Cloud Eye

User Guide

Issue	01
Date	2025-01-03

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 My Dashboards

1.1 Overview

My Dashboards allows you to view core metrics in an all-in-one dashboard based on your own needs. You can compare performance data of different services or different dimensions in one graph.

1.2 Creating a Dashboard

You must create a dashboard before adding graphs. You can create up to 10 dashboards.

Procedure

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. Choose **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. Only letters, digits, hyphens (-), and underscores (_) are allowed.
   - **Enterprise Project**: Select an enterprise project to be associated with the dashboard. Only users who have all permissions for the selected enterprise project can manage the dashboard.

     NOTE

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

1.3 Adding a Graph

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

You can add up to 50 metrics, regardless of the services and dimensions, to one graph.

Procedure

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. Choose **My Dashboards** and click the name of the dashboard to which you want to add a graph. On the displayed page, click **Add Graph**. You can select **Line Chart** or **Bar Chart** to display the graph.
4. On the **Add Graph** page, set parameters as prompted.

   Table 1-1 Parameters for adding a graph

Parameter	Description
Metric Display	• When selecting a line graph, you can select **One graph for a single metric** or **One graph for multiple metrics**. • When a bar chart is selected, only **One graph for a single metric** is available.
Monitoring Scope	Select the target resources and metrics. If you select a bar chart, all resources are selected by default.
Quantity	Metric data of selected resources is displayed. You can display the top 3 to 10 resources, in ascending or descending order.
Advanced Settings	You can configure the name, threshold, and legend name of a graph.

5. Click **Finish**.

1.4 Viewing a Graph

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

Procedure

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane, choose **Dashboard**.

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

NOTE

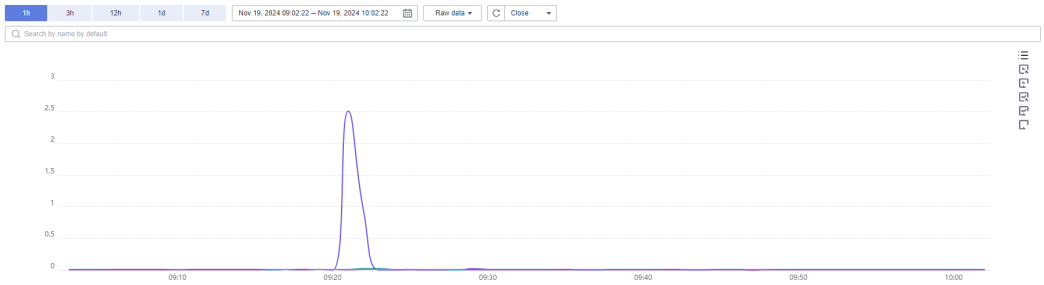
- You can drag a graph to adjust its display sequence to meet your monitoring requirements. You can also adjust the number of graphs displayed in each row.
- You can click **Full Screen** to view the graphs. For details, see **Using the Full Screen**.
- You can configure the refresh interval for graphs on the dashboard. The default option is **Never refresh**.

4. Hover your mouse over a graph. In the upper right corner, click to view monitoring details on an enlarged graph. Select a default time range or customize the time range to view the metrics.

   By default, raw metric data is displayed if **1h**, **3h**, or **12h** is selected. For **1d**, **7d**, and longer time ranges, aggregated data is displayed by default.

   On the enlarged graph, you can **Customizing a Period to View Metrics** or **Selecting Resources to Be Monitored and Viewing Metrics**.

Figure 1-1 Viewing graphs

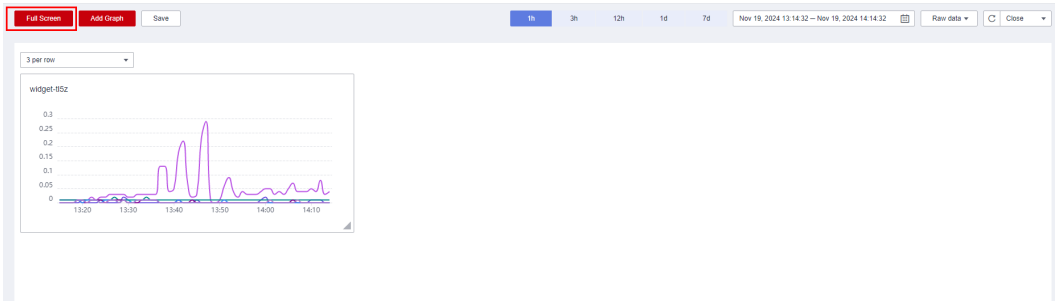


Using the Full Screen

The full screen displays metric data more clearly.

- To enter the full screen, select a dashboard, click its name, and click **Full Screen** in the upper left corner.
- To exit the full screen, press **Esc**.

Figure 1-2 Full screen

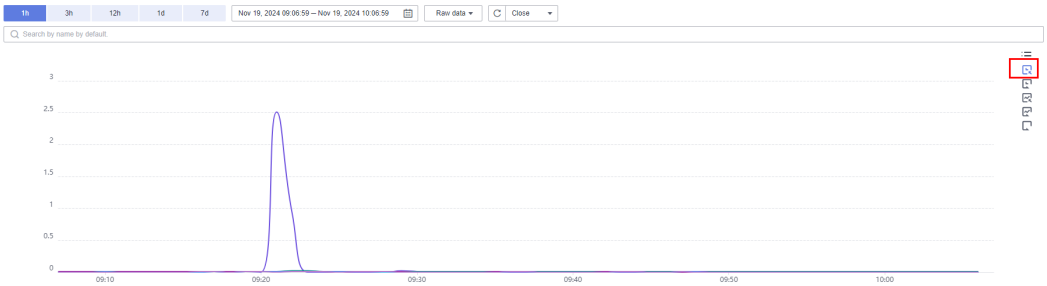


Customizing a Period to View Metrics

By default, you can select **1h**, **3h**, **12h**, **1d**, or **7d**. If you want to view metrics in the last two hours or a customized period, you can drag the mouse to select the time range you want to view on the X axis.

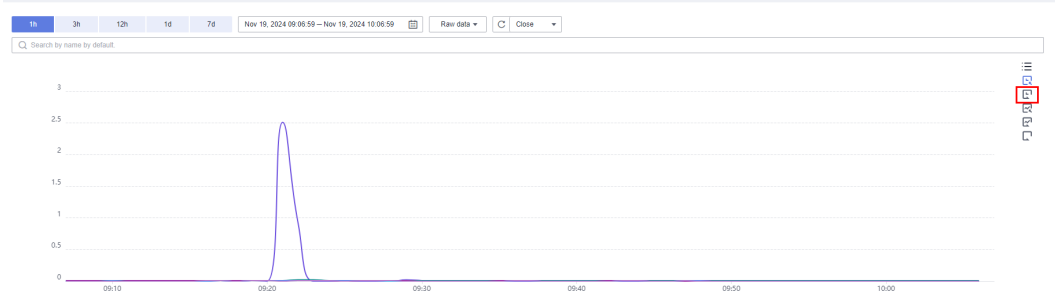
- To view metric details in a customized time range, click the first icon on the right, as shown in **Figure 1-3**. Drag the mouse to select a customized time range. The system displays the monitoring data in the selected time range.

  Figure 1-3 Customizing a time range

- To stop viewing the metric details within a customized time range, click the second icon on the right. The system will reset the time range.

  Figure 1-4 Going back to the default time range

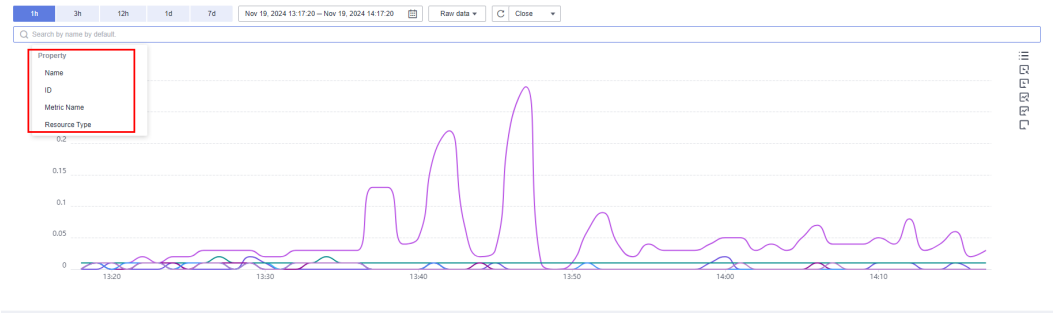
  

Selecting Resources to Be Monitored and Viewing Metrics

You can compare the same metric of multiple resources on one graph. When there are a large number of resources, you can select only some resources and compare their metrics.

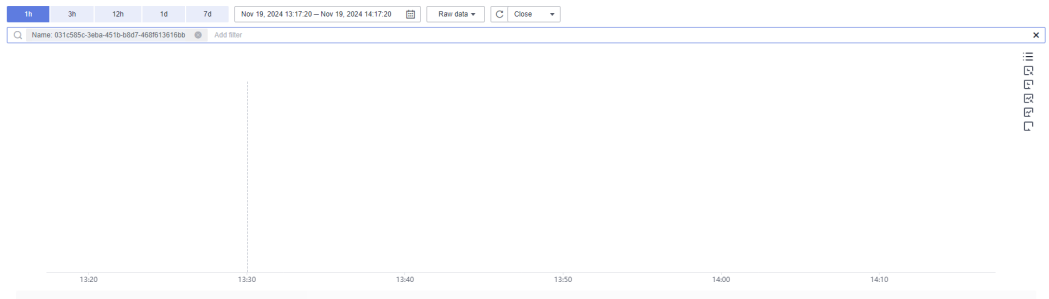
- By default, resources are sorted by **Name**, as shown in **Figure 1-5**. You can also select resources by **ID**, **Metric Name**, or **Resource Type**. The system displays the data of selected resources and hides that of other resources.

Figure 1-5 Selecting monitored objects



- To clear the monitored resources you have selected, click ✕.

Figure 1-6 Clearing monitored objects



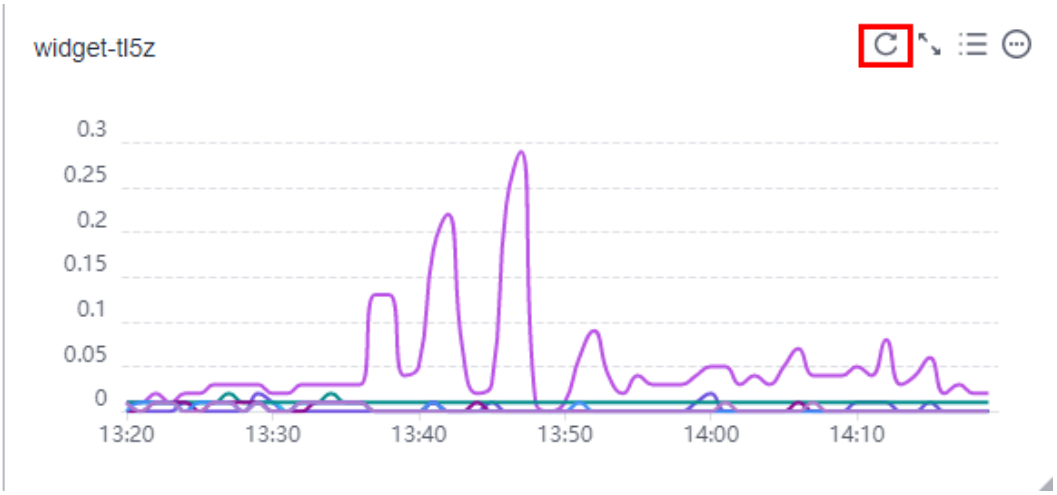
1.5 Configuring a Graph

This topic describes how you can add, modify, and delete metrics on a line chart and a bar chart.

Procedure for Configuring Line Charts

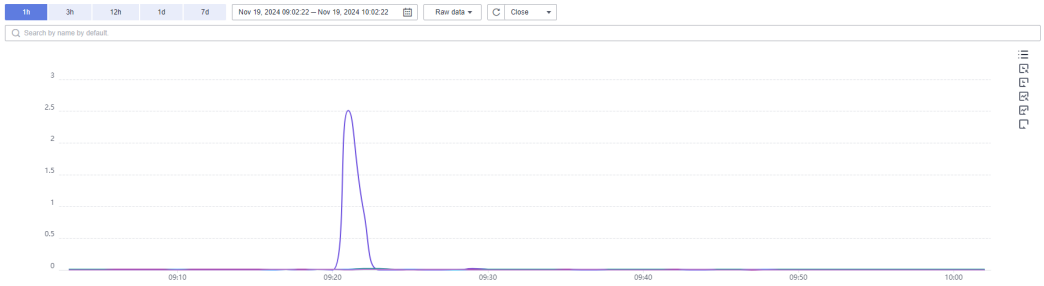
1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane, choose **My Dashboards**. Click the name of the dashboard on which you want to configure a graph.
4. In the upper right corner of each graph, click ↻ to refresh the graph.

Figure 1-7 Refreshing a graph



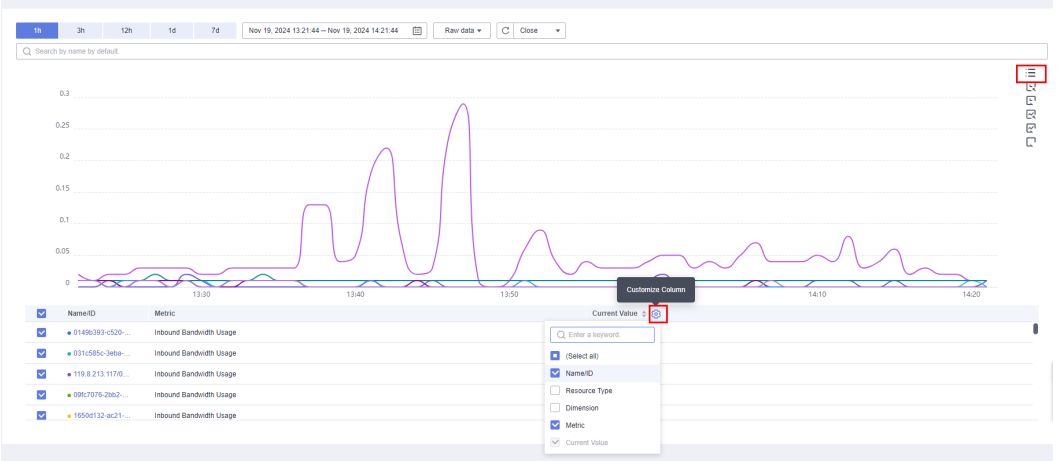
5. Locate a graph and click to enlarge it. On the enlarged graph, customize a time range for viewing metrics. In the search box, select filters and then the monitored objects to be displayed. Select the refresh interval and aggregation method to display metrics.

Figure 1-8 Viewing monitoring details in a line chart



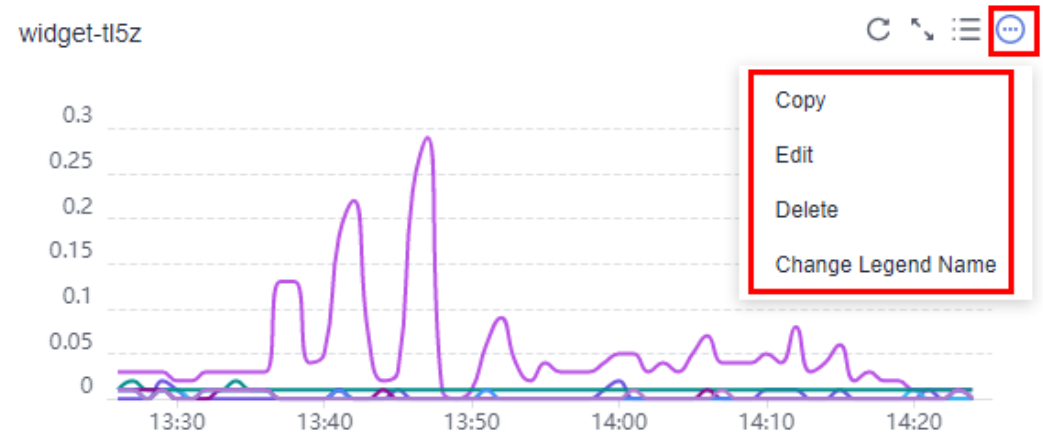
6. Click to display the monitored objects. Click to customize columns to be displayed in the list below the graph.

Figure 1-9 Viewing monitoring items



7. Go back to the dashboard of the graph. Click to copy, edit, or delete the graph, or change its legend name.

Figure 1-10 Managing a graph



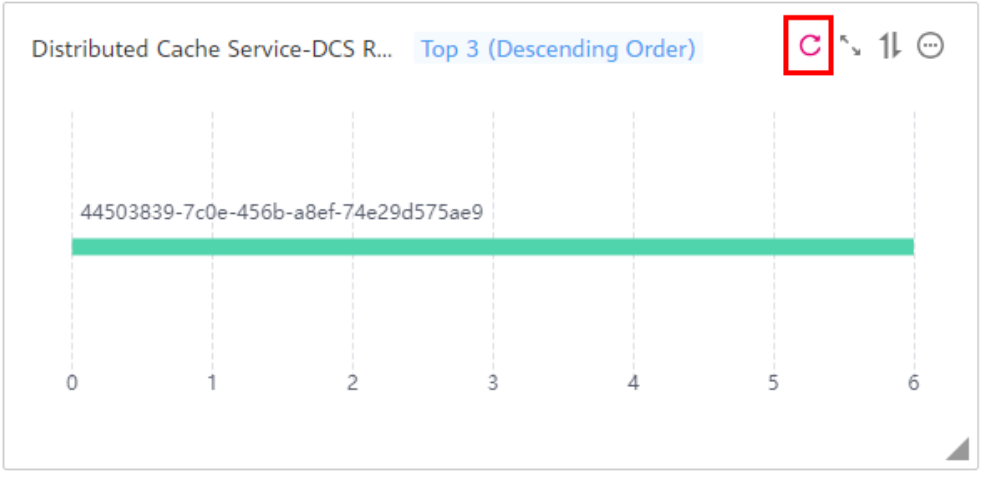
NOTE

Change Legend Name is only available if **Specific resources** is selected for **Monitoring Scope**.

Procedure for Configuring Bar Charts

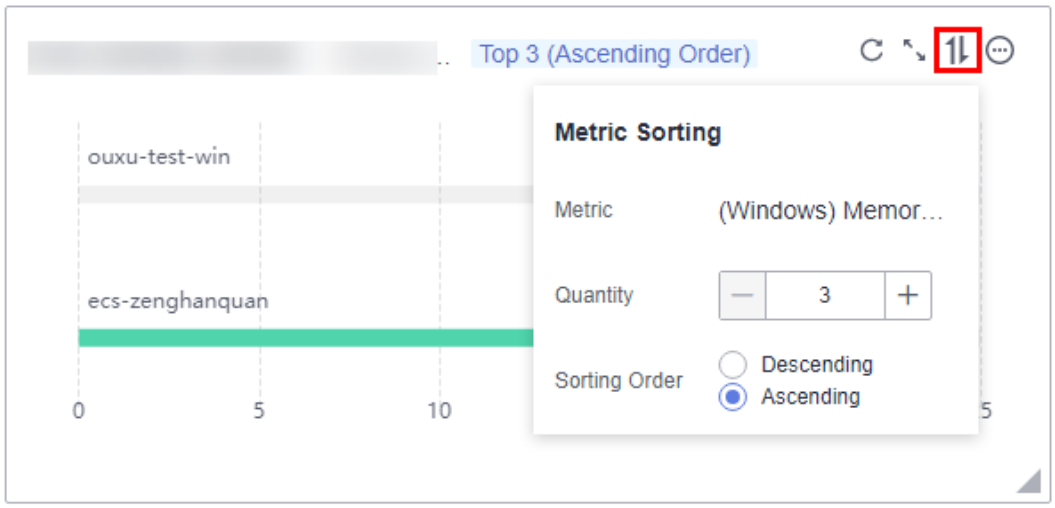
1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane, choose **My Dashboards**. Click the name of the dashboard on which you want to configure a graph.
4. In the upper right corner of each graph, click to refresh the graph.

Figure 1-11 Refreshing a graph



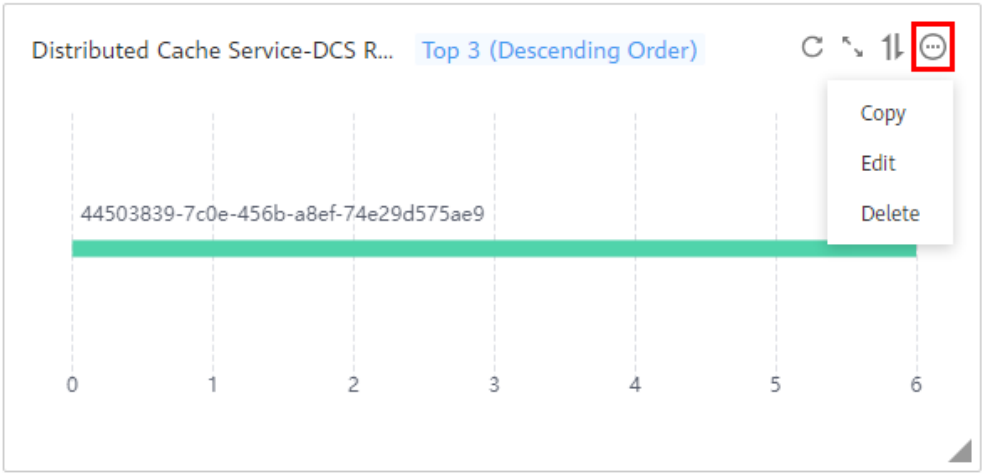
5. Locate a graph and click to enlarge it. On the enlarged graph, customize a time range for viewing metrics. Select the refresh interval and aggregation method to display metrics.
6. Click to configure **Quantity** and **Sorting Order**.

Figure 1-12 Sorting metrics



7. Go back to the dashboard of the graph. Click to copy, edit, or delete the graph, or move the graph to another graph group.

Figure 1-13 Managing a graph



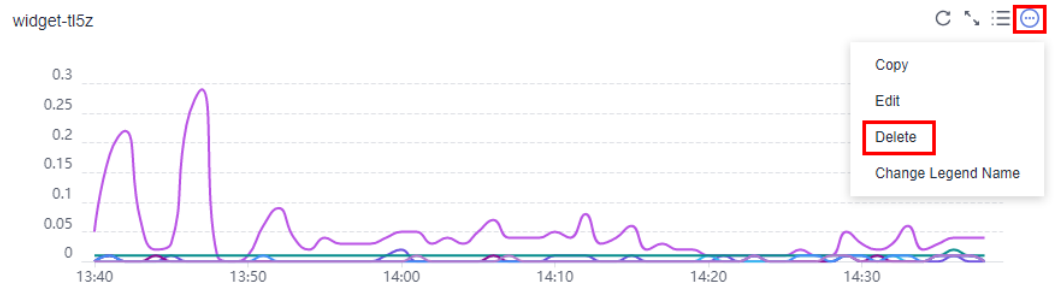
1.6 Deleting a Graph

Procedure

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

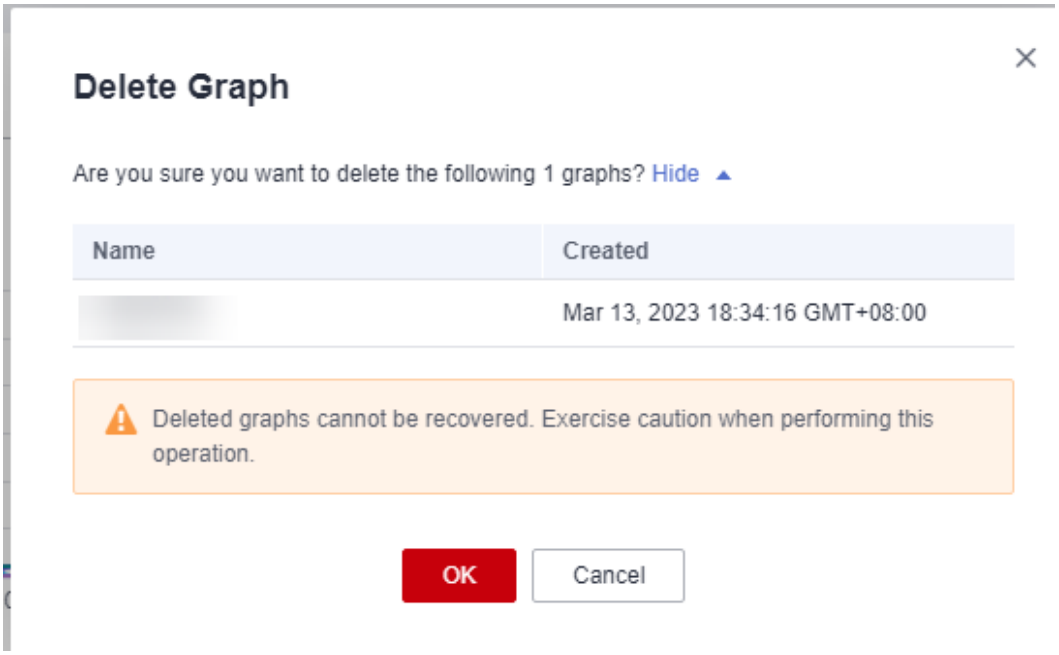
3. In the navigation pane, choose **Dashboard**.
4. Locate the dashboard from which you want to delete a graph and click the dashboard name.
5. Click  and choose **Delete**.

Figure 1-14 Deleting a graph



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

Figure 1-15 Deleting a graph



1.7 Deleting a Dashboard

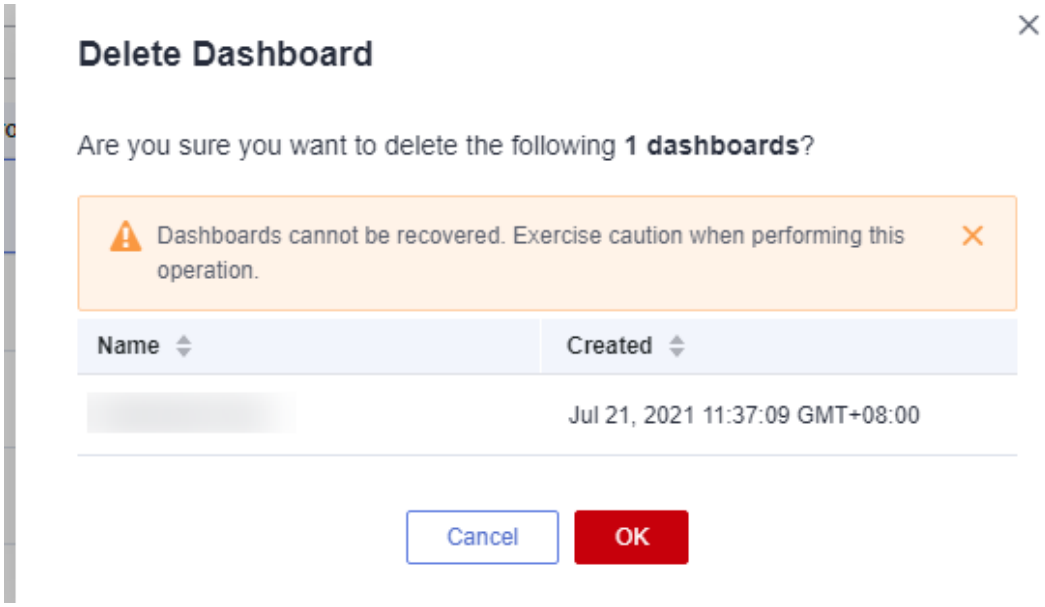
If an existing dashboard cannot meet your requirements, you can delete it and re-plan graphs on a new dashboard. After you delete a dashboard, all graphs added to it will also be deleted.

Procedure

1. Log in to the management console.

2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**.
4. Locate the dashboard to be deleted.
5. Click **Delete** in the **Operation** column.
6. In the displayed **Delete Dashboard** dialog box, click **OK**.

Figure 1-16 Deleting a dashboard



2 Resource Groups

2.1 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.

2.2 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.

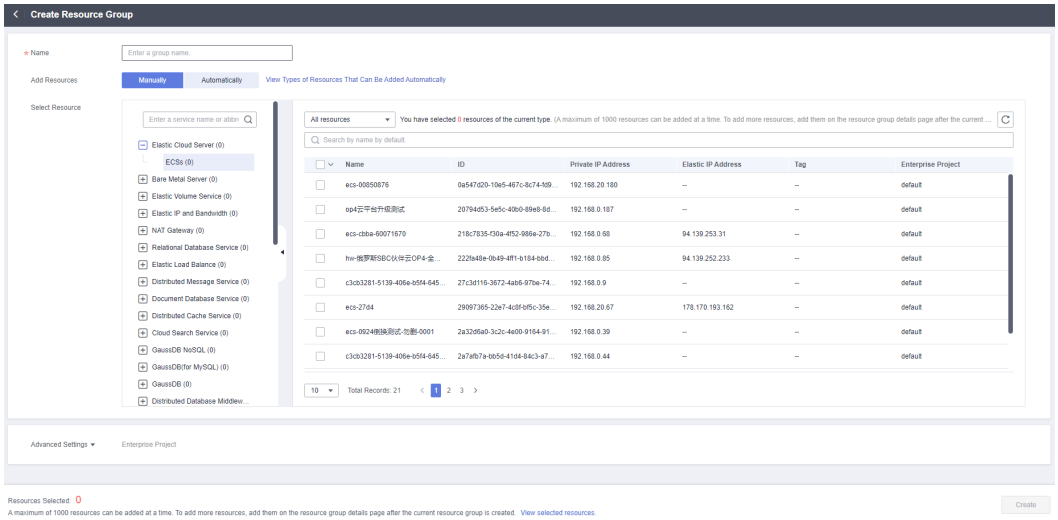
Restrictions

- Each user can create up to 1,000 resource groups.
- A resource group must 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**.
6. Enter a group name and set parameters as needed.
   a. If you select **Manually** for **Add Resources**, select resources for the resource group.

Figure 2-1 Manually adding resources



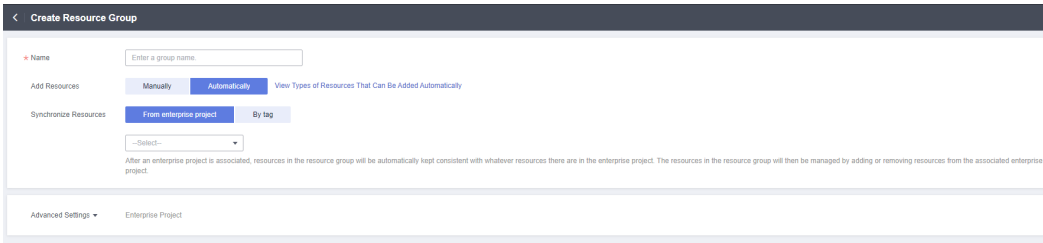
NOTE

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.

b. If you select **Automatically** for **Add Resources**, select **From enterprise project** or **By tag** for **Synchronize Resources**.

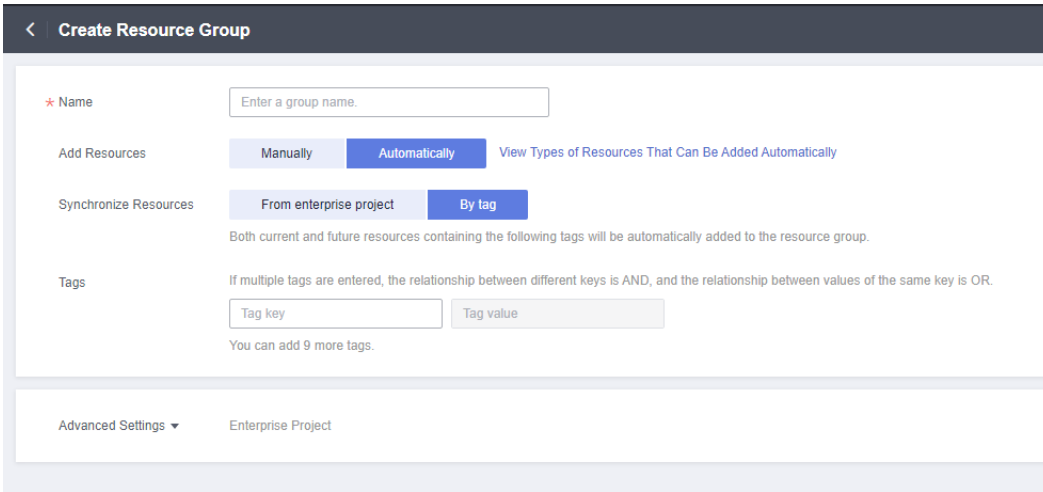
i. If you select **From enterprise project** for **Synchronize Resources**, select one or more enterprise projects. The resources in the resource group will automatically be synchronized with those in the enterprise project. To manage resources in this resource group, you can only add or remove resources to and from the enterprise project.

Figure 2-2 Synchronizing resources from enterprise projects



ii. If you select **By tag** for **Synchronize Resources**, select tags.

Figure 2-3 Matching resources by tag



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. Select an enterprise project.

Figure 2-4 Enterprise Project

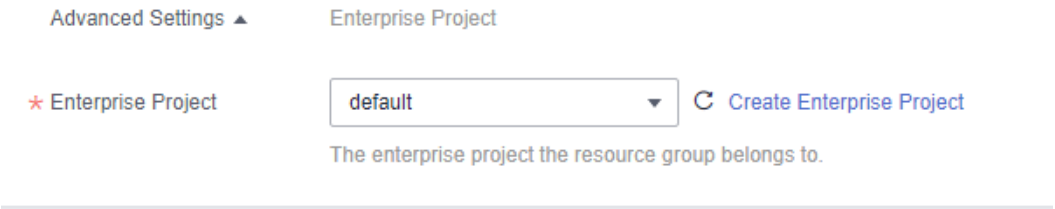


Table 2-1 Advanced settings parameters

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

8. Click **Create**.

2.3 Viewing Resource Groups

2.3.1 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 2-2 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.
Alarm Status	• 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.
Resources (Alarm/Total)	Total number of resources that are generating alarms in a group/Total number of resources in the group.
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.
Add Resources	Specifies how you add resources to a resource group. The value can be **Manually** or **Automatically**.
Synchronize Resources	You can add all resources in an enterprise project or resources with the same tags to a resource group.
Created	Specifies the time when the resource group was created.
Operation	You can create alarm rules or delete a resource group.

2.3.2 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 resource group name and remove or add resources. There is also a link for you to quickly create alarm rules for those resources.

2.3.3 Alarm Rules

The **Alarm Rules** page displays all alarm rules in a resource group. You can enable, disable, modify, or delete an alarm rule.

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.
6. In the navigation pane on the left, choose **Alarm Rules** to view all alarm rules in the resource group.

2.4 Managing Resource Groups

2.4.1 Modifying a Resource Group

When you need to add resources to or delete resources from a resource group, modify the 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. Click a resource group name to go to the **Resource Overview** page

- Adding resources: Click **Add Resources**.
- Removing resources: In the resource list, select the resource to be removed and click **Remove** in the **Operation** column.

2.4.2 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 resource group and click **Delete** in the **Operation** column.
6. In the displayed **Delete Resource Group** dialog box, click **OK**.

3 Using the Alarm Function

3.1 Introduction to the Alarm Function

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 requests, 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 account contact.

3.2 Creating Alarm Notification Topics

3.2.1 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.
6. Enter a topic name and display name (topic description).

   Table 3-1 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 once the topic is created.
Display Name	Specifies the message sender name, which can contain up to 192 bytes. **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**.
Enterprise Project	Centrally manages cloud resources and members by project.
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 (-). • You can add up to 20 tags to a topic.

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.

3.2.2 Adding Subscriptions

A topic is a channel used by SMN to publish messages. After you create a topic, add subscriptions. When the metric data reaches the specified threshold or an event occurs, Cloud Eye will send alarms to subscription endpoints of the topic.

Adding Subscriptions

1. Log in to the management console.
2. Select **Simple Message Notification** under **Application**.

   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 and click **Add Subscription** in the **Operation** column.

   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.

3.3 Creating Alarm Rules

3.3.1 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.

3.3.2 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 the parameters.
   a. Configure the alarm rule name and description.

Table 3-2 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 3-3 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	The monitoring scope of an alarm rule can be **All resources**, **Resource groups**, or **Specified resources**. **NOTE** • If you select **All resources**, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources. • If **Resource groups** is selected and any resource in the group meets the alarm policy, an alarm is triggered. • If you select **Specific resources**, select one or more resources and click  to add them to the box on the right.	All resources
Method	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 or a custom alarm template.	ECS Alarm Template
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **Custom Monitoring** or a specific cloud service, whether an alarm will be triggered 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** to **Event Monitoring**, the event that triggers an alarm is an instant operation. For example, if event improper ECS running occurs, Cloud Eye triggers an alarm. **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.

Table 3-4 Alarm Notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, SMS 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. • The account contact is the tenant owner. If a user registers both a mobile number and an email address, they will receive alarm information through both channels. However, if only one of these contact methods is registered, the alarm information will be sent exclusively to that registered one. • A topic is a specific event type for publishing messages or subscribing to notifications. If the required topic is not available, create one and add subscriptions to it first. For details, see **Creating a Topic** and **Adding Subscriptions**.
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule. If **Notification Window** is set to **08:00-20:00**, Cloud Eye sends notifications only from 08:00 to 20:00.
Trigger Condition	Specifies the condition for triggering an alarm notification. • If **Alarm Type** is set to **Metric**, you can select **Generated alarm**, **Cleared alarm**, or both. • If **Alarm Type** is set to **Event**, you can select **Generated alarm** only.

d. Select an enterprise project.

Figure 3-1 Advanced Settings

Table 3-5 Name and **Description**

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

e. Click **Create**.

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

You can choose **Alarm Management** > **Alarm Records** and click **View Details** to view recent alarms.

3.4 Viewing 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 180 days.

When an alarm is generated, you can view the alarm records about the cloud resource.

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.
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.

   NOTE

   - You can select a time range within the past 180 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.

3.5 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**.
5. Click the arrow on the left of the cloud service name to view the built-in alarm rules.

   NOTE

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

3.6 Alarm Masking

3.6.1 Introduction

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

Alarm masking applies to invalid alarms triggered for cloud resources, repeated alarms caused by known issues or faults, and frequent but unimportant alarms identified by users. To ease O&M, you can mask these alarms, in this way, you can better focus on important alarms.

You can mask a resource, or some alarm policies or system events of the resource.

3.6.2 Creating a Masking Rule

Scenarios

This section describes how to create 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. In the upper right corner of the page, click **Create Masking Rule**.
5. On the displayed page, configure parameters as prompted.

Figure 3-2 Create Masking Rule

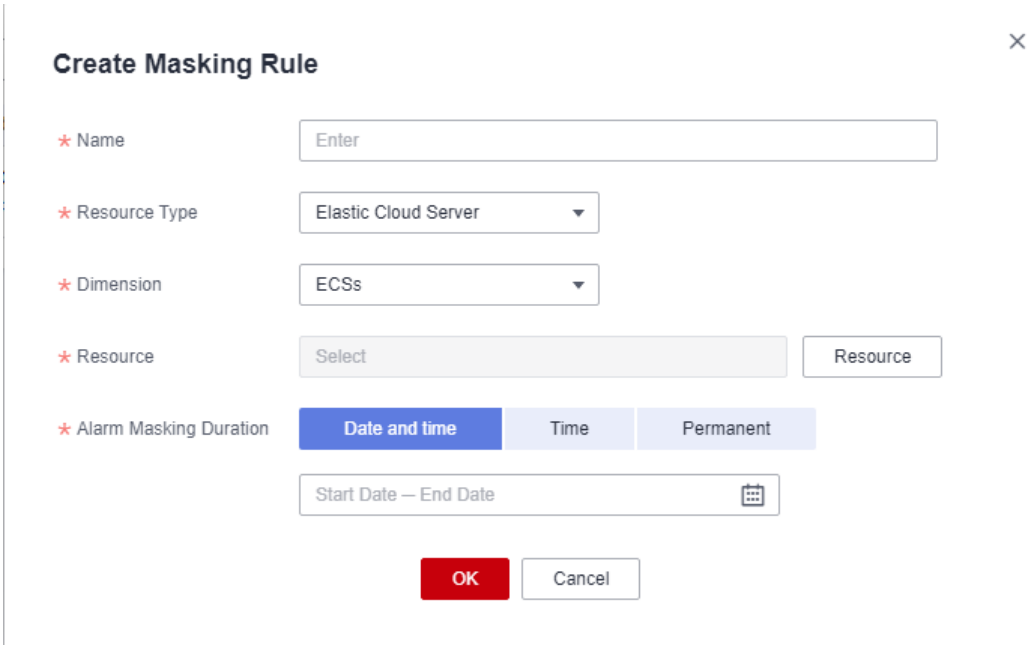


Table 3-6 Parameters

Parameter	Description
Name	Specifies the name of a masking rule.
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.
Resource	Select the object to be masked. **NOTE** A maximum of 100 resources of the service can be added at a time.

Parameter	Description
Alarm Masking Duration	Specifies the time when the masking rule takes effect. • **Time and Date**: The masking rule takes effect within the 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**-**2022-12-31** and the effective time is **08:00**-**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 takes effect permanently.

6. Click **OK**.

NOTE

If you select a resource to be masked, all metrics of the resource in this dimension will be masked.

3.6.3 Modify a Masking Rule

Scenarios

This section describes how to modify masking rules.

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 row that contains the masking rule to be modified, and click **Modify** in the **Operation** column.
5. On the displayed page, configure parameters.

Table 3-7 Parameters

Parameter	Description
Name	Specifies the name of a masking rule.
Resource	Select the object to be masked. **NOTE** A maximum of 100 resources of the service can be added at a time.

Parameter	Description
Alarm Masking Duration	Specifies the time when the masking rule takes effect. • **Time and Date**: The masking rule takes effect within the 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**-**2022-12-31** and the effective time is **08:00**-**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 takes effect permanently. **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 .

3.6.4 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. Choose **Alarm Management** > **Alarm Masking**.
4. On the displayed page, locate the row that contains the masking rule to be modified, and click **Delete** in the **Operation** column.
5. Click **OK**.

3.6.5 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.

3.7 Alarm Rule Management

This topic describes how to manage alarm rules as your system grows.

3.7.1 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 3-8 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

Parameter	Description	Example Value
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
Method	There are two options: **Use existing template** or **Configure manually**. **NOTE** Available alarm templates will be displayed in the drop-down box. If you select a template and the template is modified later, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Monitored Object	Specifies the resource the alarm rule is created for. You can specify one or more resources.	N/A
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

Parameter	Description	Example Value
Trigger Condition	Specifies the condition for triggering an 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**.

3.7.2 Disabling Alarm Rules

Scenarios

If you do not need to monitor the metrics or events of a resource, you can disable the alarm rule created for the resource. Once the alarm rule is disabled, the monitoring metrics or events configured in it will no longer trigger any alarms.

Procedure

To disable an alarm rule, go to the **Alarm Rules** page, locate 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 **OK**.

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 **OK**.

3.7.3 Enabling Alarm Rules

Scenarios

If an alarm rule has been created for a resource but is currently disabled, you can enable it to keep track of the metrics or events configured in it. This allows you to promptly identify any abnormal metric dataand quickly rectify the fault.

Procedure

To enable a single alarm rule, go to the **Alarm Rules** page, locate 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 **OK**.

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 **OK**.

3.7.4 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**.

3.8 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.

3.8.1 Viewing Alarm Templates

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. Choose **Alarm Management** > **Alarm Templates**.

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

- Viewing the template content: To view details of an alarm template, click the down arrow next to the target alarm template.
- Searching for an alarm template: You can search for an alarm template by template name or resource type.

3.8.2 Creating a Custom Alarm or Event Template

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. Choose **Alarm Management** > **Alarm Templates**.
5. Click **Create Custom Template**.
6. On the **Create Custom Template** page, configure parameters by referring to **Table 3-9**.

Figure 3-3 Create Custom Template

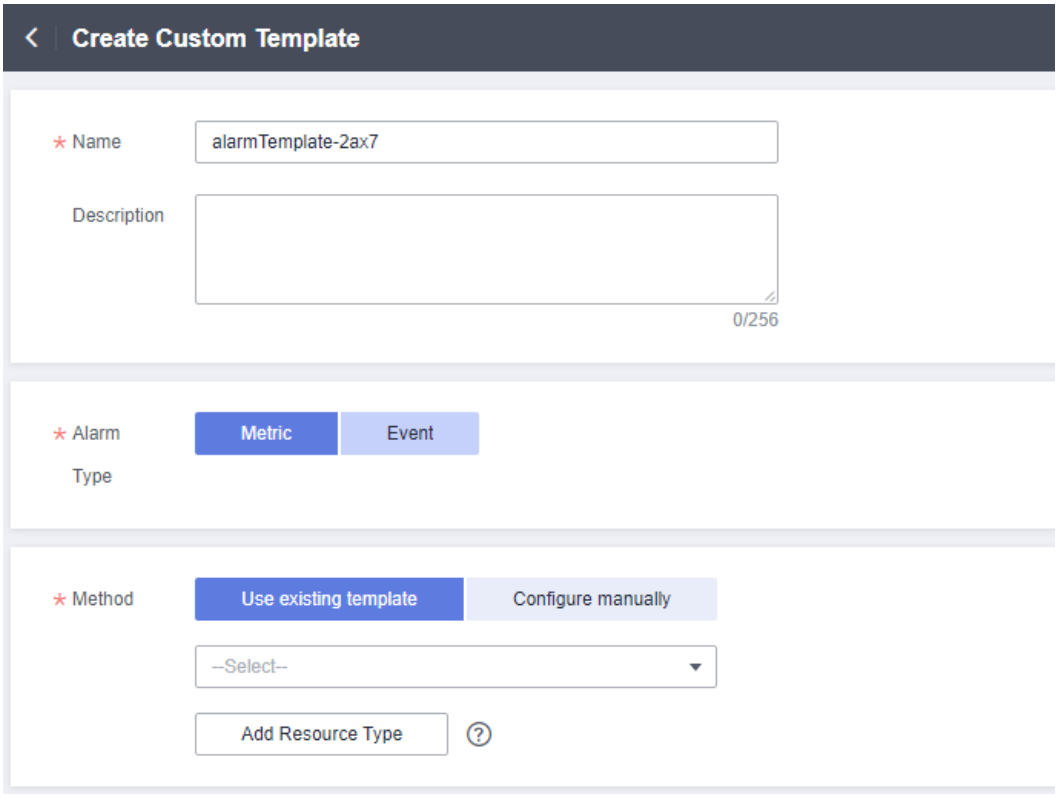


Table 3-9 Parameters

Parameter	Description
Name	Specifies the alarm template name. The system generates a random one, which you can modify. Example value: **alarmTemplate-c6ft**
Description	(Optional) Provides supplementary information about the custom template.
Alarm Type	You can select **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 **Using existing template** or **Configure manually**. • **Using existing template**: Select an existing template for **Template**. The alarm rules in the template are automatically added. • **Configure manually**: You can customize alarm policies as required.

Parameter	Description
Add Resource Type	Specifies the type of the resource the alarm rule is created for. Example value: **Elastic Cloud Server** **NOTE** A maximum of 50 resource types can be added for each service.

7. Click **Create**.

3.8.3 Modifying a Custom Alarm or Event Template

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. Choose **Alarm Management** > **Alarm Templates**.
5. Click the **Custom Templates** or **Custom Event Templates** tab.
6. Locate the row containing the alarm template to be modified, and click **Modify** in the **Operation** column.
7. On the **Modify Custom Template** page, modify the configured parameters by referring to **Table 3-9**.
8. Click **Modify**.

3.8.4 Deleting a Custom Alarm or Event Template

CAUTION

Deleted custom templates cannot be restored. Exercise caution when performing this operation.

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. Choose **Alarm Management** > **Alarm Templates**.
5. Click the **Custom Templates** or **Custom Event Templates** tab.
   - Locate the alarm template to be deleted and click **Delete** in the **Operation** column.
   - Select multiple templates and click **Delete** above the list.
6. In the displayed dialog box, click **OK**.

3.8.5 Copying an Alarm Template

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. Choose **Alarm Management** > **Alarm Templates**.
   a. On the **Default Templates** or **Default Event Templates** tab, locate the desired alarm template and click **Copy** in the **Operation** column.
   b. Click the **Custom Templates** or **Default Event Templates** tab, locate the desired alarm template, and choose **More** > **Copy** in the **Operation** column.
5. In the **Copy Template** dialog box, set parameters and click **OK**.

4 Server Monitoring

4.1 Introduction to Server Monitoring

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 **Services Interconnected with Cloud Eye**.
- 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 **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 GB memory for a Linux ECS and 4 vCPUs and 8 GB memory or higher specifications for a Windows ECS.
- The Agent will occupy system ports. For details, see descriptions of **ClientPort** and **PortNum** in section **(Optional) Manually Configuring the Agent (Linux)**. If the Agent port conflicts with a service port, see **What Should I Do If the Service Port Is Used by the Agent?**
- 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 public images provided by Huawei Cloud. If any problem occurs when you use a private image, Cloud Eye will not provide technical support.

Monitoring Capabilities

Server monitoring provides multiple metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers. For details about metrics, see **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.

4.2 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	Supported Service	Reference
Installing the Agent on a Linux server	ECS and BMS	**Installing and Configuring the Agent on a Linux ECS or BMS**
Installing the Agent on a Windows server	ECS	**Installing and Configuring the Agent on a Windows ECS**
Installing the Agent in batches on Linux servers	ECS	**Installing the Agents in Batches on Linux ECSs**

Agent installation and configuration description:

- To successfully install the Agent, ensure that both DNS and security group rules are correctly configured.
- 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, and then configure the Agent for the new ECS or BMS by following the steps in **Restoring the Agent Configurations on a Linux Server**.

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.

4.3 Agent Features per Version

Metrics or functions supported by the Agent vary depending on the Agent version. By default, the Agent is automatically upgraded, so that you can experience new functions as earlier as possible. The following describes features of each Agent version.

Version 2.4.1

The Agent can monitor more metrics.

Version 2.3.2

The Agent architecture and installation path are updated.

Version 1.2.3

The permission on the file generated after the Agent is installed is optimized.

Version 1.2.2

A 20-minute random hash is added when the Agent is started.

Version 1.1.9

Some metrics are optimized for better experience.

Version 1.1.2

The Agent performance is optimized. When the Agent does not report data, manually rectify it by referring to **What Should I Do If the Monitoring Period Is Interrupted or the Agent Status Keeps Changing?**

Version 1.0.14

CPU, CPU load, disk, and disk I/O metrics are added to **OS Monitoring**. For details, see **Services Interconnected with Cloud Eye**.

4.4 Installing and Configuring the Agent on a Linux ECS or BMS

4.4.1 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 server address of an ECS via command lines or the management console.

NOTE

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

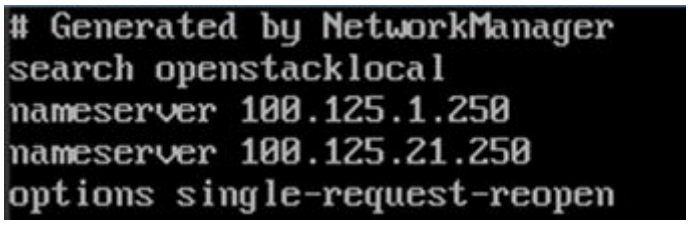
Modifying the DNS Server Address (Command Lines)

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 4-1 Adding the DNS server address (Linux)



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. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.

   On the ECS console, click the name of the ECS to view its details.
3. On the displayed **Summary** tab page, click the VPC name.

   The **Virtual Private Cloud** page is displayed.
4. Click the name of the 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 the 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**.
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. 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 4-1**.

Table 4-1 Security group rules

Protocol	Port	Type	Destination	Description
TCP	80	IPv4	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.
TCP and UDP	53	IPv4	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.
TCP	443	IPv4	100.125.0.0/16	Used to collect monitoring data and send the data to Cloud Eye.

4.4.2 Installing the Agent on a Linux Server

Scenarios

This topic describes how to manually install the Agent on a Linux ECS or BMS.

Constraints

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

Prerequisites

- 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 performed operations described in **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.

Procedure

1. Log in to the ECS or BMS as user **root**.
2. Install the Agent.

NOTE

The script supports x86 and Kunpeng Arm-based ECSs.

```
cd /usr/local && curl -k -O https://uniagent-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/package/agent_install.sh && bash agent_install.sh -r eu-west-101 -u 0.1.9 -t 2.7.2 -o myhuaweicloud.eu -d agent.ces.myhuaweicloud.eu
```

The Agent is installed if the following command output is displayed.

Figure 4-2 Successful installation

```
telescope_linux_amd64/
telescope_linux_amd64/uninstall.sh
telescope_linux_amd64/install.sh
telescope_linux_amd64/bin/
telescope_linux_amd64/bin/conf.json
telescope_linux_amd64/bin/telescope
telescope_linux_amd64/bin/conf_ces.json
telescope_linux_amd64/bin/conf_lts.json
telescope_linux_amd64/bin/record.json
telescope_linux_amd64/bin/logs_config.xml
telescope_linux_amd64/bin/agent
telescope_linux_amd64/telescoped
telescope_linux_amd64/telescope-1.0.12-release.json
Current user is root.
Current linux release version : CENTOS
Start to install telescope...
In chkconfig
Success to install telescope to dir: /usr/local/telescope.
Starting telescope...
Telescope process starts successfully.
[root@ecs-74e5-7 local]#
```

3. Configure the Agent by referring to **Restoring the Agent Configurations on a Linux Server** or **(Optional) Manually Configuring the Agent (Linux)**.

   NOTE

   - **Restoring Agent Configurations** allows you to configure **AK/SK**, **RegionID**, and **ProjectId** in just a few clicks. You can also modify related configuration files by referring to **(Optional) Manually Configuring the Agent (Linux)**.
   - Agent configuration restoration cannot be performed on BMSs. For details about how to modify the Agent configuration file on a BMS, see **(Optional) Manually Configuring the Agent (Linux)**.

4. 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

4.4.3 Restoring the Agent Configurations on a Linux Server

Scenarios

This topic describes how to restore the Agent configurations on the Cloud Eye console (recommended).

Most regions support one-click configuration of Agent permissions. You can choose **Server Monitoring** > **Elastic Cloud Server** and click **Configure** on top of the page. After the configuration is complete, the Agent configurations of all servers in these regions are restored by default, and the **Configure** button is no longer displayed. If the system displays a message indicating that you do not have the required permission, rectify the fault by referring to FAQ.

NOTE

- The **Restore Agent Configurations** option is available for Agent 1.0.14 or later. If the Agent version is earlier than 1.0.14, upgrade the Agent first and then restore the Agent configurations or manually configure the Agent by following the instructions in **(Optional) Manually Configuring the Agent (Linux)**.
- The **Restore Agent Configurations** option is unavailable for BMSs. For details, see **(Optional) Manually Configuring the Agent (Linux)**.
- After you configure the Agent, its status is still displayed as **Not installed** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.
- If the Agent is in the **Running** state and **Monitoring Status** is enabled, the Agent has been installed and has started to collect fine-grained metric data.

Restoring the Agent Configurations

1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**. In the navigation pane on the left, choose **Server Monitoring**.
3. On the **Server Monitoring** page, select a server that has the Agent installed.
4. Click **Restore Agent Configurations**.

   NOTE

   If the **Configure** button is unavailable, check whether the one-click configuration function described in the **scenario** is enabled. If it is, the Agent permissions of all servers have been configured by default. In this case, skip the next step.

5. In the displayed **Restore Agent Configurations** dialog box, click **One-Click Restore**.

   If the Agent status changes to **Running**, the Agent has been installed and has started to collect fine-grained metric data.

4.4.4 (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.

This topic takes an ECS as an example. The operations for BMSs are similar.

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 (Agent of the Earlier Version)**.
   - 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. Run the following command to open **conf.json**:

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

   b. Modify the parameters in the file. For details, see **Table 4-2**.

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

Table 4-2 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 ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.

Parameter	Description
ProjectId	(Optional) Specifies the project ID. If you do not configure **ProjectId**, retain **"ProjectId": ""**. If you 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 is located.
AccessKey / SecretKey	To obtain the AK and SK, perform the following operations: Log in to Cloud Eye, click the username in the upper right corner, and choose **My Credentials** > **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.
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 (Agent of the Earlier Version)

1. Log in to an ECS as user **root**.

2. Run the following command to go to the Agent installation path **bin**:
   cd /usr/local/telescope/bin
3. Modify configuration file **conf.json**.
   a. Run the following command to open **conf.json**:
      vi conf.json
   b. Modify the parameters in the file. For details, see **Table 4-3**.
      ECS parameters

Table 4-3 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 ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	(Optional) Specifies the project ID. If you do not configure **ProjectId**, retain **"ProjectId": ""**. If you 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 is located.

Parameter	Description
AccessKey / SecretKey	To obtain the AK and SK, perform the following operations: Log in to Cloud Eye, click the username in the upper right corner, and choose **My Credentials** > **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.
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 4-4**.

Table 4-4 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region to which the ECS or BMS belongs.

NOTE

- After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is 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.

4.5 Installing and Configuring the Agent on a Windows ECS

4.5.1 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. Click **Service List** in the upper left corner. Under **Compute**, select **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.

   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 ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console. 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 4-5**.

Table 4-5 Security group rules

Protocol	Port	Type	Destination	Description
TCP	80	IPv4	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.
TCP and UDP	53	IPv4	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.
TCP	443	IPv4	100.125.0.0/16	Used to collect monitoring data and send the data to Cloud Eye.

4.5.2 Installing and Configuring the Agent on a Windows Server

Scenarios

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

Constraints

The Agent cannot be installed on Windows BMSs.

Windows and Linux OSs 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 (Windows)**.
- Use an administrator account to install the Agent.
- Ensure that the Telescope process is not stopped by other processes after the installation.
- You have obtained the Agent installation package (Windows).

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. Access the directory storing the installation package.
4. Open Windows PowerShell and run the following command to install the plug-in:
   ```
   install_amd64.exe -r eu-west-101 -u 0.1.9 -t 2.7.2 -d agent.ces.myhuaweicloud.eu -o myhuaweicloud.eu
   ```
   Wait for 3 to 5 minutes, locate the server on the **Server Monitoring** page, and check the plug-in status.

   If the Agent status changes to **Running**, the Agent was installed and has started to collect data.

   NOTE

   After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is not reported yet. Wait 3 to 5 minutes and refresh the page.

4.5.3 (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

The Agent cannot be installed on Windows BMSs.

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 (Agent of the Earlier 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 New Version of the Agent)**.

Procedure (for the New Version of the Agent)

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 4-6**.

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


Table 4-6 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.
AccessKey/ SecretKey	To obtain the AK and SK, perform the following operations: Log in to Cloud Eye, click the username in the upper right corner, and choose **My Credentials** > **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.
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 no monitoring data is 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 (Agent of the Earlier 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 4-7**.

Table 4-7 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** > **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 the user be 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.
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.

4.6 Installing the Agents in Batches on Linux ECSs

Scenarios

This topic describes how to install Agents in batches on Linux ECSs.

Operation

After binding an elastic IP address to an ECS, install and configure the Agent by following instructions in **Installing and Configuring the Agent on a Linux ECS or BMS** to ensure that data collection is normal. Use the ECS as a jump server and run scripts in batches to copy, decompress, and install the Agent package and configuration file to other ECSs.

NOTICE

- The ECSs where the Agent is to be installed in batches must belong to the same VPC.
- Agents cannot be installed on Windows servers in batches.

Prerequisites

- The IP addresses and password of user **root** of all ECSs for which the Agent is to be installed have been collected, sorted in the iplist.txt format, and uploaded 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
  ```

Procedure

1. Use PuTTY to log in to the ECS on which the Agent has been installed as user **root**.
2. Run the following command to install the Agent in batches:

   NOTE

   The script supports x86 and Kunpeng Arm-based ECSs.

   ```
   cd /usr/local && curl -k -O https://uniagent-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/package/batch_agent_install.sh && bash batch_agent_install.sh -r eu-west-101 -u 0.1.9 -t 2.7.2 -d agent.ces.myhuaweicloud.eu -o myhuaweicloud.eu
   ```

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 has been installed.

   NOTE

   After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.

4. On the **Server Monitoring** page, select all ECSs and click **Restore Agent Configurations**.
5. On the page that is displayed, click **One-Click Restore**.
6. (Optional) If Pexpect is not required after the installation, run the following commands to delete Pexpect and Ptyprocess from the Python installation directory:

   cd /usr/lib/python2.7/site-packages

   rm pexpect-3.2-py2.7.egg-info -f

   rm ptyprocess-0.5.2-py2.7.egg-info -f

   rm pexpect -rf

   rm ptyprocess -rf

4.7 Managing the Agent

This topic describes how to manage the Agent, including how to view, start, stop, and uninstall the Agent.

4.7.1 Managing the Agent (Linux)

NOTE

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

Viewing the Agent Version

1. Log in to the 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. 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)

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

Restarting the Agent (New Version)

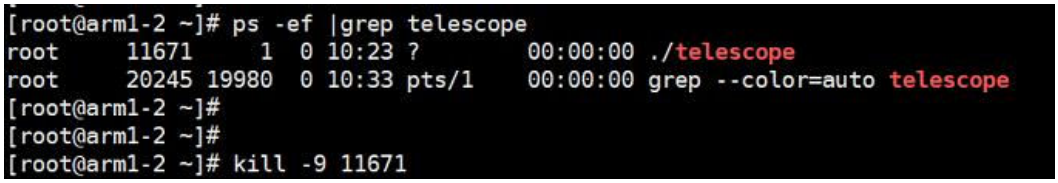
Check the Agent PID.

ps -ef |grep telescope

After the process is forcibly stopped, wait for 3 to 5 minutes for the Agent to automatically restart. **Figure 4-3** shows an operation example.

kill -9 *PID*

Figure 4-3 Restarting the Agent



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)

You can manually uninstall the Agent. After the uninstallation, Cloud Eye does not support monitoring by seconds for ECSs or BMSs. To use the Agent again, reinstall it by referring to **Installing and Configuring the Agent on a Linux ECS or BMS**.

Run the following command to uninstall the Agent:

cd /usr/local/uniagent/script/

./uninstall.sh

NOTICE

Before reinstalling the Agent, manually delete the previous Agent installation package. The installation package of the new version of the Agent is stored in **/usr/local/uniagent_install_amd64.sh**.

Checking the Agent Status (Agent of the Earlier 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 (Agent of the Earlier Version)

/usr/local/telescope/telescoped start

Restarting the Agent (Agent of the Earlier Version)

/usr/local/telescope/telescoped restart

Stopping the Agent (Agent of the Earlier 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. In this case, run the following command to stop the Agent:

/usr/local/telescope/telescoped stop

Uninstalling the Agent (Agent of the Earlier Version)

Run the following command to uninstall the Agent:

/usr/local/telescope/uninstall.sh

NOTICE

You can manually uninstall the Agent. After the uninstallation, Cloud Eye does not support monitoring by seconds (60s by default) for ECSs or BMSs. To use the Agent again, reinstall it by referring to **Installing and Configuring the Agent on a Linux ECS or BMS**. Before reinstalling the Agent, manually delete the previous Agent installation package.

4.7.2 Managing the Agent (Windows)

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

The default installation path of the new version 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.

NOTICE

Before reinstalling the Agent, manually delete the previous Agent installation package.

4.8 Installing the GPU Metrics Collection Plug-in (Linux)

Scenarios

This topic describes how to install the plug-in to collect GPU and RAID metrics.

NOTE

- ECSs support GPU metrics while BMSs do not.
- BMSs support RAID metrics while ECSs do not.
- If the Agent is upgraded to 1.0.5 or later, the corresponding plug-in must use the latest version. Otherwise, the metric collection will fail.

Prerequisites

- The Agent has been installed and is running properly.
- GPU metric collection requires ECSs to support GPU.
- 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 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.

Procedure (New Version)

1. Log in to an ECS as user **root**.

   NOTE

   - To monitor the BMS software RAID metrics, log in to a BMS.
   - The examples in the following procedure are based on the GPU plug-in installation. The installation for the software RAID plug-in is similar.

2. Run the following command to go to the Agent installation path **/usr/local/telescope**:

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

3. Run the following command to create the **plugins** folder:

   mkdir plugins

4. Run the following command to enter the **plugins** folder:

   cd plugins

5. To download the script of the GPU metric collection plug-in, run the following command:

   wget *https://telescope-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/gpu_collector*

   Table 4-8 Obtaining the plug-in installation package

Name	Download Path
Linux 64-bit installation package of the GPU metric collection plug-in	eu-west-101: **https://telescope-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/gpu_collector**

6. Run the following command to add the script execution permissions:

   chmod 755 gpu_collector

7. Run the following command to create the **conf.json** file, add the configuration content, and configure the plug-in path and metric collection period **crontime**, which is measured in seconds:

   vi conf.json

   GPU metric plug-in configuration

```
{
  "plugins": [
    {
      "path": "/usr/local/uniagent/extension/install/telescope/plugins/gpu_collector",
      "crontime": 60
    }
  ]
}
```

   RAID metric plug-in configuration

```
{
  "plugins": [
    {
      "path": "/usr/local/uniagent/extension/install/telescope/plugins/raid_monitor.sh",
      "crontime": 60
    }
  ]
}
```

   NOTE

   - The parameters **gpu_collector** and **raid_monitor.sh** indicate the GPU plug-in and RAID plug-in configuration.
   - The collection period of the plug-in is 60 seconds. If the collection period is incorrectly configured, the metric collection will be abnormal.
   - Do not change the plug-in path without permission. Otherwise, the metric collection will be abnormal.

8. Open the **conf_ces.json** file in the **/usr/local/uniagent/extension/install/telescope/bin** directory. Add **"EnablePlugin": true** to the file to enable the plug-in to collect metric data.

```
{
  "Endpoint": "Region address. Retain the default value.",
  "EnablePlugin": true
}
```


9. Restart the Agent:

   ps -ef | grep telescope | grep -v grep | awk '{print $2}' | xargs kill -9

Procedure (for the Early Version of the Agent)

1. Log in to an ECS as user **root**.

   NOTE

   - To monitor the BMS software RAID metrics, log in to a BMS.
   - The examples in the following procedure are based on the GPU plug-in installation. The installation for the software RAID plug-in is similar.

2. Run the following command to go to the Agent installation path **/usr/local/telescope**:

   cd /usr/local/telescope

3. Run the following command to create the **plugins** folder:

   mkdir plugins

4. Run the following command to enter the **plugins** folder:

   cd plugins

5. To download the script of the GPU metric collection plug-in, run the following command:

   wget *https://telescope-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/gpu_collector*

   Table 4-9 Obtaining the plug-in installation package

Name	Download Path
Linux 64-bit installation package of the GPU metric collection plug-in	eu-west-101: **https://telescope-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/gpu_collector**

6. Run the following command to add the script execution permissions:

   chmod 755 gpu_collector

7. Run the following command to create the **conf.json** file, add the configuration content, and configure the plug-in path and metric collection period **crontime**, which is measured in seconds:

   vi conf.json

   GPU metric plug-in configuration

```
{
  "plugins": [
   {
     "path": "/usr/local/telescope/plugins/gpu_collector",
     "crontime": 60
   }
 ]
}
```

   RAID metric plug-in configuration


```
{
  "plugins": [
    {
      "path": "/usr/local/telescope/plugins/raid_monitor.sh",
      "crontime": 60
    }
  ]
}
```

NOTE

- The parameters **gpu_collector** and **raid_monitor.sh** indicate the GPU plug-in and RAID plug-in configuration.
- The collection period of the plug-in is 60 seconds. If the collection period is incorrectly configured, the metric collection will be abnormal.
- Do not change the plug-in path without permission. Otherwise, the metric collection will be abnormal.

8. Open the **conf_ces.json** file in the **/usr/local/telescope/bin** directory. Add **"EnablePlugin": true** to the file to enable the plug-in to collect metric data.

```
{
   "Endpoint": "Region address. Retain the default value.",
   "EnablePlugin": true
}
```

9. Run the following command to restart the Agent:

   /usr/local/telescope/telescoped restart

4.9 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.

Constraints

The plug-in supports only Linux.

Prerequisites

- You have installed the Cloud Eye Agent. For details, see **Agent Installation and Configuration**.

- The Agent has been restored. For details, see **Restoring the Agent Configurations on a Linux Server**.
- You have obtained the password of user **root** for logging in to the 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 4-11** lists the supported regions.

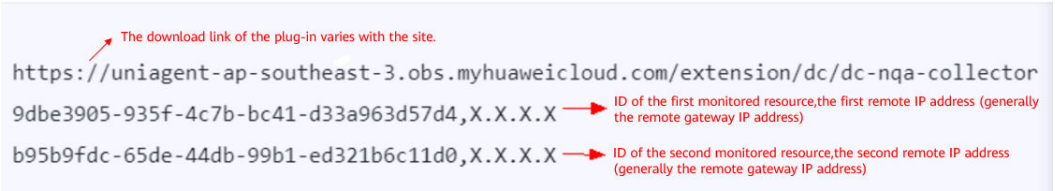
1. Log in to an ECS as user **root**.
2. Run the following command to create the **user.txt** file in the **usr/local/** directory and add user information, including the plug-in download link, monitored resource ID, and remote IP address:

   cd /usr/local/

   vi user.txt

   Figure 4-4 shows the format of the content in the **user.txt** file.

   Figure 4-4 Example of format

   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. For details about the download address of the installation package in each region, see **Table 4-10**.

   b. Information about monitored resources: One resource occupies one line, and consists of a resource ID and a remote IP address. Use a comma (,) to separate the resource ID and remote IP address. To add multiple resources, add lines in the same format.

      - **Resource ID**: The ID must contain 32 characters, including letters and digits, for 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 one remote IP address. You are not allowed to enter multiple IP addresses nor CIDR blocks.
- After the Agent 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 **4**.

Table 4-10 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** AP-Jakarta: **https://uniagent-ap-southeast-4.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** Africa-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** AP-Jakarta: **https://uniagent-ap-southeast-4.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** Africa-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 region*

Table 4-11 One-click installation script of the Direct Connect plug-ins

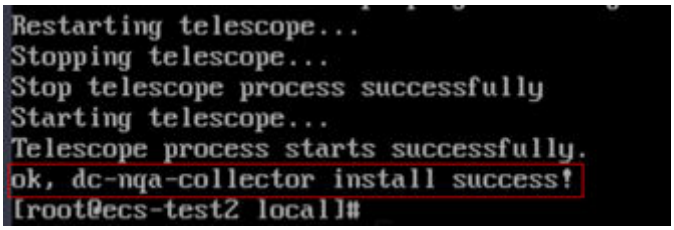
Region	Download Path
CN North-Beijing4	https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN North-Beijing1	https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN East-Shanghai1	https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
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
AP-Jakarta	https://uniagent-ap-southeast-4.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 4-5** is displayed.

   bash dc-installer.sh

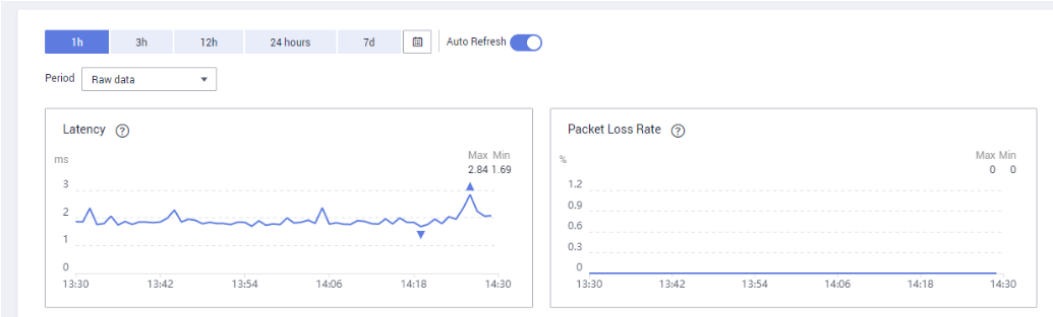
   Figure 4-5 Successful installation



5. Wait for about 1 hour 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 4-6 Network latency and packet loss rate



4.10 Process Monitoring

4.10.1 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 once 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

1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. Perform the following operations based on the resources to be viewed:
   - To check the process monitoring of an ECS, choose **Server Monitoring** > **Elastic Cloud Server**.
   - To check the process monitoring of a BMS, choose **Server Monitoring** > **Bare Metal Server**.
4. On the **Server Monitoring** page, locate the 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 4-12** describes the metrics of system processes.

Table 4-12 System process metrics

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (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 Mode (Linux)	Collection Mode (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 Running Data of Top CPU Processes

- The Agent collects process CPU usages once 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 the process is 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 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 the 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 4-13** lists **Process Monitoring** metrics.

Table 4-13 Process Monitoring metrics

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (Windows)
CPU Usage	Specifies the usage of CPU consumed by a process. **pHashId** (process name and process ID) is the value of **md5**.	0–100 %	Monitored object: ECS or BMS Check the metric value changes in file **/proc/pid/stat**.	Monitored object: ECS or BMS Call Windows API GetProcessTimes to obtain the CPU usage of the process.
Memory Usage	Specifies the memory consumed by a process. **pHashId** (process name and process ID) is the value of **md5**.	0–100 %	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 Invoke Windows API procGlobalMemoryStatusEx to obtain the total memory size. Invoke GetProcessMemoryInfo to obtain the used memory size. Use the used memory size to divide the total memory size to get the memory usage.
Open Files	Specifies 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, select a different value for **Period** to configure the aggregation method.

4.11 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 **Services Interconnected with Cloud Eye**.

Prerequisites

You have installed the Agent. For details, see **Installing and Configuring the Agent on a Linux ECS or BMS** and **Installing and Configuring the Agent on a Windows Server**.

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.
   - 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.
   - 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, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column, and then 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.

   View metric graphs based on raw data from the last 1 hour, last 3 hours, last 12 hours, last 1 day, last 7 days, or last 30 days. Cloud Eye provides the **Auto Refresh** function at 60-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.

4.12 Creating an Alarm Rule to Monitor a Server

Scenarios

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

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

5 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 containing 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**, **1d**, 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 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 3-2** and **Table 3-4**.
6. Click **Create**.

6 Event Monitoring

6.1 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 **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**.

6.2 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 view events in the last 1 hour, last 3 hours, last 12 hours, last 24 hours, last 7 days, or last 30 days. Alternatively, you can set a custom time range to view events triggered within that period.

4. Expand an event and click **View Event** in the **Operation** column to view its details.
5. In the row containing the target event, click **View Graph** in the **Operation** column. Then, you can view the monitoring data of last 24 hours.

   You can view monitoring data of a specified event in the last 1 hour, last 3 hours, last 12 hours, last 24 hours, last 7 days, or last 30 days. Alternatively, you can set a custom time range by specifying the start time and end time to view monitoring data of a specified event within that period.
6. In the upper right corner of the event list, select an event type and enter an event name to filter the desired event.
7. To view events of a specific time period, click the corresponding bar chart.

6.3 Creating an Alarm Rule to Monitor an Event

Scenarios

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

6.4 Events Supported by Event Monitoring

Table 6-1 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	Restart triggered due to system faults	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restart completed due to system faults	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None
	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 caused by system faults	VMFaultsByHostProcessExceptions	Critical	The host where the ECS resides is faulty. The system will automatically try to start the ECS.	After the ECS is started, check whether this ECS and services on it can run properly.	The ECS is faulty.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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
	Scheduled specification modification failed	instance_resize_faile d	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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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
	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 6-2 Bare Metal Server (BMS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	SYS.BMS	ECC uncorrectable error alarm generated on GPU SRAM	SRAM UncorrectableEccError	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	Namespace	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	storageError	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	Namespace	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	Namespace	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	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		ECC alarm generated on GPU Ant1	gpuAnt1EccAlarm	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	Namespace	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	Namespace	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	Namespace	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	Namespace	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	Namespace	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	Namespace	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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		System maintenance canceled	system_maintenance_canceled	Major	The scheduled BMS maintenance is canceled.	None	None
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 6-3 Elastic IP (EIP)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	SYS.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	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	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes)		
		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.
		EIP unblocked	unblockEIP	Critical	The EIP was unblocked.	Use the previous EIP again.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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	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	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes)		

Table 6-4 Advanced Anti-DDoS (AAD)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	SYS.DDOS	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		IP address scheduling triggered	ipDispatchEvents	Major	IP route changed	Check the workloads of the IP address.	Services are not affected.

Table 6-5 Advanced Anti-DDoS (AAD)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	SYS.DDOS	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		IP address scheduling triggered	ipDispatchEvents	Major	IP route changed	Check the workloads of the IP address.	Services are not affected.

Table 6-6 Elastic Load Balance (ELB)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
ELB	SYS.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 6-7 Cloud Backup and Recovery (CBR)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CBR	SYS.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.
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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 6-8 Relational Database Service (RDS) — operations

Event Source	Name space	Event Name	Event ID	Event Severity	Description
RDS	SYS.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 6-9 Document Database Service (DDS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	SYS.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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Data disk expanded and being writable	DDS DataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No further action is required.	No adverse 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 6-10 GaussDB NoSQL

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB NoSQL	SYS.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	Namespace	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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		HotKey occurred	HotKeyOccurs	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BigKey occurred	BigKeyOccurs	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.
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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 6-11 GaussDB(for MySQL)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for MySQL)	SYS.GAUSSDB	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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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.	Back up 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	Namespace	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.	Back up jobs fail.

Event Source	Namespace	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	Namespace	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	Namespace	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 6-12 GaussDB

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	SYS.GAUSSDBV5	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	Namespace	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	Namespace	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	Namespace	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		Failed to upgrade the hot patch	GaussDBV5UpgradeHotfixFailed	Major	Generally, this fault is caused by an error reported during kernel upgrade.	View the error information about the workflow and redo or skip the job.	None

Table 6-13 Distributed Database Middleware (DDM)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDM	SYS.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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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 whether • The username and password of the DB instance are correct. • The security groups associated with the DDM instance and underlying database instance are correctly configured.	Services cannot run properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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 6-14 Cloud Phone Server

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	SYS.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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	Namespace	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	Namespace	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		SCSI error	scsiError	Critical	The kernel log indicated SCSI Error.	Submit a service ticket.	Services are interrupted.
		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 /.shared path/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 6-15 Layer 2 Connection Gateway (L2CG)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	SYS.ESW	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 6-16 Elastic IP and bandwidth

Event Source	Namespace	Event Name	Event ID	Event Severity
Elastic IP and bandwidth	SYS.VPC	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 6-17 Elastic Volume Service (EVS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
EVS	SYS.EVS	Update disk	updateVolume	Minor	Update the name and description of an EVS disk.	No further action is required.	None
		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 6-18 Identity and Access Management (IAM)

Event Source	Namespace	Event Name	Event ID	Event Severity
IAM	SYS.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
		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 6-19 Key Management Service (KMS)

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

Table 6-20 Object Storage Service (OBS)

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

Table 6-21 Cloud Eye

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution
Cloud Eye	SYS.CES	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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution
						into the corresponding **hosts** file. • 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	agentFaulty	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	Namespace	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 6-22 Enterprise Switch

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
Enterprise Switch	SYS.ESW	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 6-23 Cloud Secret Management Service (CSMS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CSMS	SYS.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 6-24 Distributed Cache Service (DCS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DCS	SYS.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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 will be 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	Namespace	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance backup failure	instanceBackupFailure	Major	The DCS instance fails to be backed up due to an OBS access failure.	Retry backup manually.	Automated backup fails.
		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 will be 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 will be interrupted.

Table 6-25 Intelligent Cloud Access (ICA)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
ICA	SYS.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	Namespace	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 6-26 Cloud Storage Gateway (CSG)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description
CSG	SYS.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	Name space	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 6-27 Enterprise connection

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
EC	SYS.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.
		BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 6-28 Cloud Certificate Manager (CCM)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CCM	SYS.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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

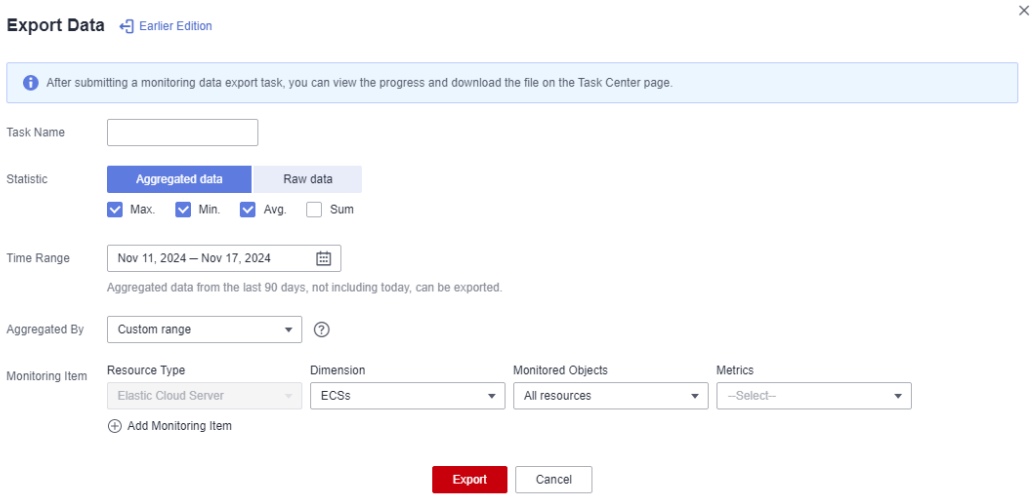
7 Task Center

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** (**Elastic Cloud Server**) 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.

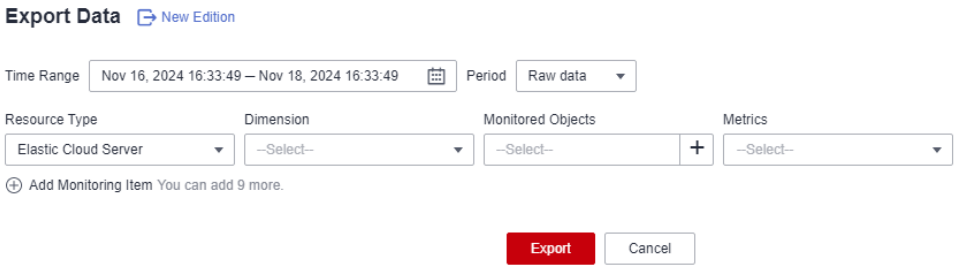
Figure 7-1 Export Data



NOTE

By default, the page of the new edition is displayed. To return to the earlier edition, 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 7-2 Earlier edition of the **Export Data** page



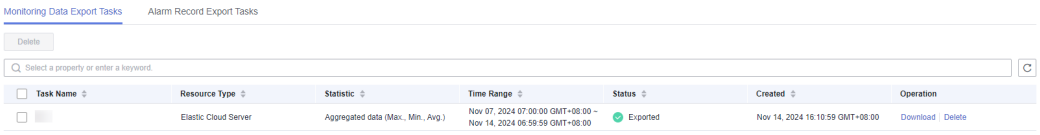
5. On the **Export Data** page, set parameters as prompted.

Table 7-1 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 . 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.

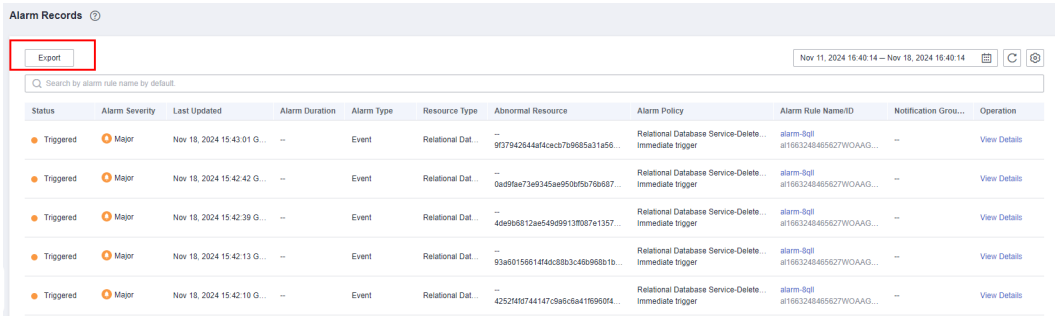
Figure 7-3 Viewing export tasks



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**.

Figure 7-4 Alarm Records page



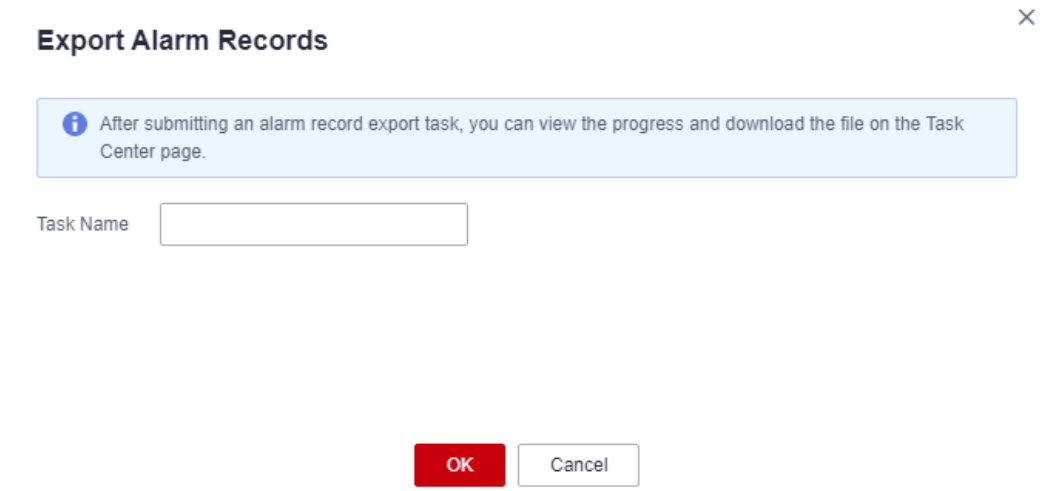
NOTE

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.

Figure 7-5 Entering an export task name



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.

8 Data Dump

8.1 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 a maximum of 20 data dump tasks.

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. On the **Add Dump Task** page, configure parameters by referring to **Table 8-1**.

Table 8-1 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 for monitored services. • If you select **All**, all monitored objects of the selected resource type will be dumped to Kafka. • If you select a specific dimension, only 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**.
Project Name	Specifies the project of the resource.
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**.

8.2 Modifying, Deleting, Enabling, or Disabling Dump Tasks

Scenarios

This topic describes how to modify, disable, enable, or delete a dump task.

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. Locate a dump task and click **Modify** in the **Operation** column.

   The **Modify Dump Task** page is displayed.
5. Modify the task settings.
6. Click **Modify**.

Disabling Dump Tasks

> **CAUTION**
>
> After you disable a dump task, collected monitoring data will not be dumped but existing data is still saved.

- Disabling a single dump task: On the **Data Dump** page, locate the dump task and click **Disable** in the **Operation** column. In the displayed **Disable Dump Task** dialog box, click **Yes**.
- Batch disabling dump tasks: On the **Data Dump** page, select the check boxes in front of the data dump tasks to be disabled and click **Disable** above the list. In the displayed **Disable Dump Task** dialog box, click **Yes**.

Enabling Dump Tasks

> **CAUTION**
>
> After you enable the dump task, collected monitoring data will be dumped.

- Enabling a single dump task: On the **Data Dump** page, locate a dump task whose status is **Disabled** and click **Enable** in the **Operation** column. In the displayed **Enable Dump Task** dialog box, click **Yes**.
- Batch enabling dump tasks: On the **Data Dump** page, select the check boxes in front of the data dump tasks to be enabled and click **Enable** above the list. In the displayed **Enable Dump Task** dialog box, click **Yes**.

Deleting a Dump Task

> **CAUTION**
>
> After you delete a dump task, collected monitoring data will not be dumped but existing data is still saved.

Locate the dump task and click **Delete** in the **Operation** column. In the displayed **Delete Data Dump** dialog box, click **Yes**.

9 Cloud Service Monitoring

9.1 Introduction to Cloud Service Monitoring

Scenarios

Cloud Service Monitoring collects data of built-in metrics of cloud services. You can monitor these metrics to track the status of corresponding cloud services. On the **Cloud Service Monitoring** page, in addition to viewing monitoring data, you can also create alarm rules and export raw data.

What You Can Do with Cloud Service Monitoring

- Viewing metrics: You can view the graphs of raw data collected in the last 1 hour, 3 hours, 12 hours, 1 day, and 7 days. You can customize the metrics to be viewed and view monitoring data that is automatically refreshed.
- Creating alarm rules: You can create alarm rules for key metrics of cloud services. When the conditions in the alarm rule are met, Cloud Eye sends emails or HTTP/HTTPS requests, enabling you to quickly respond to resource changes.
- Exporting monitoring data: Cloud Service Monitoring allows you to export a maximum of 10 monitoring items in your selected time range and aggregation period. The exported monitoring report contains the username, region name, service name, instance name, instance ID, metric name, metric data, time, and timestamp, facilitating query and filtering.

9.2 Viewing Metrics

1. Log in to the management console.
2. Click **Service List** in the upper left corner and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring** and select the cloud service whose resources you want to view.
4. Locate the cloud service resource and click **View Metric** in the **Operation** column.

NOTE

- You can sort graphs by dragging them based on service requirements.
- If **Auto Refresh** is enabled, data is automatically refreshed every minute.
- Some cloud services allow you to view resource details. You can click **View Resource Details** in the upper part of the page to view details about monitored resources.
- You can search for a specific metric in the search box.
- For details about how to export monitoring data, see **How Can I Export Collected Data?**

5. Near the top right corner of the page, click **Select Metric**.

   The **Select Metric** dialog box is displayed.

   Select at least one metric. Drag and drop the selected metrics at desired locations to sort them. This helps you customize metrics to be viewed.

6. Hover your mouse over a graph. In the upper right corner, click  to view monitoring details on an enlarged graph. Select a time period or customize a time range to view the metric in a specific monitoring interval.

   NOTE

   - If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. You can set **Period** and **Statistic** to change the aggregation period of monitoring data. For details about aggregation periods, see
   - If you select **7d** or **30d**, aggregated data is displayed by default. You can set **Period** and **Statistic** to change the aggregation period of monitoring data.

7. In the upper right corner of the monitoring graph, click  to create alarm rules for the metric. For details about the parameters, see **Creating an Alarm Rule**.

10 Permissions Management

10.1 Creating a User and Granting Permissions

You can use **IAM** for fine-grained permissions control for your Cloud Eye resources. With IAM, you can:

- 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 an account of Huawei Cloud or a 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 10-1**).

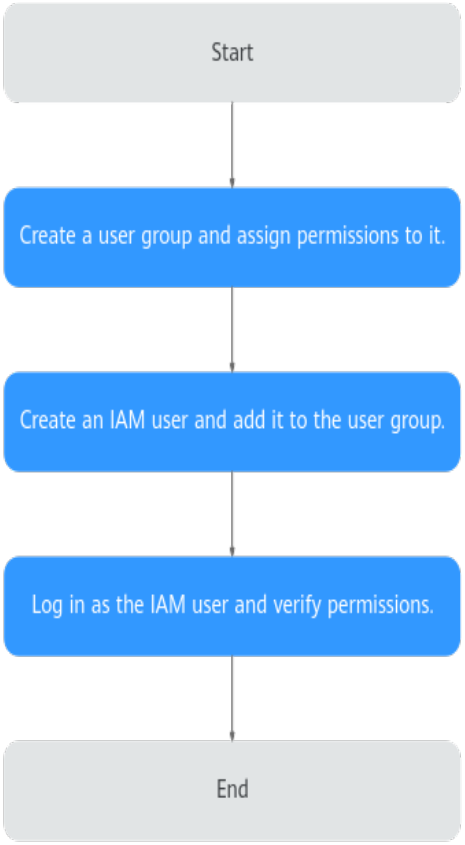
Prerequisites

You have learned about the system policies of Cloud Eye before assigning the preset Cloud Eye permissions to user groups (if needed). To grant custom permissions to a user group, ensure that you have **created a custom Cloud Eye policy**.

For details about the system policies supported by Cloud Eye and comparison between these policies, see **Permissions Management**. For the permissions of other services, see **System Permissions**.

Process Flow

Figure 10-1 Process for granting Cloud Eye permissions



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 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 has the **CES Administrator** permissions. After you log in to the Cloud Eye console and use related functions, if no authentication failure message is displayed, the authorization is successful.

10.2 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 in **Permissions Policies and Supported Actions** in *Cloud Eye API Reference*.

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 create, modify, query, and delete 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:create",
                "ces:alarms:put",
                "ces:alarms:list",
                "ces:alarms:delete"
            ],
            "Effect": "Allow"
        }
    ]
}
```


11 Quota Adjustment

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS 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.
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.

12 Services Interconnected with Cloud Eye

Category	Service	Namespace	Dimension
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECS ID
	ECS (OS monitoring)	AGT.ECS	Key: instance_id Value: ECS ID
	Bare Metal Server	SERVICE.BMS	Key: instance_id Value: BMS ID
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: auto scaling group ID
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.)
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name
	Scalable File Service	SYS.SFS	Key: share_id Value: file system name
	SFS Turbo	SYS.EFS	Key: efs_instance_id Value: instance
Network	Elastic IP and bandwidth	SYS.VPC	• Key: publicip_id Value: EIP ID • Key: bandwidth_id Value: bandwidth ID

Category	Service	Namespace	Dimension
	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
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID
	Virtual Private Network	SYS.VPN	Key: connection_id Value: VPN connection
	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
	Direct Connect	SYS.DCAAS	• Key: direct_connect_id Value: connection • Key: history_direct_connect_id Value: historical connection
	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
Middleware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.

Category	Service	Namespace	Dimension
	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
Database	Relational Database Service	SYS.RDS	For details, see the information in the right column.
	Document Database Service	SYS.DDS	• Key: mongodb_node_id Value: DDS node ID • Key: mongodb_instance_id Value: DDS DB instance ID
	GaussDB	SYS.NoSQL	For details, see the information in the right column.

Category	Service	Namespace	Dimension
	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	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
Enterprise Intelligence	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster
	ModelArts	SYS.ModelArts	• Key: service_id Value: real-time service ID • Key: model_id Value: model ID
	Data Lake Insight	SYS.DLI	• Key: queue_id Value: queue instance • Key: flink_job_id Value: Flink job

Category	Service	Namespace	Dimension
Security	Web Application Firewall	SYS.WAF	• Key: instance_id Value: dedicated WAF instance • Key: waf_instance_id Value: cloud WAF instance
	Database Security Service	SYS.DBSS	Key: audit_id Value: instance

A Change History

Released On	Description
2022-09-30	This issue is the first official release.

