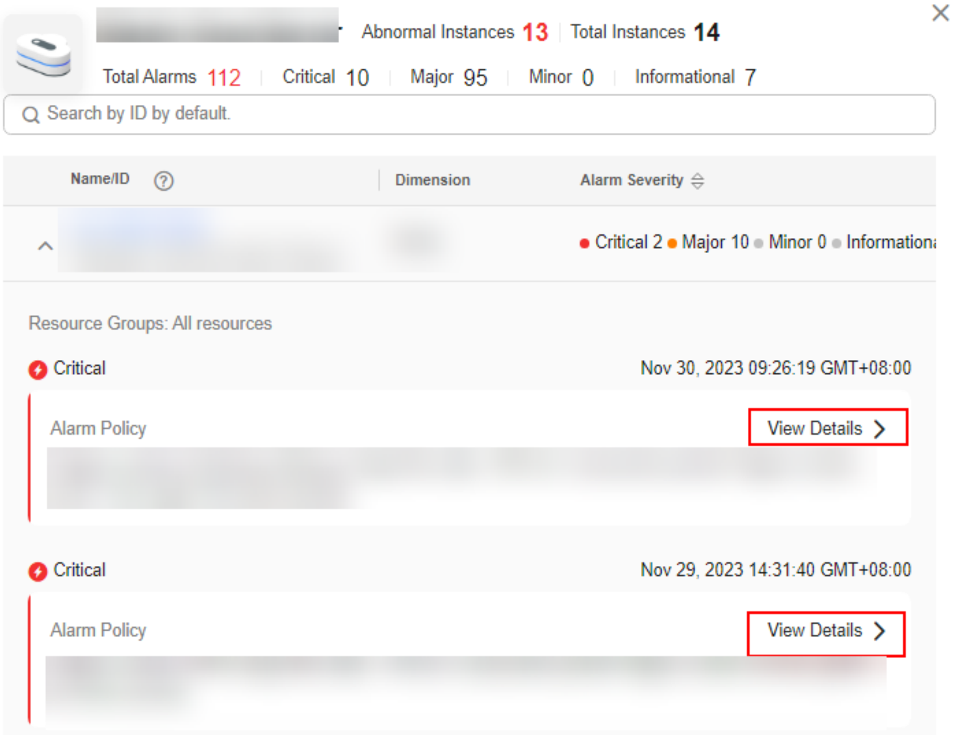
- When there are alarms generated, you can click ⌄ on the left of the resource name to expand the alarm policies.



Abnormal Instances 13 | Total Instances 14

Total Alarms 112 | Critical 10 | Major 95 | Minor 0 | Informational 7

- To view details, click **View Details**.



Abnormal Instances 13 | Total Instances 14

Total Alarms 112 | Critical 10 | Major 95 | Minor 0 | Informational 7

Resource Groups: All resources

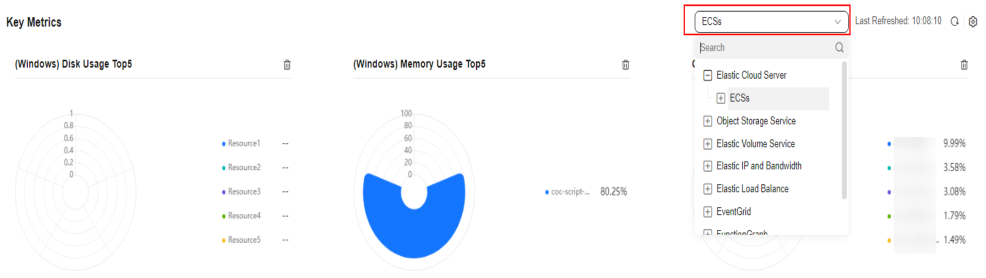
Critical Nov 30, 2023 09:26:19 GMT+08:00

Alarm Policy

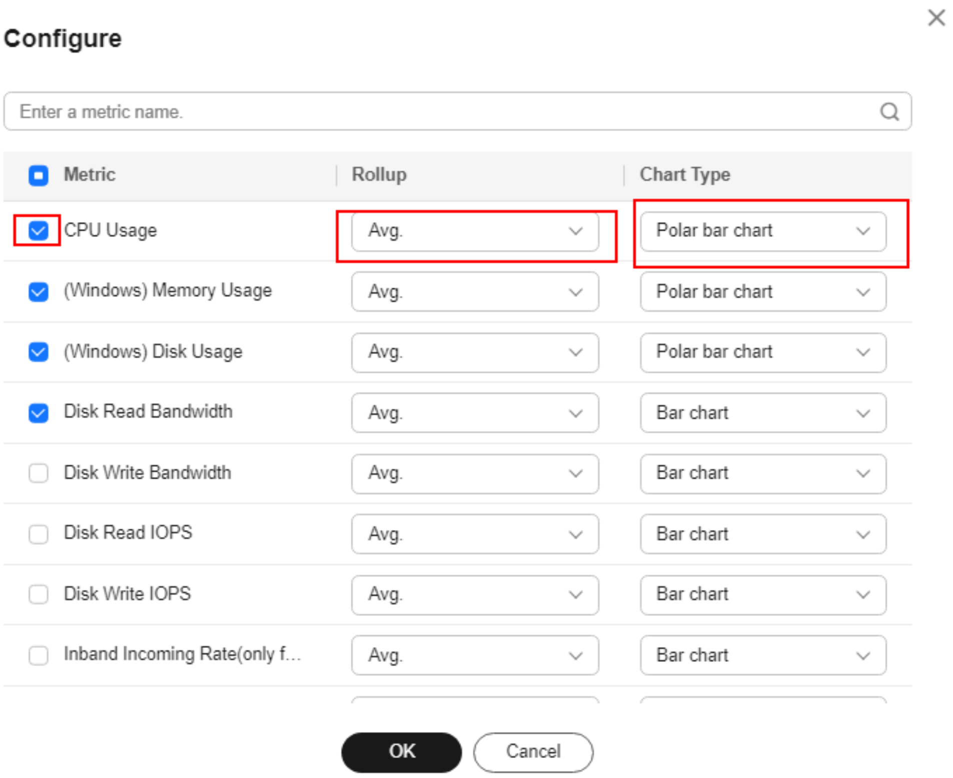
Critical Nov 29, 2023 14:31:40 GMT+08:00

Alarm Policy

- In the lower part of **Resource Monitoring**, you can view monitoring details of key metrics recommended by different services. In the selection box in the upper right corner, you can select a resource dimension to display resource details or select another resource to view its monitoring details.



- You can customize key metrics, rollup method, and chart type to display by clicking ⚙ in the upper right corner.



Configure

Enter a metric name.

■ Metric	Rollup	Chart Type
☑ CPU Usage	Avg.	Polar bar chart
☑ (Windows) Memory Usage	Avg.	Polar bar chart
☑ (Windows) Disk Usage	Avg.	Polar bar chart
☑ Disk Read Bandwidth	Avg.	Bar chart
□ Disk Write Bandwidth	Avg.	Bar chart
□ Disk Read IOPS	Avg.	Bar chart
□ Disk Write IOPS	Avg.	Bar chart
□ Inband Incoming Rate(only f...	Avg.	Bar chart

2 Dashboard (Earlier Version)

2.1 Introduction to Dashboards

Dashboards serve as custom monitoring platforms and allow you to view core metrics and compare the performance data of different services.

NOTE

Dashboards of the earlier version are used in the following regions: ME-Riyadh, AP-Jakarta, AF-Johannesburg, TR-Istanbul, and LA-Mexico City1.

2.2 Creating a Dashboard

You must create a dashboard before adding graphs. You can create a maximum of 10 dashboards.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Dashboards** > **Dashboards** and click **Create Dashboard**.

   The **Create Dashboard** dialog box is displayed.
4. Configure the following parameters:

- **Name**: Enter a maximum of 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
- **Enterprise Project**: If you associate a dashboard with an enterprise project, only users who have all permissions for the enterprise project can manage the dashboard.

  NOTE

  The enterprise project feature is available only in some regions.

5. Click **OK**.

2.3 Adding a Graph

After you create a dashboard, you can add graphs to it to monitor cloud services. Each dashboard supports up to 50 graphs.

You can add up to 50 metrics to one graph. Monitoring comparison between different services, dimensions, and metrics is supported.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Dashboards** > **Dashboards**, switch to the desired dashboard, and click **Add Graph**.

   The **Add Graph** dialog box is displayed.
4. Configure parameters based on **Table 2-1**.

Table 2-1 Graph parameters

Parameter	Description
Title	Specifies the title of the graph to be added. Only letters, digits, underscores (_), and hyphens (-) are allowed. Enter a maximum of 128 characters. Example value: **widget-axaj**
Enterprise Project	Specifies the enterprise project associated with the graph. You can view the monitoring data on the graph only when you have the enterprise project permissions.
Resource Type	Specifies the type of the resource to be monitored. Example value: **Elastic Cloud Server**
Dimension	Specifies the metric dimension. Example value: **ECSs**
Monitored Object	Specifies the monitored objects of the metric. You can select a maximum of 50 monitored objects at a time.

Parameter	Description
Metric	Specifies the metric name. Example value: **CPU Usage**

5. Click **Next: Configure Legend**.

   The graph title is displayed on the metric change curve in the monitoring graph. You can set the graph title as required, for example, ECS01-CPU usage. If the CPU usage is 10%, **ECS01 - CPU Usage: 10%** is displayed as the graph title.

   If you do not configure the graph title, the default title in the following format is displayed: monitored object (resource type) - metric: monitoring data. For example, if the CPU usage is 10%, **ECS01 (Elastic Cloud Server) - CPU Usage: 10%** is displayed as the graph title.

6. Click **OK**.

   On the selected dashboard, you can view the trends of the new graph. If you hover your mouse on the graph and click ⤡, you can view detailed metric data comparison.

2.4 Viewing a Graph

After you add a graph, you can view the metric trends on the **Dashboards** page. The system provides you both default and customizable time ranges to view trends from last month. This topic describes how to view trends for a longer time range.

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 **Dashboards** > **Dashboards**.

   You can view all graphs on the current dashboard.

   > NOTE
   >
   > - You can sort graphs by dragging them.
   > - You can click **1h**, **3h**, **12h**, **1d**, or **7d** in the upper part of graphs to switch the monitoring periods of all graphs on the dashboard. By default, raw metric data is displayed for **1h**, and the aggregated metric data is displayed for other periods.

4. Hover your mouse over a graph. In the upper right corner, click ⤡ to view monitoring details on an enlarged graph. You can select a period or customize a time range to view the metric trend in a specific monitoring interval.

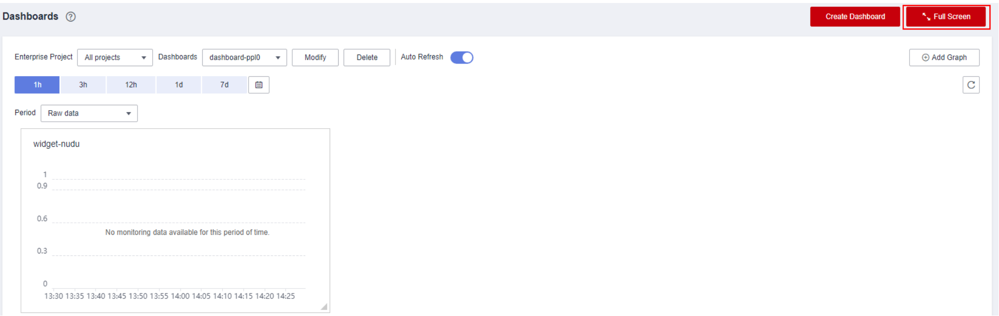
   Raw metric data is displayed for **1h**, **3h**, **12h**, and **1d** by default. For **7d** and **30d**, rolled-up data is displayed by default.

Using the Full Screen

The full screen displays metric data more clearly.

- To enter the full screen, click **Full Screen** in the upper right corner of the **Dashboard** page.
- To exit the full screen, click **Exit Full Screen** in the upper left corner of the page.

Figure 2-1 Full Screen



Enterprise Project All projects

Dashboards dashboard-ppl0

Auto Refresh

Period Raw data

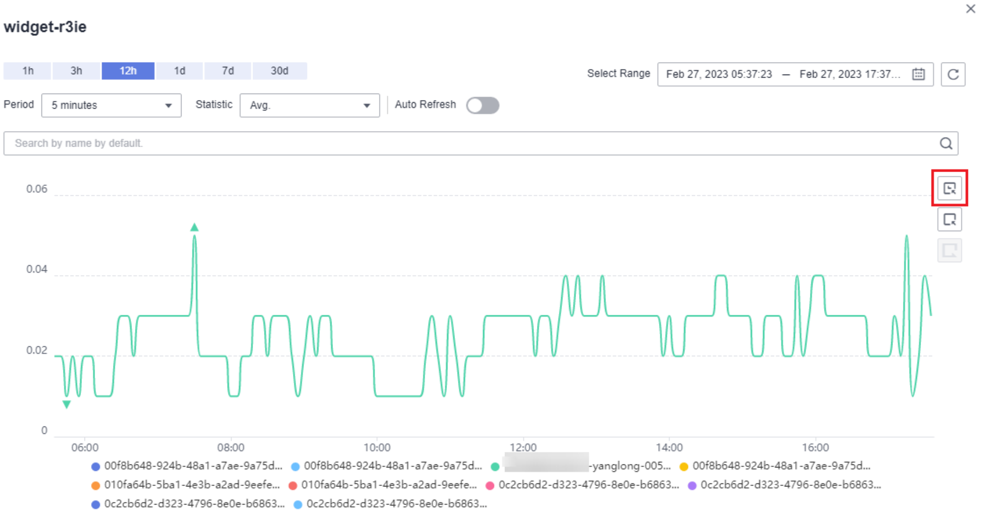
No monitoring data available for this period of time.

Customizing a Period to View the Graph

By default, metrics in the last 1 hour, last 3 hours, last 12 hours, last 24 hours, last 7 days, and last 30 days are displayed. If you want to view metrics in the last 2 hours or a customized time period, you can drag the mouse to select the time range you want to view on the X axis.

- To view metric details in a customized period, click the first icon on the right. Drag the mouse to select a customized time range. The system automatically displays the monitoring data in the selected time range.

Figure 2-2 Customizing a period


widget-r3ie
1h
3h
12h
1d
7d
30d
0.06
0.04
0.02
0
06:00
08:00
10:00
12:00
14:00
16:00
● 00f8b648-924b-48a1-a7ae-9a75d...
● 00f8b648-924b-48a1-a7ae-9a75d...
● [redacted]-yanglong-005...
● 00f8b648-924b-48a1-a7ae-9a75d...
● 010fa64b-5ba1-4e3b-a2ad-9eefe...
● 010fa64b-5ba1-4e3b-a2ad-9eefe...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...

Select Range Feb 27, 2023 05:37:23 – Feb 27, 2023 17:37...

Period 5 minutes

Statistic Avg.

Auto Refresh

Search by name by default.

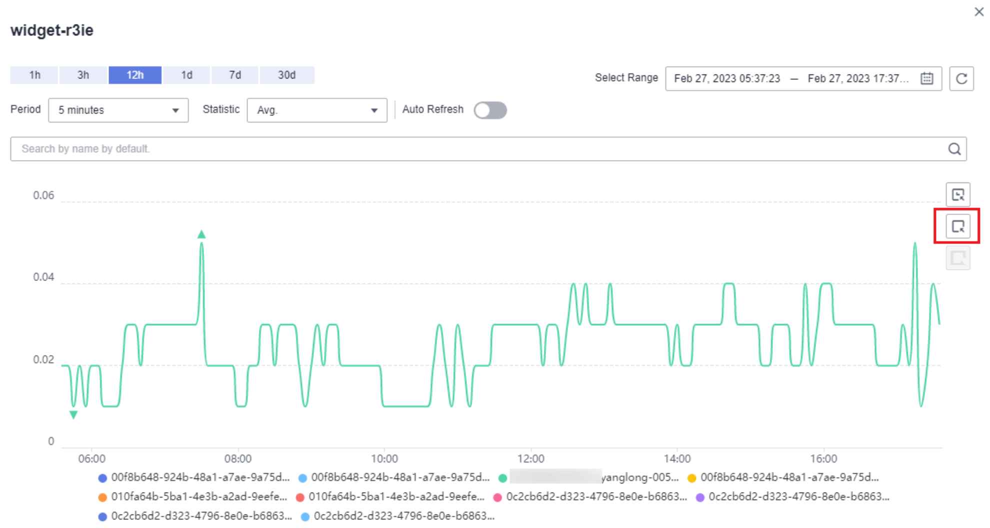
- To go back to the default graph, click the third icon on the right.

Selecting Monitoring Objects and Viewing Metrics

To compare the same metric of multiple resources, you can combine the metrics of the resources into a graph. When there are a large number of resources, you can drag to select monitored objects if you want to compare the metric data of only some of the resources.

- To select a monitored object, click the second icon on the right. Drag the mouse on part of the curve of the target monitored objects. Then, the system automatically displays the data of the selected monitored objects and hides the monitoring data of other monitored objects.

Figure 2-3 Selecting the object to be monitored



widget-r3ie

1h 3h 12h 1d 7d 30d

Select Range Feb 27, 2023 05:37:23 – Feb 27, 2023 17:37...

Period 5 minutes

Statistic Avg.

Auto Refresh

Search by name by default.

×
0.06
0.04
0.02
0
06:00
08:00
10:00
12:00
14:00
16:00
● 00f8b648-924b-48a1-a7ae-9a75d...
● 00f8b648-924b-48a1-a7ae-9a75d...
● [redacted]yanglong-005...
● 00f8b648-924b-48a1-a7ae-9a75d...
● 010fa64b-5ba1-4e3b-a2ad-9eefe...
● 010fa64b-5ba1-4e3b-a2ad-9eefe...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...
● 0c2cb6d2-d323-4796-8e0e-b6863...

- To go back to the default graph, click the third icon on the right.

NOTE

In the lower part of an enlarged graph, you can select a monitored object as follows: Click a resource object to hide its trend chart, and click the monitored object again to display its trend chart.

2.5 Configuring a Graph

This topic describes how to add, modify, and delete metrics on graphs.

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 **Dashboards** > **Dashboards**. Select the target dashboard and graph, and click the configure icon.

   On the displayed **Configure Graph** dialog box, you can edit the graph title and add new metrics. You can also delete or modify the current metrics.

   NOTE

   You can add up to 50 metrics to a graph.

2.6 Deleting a Graph

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 **Dashboards** > **Dashboards**.
4. Select the dashboard from which you want to delete a graph.
5. Hover your mouse on the target graph and click the trash icon in the upper right corner.
6. In the displayed **Delete Graph** dialog box, click **Yes**.

2.7 Deleting a Dashboard

To re-plan graphs on a dashboard, you can delete the dashboard. After that, all graphs on the dashboard will also be deleted.

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 **Dashboards** > **Dashboards**.
4. Select the dashboard to be deleted.
5. Click **Delete**.
6. In the displayed **Delete Dashboard** dialog box, click **Yes**.

3 Dashboards (New Version)

3.1 My Dashboards

3.1.1 Introduction

My Dashboards serves as a custom monitoring platform and allows you to view core metrics in all-in-one dashboard. You can also compare performance data of different services from different dimensions in one graph.

3.1.2 Creating a Dashboard

You must create a dashboard before adding graphs. You can create a maximum of 10 dashboards.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. Choose **Dashboards** > **My Dashboards** and click **Create Dashboard**.

   The **Create Dashboard** dialog box is displayed.
4. Configure the following parameters:
   - **Name**: Enter a maximum of 128 characters, including only letters, digits, underscores (_), and hyphens (-).
   - **Enterprise Project**: If you associate a dashboard with an enterprise project, only users who have all permissions for the enterprise project can manage the dashboard.

     NOTE

     Enterprise Project is available only in some regions.
5. Click **OK**.

3.1.3 Adding a Graph

After you create a dashboard, you can add graphs to it to monitor cloud services. You can add up to 50 graphs to each dashboard.

You can add up to 50 metrics to one graph. Monitoring comparison between different services, dimensions, and metrics is supported.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. Choose **Dashboards** > **My Dashboards**. Click the name of the dashboard to which you want to add a graph and click **Add Graph**.

   The **Add Graph** dialog box is displayed.
4. Select **Line Chart** or **Bar Chart** to display the graph.
   a. The line chart visualizes changes and peak values of metrics over time. Configure the parameters by referring to **Table 3-1**.

Table 3-1 Parameters in **Monitoring Item Configuration**

Item	Parameter	Description
Metric Display	One graph for a single metric	One or more graphs can be generated, and each shows only one same metric.
	One graph for multiple metrics	One graph with multiple metrics is generated.
Monitoring Scope	Select Resource and Metric	Select resources and metrics to be displayed in the line chart. For details about resource metrics, see **Services Interconnected with Cloud Eye**. **NOTE** If you select **One graph for a single metric** for **Metric Display**, you can select up to 24 metrics. If you select **One graph for multiple metrics** for **Metric Display**, the product of the number of resources and the number of metrics cannot exceed 50.
Advanced Settings	Graph Name	The graph name is displayed on the metric change curve. Default format: Monitored object-Dimension: Metric
	Threshold	Configure a threshold to generate an auxiliary line. Data points higher than the line are highlighted in red.
	Resource Type	Specifies the type of the resource to be monitored.

Item	Parameter	Description
	Dimension	Specifies the metric dimension.
	Metric	Specifies the metric name.

b. The bar chart visualizes the metrics of top-ranked resources of the same type. Configure the parameters by referring to **Table 3-2**.

Table 3-2 Parameters in **Monitoring Item Configuration**

Item	Parameter	Description
Metric Display	One graph for a single metric	One or more graphs can be generated, and each shows only one same metric.
Monitoring Scope	Select Resource and Metric	By default, all resources are selected for the bar chart. For details about resource metrics, see **Services Interconnected with Cloud Eye**.
Quantity	-	Metric data of selected resources is displayed. You can display the top 3 to 10 resources, in ascending or descending order. By default, metric data of top 3 instances are displayed in ascending order.
Advanced Settings	Graph Name	The graph name is displayed on the metric change curve. Default format: Monitored object-Dimension: Metric
	Threshold	Configure a threshold to generate an auxiliary line. Data points higher than the line are highlighted in red.
	Resource Type	Specifies the type of the resource to be monitored.
	Dimension	Specifies the metric dimension.
	Metric	Specifies the metric name.

5. Click **OK**.

   On the selected dashboard, you can view trends on the new graphs. Hover your mouse over a graph and click ⤡ to view detailed comparison of metric data.

3.1.4 Viewing a Graph

After adding a graph, you can view the metric trends on the **My Dashboards** page. The system provides you both default and customizable time ranges to view trends of the last seven days. This topic describes how to view trends for a longer time range.

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 **Dashboards** > **My Dashboards**.

   Click the name of the target dashboard and view all graphs on it.

   NOTE

   - You can drag a graph to adjust its display sequence to meet your monitoring requirements. You can also adjust the number of graphs displayed in each row as required.
   - You can configure the refresh interval for graphs on the dashboard. The default option for the refresh icon is **Close**.

4. Hover your mouse over a graph. In the upper right corner, click ⤡ to view monitoring details on an enlarged graph. You can select a period or customize a time range to view the metric trend in a specific monitoring interval.

   Raw metric data is displayed for the monitoring duration of one hour, three hours, 12 hours, and one day. Rolled-up data is displayed for the monitoring duration of seven days or more.

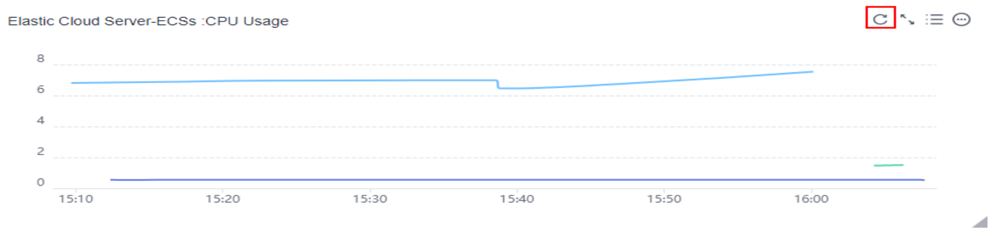
3.1.5 Configuring a Graph

This topic describes how to add, modify, and delete metrics on graphs.

Procedure for Line Charts

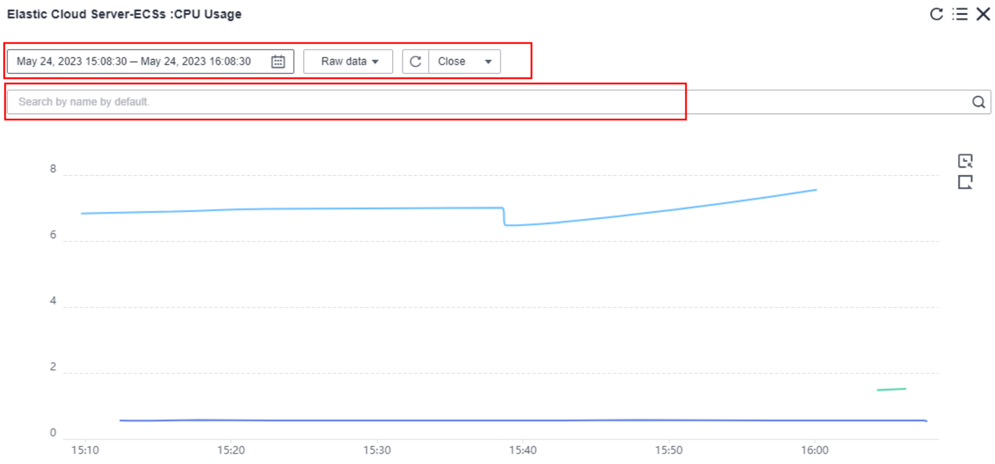
1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. In the navigation pane on the left, **Dashboards** > **My Dashboards**. On the displayed page, click the name of the dashboard to which you want to add a graph.
4. In the upper right corner of each graph, click ↻ to refresh the graph.

   Figure 3-1 Refreshing a graph

5. Click ⤡ to expand the graph. On the expanded graph, you can customize a time range for viewing metrics, select resources to be monitored, configure the refresh interval, and select different rollup methods to display metrics.

Figure 3-2 Viewing monitoring details in a line chart



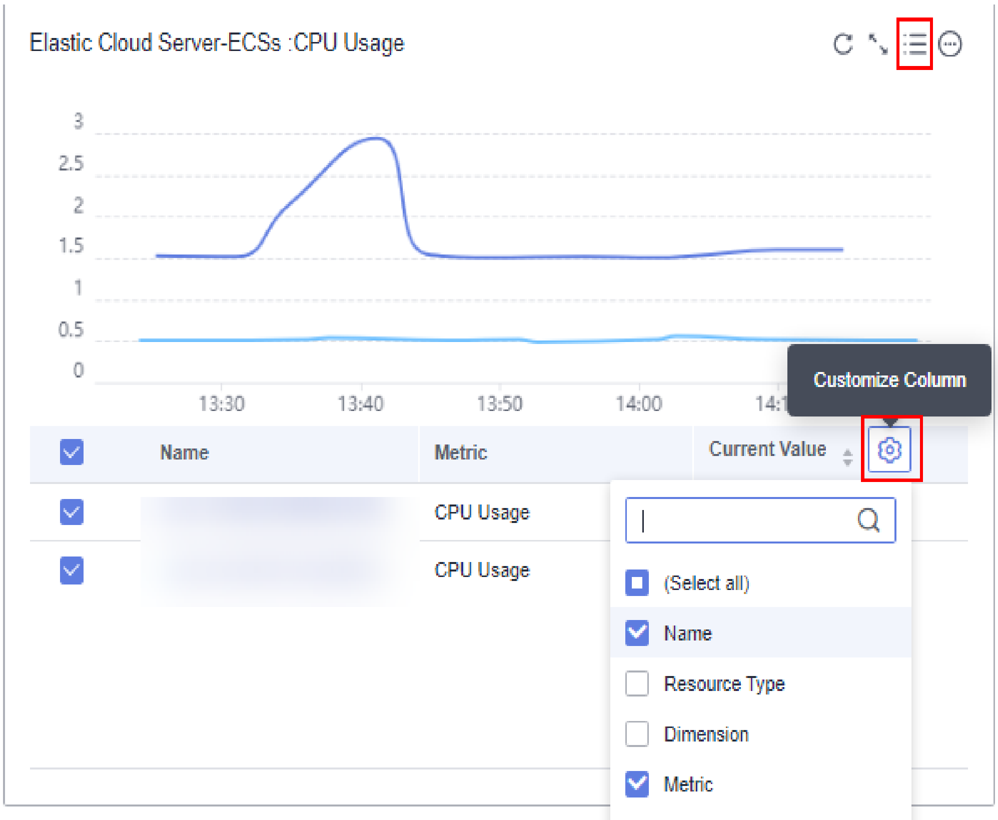
Elastic Cloud Server-ECSs :CPU Usage

May 24, 2023 15:08:30 – May 24, 2023 16:08:30 | Raw data ▾ | Close ▾

Search by name by default.

6. Click ☰ to display monitoring items of the graph. Click ⚙ to customize items to be displayed in this list.

Figure 3-3 View monitoring items



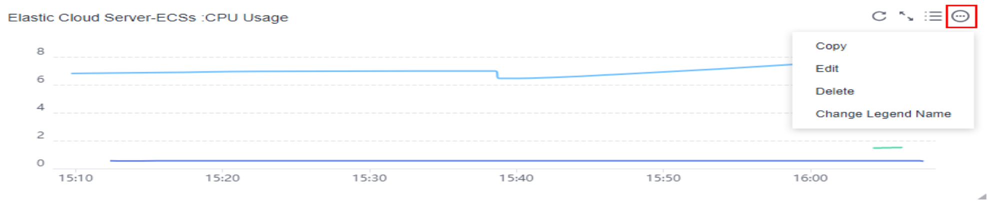
Elastic Cloud Server-ECSs :CPU Usage

☑	Name	Metric	Current Value
☑	[redacted]	CPU Usage	
☑	[redacted]	CPU Usage	

■ (Select all)
☑ Name
□ Resource Type
□ Dimension
☑ Metric

7. Click ⋯ to copy, edit, or delete a graph, or change a legend name.

Figure 3-4 Editing a graph



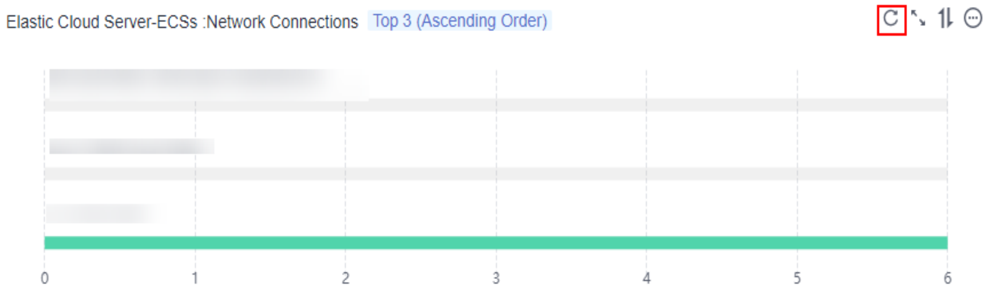
NOTE

A maximum of 20 monitoring items can be added to a graph.

Procedure for Bar Charts

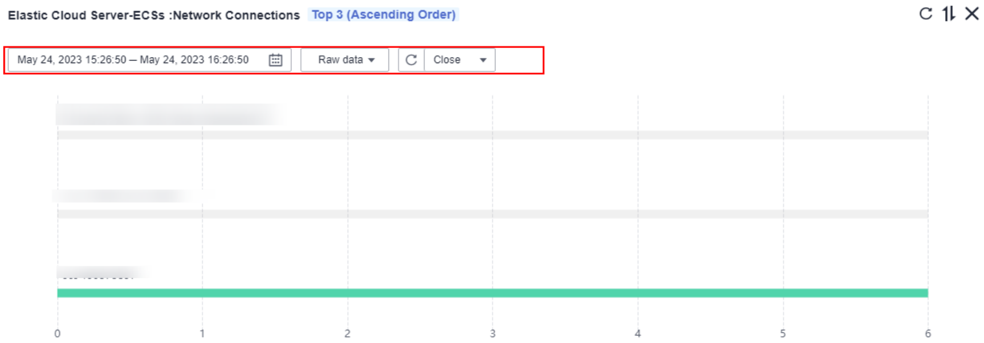
1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. In the navigation pane on the left, **Dashboards** > **My Dashboards**. On the displayed page, click the name of the dashboard to which you want to add a graph.
4. In the upper right corner of each graph, click ↻ to refresh the graph.

Figure 3-5 Refreshing a graph



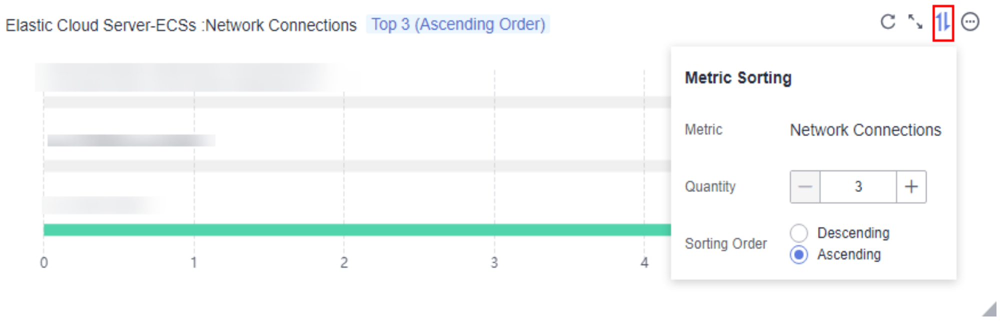
5. Click ⤡ to expand the graph. On the expanded graph, you can customize a time range for viewing metrics, select resources to be monitored, configure the refresh interval, and select different rollup methods to display metrics.

Figure 3-6 Viewing monitoring details in a bar chart


Elastic Cloud Server-ECSs :Network Connections
Top 3 (Ascending Order)
May 24, 2023 15:26:50 – May 24, 2023 16:26:50
Raw data
Close
0
1
2
3
4
5
6

6. Click ⇅ to configure **Quantity** and **Sorting Order**.

Figure 3-7 Sorting metrics



Elastic Cloud Server-ECSs :Network Connections Top 3 (Ascending Order)

Metric Sorting

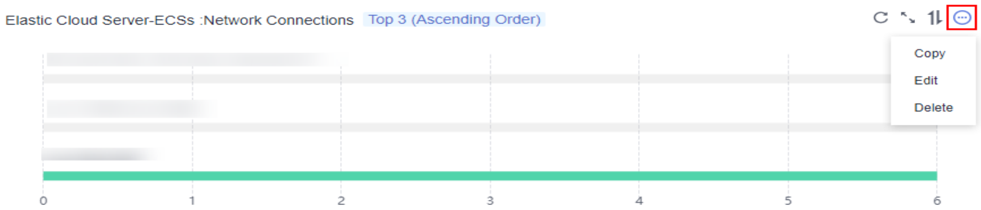
Metric: Network Connections

Quantity: − 3 +

Sorting Order: ○ Descending ● Ascending

7. Click ⋯ to copy, edit, or delete a graph.

Figure 3-8 Editing a graph

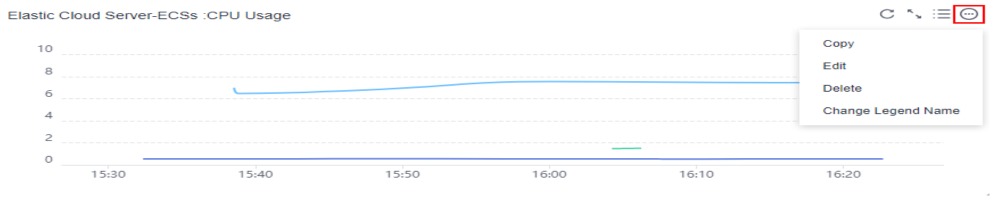


Elastic Cloud Server-ECSs :Network Connections Top 3 (Ascending Order)

3.1.6 Deleting a Graph

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, choose **Dashboards** > **My Dashboards**.
4. Select a dashboard from which you want to delete a graph and click the dashboard name.
5. Click ⋯ and choose **Delete**.

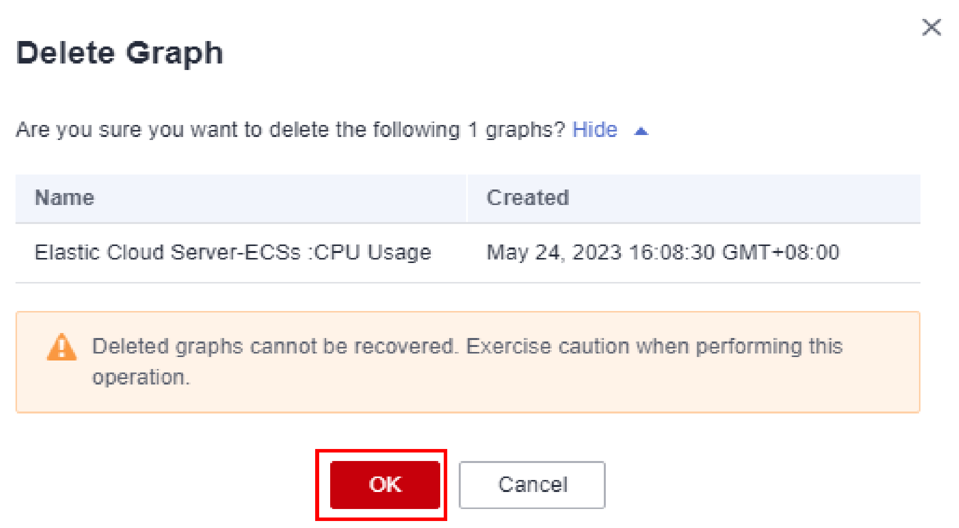
Figure 3-9 Deleting a graph



Elastic Cloud Server-ECSs :CPU Usage

6. In the displayed **Delete Graph** dialog box, click **OK**.

Figure 3-10 Delete Graph



Delete Graph

Are you sure you want to delete the following 1 graphs? Hide ▲

Name	Created
Elastic Cloud Server-ECSs :CPU Usage	May 24, 2023 16:08:30 GMT+08:00

Deleted graphs cannot be recovered. Exercise caution when performing this operation.

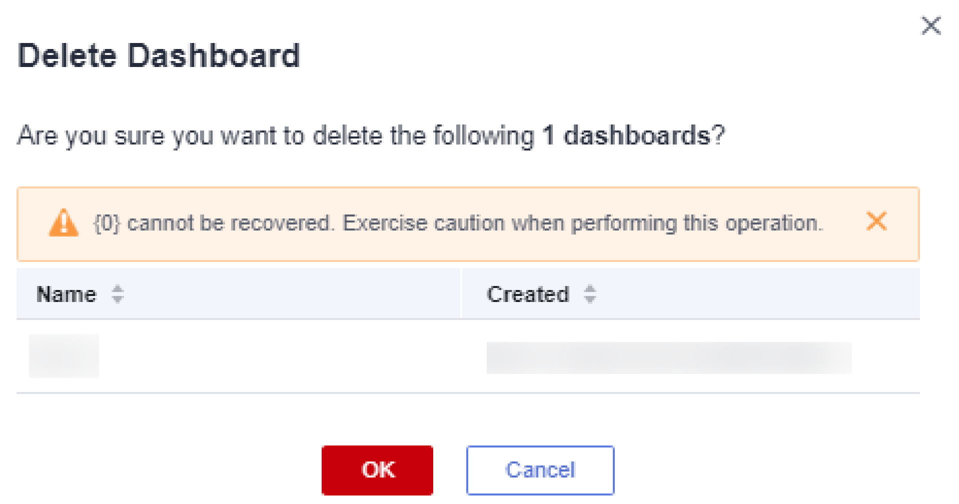
3.1.7 Deleting a Dashboard

To re-plan graphs on your dashboard, you can delete the existing dashboards. After you delete a dashboard, all graphs added to it will be deleted.

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, choose **Dashboards** > **My Dashboards**.
4. Select the dashboard to be deleted.
5. Click **Delete** in the **Operation** column.
6. In the displayed **Delete Dashboard** dialog box, click **OK**.

Figure 3-11 Delete Dashboard



Delete Dashboard

Are you sure you want to delete the following 1 dashboards?

{0} cannot be recovered. Exercise caution when performing this operation.

Name	Created

3.1.8 Viewing Dashboards Across Accounts

Scenarios

On Cloud Eye, you only need to log in to one account to view the dashboards of all accounts in the organization to which you belong.

NOTE

- **My Dashboards** can only be viewed across accounts.
- This function is available in the following regions: CN South-Guangzhou-InvitationOnly, TR-Istanbul, CN Southwest-Guiyang1, CN North-Ulanqab-Auto1, LA-Mexico City1, AP-Singapore, AF-Johannesburg, AP-Bangkok, CN-Hong Kong, LA-Mexico City2, AP-Jakarta, CN South-Guangzhou, CN North-Beijing1, CN North-Ulanqab1, CN North-Beijing4, LA-Santiago, CN East-Shanghai1, LA-Sao Paulo1, ME-Riyadh, and CN East-Qingdao.

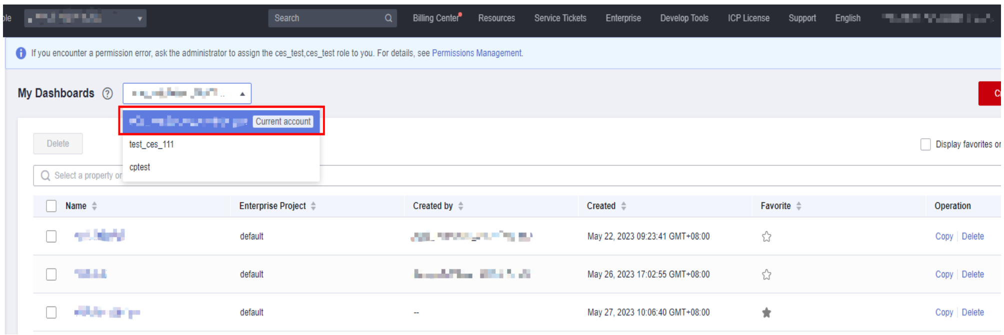
Prerequisites

1. You have enabled trusted access for Cloud Eye in the organization to which your account belongs. For details, see **Enabling or Disabling a Trusted Service**.
2. You are the organization administrator or Cloud Eye delegating administrator. For details about how to specify a delegated administrator, see **Specifying, Viewing, or Removing a Delegating Administrator**.

Procedure

1. Log in to the management console as an organization administrator or a delegating administrator of Cloud Eye.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboards** > **My Dashboards**.
4. Select an account from the drop-down list box to view dashboards of other accounts.

Figure 3-12 Switching accounts



If you encounter a permission error, ask the administrator to assign the ces_test,ces_test role to you. For details, see Permissions Management.

My Dashboards

[redacted] Current account
test_ces_111
cptest

Name	Enterprise Project	Created by	Created	Favorite	Operation
[redacted]	default	[redacted]	May 22, 2023 09:23:41 GMT+08:00	☆	Copy | Delete
[redacted]	default	[redacted]	May 26, 2023 17:02:55 GMT+08:00	☆	Copy | Delete
[redacted]	default	--	May 27, 2023 10:06:40 GMT+08:00	★	Copy | Delete

NOTE

If no dashboard is available under the account, use the account to log in to the management console and create a dashboard. For details, see **Creating a Dashboard**.

3.2 Cloud Service Dashboards

You can view all monitoring data of a single cloud service in the all-in-one cloud service dashboard. Cloud service dashboards are automatically generated and you do not need to manually configure them.

Viewing a Cloud Service Dashboard

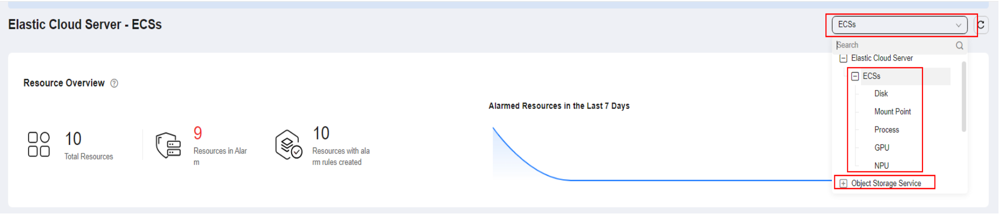
1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboards** > **Cloud Service Dashboards**.
4. Click the name of the dashboard whose resources you want to view.
5. On the displayed page, view details under **Resource Overview**, **Alarm Statistics**, and **Key Metrics**. For details, see **Table 3-3**.

Table 3-3 Details on a cloud service dashboard

Module	Description
Resource Overview	You can view the resource data of the current cloud service in the current dimension, includes **Total Resources**, **Resources in Alarm**, **Resources with alarm rules created**, and the number of resources for which alarms are generated in the last seven days.
Alarm Statistics	You can view the total number of alarms in the last seven days, alarms of different severities (critical, major, minor, and informational), and alarms in resource groups.
Key Metrics	You can view monitoring details of key metrics recommended by cloud services.

6. On the details page of a cloud service dashboard, click the selection box in the upper right corner to change the resource dimension or select another resource to view its monitoring details.

Figure 3-13 Changing the resource dimension



4 Resource Groups

4.1 Introduction to Resource Groups

A resource group allows you to add and monitor correlated resources and provides a collective health status for all resources that it contains.

4.2 Creating a Resource Group

Scenarios

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.

Restrictions

- Each user can create up to 10 resource groups.
- Each resource group can contain 1 to 1,000 cloud service resources.
- There are restrictions on the number of resources of different types that can be added to a resource group. For details, see the tips on the Cloud Eye console.

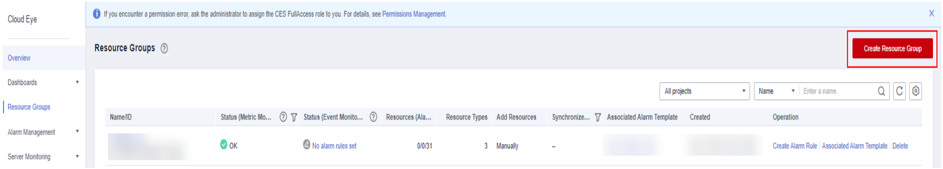
Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.

4. In the navigation pane on the left, choose **Resource Groups**.

5. In the upper right corner, click **Create Resource Group**.

Figure 4-1 Create Resource Group



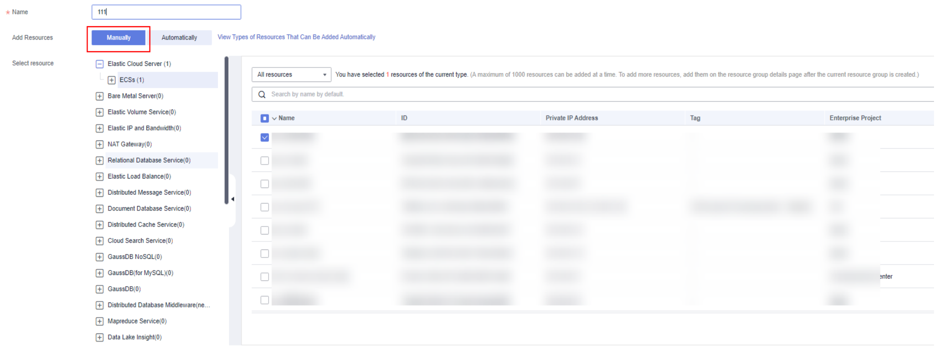
If you encounter a permission error, ask the administrator to assign the CES FullAccess role to you. For details, see Permissions Management.

Name/ID	Status (Metric Mo...	Status (Event Monito...	Resources (Ala...	Resource Types	Add Resources	Synchronize...	Associated Alarm Template	Created	Operation
	OK	No alarm rules set	0/0/31	3	Manually	--			Create Alarm Rule | Associated Alarm Template | Delete

6. On **Create Resource Group** page, enter a group name. Configure other parameters as prompted.

   a. If you select **Manually** for **Add Resources**, manually select resources for the resource group.

   Figure 4-2 Manually adding resources

   
   Manually
Automatically
View Types of Resources That Can Be Added Automatically
Elastic Cloud Server (1)
ECSs (1)
Bare Metal Server(0)
Elastic Volume Service(0)
Elastic IP and Bandwidth(0)
NAT Gateway(0)
Relational Database Service(0)
Elastic Load Balance(0)
Distributed Message Service(0)
Document Database Service(0)
Distributed Cache Service(0)
Cloud Search Service(0)
GaussDB NoSQL(0)
GaussDB(for MySQL)(0)
GaussDB(0)
Distributed Database Middleware(ne...
Mapreduce Service(0)
Data Lake Insight(0)
All resources
Search by name by default.
Name
ID
Private IP Address
Tag
Enterprise Project
enter

   * Name: 111

   Add Resources: Manually

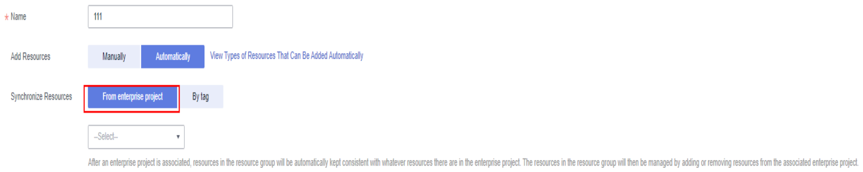
   Select resource

   You have selected 1 resources of the current type. (A maximum of 1000 resources can be added at a time. To add more resources, add them on the resource group details page after the current resource group is created.)

   b. If you select **Automatically** for **Add Resources**, all resources in an enterprise project or resources with the same tags will be added to the resource group.

      i. If you select **From enterprise project** for **Synchronize Resources**, select one or more enterprise projects. After a resource group is associated with an enterprise project, resources in the resource group will be automatically kept consistent with whatever resources there are in the enterprise project. To manage resources in this resource group, you can only add or remove resources from the associated enterprise project.

      Figure 4-3 Synchronizing resources from enterprise projects

      * Name: 111

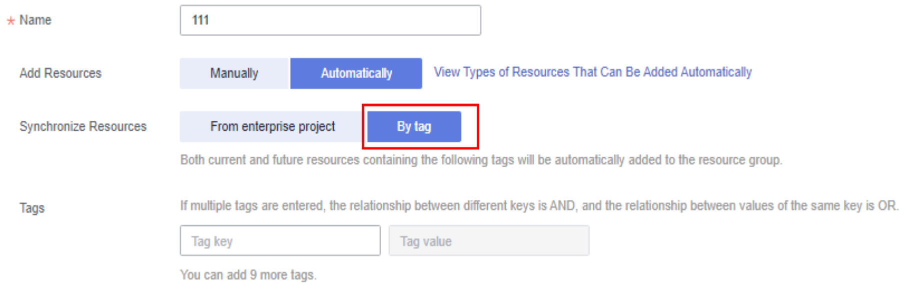
      Add Resources: Automatically

      Synchronize Resources: From enterprise project

      After an enterprise project is associated, resources in the resource group will be automatically kept consistent with whatever resources there are in the enterprise project. The resources in the resource group will then be managed by adding or removing resources from the associated enterprise project.

      ii. If you select **By tag** for **Synchronize Resources**, select or enter tag keys and values that will be used to match resources. Both existing and future resources that match the configured tags will be automatically added to the resource group. For details, see **Figure 4-4**.

Figure 4-4 Synchronizing resources by tag



* Name: 111

Add Resources: Manually | Automatically — View Types of Resources That Can Be Added Automatically

Synchronize Resources: From enterprise project | By tag

Both current and future resources containing the following tags will be automatically added to the resource group.

Tags: If multiple tags are entered, the relationship between different keys is AND, and the relationship between values of the same key is OR.

Tag key | Tag value

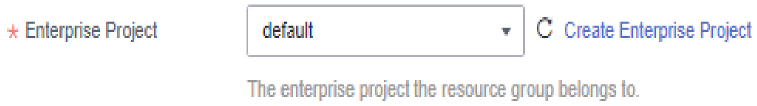
You can add 9 more tags.

NOTE

- If you enter multiple tags, the relationship between different keys is AND, and the relationship between values of the same key is OR.
- You can add up to 10 tags.

7. Configure the enterprise project.

Figure 4-5 Enterprise Project



* Enterprise Project: default — Create Enterprise Project

The enterprise project the resource group belongs to.

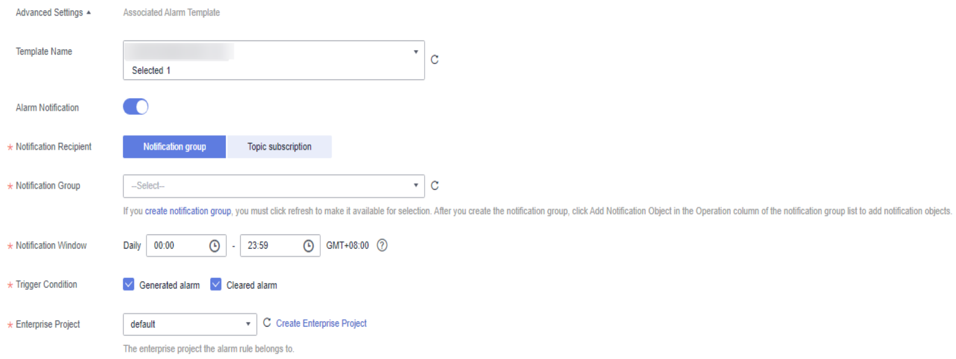
Table 4-1 Configuring **Enterprise Project**

Parameter	Description
Enterprise Project	Specifies the enterprise project to which the resource group belongs. Only users who have all permissions for the enterprise project can view and manage the resource group. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

8. (Optional) Configure **Advanced Settings** and associate an alarm template.

   Select an alarm template and configure alarm notification parameters as needed.

Figure 4-6 Alarm Notification parameters



Advanced Settings ▲ Associated Alarm Template

Template Name: [redacted] Selected 1

Alarm Notification: ●

* Notification Recipient: **Notification group** | Topic subscription

* Notification Group: --Select--

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects.

* Notification Window: Daily 00:00 - 23:59 GMT+08:00

* Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

* Enterprise Project: default Create Enterprise Project

The enterprise project the alarm rule belongs to.

Table 4-2 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.
Notification Recipient	Specifies the alarm notification recipient. You can select **Notification group** or **Topic subscription**.
Notification Group	Specifies the notification group to which alarm notifications will be sent.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the phone number and email address of the registered account. ● **Topic**: 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**.
Notification Window	Cloud Eye sends notifications only within the notification window you specified. If **Notification Window** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.
Trigger Condition	Specifies the condition that will trigger an alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.
Enterprise Project	Specifies the enterprise project that the alarm template belongs to. Only users who have all permissions for the enterprise project can manage the alarm template. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

NOTE

You can search for ECSs and BMSs by name, ID, and private IP address. For other cloud services, you can search only by name and ID.

9. Click **Create**.

4.3 Viewing Resource Groups

4.3.1 Resource Group List

The resource group list displays all resource groups you have on Cloud Eye, the resources they contain, and the health status of each resource group.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.

   On the **Resource Groups** page, you can view all the resource groups that have been created.

Table 4-3 Parameters of the resource group list

Parameter	Description
Name/ID	Specifies the resource group name and ID. **NOTE** The group name can contain a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
Status (Metric Monitoring)	● No alarm: No alarm resource exists in the group. ● In alarm: An alarm is being generated for a resource in the group. ● No alarm rules set: No alarm rules have been created for any resource in the group.
Status (Event Monitoring)	● **OK**: No events have been triggered for a resource group. ● **Triggered**: One or more events have been triggered for a resource group. ● **No alarm rules set**: No alarm rules have been created for any resource in a resource group.
Resources (Alarm/ Triggered/Total)	Specifies the total number of resources that are triggering alarms, resources that have triggered alarms, and the total number of resources in the resource group.

Parameter	Description
Resource Types	Specifies the number of different resource types in a group. For example, if there are two ECSs and one EVS disk in a resource group, then there are two types of resources and **Resource Types** is **2**.
Enterprise Project	Specifies the name of the enterprise project that has the resource group permission.
Created	Indicates the method of creating a resource group. The value can be Manual or Intelligent.
Synchronize Resources	You can add all resources in an enterprise project or resources with the same tags to a resource group.
Associated Alarm Template	Specifies the alarm template associated with the resource group.
Created	Specifies the time when the resource group was created.
Operation	You can create alarm rules, associate an alarm template, and delete a resource group.

4.3.2 Resource Overview

The **Resource Overview** page displays the resource types contained in the current group, as well as the total number of resources of each resource type, dimensions, and whether there are alarms generated for the resources.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Click a resource group name to go to the **Resource Overview** page.

   On this page, you can change the name of a resource group, and remove or add resources. There is also a link for you to quickly create alarm rules for those resources.

4.3.3 Alarm Rules

The **Alarm Rules** page displays all alarm rules in a resource group. You can create, copy, enable, disable, or delete alarm rules in a single resource group. You can also mask or unmask alarm notifications.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.

3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. In the resource group list, click the name of the target group to go to the **Resource Overview** page.
6. In the navigation pane on the left, choose **Alarm Rules** to view all alarm rules in the resource group.

   On the **Alarm Rules** page, you can quickly create alarm rules for resources in the resource group. For details, see **5.2.2 Creating an Alarm Rule**.

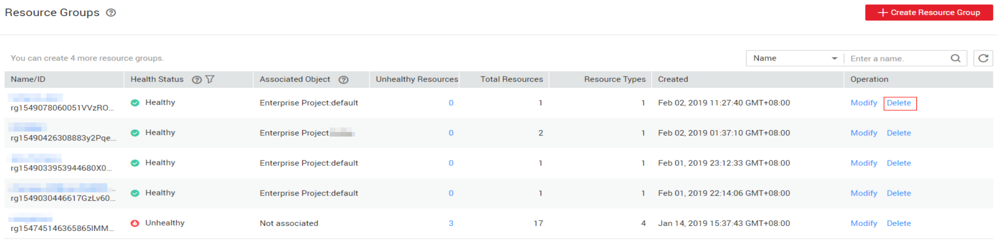
4.4 Managing Resource Groups

4.4.1 Deleting a Resource Group

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Locate the row containing the target resource group and click **Delete** in the **Operation** column.

Figure 4-7 Deleting a resource group



Name/ID	Health Status	Associated Object	Unhealthy Resources	Total Resources	Resource Types	Created	Operation
[redacted] rg1549078060051VVzRO...	Healthy	Enterprise Project:default	0	1	1	Feb 02, 2019 11:27:40 GMT+08:00	Modify Delete
[redacted] rg15490426308883y2Pqe...	Healthy	Enterprise Project[redacted]	0	2	1	Feb 02, 2019 01:37:10 GMT+08:00	Modify Delete
[redacted] rg1549033953944680X0...	Healthy	Enterprise Project:default	0	1	1	Feb 01, 2019 23:12:33 GMT+08:00	Modify Delete
[redacted] rg1549030446617GzLv60...	Healthy	Enterprise Project:default	0	1	1	Feb 01, 2019 22:14:06 GMT+08:00	Modify Delete
[redacted] rg1547451463658651MM...	Unhealthy	Not associated	3	17	4	Jan 14, 2019 15:37:43 GMT+08:00	Modify Delete

6. In the displayed **Delete Resource Group** dialog box, click **OK**.

4.4.2 Associating Resource Groups with Alarm Templates

Scenarios

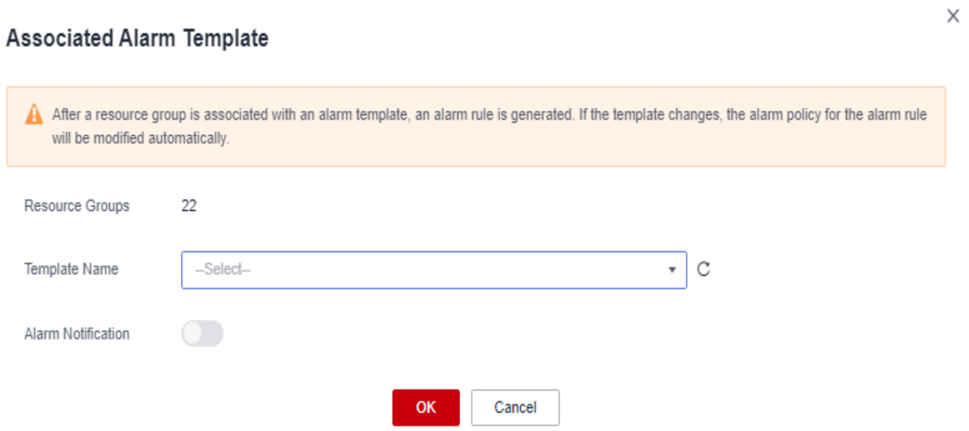
You can create resource groups and associate them with alarm templates to create alarm rules in batches, improving alarm rule configuration efficiency.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. On the **Resource Groups** page, locate the target resource group, and click **Associate Alarm Template** in the **Operation** column.

4. In the **Associate Alarm Template** dialog box, select an alarm template.

Figure 4-8 Associate Alarm Template



Associated Alarm Template

After a resource group is associated with an alarm template, an alarm rule is generated. If the template changes, the alarm policy for the alarm rule will be modified automatically.

Resource Groups: 22

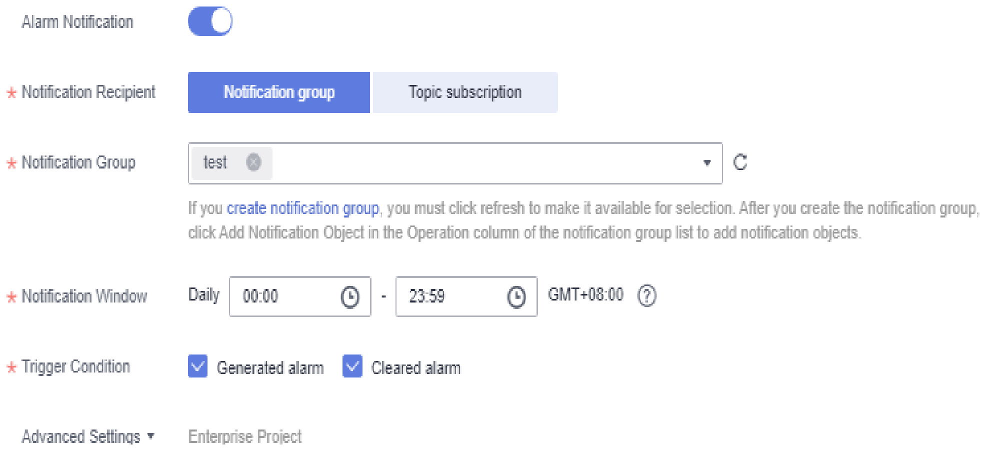
Template Name: --Select--

Alarm Notification: ○

OK | Cancel

5. Configure the alarm notification.

Figure 4-9 Alarm Notification



Alarm Notification: ●

* Notification Recipient: Notification group | Topic subscription

* Notification Group: test

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects.

* Notification Window: Daily 00:00 - 23:59 GMT+08:00

* Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

Advanced Settings ▾ Enterprise Project

Table 4-4 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.
Notification Type	You can select a notification group or topic subscription as required.
Notification Group	Specifies the notification group to which alarm notifications will be sent.

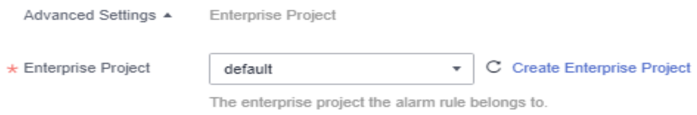
Parameter	Description
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the phone number and email address of the registered account. ● **Topic**: A topic is used to publish messages and subscribe 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**.
Notification Window	Cloud Eye sends notifications only within the notification window you specified. If **Notification Window** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.
Trigger Condition	Specifies the condition that will trigger an alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

NOTE

Alarm notifications sent by SMN will be billed. For details, see **Product Pricing Details**.

6. Configure the enterprise project as prompted.

Figure 4-10 Advanced Settings



Advanced Settings ▲ Enterprise Project

* Enterprise Project: default

The enterprise project the alarm rule belongs to.

Table 4-5 Configuring the enterprise project

Parameter	Description
Enterprise Project	Specifies the enterprise project that the alarm rules belong to. Only users who have all permissions for the enterprise project can manage the alarm rules. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

7. Click **OK**.

5 Alarm Management

5.1 Alarm Overview

You can set alarm rules for key metrics of cloud services. When the conditions in the alarm rule are met, Cloud Eye sends emails or SMS messages, or sends HTTP/HTTPS messages, enabling you to quickly respond to resource changes.

Cloud Eye invokes SMN APIs to send notifications. This requires you to create a topic and add subscriptions to this topic on the SMN console. Then, when you create alarm rules on Cloud Eye, you can enable the alarm notification function and select the topic. When alarm rule conditions are met, Cloud Eye sends the alarm information to subscription endpoints in real time.

NOTE

If no alarm notification topic is created, alarm notifications will be sent to the default email address of the login account.

5.2 Alarm Rules

As your services grow, you may find that existing alarm rules do not match your service requirements.

You can perform operations provided in this section to optimize these alarm rules.

5.2.1 Introduction to Alarm Rules

You can flexibly create alarm rules on the Cloud Eye console. You can create an alarm rule for a specific metric or use the alarm template to create alarm rules in batches for multiple cloud service resources.

Cloud Eye provides you with default alarm templates tailored to each service. In addition, you can also create custom alarm templates by modifying the default alarm template or by specifying every required field.

5.2.2 Creating an Alarm Rule

This topic describes how to create an alarm rule.

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 **Alarm Management** > **Alarm Rules**.
4. Click **Create Alarm Rule** in the upper right corner.
5. On the **Create Alarm Rule** page, configure required parameters.
   a. Set the alarm rule name and description.

Table 5-1 Name and **Description**

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarm-b6al**
Description	(Optional) Provides supplementary information about the alarm rule.

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

Table 5-2 Parameters

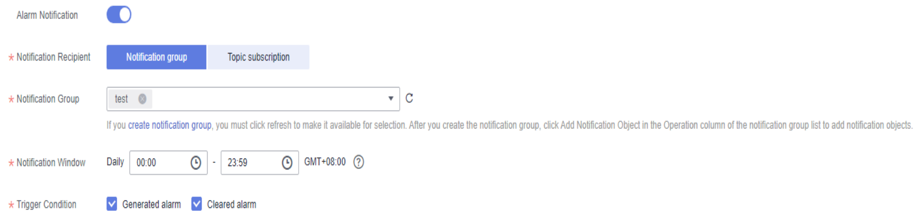
Parameter	Description	Example Value
Alarm Type	Specifies the alarm type to which the alarm rule applies. The value can be **Metric** or **Event**.	Metric
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server
Dimension	Specifies the metric dimension of the selected resource type.	ECSs

Parameter	Description	Example Value
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select **All resources**, **Resource groups**, or **Specified resources**. **NOTE** ● If you select **All resources**, an alarm will be triggered when any instance meets an alarm policy, and existing alarm rules of the current resource type and dimension will be automatically applied to newly purchased resources of the same resource type and dimension. ● If you select **Resource groups**, an alarm will be triggered when any resource in the group meets the alarm policy. ● If you select **Specific resources**, select one or more resources and click » to add them to the box on the right.	All resources
Method	You can select an associated template, use an existing template or create a custom template as required. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Template	Specifies the template to be used. You can select a default alarm template or customize an alarm template.	N/A

Parameter	Description	Example Value
Alarm Policy	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. If you set **Resource Type** is to **Event Monitoring**, the event that triggers the alarm is an instant operation. For example, if event improper ECS running occurs, Cloud Eye triggers an alarm. For details, see **5.2.3 Alarm Policies**. **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.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Figure 5-1 Alarm Notification



Alarm Notification ●

* Notification Recipient: Notification group | Topic subscription

* Notification Group: test

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects.

* Notification Window: Daily 00:00 - 23:59 GMT+08:00

* Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

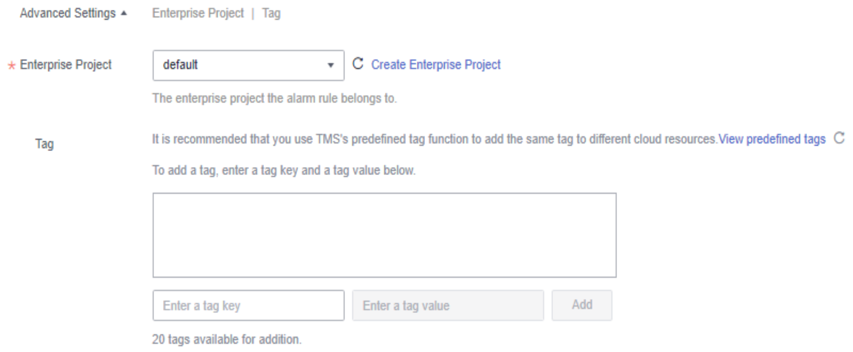
Table 5-3 Alarm Notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email or text message, or by HTTP/HTTPS request to servers.
Notification Type	You can select a notification group or topic subscription as required.
Notification Group	Specifies the notification group to which alarm notifications will be sent.

Parameter	Description
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the phone 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**.
Notification Window	Cloud Eye sends notifications only within the notification window you specified. If **Notification Window** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.
Trigger Condition	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.

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

Figure 5-2 Advanced Settings



* Enterprise Project: default

The enterprise project the alarm rule belongs to.

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources.

To add a tag, enter a tag key and a tag value below.

20 tags available for addition.

Table 5-4 Configuring **Enterprise Project** and **Tag**

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

Parameter	Description
Tag	Specifies a key-value pair. Tags identify cloud resources so that you can easily categorize and search for your resources. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags**. If your organization has configured tag policies for Cloud Eye, follow the policies when configure **Tag** for an alarm rule. If you add a tag that does not comply with the tag policies, alarm rules may fail to be created. Contact your administrator to learn more about tag policies. ● 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.

To view monitoring graphs, click **View Graph** or **View Resource** in the **Operation** column, and click **View Graph** in the displayed **View Resource** dialog box.

5.2.3 Alarm Policies

You can set alarm policies for metrics and events of a cloud service. When a metric triggers the threshold in the alarm policy for multiple times in a specified period, you will be notified. This section describes how to configure alarm policies for metrics and events.

Configuring Alarm Policies for Metrics

You can monitor key metrics of cloud services by configuring alarm rules. Then you can handle exceptions in a timely manner. A metric alarm policy must include a metric name, statistic, consecutive triggering times, threshold, and frequency. For details, see the following table.

Items in an alarm policy for metrics

Item	Description	Example Value
Metric Name	Specifies the metric name.	CPU Usage

Item	Description	Example Value
Statistic	Specifies the metric value type. Cloud Eye supports the following statistics for metrics: **Raw data**, **Avg.**, **Max.**, **Min.**, **Variance**, and **Sum**. ● **Raw data** indicates the metric data that is not processed or converted. ● **Avg.** is the value calculated by averaging raw data during a rollup period. ● **Max.** is the highest value observed during a rollup period. ● **Min.** is the lowest value observed during a rollup period. ● **Variance**: indicates the difference between each data point in the original value and the average value within a rollup period. ● **Sum** is the sum of raw data during a rollup period. **NOTE** ● A rollup period can be 5 minutes, 20 minutes, 1 hour, 4 hours, or 24 hours. Select a rollup period based on your service requirements. ● If you set a rollup period, alarm notifications will be delayed. If you set the rollup period to 5 minutes, alarm notifications will be delayed for 10 to 15 minutes. If you set the rollup period to 20 minutes, alarm notifications will be delayed for 20 minutes. If you set the rollup period to 1 hour, alarm notifications will be delayed for 1 hour and 20 minutes. If you set the rollup period to 4 hours, alarm notifications will be delayed for 4 hours and 40 minutes. If you set the rollup period to 24 hours, alarm notifications will be delayed for 25 hours.	Raw data
Consecutive Triggering Times	Specifies the number of consecutive times that an alarm is triggered. The value can be set to 1, 2, 3, 4, 5, 10, 15, 30, 60, 90, 120, or 180 times (consecutively).	2 times (consecutively)

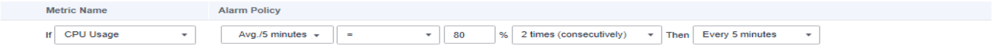
Item	Description	Example Value
Operator	Specifies the operator used to compare metric value and the threshold. Cloud Eye supports **>**, **>=**, **<**, **<=**, **=**, **!=**, **Increase compared with last period**, **Decrease compared with last period**, and **Increase or decrease compared with last period**. **NOTE** ● **Increase compared with last period**: The monitoring data in the current monitoring period increases sharply when compared with that in the previous monitoring period. ● **Decrease compared with last period**: The monitoring data in the current monitoring period decreases sharply when compared with that in the previous monitoring period. ● **Increase or decrease compared with last period**: The monitoring data in the current monitoring period increases or decreases sharply when compared with that in the previous monitoring period.	=
Threshold	Specifies the metric threshold.	70
Frequency	Specifies how often alarms are repeatedly notified when there is already an alarm. The following options are available: **Trigger only one alarm**, **Every 5 minutes**, **Every 10 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every 1 hour**, **Every 3 hours**, **Every 6 hours**, **Every 12 hours**, and **One day**.	Every 5 minutes

Example of configuring an alarm policy for a metric

For example, in an alarm policy, the metric name is CPU usage, the statistic is average, the rollup period is 5 minutes, the consecutive triggering times is 2, the operator is =, the threshold is 80%, and the frequency is every 5 minutes.

This alarm policy indicates that the average CPU usage is collected every 5 minutes. If the CPU usage of an ECS is greater than 80% for two consecutive times, an alarm is generated every 5 minutes.

Figure 5-3 Alarm policy for a metric



Metric Name	Alarm Policy
If CPU Usage	Avg./5 minutes · = · 80 % · 2 times (consecutively) · Then Every 5 minutes

Configuring Alarm Policies for Events

You can configure alarm policies for various system and custom events so that you can take measures in a timely manner when an event occurs. An event alarm policy must include the event name, triggering period, triggering type, triggering times, and alarm frequency. For details, see the following table.

Items in an alarm policy for events

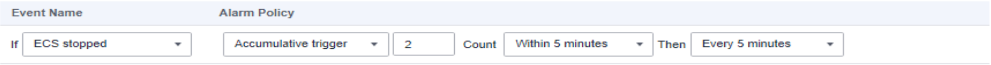
Item	Description	Example Value
Event Name	Specifies the name of a service event.	Startup failure
Triggering Period	Specifies the event triggering period. The following options are available: **Within 5 minutes**, **Within 20 minutes**, **Within 1 hours**, **Within 4 hours**, and **Within 24 hours**. **NOTE** This parameter is optional when you select **Accumulative trigger**.	Within 5 minutes
Trigger type	The value can be: **Immediate trigger** (default): After the event occurs, an alarm is triggered immediately. **Cumulative trigger**: An alarm is generated only after the event is triggered for a preset number of times within the triggering period.	Accumulative trigger
Triggering times	Specifies the cumulative number of times the event occurred within the triggering period. **NOTE** This parameter is optional when you select **Accumulative trigger**.	2
Frequency	Specifies how often alarms are repeatedly notified when there is already an alarm. The following options are available: **Trigger only one alarm**, **Every 5 minutes**, **Every 10 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every 1 hour**, **Every 3 hours**, **Every 6 hours**, **Every 12 hours**, and **One day**. **NOTE** This parameter is optional when you select **Accumulative trigger**.	Every 5 minutes

Example of configuring an alarm policy for an event

For example, in an alarm policy, the event name is startup failure, the triggering period is 5 minutes, the trigger type is cumulative trigger, the triggering times is 2, and the alarm frequency is once every 5 minutes.

This alarm policy indicates that an alarm is generated every 5 minutes if the startup failure event is triggered for 2 consecutive times within 5 minutes.

Figure 5-4 Alarm policy for an event



Event Name | Alarm Policy

If ECS stopped | Accumulative trigger 2 Count Within 5 minutes Then Every 5 minutes

5.2.4 Modifying an Alarm Rule

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Rules**.
4. On the displayed **Alarm Rules** page, use either of the following two methods to modify an alarm rule:
   - Locate the row containing the alarm rule you want to modify, click **Modify** in the **Operation** column.
   - Click the name of the alarm rule you want to modify. On the page displayed, click **Modify** in the upper right corner.
5. On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

Table 5-5 Parameters

Parameter	Description	Example Value
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.	alarm-b6al
Description	(Optional) Provides supplementary information about the alarm rule.	N/A
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to.	Resource Groups
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	N/A
Monitored Object	Specifies the resource the alarm rule is created for. You can specify one or more resources.	N/A

Parameter	Description	Example Value
Metric	For example: ● CPU Usage Indicates the CPU usage of the monitored object in percent. ● Memory Usage Indicates the memory usage of the monitored object in percent.	CPU Usage
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major
Alarm Notification	Specifies whether to notify users by sending emails, or by sending HTTP/HTTPS messages to servers.	N/A
Trigger Condition	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.	N/A

6. Click **Modify**.

5.2.5 Disabling Alarm Rules

To disable an alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to disable, and click **More** and **Disable** in the **Operation** column. In the displayed **Disable Alarm Rule** dialog box, click **Yes**.

To disable multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Disable** in the upper left of the alarm rule list. In the displayed **Disable Alarm Rule** dialog box, click **Yes**.

5.2.6 Enabling Alarm Rules

To enable a single alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to enable, and click **More** and **Enable** in the **Operation** column. In the displayed **Enable Alarm Rule** dialog box, click **Yes**.

To enable multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Enable** in the upper left of the alarm rule list. In the displayed **Enable Alarm Rule** dialog box, click **Yes**.

5.2.7 Deleting Alarm Rules

To delete a single alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to delete, click **More** in the **Operation** column, and choose **Delete**. In the displayed **Delete Alarm Rule** dialog box, click **Yes**.

To delete multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Delete** in the upper left of the alarm rule list. In the displayed **Delete Alarm Rule** dialog box, click **Yes**.

5.3 Alarm Records

The **Alarm Records** page displays the status changes of all alarm rules so that you can trace and view alarm records in a unified and convenient manner. By default, alarm records of the last seven days are displayed. You can customize the time range to display alarm records of the last 30 days.

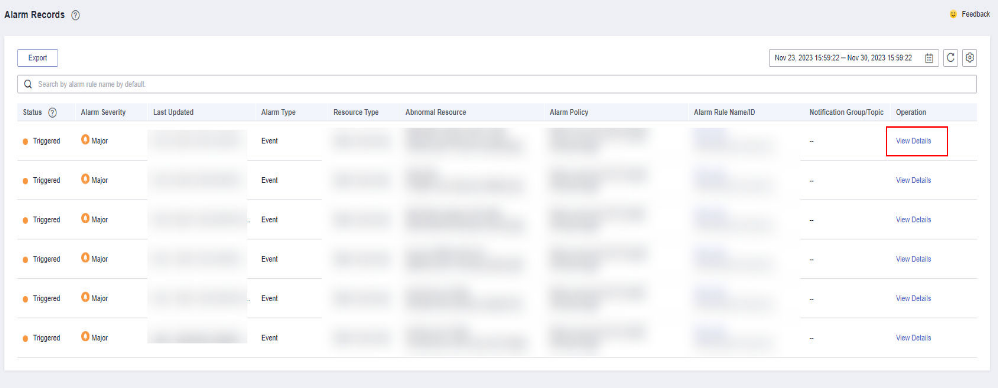
When alarms are generated, you can perform operations in this section to view alarm records of cloud resources.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Records**.

   On the **Alarm Records** page, you can view the status changes of all alarm rules in the last 7 days by default.
4. Click **View Details** in the **Operation** column. On the displayed drawer, view the basic information about the resource, and view the data that triggered the latest alarm status change.

Figure 5-5 View Details


Alarm Records
Feedback
Export
Nov 23, 2023 15:59:22 – Nov 30, 2023 15:59:22
Search by alarm rule name by default.

Status	Alarm Severity	Last Updated	Alarm Type	Resource Type	Abnormal Resource	Alarm Policy	Alarm Rule Name/ID	Notification Group/Topic	Operation
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details
Triggered	Major	[redacted]	Event	[redacted]	[redacted]	[redacted]	[redacted]	--	View Details

NOTE

- In the right corner of the alarm record list, you can select a time range within the past 30 days to view alarm records.
- In the search bar of the **Alarm Records** page, you can search for alarm records by status, alarm severity, alarm rule name, resource type, resource ID, or alarm rule ID.
- In the upper left of the alarm record list, you can click **Export** to export alarm records. For detailed operations, see **Exporting Alarm Records**.

5.4 Alarm Templates

5.4.1 Viewing Alarm Templates

An alarm template contains a group of alarm rules for a specific service. You can use it to quickly create alarm rules for multiple resources of a cloud service. Cloud Eye recommends alarm templates based on the attributes of each cloud service. It also allows you to create custom templates as needed.

Procedure

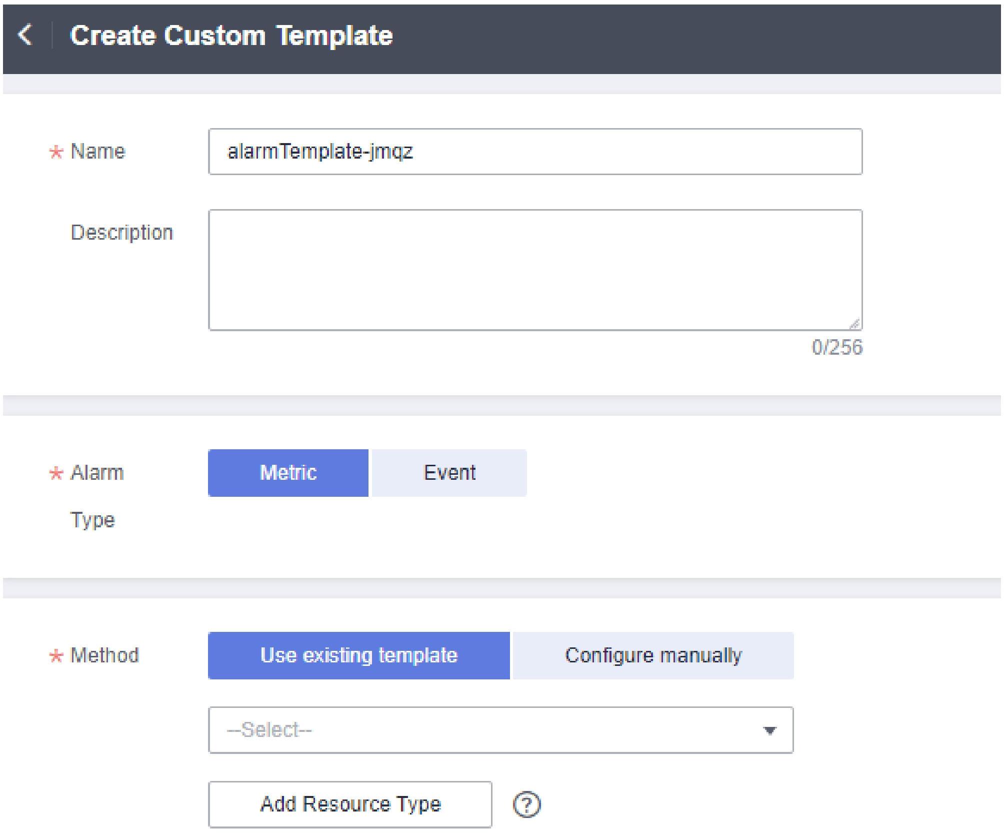
1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Templates**.

On the **Alarm Templates** page, you can create, view, modify, or delete custom templates.

5.4.2 Creating a Custom Template or Custom Event Template

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 Templates**.
4. On the **Alarm Templates** page, click **Create Custom Template**.
5. On the **Create Custom Template** page, configure parameters by referring to **Table 5-6**.

Figure 5-6 Create Custom Template



Create Custom Template

* Name: alarmTemplate-jmqz

Description:

0/256

* Alarm Type: Metric

* Method: Use existing template

--Select--

Table 5-6 Parameters

Parameter	Description
Name	Specifies the custom template name. The system generates a random name, which you can modify. Example value: **alarmTemplate-c6ft**
Description	(Optional) Provides supplementary information about the custom template.
Alarm Type	Specifies the alarm type to which the alarm template applies. The value can be **Metric** or **Event**.
Event Type	Specifies the event type when you set **Alarm Type** to **Event**. The default value is **System Event**.
Method	You can select **Use existing template** or **Configure manually**. ● **Use existing template**: Select an existing template and use or modify default alarm rules in the template. ● **Configure manually**: You can customize alarm policies as required.

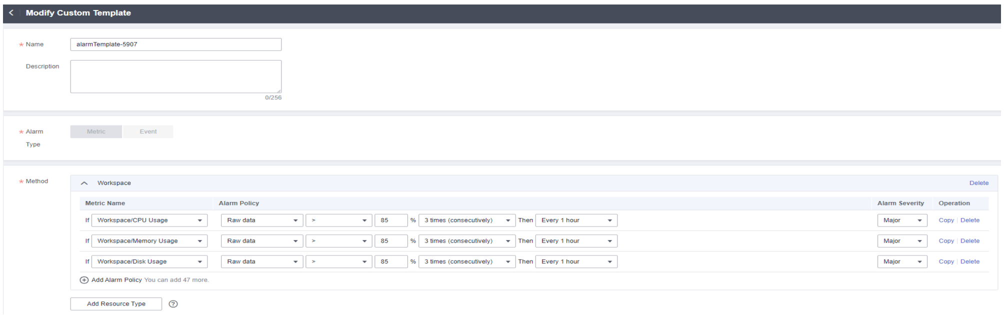
Parameter	Description
Add Resource Type	Specifies the type of the resource the alarm template is created for. Example value: **Elastic Cloud Server**
Alarm Policy	Specifies the policy for triggering an alarm. ● When you set **Alarm Type** to **Metric**, whether to trigger an alarm depends on whether the 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. ● If you set **Alarm Type** to **Event** and specify an event (such as improper ECS running), Cloud Eye triggers an alarm as long as the event occurs. For details, see **5.2.3 Alarm Policies**. **NOTE** Up to 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.
Operation	You can copy or delete an added alarm policy.

6. Click **Create**.

5.4.3 Modifying a Custom Template or Custom Event Template

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 Templates**.
4. Click the **Custom Templates** or **Custom Event Templates** tab.
5. Locate the target template and click **Modify** in the **Operation** column.
6. Modify the configured parameters by referring to **Table 5-6**.

Figure 5-7 Modify Custom Template



* Name: alarmTemplate-5907

Description: 0/256

* Alarm Type: Metric

* Method: Workspace

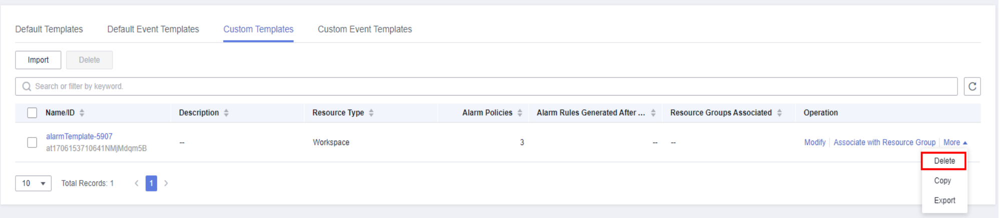
Metric Name	Alarm Policy						Alarm Severity	Operation
If Workspace/CPU Usage	Raw data	>	85 %	3 times (consecutively)	Then	Every 1 hour	Major	Copy | Delete
If Workspace/Memory Usage	Raw data	>	85 %	3 times (consecutively)	Then	Every 1 hour	Major	Copy | Delete
If Workspace/Disk Usage	Raw data	>	85 %	3 times (consecutively)	Then	Every 1 hour	Major	Copy | Delete

7. Click **Modify**.

5.4.4 Deleting a Custom Template or Custom Event Template

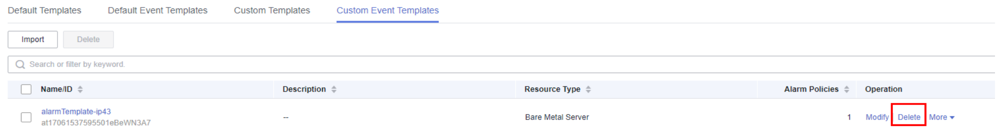
1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management** > **Alarm Templates**.
4. Click the **Custom Templates** or **Custom Event Templates** tab.
5. Locate the alarm template to be deleted and choose **More** > **Delete**, or click **Delete** in the **Operation** column.

Figure 5-8 Deleting a custom template



Name/ID	Description	Resource Type	Alarm Policies	Alarm Rules Generated After ...	Resource Groups Associated	Operation
alarmTemplate-5907 at1706153710641NMjMdqm5B	--	Workspace	3	--	--	Modify | Associate with Resource Group | More

Figure 5-9 Deleting a custom event template



Name/ID	Description	Resource Type	Alarm Policies	Operation
alarmTemplate-ip43 at17061537595501eBeWN3A7	--	Bare Metal Server	1	Modify Delete More

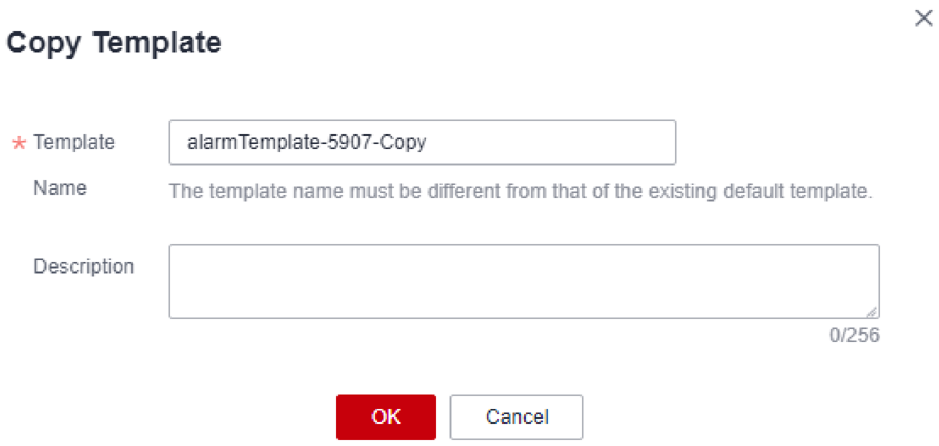
6. Click **OK**.

5.4.5 Copying a Custom Template or Custom Event Template

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 Templates**.
4. Click the **Custom Templates** or **Custom Event Templates** tab.
5. Locate the target alarm template and choose **More** > **Copy** in the **Operation** column.

6. In the **Copy Template** dialog box, set **Template Name** and **Description**.

Figure 5-10 Copy Template



Copy Template

* Template Name: alarmTemplate-5907-Copy

The template name must be different from that of the existing default template.

Description:

0/256

7. Click **OK**.

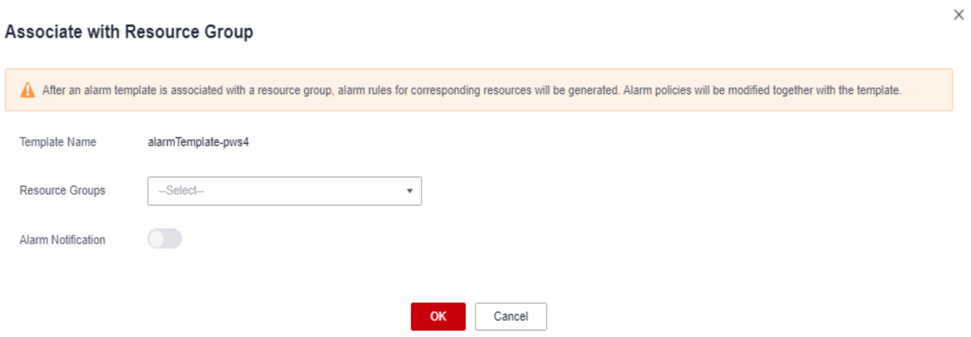
5.4.6 Associating a Custom Template with a Resource Group

By associating a custom template with a resource group, you can create alarm rules for different resources in batches. After the template is associated with the resource group, alarm rules for resources in this group will be generated. Alarm policies will be modified together with the template.

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 Templates**.
4. Click the **Custom Template** tab.
5. Locate the target template and click **Associate with Resource Group** in the **Operation** column.
6. In the displayed **Associate with Resource Group** dialog box, select a resource group.

Figure 5-11 Associate with Resource Group



Associate with Resource Group

After an alarm template is associated with a resource group, alarm rules for corresponding resources will be generated. Alarm policies will be modified together with the template.

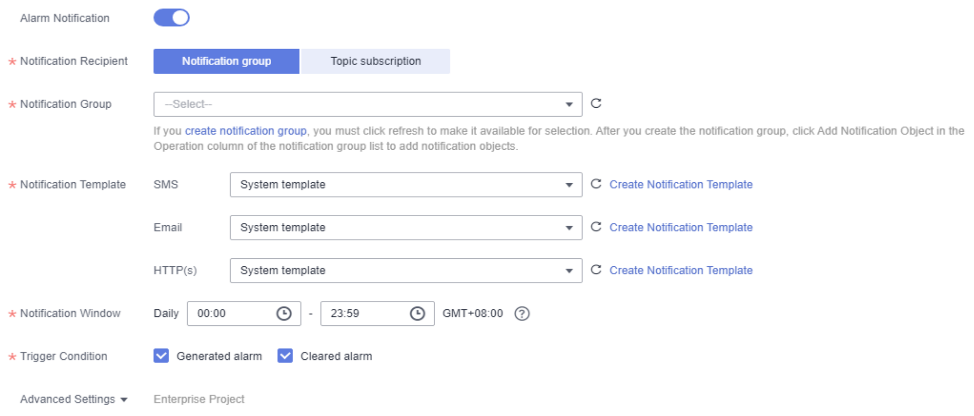
Template Name: alarmTemplate-pws4

Resource Groups: --Select--

Alarm Notification

7. Configure the alarm notification.

Figure 5-12 Alarm Notification parameters



Alarm Notification ●

* Notification Recipient: Notification group | Topic subscription

* Notification Group: --Select-- ▾ C

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects.

* Notification Template

SMS: System template ▾ C Create Notification Template

Email: System template ▾ C Create Notification Template

HTTP(s): System template ▾ C Create Notification Template

* Notification Window: Daily 00:00 - 23:59 GMT+08:00 ?

* Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

Advanced Settings ▾ Enterprise Project

Table 5-7 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.
Notification Recipient	Specifies the way to send alarm notifications. You can select **Notification group** or **Topic subscription**.
Notification Group	Specifies the notification group to which alarm notifications will be sent. This parameter is available when you select **Notification group** for **Notification Recipient**.
Notification Object	Specifies the object to which alarm notifications will be sent.. You can select the account contact or a topic name. ● **Account contact** is the phone number and email address of the registered account. ● **Topic**: 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**.
Notification Template	Specifies the SMS, email, or HTTP/HTTPS notification templates for sending alarm notifications. You can select a system template or customize a notification template.
Notification Window	Cloud Eye sends notifications only within the notification window you specified. If **Notification Window** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.

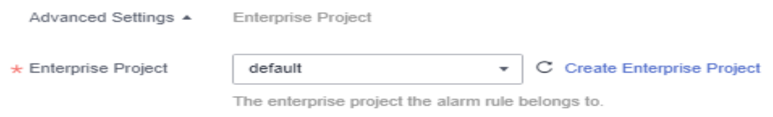
Parameter	Description
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

NOTE

Alarm notifications sent by SMN will be billed. For details, see **Product Pricing Details**.

8. Configure the enterprise project as prompted.

Figure 5-13 Advanced Settings



Advanced Settings ▴ Enterprise Project

* Enterprise Project: default

Create Enterprise Project

The enterprise project the alarm rule belongs to.

Table 5-8 Parameter of **Advanced Settings**

Parameter	Description
Enterprise Project	Specifies the enterprise project that the alarm template belongs to. Only users who have all permissions for the enterprise project can manage the alarm template. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

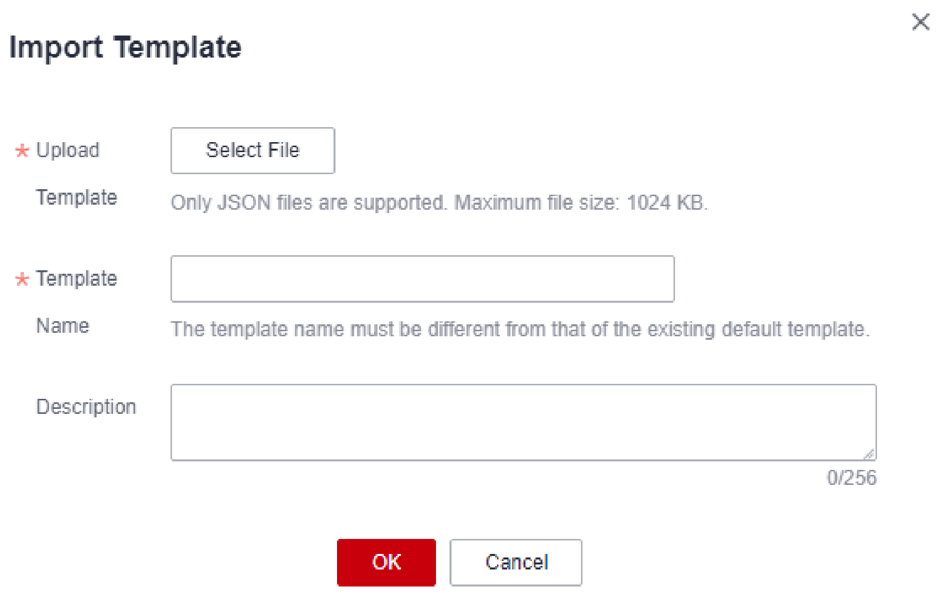
9. Click **OK**.

5.4.7 Importing and Exporting Custom Template or Custom Event Templates

Importing a Custom Template

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 Templates**.
4. Click the **Custom Templates** or **Custom Event Templates** tab.
5. Click **Import**.
6. Upload a JSON file, enter a template name, and click **OK**.

Figure 5-14 Import Template


Import Template

* Upload Template: Select File
Only JSON files are supported. Maximum file size: 1024 KB.

* Template Name:
The template name must be different from that of the existing default template.

Description:
0/256

NOTE

The template name must be different from that of a default template.

Exporting a Custom Template

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 Templates**.
4. Click the **Custom Templates** or **Custom Event Templates** tab.
5. Locate the target template and choose **More** > **Export** in the **Operation** column.

5.5 Alarm Notifications

5.5.1 Creating a Notification Object and Notification Group

Cloud Eye sends alarm notifications to notification objects and notification groups. You need to create a notification object and a notification group and add the notification object to the notification group. When creating an alarm rule, you can select a notification group that will receive the alarm notifications.

Creating a Notification Object

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 Notifications**.

4. Select the **Notification Objects** tab, click **Create** and configure parameters as prompted.

Figure 5-15 Create Notification Object

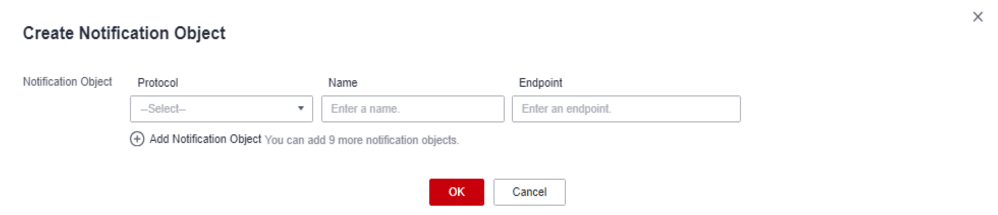

Create Notification Object
Notification Object
Protocol
Name
Endpoint
--Select--
Enter a name.
Enter an endpoint.
Add Notification Object You can add 9 more notification objects.
OK
Cancel

Table 5-9 Parameters for creating a notification object

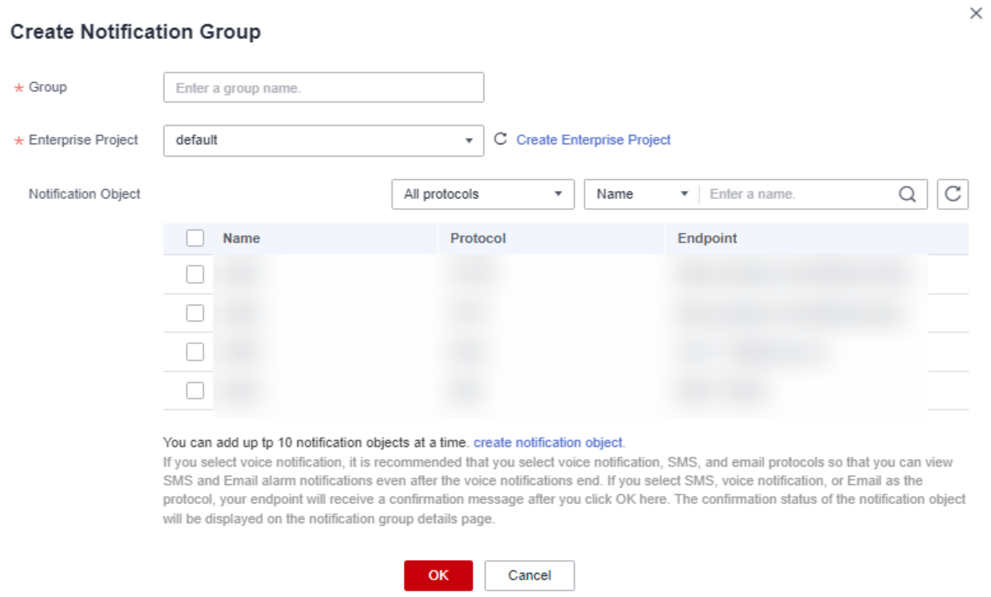
Parameter	Description
Protocol	Specifies the protocol the notification object uses to receive alarm notifications. This parameter can be set to **Email**, **SMS**, **HTTP**, or **HTTPS**.
Name	Specifies the notification object name.
Endpoint	Specifies the endpoint of the notification object. ● **Email**: Enter one or more valid email addresses. For example: username@example.com username2@example.com ● **HTTP**: Enter one or more public network URLs. For example: http://example.com/notification/action ● **HTTPS**: Enter one or more public network URLs. For example: https://example.com/notification/action **NOTE** After a notification object is added to a notification group, SMN sends a subscription confirmation message to the subscription endpoint. ● If you select **SMS** for **Protocol**, messages will be sent to the phone number you entered as text messages. ● If you select **Email** for **Protocol**, messages are sent to the email address you entered. ● If you select **HTTP** or **HTTPS** for **Protocol**, messages are sent to the URL you entered as HTTP/HTTPS requests. For details about the HTTP/HTTPS message format, see **HTTP/HTTPS Messages**.

5. Click **OK**.

Creating a Notification Group

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 Notifications**.
4. Select the **Notification Groups** tab, click **Create** and configure parameters as prompted.

Figure 5-16 Create Notification Group



You can add up tp 10 notification objects at a time. create notification object.

If you select voice notification, it is recommended that you select voice notification, SMS, and email protocols so that you can view SMS and Email alarm notifications even after the voice notifications end. If you select SMS, voice notification, or Email as the protocol, your endpoint will receive a confirmation message after you click OK here. The confirmation status of the notification object will be displayed on the notification group details page.

Table 5-10 Parameters for creating a notification group

Parameter	Description
Group	Specifies the notification group name, which can contain a maximum of 64 characters.
Enterprise Project	Specifies the enterprise project to which the notification group belongs. Only users who have all permissions for the enterprise project can manage the alarm notification group. To create an enterprise project, see **Creating an Enterprise Project**.

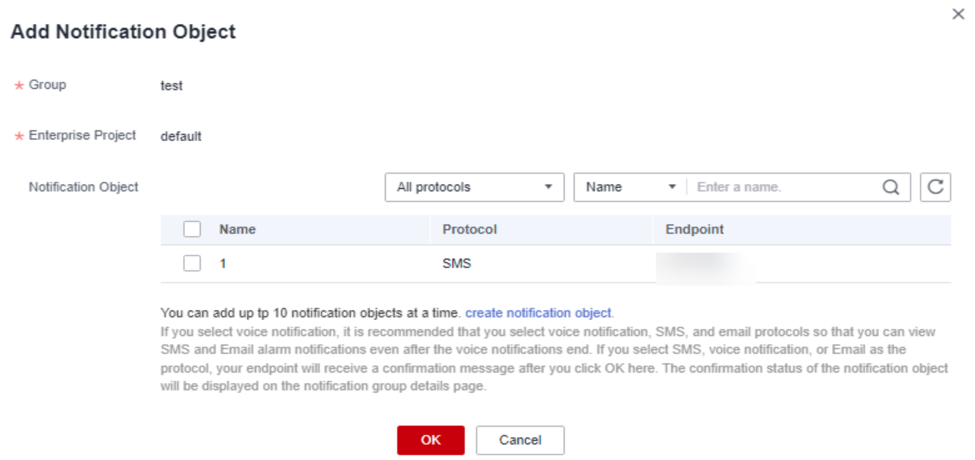
Parameter	Description
Notification Object	Specifies the object that will receive the alarm notifications. ● You can add up to 10 notification objects to a notification group at a time. ● If you select the voice protocol, you are advised to select both the SMS and email protocols to receive detailed alarm notifications. ● If **Protocol** of the notification object is set to **SMS**, **Voice**, or **Email**, the endpoint receives a confirmation message after the notification group is created. You can check whether the object status is changed to **Confirmed** on the notification group details page.

5. Click **OK**.

Adding a Notification Object to a Notification Group

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 Notifications**.
4. Locate the target notification group, and click **Add Notification Object** in the **Operation** column.
5. In the displayed **Add Notification Object** dialog box, select the notification object you want to add and click **OK**.

Figure 5-17 Add Notification Object



Add Notification Object

* Group test

* Enterprise Project default

Notification Object

□ Name	Protocol	Endpoint
□ 1	SMS	[redacted]

You can add up tp 10 notification objects at a time. create notification object.

If you select voice notification, it is recommended that you select voice notification, SMS, and email protocols so that you can view SMS and Email alarm notifications even after the voice notifications end. If you select SMS, voice notification, or Email as the protocol, your endpoint will receive a confirmation message after you click OK here. The confirmation status of the notification object will be displayed on the notification group details page.

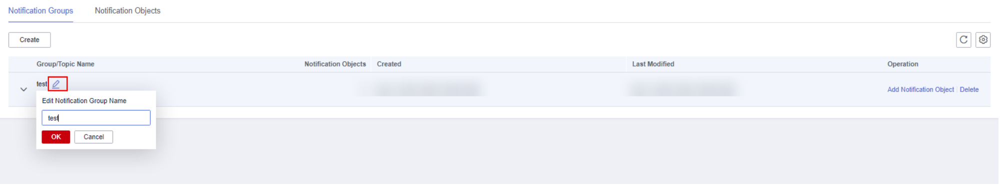
5.5.2 Modifying a Notification Group

You can modify the name of a notification group.

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 Notifications**.
4. Locate the target notification group, click ✎ next to the notification group name to change the group name.

Figure 5-18 Edit Notification Group Name



Group/Topic Name	Notification Objects	Created	Last Modified	Operation
test ✎		[redacted]	[redacted]	Add Notification Object Delete

Edit Notification Group Name: test

5. Click **OK**.

5.5.3 Deleting a Notification Object or Notification Group

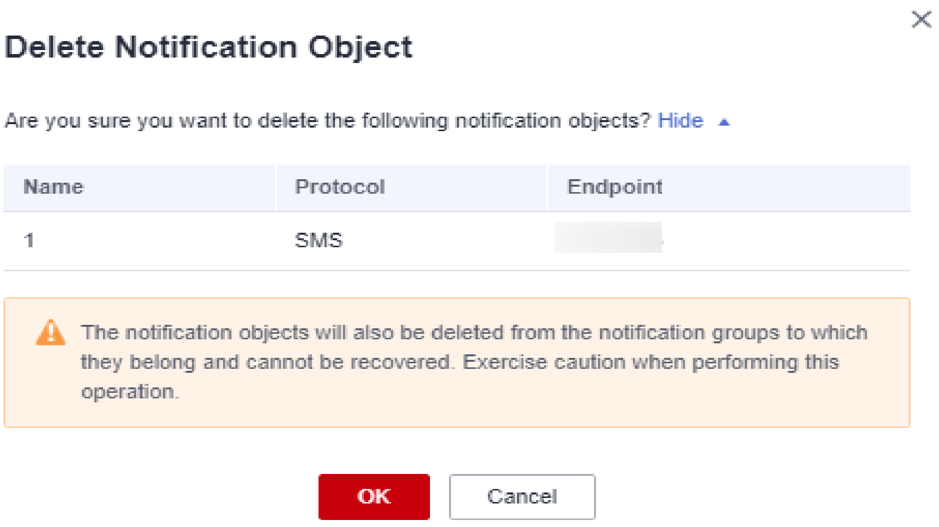
If you do not need a notification object or notification group, you can delete it.

Deleting a Notification Object

When a notification object is deleted, it is also automatically deleted from its notification 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 **Alarm Management** > **Alarm Notifications**.
4. Select the **Notification Objects** tab. To delete a single notification object, locate the target notification object and click **Delete** in the **Operation** column. To batch delete notification objects, select multiple notification objects and click **Delete** in the upper left of the list.

Figure 5-19 Delete Notification Object



Delete Notification Object

Are you sure you want to delete the following notification objects? Hide ▲

Name	Protocol	Endpoint
1	SMS	

The notification objects will also be deleted from the notification groups to which they belong and cannot be recovered. Exercise caution when performing this operation.

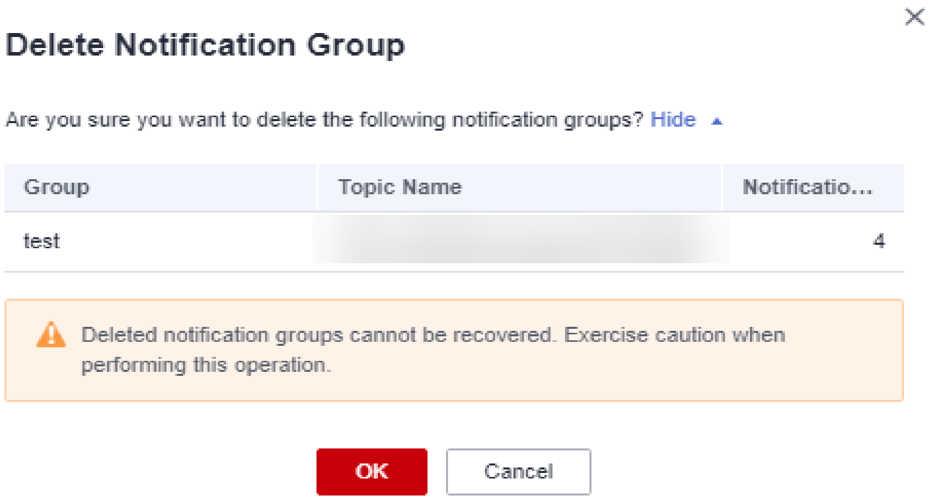
5. In the displayed **Delete Notification Object** dialog box, click **OK**.

Deleting a Notification Group

Deleting a notification group does not delete the notification objects in it.

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 Notifications**.
4. On the **Notification Groups** tab, locate the target notification group, and click **Delete** in the **Operation** column.

Figure 5-20 Delete Notification Group



Delete Notification Group

Are you sure you want to delete the following notification groups? Hide ▲

Group	Topic Name	Notificatio...
test		4

Deleted notification groups cannot be recovered. Exercise caution when performing this operation.

5. In the displayed **Delete Notification Object** dialog box, click **OK**.

Deleting a Notification Object from a Notification Group

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 Notifications**.
4. On the **Notification Groups** tab, click ⌄ next to a notification group to expand the notification objects in the notification group.
5. In the notification object list, locate the target notification object and click **Delete** in the **Operation** column. To batch delete notification objects, select them and click **Delete** in the upper left of the list.
6. In the displayed **Delete Notification Object** dialog box, click **OK**.

5.5.4 Creating Alarm Notification Topics

5.5.4.1 Creating a Topic

Scenarios

A topic serves as a message sending channel, where publishers and subscribers can interact with each other.

You can create your own topic.

Creating a Topic

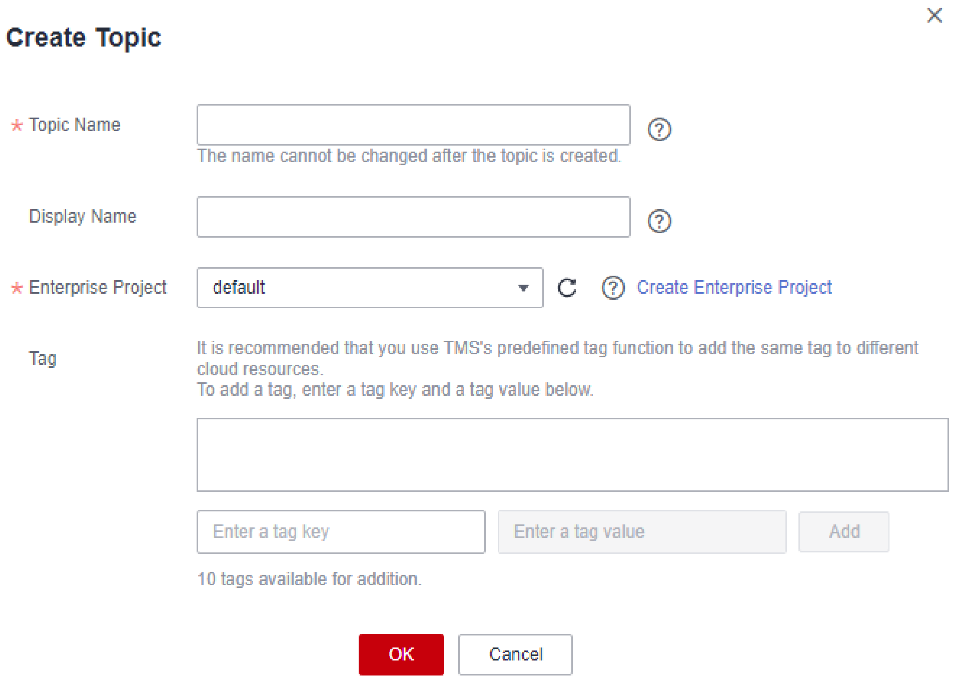
1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. In the service list, select **Simple Message Notification**.

   The SMN console is displayed.
4. In the navigation pane on the left, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.
5. Click **Create Topic**.

   The **Create Topic** dialog box is displayed.

Figure 5-21 Creating a topic


Create Topic

* Topic Name

The name cannot be changed after the topic is created.

Display Name

* Enterprise Project: default

Create Enterprise Project

Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources.
To add a tag, enter a tag key and a tag value below.

10 tags available for addition.

6. Enter a topic name and display name (topic description).

Table 5-11 Parameters required for creating a topic

Parameter	Description
Topic Name	Specifies the topic name, which ● Contains only letters, digits, hyphens (-), and underscores (_) and must start with a letter or a digit. ● Must contain 1 to 255 characters. ● Must be unique and cannot be modified after the topic is created.
Display Name	Specifies the message sender name, which must be less than 192 characters. **NOTE** After you specify a display name in *Display name***<username@example.com>** format, the name you specify will be displayed as the email sender. Otherwise, the sender will be **username@example.com**.

Parameter	Description
Tag	Tags identify cloud resources so that they can be categorized easily and searched quickly. ● For each resource, each tag key must be unique, and each tag key can have only one tag value. ● A tag key can contain a maximum of 36 characters, including digits, letters, underscores (_), and hyphens (-). ● A tag value can contain a maximum of 43 characters, including digits, letters, underscores (_), periods (.), and hyphens (-). ● Each topic supports up to 10 tags.

7. Click **OK.**

   The topic you created is displayed in the topic list.

   After you create a topic, the system generates a uniform resource name (URN) for the topic, which uniquely identifies the topic and cannot be changed.

8. Click a topic name to view the topic details and the total number of topic subscriptions.

Follow-up Operations

After you create a topic, **add subscriptions**. After the subscriptions have been confirmed, alarm notifications will be sent to the subscription endpoints via SMN.

5.5.4.2 Adding Subscriptions

A topic is a channel used by SMN to broadcast messages. Therefore, after you create a topic, add subscriptions. In this way, when the metric triggers an alarm, Cloud Eye sends the alarm information to subscription endpoints of the topic.

Adding Subscriptions

1. Log in to the management console.
2. Click ≡ and select **Simple Message Notification** under **Management & Governance**.

   The SMN console is displayed.

3. In the navigation pane on the left, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.

4. Locate the topic you want to add subscriptions to, click **More** in the **Operation** column, and select **Add Subscription**.

   The **Add Subscription** dialog box is displayed.

5. Specify the subscription protocol and endpoints.

   If you enter multiple endpoints, enter each endpoint on a separate line.

6. Click **OK**.

   The subscription you added is displayed in the subscription list.

   NOTE

   After the subscription is added, the corresponding subscription endpoint will receive a subscription notification. You need to confirm the subscription so that the endpoint can receive alarm notifications.

5.6 Example: Creating an Alarm Rule to Monitor ECS CPU Usage

This topic describes how to create an alarm rule to monitor ECS CPU usage, in which **Threshold** is set to **>= 80%**.

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 **Server Monitoring**.

   The list of ECSs on the public cloud platform is displayed.
4. Locate the ECS, and choose **More** > **Create Alarm Rule** in the **Operation** column.

   The **Create Alarm Rule** page is displayed.
5. Enter **Name** and **Description**.
6. Configure the following parameters one by one:
   a. **Method**: Select **Configure manually**.
   b. **Metric Name**: Select **CPU Usage** from the drop-down list.
   c. **Alarm Policy**: The value can be **Avg.**, **5 minutes**, **3 consecutive periods**, **>=**, **80%**, and **One day**.
   d. **Alarm Severity**: Set it to **Major**.
   e. Enable **Alarm Notification**.
   f. **Notification recipient**: Select **Topic Subscription**.
   g. **Notification Object**: Select the topic created in **5.5.4 Creating Alarm Notification Topics**.
   h. **Trigger Condition**: Select **Generated alarm** and **Cleared alarm**.
7. Click **Create**.

5.7 One-Click Monitoring

Scenarios

One-click monitoring enables you to quickly and easily enable or disable monitoring of common events for certain services. This topic describes how to use the one-click monitoring function to monitor key metrics.

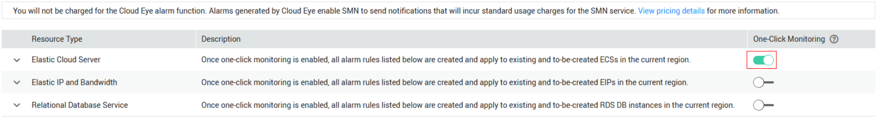
Constraints

- One-click monitoring sends notifications only when alarms are generated and does not send notifications when alarms are cleared.
- Once the alarm threshold is reached, one-click monitoring will trigger alarms immediately.
- Alarm policies cannot be modified in one-click monitoring.

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** > **One-Click Monitoring**.
4. Locate the cloud service you want to monitor, and enable **One-Click Monitoring**.

Figure 5-22 Enable one-click monitoring



You will not be charged for the Cloud Eye alarm function. Alarms generated by Cloud Eye enable SMN to send notifications that will incur standard usage charges for the SMN service. View pricing details for more information.

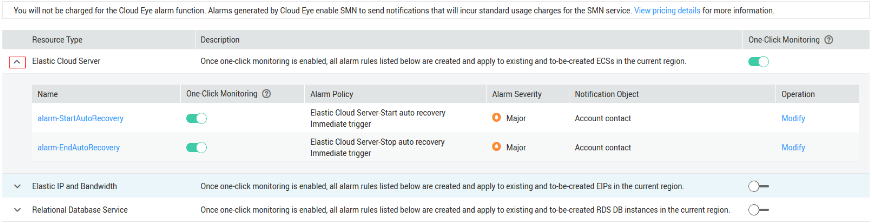
	Resource Type	Description	One-Click Monitoring ⓘ
∨	Elastic Cloud Server	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created ECSs in the current region.	●
∨	Elastic IP and Bandwidth	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created EIPs in the current region.	○
∨	Relational Database Service	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created RDS DB instances in the current region.	○

5. Click the arrow on the left of the cloud service name to view the built-in alarm rules.

NOTE

The notification object of one-click monitoring rule is the account contact.Alarm notifications will be sent to the phone number or email address provided during registration.

Figure 5-23 Viewing alarm rules



You will not be charged for the Cloud Eye alarm function. Alarms generated by Cloud Eye enable SMN to send notifications that will incur standard usage charges for the SMN service. View pricing details for more information.

	Resource Type	Description	One-Click Monitoring ⓘ
∧	Elastic Cloud Server	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created ECSs in the current region.	●

Name	One-Click Monitoring ⓘ	Alarm Policy	Alarm Severity	Notification Object	Operation
alarm-StartAutoRecovery	●	Elastic Cloud Server-Start auto recovery Immediate trigger	Major	Account contact	Modify
alarm-EndAutoRecovery	●	Elastic Cloud Server-Stop auto recovery Immediate trigger	Major	Account contact	Modify

	Resource Type	Description	One-Click Monitoring ⓘ
∨	Elastic IP and Bandwidth	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created EIPs in the current region.	○
∨	Relational Database Service	Once one-click monitoring is enabled, all alarm rules listed below are created and apply to existing and to-be-created RDS DB instances in the current region.	○

5.8 Alarm Masking

5.8.1 Introduction

Cloud Eye can mask alarm notifications based on masking rules that you configure. If an alarm is masked, alarm records are still generated, but you will not receive any notifications.

You can mask alarm notifications for a resource or some alarm policies of the resource.

5.8.2 Creating a Masking Rule

Scenarios

This section describes how to create a masking rule.

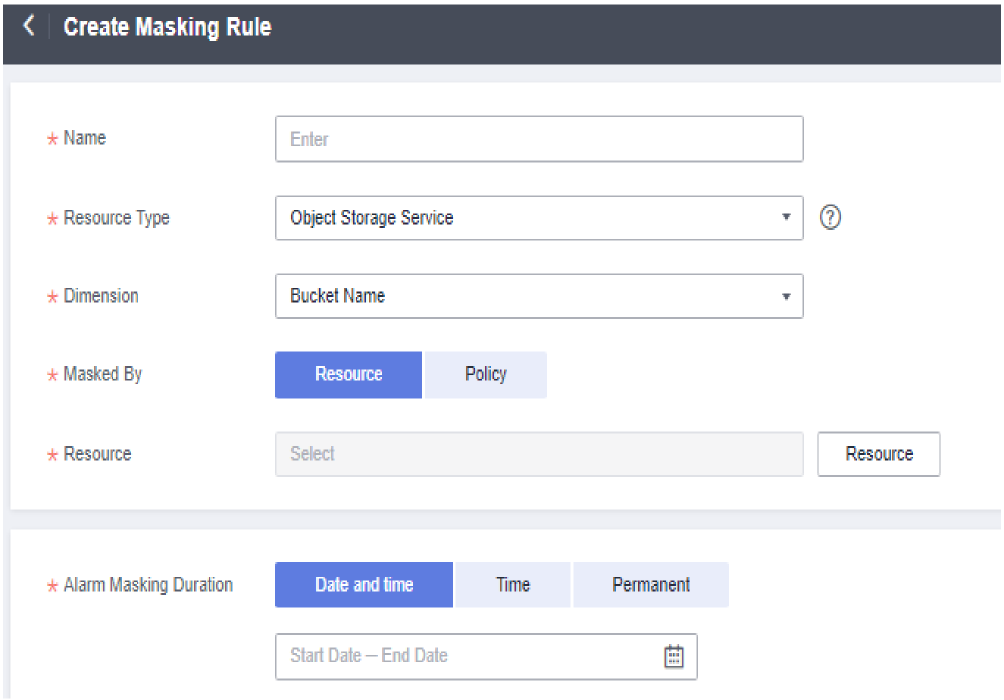
NOTE

Event monitoring does not support alarm masking.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Masking**.
4. In the upper right corner of the page, click **Create Masking Rule**.
5. On the displayed page, configure parameters as prompted.

Figure 5-24 Create Masking Rule



Create Masking Rule

* Name: Enter
* Resource Type: Object Storage Service
* Dimension: Bucket Name
* Masked By: Resource
* Resource: Select
* Alarm Masking Duration: Date and time
Start Date – End Date

Table 5-12 Parameters for configuring a masking rule

Parameter	Description
Name	Specifies the masking rule name.
Resource Type	Specifies the service name to which the masking rule is applied.
Dimension	Specifies the dimension name of the metric corresponding to the masking rule.

Parameter	Description
Masked By	Specifies whether you mask alarm notifications for a resource or an alarm policy. You can select **Resource** or **Policy**.
Resource	Specifies the resource whose alarm notifications need to be masked. **NOTE** ● If you select **Resource** for **Masked By**, a maximum of 100 resources can be added at a time. ● If you select **Policy** for **Masked By**, only one resource can be added at a time.
Select Rule	Select alarm rules for the resource only when you select **Policy** for **Masked By**.
Select Policies	Select alarm policies for the resource only when you select **Policy** for **Masked By**. **NOTE** You can select one or more alarm policies to mask alarms.
Alarm Masking Duration	Specifies the time or duration when the masking rule takes effect. ● **Date and time**: The masking rule takes effect within a specified time range. ● **Time**: The masking rule takes effect in a fixed time range every day. You can also configure the effective date range when the masking rule takes effect. For example, if the effective date is **2022-12-01** to **2022-12-31** and the effective time is **08:00** to **20:00**, the masking rule takes effect from 08:00–20:00 every day from December 1, 2022 to December 31, 2022. ● **Permanent**: The masking rule always takes effect.

6. Click **Create**.

NOTE

If you select **Resource** for **Masked By**, all alarm notifications of the resource in this dimension will be masked.

5.8.3 Modify a Masking Rule

Scenarios

This section describes how you can modify a masking rule.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Masking**.
4. On the displayed page, locate the target masking rule, and click **Modify** in the **Operation** column.
5. On the displayed **Modify Masking Rule** page, configure parameters as prompted.

Table 5-13 Parameters for a masking rule

Parameter	Description
Name	Specifies the name of a masking rule.
Resource	Specifies the resource to which the masking rule will apply. **NOTE** A maximum of 100 resources of the service can be added at a time.
Alarm Masking Duration	Specifies the time or duration when the masking rule takes effect. ● **Date and time**: The masking rule takes effect within a specified time range. ● **Date**: The masking rule takes effect in a fixed time range every day. You can also configure the effective date range when the masking rule takes effect. For example, if the effective date is **2022-12-01** to **2022-12-31** and the effective time is **08:00** to **20:00**, the masking rule takes effect from 10:00–11:00 every day from December 1, 2022 to December 31, 2022. ● **Permanent**: The masking rule always takes effect. **NOTE** To change **Alarm Masking Duration** in batches, select multiple masking rules on the **Alarm Masking** page and click **Modify Alarm Masking Duration**.

6. Click **Modify**.

5.8.4 Deleting a Masking Rule

Scenarios

If a masking rule is no long used, you can delete it.

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 Masking**.
4. On the **Alarm Masking** page, locate the target masking rule, and click **Delete** in the **Operation** column. Alternatively, select one or more masking rules and click **Delete** in the upper left of the list.
5. Click **OK**.

5.8.5 Masking an Alarm Rule

Scenarios

This section describes how to mask an alarm rule.

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**.
4. On the **Alarm Rules** page, locate the row that contains the alarm rule to be masked, click **More** in the **Operation** column, and select **Mask Alarms**. On the displayed **Create Alarm Masking** dialog box, configure **Alarm Masking Duration** and click **OK**.

NOTE

The differences between masking an alarm rule and disabling an alarm rule are as follows:

- After an alarm rule is disabled, Cloud Eye does not check whether its metrics reach the threshold or trigger an alarm.
- After an alarm rule is masked, alarm records are still generated but you cannot receive alarm notifications.

6 Server Monitoring

6.1 Overview

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

- Basic monitoring covers metrics automatically reported by ECSs. The data is collected every 5 minutes. For details, see **15 Services Interconnected with Cloud Eye**. BMSs do not support basic monitoring. You need to install the Agent on the BMSs to be monitored.
- OS monitoring provides proactive and fine-grained OS monitoring for ECSs or BMSs, and it requires the Agent to be installed on all servers that will be monitored. The data is collected every minute. OS monitoring supports metrics such as CPU usage and memory usage (Linux). For details, see **15 Services Interconnected with Cloud Eye**.
- Process monitoring provides monitoring of active processes on hosts. By default, Cloud Eye collects CPU usage, memory usage, and number of opened files of active processes.

NOTE

- Windows and Linux OSs are supported. For details, see **What OSs Does the Agent Support?**
- For the ECS specifications, use 2 vCPUs and 4 GiB memory for a Linux ECS and 4 vCPUs and 8 GiB memory or higher specifications for a Windows ECS.
- To install the Agent in a Linux server, you must have the root permissions. For a Windows server, you must have the administrator permissions.

Scenarios

Whether you are using ECSs or BMSs, you can use server monitoring to track various OS metrics, monitor server resource usage, and query monitoring data when faults occur.

Constraints

Server monitoring is available only for servers using Huawei Cloud public images. If any problem occurs when you use a private image, Cloud Eye will not provide technical support.

Monitoring Capabilities

Multiple metrics, such as metrics for CPU, memory, disk, and network usage, will be monitored, meeting the basic monitoring and O&M requirements for servers. For details about metrics, see **15 Services Interconnected with Cloud Eye**.

Resource Usage

The Agent uses considerably less resources. When the Agent is installed on a server, it uses less than 5% of the CPU and less than 100 MB of memory.

6.2 Agent Installation and Configuration

Based on the OS you are going to use, server quantity, and personal habits, install the Agent by choosing one or more of the following scenarios:

Scenario	Service	Reference
Installing the Agent on a Linux server	ECS and BMS	**6.4.1.1 Installing the Agent on a Linux Server**
Installing the Agent on a Windows server	ECS	**6.4.2 Installing the Agent on a Windows Server**
Installing the Agent in batches on Linux servers	ECS	**6.4.1.2 Batch Installing the Agent on Linux Servers**

Agent installation and configuration description:

- To successfully install the Agent, ensure that both DNS and security group rules are correctly configured.

  If the installation fails, restore the DNS configuration of the server by referring to **How Do I Configure DNS and Security Groups?**
- After you install the Agent, you can click **Restore Agent Configurations** on the Cloud Eye console to complete the agency and Agent configuration.
- If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it.
- For details about the OSs that support the Agent, see **What OSs Does the Agent Support?**
- It is recommended that you use an ECS or BMS with the Agent installed to create a private image, use the private image to create another ECS or BMS.

  NOTE

  A private image created in one region cannot be used in another region. Otherwise, no monitoring data will be generated for the ECSs created by using this private image.

  If you install the Agent on an ECS created using a private image, and any problem occurs during the Agent installation and usage, Cloud Eye does not provide technical support.

6.3 Agent Features per Version

NOTE

- By default, the Agent is automatically upgraded, so that you can experience new functions as earlier as possible.
- For details about the images supported by the Cloud Eye Agent, see **What OSs Does the Agent Support?**

This section describes the Agent features provided by each version.

Version 2.6.4.1

Added the following features compared with version 2.6.4:

- GPU metrics
- NPU metrics
- BMS hardware monitoring For details, see **6.7.1 BMS Hardware Monitoring Plug-in**.

Version 2.6.4

Metric UDP Connections is added.

Version 2.5.6.1

Added the following features compared with version 2.5.6:

- GPU metrics
- BMS hardware monitoring For details, see **6.7.1 BMS Hardware Monitoring Plug-in**.

Version 2.5.6

- The Agent architecture is optimized.
- Collection of some metrics is optimized.
- Servers in the same pool can be correctly identified.

Version 2.4.1

The Agent can monitor more metrics.

6.4 Installing the Agent

6.4.1 Installing the Agent on a Linux Server

6.4.1.1 Installing the Agent on a Linux Server

Scenarios

This topic describes how to manually install the Agent on a Linux server.

Constraints

Only Windows and Linux are supported. For details, see **What OSs Does the Agent Support?**

Prerequisites

- You have performed operations described in **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.
- An agency has been configured. For details, see **How Do I Configure an Agency?**
- You have the read and write permissions for the installation directories in **Procedure**. The Telescope process will not be stopped by other software after the installation.
- You have downloaded the Agent installation script.

Table 6-1 Download paths of the Agent installation scripts

Region	Region ID	Download Path
CN North-Beijing1	cn-north-1	**https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/package/agent_install.sh**
CN North-Beijing4	cn-north-4	**https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/package/agent_install.sh**
CN North-Ulanqab1	cn-north-9	**https://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/agent_install.sh**

Region	Region ID	Download Path
CN South-Guangzhou	cn-south-1	**https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/package/agent_install.sh**
CN South-Guangzhou-InvitationOnly	cn-south-4	**https://telescope-cn-south-4.obs.cn-south-4.myhuaweicloud.com/scripts/agentInstall.sh**
CN South-Shenzhen	cn-south-2	**https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/package/agent_install.sh**
CN East-Shanghai1	cn-east-3	**https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/package/agent_install.sh**
CN East-Shanghai2	cn-east-2	**https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/package/agent_install.sh**
CN Southwest-Guiyang1	cn-southwest-2	**https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/package/agent_install.sh**
CN-Hong Kong	ap-southeast-1	**https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/package/agent_install.sh**
AP-Bangkok	ap-southeast-2	**https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/package/agent_install.sh**
AP-Singapore	ap-southeast-3	**https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/package/agent_install.sh**
AP-Jakarta	ap-southeast-4	**https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/agent_install.sh**
AF-Johannesburg	af-south-1	**https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/package/agent_install.sh**
LA-Santiago	la-south-2	**https://obs.la-south-2.myhuaweicloud.com/uniagent-la-south-2/package/agent_install.sh**
LA-Sao Paulo1	sa-brazil-1	**https://telescope-sa-brazil-1.obs.myhuaweicloud.com/scripts/agentInstall.sh**
LA-Mexico City1	na-mexico-1	**https://telescope-na-mexico-1.obs.myhuaweicloud.com/scripts/agentInstall.sh**
LA-Mexico City2	la-north-2	**https://uniagent-la-north-2.obs.la-north-2.myhuaweicloud.com/package/agent_install.sh**

Region	Region ID	Download Path
ME-Riyadh	me-east-1	**https://uniagent-me-east-1.obs.me-east-1.myhuaweicloud.com/package/agent_install.sh**

Procedure

1. Log in to an ECS as user **root**.
2. Run either of the commands below to install the Agent. **agent_install.sh** and **agentInstall.sh** are the installation scripts.

```
Agent of the new architecture: cd /usr/local && curl -k -O ${download_url} && bash
agent_install.sh -t ${version} -u {uniagentVersion} -r {regionID}
Agent of the earlier architecture: cd /usr/local && curl -k -O ${download_url} && bash
agentInstall.sh
```

   Replace *${download_url}* with the download path in **Table 6-1** and *${version}* with the actual Agent version in **Agent Features per Version**. For example, replace *${download_url}* with the download path of CN North-Beijing1. The corresponding installation command is as follows:

```
cd /usr/local && curl -k -O https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/package/
agent_install.sh && bash agent_install.sh -t 2.5.6
```

   If **Telescope process starts successfully.** is displayed after the command is executed, the installation is successful.

3. Run the following command to clear the installation script:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then rm /usr/
local/agent_install.sh; else rm /usr/local/agentInstall.sh; fi
```

NOTE

After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.

6.4.1.2 Batch Installing the Agent on Linux Servers

Scenarios

This topic describes how to batch install the Agent on Linux servers.

Constraints

- Batch installation cannot be performed across regions.
- The servers where the Agent is to be installed in batches must belong to the same VPC.
- The Agent cannot be installed on Windows servers in batches.

Prerequisites

- You have performed operations described in **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.
- An agency has been configured. For details, see **How Do I Configure an Agency?**

- You have the read and write permissions for the installation directories in **Procedure**. The Telescope process will not be stopped by other software after the installation.
- If you will use usernames and passwords to log in to ECSs on which the Agent is to be installed, you have collected IP addresses of all ECSs and the password of user **root**, kept them in the iplist.txt format, and uploaded them to the **/usr/local** directory on the first ECS.

  NOTE

  In the **iplist.txt** file, each line contains only one IP address in the "IP address,Password of user **root**" format.

  In the following example, **abcd** is the password.

  ```
  192.168.1.1,abcd
  192.168.1.2,abcd
  ```

- If you will use key pairs to log in to the ECSs, you have collected IP addresses of all ECSs, kept them in the iplist.txt format, uploaded them to the **/usr/local** directory on the first ECS, and uploaded the key file **user.pem** to the **/usr/local** directory on the ECS.

  NOTE

  In the **iplist.txt** file, each line contains only one IP address.

  An example is provided as follows:

  ```
  192.168.1.1
  192.168.1.2
  ```

- The Agent installation package has been downloaded.

Table 6-2 Download paths of the Agent installation packages

Region	Region ID	Download Path
CN North-Beijing1	cn-north-1	**https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/package/batch_agent_install.sh**
CN North-Beijing4	cn-north-4	**https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/package/batch_agent_install.sh**
CN North-Ulanqab1	cn-north-9	**https://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/batch_agent_install.sh**
CN South-Guangzhou	cn-south-1	**https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/package/batch_agent_install.sh**
CN South-Guangzhou-InvitationOnly	cn-south-4	**https://telescope-cn-south-4.obs.cn-south-4.myhuaweicloud.com/scripts/agentBatchPackage.sh**

Region	Region ID	Download Path
CN South-Shenzhen	cn-south-2	**https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/package/batch_agent_install.sh**
CN East-Shanghai1	cn-east-3	**https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/package/batch_agent_install.sh**
CN East-Shanghai2	cn-east-2	**https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/package/batch_agent_install.sh**
CN Southwest-Guiyang1	cn-southwest-2	**https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/package/batch_agent_install.sh**
CN-Hong Kong	ap-southeast-1	**https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/package/batch_agent_install.sh**
AP-Bangkok	ap-southeast-2	**https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/package/batch_agent_install.sh**
AP-Singapore	ap-southeast-3	**https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/package/batch_agent_install.sh**
AP-Jakarta	ap-southeast-4	**https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/batch_agent_install.sh**
AF-Johannesburg	af-south-1	**https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/package/batch_agent_install.sh**
LA-Santiago	la-south-2	**https://obs.la-south-2.myhuaweicloud.com/uniagent-la-south-2/script/batch_agent_install.sh**
LA-Sao Paulo1	sa-brazil-1	**http://telescope-sa-brazil-1.obs.myhuaweicloud.com/scripts/agentBatchPackage.sh**
LA-Mexico City1	na-mexico-1	**http://telescope-na-mexico-1.obs.myhuaweicloud.com/scripts/agentBatchPackage.sh**
LA-Mexico City2	la-north-2	**https://uniagent-la-north-2.obs.la-north-2.myhuaweicloud.com/package/batch_agent_install.sh**

Region	Region ID	Download Path
ME-Riyadh	me-east-1	**https://uniagent-me-east-1.obs.me-east-1.myhuaweicloud.com/package/batch_agent_install.sh**

Procedure

1. Use SSH to log in to the ECS where the Agent has been installed as user **root**.
2. Run either of the commands below to install the Agent in batches. **batch_agent_install.sh** and **agentBatchPackage.sh** are the installation scripts

```
cd /usr/local && curl -k -O ${download_url} && bash batch_agent_install.sh -t ${version}
cd /usr/local && curl -k -O ${download_url} && bash agentBatchPackage.sh
```

   Replace **${*download_url*}** with the download path in **Table 6-2** and **${*version*}** with the actual Agent version in **6.3 Agent Features per Version**. For example, the installation command for the CN North-Beijing1 region is as follows:

```
cd /usr/local && curl -k -O  https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/script/
batch_agent_install.sh && bash batch_agent_install.sh -t 2.5.6
```

3. After the installation is complete, log in to the Cloud Eye console and choose **Server Monitoring** in the navigation pane on the left.

   View the list of ECSs on which the Agent have been installed.

   NOTE

   After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.

6.4.2 Installing the Agent on a Windows Server

Scenarios

This topic describes how to install the Agent on a Windows server.

Constraints

Only Windows and Linux are supported. For details, see **What OSs Does the Agent Support?**

Prerequisites

- You have performed operations described in **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.
- An agency has been configured. For details, see **How Do I Configure an Agency?**
- An account with the administrator permissions, for example, the administrator account, is used to install the Agent. The Telescope process will not be stopped by other software after the installation.

- You have obtained the Agent installation package in .exe or .zip format.

Table 6-3 Download paths of the Agent installation packages

Region	Region ID	Download Path
CN North-Beijing1	cn-north-1	**https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/package/install_amd64.exe**
CN North-Beijing4	cn-north-4	**https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/package/install_amd64.exe**
CN North-Ulanqab1	cn-north-9	**http://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/install_amd64.exe**
CN Southwest-Guiyang1	cn-southwest-2	**https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/package/install_amd64.exe**
CN South-Guangzhou	cn-south-1	**https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/package/install_amd64.exe**
CN South-Guangzhou-InvitationOnly	cn-south-4	**https://telescope-cn-south-4.obs.cn-south-4.myhuaweicloud.com/agent/telescope_windows_amd64.zip**
CN South-Shenzhen	cn-south-2	**https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/package/install_amd64.exe**
CN East-Shanghai2	cn-east-2	**https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/package/install_amd64.exe**
CN East-Shanghai1	cn-east-3	**https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/package/install_amd64.exe**
CN-Hong Kong	ap-southeast-1	**https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/package/install_amd64.exe**
AP-Bangkok	ap-southeast-2	**https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/package/install_amd64.exe**
AP-Singapore	ap-southeast-3	**https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/package/install_amd64.exe**

Region	Region ID	Download Path
AP-Jakarta	ap-southeast-4	**https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/install_amd64.exe**
AF-Johannesburg	af-south-1	**https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/package/install_amd64.exe**
LA-Santiago	la-south-2	**https://uniagent-la-south-2.obs.la-south-2.myhuaweicloud.com/package/install_amd64.exe**
LA-Sao Paulo1	sa-brazil-1	**https://telescope-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.com/agent/telescope_windows_amd64.zip**
LA-Mexico City1	na-mexico-1	**https://telescope-na-mexico-1.obs.myhuaweicloud.com/agent/telescope_windows_amd64.zip**
LA-Mexico City2	la-north-2	**https://uniagent-la-north-2.obs.la-north-2.myhuaweicloud.com/package/install_amd64.exe**

Procedure

1. Log in to the Windows ECS as an administrator.
2. Open a browser and enter the address of the Agent installation package in the address box to download and save the installation package.
3. Create a directory for storing the installation package, for example, **D:\Agent**.
4. If the installation package is **telescope_windows_amd64.zip**, decompress it and double-click the **install.bat** script to install and start the Agent.
5. If the installation package is **install_amd64.exe**, run the following command using PowerShell:

```
D:\Agent\install_amd64.exe -t ${version}
```

   Replace **${*version*}** with the version in **6.3 Agent Features per Version**. For example, the command for the CN North-Beijing1 region is as follows:

```
D:\Agent\install_amd64.exe -t 2.5.6
```

   NOTE

   After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.

6.5 Installing and Configuring the Agent

6.5.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux)

Scenarios

This topic describes how to add the DNS server address and security group rules to a Linux ECS or BMS to ensure successful downloading of the Agent installation package and successful monitoring data collection. This topic takes an ECS as an example. The operations for BMSs are similar.

You can modify the DNS configuration of an ECS in either of the following ways: command line and management console. Choose a method based on your habits.

NOTE

DNS and security group configuration are intended for the primary NIC.

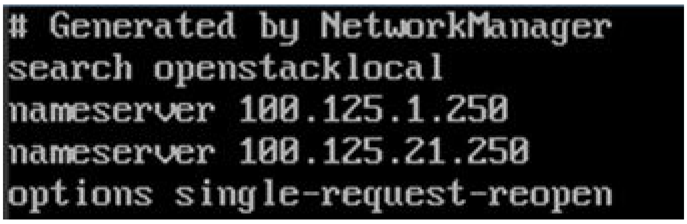
Modifying the DNS Server Address (Command Lines)

The following describes how to add the DNS server address to the **resolv.conf** file using command lines.

To use the management console, see **Modifying the DNS Server Address (Management Console)**.

1. Log in to an ECS as user **root**.
2. Run the **vi /etc/resolv.conf** command to open the file.
3. Add the DNS server address, for example, **nameserver 100.125.1.250** and **nameserver 100.125.21.250** to the file. Enter **:wq** and press **Enter** to save the change.

Figure 6-1 Adding the DNS server address (Linux)



```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 100.125.21.250
options single-request-reopen
```

NOTE

The **nameserver** value varies depending on the region. For details, see **What Are the Private DNS Servers Provided by the Huawei Cloud?**

Modifying the DNS Server Address (Management Console)

The following describes how to modify the DNS server address of an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. In the upper left corner, select a region and project.

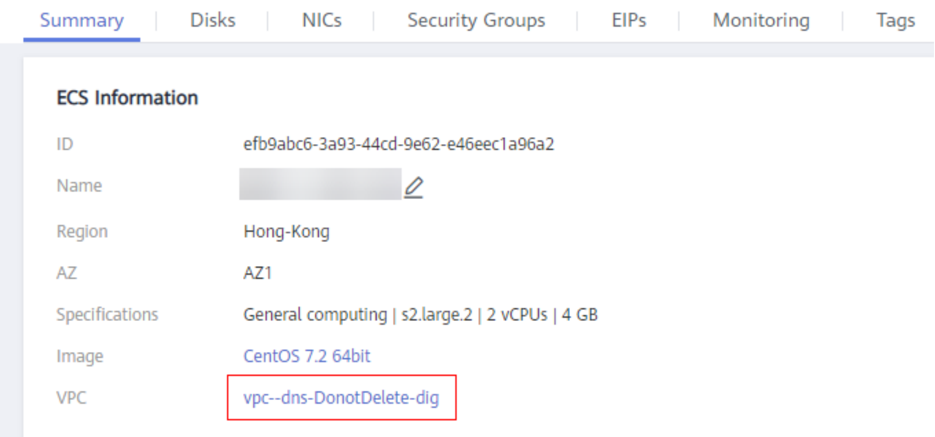
2. Under **Service List**, choose **Computing** > **Elastic Cloud Server**.

   On the ECS console, click the name of the target ECS to view its details.

3. In the **ECS Information** area of the **Summary** tab, click the VPC name. See **Figure 6-2**.

   The **Virtual Private Cloud** page is displayed.

Figure 6-2 VPC



ECS Information

ID efb9abc6-3a93-44cd-9e62-e46eec1a96a2

Name [redacted]

Region Hong-Kong

AZ AZ1

Specifications General computing | s2.large.2 | 2 vCPUs | 4 GB

Image CentOS 7.2 64bit

VPC vpc--dns-DonotDelete-dig

4. Click the name of the target VPC.

5. In the **Networking Components** area, click the number following **Subnets**.

   The **Subnets** page is displayed.

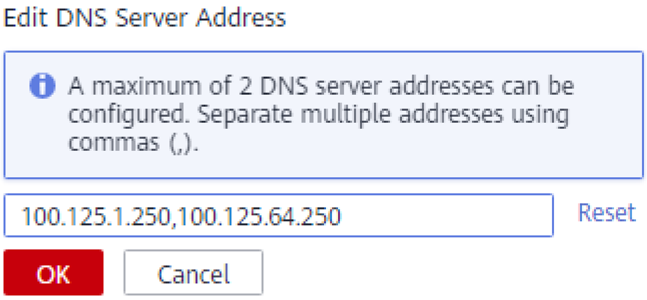
6. In the subnet list, click the name of target subnet.

7. In the **Gateway and DNS Information** area, click ✎ following **DNS Server Address**.

   NOTE

   Set the DNS server address to the value of **nameserver** in **3**.

Figure 6-3 Modify Subnet



Edit DNS Server Address

A maximum of 2 DNS server addresses can be configured. Separate multiple addresses using commas (,).

100.125.1.250,100.125.64.250

8. Click **OK**.

   NOTE

   The new DNS server address takes effect after the ECS or BMS is restarted.

Modifying the ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. On the ECS details page, click the **Security Groups** tab.

   The security group list is displayed.
2. Click the security group name.
3. Click **Modify Security Group Rule**.

   The security group details page is displayed.

   NOTE

   Procedure for BMS:

   1. Click the security group ID on the upper left.
   2. Click **Manage Rule** in the **Operation** column of the security group.
4. Click the **Outbound Rules** tab, and click **Add Rule**.
5. Add rules based on **Table 6-4**.

Table 6-4 Security group rules

Priority	Action	Type	Protocol & Port		Destination	Description
1	Allow	IPv4	TCP	80	100.125.0.0/16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.
1	Allow	IPv4	TCP and UDP	53	100.125.0.0/16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
1	Allow	IPv4	TCP	443	100.125.0.0/16	Used to collect monitoring data to Cloud Eye.

6.5.2 Modifying the DNS Server Address and Adding Security Group Rules (Windows)

Scenarios

This topic describes how to add the DNS server address and security group rules to a Windows ECS to ensure successful downloading of the Agent installation package and successful monitoring data collection.

The DNS server address of an ECS can be modified in either of the following ways: Windows GUI or management console. Choose a method based on your habits.

NOTE

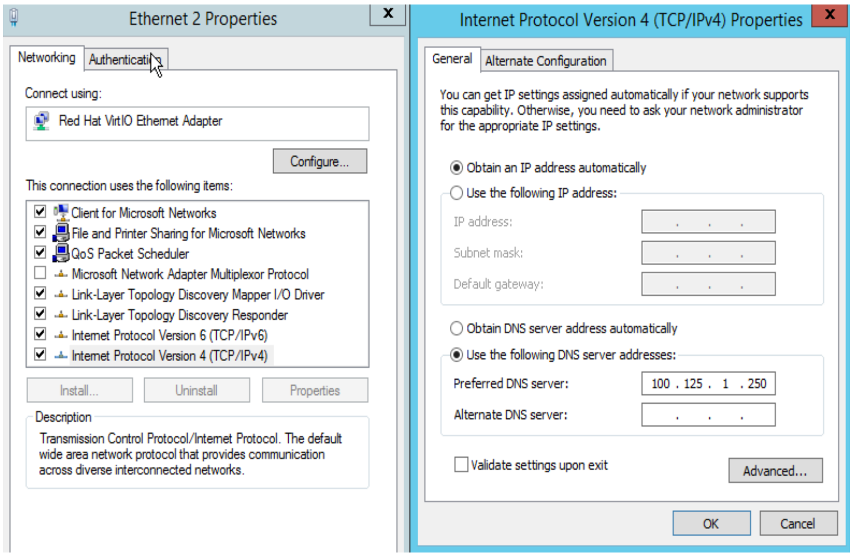
DNS and security group configuration are intended for the primary NIC.

Modifying the DNS Server Address (Windows GUI)

The following describes how to use the Windows GUI to add the DNS server address.

1. Under **Service List**, choose **Computing** > **Elastic Cloud Server**. Use VNC to log in to the Windows ECS.
2. Choose **Control Panel** > **Network and Sharing Center**, and click **Change adapter settings**.
3. Right-click the used network, choose **Settings** from the shortcut menu, and configure the DNS.

Figure 6-4 Adding the DNS server address (Windows)



Ethernet 2 Properties

Networking | Authenticati

Connect using:

Red Hat VirtIO Ethernet Adapter

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 100 . 125 . 1 . 250
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK | Cancel

NOTE

The **nameserver** value varies depending on the region. For details, see **What Are the Private DNS Servers Provided by the Huawei Cloud?**

Modifying the DNS Server Address (Management Console)

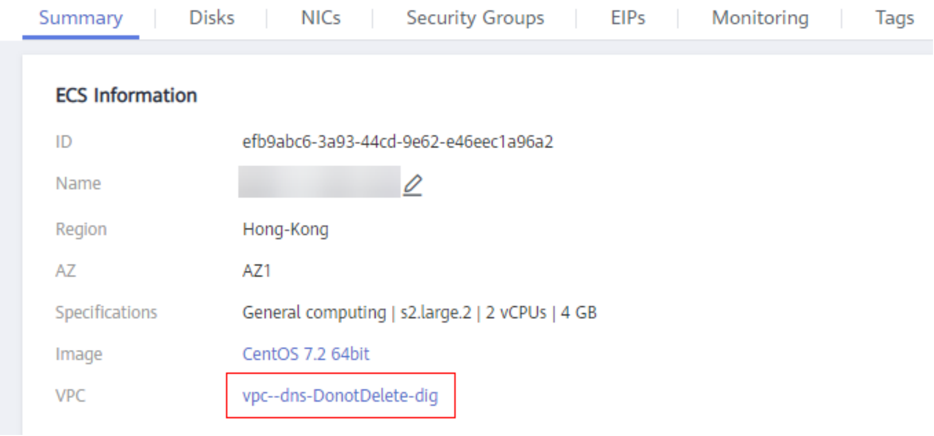
The following describes how to modify the DNS server address of an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. In the upper left corner, select a region and project.
2. Under **Service List**, choose **Computing** > **Elastic Cloud Server**.

   On the ECS console, click the name of the target ECS to view its details.
3. In the **ECS Information** area of the **Summary** tab, click the VPC name.

   The **Virtual Private Cloud** page is displayed.

Figure 6-5 VPC



ECS Information

ID	efb9abc6-3a93-44cd-9e62-e46eec1a96a2
Name	[redacted]
Region	Hong-Kong
AZ	AZ1
Specifications	General computing | s2.large.2 | 2 vCPUs | 4 GB
Image	CentOS 7.2 64bit
VPC	vpc--dns-DonotDelete-dig

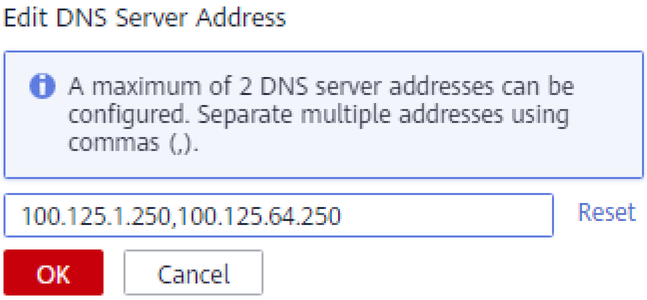
4. Click the name of the target VPC.
5. In the **Networking Components** area, click the number following **Subnets**.

   The **Subnets** page is displayed.
6. In the subnet list, click the name of target subnet.
7. In the **Gateway and DNS Information** area, click ✎ following **DNS Server Address**.

   NOTE

   Set the DNS server address to the value of **nameserver** in **3**.

Figure 6-6 Modify Subnet


Edit DNS Server Address

A maximum of 2 DNS server addresses can be configured. Separate multiple addresses using commas (,).

100.125.1.250,100.125.64.250

8. Click **OK**.

NOTE

The new DNS server address takes effect after the ECS or BMS is restarted.

Modifying the ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. On the ECS details page, click the **Security Groups** tab.

   The security group list is displayed.
2. Click the security group name.
3. Click **Modify Security Group Rule**.

   The security group details page is displayed.

   NOTE

   Procedure for BMS:

   1. Click the security group ID on the upper left.
   2. Click **Manage Rule** in the **Operation** column of the security group.
4. Click the **Outbound Rules** tab, and click **Add Rule**.
5. Add rules based on **Table 6-5**.

Table 6-5 Security group rules

Priority	Action	Type	Protocol & Port		Destination IP Address	Description
1	Allow	IPv4	TCP	80	100.125.0.0/16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.
1	Allow	IPv4	TCP and UDP	53	100.125.0.0/16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.

Priority	Action	Type	Protocol & Port		Destination IP Address	Description
1	Allow	IPv4	TCP	443	100.125.0.0/16	Used to collect monitoring data to Cloud Eye.

6.5.3 (Optional) Manually Configuring the Agent (Linux)

Scenarios

After you install the Agent, configure it by clicking **Restore Agent Configurations** on the Cloud Eye console. If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it by following the instructions provided in this topic.

Prerequisites

The Agent has been installed.

Checking the Version of the Agent In Use

1. Log in to an ECS as user **root**.
2. Run the following command to check the Agent version:

   ```
   if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
   ```

   – If **old agent** is returned, the early version of the Agent is used. For details about how to manually configure the Agent, see **Procedure (for the Early Version of the Agent)**.

   – If a version is returned, the new version of the Agent is used. For details about how to manually configure the Agent, see **Procedure (for the New Version of the Agent)**.

   – If **0** is returned, the Agent is not installed.

Procedure (for the New Version of the Agent)

1. Log in to an ECS as user **root**.
2. Modify the **conf.json** file in the **bin** directory.

   a. Open **conf.json**:

   ```
   vi /usr/local/uniagent/extension/install/telescope/bin/conf.json
   ```

   b. Modify the parameters in the file. For details, see **Table 6-6**.

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all ECS or BMS Agents in the region. For details, see **How Do I Configure an Agency?**

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "ap-southeast-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

Table 6-6 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: ● The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. ● The **InstanceId** value must be consistent with the actual ECS or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you wish to configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS or BMS is located.

Parameter	Description
AccessKey/SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. ● If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. ● If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. **NOTICE** ● For the security purpose, use an IAM username with the **CES Administrator** and **LTS Administrator** permissions. ● The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, if the ECS or BMS is located in the CN-Hong Kong region, **RegionId** is **ap-southeast-1**. For IDs of other regions, see **https://developer.huaweicloud.com/intl/en-us/endpoint**.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.
BmsFlag	Set this parameter to **true** for a BMS. This parameter is not required by an ECS. You do not need to set this parameter for the Windows OS.

Procedure (for the Early Version of the Agent)

1. Log in to an ECS as user **root**.
2. Go to the Agent installation path **bin**:

   cd /usr/local/uniagent/extension/install/telescope/bin

3. Modify configuration file **conf.json**.

   a. Open **conf.json**:

      vi conf.json

b. Modify the parameters in the file. For details, see **Table 6-7**.

ECS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "ap-southeast-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

BMS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "ap-southeast-1",
    "ClientPort": 0,
    "PortNum": 200,
    "BmsFlag": true
}
```

Table 6-7 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: ● The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. ● The **InstanceId** value must be consistent with the actual ECS or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you wish to configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS or BMS is located.

Parameter	Description
AccessKey / SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. ● If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. ● If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. **NOTICE** ● For the security purpose, use an IAM username with the **CES Administrator** and **LTS Administrator** permissions.. ● The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, if the ECS or BMS is located in the CN-Hong Kong region, **RegionId** is **ap-southeast-1**. For IDs of other regions, see **https://developer.huaweicloud.com/intl/en-us/endpoint**.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.
BmsFlag	Set this parameter to **true** for a BMS. This parameter is not required by an ECS. You do not need to set this parameter for the Windows OS.

4. Modify configuration file **conf_ces.json** for the Cloud Eye metric collection module.

   a. Run the following command to open public configuration file **conf_ces.json**:

      vi conf_ces.json

   b. Modify the endpoint in **conf_ces.json**, and save the **conf_ces.json** file. For details, see **Table 6-8**.

```
{
  "Endpoint": "https://ces.ap-southeast-1.myhuaweicloud.com"
}
```

Table 6-8 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region where the ECS or BMS is located. For example, if the ECS or BMS is in the CN-Hong Kong region, **Endpoint** is **ces.ap-southeast-1.myhwclouds.com**. For the endpoint values of other regions, see **https://developer.huaweicloud.com/intl/en-us/endpoint**.

NOTE

- After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.
- If the Agent is in the **Running** state, the Agent has been installed and has started to collect fine-grained metric data.

6.5.4 (Optional) Manually Configuring the Agent on a Windows Server

Scenarios

After you install the Agent, configure it by clicking **Restore Agent Configurations** on the Cloud Eye console. If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it by following the instructions provided in this topic.

Constraints

Windows and Linux OSs are supported. For details, see **What OSs Does the Agent Support?**

Prerequisites

The Agent has been installed.

Checking the Version of the Agent In Use

1. Log in to an ECS as an administrator.
2. Check the installation path and the Agent version.
   - The installation path of the early version of the Agent is **C:\Program Files\telescope**. For details about how to manually configure the Agent, see **Procedure (for the Agent of the Early Version)**.
   - The installation path of the new version of the Agent is **C:\Program Files\uniagent\extension\install\telescope**. For details about how to

manually configure the Agent, see **Procedure (for the Agent of the New Version)**.

Procedure (for the Agent of the New Version)

1. Log in to the ECS.
2. Open the **conf.json** file in the **C:\Program Files\uniagent\extension\install\telescope\bin** folder.
3. Configure the following parameters. For details, see **Table 6-9**.

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all ECS or BMS Agents in the region. For details, see **How Do I Configure an Agency?**

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "ap-southeast-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

Table 6-9 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: ● The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. ● The **InstanceId** value must be consistent with the actual ECS or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you wish to configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS or BMS is located.

Parameter	Description
AccessKey/ SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. ● If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. ● If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. NOTICE ● For the security purpose, use an IAM username with the **CES Administrator** and **LTS Administrator** permissions.. ● The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, if the ECS or BMS is located in the CN-Hong Kong region, **RegionId** is **ap-southeast-1**. For IDs of other regions, see **https://developer.huaweicloud.com/intl/zh-cn/endpoint**.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.

NOTE

- After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.
- If the Agent is in the **Running** state, the Agent has been installed and has started to collect fine-grained metric data.

Procedure (for the Agent of the Early Version)

1. Log in to the ECS.
2. Open the **conf.json** file in the **telescope_windows_amd64\bin** directory.
3. Configure the following parameters. For details, see **Table 6-10**.

```
{
    "InstanceId":"",
    "ProjectId": "",
    "AccessKey": "",
    "SecretKey": "",
    "RegionId": "ap-southeast-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

Table 6-10 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: - The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. - The **InstanceId** value must be consistent with the actual ECS or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you wish to configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS or BMS is located.
AccessKey/ SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. - If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. - If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. **NOTICE** - For security purposes, it is recommended that you perform the above operations as an IAM user with the **CES Administrator** and **LTS Administrator** permissions only.. - The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, if the ECS or BMS is located in the CN-Hong Kong region, **RegionId** is **ap-southeast-1**. For IDs of other regions, see **https://developer.huaweicloud.com/intl/en-us/endpoint**.

Parameter	Description
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.

4. Wait for a few minutes. If **Agent Status** is **Running**, the Agent has been installed and starts to collect fine-grained metric data.

6.6 Managing the Agent

Managing the Agent (Linux)

NOTE

To view, start, stop, update, and uninstall the Agent, you must log in as user **root**.

- **Checking the Agent Version**
  a. Log in to the target ECS as user **root**.
  b. Run the following command to check the Agent version:

     if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then

     /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[-f /usr/local/telescope/bin/telescope]]; then echo "old agent"; else echo 0; fi

     - If **old agent** is returned, the early version of the Agent is used. Manage the Agent based on the Agent version.
     - If a version is returned, the new version of the Agent is used. Manage the Agent based on the Agent version.
     - If **0** is returned, the Agent is not installed.
- **Checking the Agent Status (New Version)**

  Log in to an ECS or BMS as user **root** and run the following command to check the Agent status:

  ```
  /usr/local/uniagent/extension/install/telescope/telescoped status
  ```

  The following message indicates that the Agent is running properly:

  ```
  "Telescope process is running well."
  ```
- **Starting the Agent (New Version)**

  Run the following command to start the Agent:

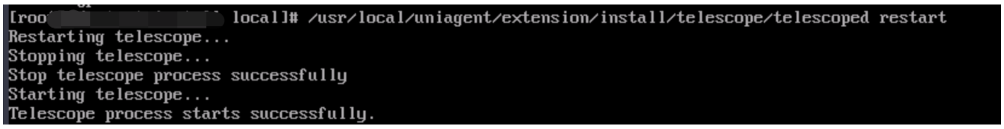
  ```
  /usr/local/uniagent/extension/install/telescope/telescoped start
  ```

- **Restarting the Agent (New Version)**

  Check the Agent PID.

  ```
  /usr/local/uniagent/extension/install/telescope/telescoped restart
  ```

  Figure 6-7 Restarting the Agent

  ```
  [roo[redacted] local]# /usr/local/uniagent/extension/install/telescope/telescoped restart
  Restarting telescope...
  Stopping telescope...
  Stop telescope process successfully
  Starting telescope...
  Telescope process starts successfully.
  ```

- **Stopping the Agent (New Version**)

  Log in to an ECS or BMS and run the following command to stop the Agent:

  ```
  service uniagent stop
  /usr/local/uniagent/extension/install/telescope/telescoped stop
  ```

- **Uninstalling the Agent (New Version)**

  Run the following command to uninstall the Agent:

  ```
  bash /usr/local/uniagent/script/uninstall.sh
  ```

  NOTE

  You can manually uninstall the Agent. After that, Cloud Eye does not proactively collect monitoring data of the server. To use the Agent again, reinstall it by referring to **Procedure** or **Procedure**.

- Checking the Agent Status **(Early Version)**

  Log in to an ECS or BMS as user **root** and run the following command to check the Agent status:

  ```
  service telescoped status
  ```

  The following message indicates that the Agent is running properly:

  "**Active (running)**" or "**Telescope process is running well**."

- **Starting the Agent (Early Version)**

  Run the following command to start the Agent:

  ```
  /usr/local/telescope/telescoped start
  ```

- **Restarting the Agent (Early Version)**

  Run the following command to restart the Agent:

  ```
  /usr/local/telescope/telescoped restart
  ```

- **Stopping the Agent (Early Version)**

  Log in to an ECS or BMS and run the following command to stop the Agent:

  ```
  service telescoped stop
  ```

  NOTE

  If the Agent installation fails, it may be impossible to stop the Agent normally. In this case, run the following command to stop the Agent:

  /usr/local/telescope/telescoped stop

- **Uninstalling the Agent (Early Version)**

  Run the following command to uninstall the Agent:

  ```
  /usr/local/telescope/uninstall.sh
  ```

NOTICE

You can manually uninstall the Agent. After that, Cloud Eye does not proactively collect monitoring data of the server. To use the Agent again, reinstall it by referring to **Procedure** or **Procedure**.

Managing the Agent (Windows)

The default installation path of the early version of the Agent is **C:\Program Files\telescope**.

The default installation path of the Agent is **C:\Program Files\uniagent\extension\install\telescope**.

- **Checking the Agent Status**

  In the task manager, check the status of the telescope process.

- **Starting the Agent**

  In the directory where the Agent installation package is stored, double-click the **start.bat** script.

- **Stopping the Agent**

  In the directory where the Agent installation package is stored, double-click the **shutdown.bat** script.

- **Uninstalling the Agent**

  In the directory where the Agent installation package is stored, double-click the **uninstall.bat** script.

6.7 Installing Other Monitoring Plug-ins

6.7.1 BMS Hardware Monitoring Plug-in

Agent 2.5.6.1 and later versions integrates the BMS hardware monitoring plug-in. The plug-in detects the sub-health status of hardware through real-time inspection, prevents fault risks, and provides comprehensive hardware fault monitoring capabilities for BMSs.

The physical machine hardware monitoring plug-in takes effect only for BMSs.

If the BMS does not have the hardware monitoring plug-in, Huawei Cloud cannot detect the hardware fault in a timely manner, which may affect service availability. In addition, you need to contact technical support to rectify the fault.

After the hardware monitoring plug-in is installed, you will be notified of hardware fault risks in the form of events. You need to authorize Huawei Cloud to repair or replace the risky hardware in a timely manner.

NOTE

- The monitoring plug-in only collect some necessary OS metrics to identify the hardware fault risk. For details, see **Hardware Metric Collection**.
- Only some Linux OSs are supported. For details, see **What OSs Does the Agent Support?**
- Supported flavors: BMSs of all flavors
- If your BMS uses a private image as the OS, ensure that the image have the following software installed: dmidecode, lscpu, dmesg, lspci, modinfo, ifconfig, ethtool, hinicadm, smartctl, lsscsi, and uname.

6.7.2 Installing the GPU Monitoring Plug-in

Scenarios

After the GPU monitoring plug-in is installed on a GPU-accelerated Linux ECS, Cloud Eye provides active and fine-grained GPU monitoring, including collecting GPU metrics and reporting GPU system events. For details about GPU metrics, see **GPU Metrics**.

This section describes how you can use the Cloud Eye Agent installation script to install the new GPU monitoring plug-in on a GPU-accelerated ECS.

- **Procedure (Single-Node Installation)**
- **Procedure (Batch Installation on Multiple Nodes)**

Constraints

- Only ECSs that use certain Linux public images support GPU monitoring. For details, see **What OSs Does the Agent Support?**
- Supported GPU-accelerated ECS specifications: G6v, G6, P2s, P2v, P2vs, G5, Pi2, Pi1 and P1.
- GPU-accelerated ECSs managed by Cloud Container Engine (CCE) are not supported.

Prerequisites

- The GPU driver has been installed on the ECS.

  If no GPU driver is installed on your ECS, install the GPU driver by referring to **GPU Driver**.

  NOTE

  - Use the default path to install the GPU driver.
  - After the GPU driver is installed, restart the GPU-accelerated ECS. Otherwise, GPU metrics may fail to be collected and GPU events may fail to be reported.
  - After the GPU driver is installed, you can view the collected GPU metric data on the Cloud Eye console within 10 minutes.
- lspci is installed on the ECS. Otherwise, GPU metric data cannot be collected and GPU events cannot be reported.

  For details about how to install lspci, see **Installing lspci**.

- Ensure that you have the read and write permissions on the installation directory of the ECS and that the Telescope process will not be stopped by other software after the installation.

Procedure (Single-Node Installation)

For details about the installation commands, see **Procedure**. Replace the version following **-t** in the commands with the version of the plug-in that collects GPU metrics.

Procedure (Batch Installation on Multiple Nodes)

See **Procedure**. Replace the version following **-t** in the installation commands with the version of the plug-in that collects GPU metrics.

Installing lspci

1. Log in to the ECS.
2. Update the image source to obtain the installation dependency.

   wget http://mirrors.myhuaweicloud.com/repo/mirrors_source.sh && bash mirrors_source.sh

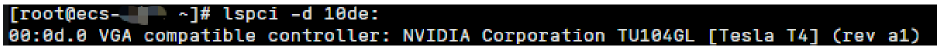
   For more information, see **How Can I Use an Automated Tool to Configure a HUAWEI CLOUD Image Source (x86_64 and Arm)?**
3. Run the following command to install lspci:
   - CentOS:

     yum install pciutils
   - Ubuntu

     apt install pciutils
4. Run the following command to check the installation result:

   lspci -d 10de:

Figure 6-8 Installation result



```
[root@ecs-[redacted] ~]# lspci -d 10de:
00:0d.0 VGA compatible controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
```

NOTE

If the command is not displayed after lspci is installed, restart the ECS.

6.7.3 Installing the Direct Connect Metric Collection Plug-ins

The Direct Connect plug-ins detect the end-to-end network quality of connections, and mainly monitor two metrics of remote subnets: network latency and packet loss rate.

There are two types of Direct Connect plug-ins:

- dc-nqa-collector: monitors the connections created on the Direct Connect console.

- history-dc-nqa-collector: monitors connections created through self-service.

NOTE

- Automated connections are requested by yourself on the console and are classified into self-service connections and full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised. Connections in most regions are automated connections.
- Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be manually configured. Historical connections exist only in some regions.
- If Direct Connect goes offline, manually delete the plug-ins or plug-in configurations. Otherwise, metrics are still collected and reported, triggering false alarms.

Constraints

The plug-ins support only Linux.

Prerequisites

- You have installed the Cloud Eye Agent by referring to **6.4.1 Installing the Agent on a Linux Server**.
- The Agent has been restored.
- You have obtained the password of user **root** for logging in to the target ECS.

Using the One-Click Installation Script to Configure the Plug-ins

In some regions of Huawei Cloud, you can use the one-click installation script to configure the plug-ins. **Table 6-12** lists the supported regions.

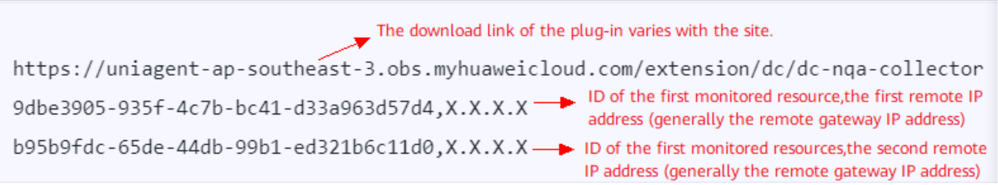
1. Log in to an ECS as user **root**.
2. Run the following command to create the **user.txt** file in the **usr/local/** directory and add user information, including the plug-in download link, monitored resource ID, and remote IP address:

   cd /usr/local/

   vi user.txt

   The content of the **user.txt** file is in the following format.

   Figure 6-9 Example of format



```
https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector
9dbe3905-935f-4c7b-bc41-d33a963d57d4,X.X.X.X
b95b9fdc-65de-44db-99b1-ed321b6c11d0,X.X.X.X
```

The download link of the plug-in varies with the site.
ID of the first monitored resource,the first remote IP address (generally the remote gateway IP address)
ID of the first monitored resources,the second remote IP address (generally the remote gateway IP address)

   Parameter descriptions are as follows:

   a. Plug-in download link: To monitor the connections created on the Direct Connect console, select the dc-nqa-collector plug-in. To monitor the connections created through self-service, select the history-dc-nqa-collector plug-in. To obtain the download address of the installation package in each region, see **Table 6-11**.

b. Information about monitored resources: Enter one resource ID, a comma (,), and one remote IP address in one line. You can add multiple lines of resources in the same format.

   - **Resource ID**: The ID must contain 32 characters, including letters and digits.

     Example: **b95b9fdc-65de-44db-99b1-ed321b6c11d0** or **b95b9fdc65de44db99b1ed321b6c11d0**

     - If the dc-nqa-collector plug-in is used, the resource ID is the virtual interface ID, which can be queried on the **Virtual Interfaces** page of the Direct Connect console.

     - If the history-dc-nqa-collector plug-in is used, the resource ID is the ID of the connection created through self-service, which can be queried on the **Historical Connections** page of the Direct Connect console.

   - **Remote IP address**: indicates the remote IP address that needs to be pinged with the VPC. Generally, it is the remote gateway IP address.

     - If the dc-nqa-collector plug-in is used, enter the IP address of the remote gateway, which can be obtained on the **Virtual Gateways** page of the Direct Connect console.

     - If the history-dc-nqa-collector plug-in is used, enter the host address in the **Remote Subnet** column on the **Historical Connections** page of the Direct Connect console.

NOTE

- Ensure that each monitored resource ID matches only one remote IP address. You are not allowed to enter multiple IP addresses nor CIDR blocks.
- After the plug-in is installed, if you want to add more resources to be monitored, edit the **user.txt** file by adding new IDs and IP addresses in sequence, and then perform **3** and **4**.

Table 6-11 Obtaining the plug-in installation package

Name	Download Path
dc-nqa-collector installation package	CN North-Beijing4: **https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN North-Beijing1: **https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN East-Shanghai1: **https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN East-Shanghai2: **https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN South-Guangzhou: **https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN-Hong Kong: **https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AP-Bangkok: **https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AP-Singapore: **https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AF-Johannesburg: **https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Sao Paulo1: **https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Santiago: **https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Mexico City 1: **https://uniagent-na-mexico-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Mexico City2: **https://uniagent-la-north-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector**

Name	Download Path
history-dc-nqa-collector installation package	CN North-Beijing4: **https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN North-Beijing1: **https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN East-Shanghai1: **https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN East-Shanghai2: **https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN South-Guangzhou: **https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN-Hong Kong: **https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AP-Bangkok: **https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AP-Singapore: **https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AF-Johannesburg: **https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Sao Paulo1: **https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Santiago: **https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Mexico City 1: **https://uniagent-na-mexico-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Mexico City2: **https://uniagent-la-north-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector**

3. Download the one-click installation script to the **/usr/local/** directory.

   wget *Download path of the target region*

Table 6-12 One-click installation script of the Direct Connect plug-ins

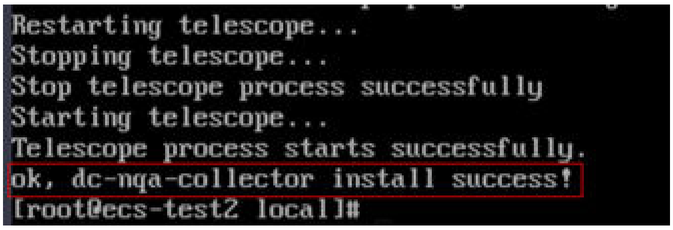
Region	Download Path
CN North-Beijing4	**https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN North-Beijing1	**https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN East-Shanghai1	**https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN East-Shanghai2	**https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN South-Guangzhou	**https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN-Hong Kong	**https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AP-Bangkok	**https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AP-Singapore	**https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AF-Johannesburg	**https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Sao Paulo1	**https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Santiago	**https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Mexico City1	**https://uniagent-na-mexico-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Mexico City2	**https://uniagent-la-north-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**

4. Run the following command to run the plug-in script.

If the installation is successful, the information shown in **Figure 6-10** is displayed.

bash dc-installer.sh

Figure 6-10 Successful installation

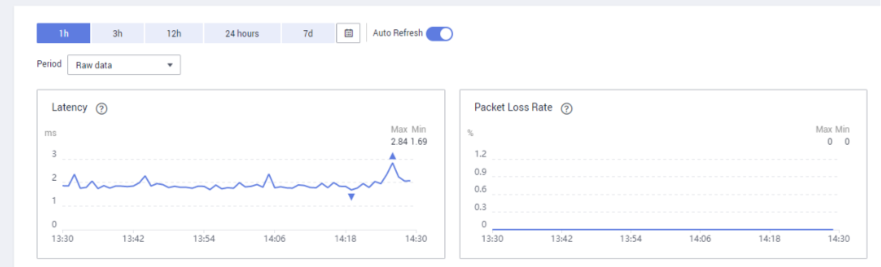


```
Restarting telescope...
Stopping telescope...
Stop telescope process successfully
Starting telescope...
Telescope process starts successfully.
ok, dc-nqa-collector install success!
[root@ecs-test2 local]#
```

5. Wait for about 1 minute after installation and view the Direct Connect monitoring data on the Cloud Eye console.

   Click **Service List**, and select **Cloud Eye**. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Direct Connect**. You can click the name of a monitored object to view the latency and packet loss rate.

Figure 6-11 Network latency and packet loss rate



6.8 Upgrading the Agent

6.8.1 Upgrading the Agent on a Linux Server

Scenarios

This topic describes how you can upgrade the Agent of the early architecture to that of the new architecture.

Constraints

You cannot upgrade the Agent in the following regions: CN South-Guangzhou-InvitationOnly, LA-Sao Paulo1, and LA-Mexico City1.

Procedure

1. Log in to the ECS as user **root**.
2. Run the following command to check the current Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
```

   - If **old agent** is displayed, the early version of the Agent is used.
   - If a version is returned, the new version of the Agent is used.
   - If **0** is returned, the Agent is not installed.
3. Uninstall the Agent.
   - Early version: Run the command in **Uninstalling the Agent (Early Version)**.
   - New version: Run the command in **Uninstalling the Agent (New Version)**.
4. Install the Agent of the latest version by running the command in **Procedure**.

6.8.2 Upgrading the Agent on a Windows Server

Scenarios

This topic describes how to upgrade the Agent of the early architecture to the Agent of the new architecture.

Constraints

You cannot upgrade the Agent in the following regions: CN South-Guangzhou-InvitationOnly, LA-Sao Paulo1, and LA-Mexico City1.

Procedure

1. Log in to the Windows ECS as an administrator.
2. Determine the current Agent version based on the Agent installation path in **Managing the Agent (Windows)**.
3. Uninstall the Agent of the current version by running the command in **Uninstalling the Agent**.
4. Install the Agent of the latest version by running the command in **Procedure**.

6.9 Process Monitoring

Viewing Process Monitoring

Process monitoring is used to monitor active processes on a host. By default, the Agent collects CPU usage, memory usage, and the number of opened files of the active processes. If you have customized process monitoring, the number of processes containing keywords is also monitored.

The Agent collects process CPU usages every minute and displays the top 5 processes, ranked by the CPU usage over the last 24 hours.

NOTE

To view the process monitoring information, install the Agent.

Querying the System Processes

After the Agent is installed, you can check system processes on Cloud Eye.

To query the number of processes, perform the following steps:

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. On the **Server Monitoring** page, locate the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.

   In the **System Processes** area, the process information is displayed. **Table 6-13** describes the metrics of system processes.

Table 6-13 System process metrics

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Running Processes	Number of processes that are running	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Idle Processes	Number of processes that are idle	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Zombie Processes	Number of zombie processes	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Blocked Processes	Number of processes that are blocked	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Sleeping Processes	Number of processes that are sleeping	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Total Processes	Total number of processes	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Monitored object: ECS or BMS Obtain the total number of processes by using the system process status support module **psapi.dll**.

Viewing the Data of Top CPU Processes

- The Agent collects process CPU usages every minute and displays the top 5 processes, ranked by the CPU usage over the last 24 hours.
- Run the **top** command to query the CPU usage and memory usage of a process.
- Run the **lsof** or **ls /proc/*pid*/fd |wc -l** command to query the number of files opened by the current process. In the command, replace *pid* with the ID of the process to be queried.

> **NOTE**
>
> - If a process occupies multiple CPUs, the CPU usage may exceed 100% because the collection result is the total usage of multiple CPUs.
> - The top 5 processes are not fixed. The process list displays the top 5 processes that have entered the statistical period of 1 minute in the last 24 hours.
> - The CPU usage, memory usage, and number of opened files are collected only for the top 5 processes for which monitoring has been enabled in the last 24 hours. If such a process has been stopped, its data will not be displayed.
> - The time in the list indicates the time when a process was created.
> - If the system time on the client browser is different from that on the monitored ECS, the graph may have no metric data. In this case, synchronize the local time with the ECS time.

To query information about top 5 processes with the highest CPU usages

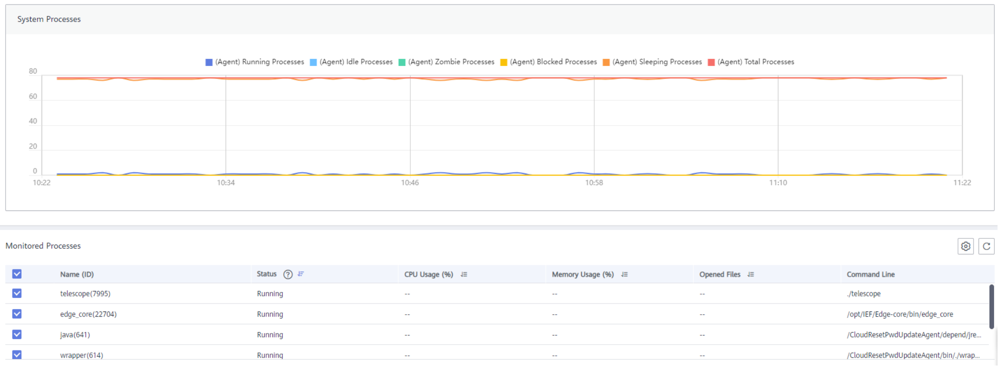
1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.
4. On the **Server Monitoring** page, locate the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.
6. In the **Monitored Processes** area, click ⚙ in the upper right corner to view **Top 5 Processes with Highest CPU Usage**.
7. In the displayed **TOP 5 Processes with Highest CPU Usage** window, enable process monitoring for target processes, and click **OK**.

   In the **Monitored Processes** area, the system selects processes in the **Running** state by default and displays CPU usage curves of those processes in **1h**. The displayed data is raw data.

   You can also select the process to be displayed and view its CPU usage curve in **1h**.

   You can click **CPU Usage**, **Memory Usage**, or **Open Files** above the graph to view the curves of different metrics of the currently displayed process. **Table 6-14** lists **Process Monitoring** metrics.

Figure 6-12 Process monitoring



Monitored Processes

☑	Name (ID)	Status	CPU Usage (%)	Memory Usage (%)	Opened Files	Command Line
☑	telescope(7995)	Running	--	--	--	./telescope
☑	edge_core(22704)	Running	--	--	--	/opt/IEF/Edge-core/bin/edge_core
☑	java(641)	Running	--	--	--	/CloudResetPwdUpdateAgent/depend/jre...
☑	wrapper(614)	Running	--	--	--	/CloudResetPwdUpdateAgent/bin/./wrap...

Table 6-14 Process Monitoring metrics

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
CPU Usage	CPU consumed by a process **pHashId** (process name and process ID) is the value of **md5**.	0 to 1	Monitored object: ECS or BMS Check the metric value changes in file **/proc/pid/stat**.	Monitored object: ECS or BMS Call the API GetProcessTimes to obtain the CPU usage of the process.
Memory Usage	Memory consumed by a process **pHashId** (process name and process ID) is the value of **md5**.	0 to 1	Monitored object: ECS or BMS **Memory Usage** = **RSS*PAGESIZE**/**MemTotal** **RSS**: Obtain its value by checking the second column of file **/proc/pid/statm**. **PAGESIZE**: Obtain its value by running the **getconf PAGESIZE** command. **MemTotal**: Obtain its value by checking file **/proc/meminfo**.	Monitored object: ECS or BMS 1. Invoke Windows API procGlobalMemoryStatusEx to obtain the total memory size. 2. Invoke GetProcessMemoryInfo to obtain the used memory size. 3. Use the used memory size to divide the total memory size to get the memory usage.

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Open Files	The number of opened files consumed by the process **pHashId** (process name and process ID) is the value of **md5**.	≥ 0	Monitored object: ECS or BMS You can run the **ls -l /proc/pid/fd** command to view the number.	Not supported

8. Hover your mouse over a graph. In the upper right corner, click ⤡ to enlarge the graph for viewing detailed data.

   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, you can click **Settings** to configure the rollup method.

Adding Process Monitoring

Process monitoring is used to monitor active processes on a host. By default, the Agent collects CPU usage, memory usage, and the number of opened files of the active processes. Customized process monitoring can collect the number of key processes and obtain the status of key processes at any time.

Monitoring Specified Processes

Suppose that the following processes are running on a server:

```
/usr/bin/java
/usr/bin/ntpd
/telescope
/usr/bin/python
```

Three keywords are configured, and the collection results are as follows:

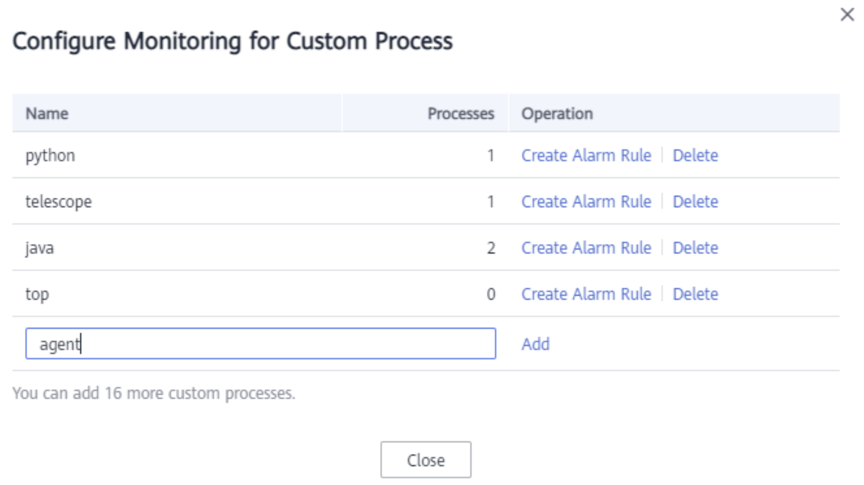
- Key word: Java, number of processes: 1
- Key word: telescope, number of processes: 1
- Key word: /usr/bin, number of processes: 3

Add specified processes.

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. On the **Server Monitoring** page, locate the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.
6. On the **Process Monitoring** page, click **Configure** on the right of the **Custom Processes** area. On the **Configure Monitoring for Custom Process** page, configure the process name or keyword.

Figure 6-13 Configure Monitoring for Custom Process



Configure Monitoring for Custom Process

Name	Processes	Operation
python	1	Create Alarm Rule | Delete
telescope	1	Create Alarm Rule | Delete
java	2	Create Alarm Rule | Delete
top	0	Create Alarm Rule | Delete
agent		Add

You can add 16 more custom processes.

NOTE

You do not need to configure the **Processes** column. After you set the process name, the system will return the number of matched processes.

After the configuration is complete, you can view the number of custom processes in the **Custom Processes** area on the **Process Monitoring** tab.

Enabling Alarm Notification for Custom Process Monitoring

You can configure alarm notifications. When the number of processes decreases or increases, Cloud Eye will notify you immediately.

To enable alarm notifications custom processes, perform the following steps:

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. On the **Server Monitoring** page, locate the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.
6. On the **Process Monitoring** page, click **Configure** on the right of the **Custom Processes** area.

   The **Configure Monitoring for Custom Process** box is displayed.
7. Locate the desired process and click **Create Alarm Rule**.
8. Configure alarm rule information by setting the metric in **Alarm Policy** to **(Agent) Specifies Processes**.

5.2.2 Creating an Alarm Rule lists the parameters to be configured.

6.10 Viewing Server Monitoring Metrics

Scenarios

This topic describes how to view server monitoring metrics, including fine-grained OS metrics collected by the Agent and basic ECS metrics.

For details, see **15 Services Interconnected with Cloud Eye**.

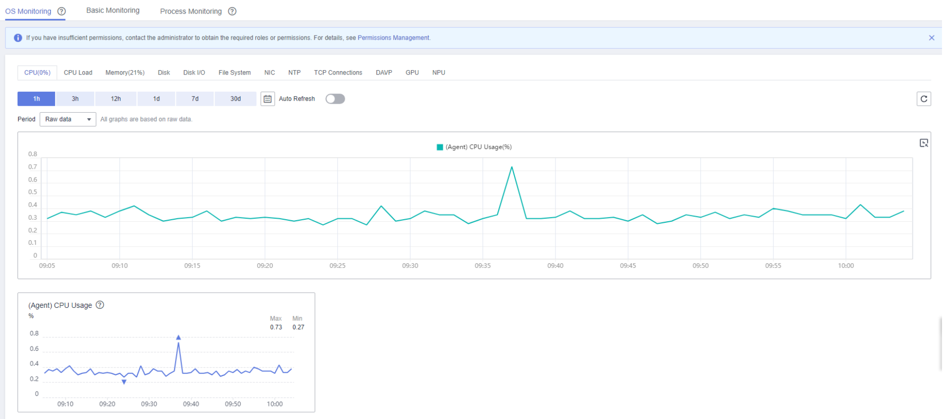
Prerequisites

You have installed the Agent. For details, see **6.5 Installing and Configuring the Agent**.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. View ECS or BMS metrics.
   - To view OS monitoring metrics of an ECS, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column.

Figure 6-14 OS Monitoring



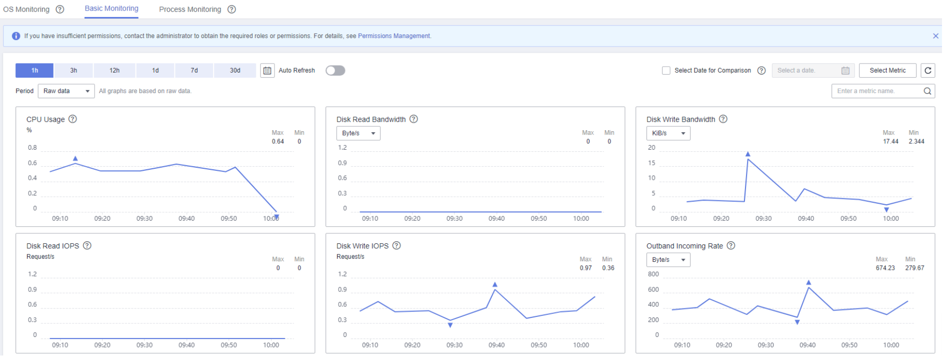
If you have insufficient permissions, contact the administrator to obtain the required roles or permissions. For details, see Permissions Management.

Period: Raw data

All graphs are based on raw data.

   - To view basic monitoring metrics of an ECS, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column. Click the **Basic Monitoring** tab.

Figure 6-15 Basic Monitoring



If you have insufficient permissions, contact the administrator to obtain the required roles or permissions. For details, see Permissions Management.

Period: Raw data — All graphs are based on raw data.

- To view OS monitoring metrics of a BMS, in the left navigation pane, choose **Server Monitoring** > **Bare Metal Server**, locate the BMS, and click **View Metric** in the **Operation** column.
- To view processing monitoring metrics, click the **Process Monitoring** tab.

4. View metrics.

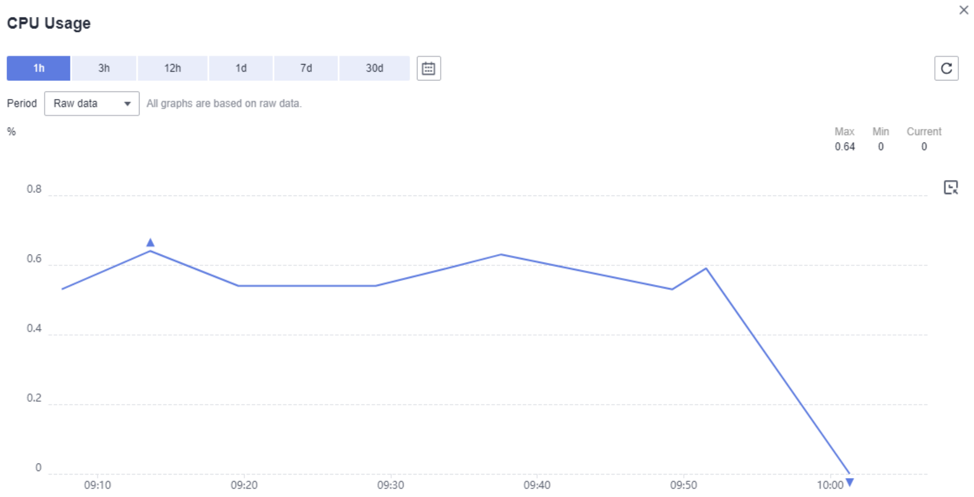
   In the upper part of the **OS Monitoring** page, different metric types, such as CPU, memory, and disk metrics are displayed.

   You can view the monitoring data curves of different metrics. Raw metric data is displayed for the monitoring duration of one hour, three hours, 12 hours, and one day. Rolled-up data is displayed for the monitoring duration of seven days or more. Cloud Eye provides the **Auto Refresh** function at 30-second intervals.

5. Hover your mouse over a graph. In the upper right corner, click to enlarge the graph for viewing detailed data.

   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.

Figure 6-16 (Agent) CPU Usage



Period: Raw data — All graphs are based on raw data.

6.11 Creating an Alarm Rule to Monitor a Server

Scenarios

This topic describes how to create an alarm rule to monitor an ECS or BMS.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Server Monitoring**.
5. Locate the target ECS or BMS. In the **Operation** column, choose **More** > **Create Alarm Rule**.
6. On the **Create Alarm Rule** page, follow the prompts to configure parameters.
   a. Set the alarm rule name, description, and associated enterprise project.

Table 6-15 Parameter description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.
Description	(Optional) Provides supplementary information about the alarm rule.

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

Table 6-16 Parameter description

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
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to.	Specific resources

Parameter	Description	Example Value
Monitored Object	You do not need to set the monitored object because it is the current ECS.	N/A
Method	There are three options: **Associate template**, **Use existing template**, and **Configure manually**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Create manually
Template	Specifies the template to be used. You can select a default alarm template or **a custom template**.	N/A
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average CPU usage of the ECS is 80% or more for three consecutive 5-minute periods. Cloud Eye triggers an alarm every one hour again if the alarm persists. For details about basic and OS monitoring metrics, see **15 Services Interconnected with Cloud Eye**. **NOTE** ● That is, if the alarm is not cleared after it is generated, an alarm notification is sent every hour. ● 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.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

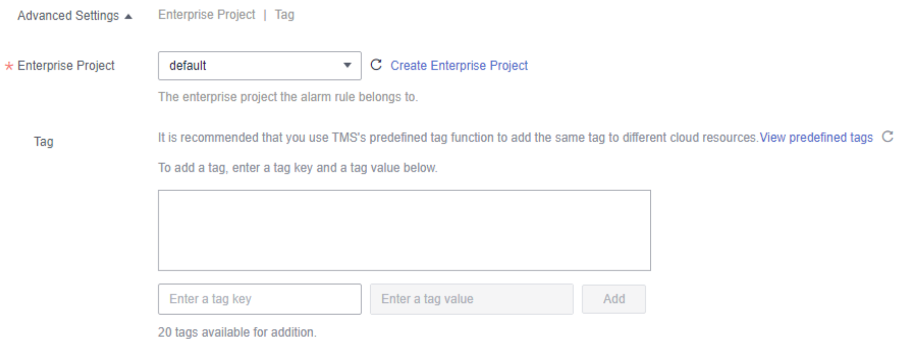
Table 6-17 Alarm Notification parameters

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	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile number and email address of the registered account. ● Topic: A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see **5.5.4.1 Creating a Topic** and **5.5.4.2 Adding Subscriptions**. For the HTTP/HTTPS messages, see **HTTP/HTTPS Messages**.
Validity Period	Cloud Eye sends notifications only within the notification window specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.
Trigger Condition	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.

d. Configure the enterprise project and tag.

Figure 6-17 Advanced Settings



Advanced Settings ▲ Enterprise Project | Tag

* Enterprise Project: default ▾ Create Enterprise Project

The enterprise project the alarm rule belongs to.

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

Enter a tag key | Enter a tag value | Add

20 tags available for addition.

Table 6-18 Parameters of **Advanced Settings**

Parameter	Description
Enterprise Project	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, see **Creating an Enterprise Project**.

Parameter	Description
Tag	A tag is a key-value pair. Tags identify cloud resources so that you can easily categorize and search for your resources. You are advised to create predefined tags in TMS. For details, see **Creating Predefined Tags**. If you have configured tag policies for Cloud Eye, add tags to alarm rules based on the tag policies. If you add a tag that does not comply with the tag policies, alarm rules may fail to be created. Contact your administrator to learn more about tag policies. ● A key can contain a maximum of 128 characters, and a value can contain a maximum of 225 characters. ● A maximum of 20 tags can be added.

e. Click **Create**.

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

7 Cloud Service Monitoring

7.1 Viewing Raw Data

Scenarios

This topic describes how to view the monitoring data saved in the OBS bucket by downloading metric data files.

Prerequisites

- You have successfully configured data storage on Cloud Eye.
- You have installed Java and configured environment variables.
- You have downloaded the format conversion tool metric-transfer-merge.jar .

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**. Locate the target resource and select the specified OBS bucket in the **Permanent Data Storage** column.

   Alternatively, in the navigation pane on the left, choose **Server Monitoring**. Locate the target ECS, and select the specified OBS bucket in the **Permanent Data Storage** column.
4. Select the metric data file you want to view in the OBS bucket. Based on the storage path of the metric data file, select *OBS bucket name* > *CloudEye* > *Region* > *Year* > *Month* > *Day* > *Service type directory* > *Resource type directory*. Click **Download** in the **Operation** column to download the file to the default path. To download the metric data file to a customized path, click **Download As**.

   The metric data file is named in the following format:

*Metric data file prefix*_CloudEye_*Region*_*Time when the log was uploaded to the OBS: year-month-day*T*hour-minute-second*Z_*Randomly generated character*.json.gz

Example: *File Prefix*_CloudEye_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.json

NOTE

- The OBS bucket name and trace file prefix are user-defined, and other parameters are automatically generated.
- Original metric data files are segment files of time granularity. The files include all metric data of a resource under the time segment. The metric data is stored in the JSON format.
- To facilitate your operations, Cloud Eye provides the format conversion and content combination tool. Using this tool, you can combine the files of several time slices in a specific resource into a time-staged file in the chronological order in the .csv format. In addition, you can use the tool to generate an independent time splice file for every metric of the resource in the .csv format.

5. Access the cmd tool in the Windows system. Go to the folder where **metric-transfer-merge.jar** is located, run the **java -jar metric-transfer-merge.jar j2c inputDirectory outputDirectory mergFileName** command.

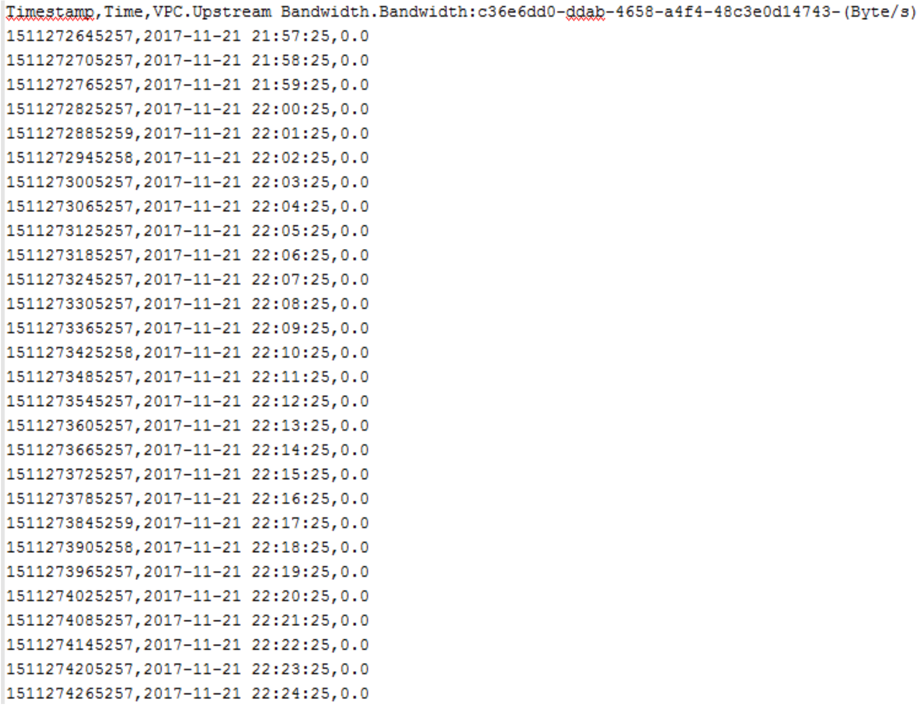
   In the Linux system, run the **java-jar metric-transfer-merge.jar inputDirectory outputDirectory mergFileName** command in the shell command line.

   NOTE

   - **j2c** is the command to convert JSON into CSV.
   - **inputDirectory** is the directory to store the downloaded JSON files.
   - **outputDirectory** is the directory to store the generated files.
   - **mergFileName** is the name of the specified combined file for users. This parameter can be ignored because the tool will name the combined file as **mergeResult.csv** by default.

   After running the java command, you can view the converted files in the **outputDirectory** directory. Each file corresponds to the data of one metric at all time points. **mergeResult.csv** is a large file generated by combining the data of all metrics. **Figure 7-1** shows the content of the converted file.

Figure 7-1 Metric data



```
Timestamp,Time,VPC.Upstream Bandwidth.Bandwidth:c36e6dd0-ddab-4658-a4f4-48c3e0d14743-(Byte/s)
1511272645257,2017-11-21 21:57:25,0.0
1511272705257,2017-11-21 21:58:25,0.0
1511272765257,2017-11-21 21:59:25,0.0
1511272825257,2017-11-21 22:00:25,0.0
1511272885259,2017-11-21 22:01:25,0.0
1511272945258,2017-11-21 22:02:25,0.0
1511273005257,2017-11-21 22:03:25,0.0
1511273065257,2017-11-21 22:04:25,0.0
1511273125257,2017-11-21 22:05:25,0.0
1511273185257,2017-11-21 22:06:25,0.0
1511273245257,2017-11-21 22:07:25,0.0
1511273305257,2017-11-21 22:08:25,0.0
1511273365257,2017-11-21 22:09:25,0.0
1511273425258,2017-11-21 22:10:25,0.0
1511273485257,2017-11-21 22:11:25,0.0
1511273545257,2017-11-21 22:12:25,0.0
1511273605257,2017-11-21 22:13:25,0.0
1511273665257,2017-11-21 22:14:25,0.0
1511273725257,2017-11-21 22:15:25,0.0
1511273785257,2017-11-21 22:16:25,0.0
1511273845259,2017-11-21 22:17:25,0.0
1511273905258,2017-11-21 22:18:25,0.0
1511273965257,2017-11-21 22:19:25,0.0
1511274025257,2017-11-21 22:20:25,0.0
1511274085257,2017-11-21 22:21:25,0.0
1511274145257,2017-11-21 22:22:25,0.0
1511274205257,2017-11-21 22:23:25,0.0
1511274265257,2017-11-21 22:24:25,0.0
```

8 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.

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.

   📖 NOTE

   Only after you add monitoring data through APIs, will those data be displayed on the Cloud Eye console. For details about how to add monitoring data, see **Adding Monitoring Data**.
5. Locate the row that contains the cloud resource to be viewed, and click **View Metric**.

   On the page displayed, you can view graphs based on raw data collected in **1h**, **3h**, **12h**, **24h**, and **7d**. In the upper right corner of each graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed.

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. On the **Custom Monitoring** page, locate the target resource and click **Create Alarm Rule** in the **Operation** column.
5. On the **Create Alarm Rule** page, follow the prompts to configure the parameters. For details, see **Table 5-1** and **Table 5-3**.
6. Click **Create**.

9 Event Monitoring

9.1 Introduction to Event Monitoring

In event monitoring, you can query system events that are automatically reported to Cloud Eye 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. Event monitoring does not depend on the Agent.

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. For details, see **9.4 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**.

9.2 Viewing Event Monitoring Data

Scenarios

This topic describes how to view the event monitoring data.

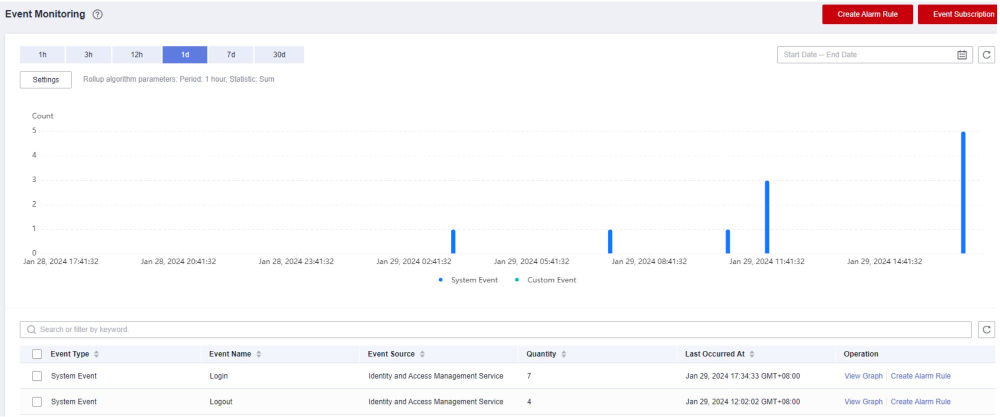
Procedure

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 **Event Monitoring**.

   On the displayed **Event Monitoring** page, all system events generated in the last 24 hours are displayed by default.

   You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view events generated in different periods.

   Figure 9-1 Event monitoring

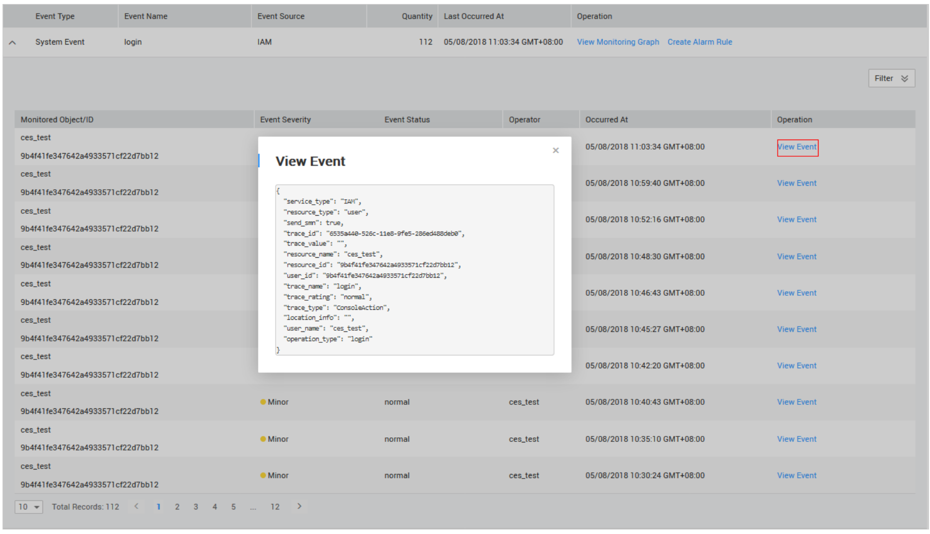


Rollup algorithm parameters: Period: 1 hour, Statistic: Sum

□ Event Type	Event Name	Event Source	Quantity	Last Occurred At	Operation
□ System Event	Login	Identity and Access Management Service	7	Jan 29, 2024 17:34:33 GMT+08:00	View Graph | Create Alarm Rule
□ System Event	Logout	Identity and Access Management Service	4	Jan 29, 2024 12:02:02 GMT+08:00	View Graph | Create Alarm Rule

4. Expand an event, and click **View Event** in the **Operation** column to view details about a specific event.

   Figure 9-2 Viewing event details



Event Type	Event Name	Event Source	Quantity	Last Occurred At	Operation
System Event	login	IAM	112	05/08/2018 11:03:34 GMT+08:00	View Monitoring Graph Create Alarm Rule

Monitored Object/ID	Event Severity	Event Status	Operator	Occurred At	Operation
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 11:03:34 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:59:40 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:52:16 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:48:30 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:46:43 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:45:27 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12				05/08/2018 10:42:20 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12	● Minor	normal	ces_test	05/08/2018 10:40:43 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12	● Minor	normal	ces_test	05/08/2018 10:35:10 GMT+08:00	View Event
ces_test 9b4f41fe347642a4933571cf22d7bb12	● Minor	normal	ces_test	05/08/2018 10:30:24 GMT+08:00	View Event

10 ▾ Total Records: 112 < 1 2 3 4 5 ... 12 >

View Event

```
{
  "service_type": "IAM",
  "resource_type": "user",
  "send_smn": true,
  "trace_id": "6535a440-526c-11e8-9fe5-286ed488deb0",
  "trace_value": "",
  "resource_name": "ces_test",
  "resource_id": "9b4f41fe347642a4933571cf22d7bb12",
  "user_id": "9b4f41fe347642a4933571cf22d7bb12",
  "trace_name": "login",
  "trace_rating": "normal",
  "trace_type": "ConsoleAction",
  "location_info": "",
  "user_name": "ces_test",
  "operation_type": "login"
}
```

9.3 Creating an Alarm Rule to Monitor an Event

Scenarios

This topic describes how to create an alarm rule to monitor an event.

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 **Event Monitoring**.
4. On the event list page, click **Create Alarm Rule** in the upper right corner.
5. On the **Create Alarm Rule** page, configure the parameters.

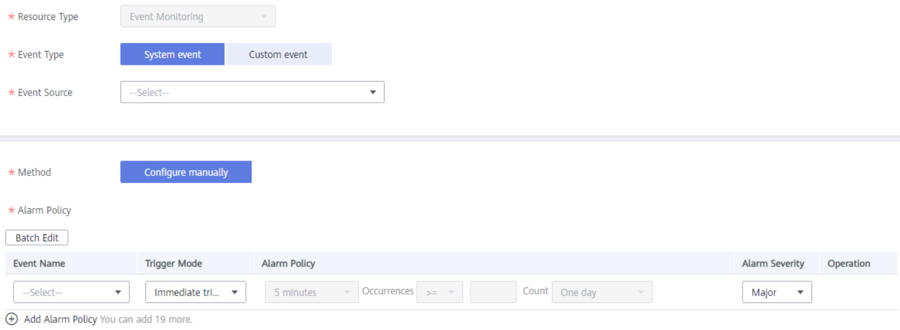
   a. Set the alarm rule name and description.

   Table 9-1 Parameter description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.
Description	(Optional) Provides supplementary information about the alarm rule.

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

   Figure 9-3 Configuring parameters



* Resource Type: Event Monitoring

* Event Type: System event | Custom event

* Event Source: --Select--

* Method: Configure manually

* Alarm Policy

Batch Edit

Event Name	Trigger Mode	Alarm Policy	Alarm Severity	Operation
--Select--	Immediate tri...	5 minutes Occurrences >= Count One day	Major	

Add Alarm Policy You can add 19 more.

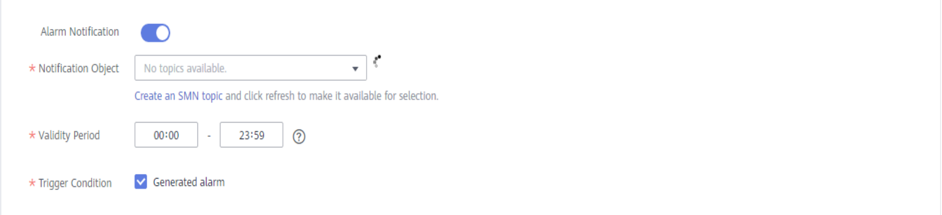
   Table 9-2 Parameter description

Parameter	Description
Alarm Type	Specifies the alarm type to which the alarm rule applies. The value can be **Metric** or **Event**.

Parameter	Description
Event Type	Specifies the event type, which can be **System event** or **Custom event**.
Event Source	Specifies the service the event is generated for. Example value: **Elastic Cloud Server** For a custom event, set **Event Source** to the value of **event_source**.
Monitoring Scope	Specifies the monitoring scope for event monitoring. Example value: **All resources**
Method	Specifies the means you use to create the alarm rule.
Event Name	Specifies the instantaneous operations users performed on resources, such as login and logout. For events supported by event monitoring, see **9.4 Events Supported by Event Monitoring**. Example value: **Delete ECS**
Trigger Mode	You can select immediate trigger or accumulative trigger based on the operation severity. Example value: **Immediate trigger**
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the event occurred for three consecutive periods of 5 minutes. **NOTE** This parameter is mandatory when **Triggering Mode** is set to **Accumulative Trigger**.
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**. Example value: **Major**

c. Configure the alarm notification.

Figure 9-4 Alarm notification



Alarm Notification

* Notification Object: No topics available.

Create an SMN topic and click refresh to make it available for selection.

* Validity Period: 00:00 - 23:59

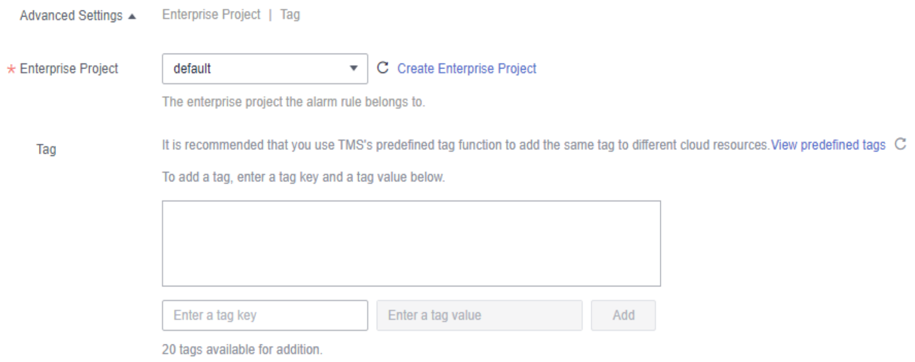
* Trigger Condition: ☑ Generated alarm

Table 9-3 Parameter description

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.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● **Topic**: 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 **5.5.4.1 Creating a Topic** and **5.5.4.2 Adding Subscriptions**.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00–20:00.
Trigger Condition	Specifies the trigger of alarm notifications.

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

Figure 9-5 Advanced Settings



Advanced Settings ▴ Enterprise Project | Tag

* Enterprise Project: default

The enterprise project the alarm rule belongs to.

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

20 tags available for addition.

Table 9-4 Name and **Description**

Parameter	Description
Enterprise Project	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**.

Parameter	Description
Tag	A tag consists of a key-value pair. Tags can be used to categorize and search for your resources. You can create tags using TMS. For details, see **Creating Predefined Tags**. 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, contact your administrator to learn more about the tag policies. ● 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**.

9.4 Events Supported by Event Monitoring

Table 9-5 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	Restart triggered due to hardware fault	startAutoRecovery	Major	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs was restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.
	Restart completed due to hardware failure	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Auto recovery timeout (being processed on the backend)	faultAutoRecovery	Major	Migrating the ECS to a normal host timed out.	Migrate services to other ECSs.	Services are interrupted.
	GPU link fault	GPULinkFault	Critical	The GPU of the host on which the ECS is located was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the GPU fault is rectified, check whether services are restored.	Services are interrupted.
	ECS deleted	deleteServer	Major	The ECS was deleted ● on the management console. ● by calling APIs.	Check whether the deletion was performed intentionally by a user.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS restarted	rebootServer	Minor	The ECS was restarted ● on the management console. ● by calling APIs.	Check whether the restart was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the ECS starts up, check whether services recover.	Services are interrupted.
	ECS stopped	stopServer	Minor	The ECS was stopped ● on the management console. ● by calling APIs. **NOTE** The ECS is stopped only **after CTS is enabled**.	● Check whether the restart was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NIC deleted	deleteNic	Major	The ECS NIC was deleted ● on the management console. ● by calling APIs.	● Check whether the deletion was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the NIC is deleted, check whether services recover.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS resized	resizeServer	Minor	The ECS specifications were resized - on the management console. - by calling APIs.	- Check whether the operation was performed by a user. - Deploy service applications in HA mode. - After the ECS is resized, check whether services have recovered.	Services are interrupted.
	GuestOS restarted	RestartGuestOS	Minor	The guest OS was restarted.	Contact O&M personnel.	Services may be interrupted.
	ECS failure due to abnormal host processes	VMFaultsByHostProcessExceptions	Critical	The processes of the host accommodating the ECS were abnormal.	Contact O&M personnel.	The ECS is faulty.
	Startup failure	faultPowerOn	Major	The ECS failed to start.	Start the ECS again. If the problem persists, contact O&M personnel.	The ECS cannot start.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Host breakdown risk	hostMayCrash	Major	The host where the ECS resides may break down, and the risk cannot be prevented through live migration due to some reasons.	Migrate services running on the ECS first and delete or stop the ECS. Start the ECS only after the O&M personnel eliminate the risk.	The host may break down, causing service interruption.
	Scheduled migration completed	instance_migrate_completed	Major	Scheduled ECS migration is completed.	Wait until the ECSs become available and check whether services are affected.	Services may be interrupted.
	Scheduled migration being executed	instance_migrate_executing	Major	ECSs are being migrated as scheduled.	Wait until the event is complete and check whether services are affected.	Services may be interrupted.
	Scheduled migration canceled	instance_migrate_canceled	Major	Scheduled ECS migration is canceled.	None	None
	Scheduled migration failed	instance_migrate_failed	Major	ECSs failed to be migrated as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled migration to be executed	instance_migrate_scheduled	Major	ECSs will be migrated as scheduled.	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled specification modification failed	instance_resize_failed	Major	Specifications failed to be modified as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled specification modification completed	instance_resize_completed	Major	Scheduled specifications modification is completed.	None	None
	Scheduled specification modification being executed	instance_resize_executing	Major	Specifications are being modified as scheduled.	Wait until the event is completed and check whether services are affected.	Services are interrupted.
	Scheduled specification modification canceled	instance_resize_canceled	Major	Scheduled specifications modification is canceled.	None	None
	Scheduled specification modification to be executed	instance_resize_scheduled	Major	Specifications will be modified as scheduled.	Check the impact on services during the execution window.	None
	Scheduled redeployment to be executed	instance_redeploy_scheduled	Major	ECSs will be redeployed on new hosts as scheduled.	Check the impact on services during the execution window.	None
	Scheduled restart to be executed	instance_reboot_scheduled	Major	ECSs will be restarted as scheduled.	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled stop to be executed	instance_stop_scheduled	Major	ECSs will be stopped as scheduled as they are affected by underlying hardware or system O&M.	Check the impact on services during the execution window.	None
	Live migration started	liveMigrationStarted	Major	The host where the ECS is located may be faulty. Live migrate the ECS in advance to prevent service interruptions caused by host breakdown.	Wait for the event to end and check whether services are affected.	Services may be interrupted for less than 1s.
	Live migration completed	liveMigrationCompleted	Major	The live migration is complete, and the ECS is running properly.	Check whether services are running properly.	None
	Live migration failure	liveMigrationFailed	Major	An error occurred during the live migration of an ECS.	Check whether services are running properly.	There is a low probability that services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECC uncorrectable error alarm generated on GPU SRAM	SRAMUncorrectableEccError	Major	There are ECC uncorrectable errors generated on GPU SRAM.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the GPU memory is faulty, and services exit abnormally.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host on which the ECS is located was ● faulty. ● recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.
	Scheduled redeployment to be authorized	instance_redeploy_inquiring	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Authorize scheduled redeployment.	None
	Local disk replacement canceled	localdisk_recovery_canceled	Major	Local disk failure	None	None
	Local disk replacement to be executed	localdisk_recovery_scheduled	Major	Local disk failure	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Xid event alarm generated on GPU	commonXidError	Major	A xid event alarm occurs on GPU.	If services are affected, submit a service ticket.	The GPU hardware, driver, and application problems lead to Xid events, which may lead to abnormal exit of the business.
	nvidia-smi suspended	nvidiaSmiHangEvent	Major	nvidia-smi timed out.	If services are affected, submit a service ticket.	The driver may report an error during service running.
	NPU: uncorrectable ECC error	UncorrectableEccErrorCount	Major	There are uncorrectable ECC errors generated on GPU SRAM.	If services are affected, replace the NPU with another one.	Services may be interrupted.
	Scheduled redeployment canceled	instance_redeploy_canceled	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled redeployment being executed	instance_redeploy_executing	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Wait until the event is complete and check whether services are affected.	Services are interrupted.
	Scheduled redeployment completed	instance_redeploy_completed	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Wait until the redeployed ECSs are available and check whether services are affected.	None
	Scheduled redeployment failed	instance_redeploy_failed	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Contact O&M personnel.	Services are interrupted.
	Local disk replacement to be authorized	localdisk_recovery_inquiring	Major	Local disks are faulty.	Authorize local disk replacement.	Local disks are unavailable.
	Local disks being replaced	localdisk_recovery_executing	Major	Local disk failure	Wait until the local disks are replaced and check whether the local disks are available.	Local disks are unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Local disks replaced	localdisk_recovery_completed	Major	Local disk failure	Wait until the services are running properly and check whether local disks are available.	None
	Local disk replacement failed	localdisk_recovery_failed	Major	Local disks are faulty.	Contact O&M personnel.	Local disks are unavailable.

NOTE

Once a physical host running ECSs breaks down, the ECSs are automatically migrated to a functional physical host. During the migration, the ECSs will be restarted.

Table 9-6 Bare Metal Server (BMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	ECC uncorrectable error alarm generated on GPU SRAM	SRAMUncorrectableEccError	Major	There are ECC uncorrectable errors generated on GPU SRAM.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the GPU memory is faulty, and services exit abnormally.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	BMS restarted	osReboot	Major	The BMS was restarted ● on the management console. ● by calling APIs.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	Unexpected restart	serverReboot	Major	The BMS restarted unexpectedly, which may be caused by ● OS faults. ● hardware faults.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	BMS stopped	osShutdown	Major	The BMS was stopped ● on the management console. ● by calling APIs.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Unexpected shutdown	serverShutdown	Major	The BMS was stopped unexpectedly, which may be caused by ● unexpected power-off. ● hardware faults.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.
	Network disconnection	linkDown	Major	The BMS network was disconnected. Possible causes are as follows: ● The BMS was unexpectedly stopped or restarted. ● The switch was faulty. ● The gateway was faulty.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	PCIe error	pcieError	Major	The PCIe devices or main board of the BMS was faulty.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	The network or disk read/write services are affected.
	Disk fault	diskError	Major	The disk backplane or disks of the BMS were faulty.	● Deploy service applications in HA mode. ● After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	EVS error	storage Error	Major	The BMS failed to connect to EVS disks. Possible causes are as follows: ● The SDI card was faulty. ● Remote storage devices were faulty.	● Deploy service applications in HA mode. ● After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Inforom alarm generated on GPU	gpuInfoROMAlarm	Major	The driver failed to read inforom information due to GPU faults.	Non-critical services can continue to use the GPU card. For critical services, submit a service ticket to resolve this issue.	Services will not be affected if inforom information cannot be read. If error correction code (ECC) errors are reported on GPU, faulty pages may not be automatically retired and services are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Double-bit ECC alarm generated on GPU	doubleBitEccError	Major	A double-bit ECC error occurred on GPU.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted. After faulty pages are retired, the GPU card can continue to be used.
	Too many retired pages	gpuTooManyRetiredPagesAlarm	Major	An ECC page retirement error occurred on GPU.	If services are affected, submit a service ticket.	Services may be affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECC alarm generated on GPU A100	gpuA100EccAlarm	Major	An ECC error occurred on GPU.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted. After faulty pages are retired, the GPU card can continue to be used.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU ECC memory page retirement failure	eccPageRetirementRecordingFailure	Major	Automatic page retirement failed due to ECC errors.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted, and memory page retirement fails. As a result, services cannot no longer use the GPU card.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU ECC page retirement alarm generated	eccPageRetirementRecordingEvent	Minor	Memory pages are automatically retired due to ECC errors.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Generally, this alarm is generated together with the ECC error alarm. If this alarm is generated independently, services are not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Too many single-bit ECC errors on GPU	highSingleBitEccErrorRate	Major	There are too many single-bit ECC errors.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Single-bit errors can be automatically rectified and do not affect GPU-related applications.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU card not found	gpuDriverLinkFailureAlarm	Major	A GPU link is normal, but the NVIDIA driver cannot find the GPU card.	1. Restart the VM to restore services. 2. If services still cannot be restored, submit a service ticket.	The GPU card cannot be found.
	GPU link faulty	gpuPcieLinkFailureAlarm	Major	GPU hardware information cannot be queried through lspci due to a GPU link fault.	If services are affected, submit a service ticket.	The driver cannot use GPU.
	GPU card lost	vmLostGpuAlarm	Major	The number of GPU cards on the VM is less than the number specified in the specifications.	If services are affected, submit a service ticket.	GPU cards get lost.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU memory page faulty	gpuMemoryPageFault	Major	The GPU memory page is faulty, which may be caused by applications, drivers, or hardware.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the GPU memory is faulty, and services exit abnormally.
	GPU image engine faulty	graphicsEngineException	Major	The GPU image engine is faulty, which may be caused by applications, drivers, or hardware.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the image engine is faulty, and services exit abnormally.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU temperature too high	highTemperatureEvent	Major	GPU temperature too high	If services are affected, submit a service ticket.	If the GPU temperature exceeds the threshold, the GPU performance may deteriorate.
	GPU NVLink faulty	nvlinkError	Major	A hardware fault occurs on the NVLink.	If services are affected, submit a service ticket.	The NVLink link is faulty and unavailable.
	System maintenance inquiring	system_maintenance_inquiring	Major	The scheduled BMS maintenance task is being inquired.	Authorize the maintenance.	None
	System maintenance waiting	system_maintenance_scheduled	Major	The scheduled BMS maintenance task is waiting to be executed.	Clarify the impact on services during the execution window and ensure that the impact is acceptable to users.	None
	System maintenance canceled	system_maintenance_canceled	Major	The scheduled BMS maintenance is canceled.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	System maintenance executing	system_maintenance_executing	Major	BMSs are being maintained as scheduled.	After the maintenance is complete, check whether services are affected.	Services are interrupted.
	System maintenance completed	system_maintenance_completed	Major	The scheduled BMS maintenance is completed.	Wait until the BMSs become available and check whether services recover.	None
	System maintenance failure	system_maintenance_failed	Major	The scheduled BMS maintenance task failed.	Contact O&M personnel.	Services are interrupted.
	GPU Xid error	commonXidError	Major	An Xid event alarm is generated on the GPU.	If services are affected, submit a service ticket.	An Xid error is caused by GPU hardware, driver, or application problems, which may result in abnormal service exit.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NPU: device not found by npu-smi info	NPUSMICardNotFound	Major	The Ascend driver is faulty or the NPU is disconnected.	Transfer this issue to the Ascend or hardware team for handling.	The NPU cannot be used normally.
	NPU: PCIe link error	PCIeErrorFound	Major	The **lspci** command returns **rev ff** indicating that the NPU is abnormal.	Restart the BMS. If the issue persists, transfer it to the hardware team for processing.	The NPU cannot be used normally.
	NPU: device not found by lspci	LspciCardNotFound	Major	The NPU is disconnected.	Transfer this issue to the hardware team for handling.	The NPU cannot be used normally.
	NPU: overtemperature	TemperatureOverUpperLimit	Major	The temperature of DDR or software is too high.	Stop services, restart the BMS, check the heat dissipation system, and reset the devices.	The BMS may be powered off and devices may not be found.
	NPU: uncorrectable ECC error	UncorrectableEccErrorCount	Major	There are uncorrectable ECC errors generated on GPU SRAM.	If services are affected, replace the NPU with another one.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NPU: request for BMS restart	RebootVirtualMachine	Informational	A fault occurs and the BMS needs to be restarted.	Collect the fault information, and restart the BMS.	Services may be interrupted.
	NPU: request for SoC reset	ResetSOC	Informational	A fault occurs and the SoC needs to be reset.	Collect the fault information, and reset the SoC.	Services may be interrupted.
	NPU: request for restart AI process	RestartAIProcess	Informational	A fault occurs and the AI process needs to be restarted.	Collect the fault information, and restart the AI process.	The current AI task will be interrupted.
	NPU: error codes	NPUErrorCodeWarning	Major	A large number of NPU error codes indicating major or higher-level errors are returned. You can further locate the faults based on the error codes.	Locate the faults according to the *Black Box Error Code Information List* and *Health Management Error Definition*.	Services may be interrupted.
	nvidia-smi suspended	nvidiaSmiHangEvent	Major	nvidia-smi timed out.	If services are affected, submit a service ticket.	The driver may report an error during service running.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	nv_peer_mem loading error	NvPeerMemException	Minor	The NVLink or nv_peer_mem cannot be loaded.	Restore or reinstall the NVLink.	nv_peer_mem cannot be used.
	Fabric Manager error	NvFabricManagerException	Minor	The BMS meets the NVLink conditions and NVLink is installed, but Fabric Manager is abnormal.	Restore or reinstall the NVLink.	NVLink cannot be used normally.
	IB card error	InfinibandStatusException	Major	The IB card or its physical status is abnormal.	Transfer this issue to the hardware team for handling.	The IB card cannot work normally.

Table 9-7 Elastic IP (EIP)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	EIP bandwidth exceeded	EIPBandwidthOverflow	Major	The used bandwidth exceeded the purchased one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. The metrics are described as follows: **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**:	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				peak inbound bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes) **NOTE** EIP bandwidth overflow is available only in the following regions: CN North-Beijing1, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN Southwest-Guiyang1, and CN South-Guangzhou.		
	EIP released	deleteEip	Minor	The EIP was released.	Check whether the EIP was release by mistake.	The server that has the EIP bound cannot access the Internet.
	EIP blocked	blockEIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Replace the EIP to prevent services from being affected. Locate and deal with the fault.	Services are impacted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	EIP unblocked	unblockEIP	Critical	The EIP was unblocked.	Use the previous EIP again.	None
	EIP traffic scrubbing started	ddosCleanEIP	Major	Traffic scrubbing on the EIP was started to prevent DDoS attacks.	Check whether the EIP was attacked.	Services may be interrupted.
	EIP traffic scrubbing ended	ddosEndCleanEip	Major	Traffic scrubbing on the EIP to prevent DDoS attacks was ended.	Check whether the EIP was attacked.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	QoS bandwidth exceeded	EIPBandwidthRuleOverflow	Major	The used QoS bandwidth exceeded the allocated one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (byte/s)	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				ingressDropBandwidth: dropped inbound packets (bytes)		

Table 9-8 Advanced Anti-DDoS (AAD)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	DDoS Attack Events	ddosAttackEvents	Major	A DDoS attack occurs in the AAD protected lines.	Judge the impact on services based on the attack traffic and attack type. If the attack traffic exceeds your purchased elastic bandwidth, change to another line or increase your bandwidth.	Services may be interrupted.
	Domain name scheduling event	domainNameDispatchEvents	Major	The high-defense CNAME corresponding to the domain name is scheduled, and the domain name is resolved to another high-defense IP address.	Pay attention to the workloads involving the domain name.	Services are not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Blackhole event	blackHoleEvents	Major	The attack traffic exceeds the purchased AAD protection threshold.	A blackhole is canceled after 30 minutes by default. The actual blackhole duration is related to the blackhole triggering times and peak attack traffic on the current day. The maximum duration is 24 hours. If you need to permit access before a blackhole becomes ineffective, contact technical support.	Services may be interrupted.
	Cancel Blackhole	cancelBlackHole	Informational	The customer's AAD instance recovers from the black hole state.	This is only a prompt and no action is required.	Customer services recover.

Table 9-9 Elastic Load Balance (ELB)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ELB	The backend servers are unhealthy.	healthCheckUnhealthy	Major	Generally, this problem occurs because backend server services are offline. This event will not be reported after it is reported for several times.	Ensure that the backend servers are running properly.	ELB does not forward requests to unhealthy backend servers. If all backend servers in the backend server group are detected unhealthy, services will be interrupted.
	The backend server is detected healthy.	healthCheckRecovery	Minor	The backend server is detected healthy.	No further action is required.	The load balancer can properly route requests to the backend server.

Table 9-10 Cloud Backup and Recovery (CBR)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CBR	Failed to create the backup.	backupFailed	Critical	The backup failed to be created.	Manually create a backup or contact customer service.	Data loss may occur.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to restore the resource using a backup.	restorationFailed	Critical	The resource failed to be restored using a backup.	Restore the resource using another backup or contact customer service.	Data loss may occur.
	Failed to delete the backup.	backupDeleteFailed	Critical	The backup failed to be deleted.	Try again later or contact customer service.	Charging may be abnormal.
	Failed to delete the vault.	vaultDeleteFailed	Critical	The vault failed to be deleted.	Try again later or contact technical support.	Charging may be abnormal.
	Replication failure	replicationFailed	Critical	The backup failed to be replicated.	Try again later or contact technical support.	Data loss may occur.
	The backup is created successfully.	backupSucceeded	Major	The backup was created.	None	None
	Resource restoration using a backup succeeded.	restorationSucceeded	Major	The resource was restored using a backup.	Check whether the data is successfully restored.	None
	The backup is deleted successfully.	backupDeletionSucceeded	Major	The backup was deleted.	None	None
	The vault is deleted successfully.	vaultDeletionSucceeded	Major	The vault was deleted.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication success	replicationSucceeded	Major	The backup was replicated successfully.	None	None
	Client offline	agentOffline	Critical	The backup client was offline.	Ensure that the Agent status is normal and the backup client can be connected to Huawei Cloud.	Backup tasks may fail.
	Client online	agentOnline	Major	The backup client was online.	None	None

Table 9-11 Relational Database Service (RDS) — resource exception

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
RDS	DB instance creation failure	createInstanceFailed	Major	Generally, the cause is that the number of disks is insufficient due to quota limits, or underlying resources are exhausted.	The selected resource specifications are insufficient. Select other available specifications and try again.	DB instances cannot be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Full backup failure	fullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Try again.	Restoration using backups will be affected.
	Read replica promotion failure	activeStandBySwitchFailed	Major	The standby DB instance does not take over workloads from the primary DB instance due to network or server failures. The original primary DB instance continues to provide services within a short time.	Perform the operation again during off-peak hours.	Read replica promotion failed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication status abnormal	abnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	The issue is being fixed. Please wait for our notifications.	The replication status is abnormal.
	Replication status recovered	replicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	Check whether services are running properly.	Replication status is recovered.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance faulty	faultyDBInstance	Major	A single or primary DB instance was faulty due to a catastrophic failure, for example, server failure.	The issue is being fixed. Please wait for our notifications.	The instance status is abnormal.
	DB instance recovered	DBInstanceRecovered	Major	RDS rebuilds the standby DB instance with its high availability. After the instance is rebuilt, this event will be reported.	The DB instance status is normal. Check whether services are running properly.	The instance is recovered.
	Failure of changing single DB instance to primary/standby	singleToHaFailed	Major	A fault occurs when RDS is creating the standby DB instance or configuring replication between the primary and standby DB instances. The fault may occur because resources are insufficient in the data center where the standby DB instance is located.	Automatic retry is in progress.	Changing a single DB instance to primary/standby failed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database process restarted	DatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Check whether services are running properly.	The primary instance is restarted. Services are interrupted for a short period of time.
	Instance storage full	instanceDiskFull	Major	Generally, the cause is that the data space usage is too high.	Scale up the storage.	The instance storage is used up. No data can be written into databases.
	Instance storage full recovered	instanceDiskFullRecovered	Major	The instance disk is recovered.	Check whether services are running properly.	The instance has available storage.
	Kafka connection failed	kafkaConnectionFailed	Major	The network is unstable or the Kafka server does not work properly.	Check whether services are affected.	None

Table 9-12 Relational Database Service (RDS) — operations

Event Source	Event Name	Event ID	Event Severity	Description
RDS	Reset administrator password	resetPassword	Major	The password of the database administrator is reset.
	Operate DB instance	instanceAction	Major	The storage space is scaled or the instance class is changed.
	Delete DB instance	deleteInstance	Minor	The DB instance is deleted.
	Modify backup policy	setBackupPolicy	Minor	The backup policy is modified.
	Modify parameter group	updateParameterGroup	Minor	The parameter group is modified.
	Delete parameter group	deleteParameterGroup	Minor	The parameter group is deleted.
	Reset parameter group	resetParameterGroup	Minor	The parameter group is reset.
	Change database port	changeInstancePort	Major	The database port is changed.
	Primary/standby switchover or failover	PrimaryStandbySwitched	Major	A switchover or failover is performed.

Table 9-13 Document Database Service (DDS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	DB instance creation failure	DDSCreateInstanceFailed	Major	A DDS instance fails to be created due to insufficient disks, quotas, and underlying resources.	Check the number and quota of disks. Release resources and create DDS instances again.	DDS instances cannot be created.
	Replication failed	DDSAbnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication recovered	DDSReplicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No action is required.	None
	DB instance failed	DDSFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DDSDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Faulty node	DDSFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Node recovered	DDSDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Primary/ standby switchover or failover	DDSPrimaryStandbySwitched	Major	A primary/ standby switchover is performed or a failover is triggered.	No action is required.	None
	Insufficient storage space	DDSRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	DDSDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No further action is required.	No adverse impact.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Schedule for deleting a KMS key	DDSplanDeleteKmsKey	Major	A request to schedule deletion of a KMS key was submitted.	After the KMS key is scheduled to be deleted, either decrypt the data encrypted by KMS key in a timely manner or cancel the key deletion.	After the KMS key is deleted, users cannot encrypt disks.

Table 9-14 GaussDB NoSQL

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB NoSQL	DB instance creation failed	NoSQLCreateInstanceFailed	Major	The instance quota or underlying resources are insufficient.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Specifications modification failed	NoSQLResizeInstanceFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you need to change the specifications again.	Services are interrupted.
	Node adding failed	NoSQLAddNodesFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
	Node deletion failed	NoSQLDeleteNodesFailed	Major	The underlying resources fail to be released.	Delete the node again.	None
	Storage space scale-up failed	NoSQLScaleUpStorageFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Password reset failed	NoSQLResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
	Parameter group change failed	NoSQLUpdateInstanceParamGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
	Backup policy configuration failed	NoSQLSetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
	Manual backup creation failed	NoSQLCreateManualBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Automated backup creation failed	NoSQLCreateAutomatedBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Faulty DB instance	NoSQLFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance recovered	NoSQLDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Faulty node	NoSQLFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
	Node recovered	NoSQLDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Primary/standby switchover or failover	NoSQLPrimaryStandbySwitched	Major	This event is reported when a primary/standby switchover is performed or a failover is triggered.	No action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HotKey occurred	HotKey Occurs	Major	The primary key is improperly configured. As a result, hotspot data is distributed in one partition. The improper application design causes frequent read and write operations on a key.	1. Choose a proper partition key. 2. Add service cache. The service application reads hotspot data from the cache first.	The service request success rate is affected, and the cluster performance and stability also be affected.
	BigKey occurred	BigKey Occurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	1. Choose a proper partition key. 2. Add a new partition key for hashing data.	As the data in the large partition increases, the cluster stability deteriorates.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Insufficient storage space	NoSQLRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	NoSQLDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No operation is required.	None
	Index creation failed	NoSQLCreateIndexFailed	Major	The service load exceeds what the instance specifications can take. In this case, creating indexes consumes more instance resources. As a result, the response is slow or even frame freezing occurs, and the creation times out.	Select the matched instance specifications based on the service load. Create indexes during off-peak hours. Create indexes in the background. Select indexes as required.	The index fails to be created or is incomplete. As a result, the index is invalid. Delete the index and create an index.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Write speed decreased	NoSQLStallingOccurs	Major	The write speed is fast, which is close to the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.
	Data write stopped	NoSQLStoppingOccurs	Major	The data write is too fast, reaching the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.
	Database restart failed	NoSQLRestartDBFailed	Major	The instance status is abnormal.	Submit a service ticket to the O&M personnel.	The DB instance status may be abnormal.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restoration to new DB instance failed	NoSQLRestoreToNewInstanceFailed	Major	The underlying resources are insufficient.	Submit a service order to ask the O&M personnel to coordinate resources in the background and add new nodes.	Data cannot be restored to a new DB instance.
	Restoration to existing DB instance failed	NoSQLRestoreToExistInstanceFailed	Major	The backup file fails to be downloaded or restored.	Submit a service ticket to the O&M personnel.	The current DB instance may be unavailable.
	Backup file deletion failed	NoSQLDeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
	Failed to enable Show Original Log	NoSQLSwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the *GaussDB NoSQL User Guide* to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	EIP binding failed	NoSQLBindEipFailed	Major	The node status is abnormal, an EIP has been bound to the node, or the EIP to be bound is invalid.	Check whether the node is normal and whether the EIP is valid.	The DB instance cannot be accessed from the Internet.
	EIP unbinding failed	NoSQLUnbindEipFailed	Major	The node status is abnormal or the EIP has been unbound from the node.	Check whether the node and EIP status are normal.	None
	Parameter modification failed	NoSQLModifyParameterFailed	Major	The parameter value is invalid.	Check whether the parameter value is within the valid range and submit a service ticket to the O&M personnel.	None
	Parameter group application failed	NoSQLApplyParameterGroupFailed	Major	The instance status is abnormal. As a result, the parameter group cannot be applied.	Submit a service ticket to the O&M personnel.	None
	Failed to enable or disable SSL	NoSQLSwitchSSLFailed	Major	Enabling or disabling SSL times out.	Try again or submit a service ticket. Do not change the connection mode.	The connection mode cannot be changed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Row size too large	LargeRowOccurs	Major	If there is too much data in a single row, queries may time out, causing faults like OOM error.	1. Control the length of each column and row so that the sum of key and value lengths in each row does not exceed the preset threshold. 2. Check whether there are invalid writes or encoding resulting in large keys or values.	If there are rows that are too large, the cluster performance will deteriorate as the data volume grows.
	Schedule for deleting a KMS key	NoSQLplanDeleteKmsKey	Major	A request to schedule deletion of a KMS key was submitted.	After the KMS key is scheduled to be deleted, either decrypt the data encrypted by KMS key in a timely manner or cancel the key deletion.	After the KMS key is deleted, users cannot encrypt disks.
	Too many query tombstones	TooManyQueryTombstones	Major	If there are too many query tombstones, queries may time out, affecting query performance.	Select right query and deleting methods and avoid long range queries.	Queries may time out, affecting query performance.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Too large collection column	TooLargeCollectionColumn	Major	If there are too many elements in a collection column, queries to the column will fail.	1. Limit elements in a collection column. 2. Check for abnormal writes or coding at the service side.	Queries to the collection column will fail.

Table 9-15 GaussDB(for MySQL)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for MySQL)	Incremental backup failure	TaurusIncrementalBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.
	Read replica creation failure	addReadonlyNodesFailed	Major	The quota is insufficient or underlying resources are exhausted.	Check the read replica quota. Release resources and create read replicas again.	Read replicas fail to be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance creation failure	createInstanceFailed	Major	The instance quota or underlying resources are insufficient.	Check the instance quota. Release resources and create instances again.	DB instances fail to be created.
	Read replica promotion failure	activeStandBySwitchFailed	Major	The read replica fails to be promoted to the primary node due to network or server failures. The original primary node takes over services quickly.	Submit a service ticket.	The read replica fails to be promoted to the primary node.
	Instance specifications change failure	flavorAlterationFailed	Major	The quota is insufficient or underlying resources are exhausted.	Submit a service ticket.	Instance specifications fail to be changed.
	Faulty DB instance	TaurusInstanceRunningStatusAbnormal	Major	The instance process is faulty or the communications between the instance and the DFV storage are abnormal.	Submit a service ticket.	Services may be affected.
	DB instance recovered	TaurusInstanceRunningStatusRecovered	Major	The instance is recovered.	Observe the service running status.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Faulty node	TaurusNodeRunningStatusAbnormal	Major	The node process is faulty or the communications between the node and the DFV storage are abnormal.	Observe the instance and service running statuses.	A read replica may be promoted to the primary node.
	Node recovered	TaurusNodeRunningStatusRecovered	Major	The node is recovered.	Observe the service running status.	None
	Read replica deletion failure	TaurusDeleteReadOnlyNodeFailed	Major	The communications between the management plane and the read replica are abnormal or the VM fails to be deleted from IaaS.	Submit a service ticket.	Read replicas fail to be deleted.
	Password reset failure	TaurusResetInstancePasswordFailed	Major	The communications between the management plane and the instance are abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Passwords fail to be reset for instances.
	DB instance reboot failure	TaurusRestartInstanceFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instances fail to be rebooted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restoration to new DB instance failure	TaurusRestoreToNewInstanceFailed	Major	The instance quota is insufficient, underlying resources are exhausted, or the data restoration logic is incorrect.	If the new instance fails to be created, check the instance quota, release resources, and try to restore to a new instance again. In other cases, submit a service ticket.	Backup data fails to be restored to new instances.
	EIP binding failure	TaurusBindEIPToInstanceFailed	Major	The binding task fails.	Submit a service ticket.	EIPs fail to be bound to instances.
	EIP unbinding failure	TaurusUnbindEIPFromInstanceFailed	Major	The unbinding task fails.	Submit a service ticket.	EIPs fail to be unbound from instances.
	Parameter modification failure	TaurusUpdateInstanceParameterFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instance parameters fail to be modified.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter template application failure	TaurusApplyParameterGroupToInstanceFailed	Major	The network between the management plane and instances is abnormal or the instances are abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Parameter templates fail to be applied to instances.
	Full backup failure	TaurusBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby failover	TaurusActiveStandbySwitched	Major	When the network, physical machine, or database of the primary node is faulty, the system promotes a read replica to primary based on the failover priority to ensure service continuity.	1. Check whether the service is running properly. 2. Check whether an alarm is generated, indicating that the read replica failed to be promoted to primary.	During the failover, database connection is interrupted for a short period of time. After the failover is complete, you can reconnect to the database.
	Database read-only	NodeReadonlyMode	Major	The database supports only query operations.	Submit a service ticket.	After the database becomes read-only, write operations cannot be processed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database read/ write	NodeReadWriteMode	Major	The database supports both write and read operations.	Submit a service ticket.	None.
	Instance DR switchover	DisasterSwitchOver	Major	If an instance is faulty and unavailable, a switchover is performed to ensure that the instance continues to provide services.	Contact technical support.	The database connection is intermittently interrupted. The HA service switches workloads from the primary node to a read replica and continues to provide services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database process restarted	TaurusDatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Log in to the Cloud Eye console. Check whether the memory usage increases sharply or the CPU usage is too high for a long time. You can increase the specifications or optimize the service logic.	When the database process is suspended, workloads on the node are interrupted. In this case, the HA service automatically restarts the database process and attempts to recover the workloads.

Table 9-16 GaussDB

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	Process status alarm	ProcessStatusAlarm	Major	Key processes exit, including CMS/CMA, ETCD, GTM, CN, and DN processes.	Wait until the process is automatically recovered or a primary/ standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes are faulty, services are interrupted and then rolled back. If processes on standby nodes are faulty, services are not affected.
	Component status alarm	ComponentStatusAlarm	Major	Key components do not respond, including CMA, ETCD, GTM, CN, and DN components.	Wait until the process is automatically recovered or a primary/ standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes do not respond, neither do the services. If processes on standby nodes are faulty, services are not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cluster status alarm	ClusterStatusAlarm	Major	The cluster status is abnormal. For example, the cluster is read-only; majority of ETCDs are faulty; or the cluster resources are unevenly distributed.	Contact SRE engineers.	If the cluster status is read-only, only read services are processed. If the majority of ETCDs are fault, the cluster is unavailable. If resources are unevenly distributed, the instance performance and reliability deteriorate.
	Hardware resource alarm	HardwareResourceAlarm	Major	A major hardware fault occurs in the instance, such as disk damage or GTM network fault.	Contact SRE engineers.	Some or all services are affected.
	Status transition alarm	StateTransitionAlarm	Major	The following events occur in the instance: DN build failure, forcible DN promotion, primary/standby DN switchover/failover, or primary/standby GTM switchover/failover.	Wait until the fault is automatically rectified and check whether services are recovered. If no, contact SRE engineers.	Some services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Other abnormal alarm	OtherAbnormalAlarm	Major	Disk usage threshold alarm	Focus on service changes and scale up storage space as needed.	If the used storage space exceeds the threshold, storage space cannot be scaled up.
	Faulty DB instance	TaurusInstanceRunningStatusAbnormal	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	TaurusInstanceRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
	Faulty DB node	TaurusNodeRunningStatusAbnormal	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB node recovered	TaurusNodeRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
	DB instance creation failure	GaussDBV5CreateInstanceFailed	Major	Instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.
	Node adding failure	GaussDBV5ExpandClusterFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storage scale-up failure	GaussDBV5EnlargeVolumeFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
	Reboot failure	GaussDBV5RestartInstanceFailed	Major	The network is abnormal.	Retry the reboot operation or submit a service ticket to the O&M personnel.	The database service may be unavailable.
	Full backup failure	GaussDBV5FullBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Differential backup failure	GaussDBV5DifferentialBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Backup deletion failure	GaussDBV5DeleteBackupFailed	Major	This function does not need to be implemented.	N/A	N/A

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	EIP binding failure	GaussDBV5BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the Internet.
	EIP unbinding failure	GaussDBV5UnbindEIPFailed	Major	The network is faulty or EIP is abnormal.	Unbind the IP address again or submit a service ticket to the O&M personnel.	IP addresses may be residual.
	Parameter template application failure	GaussDBV5ApplyParamFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
	Parameter modification failure	GaussDBV5UpdateInstanceParamGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
	Backup and restoration failure	GaussDBV5RestoreFromBcakupFailed	Major	The underlying resources are insufficient or backup files fail to be downloaded.	Submit a service ticket.	The database service may be unavailable during the restoration failure.

Table 9-17 Distributed Database Middleware (DDM)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDM	Failed to create a DDM instance	createDdmInstanceFailed	Major	The underlying resources are insufficient.	Release resources and create the instance again.	DDM instances cannot be created.
	Failed to change class of a DDM instance	resizeFlavorFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources and try again.	Services on some nodes are interrupted.
	Failed to scale out a DDM instance	enlargeNodeFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources, delete the node that fails to be added, and add a node again.	The instance fails to be scaled out.
	Failed to scale in a DDM instance	reduceNodeFailed	Major	The underlying resources fail to be released.	Submit a service ticket to the O&M personnel to release resources.	The instance fails to be scaled in.
	Failed to restart a DDM instance	restartInstanceFailed	Major	The DB instances associated are abnormal.	Check whether DB instances associated are normal. If the instances are normal, submit a service ticket to the O&M personnel.	Services on some nodes are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to create a schema	createLogicDbFailed	Major	The possible causes are as follows: ● The password for the DB instance account is incorrect. ● The security group of the DDM instance and the associated DB instance are incorrectly configured. As a result, the DDM instance cannot communicate with the associated DB instance.	Check the following items: ● Whether the username and password of the DB instance are correct. ● Whether the security groups associated with the DDM instance and underlying database instance are correctly configured.	Services cannot run properly.
	Failed to bind an EIP	bindEipFailed	Major	The EIP is abnormal.	Try again later. In case of emergency, contact O&M personnel to rectify the fault.	The DDM instance cannot be accessed from the Internet.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to scale out a schema	migrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.
	Failed to re-scale out a schema	retryMigrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.

Table 9-18 Cloud Phone Server

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	Server shutdown	cphServerOsShutdown	Major	The cloud phone server was stopped ● on the management console. ● by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server abnormal shutdown	cphServerShutdown	Major	The cloud phone server was stopped unexpectedly. Possible causes are as follows: ● The cloud phone server was powered off unexpectedly. ● The cloud phone server was stopped due to hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Server reboot	cphServerOsReboot	Major	The cloud phone server was rebooted - on the management console. - by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server abnormal reboot	cphServerReboot	Major	The cloud phone server was rebooted unexpectedly due to - OS faults. - hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Network disconnection	cphServerlinkDown	Major	The network where the cloud phone server was deployed was disconnected. Possible causes are as follows: - The cloud phone server was stopped unexpectedly and rebooted. - The switch was faulty. - The gateway node was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	PCIe error	cphServerPcieError	Major	The PCIe device or main board on the cloud phone server was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	The network or disk read/write is affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Disk error	cphServerDiskError	Major	The disk on the cloud phone server was faulty due to - disk backplane faults. - disk faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	Storage error	cphServerStorageError	Major	The cloud phone server could not connect to EVS disks. Possible causes are as follows: - SDI card faults - Remote storage devices were faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	GPU offline	cphServerGpuOffline	Major	GPU of the cloud phone server was loose and disconnected.	Stop the cloud phone server and reboot it.	Faults occur on cloud phones whose GPUs are disconnected. Cloud phones cannot run properly even if they are restarted or reconfigured.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU timeout	cphServerGpuTimeOut	Major	GPU of the cloud phone server timed out.	Reboot the cloud phone server.	Cloud phones whose GPUs timed out cannot run properly and are still faulty even if they are restarted or reconfigured.
	Disk space full	cphServerDiskFull	Major	Disk space of the cloud phone server was used up.	Clear the application data in the cloud phone to release space.	Cloud phone is sub-healthy, prone to failure, and unable to start.
	Disk readonly	cphServerDiskReadOnly	Major	The disk of the cloud phone server became read-only.	Reboot the cloud phone server.	Cloud phone is sub-healthy, prone to failure, and unable to start.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cloud phone metadata damaged	cphPhoneMetaDataDamage	Major	Cloud phone metadata was damaged.	Contact O&M personnel.	The cloud phone cannot run properly even if it is restarted or reconfigured.
	GPU failed	gpuAbnormal	Critical	The GPU was faulty.	Submit a service ticket.	Services are interrupted.
	GPU recovered	gpuNormal	Informational	The GPU was running properly.	No further action is required.	N/A
	Kernel crash	kernelCrash	Critical	The kernel log indicated crash.	Submit a service ticket.	Services are interrupted during the crash.
	Kernel OOM	kernelOom	Major	The kernel log indicated out of memory.	Submit a service ticket.	Services are interrupted.
	Hardware malfunction	hardwareError	Critical	The kernel log indicated **Hardware Error**.	Submit a service ticket.	Services are interrupted.
	PCIe error	pcieAer	Critical	The kernel log indicated **PCIe Bus Error**.	Submit a service ticket.	Services are interrupted.
	SCSI error	scsiError	Critical	The kernel log indicated SCSI Error.	Submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Image storage became read-only	partReadOnly	Critical	The image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Image storage superblock damaged	badSuperBlock	Critical	The superblock of the file system of the image storage was damaged.	Submit a service ticket.	Services are interrupted.
	Image storage /.sharedpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.sharedpath/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk became read-only	cphDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk superblock damaged	cphDiskBadSuperBlock	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

Table 9-19 Layer 2 Connection Gateway (L2CG)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 9-20 Elastic IP and bandwidth

Event Source	Event Name	Event ID	Event Severity
Elastic IP and bandwidth	VPC deleted	deleteVpc	Major
	VPC modified	modifyVpc	Minor
	Subnet deleted	deleteSubnet	Minor
	Subnet modified	modifySubnet	Minor
	Bandwidth modified	modifyBandwidth	Minor
	VPN deleted	deleteVpn	Major
	VPN modified	modifyVpn	Minor

Table 9-21 Elastic Volume Service (EVS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EVS	Update disk	updateVolume	Minor	Update the name and description of an EVS disk.	No further action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Expand disk	extendVolume	Minor	Expand an EVS disk.	No further action is required.	None
	Delete disk	deleteVolume	Major	Delete an EVS disk.	No further action is required.	Deleted disks cannot be recovered.
	QoS upper limit reached	reachQoS	Major	The I/O latency increases as the QoS upper limits of the disk are frequently reached and flow control triggered.	Change the disk type to one with a higher specification.	The current disk may fail to meet service requirements.

Table 9-22 Identity and Access Management (IAM)

Event Source	Event Name	Event ID	Event Severity
IAM	Login	login	Minor
	Logout	logout	Minor
	Password changed	changePassword	Major
	User created	createUser	Minor
	User deleted	deleteUser	Major
	User updated	updateUser	Minor
	User group created	createUserGroup	Minor
	User group deleted	deleteUserGroup	Major
	User group updated	updateUserGroup	Minor

Event Source	Event Name	Event ID	Event Severity
	Identity provider created	createIdentityProvider	Minor
	Identity provider deleted	deleteIdentityProvider	Major
	Identity provider updated	updateIdentityProvider	Minor
	Metadata updated	updateMetadata	Minor
	Security policy updated	updateSecurityPolicies	Major
	Credential added	addCredential	Major
	Credential deleted	deleteCredential	Major
	Project created	createProject	Minor
	Project updated	updateProject	Minor
	Project suspended	suspendProject	Major

Table 9-23 Key Management Service (KMS)

Event Source	Event Name	Event ID	Event Severity
KMS	Key disabled	disableKey	Major
	Key deletion scheduled	scheduleKeyDeletion	Minor
	Grant retired	retireGrant	Major
	Grant revoked	revokeGrant	Major

Table 9-24 Object Storage Service (OBS)

Event Source	Event Name	Event ID	Event Severity
OBS	Bucket deleted	deleteBucket	Major
	Bucket policy deleted	deleteBucketPolicy	Major
	Bucket ACL configured	setBucketAcl	Minor

Event Source	Event Name	Event ID	Event Severity
	Bucket policy configured	setBucketPolicy	Minor

Table 9-25 Cloud Eye

Event Source	Event Name	Event ID	Event Severity	Description	Solution
Cloud Eye	Agent heartbeat interruption	agentHeartbeatInterrupted	Major	The Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye cannot receive a heartbeat for 3 minutes, **Agent Status** is displayed as **Faulty**.	● Confirm that the Agent domain name cannot be resolved. ● Check whether your account is in arrears. ● The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. ● Confirm that the server time is inconsistent with the local standard time. ● If the DNS server is not a Huawei Cloud DNS server, run the **dig** *domain name* command to obtain the IP address of **agent.ces.myhuaweicloud.com** which is resolved by the Huawei Cloud DNS server over the intranet and then add the IP address into the corresponding **hosts** file.

Event Source	Event Name	Event ID	Event Severity	Description	Solution
					- Update the Agent to the latest version.
	Agent back to normal	agentResumed	Informational	The Agent was back to normal.	No further action is required.
	Agent faulty	agentFaulted	Major	The Agent was faulty and this status was reported to Cloud Eye.	The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. Update the Agent to the latest version.

Event Source	Event Name	Event ID	Event Severity	Description	Solution
	Agent disconnected	agentDisconnected	Major	The Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye cannot receive a heartbeat for 3 minutes, **Agent Status** is displayed as **Faulty**.	Confirm that the Agent domain name cannot be resolved. Check whether your account is in arrears. The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. Confirm that the server time is inconsistent with the local standard time. If the DNS server is not a Huawei Cloud DNS server, run the **dig** *domain name* command to obtain the IP address of **agent.ces.myhuaweicloud.com** which is resolved by the Huawei Cloud DNS server over the intranet, and then add the IP address into the corresponding **hosts** file. Update the Agent to the latest version.

Table 9-26 DataSpace

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DataSpace	New revision	newRevision	Minor	An updated version was released.	After receiving the notification, export the data of the updated version as required.	None.

Table 9-27 Enterprise Switch

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
Enterprise Switch	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 9-28 Cloud Secret Management Service (CSMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CSMS	Operation on secret scheduled for deletion	operateDeletedSecret	Major	A user attempts to perform operations on a secret that is scheduled to be deleted.	Check whether the scheduled secret deletion needs to be canceled.	The user cannot perform operations on the secret scheduled to be deleted.

Table 9-29 Distributed Cache Service (DCS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DCS	Full sync retry during online migration	migrationFullResync	Minor	If online migration fails, full synchronization will be triggered because incremental synchronization cannot be performed.	Check whether full sync retries are triggered repeatedly. Check whether the source instance is connected and whether it is overloaded. If full sync retries are triggered repeatedly, contact O&M personnel.	The migration task is disconnected from the source instance, triggering another full sync. As a result, the CPU usage of the source instance may increase sharply.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Automatic failover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance are interrupted.
	Memcached master/standby switchover	memcachedMasterStandbyFailover	Minor	The master node was abnormal, promoting the standby node to master.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance are interrupted.
	Redis server abnormal	redisNodeStatusAbnormal	Major	The Redis server status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	If the master node is abnormal, an automatic failover is performed. If a standby node is abnormal and the client directly connects to the standby node for read/write splitting, no data can be read.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Redis server recovered	redisNodeStatusNormal	Major	The Redis server status recovered.	Check whether services can recover. If the applications are not reconnected, restart them.	Recover from an exception.
	Sync failure in data migration	migrateSyncDataFail	Major	Online migration failed.	Reconfigure the migration task and migrate data again. If the fault persists, contact O&M personnel.	Data migration fails.
	Memcached instance abnormal	memcachedInstanceStatusAbnormal	Major	The Memcached node status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	The Memcached instance is abnormal and may not be accessed.
	Memcached instance recovered	memcachedInstanceStatusNormal	Major	The Memcached node status recovered.	Check whether services can recover. If the applications are not reconnected, restart them.	Recover from an exception.
	Instance backup failure	instanceBackupFailure	Major	The DCS instance fails to be backed up due to an OBS access failure.	Retry backup manually.	Automatic backup fails.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services can recover. If the applications are not reconnected, restart them.	Persistent connections to the instance are interrupted.
	Long-running Lua scripts stopped	scriptsStopped	Informational	Lua scripts that had timed out automatically stopped running.	Optimize Lua scrips to prevent execution timeout.	If Lua scripts take a long time to execute, they will be forcibly stopped to avoid blocking the entire instance.
	Node restarted	nodeRestarted	Informational	After write operations had been performed, the node automatically restarted to stop Lua scripts that had timed out.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance are interrupted.

Table 9-30 Intelligent Cloud Access (ICA)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ICA	BGP peer disconnection	BgpPeerDisconnection	Major	The BGP peer is disconnected.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
	Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	The GRE tunnel status is abnormal.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
	WAN interface goes up	EquipmentWanGoingOnline	Major	The WAN interface goes online.	None	None
	WAN interface goes down	EquipmentWanGoingOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
	Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoingOnline	Major	The intelligent enterprise gateway goes online.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoingOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table 9-31 Multi-Site High Availability Service (MAS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
MAS	Abnormal database instance	dbError	Major	Abnormal database instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Database instance recovered	dbRecovery	Major	The database instance is recovered.	None	Services are interrupted.
	Abnormal Redis instance	redisError	Major	Abnormal Redis instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Redis instance recovered	redisRecovery	Major	The Redis instance is recovered.	None	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal MongoDB database	mongodbError	Major	Abnormal MongoDB database is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	MongoDB database recovered	mongodbRecovery	Major	The MongoDB database is recovered.	None	Services are interrupted.
	Abnormal Elasticsearch instance	esError	Major	Abnormal Elasticsearch instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Elasticsearch instance recovered	esRecovery	Major	The Elasticsearch instance is recovered.	None	Services are interrupted.
	Abnormal API	apiError	Major	The abnormal API is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	API recovered	apiRecovery	Major	The API is recovered.	None	Services are interrupted.
	Area status changed	netChange	Major	Area status changes are detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Network of the multi-active areas may change.

Table 9-32 Config

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
Config	Configuration noncompliance notification	configurationNoncomplianceNotification	Major	The assignment evaluation result is **Non-compliant**.	Modify the noncompliant configuration items of the resource.	None
	Configuration compliance notification	configurationComplianceNotification	Informational	The assignment evaluation result changed to be **Compliant**.	None	None

Table 9-33 SecMaster

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
SecMaster	Exclusive engine creation failed	createEngineFailed	Major	The underlying resources are insufficient.	Submit a ticket to request sufficient resources from the O&M personnel and try again.	The exclusive engine cannot be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Exclusive engine exception	engineException	Critical	The traffic is too heavy or there are malicious processes or plug-ins.	1. Check the executions of plug-ins and processes, see if they occupy too many resources. 2. Check the instance monitoring information to see whether there is a sharp increase in the number of instances.	The instance cannot be executed.
	Playbook instance execution failed	playbookInstanceExecFailed	Minor	Playbooks or processes are incorrectly configured.	Check the instance monitoring information to find the cause of the failure, and modify the playbook and process configuration.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Playbook instance increased sharply	playbookInstanceIncreaseSharply	Minor	Playbooks or processes are incorrectly configured.	Check the instance monitoring information to find the cause of the increase, and modify the playbook and process configuration.	None
	Log messages increased sharply	logIncrease	Major	The upstream services suddenly generate a large number of log messages.	Check whether the upstream services are normal.	None
	Log messages decreased sharply	logsDecrease	Major	Logs generated by the upstream services suddenly decrease.	Check whether the upstream services are normal.	None

Table 9-34 Key Pair Service

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
KPS	Key pair deleted	KPSDeleteKeypair	Informational	A key pair was deleted. This operation cannot be undone.	If this event occurred frequently within a short period of time, check whether malicious deletion took place.	Deleted key pairs cannot be restored.

Table 9-35 Host Security Service

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
HSS	HSS agent disconnected	hssAgentAbnormalOffline	Major	The communication between the agent and the server is abnormal, or the agent process on the server is abnormal.	Fix your network connection. If the agent is still offline for a long time after the network recovers, the agent process may be abnormal. In this case, log in to the server and restart the agent process.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal HSS agent status	hssAgentAbnormalProtection	Major	The agent is abnormal probably because it does not have sufficient resources.	Log in to the server and check your resources. If the usage of memory or other system resources is too high, increase their capacity first. If the resources are sufficient but the fault persists after the agent process is restarted, submit a service ticket to the O&M personnel.	Services are interrupted.

Table 9-36 Image Management Service

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
IMS	Create Image	createImage	Major	An image was created.	None	You can use this image to create cloud servers.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Update Image	updateImage	Major	Metadata of an image was modified.	None	Cloud servers may fail to be created from this image.
	Delete Image	deleteImage	Major	An image was deleted.	None	This image will be unavailable on the management console.

Table 9-37 Cloud Storage Gateway (CSG)

Event Source	Event Name	Event ID	Event Severity	Description
CSG	Abnormal CSG process status	gatewayProcessStatusAbnormal	Major	This event is triggered when an exception occurs in the CSG process status.
	Abnormal CSG connection status	gatewayToServiceConnectAbnormal	Major	This event is triggered when no CSG status report is returned for five consecutive periods.
	Abnormal connection status between CSG and OBS	gatewayToObsConnectAbnormal	Major	This event is triggered when CSG cannot connect to OBS.
	Read-only file system	gatewayFileSystemReadOnly	Major	This event is triggered when the partition file system on CSG becomes read-only.

Event Source	Event Name	Event ID	Event Severity	Description
	Read-only file share	gatewayFileShareReadOnly	Major	This event is triggered when the file share becomes read-only due to insufficient cache disk storage space.

Table 9-38 Global Accelerator (GA)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GA	Anycast IP address blocked	blockAIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Locate the root cause and rectify the fault.	Services are affected. The traffic will not be properly forwarded.
	Anycast IP address unblocked	unblockAIP	Critical	The anycast IP address was unblocked.	Ensure that traffic can be properly forwarded.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Unhealthy endpoint	healthCheckError	Major	Health check detects the endpoint unhealthy.	Perform operations as described in **What Should I Do If an Endpoint Is Unhealthy?** If the endpoint is still unhealthy, submit a service ticket.	If an endpoint is considered unhealthy, traffic will not be forwarded to it until the endpoint recovers.

Table 9-39 Enterprise connection

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EC	WAN interface goes up	EquipmentWanGoesOnline	Major	The WAN interface goes online.	None	None
	WAN interface goes down	EquipmentWanGoesOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
	BGP peer disconnection	BgpPeerDisconnection	Major	BGP peer disconnection	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
	Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	Abnormal GRE tunnel status	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
	Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
	Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoesOnline	Major	The intelligent enterprise gateway goes online.	None	None
	Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoesOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table 9-40 Cloud Certificate Manager (CCM)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CCM	Certificate revocation	CCMRevokeCertificate	Major	The certificate enters into the revocation process. Once revoked, the certificate cannot be used anymore.	Check whether the certificate revocation is really needed. Certificate revocation can be canceled.	If a certificate is revoked, the website is inaccessible using HTTPS.
	Certificate auto-deployment failure	CCMAutoDeploymentFailure	Major	The certificate fails to be automatically deployed.	Check service resources whose certificates need to be replaced.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.
	Certificate expiration	CCMCertificateExpiration	Major	An SSL certificate has expired.	Purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Certificate about to expire	CCMcertificateAboutToExpiration	Major	This alarm is generated when an SSL certificate is about to expire in one week, one month, and two months.	Renew or purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.

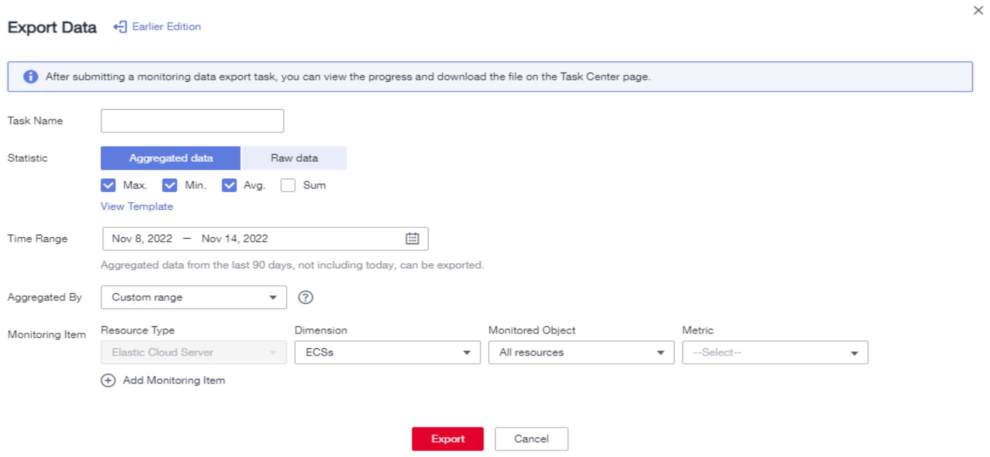
10 Task Center

On the **Task Center** page, you can export data including monitoring data and alarm records. You can go to the **Alarm Records** and **Server Monitoring** pages to create an export task. After the export task is submitted, you can view the progress and download the file on the **Task Center** page.

Exporting Monitoring Data

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring** > **Elastic Cloud Server**.
4. Click **Export Data** in the upper right corner.

Figure 10-1 Exporting data



Export Data

After submitting a monitoring data export task, you can view the progress and download the file on the Task Center page.

Task Name:

Statistic: Aggregated data (selected) | Raw data

☑ Max. ☑ Min. ☑ Avg. □ Sum

Time Range: Nov 8, 2022 — Nov 14, 2022

Aggregated data from the last 90 days, not including today, can be exported.

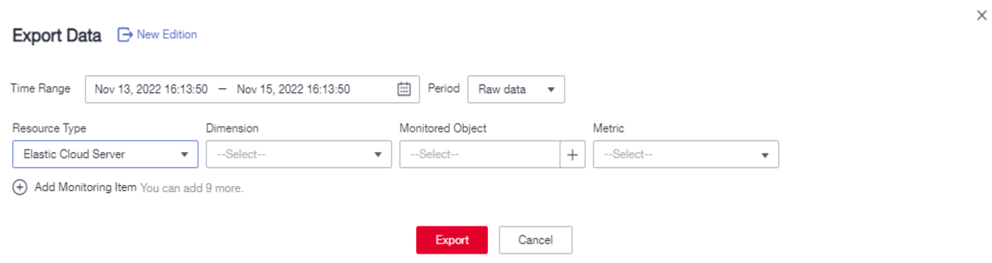
Aggregated By: Custom range

Monitoring Item	Resource Type	Dimension	Monitored Object	Metric
	Elastic Cloud Server	ECSs	All resources	--Select--

NOTE

By default, the new edition page is displayed. To return to the old version, click **Earlier Edition**. In the earlier edition, the data export task is not displayed on the **Task Center** page and can be downloaded on the current page.

Figure 10-2 Earlier edition of the **Export Data** page



Export Data

Time Range: Nov 13, 2022 16:13:50 — Nov 15, 2022 16:13:50

Period: Raw data

Resource Type: Elastic Cloud Server

Dimension: --Select--

Monitored Object: --Select--

Metric: --Select--

Add Monitoring Item You can add 9 more.

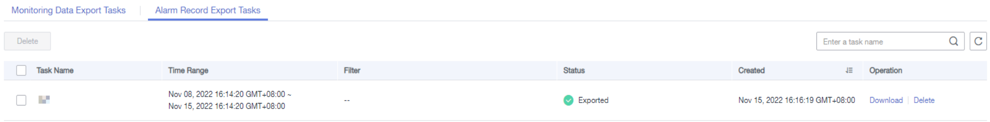
5. On the **Export Data** page, set parameters as prompted.

Table 10-1 Configuring parameters for exporting data

Parameter	Description
Task Name	Name of an export task. It contains 1 to 32 characters.
Statistic	There are two modes: **Aggregated data** and **Raw data**. ● **Aggregated data**: Data can be exported after being aggregated using the maximum value, minimum value, average value, or sum value. ● **Raw data**: The original data is exported.
Time Range	Select the time range for the data to be exported. ● Data of a maximum of the last 90 days can be exported for an aggregate value. ● Raw data from the last 48 hours is available for export.
Aggregated By	This parameter is mandatory when **Statistics** is set to **Aggregate data**. If you select **Custom range**, data aggregated during your configured time range will be exported. If you select one of the other options, data will be aggregated based on your selected granularity and then exported.
Monitoring Item	● **Resource Type**: The default value is **Elastic Cloud Server**. You do not need to set this parameter. ● **Dimension**: Specify the dimension name of the metric to be exported. ● **Monitored Object**: You can select **All Resources** or **Specific resources**. ● **Metric**: Specify the metric to be exported.

6. After the configuration is complete, click **Export**.
7. After the export task is submitted, you can view and download the monitoring data under the **Monitoring Data Export Tasks** tab on the **Task Center** page.

Figure 10-3 Viewing export tasks



Task Name	Time Range	Filter	Status	Created	Operation
	Nov 08, 2022 16:14:20 GMT+08:00 ~ Nov 15, 2022 16:14:20 GMT+08:00	--	Exported	Nov 15, 2022 16:16:19 GMT+08:00	Download | Delete

8. On the **Monitoring Data Export Tasks** tab, select a target record and click **Download** in the **Operation** column, or select multiple target records and click **Download** above the list to download the exported monitoring data.
9. On the **Monitoring Data Export Tasks** tab, select a target record and click **Delete** in the **Operation** column, or select multiple target records and click **Delete** above the list to delete the exported monitoring data.

Exporting Alarm Records

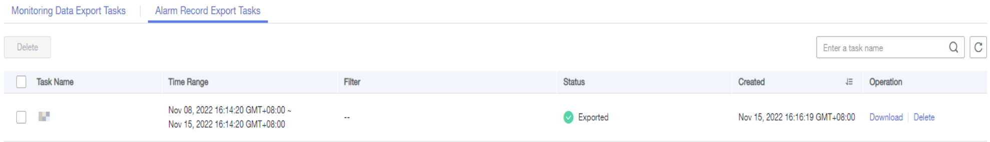
1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Records**.
4. On the **Alarm Records** page, click **Export**.

   NOTE

   You can export all alarm records or alarm records filtered by status, alarm severity, alarm rule name, resource type, resource ID, and alarm rule ID above the alarm record list.
5. In the displayed **Export Alarm Records** dialog box, enter an export task name and click **OK**.

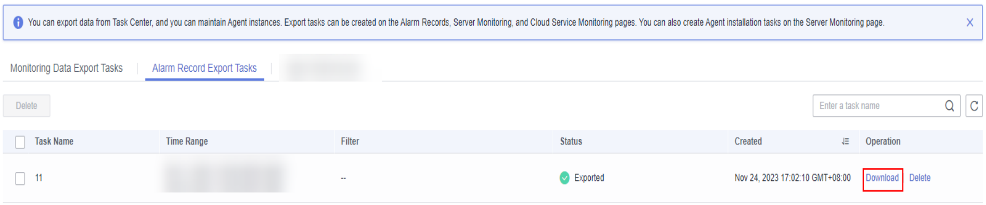
   The task name contains 1 to 32 characters.
6. After the export task is submitted, you can view and download the alarm records under the **Alarm Record Export Task** tab on the **Task Center** page.

Figure 10-4 Viewing export tasks



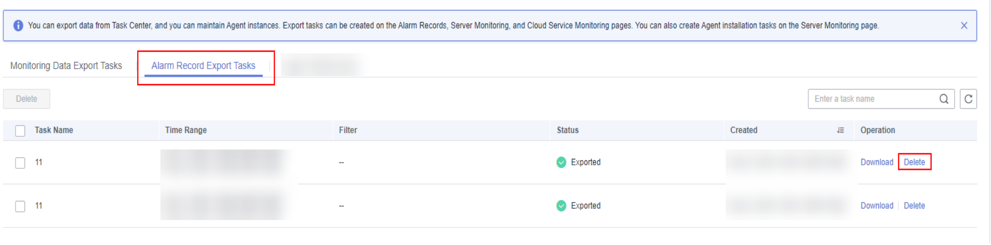
Task Name	Time Range	Filter	Status	Created	Operation
	Nov 08, 2022 16:14:20 GMT+08:00 ~ Nov 15, 2022 16:14:20 GMT+08:00	--	Exported	Nov 15, 2022 16:16:19 GMT+08:00	Download | Delete

7. On the **Alarm Record Export Tasks** tab, select a target record and click **Download** in the **Operation** column, or select multiple target records and click **Download** above the list to download the exported alarm data.


You can export data from Task Center, and you can maintain Agent instances. Export tasks can be created on the Alarm Records, Server Monitoring, and Cloud Service Monitoring pages. You can also create Agent installation tasks on the Server Monitoring page.

Task Name	Time Range	Filter	Status	Created	Operation
11	[redacted]	--	Exported	Nov 24, 2023 17:02:10 GMT+08:00	Download Delete

8. On the **Alarm Record Export Tasks** tab, select a target record and click **Delete** in the **Operation** column, or select multiple target records and click **Delete** above the list to delete the exported alarm data.



You can export data from Task Center, and you can maintain Agent instances. Export tasks can be created on the Alarm Records, Server Monitoring, and Cloud Service Monitoring pages. You can also create Agent installation tasks on the Server Monitoring page.

Monitoring Data Export Tasks | Alarm Record Export Tasks | [redacted]

Delete

Enter a task name

□ Task Name	Time Range	Filter	Status	Created	Operation
□ 11	[redacted]	--	Exported	[redacted]	Download Delete
□ 11	[redacted]	--	Exported	[redacted]	Download | Delete

11 Data Dump

11.1 Adding a Dump Task

Scenarios

You can dump cloud service monitoring data to DMS for Kafka in real time and query the metrics on the DMS for Kafka console or using an open-source Kafka client.

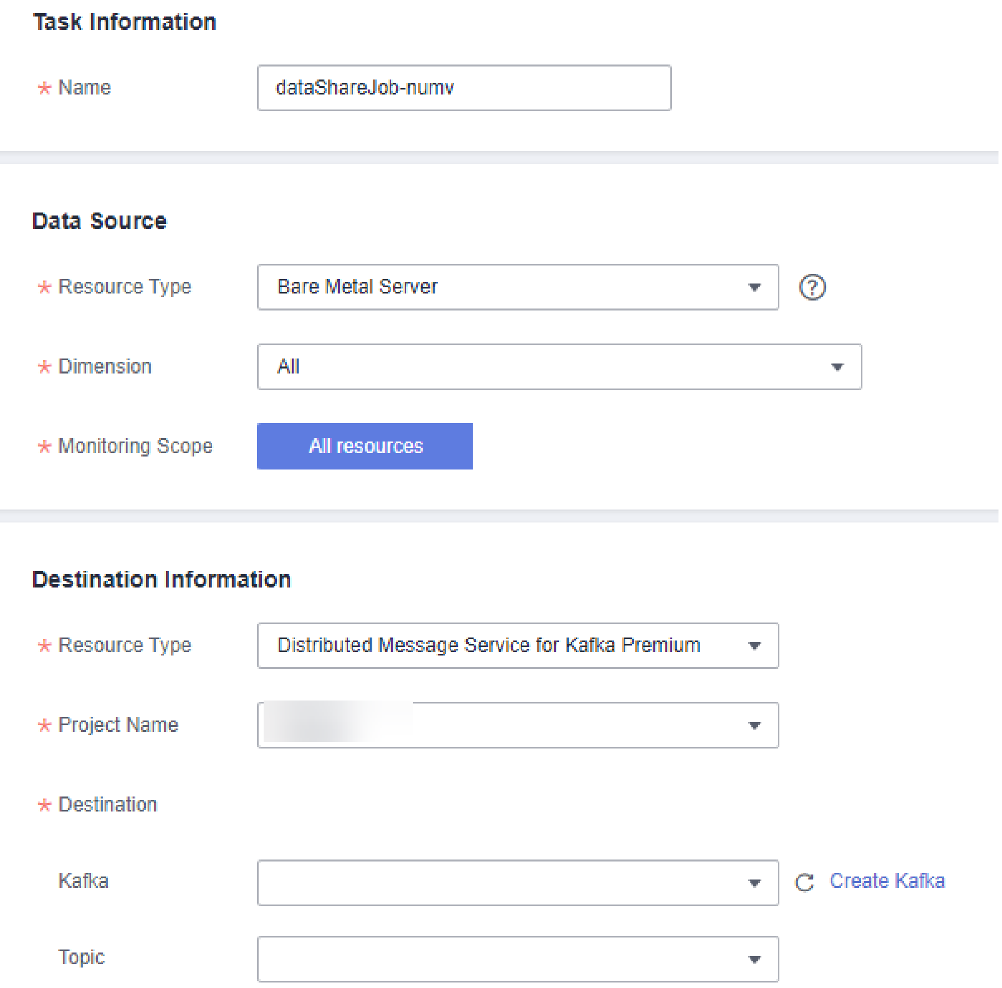
NOTE

- An account can create up to 20 data dump tasks.
- The data dump function is only available for whitelisted customers.

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 **Data Dump**.
4. Click **Add Dump Task**.
5. In the **Add Dump Task** dialog box, configure parameters as prompted.

Figure 11-1 Creating a dump task



Task Information

* Name: dataShareJob-numv

Data Source

* Resource Type: Bare Metal Server
* Dimension: All
* Monitoring Scope: All resources

Destination Information

* Resource Type: Distributed Message Service for Kafka Premium
* Project Name:
* Destination

Kafka:

Topic:

Table 11-1 Dump task parameters

Parameter	Description
Name	Specifies the dump task name. The name can contain 1 to 128 characters and consist of only letters, digits, underscores (_), and hyphens (-). Example value: **dataShareJob-ECSMetric**
Resource Type	Specifies the type of resources monitored by Cloud Eye. Example value: **Elastic Cloud Server**

Parameter	Description
Dimension	Specifies the dimension of the monitored object. For details, see **Metrics** and **Dimension** on the monitoring metric description page. If **All** is selected, all monitored objects of the selected service will be dumped to Kafka. If **ECSs** is selected, metrics of this dimension will be dumped to Kafka. Example value: **All**
Monitoring Scope	The scope can only be **All resources**, indicating that all metrics of the specified monitored object will be dumped to DMS for Kafka.
Resource Type	The type can only be **Distributed Message Service for Kafka**.
Destination	Specifies the Kafka instance and topic where the data is to be dumped. If no Kafka instance or topic is available, see **Buying an Instance** and **Creating a Topic**.

6. Click **Add** after the configuration is complete.

   NOTE

   You can query the dumped data in Kafka. For details, see **Querying Messages**.

11.2 Modifying, Deleting, Enabling, or Disabling a Dump Task

Scenarios

This topic describes how to modify, disable, enable, or delete dump tasks.

Modifying a Dump Task

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, choose **Data Dump**.
4. Click **Modify** in the **Operation** column.

   The **Modify Dump Task** page is displayed.
5. Modify the task settings.
6. Click **Modify**.

Disabling a Dump Task

Locate the dump task and click **Disable** in the **Operation** column. In the pop-up window, click **OK** to disable the dump task.

Enabling a Dump Task

Locate a dump task whose status is **Disabled** and click **Enable** in the **Operation** column. In the pop-up window, click **OK** to enable the dump task.

Deleting a Dump Task

Locate the dump task and click **Delete** in the **Operation** column. In the pop-up window, click **OK** to delete the dump task.

12 Auditing Operation Records on Cloud Eye

Cloud Trace Service (CTS) records Cloud Eye operation requests initiated from the public cloud management console or open APIs and responses to the requests. You can query, audit, and trace back the operation records.

12.1 Key Cloud Eye Operations

Table 12-1 Cloud Eye operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an alarm rule	alarm_rule	createAlarmRule
Deleting an alarm rule	alarm_rule	deleteAlarmRule
Disabling an alarm rule	alarm_rule	disableAlarmRule
Enabling an alarm rule	alarm_rule	enableAlarmRule
Modifying an alarm rule	alarm_rule	updateAlarmRule
Updating the alarm status to Alarm	alarm_rule	alarmStatusChangeToAlarm
Updating the alarm status to Insufficient data	alarm_rule	alarmStatusChangeToInsufficientData
Updating the alarm status to OK	alarm_rule	alarmStatusChangeToOk
Creating a custom template	alarm_template	createAlarmTemplate

Operation	Resource Type	Trace Name
Deleting a custom template	alarm_template	deleteAlarmTemplate
Modifying a custom template	alarm_template	updateAlarmTemplate
Creating a dashboard	dashboard	createDashboard
Deleting a dashboard	dashboard	deleteDashboard
Modifying a dashboard	dashboard	updateDashboard
Exporting monitoring data	metric	downloadMetricsReport
Configuring OBS dump	obs_transfer	createObsTransfer
Modifying OBS dump	obs_transfer	updateObsTransfer
Configuring OBS dump in batches	obs_transfer	batchCreateObsTransfer
Creating a monitor	remote_check	createRemoteMonitoring-Rules
Deleting a monitor	remote_check	deleteRemoteMonitoring-Rules
Modifying a monitor	remote_check	updateRemoteMonitoring-Rule
Enabling or disabling one-click monitoring	one_click_alarm	updateOneClickAlarm

12.2 Viewing Cloud Eye Logs

Scenarios

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the operation records of the last 7 days.

This section describes how to query or export the last seven days of operation records on the CTS console.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Click **Filter** and specify filters as needed. You can query traces by combining the following filters:

- **Trace Source**, **Resource Type**, and **Search By**

  Select a filter from the drop-down list.

  After you select **Trace name** for **Search By**, you also need to select a trace name.

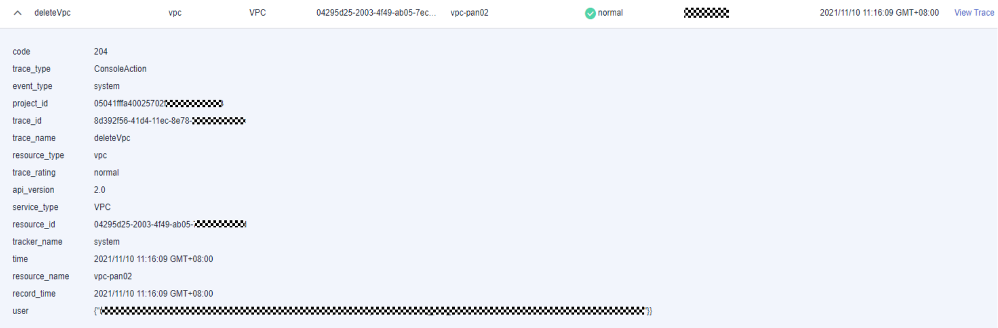
  After you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.

  After you select **Resource name** for **Search By**, you also need to select or enter a resource name.

- **Operator**: Select a specific operator.
- **Trace Status**: Select only one from the four available options: **All trace statuses**, **normal**, **warning**, and **incident**.
- Time range: You can select start and end time to query traces generated during the selected time range.

6. Click on the left of a trace to expand its details.

Figure 12-1 Expanding trace details

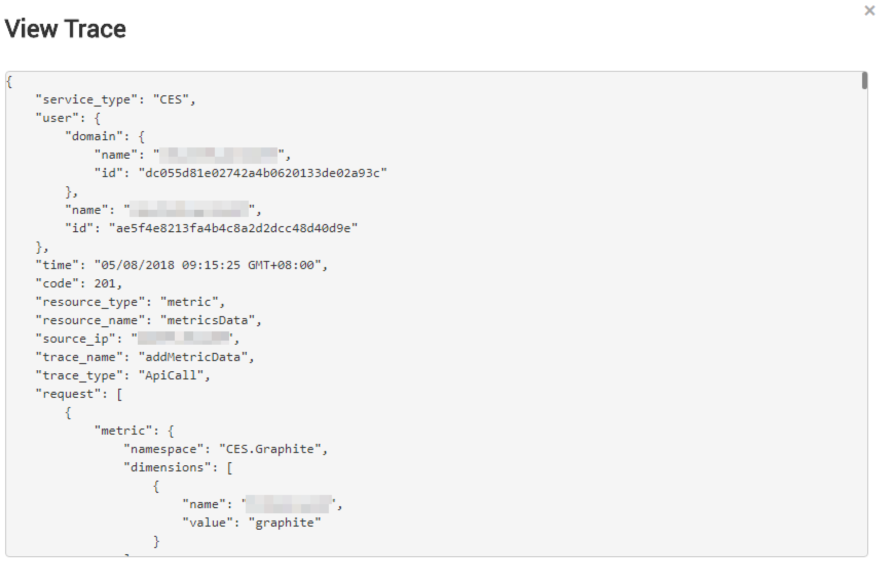


deleteVpc vpc VPC 04295d25-2003-4f49-ab05-7ec... vpc-pan02 normal [redacted] 2021/11/10 11:16:09 GMT+08:00 View Trace

code	204
trace_type	ConsoleAction
event_type	system
project_id	05041fffa40025702[redacted]
trace_id	8d392f56-41d4-11ec-8e78-[redacted]
trace_name	deleteVpc
resource_type	vpc
trace_rating	normal
api_version	2.0
service_type	VPC
resource_id	04295d25-2003-4f49-ab05-[redacted]
tracker_name	system
time	2021/11/10 11:16:09 GMT+08:00
resource_name	vpc-pan02
record_time	2021/11/10 11:16:09 GMT+08:00
user	{"[redacted]"}}

7. Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box, view details of the trace.

Figure 12-2 View Trace



View Trace

```
{
    "service_type": "CES",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "dc055d81e02742a4b0620133de02a93c"
        },
        "name": "[redacted]",
        "id": "ae5f4e8213fa4b4c8a2d2dcc48d40d9e"
    },
    "time": "05/08/2018 09:15:25 GMT+08:00",
    "code": 201,
    "resource_type": "metric",
    "resource_name": "metricsData",
    "source_ip": "[redacted]",
    "trace_name": "addMetricData",
    "trace_type": "ApiCall",
    "request": [
        {
            "metric": {
                "namespace": "CES.Graphite",
                "dimensions": [
                    {
                        "name": "[redacted]",
                        "value": "graphite"
                    }
```

13 Permissions Management

13.1 Creating a User and Granting Permissions

IAM enables you to perform a refined management on your Cloud Eye service. It allows you to:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing Cloud Eye resources.
- Grant different permissions to IAM users based on their job responsibilities.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your Cloud Eye resources.

If your Huawei Cloud account does not require individual IAM users, skip this topic.

This topic describes the procedure for granting permissions (see **Figure 13-1**).

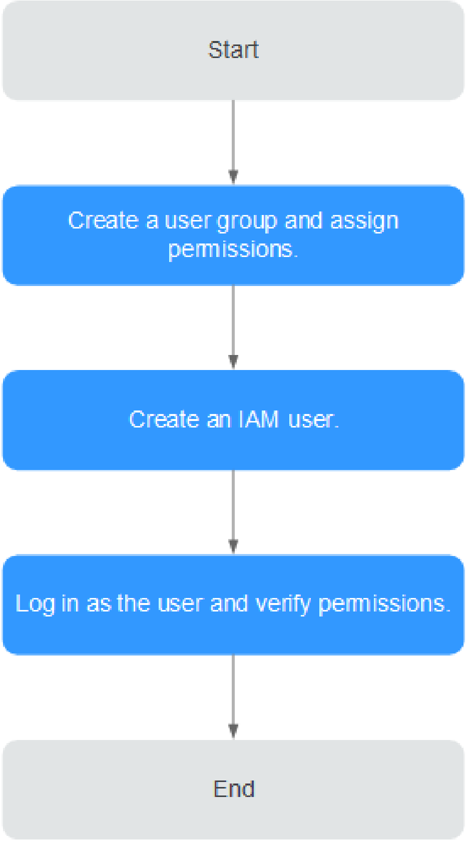
Prerequisites

Before assigning permissions to a user group, you need to understand the Cloud Eye system policies that can be added to the user group and select a policy as required.

For details about the system policies supported by CES and comparison between these policies, see **Permissions Management**. For the permissions of other services, see **System Permissions**.

Process Flow

Figure 13-1 Process for granting Cloud Eye permissions


Start
Create a user group and assign permissions.
Create an IAM user.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and attach the **CES Administrator**, **Tenant Guest**, and **Server Administrator** policies to the group.

   NOTE

   - Cloud Eye is a region-specific service and must be deployed in specific physical regions. Cloud Eye permissions can be assigned and take effect only in specific regions. If you want a permission to take effect for all regions, assign it in all these regions. The global permission does not take effect.
   - The preceding permissions are all Cloud Eye permissions. For more refined Cloud Eye permissions, see **Permissions Management**.

2. **Create an IAM user**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the Cloud Eye console as the created user, and verify that the user only has the **CES Administrator** permissions.

13.2 Cloud Eye Custom Policies

Custom policies can be created to supplement the system-defined policies of Cloud Eye. For the actions that can be added to custom policies, see **Permissions Policies and Supported Actions** .

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. This topic contains examples of common Cloud Eye custom policies.

Example Custom Policies

- Example 1: Allowing users to modify alarm rules

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "ces:alarms:put"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- Example 2: Denying alarm rule deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CES FullAccess** policy to a user but you want to prevent the user from deleting alarm rules. Create a custom policy for denying alarm rule deletion, and attach both policies to the group the user belongs. Then the user can perform all operations on alarm rules except deleting alarm rules. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "ces:alarms:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- Example 3: Allowing users to have all operation permissions on alarm rules, including creating, modifying, querying, and deleting alarm rules

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is a policy with multiple actions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "ces:alarms:put",
                "ces:alarms:create",
                "ces:alarms:delete"
            ],
            "Effect": "Allow"
        }
    ]
}
```

14 Quota Adjustment

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

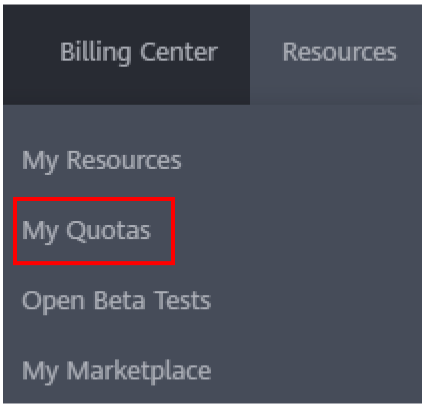
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 14-1 My Quotas

4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

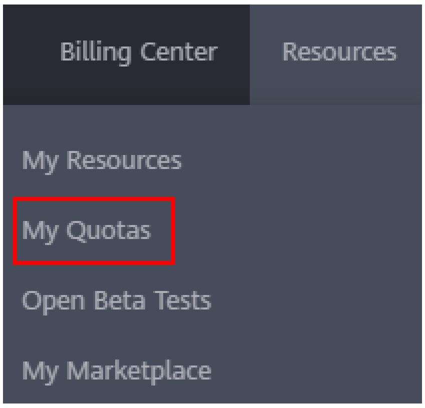
How Do I Apply for a Higher Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

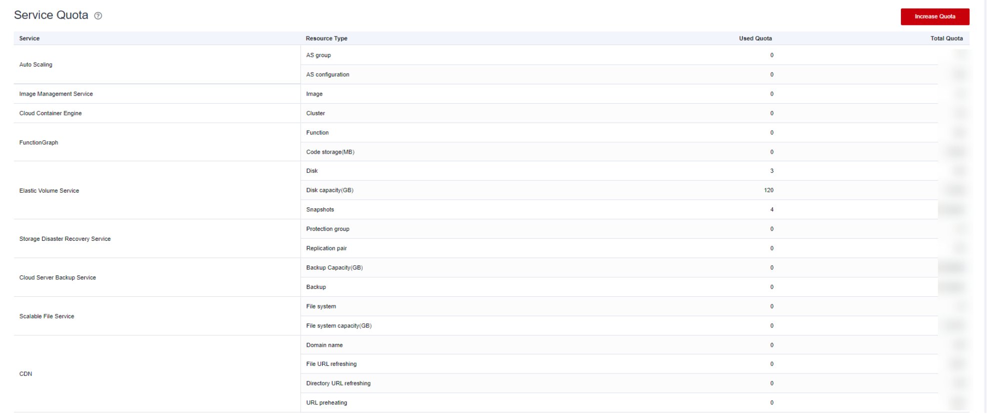
   The **Service Quota** page is displayed.

   Figure 14-2 My Quotas

3. Click **Increase Quota** in the upper right corner of the page.

   Figure 14-3 Increasing quota

   Service Quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	[redacted]
	AS configuration	0	[redacted]
Image Management Service	Image	0	[redacted]
Cloud Container Engine	Cluster	0	[redacted]
FunctionGraph	Function	0	[redacted]
	Code storage(MB)	0	[redacted]
Elastic Volume Service	Disk	3	[redacted]
	Disk capacity(GB)	120	[redacted]
	Snapshots	4	[redacted]
Storage Disaster Recovery Service	Protection group	0	[redacted]
	Replication pair	0	[redacted]
Cloud Server Backup Service	Backup Capacity(GB)	0	[redacted]
	Backup	0	[redacted]
Scalable File Service	File system	0	[redacted]
	File system capacity(GB)	0	[redacted]
CDN	Domain name	0	[redacted]
	File URL refreshing	0	[redacted]
	Directory URL refreshing	0	[redacted]
	URL preheating	0	[redacted]

4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

15 Services Interconnected with Cloud Eye

NOTE

By default, monitoring data of global services is stored in the CN North-Beijing4 region. To query data of global services, switch to CN North-Beijing4.

Category	Service	Namespace	Dimension	Reference
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECS ID	**ECS metrics**
	ECS (OS monitoring)	AGT.ECS	Key: instance_id Value: ECS ID	**ECS OS monitoring metrics**
	Bare Metal Server	SERVICE.BMS	Key: instance_id Value: BMS ID	**BMS Metrics Under OS Monitoring (with Agent Installed)**
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: AS group ID	**AS metrics**
Storage	Elastic Volume Service (attached to an ECS or BMS)	SYS.EVS	Key: disk_name Value: server ID-drive letter (sda is the drive letter.)	**EVS metrics**

Category	Service	Namespace	Dimension	Reference
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name	**OBS metrics**
	Scalable File Service	SYS.SFS	Key: share_id Value: file system name	**SFS metrics**
	SFS Turbo	SYS.EFS	Key: efs_instance_id Value: instance	**SFS Turbo metrics**
Networking	Elastic IP and bandwidth	SYS.VPC	● Key: publicip_id Value: EIP ID ● Key: bandwidth_id Value: bandwidth ID	**VPC metrics**
	Elastic Load Balance	SYS.ELB	● Key: lb_instance_id Value: ID of a classic load balancer ● Key: lbaas_instance_id Value: ID of a shared load balancer ● Key: lbaas_listener_id Value: ID of a shared load balancer listener	**ELB metrics**

Category	Service	Namespace	Dimension	Reference
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID	**NAT Gateway metrics**
	Virtual Private Network	SYS.VPN	Key: connection_id Value: VPN connection	**VPN metrics**
	Cloud Connect	SYS.CC	● Key: cloud_connect_id Value: cloud connection ID ● Key: bwp_id Value: bandwidth package ID ● Key: region_bandwidth_id Value: inter-region bandwidth ID	**CC metrics**
	Direct Connect	SYS.DCAAS	● Key: direct_connect_id Value: connection ● Key: history_direct_connect_id Value: historical connection	**Direct Connect metrics**

Category	Service	Namespace	Dimension	Reference
	Global Accelerator	SYS.GA	● Key: ga_accelerator_id Value: ID of the global accelerator ● Key: ga_listener_id Value: ID of a listener added to the global accelerator	**Global Accelerator metrics**
App middleware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.	**Kafka metrics** **RabbitMQ metrics** **DMS for RocketMQ Metrics**

Category	Service	Namespace	Dimension	Reference
	Distributed Cache Service	SYS.DCS	● Key: dcs_instance_id Value: DCS Redis instance ● Key: dcs_cluster_redis_node Value: Redis Server ● Key: dcs_cluster_proxy_node Value: Proxy in a Proxy Cluster DCS Redis 3.0 instance ● Key: dcs_cluster_proxy2_node Value: Proxy in a Proxy Cluster DCS of Redis 4.0 or Redis 5 instance ● Key: dcs_memcached_instance_id Value: DCS Memcached instance	**DCS metrics**
Database	Relational Database Service	SYS.RDS	For details, see the information in the right column.	**RDS for MySQL metrics** **RDS for MariaDB metrics** **RDS for PostgreSQL metrics** **RDS for SQL Server metrics**

Category	Service	Namespace	Dimension	Reference
	Document Database Service	SYS.DDS	- Key: mongodb_node_id Value: DDS node ID - Key: mongodb_instance_id Value: DDS DB instance ID	**DDS metrics**
	GaussDB (for NoSQL)	SYS.NoSQL	For details, see the information in the right column.	**GaussDB(for Cassandra) metrics** **GaussDB(for Mongo) metrics** **GaussDB(for Influx) metrics** **GaussDB(for Redis) metrics**

Category	Service	Namespace	Dimension	Reference
	GaussDB(for MySQL)	SYS.GAUSSDB	● Key: gaussdb_mysql_instance_id Value: GaussDB(for MySQL) instance ID ● Key: gaussdb_mysql_node_id Value: GaussDB(for MySQL) instance ID ● Key: dbproxy_instance_id Value: GaussDB(for MySQL) Proxy instance ID ● Key: dbproxy_node_id Value: GaussDB(for MySQL) Proxy node ID	**GaussDB(for MySQL) metrics**

Category	Service	Namespace	Dimension	Reference
	GaussDB	SYS.GAUSSDBV5	- Key: gaussdbv5_instance_id Value: GaussDB instance ID - Key: gaussdbv5_node_id Value: GaussDB node ID - Key: gaussdbv5_component_id Value: GaussDB component ID	**GaussDB metrics**
Enterprise Intelligence	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster	**CSS metrics**
	ModelArts	SYS.ModelArts	- Key: service_id Value: real-time service ID - Key: model_id Value: model ID	**ModelArts metrics**
	Data Lake Insight	SYS.DLI	- Key: queue_id Value: queue instance - Key: flink_job_id Value: Flink job	**DLI metrics**
	Data Ingestion Service (DIS)	SYS.DAYU	Key: stream_id Value: real-time data ingestion	**DIS Metrics**

Category	Service	Namespace	Dimension	Reference
Security	Web Application Firewall	SYS.WAF	● Key: instance_id Value: dedicated WAF instance ● Key: waf_instance_id Value: cloud WAF instance	**WAF metrics**
	Database Security Service	SYS.DBSS	Key: audit_id Value: instance	**DBSS metrics**
Management & Governance	Simple Message Notification	SYS.SMN	Key: topic_id Value: topic ID	**SMN metrics**

A Change History

Released On	Description
2023-11-01	This is the fifteenth official release. - Optimized the document structure. - Added 1 Overview. - Added 3 Dashboards (New Version). - Updated the procedure in 4.2 Creating a Resource Group. - Updated 4.3.2 Resource Overview. - Added 4.4.2 Associating Resource Groups with Alarm Templates. - Added 5.2.3 Alarm Policies. - Updated 5.3 Alarm Records. - Updated 5.4.4 Deleting a Custom Template or Custom Event Template. - Added 5.4.5 Copying a Custom Template or Custom Event Template. - Added 5.4.6 Associating a Custom Template with a Resource Group. - Added 5.4.7 Importing and Exporting Custom Template or Custom Event Templates. - Updated 5.2.4 Modifying an Alarm Rule. - Updated 7 Cloud Service Monitoring. - Added 10 Task Center.
2023-06-30	This issue is the fourteenth official release. - Added 5.6 Example: Creating an Alarm Rule to Monitor ECS CPU Usage. - Added 7.1 Viewing Raw Data.
2023-05-30	This issue is the fifty-eighth official release. - Added 5.8 Alarm Masking.

Released On	Description
2020-05-30	This issue is the twelfth official release. - Added **6.7.3 Installing the Direct Connect Metric Collection Plug-ins**.
2019-09-19	This issue is the tenth official release. - Optimized **6.2 Agent Installation and Configuration**. - Optimized **9.4 Events Supported by Event Monitoring**.
2019-05-10	This issue is the ninth official release. - Optimized the procedure for installing the Agent. - Added application scenarios to the product introduction.
2019-03-30	This issue is the eighth official release. - Changed **Virtual Private Cloud** to **Elastic IP and Bandwidth** under **Cloud Service Monitoring** on the Cloud Eye console. - Optimized the Distributed Message Service (DMS) metrics.
2019-03-04	This issue is the seventh official release. Optimized the strings in several sections, such as "Creating Alarm Rules" and "Viewing Metrics".
2019-02-21	This issue is the sixth official release. - Added "Quota Adjustment".
2018-12-30	This issue is the fifth official release. - Optimized the names of Elastic Cloud Server (ECS) and Elastic Volume Service (EVS) disk metrics. - Optimized the names of several Relational Database Service (RDS) metrics.
2018-09-14	This issue is the fourth official release. - Launched the **Server Monitoring** function. - Added descriptions that resource groups support BMSs. - Optimized the strings for alarm rule creation.
2018-04-30	This issue is the third official release. - Optimized the **Dashboard** page. - Launched the **Resource Groups** function. - Launched the **Custom Monitoring** function. - Interconnected with Workspace, Distributed Message Service (DMS), Distributed Cache Service (DCS), and NAT Gateway.

Released On	Description
2018-01-30	This issue is the second official release. ● Updated the document structure.
2017-12-31	This issue is the first official release.