

Cloud Eye

User Guide

Issue 01
Date 2025-12-02



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Overview.....	1
2 Permissions Management.....	3
2.1 Creating a User and Granting Permissions.....	3
2.2 Cloud Eye Custom Policies.....	5
3 Cloud Resource Monitoring.....	7
3.1 Resource Groups.....	7
3.1.1 Overview.....	7
3.1.2 Creating a Resource Group.....	7
3.1.3 Viewing Resource Groups.....	14
3.1.3.1 Resource Group List.....	15
3.1.3.2 Resource Overview.....	16
3.1.3.3 Alarm Rules.....	16
3.1.4 Managing Resource Groups.....	17
3.1.4.1 Modifying a Resource Group.....	17
3.1.4.2 Deleting a Resource Group.....	17
3.1.4.3 Associating a Resource Group with an Alarm Template.....	17
3.1.5 Cloud Services Supported by Resource Groups.....	18
3.2 Server Monitoring.....	25
3.2.1 Overview.....	25
3.2.2 Cloud Eye Plug-in (Agent).....	27
3.2.2.1 Installing and Configuring the Agent.....	28
3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure.....	29
3.2.2.3 Installing the Agent.....	30
3.2.2.3.1 Installing the Agent on a Linux Server.....	30
3.2.2.3.2 Installing the Agent on a Windows Server.....	32
3.2.2.4 Installing and Configuring the Agent.....	33
3.2.2.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux).....	33
3.2.2.4.2 Modifying the DNS Server Address and Adding Security Group Rules (Windows).....	36
3.2.2.4.3 (Optional) Manually Configuring the Agent (Linux).....	38
3.2.2.4.4 (Optional) Manually Configuring the Agent on a Windows Server.....	43
3.2.2.5 Managing the Agent.....	47
3.2.2.6 Installing Other Monitoring Plug-ins.....	51

3.2.2.6.1 Installing Direct Connect Metric Collection Plug-ins.....	51
3.2.2.7 Upgrading the Agent.....	60
3.2.2.7.1 Upgrading the Agent on a Linux Server.....	60
3.2.2.7.2 Upgrading the Agent on a Windows Server.....	61
3.2.2.8 Agent Features per Version.....	61
3.2.3 Viewing Server Monitoring Metrics.....	64
3.2.4 Process Monitoring.....	65
3.2.5 Creating an Alarm Rule to Monitor a Server.....	76
3.2.6 Viewing Resource Details.....	79
3.3 Cloud Service Monitoring.....	80
3.3.1 Overview.....	80
3.3.2 Viewing a Cloud Service Dashboard.....	80
3.3.3 Viewing Raw Data.....	82
3.3.4 Cloud Services Displayed in the Cloud Service Monitoring List.....	83
3.4 Task Center.....	83
4 My Dashboards	89
4.1 Overview.....	89
4.2 Creating a Dashboard.....	89
4.3 Adding a Graph.....	90
4.4 Viewing a Graph.....	91
4.5 Configuring a Graph.....	94
4.6 Deleting a Graph.....	96
4.7 Deleting a Dashboard.....	96
5 Alarm Management.....	98
5.1 Overview.....	98
5.2 Alarm Rules.....	98
5.2.1 Overview.....	98
5.2.2 Creating an Alarm Rule and Notifications.....	99
5.2.3 Alarm Policies.....	106
5.2.4 Modifying an Alarm Rule.....	110
5.2.5 Disabling Alarm Rules.....	110
5.2.6 Enabling Alarm Rules.....	111
5.2.7 Deleting Alarm Rules.....	111
5.2.8 Exporting Alarm Rules.....	112
5.2.9 Filtering Alarm Rules.....	112
5.3 Alarm Records.....	112
5.3.1 Viewing Alarm Records.....	112
5.3.2 Forcibly Clearing an Alarm.....	113
5.4 Alarm Templates.....	114
5.4.1 Overview.....	114
5.4.2 Viewing Alarm Templates.....	114
5.4.3 Creating a Custom Metric or Event Template.....	115

5.4.4 Modifying a Custom Metric or Event Template.....	116
5.4.5 Deleting a Custom Metric or Event Template.....	116
5.4.6 Copying a Custom Metric or Event Template.....	117
5.4.7 Associating a Custom Metric Template with a Resource Group.....	117
5.4.8 Importing and Exporting Custom Metric or Event Templates.....	120
5.5 Alarm Notifications.....	120
5.5.1 Creating Alarm Notification Topics.....	120
5.5.1.1 Creating a Topic.....	120
5.5.1.2 Adding Subscriptions.....	122
5.6 One-Click Monitoring.....	122
5.7 Alarm Masking.....	126
5.7.1 Introduction.....	126
5.7.2 Creating a Masking Rule.....	126
5.7.3 Modify a Masking Rule.....	129
5.7.4 Deleting a Masking Rule.....	131
5.7.5 Masking an Alarm Rule.....	132
6 Event Monitoring.....	133
6.1 Overview.....	133
6.2 Viewing Events.....	134
6.3 Creating an Alarm Rule and Notification for Event Monitoring.....	134
6.4 Events Supported by Event Monitoring.....	138
7 Access Center.....	309
7.1 Custom Monitoring.....	309
8 Data Dump.....	311
8.1 Overview.....	311
8.2 Dumping Data.....	311
8.3 Modifying, Deleting, Enabling, or Disabling a Dump Task.....	313
9 Quotas.....	315
10 Cloud Product Metrics.....	316

1 Overview

Overview concludes **Resource Monitoring**. You can learn about resource alarms of each cloud service in real time.

Constraints

The **Overview** page aggregates data from all resources. When you enable enterprise project authorization, it also includes data that is not managed by the current enterprise project. If you want to view a specific resource, a message will be displayed indicating insufficient permissions.

Viewing Cloud Service Resource Monitoring

Resource Monitoring displays real-time alarms of each resource group and cloud service. You can view resource alarms in different dimensions to efficiently manage resources. The following describes how you can use **Resource Monitoring**.

1. Log in to the [Cloud Eye console](#).
2. Choose **Overview**.
3. On the upper left corner of the **Overview** page, view the total number of resources and identify how many of them have active alarms.
4. On the left of **Resource Monitoring**, view the health score of all resources, total number of resources, total number of resources with active alarms, as well as the number of resources at different alarm severities.

NOTE

- Health score = (Number of resources without alarms/Total number of resources) x 100 (rounded down to an integer)
 - The new overview page uses a different statistical method than the old one. This means the total resource count and the number of resources with active alarms may differ between the two pages. Since the data statistics API on the old overview page is no longer updated, data on the new page is used.
5. Select a cloud service and view its resource distribution. Alternatively, click a resource group to view its resources.
 6. Click a service resource to view its alarm details in the right pane.

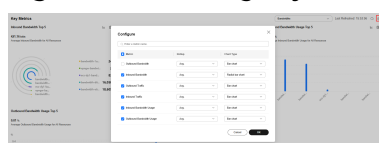
- a. Click an instance name to go to the **Alarm Records** page. Filter all active alarm records by resource ID and resource type.
- b. Click  next to an instance name to view all of its alarm records and alarm policies.
- c. Click **View Details** on the right of an alarm policy. On the **Alarm Records** page, filter the active alarm records that meet the selected alarm policy by alarm severity, alarm rule ID, resource ID, and resource type.

Querying Key Metrics of a Cloud Service

In the lower part of the **Resource Monitoring** page, you can view the top 5 key metrics for your service and the average values of all instances in the current dimension.

1. Log in to the [Cloud Eye console](#).
1. Choose **Overview**.
2. In the upper right corner of the **Key Metrics** area, select a resource dimension from the drop-down list to display resource details or select another resource to view its monitoring details.

Figure 1-1 Viewing key metrics



3. Click  in the upper right corner of a key metric to select another metric as needed. Configure the aggregation method and chart type for the metric as needed.
The aggregation method can be **Max**, **Min**, **Avg**, or **Sum**. The graph type can be **Bar chart**, **Horizontal bar chart**, **Radial bar chart**, or **Polar bar chart**.
4. Click  in the upper right corner of the graph. In the displayed dialog box, click **OK** to delete the displayed metrics.

2 Permissions Management

[2.1 Creating a User and Granting Permissions](#)

[2.2 Cloud Eye Custom Policies](#)

2.1 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 only the minimum permissions required for users to perform a given task.
- 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 2-1](#)).

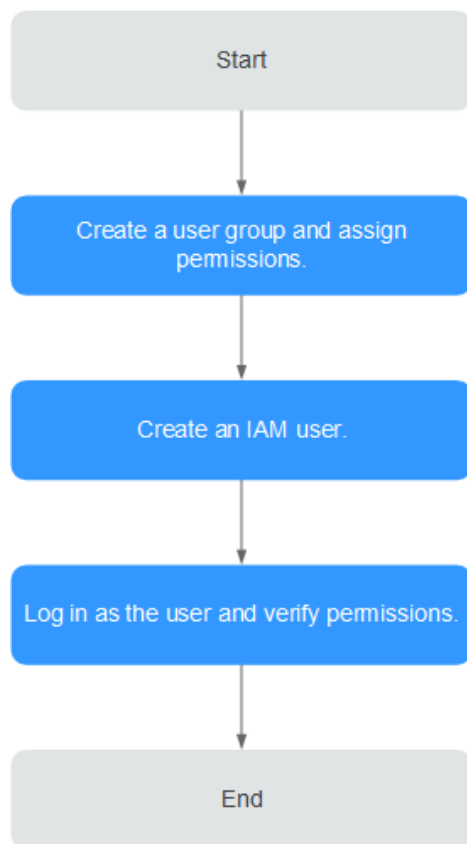
Prerequisites

Before assigning permissions to a user group, you need to understand the Cloud Eye system policies that can be added to the user group and select a policy as required.

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

Process Flow

Figure 2-1 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 the permissions to take effect for all regions, assign them in all these regions. The global permission does not take effect.
- The preceding permissions are all Cloud Eye permissions. For more refined Cloud Eye permissions, see [Permissions Management](#).

2. **Create an IAM user.**

Create a user on the IAM console and add it to the group created in [1](#).

3. **Log in as the IAM user** and verify permissions.

After you log in to the [Cloud Eye management console](#) as the created user, verify that the user has the **CES Administrator** permissions. If no authentication failure message is displayed, the authorization is successful.

2.2 Cloud Eye Custom Policies

Custom policies can be created to supplement the system-defined policies of Cloud Eye. For the actions that can be added to custom policies, see [Permissions Policies and Supported Actions](#).

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). This topic contains examples of common Cloud Eye custom policies.

Example Custom Policies

- Example 1: Granting permissions to modify an alarm rule

```
{
  "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 together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **CES FullAccess** policy to a user but you want to prevent the user from deleting alarm rules. Create a custom policy for denying alarm rule deletion, and attach both policies to the group the user belongs. Then the user can perform all operations on alarm rules except deleting alarm rules. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "ces:alarms:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- Example 3: Allowing users to have all operation permissions on alarm rules, including creating, modifying, querying, and deleting alarm rules

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is a policy with multiple actions:

```
{
  "Version": "1.1",
  "Statement": [
```

```
{
  "Action": [
    "ces:alarms:put",
    "ces:alarms:create",
    "ces:alarms:list",
    "ces:alarms:delete"
  ],
  "Effect": "Allow"
}
```

3 Cloud Resource Monitoring

[3.1 Resource Groups](#)

[3.2 Server Monitoring](#)

[3.3 Cloud Service Monitoring](#)

[3.4 Task Center](#)

3.1 Resource Groups

3.1.1 Overview

A resource group allows you to add and manage related resources and provides a collective health status for all resources in the group.

If you use multiple cloud services, you can add all related resources, such as cloud servers, EVS disks, elastic IP addresses, bandwidths, and databases to the same resource group. You can manage alarm rules and view monitored data by resource group. This greatly simplifies O&M.

Resource Groups supports enterprise projects. If a resource group is associated with an enterprise project, only users who have the permission of the enterprise project can view and manage the resource group.

3.1.2 Creating a Resource Group

If you use multiple types of cloud services, you can add all related resources, such as ECSs, BMSs, EVS disks, EIPs, bandwidths, and databases to the same resource group for easier management and O&M.

Constraints

- You can create up to 1,000 resource groups.
- Each resource group can contain 1 to 10,000 cloud service resources.
- You can add limited number of resources of different types to a resource group. For details, see the tips on the Cloud Eye console.

- After a resource group is created, it takes about three hours for the new resource group rule to be applied.

Creating a Resource Group

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. In the upper right corner, click **Create Resource Group**.
4. On the **Create Resource Group** page, enter a group name. Select the way you want to add a resource and define resource matching rule as required.

Creating a Resource Group by Matching Resources by Instance Name

1. Select **Automatically** for **Add Resources**.
2. Select **Instance name** for **Match Resources By** and set other parameters based on [Table 3-1](#).

Table 3-1 Parameters for adding resources by instance name

Parameter	Description	Example Value
Cloud Product	Select the cloud product where the instance is located and configure resource matching rules. You can select one or more cloud products. For each product, you can add up to 50 combination conditions. You can select any or all combination conditions. The relationship between different cloud products is OR. You can select Equal , All , Include , Prefix , Suffix , or Not include . If All is selected, all instances of the cloud product are selected, and you do not need to enter an instance name. The instance name can contain a maximum of 128 characters, including only letters, digits, underscores (_), periods (.), and hyphens (-).	Elastic Cloud Server - ECSs Add to the resource group when any combined condition is met Instance Name Equal test1
Enterprise Project	Enterprise project that the resource group belongs to.	default

3. (Optional) After the basic configuration is complete, select whether to associate the custom metric alarm template in the **Advanced Settings** area. For parameter details, see [\(Optional\) Advanced Configurations](#).
4. Click **Create**.

Creating a Resource Group by Matching Resources by Enterprise Project

1. Select **Automatically** for **Add Resources**.
2. Select **Enterprise project** for **Match Resources By** and set other parameters based on [Table 3-2](#).

After you select an enterprise project, resources in the resource group will be automatically kept consistent with the resources in the enterprise project. To manage resources in this resource group, you can only add or remove resources to and from the enterprise project.

Table 3-2 Parameters for matching resources by enterprise project

Parameter	Description	Example Value
Resource Level	Resource level of the monitored object. You can select Cloud product or Specific dimension . If you select Cloud product for Resource Level , select a cloud product. If Resource Level is set to Specific dimension , all available resources in the selected dimensions will be automatically added to this resource group. For details, click View monitored dimensions .	Cloud product
Cloud Product	If you select Cloud service for Resource Level , you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If Cloud Product is set to All , all cloud products that are interconnected with Cloud Eye will be selected.	All
Enterprise Project	Enterprise project for matching resources. You can select multiple enterprise projects.	default
Enterprise Project	Enterprise project that the resource group belongs to.	default

3. (Optional) After the basic configuration is complete, select whether to associate the custom metric alarm template in the **Advanced Settings** area. For parameter details, see [\(Optional\) Advanced Configurations](#).
4. Click **Create**.

Creating a Resource Group by Matching Resources by Tag

1. Select **Automatically** for **Add Resources**.
2. Select **Tag** for **Match Resources By** and set other parameters based on [Table 3-3](#).

Table 3-3 Parameters for matching resources by tag

Parameter	Description	Example Value
Resource Level	Resource level of the monitored object. You can select Cloud product or Specific dimension . If you select Cloud product for Resource Level , select a cloud product. If Resource Level is set to Specific dimension , all available resources in the selected dimensions will be automatically added to this resource group. For details, click View monitored dimensions .	Cloud product
Cloud Product	If you select Cloud service for Resource Level , you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If Cloud Product is set to All , all cloud products that are interconnected with Cloud Eye will be selected. For details, see 3.1.5 Cloud Services Supported by Resource Groups .	All

Parameter	Description	Example Value
Matching Rule	Matching rule of the tag. You can add up to 50 tags. Each tag is a key-value pair. You can tag cloud resources to easily categorize and search for them. - Resource tag key: A tag key cannot start or end with a space, or start with _sys_. It can contain a maximum of 128 characters and contain letters, digits, spaces, and the following special characters: _.:=-+@ - Resource tag value: A resource tag value consists of the matching method and value. The matching method can be set to Equal, All, Include, Prefix, Suffix, or Not include. The value can contain a maximum of 255 characters and contain letters, digits, spaces, and the following special characters: _.:=-+@ NOTE If you enter multiple tags, the relationship between different keys is AND, and the relationship between values of the same key is OR.	Usage Equal to Project1
Enterprise Project	Enterprise project that the resource group belongs to.	default

- (Optional) After the basic configuration is complete, select whether to associate the custom metric alarm template in the **Advanced Settings** area. For parameter details, see [\(Optional\) Advanced Configurations](#).
- Click **Create**.

Creating a Resource Group by Matching Resources by Multiple Criteria

- Select **Automatically** for **Add Resources**.
- Select **Multiple criteria** for **Match Resources By** and set other parameters based on [Table 3-4](#).

Table 3-4 Parameters for matching resources by multiple criteria

Parameter	Description	Example Value
Resource Level	Resource level of the monitored object. You can select Cloud product or Specific dimension . If you select Cloud product for Resource Level , select a cloud product. If Resource Level is set to Specific dimension , all available resources in the selected dimensions will be automatically added to this resource group. For details, click View monitored dimensions .	Cloud product
Cloud Product	If you select Cloud service for Resource Level , you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If Cloud Product is set to All , all cloud products that are interconnected with Cloud Eye will be selected.	All
Multi-Criteria Match	Combination method for matching resources by multiple criteria. After selecting a combination method, you need to configure the matching rule. For details, see Table 3-1 to Table 3-3 . You can add up to 50 combinations. If Resource Level is set to Cloud product , you can select at least two matching criteria from Enterprise project , Tag , and Instance name . If Resource Level is set to Specific dimension , Enterprise project and Tag are selected by default and cannot be changed. NOTE The relationship between different combinations is OR. The relationship between different matching rules in the same combination is AND.	Enterprise project and Tag
Enterprise Project	Enterprise project that the resource group belongs to.	default

3. (Optional) After the basic configuration is complete, select whether to associate the custom metric alarm template in the **Advanced Settings** area. For parameter details, see [\(Optional\) Advanced Configurations](#).
4. Click **Create**.

Creating a Resource Group by Adding Resources Manually

1. Select **Manually** for **Add Resources** and set other parameters based on [Table 3-5](#).

Table 3-5 Parameters for adding resources manually

Parameter	Description	Example Value
Resource Level	Resource level of the monitored object. You can select Cloud product or Specific dimension. If you select Cloud product for Resource Level, select a cloud product and desired resources. If you select Specific dimension for Resource Level, manually select resources to be added to the resource group. CAUTION If you created a resource group with Add Resources set to Manually, and then release resources in the resource group, some cloud services do not support automatic deletion of these resources in that group. Such services include: • GaussDB • GeminiDB • Relational Database Service • Other cloud services that do not support creating a resource group whose resources are added automatically. For details about these cloud services, see 3.1.5 Cloud Services Supported by Resource Groups.	Cloud product
Cloud Product	If you select Cloud product for Resource Level , you need to select the cloud product that the instance belongs to and specify resources. You can select one or more cloud products.	Elastic Cloud Server - ECSs
Enterprise Project	Enterprise project that the resource group belongs to.	default

2. (Optional) After the basic configuration is complete, select whether to associate the custom metric alarm template in the **Advanced Settings** area. For parameter details, see [\(Optional\) Advanced Configurations](#).
3. Click **Create**.

(Optional) Advanced Configurations

You can configure whether to associate an alarm template and send alarm notifications when creating a resource group or afterward. This streamlines alarm rules management and simplifies alarm rule configuration. For details, see .

Step 1 In the **Advanced Settings** area, select the template to be associated.

Step 2 Configure alarm notifications.

Table 3-6 Configuring alarm notifications

Parameter	Description
Alarm Notifications	Whether to send alarm notifications by SMS, email, HTTP, or HTTPS. This parameter is enabled by default.
Recipient	Target recipient of alarm notifications. You can select the account contact or a topic. This parameter is available only if Notified By is set to Topic subscriptions. If there is a display name of a topic, the format is <i>Topic name (Display name)</i>, and you can search for a topic by name or display name. If no display name is set for a topic, only the topic name will be displayed. • The account contact is the mobile number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If there is no topic you need, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.
Notification Window	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If you set Notification Window to 08:00 to 20:00, Cloud Eye only sends notifications within this period.
Time Zone	Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured.
Trigger Condition	Condition that will trigger an alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.

----End

3.1.3 Viewing Resource Groups

3.1.3.1 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 [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.

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

Table 3-7 Parameters of the resource group list

Parameter	Description
Name/ID	Resource group name and ID. NOTE The group name can contain a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
Status (Metric Monitoring)	• No alarm: No alarm resource exists in the group. • In alarm: An alarm is being generated for a resource in the group. • No alarm rules set: No alarm rules have been created for any resource in the group.
Status (Event Monitoring)	• OK: No events have been triggered for the resource group. • Triggered: One or more events have been triggered for the resource group. • No alarm rules set: No alarm rules have been created for any resource in the group.
Resources (Alarm/Triggered/Total)	Total number of resources with active alarms, resources with triggered alarms, and the total number of resources in the resource group.
Resource Types	Number of resource types in a resource group. For example, if there are two ECSs and one EVS disk in a resource group, Resource Types is 2 .
Enterprise Project	Name of the enterprise project that has the resource group permissions.
Add Resources	Method for adding resources when you create a resource group. The value can be Manually or Automatically .
Match Resources By	When you select Automatically for Add Resources , resources can be matched by instance name, enterprise project, tag, or multiple criteria.

Parameter	Description
Resource Level	Resource level, which can be Cloud product or Specific dimension .
Associated Alarm Template	Alarm template associated with the resource group. You can associate an alarm template when creating a resource group or afterwards. For details, see 3.1.4.3 Associating a Resource Group with an Alarm Template .
Created	Time when the resource group was created.
Modified	Last time when the resource group was modified.
Operation	You can create alarm rules, associate alarm templates, or delete the resource group.

3.1.3.2 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 [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. Click a resource group name to go to the **Resource Overview** page.

On this page, you can change the name of a resource group, modify resource matching rules, remove resources, and set alarm rules.

3.1.3.3 Alarm Rules

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

In a resource group, you can view only alarm rules of this group, but not those of a specified resource or all resources.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. In the resource group list, click the name of the target group to go to the **Resource Overview** page.
4. In the navigation pane on the right, choose **Alarm Rules** to view all alarm rules in the resource group.

On the **Alarm Rules** page, you can quickly create alarm rules for resources in the resource group. For details, see [5.2.2 Creating an Alarm Rule and Notifications](#).

3.1.4 Managing Resource Groups

3.1.4.1 Modifying a Resource Group

When you need to add resources to or delete resources from a resource group, modify the resource group.

Constraints

After a resource group is modified, it takes about three hours for the new resource matching rule to be applied. During this time, resources are still matched based on the old rule.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. Click the name of the resource group to be modified to go to its details page.
4. To rename the resource group, click  next to **Name** in the **Basic Information** area, enter a new name, and click .
5. Click **Modify Resource Matching Rule**.
If **Add Resources** is set to **Manually**, you can reselect resources on the **Modify Resource Matching Rule** page or remove selected resources on the resource details page.

3.1.4.2 Deleting a Resource Group

You can delete a resource group when you no longer need it.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. Locate the row containing the target resource group and click **Delete** in the **Operation** column.
4. In the displayed **Delete Resource Group** dialog box, click **OK**.

3.1.4.3 Associating a Resource Group with an Alarm Template

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

If you have many cloud resources, you are advised to create resource groups by service application, create alarm templates, and associate resource groups with the alarm templates to create alarm rules in batches. This makes it easier and

faster to create and maintain alarm rules. After the association, alarm rules for resources in this group will be generated. Any changes to the templates will automatically update the alarm policies.

Prerequisites

You have created a resource group.

Associating Alarm Templates

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Resource Groups**.
3. Locate the target resource group and click **Associate Alarm Template** in the **Operation** column.
4. On the displayed page, select an alarm template.
5. Configure alarm notification parameters based on [Table 3-6](#).
6. Select an enterprise project.

Figure 3-1 Advanced settings

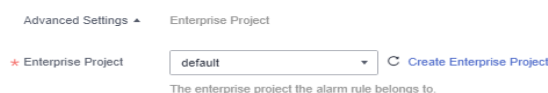


Table 3-8 Enterprise project

Parameter	Description
Enterprise Project	Enterprise project that the alarm rules belong 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 .

7. Click **OK**.

NOTE

Associating an alarm template with a resource group triggers asynchronous operations such as creating, updating, and deleting alarm rules. This process typically lasts for 5 to 10 minutes but may take longer if there are multiple association tasks.

3.1.5 Cloud Services Supported by Resource Groups

NOTE

To automatically create resource groups, the related cloud services must have been connected to the Config service. In certain regions, some cloud services may not be connected to Config. When configuring resource groups, you can verify if all the cloud services involved have been connected to Config.

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
Elastic Cloud Server	ECS	ECS	Supported	Supported	Supported	Supported	Supported
Bare Metal Server	BMS	BMS	Supported	Supported	Supported	Supported	Supported
Cloud Phone Host	CPH	Cloud phone server	Supported	Supported	Not supported	Supported	Not supported
API Gateway (Dedicated)	APIG (Dedicated)	API gateway	Supported	Supported	Supported	Supported	Supported
API Gateway	APIG	API	Supported	Not supported	Not supported	Not supported	Not supported
Auto Scaling	AS	AS group	Supported	Supported	Supported	Supported	Supported
Cloud Bastion Host	CBH	CBH	Supported	Supported	Supported	Supported	Supported
Cloud Backup and Recovery	CBR	Vault	Supported	Supported	Supported	Supported	Supported
Cloud Connect	CC	Cloud connection	Supported	Not supported	Not supported	Not supported	Not supported
Cloud Data Migration	CDM	CDM instance	Supported	Not supported	Not supported	Not supported	Not supported
Content Delivery Network	CDN	Domain name	Supported	Supported	Not supported	Supported	Not supported
Cloud Firewall	CFW	CFW instance	Supported	Not supported	Not supported	Not supported	Not supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
CloudTable Service	CloudTable	Cluster ID	Supported	Supported	Not supported	Supported	Not supported
Direct Connect	DCAAS	Connections	Supported	Not supported	Not supported	Not supported	Not supported
		Historical connections	Supported	Not supported	Not supported	Not supported	Not supported
		Virtual interface	Supported	Not supported	Not supported	Not supported	Not supported
		Virtual gateways	Supported	Not supported	Not supported	Not supported	Not supported
Distributed Cache Service	DCS	DCS for Redis instance	Supported	Supported	Supported	Supported	Supported
		DCS IMDG instance	Supported	Not supported	Not supported	Not supported	Not supported
		DCS Memcached instance	Supported	Not supported	Not supported	Not supported	Not supported
Distributed Database Middleware	DDMS	DDM instance	Supported	Supported	Supported	Supported	Supported
Document Database Service	DDS	DDS instances	Supported	Supported	Supported	Supported	Supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
Data Lake Insight	DLI	Queue	Supported	Not supported	Not supported	Not supported	Not supported
Distributed Message Service	DMS	DMS for Kafka	Supported	Supported	Supported	Supported	Supported
		Rabbit MQ instance	Supported	Supported	Supported	Supported	Supported
		DMS for Rocket MQ	Supported	Supported	Supported	Supported	Supported
		Consumer groups in queues	Supported	Not supported	Not supported	Not supported	Not supported
		Queue	Supported	Not supported	Not supported	Not supported	Not supported
Cloud Domain Name Service	DNS	Record set	Supported	Supported	Supported	Supported	Supported
		Domain name	Supported	Supported	Supported	Supported	Supported
Data Replication Service	DRS	DRS instance	Supported	Supported	Supported	Supported	Supported
Data Warehouse Service	DWS	DWS service	Supported	Supported	Supported	Supported	Supported
		DWS node	Supported	Not supported	Not supported	Not supported	Not supported
		DWS instance	Supported	Not supported	Not supported	Not supported	Not supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
Scalable File Service Turbo	SFS Turbo	Instance	Supported	Supported	Not supported	Supported	Not supported
Elastic Load Balance	ELB	Load balancer	Supported	Supported	Supported	Supported	Supported
		Classic load balancer	Supported	Not supported	Not supported	Not supported	Not supported
Cloud Search Service	CSS	CSS cluster	Supported	Supported	Supported	Supported	Supported
Elastic Volume Service	EVS	Disk	Supported	Supported	Not supported	Supported	Not supported
FunctionGraph	FunctionGraph	Tenant	Supported	Not supported	Not supported	Not supported	Not supported
		Flow	Supported	Not supported	Not supported	Not supported	Not supported
		Function	Supported	Not supported	Not supported	Not supported	Not supported
GaussDB	GaussDB	GaussDB instance	Supported	Not supported	Not supported	Not supported	Not supported
Taurus DB	Taurus DB	Taurus DB instance	Supported	Supported	Supported	Supported	Supported
Global Elastic IP and Bandwidth	Global EIP	Public bandwidth	Supported	Not supported	Not supported	Not supported	Not supported
		Global EIP	Supported	Not supported	Not supported	Not supported	Not supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
		Global EIP range	Supported	Not supported	Not supported	Not supported	Not supported
Graph Engine Service	GES	Graph instance	Supported	Supported	Supported	Supported	Supported
Host Security Service	HSS	Host instance	Supported	Supported	Supported	Supported	Supported
		Host security	Supported	Supported	Supported	Supported	Supported
Live	LIVE	Domain name	Supported	Not supported	Not supported	Not supported	Not supported
MapReduce	MRS	Cluster	Supported	Supported	Supported	Supported	Supported
NAT Gateway	NAT	Private NAT gateway	Supported	Not supported	Not supported	Not supported	Not supported
		Public NAT gateway	Supported	Supported	Supported	Supported	Supported
Gemini DB	NoSQL	Cassandra	Supported	Supported	Supported	Supported	Supported
		Redis	Supported	Supported	Supported	Supported	Supported
		InfluxDB	Supported	Not supported	Not supported	Not supported	Not supported
		MongoDB	Supported	Not supported	Not supported	Not supported	Not supported
Object Storage Service	OBS	Bucket	Supported	Supported	Supported	Supported	Supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
Relational Database Service	RDS	PostgreSQL instance	Supported	Supported	Supported	Supported	Supported
		MySQL instance	Supported	Supported	Supported	Supported	Supported
		Microsoft SQL Server instance	Supported	Supported	Supported	Supported	Supported
ROMA	ROMA	ROMA instance	Supported	Not supported	Not supported	Not supported	Not supported
Scalable File Service	SFS	SFS Capacity-Oriented	Supported	Not supported	Not supported	Not supported	Not supported
		General Purpose File System	Supported	Not supported	Not supported	Not supported	Not supported
Virtual Private Cloud	VPC	Bandwidth	Supported	Supported	Supported	Supported	Not supported
		EIP	Supported	Supported	Supported	Supported	Not supported
Virtual Private Network	VPN	VPN connection	Supported	Supported	Not supported	Supported	Not supported
		Enterprise Edition S2C VPN gateway	Supported	Supported	Supported	Supported	Supported

Cloud Service	Abbreviation	Product	Manually	Enterprise Project	Tag	Instance Name	Multiple Criteria
		Enterprise Edition S2C VPN connection	Supported	Supported	Supported	Supported	Supported
		Enterprise Edition P2C VPN gateway	Supported	Supported	Supported	Supported	Supported
		New VPN connection	Supported	Not supported	Not supported	Not supported	Not supported
		Dedicated VPN connection	Supported	Not supported	Not supported	Not supported	Not supported
Web Application Firewall	WAF	Protected domain name	Supported	Supported	Not supported	Supported	Not supported
		Dedicated instance	Supported	Not supported	Not supported	Not supported	Not supported

3.2 Server Monitoring

3.2.1 Overview

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.

Server monitoring consists of 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 [10 Cloud Product Metrics](#). Basic monitoring is unavailable for BMSs.
- OS monitoring provides proactive and fine-grained OS monitoring for ECSs or BMSs provided that the Agent is installed. Data is collected every minute, capturing metrics such as CPU usage and memory usage. For more information, see [10 Cloud Product Metrics](#).
- 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?](#)
- Recommended specifications for server monitoring are 2 vCPUs and 4GiB for Linux servers and 4 vCPUs and 8GiB or higher for Windows servers.
- To install the Agent on a Linux server, you must have the root permissions. For a Windows server, you must have the administrator permissions.

Constraints

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

Monitoring Capabilities

Multiple metrics, such as metrics for CPU, memory, disk, and network usage, will be monitored, meeting the basic monitoring and O&M requirements for servers. For details about metrics, see [10 Cloud Product Metrics](#).

Resource Usage

The Agent uses very few system resources (no more than 10% of a single CPU core and no more than 200 MB memory). Generally, the CPU usage of a single core is less than 5%, and the memory is less than 100 MB.

In certain scenarios, server operations may cause the Agent CPU and memory usage to increase sharply. If resource usage exceeds the preset threshold, circuit breaking is triggered, causing the Agent process to exit and restart. If the excessive usage continues, the Agent process will repeatedly stop and start, resulting in unstable operation. The following table describes typical scenarios and respective solutions.

Table 3-9 High Agent resource usage scenarios

Cause	Scenario	Procedure
Too many TCP connections	By default, the Agent collects only two basic metrics TCP TOTAL and TCP ESTABLISHED, which use a few CPU resources. If you choose to enable any detailed TCP metric by updating the configuration file, the Agent will start collecting all TCP metrics, which will consume a lot of CPU resources. Basic TCP metrics: TCP TOTAL and TCP ESTABLISHED TCP detailed metrics: TCP SYS_SENT, TCP SYS_RECV, TCP FIN_WAIT1, TCP FIN_WAIT2, TCP TIME_WAIT, TCP CLOSE, TCP CLOSE_WAIT, TCP LAST_ACK, TCP LISTEN, and TCP CLOSING	Method 1: Modify the configuration file to stop collecting TCP detailed metrics and reduce the CPU usage. For details, see How Do I Enable or Disable Metric Collection by Modifying the Configuration File? Method 2: Modify the configuration file to change the Agent resource usage threshold. For details, see How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File?
Too many file handles	While the Agent is running, it monitors all files opened by processes on the server to track and sum the number of file handles. If there are too many file handles, the Agent task will be re-executed, resulting in high CPU usage.	Method 1: Modify the configuration file to reduce the metric update frequency for the Agent process to lower the CPU usage. For details, see How Do I Change the Process Collection Frequency by Modifying the Configuration File? Method 2: Modify the configuration file to change the Agent resource usage threshold. For details, see How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File?
Too many processes	When the Agent is running, it scans all processes on the current server and collects process-level metrics by reviewing process information. When there are too many processes, the Agent task is re-executed, leading to high CPU usage.	Method 1: Modify the configuration file to reduce the metric update frequency for the Agent process to lower the CPU usage. For details, see How Do I Change the Process Collection Frequency by Modifying the Configuration File? Method 2: Modify the configuration file to change the Agent resource usage threshold. For details, see How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File?

3.2.2 Cloud Eye Plug-in (Agent)

3.2.2.1 Installing and Configuring the Agent

You can install the Agent on your servers to enable proactive, system-level monitoring with fine-grained metrics.

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

Scenario	Service	Reference
Installing the Agent on a Linux server	ECS and BMS	Installing the Agent on a Linux Server
Installing the Agent on a Windows server	ECS	3.2.2.3.2 Installing the Agent on a Windows Server
Installing the Agent in batches on Linux servers	ECS	Batch Installing Agents

Configuration Dependencies

- Agent installation requires proper DNS and security group settings. If they are not correctly configured, the Agent package will fail to be downloaded. Therefore, you need to modify the DNS configuration and configure security group rules before installing the Agent.
- After you install the Agent, you can click **Restore Agent Configurations** on the Cloud Eye console to configure the agency and files.
- If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it.
- To check the OSs supported by the Agent, see [What OSs Does the Agent Support?](#)
- You are advised to use an ECS or BMS which has installed an Agent to create a private image and create an ECS or BMS from the image.

CAUTION

- A private image created in one region cannot be used in another region. If used, no monitoring data will be generated for the servers created from that private image.
 - Cloud Eye does not provide technical support for Agent installation issues on servers created from private images.
-

BMS Hardware Monitoring Plug-in

Agent 2.5.6.1 and later enhanced versions integrate the BMS hardware monitoring plug-in. The plug-in checks hardware health in real time, identifies potential issues early, and detects all BMS hardware faults.

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

After the hardware monitoring plug-in is installed, you will be notified of potential hardware issues through event notifications. You need to authorize the BMS to repair or replace the risky hardware in a timely manner.

NOTE

- The hardware monitoring plug-in only collects some necessary OS metrics to identify hardware faults. For details, see [BMS Hardware Metrics](#).
- Only some Linux OSs are supported.
- BMSs of all specifications support the hardware monitoring plug-in.
- If your BMS uses a private image as the OS, ensure that the image has the following software installed: dmidecode, lscpu, dmesg, lspci, modinfo, ifconfig, ethtool, hnicadm, smartctl, lsccsi, and uname.

3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure

To enable you to monitor servers more securely and efficiently, Cloud Eye provides the latest Agent permission-granting method. That is, before installing Agents, you only need to click **Configure** on the **Server Monitoring** page of the Cloud Eye console, the system will perform temporary AK/SK authorization for the Agents installed on all ECSs or BMSs in the region. And in the future, newly created ECSs or BMSs in this region will automatically get this authorization. This section describes the authorization as follows:

- Authorization object

On the Cloud Eye console, if you choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**), select a server, and click **Configure**, the system will create an agency named **cesagency** on IAM. The agency permissions are automatically granted to Cloud Eye internal account **op_svc_ces**.

NOTE

If the system displays a message indicating that the tenant does not have insufficient permissions, see [What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?](#)

- Authorization scope

Add the **CES AgentAccess** permissions to internal account **op_svc_ces** in the region.

- Authorization reason

The Cloud Eye Agent runs on ECSs or BMSs and reports the collected monitoring data to Cloud Eye. After being authorized, the Agent automatically obtains a temporary AK/SK. This way, you can query the ECS or BMS monitoring data on the Cloud Eye console or by calling the Cloud Eye APIs.

- a. Security: The AK/SK used by the Agent is only the temporary AK/SK that has the **CES AgentAccess** permissions. That is, the temporary AK/SK can only be used to operate Cloud Eye resources.
- b. Convenient: You only need to configure the Cloud Eye Agent once in each region instead of manually configuring each Agent.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Click **Configure** above the host list to grant the Agent-related permissions for the current region.

3.2.2.3 Installing the Agent

3.2.2.3.1 Installing the Agent on a Linux Server

Installing the Agent on a Linux Server

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

Constraints

Only Windows and Linux are supported.

Prerequisites

- Required permissions have been granted to the Agent in the current region. For details, see [3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure](#).
- You have modified DNS server addresses and added security group rules. For details, see [Modifying the DNS Server Address and Adding Security Group Rules](#)
- You have the read and write permissions for the installation directories. The Telescope process will not be stopped by other software after the installation.

Procedure

1. Log in to a server as user **root**.
2. Run either of the commands below to install the Agent.

```
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 0.2.3 -t 2.7.6 -o myhuaweicloud.eu -d agent.ces.myhuaweicloud.eu
```

The Agent is installed if the command output similar to the following figure is displayed.

Figure 3-2 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. Clear the installation script.
if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then rm /usr/local/agent_install.sh; else rm /usr/local/agentInstall.sh; fi

NOTE

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

Batch Installing Agents

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

Constraints

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

Prerequisites

- Required permissions have been granted to the Agent in the current region. For details, see [3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure](#).
- You have modified DNS server addresses and added security group rules.
- You have the read and write permissions for the installation directories. The Telescope process will not be stopped by other software after the installation.
- Username and password: As you have collected IP addresses of all ECSs and the password of user **root**, keep them in the **iplist.txt** file and upload them to the **/usr/local** directory on the first ECS.

 NOTE

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

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

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

- Key: As you have collected IP addresses of all ECSs, keep them in the **iplist.txt** file, upload them to the **/usr/local** directory on the first ECS, and uploaded the key file **user.pem** to the **/usr/local** directory on the ECS.

 NOTE

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

An example is provided as follows:

```
192.168.1.1
192.168.1.2
```

Procedure

1. Use SSH to log in to the ECS where the Agent has been installed as user **root**.
2. Install the Agents in batches.

```
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 0.2.3 -t 2.7.6 -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 all ECSs with the Agent installed.

 NOTE

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

3.2.2.3.2 Installing the Agent on a Windows Server

Scenarios

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

Constraints

Windows OSs support only the **Normal installation** method.

Prerequisites

- Required permissions have been granted to the Agent in the current region. For details, see [3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure](#).
- You have modified DNS server addresses and added security group rules.
- An account with the administrator permissions, for example, the administrator account, is used to install the Agent. The Telescope process will not be stopped by other software after the installation.

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

Table 3-10 Paths for obtaining the Agent installation package

Name	Format	Path
Agent installation package for 64-bit Windows	exe	https://uniagent-eu-west-101.obs.eu-west-101.myhuaweicloud.eu/package/install_amd64.exe

Procedure

- Log in to a Windows ECS as an administrator.
- Open a browser and enter the path of the Agent installation package in the address box to download and save the installation package. For details, see [Table 3-10](#).
- Access the directory storing the installation package.
- Open Windows PowerShell and run the following command to go to the installation package directory (for example, **C:\Users\Administrator\Downloads**).

```
cd C:\Users\Administrator\Downloads
```
- Install the Agent.

```
install_amd64.exe -r eu-west-101 -u 0.2.3 -t 2.7.6 -d agent.ces.myhuaweicloud.eu -o myhuaweicloud.eu
```

NOTE

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

3.2.2.4 Installing and Configuring the Agent

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

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

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

NOTE

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

Modifying the DNS Server Address (Command Lines)

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

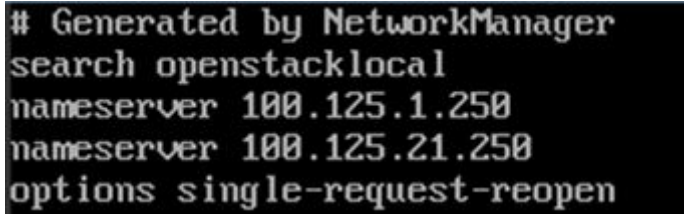
To use the management console, see [Modifying the DNS Server Address \(Management Console\)](#).

 NOTE

The **nameserver** value varies depending on the region. For details, see [What Are Huawei Cloud Private DNS Server Addresses?](#)

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. Press **Esc** and enter **:wq**. Then, press **Enter** to save the change.

Figure 3-3 Adding DNS server addresses (Linux)



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

Modifying the DNS Server Address (Management Console)

The following describes how to modify the DNS server address of an ECS in the region on the management console. 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 target ECS name to view its details.

3. In the **ECS Information** area of the **Summary** tab, click the VPC name. The **Virtual Private Cloud** page is displayed.
4. Locate the target VPC and click the number of subnets.
5. In the subnet list, locate the subnet of the ECS and click its name.
6. On the subnet details page, click  next to **DNS Server Address** in the **Gateway and DNS Information** area.
7. In the **Edit DNS Server Address** dialog box, enter a 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 is applied 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 a security group name.
3. On the security group details page, click **Outbound Rules**.

NOTE

For BMSs:

1. Click the security group ID on the upper left.
2. Locate the security group and click **Manage Rule** in the **Operation** column.
4. On the **Outbound Rules** page, click **Add Rule**.
5. Add rules based on [Table 3-11](#).

Table 3-11 Security group rules

Pri ori ty	Ac tio n	Typ e	Protocol & Port		Destination IP Address	Description
1	All ow	IPv 4	TCP	80	100.125.0.0/ 16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.
1	All ow	IPv 4	TCP	53	100.125.0.0/ 16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.

Pri ori ty	Ac tio n	Typ e	Protocol & Port		Destination IP Address	Description
1	All ow	IPv 4	UDP	53	100.125.0.0/ 16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
1	All ow	IPv 4	TCP	443	100.125.0.0/ 16	Used to collect monitoring data to Cloud Eye.

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

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**. Log in to the Windows ECS using VNC.
2. Choose **Control Panel > Network and Sharing Center**, and click **Change adapter settings**.
3. Right-click the network in use, select properties, and configure DNS server addresses.

NOTE

The **nameserver** value varies depending on the region. For details, see [What Are Huawei Cloud Private DNS Server Addresses?](#)

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 target ECS name to view its details.
3. In the **ECS Information** area of the **Summary** page, click the VPC name.
The **Virtual Private Cloud** page is displayed.
4. Click the VPC name.
5. In the **Networking Components** area, click the number following **Subnets**.
The **Subnets** page is displayed.
6. In the subnet list, locate the subnet of the ECS and click its name.
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 is applied 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 a security group name.
3. On the security group details page, click **Outbound Rules**.

NOTE

For BMSs:

1. Click the security group ID on the upper left.
2. Locate the security group and click **Manage Rule** in the **Operation** column.
4. Click the **Outbound Rules** tab and click **Add Rule**.
5. Add rules based on [Table 3-12](#).

Table 3-12 Security group rules

Pri ori ty	Ac tio n	Typ e	Protocol & Port		Destination IP Address	Description
1	All ow	IPv 4	TCP	80	100.125.0.0/ 16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.
1	All ow	IPv 4	TCP	53	100.125.0.0/ 16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
1	All ow	IPv 4	UDP	53	100.125.0.0/ 16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
1	All ow	IPv 4	TCP	443	100.125.0.0/ 16	Used to collect monitoring data to Cloud Eye.

3.2.2.4.3 (Optional) Manually Configuring the Agent (Linux)

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

Prerequisites

You have installed the Agent.

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. Open **conf.json**:

```
vi /usr/local/uniagent/extension/install/telescope/bin/conf.json
```
 - b. Modify the parameters in the file. For details, see [Table 3-13](#).

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all Agents installed on ECSs or BMSs in the region. For details, see [How Do I Configure an Agency?](#)

```
{  
  "InstanceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",  
  "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",  
  "AccessKey": "XXXXXXXXXXXXXXXXXXXX",  
  "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",  
  "RegionId": "xx-xx-xx",  
  "ClientPort": 0,  
  "PortNum": 200  
}
```

Table 3-13 Public parameters

Parameter	Description
InstanceId	(Optional) ECS ID. You can log in to the management console and view the ECS ID in the ECS list. NOTE If you choose not to configure InstanceId, retain "InstanceId":"". If you do configure it, ensure that both of the following 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, or 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) Project ID. If you do not configure ProjectId, retain "ProjectId":"". If you do configure it, perform the following operations: 1. Log in to the Cloud Eye console, click your 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	Access key (AK) and secret key (SK). To obtain them: Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials, and choose Access Keys. • If you have obtained the access key, obtain the AccessKey value and the SecretKey value in the credentials.csv file saved when you create Access Keys. • If no access keys are available, click Create Access Key to create one. Save the credentials.csv file and obtain the AccessKey value and the SecretKey value in it. NOTICE • For security purposes, 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, or its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Region ID.
ClientPort	Start port number used by the Agent. NOTE The default value is 0, indicating that the Agent will randomly use an available port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.

Parameter	Description
PortNum	Number of ports configured for the Agent. NOTE The default value is 200 . If ClientPort is 5000 , the Agent will use ports in the range port 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. Go to the Agent installation path **bin**:
cd /usr/local/uniagent/extension/install/telescope/bin
3. Modify configuration file **conf.json**.
 - a. Open **conf.json**:
vi conf.json
 - b. Modify the parameters in the file. For details, see [Table 3-14](#).

ECS parameters

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

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

Table 3-14 Public parameters

Parameter	Description
InstanceId	(Optional) ECS ID. You can log in to the management console and view the ECS ID in the ECS list. NOTE If you choose not to configure InstanceId , retain " InstanceId ":"". If you do configure it, ensure that both of the following 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, or 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) Project ID. If you do not configure ProjectId , retain " ProjectId ":"". If you do configure it, perform the following operations: 1. Log in to the Cloud Eye console, click your 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	Access key (AK) and secret key (SK). To obtain them: Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials , and choose Access Keys . • If you have obtained the access key, obtain the AccessKey value and the SecretKey value in the credentials.csv file saved when you create Access Keys. • If no access keys are available, click Create Access Key to create one. Save the credentials.csv file and obtain the AccessKey value and the SecretKey value in it. NOTICE • For security purposes, 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, or its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Region ID.
ClientPort	Start port number used by the Agent. NOTE The default value is 0 , indicating that the Agent will randomly use an available port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.

Parameter	Description
PortNum	Number of ports configured for the Agent. NOTE The default value is 200 . If ClientPort is 5000 , the Agent will use ports in the range port 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 the **conf_ces.json** configuration file 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 3-15](#).

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

Table 3-15 Parameter setting of the metric collection module

Parameter	Description
Endpoint	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 the monitoring data has not been reported yet. Wait for 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.

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

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

Constraints

Windows and Linux OSs are supported. For details, see [What OSs Does the Agent Support?](#)

Prerequisites

You have installed the Agent.

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 3-16](#).

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all Agents installed on ECSs or BMSs in the region. For details, see [How Do I Configure an Agency?](#)

```
{
  "InstanceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
  "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
  "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "RegionId": "xx-xx-xx",
  "ClientPort": 0,
  "PortNum": 200
}
```

Table 3-16 Public parameters

Parameter	Description
InstanceId	(Optional) ECS ID. You can log in to the management console and view the ECS ID in the ECS list. NOTE If you choose not to configure InstanceId , retain " InstanceId ":"". If you do configure it, ensure that both of the following 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, or errors may occur. • The InstanceId value must be consistent with the actual ECS or BMS ID, or the OS monitoring data for the ECS or BMS will not be displayed on Cloud Eye.
ProjectId	(Optional) Project ID. If you do not configure ProjectId , retain " ProjectId ":"". If you do configure it, perform the following operations: 1. Log in to the Cloud Eye console, click your username in the upper right corner, and choose My Credentials. 2. Under Projects, obtain the project ID for the region of the ECS or BMS.
AccessKey/ SecretKey	Access key (AK) and secret key (SK). To obtain them: Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials , and choose Access Keys . • If you have obtained the access key, obtain the AccessKey value and the SecretKey value in the credentials.csv file saved when you create Access Keys. • If no access keys are available, click Create Access Key to create one. Save the credentials.csv file and obtain the AccessKey value and the SecretKey value in it. NOTICE • For security purposes, 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, or its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Region ID.
ClientPort	Start port number used by the Agent. NOTE The default value is 0 , indicating that the Agent will randomly use an available port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.

Parameter	Description
PortNum	Number of ports configured for the Agent. NOTE The default value is 200 . If ClientPort is 5000 , the Agent will use ports in the range port 5000 to 5199.

 NOTE

- After you configure the Agent, its status is still displayed as **Uninstalled** because the monitoring data has not been reported yet. Wait for 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 3-17](#).

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

Table 3-17 Public parameters

Parameter	Description
InstanceId	(Optional) ECS ID. You can log in to the management console and view the ECS ID in the ECS list. NOTE If you choose not to configure InstanceId , retain " InstanceId :". If you do configure it, ensure that both of the following 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, or errors may occur. • The InstanceId value must be consistent with the actual ECS or BMS ID, or you cannot see the OS monitoring data on Cloud Eye.

Parameter	Description
ProjectId	(Optional) Project ID. If you do not configure ProjectId , retain " ProjectId ": "". If you do configure it, perform the following operations: 1. Log in to the Cloud Eye console, click your 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	Access key (AK) and secret key (SK). To obtain them: Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials , and choose Access Keys . • If you have obtained the access key, obtain the AccessKey value and the SecretKey value in the credentials.csv file saved when you create Access Keys. • If no access keys are available, click Create Access Key to create one. Save the credentials.csv file and obtain the AccessKey value and the SecretKey value in it. NOTICE • For security purposes, it is recommended that you perform the above operations as an IAM user with the CES Administrator and LTS Administrator permissions only.. • The configured access key must be within the Access Keys list on the My Credentials page, or its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Region ID.
ClientPort	Start port number used by the Agent. NOTE The default value is 0 , indicating that the Agent will randomly use an available port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Number of ports configured for the Agent. NOTE The default value is 200 . If ClientPort is 5000 , the Agent will use ports in the range port 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.

3.2.2.5 Managing the Agent

After the Agent is installed, you can view, start, stop, update, or uninstall it as needed. This section describes how to manage the Agent on Linux and Windows systems.

**CAUTION**

You can only manage the Agent as an administrator (**root** user for Linux and **Administrator** user for Windows). Any improper use of this account may cause system stability or data security issues. Exercise caution when using this account.

Prerequisites

- You have installed the Agent on a server. For details, see [Installing the Agent](#).
- You have confirmed the Agent version. The Agent has two versions: new and old. The operations vary according to the version.

Linux:

a. Log in to the server as user **root**.

b. 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, an early version of the Agent is used. Manage the Agent using the instructions for the early version.
- If a particular version is returned, the new version of the Agent is used. Manage the Agent using the instructions for the early version.
- If **0** is returned, the Agent is not installed.

Windows: Determine the Agent version based on the installation path.

- New version: **C:\Program Files\uniagent\extension\install\telescope**
- Earlier version: **C:\Program Files\telescope**

Checking the Agent Status

After the Agent is installed, you can also log in to the server to check its running status.

New Version

Linux:

1. Log in to the server as user **root**.

2. Check the Agent status.

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

3. Check whether the following information is displayed. If so, the Agent is running properly.

```
"Telescope process is running well."
```

Windows:

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

Earlier Version

1. Log in to the server as user **root**.
2. Check the Agent status.
`service telescoped status`
3. Check whether the following information is displayed. If so, the Agent is running properly.
"Active (running)" or "Telescope process is running well."

Stopping the Agent

You can disable the Agent during monitoring policy changes or temporary system maintenance.

New Version

Linux:

1. Log in to the server as user **root**.
2. Stop the Agent.
`/usr/local/uniagent/bin/uniagent stop`
`/usr/local/uniagent/extension/install/telescope/telescoped stop`

Windows:

1. Go to the **C:\Program Files\uniagent\extension\install\telescope** directory for storing the Agent installation package.
2. Double-click the **shutdown.bat** script to stop the Agent.

Earlier Version

Linux:

1. Log in to the server as user **root**.
2. Stop the Agent.
`service telescoped stop`

Windows:

1. Go to the **C:\Program Files\telescope** directory for storing the Agent installation package.
2. Double-click the **shutdown.bat** script to stop the Agent.

Starting the Agent

If the Agent is in the **Stopped** state, perform the following operations to start the Agent.

New Version

Linux:

1. Log in to the server as user **root**.
2. Start the Agent.
`/usr/local/uniagent/bin/uniagent start`
`/usr/local/uniagent/extension/install/telescope/telescoped start`

Windows:

1. Go to the **C:\Program Files\uniagent\extension\install\telescope** directory for storing the Agent installation package.
2. Double-click the **start.bat** script to start the Agent.

Earlier Version**Linux:**

1. Log in to the server as user **root**.
2. Start the Agent.

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

Windows:

1. Go to the **C:\Program Files\telescope** directory for storing the Agent installation package.
2. Double-click the **start.bat** script to start the Agent.

Restarting the Agent

If the Agent process is faulty, restart the Agent. If the fault persists after the restart, the Agent files may be damaged. In this case, reinstall the Agent. For details, see [Installing and Configuring the Agent](#).

New Version**Linux:**

1. Log in to the server as user **root**.
2. Restart the Agent.

```
/usr/local/uniagent/bin/uniagent stop  
/usr/local/uniagent/bin/uniagent start  
/usr/local/uniagent/extension/install/telescope/telescoped restart
```

Windows:

The Agent cannot be restarted.

Earlier Version**Linux:**

1. Log in to the server as user **root**.
2. Restart the Agent.

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

Windows:

The Agent cannot be restarted.

Uninstalling the Agent

If you need to log in to the server to upgrade the Agent, uninstall the Agent of an earlier version.

New Version

Linux:

1. Log in to the server as user **root**.
2. Uninstall the Agent.
`bash /usr/local/uniagent/script/uninstall.sh`

Windows:

1. Go to the **C:\Program Files\uniagent\script** directory for storing the Agent installation package.
2. Double-click the **uninstall.bat** script to uninstall the Agent.

CAUTION

After you run the Agent uninstallation command on a Windows server, go to the **C:\Program Files\uniagent** directory to check whether there are residual files. If there are, manually delete this directory.

Earlier Version

Linux:

1. Log in to the server as user **root**.
2. Uninstall the Agent.
`/usr/local/telescope/uninstall.sh`

Windows:

1. Go to the **C:\Program Files\telescope** directory for storing the Agent installation package.
2. Double-click the **uninstall.bat** script to uninstall the Agent.

CAUTION

After you run the Agent uninstallation command on a Windows server, go to the **C:\Program Files\telescope** directory to check whether there are residual files. If there are, manually delete this directory.

3.2.2.6 Installing Other Monitoring Plug-ins

3.2.2.6.1 Installing Direct Connect Metric Collection Plug-ins

Scenarios

Direct Connect metric collection plug-ins are used to monitor the end-to-end network quality of Direct Connect connections. They must be deployed on an ECS in the VPC that connects to a Direct Connect connection. By default, the plug-ins send ping packets to the remote IP address of the on-premises data center every second. Based on the ping responses, the plug-ins calculate the E2E network

latency and packet loss rate of the Direct Connect connection and report these metrics to Cloud Eye.

There are two types of such plug-ins:

- **dc-nqa-collector**: It is used to monitor automated connections and detect the latency and packet loss rate of remote subnets.

If Direct Connect resources include a physical connection, virtual gateway, and virtual interface, they are considered as automated connections. Route configurations can be automatically delivered. Most regions now use automated connections. For more information, see [Direct Connect console](#).

- **history-dc-nqa-collector**: It is used to monitor historical Direct Connect connections and detect the latency and packet loss rate of remote subnets.

If Direct Connect resources include just a physical connection (no virtual gateway or interface included), they are considered as historical connections. You need to manually configure the routes. Only some legacy resources in certain regions use historical connections. For more information, see the Historical Connections page of the Direct Connect console.

Metrics

Direct Connect metric collection plug-ins are mainly used to monitor the **Latency** and **Packet Loss Rate** metrics.

Table 3-18 Network quality metrics

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval
latency	Latency	Network latency of a connection	≥ 0	ms	N/A	Virtual interfaces and historical connections	1 minute
packet_loss_rate	Packet Loss Rate	Packet loss rate of a connection	0 to 100	%	N/A	Virtual interfaces and historical connections	1 minute

Constraints

Direct Connect metric collection plug-ins can only be installed on Linux ECSs. It is recommended that you use CentOS and select 2 vCPUs and 4 GiB or higher specifications.

Prerequisites

- You have created an ECS for deploying the Direct Connect metric collection plug-in and have obtained the password of user **root**.
An ECS has been added to each VPC that connects to a Direct Connect connection for deploying the Direct Connect metric collection plug-in. Existing ECSs running other workloads cannot be used. You can view the associated VPCs that connect to automated connections on the [virtual gateway list](#) on the Direct Connect console.
- You have granted required plug-in permissions to servers in the current region. For details, see [3.2.2.2 Granting Agent Permissions for Servers by Clicking Configure](#).
- The Cloud Eye Agent has been installed on the server. For details, see [Installing the Agent](#).

Procedure

In some regions, you can use the one-click installation script to install the Direct Connect metric collection plug-in. For details about the supported regions, see [Table 3-21](#).

NOTE

If one-click installation is unavailable in your region, [submit a service ticket](#) or contact your account manager to obtain the plug-in installation package and complete the installation.

- Log in to the ECS for deploying the plug-in as the **root** user.
- Create a **user.txt** file in the **/usr/local/** directory and add user information, including the plug-in download link, monitored resource ID, and remote IP address.

```
cd /usr/local/  
vi user.txt
```

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

```
https://uniagent-xx-xxx-x.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector //Link for  
downloading the plug-in  
9dbe3905-935f-4c7b-bc41-d33a963d57d4,X.X.X.X //ID of a monitored resource 1, Remote IP address  
1 (IP address of the remote gateway)  
b95b9fdc-65de-44db-99b1-ed321b6c11d0,X.X.X.X //ID of a monitored resource 2, Remote IP address  
2 (IP address of the remote gateway)
```

Table 3-19 User information parameters

User Info	Description
Plug-in Download Link	- To monitor automated connections, select the dc-nqa-collector plug-in. - To monitor historical connections, select the history-dc-nqa-collector plug-in. For details about links for downloading plug-in installation packages in each region, see Table 3-20.

User Info	Description
Monitored Resource Info	Each monitored resource is represented on a separate line, containing a resource ID and remote IP address, separated by a comma (,). CAUTION • Make sure each monitored resource's ID aligns with its specific remote IP address. A single resource ID cannot link to multiple IP addresses or CIDR blocks. • If multiple Direct Connect resources need to be monitored, add corresponding resource lines in the same format. • Resource ID: The value contains 32 characters of letters and digits. The format is b95b9fdc-65de-44db-99b1-ed321b6c11d0 or b95b9fdc65de44db99b1ed321b6c11d0. – For automated connections, the resource ID is that of the virtual interface. You can log in to the Virtual Interfaces page on the Direct Connect console, and obtain the virtual interface ID from the Name/ID column in the virtual interface list. – For historical connections, the resource ID is that of the historical connection. You can access the Historical Connections page on the Direct Connect console, and obtain the historical connection ID from the Name column in the historical connection list. • Remote IP Address: The remote IP address is one that you can ping from the VPC. It usually matches the IP address of the remote gateway. – For automated connections, the value is the remote gateway IP address. You can access the Virtual Interfaces page of the Direct Connect console, click the name of the virtual interface to be viewed, and obtain the IP address of the remote gateway from the Remote Gateway field in the peer list. – For historical connections, the value is the host IP address in the remote subnet. You can access the Historical Information page on the console, and obtain the required host IP address from the Remote Subnet field in the historical information list.

Table 3-20 Paths for obtaining the plug-in installation packages

Name	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 Southwest-Guiyang1: https://uniagent-cn-southwest-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector CN East-Qingdao: https://uniagent-cn-east-5.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector CN South-Shenzhen: https://uniagent-cn-south-2.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

Name	Path
	LA-Mexico City1: 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 AP-Manila: https://uniagent-ap-southeast-5.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector TR-Istanbul: https://uniagent-tr-west-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector LA-Buenos Aires1: https://uniagent-sa-argentina-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector LA-Lima1: https://uniagent-sa-peru-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector

Name	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 City1: 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 Path for obtaining the one-click installation script

Table 3-21 Paths for obtaining the one-click installation script

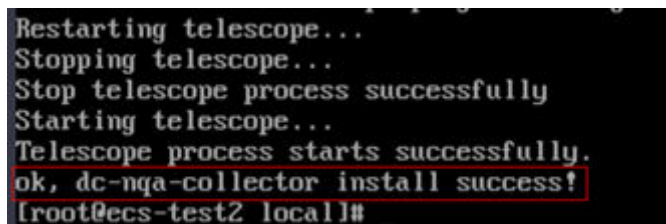
Region	Path
CN North-Beijing4	https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN North-Beijing1	https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN East-Shanghai1	https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
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 Southwest-Guiyang1	https://uniagent-cn-southwest-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN East-Qingdao	https://uniagent-cn-east-5.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
CN South-Shenzhen	https://uniagent-cn-south-2.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

Region	Path
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
AP-Manila	https://uniagent-ap-southeast-5.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
TR-Istanbul	https://uniagent-tr-west-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
LA-Buenos Aires1	https://uniagent-sa-argentina-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh
LA-Lima1	https://uniagent-sa-peru-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh

4. Install the plug-in. If the information shown in [Figure 3-4](#) is displayed, the installation is successful.

```
bash dc-installer.sh
```

Figure 3-4 Installation succeeded



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

NOTE

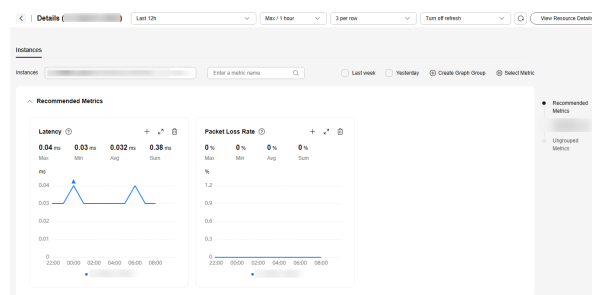
Once installed, if you need to add more monitored resources, edit the **user.txt** file, insert new lines with a resource ID and remote IP address for each one, and perform [3](#) and [4](#) again.

5. After the installation is successful, wait for about one hour for synchronizing Direct Connect resources.

Viewing Metrics

After Direct Connect resources are synchronized, you can view the latency and packet loss rate on the Cloud Eye console.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Cloud Service Monitoring**.
3. In the cloud service dashboard list, click **Direct Connect DCAAS**.
4. On the cloud service details page:
 - To view the metrics of automated connections, select **Virtual Interfaces** from the drop-down list on the right of the Direct Connect console.
 - To view the metrics of historical connections, select **Historical Direct Connections** from the drop-down list on the right of the Direct Connect console.
5. In the instance list, locate the instance whose monitoring information you want to view and click **View Metric** in the **Operation** column.



3.2.2.7 Upgrading the Agent

3.2.2.7.1 Upgrading the Agent on a Linux Server

If the Agent of the early architecture cannot meet the requirements, you can upgrade the Agent. The Cloud Eye Agent will be continuously upgraded to provide you with a better monitoring experience. The following describes how to upgrade the Agent of an early architecture (Telescope) to that of the new architecture (Uniagent) on the Linux OS.

Procedure

1. Log in to an ECS as user **root**.
2. Run the following command to check whether the current Agent is using the Uniagent or Telescope architecture:

```
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 Agent of an early architecture (Telescope) is used.
 - If a version is returned, the Agent of the new version (Uniagent) is used.
 - If **0** is returned, the Agent is not installed.
3. Uninstall the Agent of the current version.
 - Early version: Run the command in [Uninstalling the Agent \(Early Version\)](#).
 - New version: Run the command in [Uninstalling the Agent \(Early Version\)](#).

4. Install the Agent of the latest version by running the command in [Procedure](#).

3.2.2.7.2 Upgrading the Agent on a Windows Server

If the Agent of the early architecture cannot meet the requirements, you can upgrade the Agent. The Cloud Eye Agent will be continuously upgraded to provide you with a better monitoring experience. This topic describes how you can upgrade the Agent of the early architecture to that of the new architecture on the Windows OS.

Procedure

1. Log in to a Windows ECS using an account with administrator permission.
2. Determine the current Agent version based on the Agent installation path.
 - New version: **C:\Program Files\uniagent\extension\install\telescope**
 - Earlier version: **C:\Program Files\telescope**
3. Uninstall the Agent. For details about the uninstallation command, see [Uninstalling the Agent \(Early Version\)](#).
4. Install the Agent of the latest version by running the command in [Procedure](#).

3.2.2.8 Agent Features per Version

This section describes the versions of the Cloud Eye Agent.

For details about the OSs supported by the Cloud Eye Agent, see [What OSs Does the Agent Support?](#)

This section describes the Agent features provided by each version.

Version 2.7.6.1

Category	Description
Released On	2025-04-15
New Features	Added the following feature compared with version 2.7.6: Optimized NPU metric collection.
Resolved Issues	None

Version 2.7.6

Category	Description
Released On	2025-04-15
New Features	Optimized the resource usage of process metrics in Windows.

Category	Description
Resolved Issues	Fixed the metric exception caused by frequent disk/NIC attachment and detachment.

Version 2.7.5.1

Category	Description
Released On	2024-12-20
New Features	Added the following feature compared with version 2.7.5: Optimized GPU metric collection.
Resolved Issues	None

Version 2.7.5

Category	Description
Released On	2024-12-20
New Features	Optimized the NIC metric collection logic and NIC dimension value verification.
Resolved Issues	- Fixed the bug that the CPU usage is high when there are a large number of TCP connections. By default, the ss-s collects TCP metrics in lightweight mode. - Fixed the bug that system process metrics and total file handle metrics are not updated.

Version 2.7.2.1

Category	Description
Released On	2024-07-15
New Features	Added the following metrics and feature compared with version 2.7.2: - GPU metrics - NPU metrics - BMS hardware monitoring For details, see BMS Hardware Monitoring Plug-in.
Resolved Issues	None

Version 2.7.2

Category	Description
Released On	2024-07-15
New Features	- Added metrics for custom process monitoring. - Added metrics for disk read/write queues (Windows servers only). - Added availability monitoring metrics. - Added Network Time Protocol (NTP) metrics. - Added NIC metrics (Linux servers only).
Resolved Issues	Fixed false alarms generated for <i>/snap/mount point</i> in Linux Ubuntu.

Version 2.6.4.1

Category	Description
Released On	2023-10-30
New Features	Added the following features compared with version 2.6.4: - GPU metrics - Neural processing unit (NPU) metrics - BMS hardware monitoring For details, see BMS Hardware Monitoring Plug-in.
Resolved Issues	None

Version 2.6.4

Category	Description
Released On	2023-10-30
New Features	Added the metric Total UDP Connections.
Resolved Issues	None

Version 2.5.6.1

Category	Description
Released On	2023-08-14

Category	Description
New Features	Added the following features compared with version 2.5.6: • GPU metrics • Descriptions about BMS hardware monitoring. For details, see BMS Hardware Monitoring Plug-in.
Resolved Issues	None

Version 2.5.6

Category	Description
Released On	2023-08-14
New Features	• Optimized the Agent architecture, including the scheduling framework. • Optimized the collection of some metrics.
Resolved Issues	Servers in the same pool can be correctly identified.

Version 2.4.1

Category	Description
Released On	2021-09-26
New Features	The Agent can monitor more metrics.
Resolved Issues	None

3.2.3 Viewing Server Monitoring Metrics

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 [10 Cloud Product Metrics](#).

Prerequisites

You have installed the Agent. For details, see [3.2.2.3 Installing the Agent](#).

Procedure

1. Log in to the [Cloud Eye console](#).
2. 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, choose **Server Monitoring > Elastic Cloud Server** in the navigation pane, locate the ECS, and click **View Metric** in the **Operation** column. Click the **Process Monitoring** tab.
3. View metrics.
- In the upper part of the **OS Monitoring** page, different metric types, such as CPU, memory, and disk metrics are displayed.
- You can view the monitoring data curves of different metrics. By default, raw metric data is displayed if you select **Last 1h**, **Last 3h**, **Last 12h**, or **Last 1d**. For **Last 7d** and longer time ranges, aggregated data is displayed. Cloud Eye provides a 30-second refresh interval. You can choose whether to enable auto refresh
4. Hover your mouse over a graph. In the upper right corner, click  to enlarge the graph for detailed data.
- In the upper right corner, you can check monitoring data from the default monitoring periods **Last 1h**, **Last 3h**, **Last 12h**, **Last 1d**, **Last 7d**, and **Last 30d**. You can also customize one to view historical monitoring data for any period within the last 155 days.
5. In the upper right corner of the graph, click **Period** to configure the aggregation type.
- If you select **Last 1h**, **Last 3h**, **Last 12h**, or **Last 1d**, raw data is displayed by default.
 - If you select **Last 7d** or **Last 30d**, aggregated data is displayed by default.
 - After clicking the zoom in icon in the upper right of an enlarged graph, you can drag the mouse to customize the time range.

3.2.4 Process Monitoring

Process monitoring monitors active processes on a server. After the Cloud Eye Agent is installed, it collects information such as CPU usage, memory usage, and the number of opened files of these processes. You can also configure custom process monitoring to monitor processes with specified keywords, and set alarm rules for these processes to track changes to the number of processes, helping ensure the processes run smoothly.

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

Prerequisites

Ensure that the Cloud Eye Agent has been installed on a server. For details, see [3.2.2.3 Installing the Agent](#).

Constraints

There's no limit on the number of processes to be added, but the Agent collects only the first 16 processes.

Adding Processes for Monitoring

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

Suppose that the following processes are running on a server:

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

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

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

NOTE

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

Adding specified processes

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - 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**.
3. On the **Server Monitoring** page, locate the ECS and click **View Metric** to go to the **OS Monitoring** page.
4. Click the **Process Monitoring** tab.
5. On the **Process Monitoring** page, click **Add Process** under **Custom Process Monitoring**.
6. On the **Add Process** page, the cloud product and monitoring scope use the default settings of the current resource and can be changed. Configure the task name and process name for process monitoring.

Table 3-22 Parameters for adding specific processes for monitoring

Parameter	Description	Example Value
Task	Name of a process monitoring task. The value can only contain letters, digits, slashes (/), parentheses, number signs (#), underscores (_), asterisks (*) at the beginning, and hyphens (-). The value cannot start with hyphen (-). The task name can contain a maximum of 255 characters. Once a process monitoring task is created, its name cannot be changed.	Process_Monitoring
Description	Description of the process monitoring task. This is an optional parameter.	-
Cloud Product	Cloud product that requires process monitoring. You can select Elastic Cloud Server or Bare Metal Server . Once you create a process monitoring task, the cloud product cannot be modified.	Elastic Cloud Server
Monitoring Scope	Resources that require process monitoring.	-
Monitored Processes	Name of the monitored process. The value can only contain letters, digits, slashes (/), parentheses, number signs (#), underscores (_), asterisks (*) at the beginning, and hyphens (-). The value cannot start with hyphen (-). It can contain a maximum of 255 characters.	java

7. Click **OK**.

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

Adding processes in batches

1. Log in to the [Cloud Eye console](#).
2. Choose **Server Monitoring** > **Process Monitoring**.
3. On the **Process Monitoring** page, click **Add Process**. The **Add Process** page is displayed.
4. Configure a task name, select a cloud product, select specified resources, and configure the process name. For details about the parameters, see [Table 3-23](#).

Table 3-23 Parameters for batch adding processes for monitoring

Parameter	Description	Example Value
Task	Name of a process monitoring task. The value can only contain letters, digits, slashes (/), parentheses, number signs (#), underscores (_), asterisks (*) at the beginning, and hyphens (-). The value cannot start with hyphen (-). The task name can contain a maximum of 255 characters.	Process_Monitoring
Description	Description of the process monitoring task. This is an optional parameter.	-
Cloud Product	Cloud product that requires process monitoring. You can select Elastic Cloud Server or Bare Metal Server .	Elastic Cloud Server
Monitoring Scope	Resources that require process monitoring.	-
Monitored Processes	Name of the monitored processes. The value can only contain letters, digits, slashes (/), parentheses, number signs (#), underscores (_), asterisks (*) at the beginning, and hyphens (-). The value cannot start with hyphen (-). It can contain a maximum of 255 characters.	java

5. Click **OK**.

Modifying a Process Monitoring Task

1. Log in to the [Cloud Eye console](#).
2. Choose **Server Monitoring** > **Process Monitoring**.
3. Locate the target process monitoring task and click **Modify** in the **Operation** column. The **Modify Process Monitoring** page is displayed.
4. Modify the description, specified resources, and name of the monitored process. For details about the parameters, see [Table 3-23](#).
5. Click **OK**.

Deleting a Process Monitoring Task

1. Log in to the [Cloud Eye console](#).
2. Choose **Server Monitoring** > **Process Monitoring**.
3. Locate the target process monitoring task and click **Delete** in the **Operation** column.
4. In the **Delete Monitored Process** dialog box, enter **DELETE** and click **OK**.

Viewing Process Monitoring Metrics

1. Log in to the [Cloud Eye console](#).
2. Choose **Server Monitoring** > **Process Monitoring**.
3. Click  in the **Monitoring** column of a process monitoring task to go to the **View Metric** page.
4. Set **Instance**, **Process Name**, and **Process ID** to view the CPU usage, memory usage, and number of opened files of a specified process in line graphs. For details about related metrics, see [Table 3-24](#).
5. On the **View Metric** page, select a monitoring period (**Last 15 min**, **Last 30 min**, **Last 1h**, **Last 2h**, **Last 3h**, **Last 12h**, **Last 1d**, **Last 7d**, or **Last 30d**), or select **Select Range** to customize one to view historical monitoring data from the last 155 days.

Viewing Custom Process Monitoring

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - 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**.
3. On the **Server Monitoring** page, locate the ECS and click **View Metric** to go to the **OS Monitoring** page.
4. Click the **Process Monitoring** tab.
5. Under **Custom Process Monitoring**, locate a custom process and click  on the left of the process name.
6. Locate the row containing the target process ID and click **View Details** in the **Operation** column. On the **View Metric** drawer that is slid out, view the CPU usage, memory usage, and number of opened files of the current process. For details about the metrics, see [Table 3-24](#). Above the graphs, **Time Range** can be **Last 1h**, **Last 3h**, **Last 12h**, **Last 1d**, or **Last 7d**. You can also customize the time range to view historical monitoring data for any period within the last 155 days.
7. In the **Custom Processes** area, details of custom processes running on the host is displayed.

Table 3-24 Process Monitoring metrics

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
CPU Usage	CPU consumed by a process	0 to 1 x Number of CPU cores	Monitored object: ECSs or BMSs Check the metric value changes in the /proc/pid/stat file.	Monitored object: ECSs or BMSs Call the Windows API GetProcessTimes to obtain the CPU usage of the process.
Memory Usage	Memory consumed by a process	0 to 1	Monitored object: ECSs or BMSs Memory Usage = RSS x PAGESIZE / MemTotal RSS : Obtain its value by checking the second column of the /proc/pid/statm file. PAGESIZE : Obtain its value by running the getconf PAGESIZE command. MemTotal : Obtain its value from the /proc/meminfo file.	Monitored object: ECSs or BMSs Call Windows API procGlobalMemoryStatusEx to obtain the total memory size. Call GetProcessMemoryInfo to obtain the used memory size. Use the used memory size to divide the total memory size to get the memory usage.

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Open ed Files	The number of opened files consumed by the process	≥ 0	Monitored object: ECSs or BMSs You can run the <code>ls -l /proc/pid/fd</code> command to view the number.	Monitored object: ECSs or BMSs Run Windows API NtQuerySystemInformation to obtain information about all opened handles in the system, check whether each handle is a file handle opened by the current process, and obtain the number of files opened by the current process. In Windows, the specified_process_file metric of some processes cannot be collected due to causes like insufficient permissions.

Enabling Alarm Notifications for Custom Process Monitoring

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

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - 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**.
3. On the **Server Monitoring** page, locate the ECS and click **View Metric** to go to the **OS Monitoring** page.
4. Click the **Process Monitoring** tab.
5. On the **Custom Process Monitoring** page, create an alarm rule for a process by using either of the following methods:

- Locate a process and click **Create alarm rules** in the **Operation** column.
 - Click the  icon next to the process name and click **Create Alarm Rule** in the row where the process ID is located.
6. Configure basic information about the alarm rule. For details, see [5.2.2 Creating an Alarm Rule and Notifications](#).

Querying the System Processes

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

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

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - 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**.
3. On the **Server Monitoring** page, locate the ECS and click **View Metric** to go to the **OS Monitoring** page.
4. Click the **Process Monitoring** tab.

In the **System Processes** area, the process information is displayed. [Table 3-25](#) describes the metrics of system processes.

Table 3-25 System process metrics

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Running Processes	Number of processes that are running	≥ 0	Monitored object: ECSs or BMSs 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

Metri c	Description	Value Rang e	Collection (Linux)	Collection (Windows)
Idle Proces ses	Number of processes that are idle	≥ 0	Monitored object: ECSs or BMSs 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
Zombi e Proces ses	Number of zombie processes	≥ 0	Monitored object: ECSs or BMSs 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
Blocke d Proces ses	Number of processes that are blocked	≥ 0	Monitored object: ECSs or BMSs 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
Sleepi ng Proces ses	Number of processes that are sleeping	≥ 0	Monitored object: ECSs or BMSs You can obtain the state of each process by checking the Status value in the /proc/pid/ status file, and then collect the total number of processes in each state.	Not supported

Metric	Description	Value Range	Collection (Linux)	Collection (Windows)
Total Processes	Total number of processes	≥ 0	Monitored object: ECSs or BMSs 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: ECSs or BMSs Obtain the total number of processes by using the system process status support module psapi.dll .

Viewing Top Processes with the Highest CPU Usage

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

NOTE

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

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

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - 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**.

3. On the **Server Monitoring** page, locate the ECS and click **View Metric** to go to the **OS Monitoring** page.
4. Click the **Process Monitoring** tab.
5. Click **Configure** under **TOP 5 Processes with Highest CPU Usage**.
6. In the displayed **TOP 5 Processes with Highest CPU Usage** dialog box, enable monitoring for target processes and click **OK**.

Locate a process and click **View Details** in the **Operation** column. On the **View Metric** drawer that is slid in, view the CPU usage, memory usage, and number of opened files of the process. For details about the metrics, see [Table 3-26](#). Above the graphs, **Time Range** can be **Last 1h**, **Last 3h**, **Last 12h**, **Last 1d**, or **Last 7d**. You can also customize the time range to view historical monitoring data for any period within the last 155 days.

Table 3-26 Process Monitoring metrics

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

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

3.2.5 Creating an Alarm Rule to Monitor a Server

To monitor the resource usage for servers, you can access the **Server Monitoring** page and create alarm rules and configure alarm notifications for specified resources. In this way, you will be notified immediately after the set thresholds are reached. This topic describes how to create an alarm rule to monitor specified resources of an ECS or BMS.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**).
3. Locate the target ECS or BMS and click **Create Alarm Rule** in the **Operation** column.
4. On the **Create Alarm Rule** page, configure parameters.
 - a. Configure the alarm rule name, description, and associated enterprise project.

Table 3-27 Parameter description

Parameter	Description
Name	Alarm rule name. The system generates a random name, which you can modify. The rule name cannot exceed 128 characters and can contain only letters, digits, underscores (_), and hyphens (-). Example value: alarm-b6al
Description	(Optional) Alarm rule description. It can contain up to 256 characters.

- b. Select monitored objects and configure alarm parameters.

Table 3-28 Parameter description

Parameter	Description	Example Value
Alarm Type	Alarm type that the alarm rule applies to. The default value is Metric .	Metric
Cloud Product	Name of the monitored service. By default, it is the cloud service that the selected resource belongs to. For details about supported cloud products and their metrics, see 10 Cloud Product Metrics .	Elastic Cloud Server - ECSs
Resource Level	Resource level of the monitored object. When you create an alarm rule for a specified resource in Server Monitoring , the resource level is set to Cloud product by default.	Cloud Product
Monitoring Scope	Monitoring scope the alarm rule applies to. When you create an alarm rule for a specified resource in Server Monitoring , the monitoring scope is set to Specific resources by default.	Specific resources
Instance	You do not need to set this parameter because it is the resource you selected.	-
Method	Method for configuring an alarm policy. The options are as follows: • Configure manually: You can create a custom alarm policy as needed. • Associate template: If you need to configure the same alarm rule for multiple groups of resources under the same cloud product, you can use an alarm template to simplify operations.	Configure manually
Template	Select the template to be imported. This parameter is mandatory when Method is set to Associate template . You can select a default or custom template .	-

Parameter	Description	Example Value
Alarm Policy	If you select Configure manually for Method, you need to configure alarm policies. For example, an alarm is triggered if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. Cloud Eye triggers an alarm every one hour again if the alarm persists. You can add up to 50 alarm policies for a single alarm rule. You can choose to send alarm notifications when any of the policies is met or when all policies are met. For details about alarm policy parameters, see 5.2.3 Alarm Policies. For details about basic and OS monitoring metrics, see 10 Cloud Product Metrics. NOTE If the alarm is not cleared after it is generated, an alarm notification is sent, once every hour.	-

- c. Configure alarm notifications.

Table 3-29 Parameters for configuring alarm notifications

Parameter	Description
Alarm Notifications	Whether to send alarm notifications by SMS, email, HTTP, or HTTPS. This parameter is enabled by default.
Recipient	Target recipient of alarm notifications. You can select the account contact or a topic. This parameter is available only if Notified By is set to Topic subscriptions. If there is a display name of a topic, the format is <i>Topic name (Display name)</i>, and you can search for a topic by name or display name. If no display name is set for a topic, only the topic name will be displayed. - The account contact is the mobile number and email address of the registered account. - A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see 5.5.1.1 Creating a Topic and 5.5.1.2 Adding Subscriptions. For the HTTP/HTTPS messages, see Simple Message Notification User Guide.

Parameter	Description
Notification Window	Notification window during which Cloud Eye only sends notifications. If you set Notification Window to 08:00 to 20:00, Cloud Eye only sends notifications within this period.
Time Zone	Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured.
Trigger Condition	Condition that will trigger an alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.

- d. Select an enterprise project.

Figure 3-5 Advanced settings

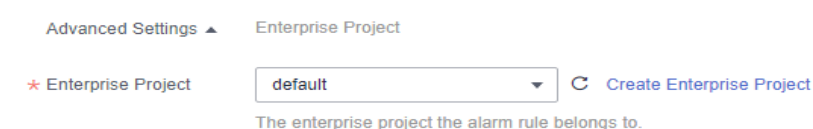


Table 3-30 Parameter of **Advanced Settings**

Parameter	Description
Enterprise Project	Enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can manage the alarm rule. To create an enterprise project, see Creating an Enterprise Project .

- e. Click **Create**.

After the alarm rule is created, if a metric reaches the specified threshold, Cloud Eye immediately informs you of the exception through SMN.

3.2.6 Viewing Resource Details

As cloud resources continue to grow, identifying the resource group for a specific resource becomes challenging. You can view resource details to learn the resource group and instance details. This section describes how to view resource details in **Server Monitoring**.

Procedure

1. Log in to the [Cloud Eye console](#).
2. Perform the following operations based on your resources.
 - In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.

- In the navigation pane, choose **Server Monitoring > Bare Metal Server**.
- 3. Locate the target resource and click **View Metric** in the **Operation** column. The metric details page is displayed.
- 4. Click **View Resource Details** in the upper right corner.
- 5. On the displayed page, view the instance name, instance ID, and resource group of the resource.
- 6. Click the name of the resource group to be viewed to go to its details page.

3.3 Cloud Service Monitoring

3.3.1 Overview

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 monitoring data.

What You Can Do with Cloud Service Monitoring

- Viewing metrics: You can view the graphs of monitoring data collected in the last 1 hour, 3 hours, 12 hours, 1 day, 7 days, and 30 days. You can customize the metrics to be viewed and view monitoring data that is automatically updated.
- Create alarm rules: You can create alarm rules for key metrics of cloud services. When the conditions in the alarm rule are met, Cloud Eye notifies you by email, SMS, or HTTP/HTTPS message, so you can quickly respond to resource changes and avoid unnecessary loss.
- Exporting monitoring data: Cloud Service Monitoring allows you to export a maximum of 10 monitoring items in your selected time range and rollup 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.

3.3.2 Viewing a Cloud Service Dashboard

Cloud Eye automatically obtains resources of cloud services connected to your account and creates dashboards for each cloud service. You can view graphs of each cloud service to learn about their running statuses. You can also set alarm rules and notifications to monitor the resource performance. If a metric surpasses its limit, Cloud Eye alerts you immediately, keeping you informed in real time.

Constraints

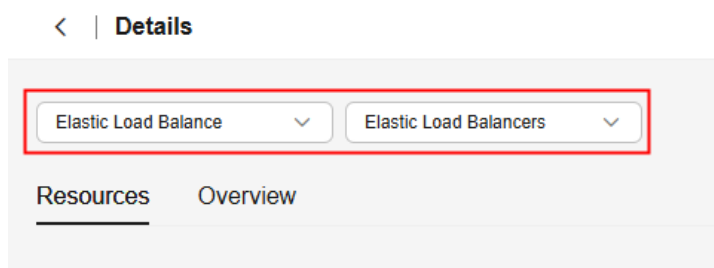
- CDN monitoring data is sent to Cloud Eye with a 5-minute delay, so you cannot see the latest 5 minutes of data on the graph.
- On the monitoring details page, the top *N* graphs cannot compare data from yesterday or last month.

- After you change the name of a cloud service, the resource name on the dashboard will be updated 12 hours later.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Cloud Service Monitoring**.
3. Click the name of the cloud service dashboard you want to view.
4. On the cloud service monitoring details page, view service details on the **Overview** and **Resources** pages.
5. In the upper left corner of the cloud service dashboard details page, select another dimension to view corresponding monitoring details or select another cloud service to switch to its dashboard.

Figure 3-6 Selecting another cloud service



6. On the **Resources** tab, perform the following operations:
 - Click **Export Data** to export cloud service monitoring data. For details, see [Exporting Monitoring Data](#)
 - Locate the target instance and click **View Metric**. On the displayed page, click **View Resource Details** in the upper right corner to view the resource groups that the resources belong to.
 - Locate an instance and choose **More > Create Alarm Rule** to create an alarm rule for the instance. For details about the parameters, see [5.2.2 Creating an Alarm Rule and Notifications](#).
 - Locate an instance and choose **More > View Alarm Rule** in the **Operation** column to view the alarm rules created for the instance.
7. On the service overview page, view details under **Resource Overview**, **Alarm Statistics**, and **Key Metrics**. For details, see [Table 3-31](#).

Table 3-31 Three modules on the **Overview** tab

Module	Description
Resource Overview	You can view the resource data of the current cloud service in the current dimension, for example, you can see Total Resources , Resources With Alarms , and Resources With Alarms in the Last 7 Days .

Module	Description
Alarm Statistics	You can view the total number of alarms from the last seven days and the number of alarms at different severities (critical, major, minor, and warning). You can also view the top 5 instances and resource groups with the most alarms.
Key Metrics	You can view monitoring details of key metrics recommended by the cloud service.

3.3.3 Viewing Raw Data

This topic describes how you can view the raw data saved in the OBS bucket by downloading metric data files.

Constraints

This operation is only supported on **Cloud Service Monitoring** of the earlier Cloud Eye edition.

Prerequisites

- You have successfully configured data storage on Cloud Eye.

Procedure

- Log in to the [Cloud Eye console](#).
- In the navigation pane, choose **Cloud Service Monitoring**. Click the name of the cloud service. On the displayed **Details** page, click **Earlier Edition** in the upper right corner.
- Locate the cloud service resource to be viewed and click the OBS bucket name in the **Permanent Data Storage** column.

Alternatively, in the navigation pane, choose **Server Monitoring**. Locate the ECS and select the specified OBS bucket in the **Permanent Data Storage** column.

- Select the metric data file you want to view in the OBS bucket. Based on the storage path of the metric data file, select *OBS bucket name > CloudEye > Region > Year > Month > Day > Service type directory > Resource type directory*. Click **Download** in the **Operation** column to download the file to the default path. To download the metric data file to a customized path, click **Download As**.

The metric data file is named in the following format:

Metric data file prefix_CloudEye_Region_Time when the log was uploaded to the OBS: year-month-dayT hour-minute-secondZ_Randomly generated character.json.gz

Example: *File*

Prefix_CloudEye_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.json

 NOTE

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

3.3.4 Cloud Services Displayed in the Cloud Service Monitoring List

Some connected cloud services may not appear in the monitoring list. If no monitoring data is reported for all instances of a cloud service for a certain period of time, the cloud service will not be displayed in the list.

For cloud services listed in [Table 3-32](#), if all instances of a cloud service have not reported any data to Cloud Eye for more than three hours but less than seven days, the cloud service remains on the cloud service monitoring list. However, if no data is sent for more than seven days, the service will be removed from the list.

For other cloud services, if all instances of a cloud service have not reported any data to Cloud Eye for more than three hours, this cloud service will not be displayed in the service list.

Table 3-32 Cloud services with their monitoring data retained for seven days

Cloud Service	Namespace
API Gateway	SYS.APIG
Object Storage Service	SYS.OBS
FunctionGraph	SYS.FunctionGraph
Dedicated API Gateway	SYS.APIC
Data Ingestion Service	SYS.DAYU
DataArts Studio	SYS.DATAARTS_MIGRATION
Scalable File Service	SYS.SFS
Live	SYS.LIVE
API Calling	SYS.APIGATEWAY

3.4 Task Center

On **Data Center**, you can view details of the data export tasks you created on the **Alarm Records**, **Server Monitoring**, and **Cloud Service Monitoring** pages, or the

Agent installation tasks you created on the **Server Monitoring** page. You can also download or delete those tasks.

Constraints

- Export tasks created in the **Exporting Monitoring Data**, **Exporting Alarm Records**, or **Exporting the Server List** section will be cleared seven days after they were created.
- The tasks in **Agent Maintenance** will be cleared three months after they were created.

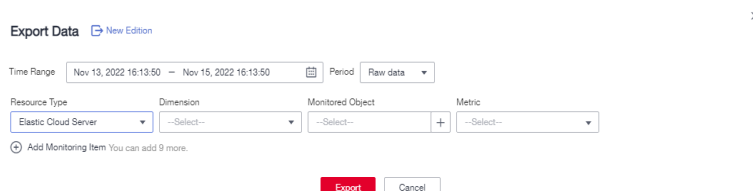
Exporting Monitoring Data

1. Log in to the [Cloud Eye console](#).
2. On the **Resources** tab page, select the resource whose monitoring data you want to export and click **Export Data**.
3. To export the monitoring data of an ECS or BMS, go to the server monitoring page.
 - a. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**).
 - b. Above the server list, choose **Export** > **Export Data**.

NOTE

By default, the **Export Data** dialog box of the new edition is displayed. To return to the earlier edition, click **Earlier Edition** (see [Figure 3-7](#)). For the earlier edition, the data export task is not displayed on the **Task Center** page and can be downloaded on the current page.

Figure 3-7 Earlier edition of the **Export Data** dialog box



4. In the **Export Data** dialog box, configure parameters.

Table 3-33 Parameters for exporting data

Parameter	Description
Task Name	Name of the task for exporting monitoring data. The value can contain 1 to 32 characters, including only letters, digits, underscores (_), and hyphens (-).

Parameter	Description
Statistic	Monitoring data statistics method, which can be Aggregated data or Raw data . • Aggregated data: The aggregated maximum value, minimum value, average value, or sum value can be exported. • Raw data: The raw data is exported.
Time Range	Select the time range of the monitoring data to be exported. • Aggregated data from the last 90 days can be exported. • Raw data from the last 48 hours can be exported.
Aggregated By	Aggregation interval of aggregated data. This parameter is mandatory when Statistic is set to Aggregated data . You can select Custom range , Week , Day , or Hour . 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.
Metrics	Select the resource and metrics for exporting data. • Cloud Product: The selected cloud service and dimension are used by default. • Resource Scope: You can select All resources, Resource group, Enterprise project, or Specified resource. If you select Resource groups or Enterprise projects for Resource Scope, the metrics you select later must be included in the enterprise project or resource group. Otherwise, the exported monitoring data will be empty. • Metrics: Specify the metrics to be exported.

5. Click **OK**.
6. Choose **Task Center**. On the **Monitoring Data Export Tasks** tab, view and download the task.
7. Locate the task and click **Download** in the **Operation** column to download the exported monitoring data.
8. Locate a task and click **Delete** in the **Operation** column, or select multiple tasks and click **Delete** above the list to delete the exported monitoring data.

Exporting Alarm Records

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Records**.
3. On the **Alarm Records** page, filter desired alarm records and click **Export**.
4. In the displayed **Export Alarm Records** dialog box, set parameters based on [Table 2](#).

Table 3-34 Parameters for exporting alarm records

Parameter	Description
Task Name	Name of the task for exporting alarm records. The value can contain 1 to 32 characters, including only letters, digits, underscores (_), and hyphens (-).
Fields	Fields of the alarm records to be exported. You can select Record ID, Status, Alarm Severity, Alarm Generated, Last Updated, Alarm Duration, Alarm Type, Resource Type, Abnormal Resource, Alarm Policy, Alarm Rule Name, Alarm Rule ID, or Notification Cause. Multiple options can be selected. Abnormal Resource is mandatory. NOTE • If Notified By is set to Notification policies in Alarm Notifications and the notification policy has been deleted, selecting the Notified By field during data export will not show the policy name in the exported alarm records. • Some cloud service resources may not contain the resource name in the exported data. This issue is being resolved.

5. Click **Export** to submit the export task.
6. After the export task is submitted, click **Task Center**. On the **Alarm Data Export Tasks** tab page, click **Alarm Record Export Tasks** to view the tasks or download the export result.
7. On the **Alarm Record Export Tasks** tab, to delete a task, locate it and click **Delete** in the **Operation** column; to delete multiple tasks, select them and click **Delete** above the list.

Exporting Alarm Rules

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Rules**.
3. On the displayed page, filter alarm rules as needed, or select the alarm rules to be exported and click **Export**.
4. In the displayed **Export Alarm Rules** dialog box, set parameters based on [Table 3-35](#).

Table 3-35 Parameters for exporting alarm rules

Parameter	Description
Task Name	Name of the task for exporting alarm rules. The value can contain 1 to 32 characters, including only letters, digits, underscores (_), and hyphens (-).

Parameter	Description
Fields	Fields contained in the alarm rules to be exported. You can select Alarm Rule Name , Alarm Rule ID , Resource Type , Monitored Objects , Alarm Policy , Status , Notification Cause , Tags , Alarm Masking Status , Created , or Modified . Multiple options can be selected. Alarm Rule Name and Alarm Rule ID are mandatory. NOTE Some cloud services do not display the resource name in the exported data of the current alarm rules. This issue is being resolved.
Export Specific Resources	The data to be exported contains specific resources monitored by Cloud Eye. You can choose whether to export the specified resource list as needed.

- Click **Export** to submit the export task.
- After the export task is submitted, click **Task Center**. On the **Alarm Data Export Tasks** tab page, click **Alarm Rule Export Tasks** to view the tasks or download the export result.
- On the **Alarm Rule Export Tasks** tab, to delete a task, locate it and click **Delete** in the **Operation** column; to delete multiple tasks, select them and click **Delete** above the list.

Exporting the Server List

- Log in to the [Cloud Eye console](#).
- In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**).
- On the **Server Monitoring** page, filter the resources to be exported and choose **Export** > **Export Server List**.
- In the displayed **Export Server List** dialog box, set parameters based on [Table 3-36](#).

Table 3-36 Parameters for exporting the server list

Parameter	Description
Task Name	Name of the server exporting task. The value can contain 1 to 32 characters, including only letters, digits, underscores (_), and hyphens (-).
Fields	Select the fields contained in the server list to be exported. You can select ID , Name , Elastic IP Address , Private IP Address , ECS Status , Agent Status , Agent Edition , Enterprise Project , Tags , Created , Region , Server Name , OS , Agent Edition Type , Flavor , and Image .

5. Click **Export**.
6. After the export task is submitted, click **Task Center**. On the **Server List Export** tab page, you can view the task details and download the export result.
7. On the **Server List Export** tab, to delete a task, locate it and click **Delete** in the **Operation** column; to delete multiple tasks, select them and click **Delete** above the list.

4 My Dashboards

- [4.1 Overview](#)
- [4.2 Creating a Dashboard](#)
- [4.3 Adding a Graph](#)
- [4.4 Viewing a Graph](#)
- [4.5 Configuring a Graph](#)
- [4.6 Deleting a Graph](#)
- [4.7 Deleting a Dashboard](#)

4.1 Overview

You can use dashboards to view core metrics and compare the performance data of different services.

You can create or delete a dashboard, and add graphs to the dashboard to view custom monitoring data. You can also edit or delete the graphs on the dashboard.

4.2 Creating a Dashboard

You can create a dashboard to monitor metrics. Before adding graphs, you need to create a dashboard first.

Constraints

You can create a maximum of 10 dashboards.

Procedure

1. Log in to the [Cloud Eye console](#).
2. Choose **My Dashboards** and click **Create Dashboard**.
The **Create Dashboard** dialog box is displayed.

3. 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.

4. Click **OK**.

4.3 Adding a Graph

If you are using multiple cloud services, you can add their metrics to the same dashboard by creating graphs. This way, you can view global monitoring data of these cloud services.

In the same graph, you can compare data across services, dimensions, and metrics.

Constraints

- You can add a maximum of 50 graphs to a dashboard.
- You can add a maximum of 50 monitoring metrics to a graph.
- If **Monitoring Scope** is set to **Resource groups** and the selected resource group contains an EVS resource with the type in the format of *ECS instance ID-volume-Volume ID*, you cannot check the monitoring data of this instance.

Prerequisites

You have created a dashboard by referring to [4.2 Creating a Dashboard](#).

Procedure

1. Log in to the [Cloud Eye console](#).
2. Choose **My Dashboards** and click the name of the dashboard to which you want to add a graph. On the displayed page, click **Create > Create Graph** or **Create Graph Group**.

You can create a graph or a graph group. In this example, click **Create Graph**. The **Create Graph** dialog box is displayed.
3. On the **Create Graph** page, perform the following operations:
 - a. Set **Graph Type** to **Line chart**, **Stacked area line chart**, **Bar chart**, **Horizontal bar chart**, **Donut chart**, or **Table chart**.
 - b. On the **Graph Settings** area on the right, select **One graph for a single metric** or **One graph for multiple metrics** (only for line charts, area charts, or table charts). In this example, select **One graph for multiple metrics**. Under **Graph Group**, select an existing group or click **Create Graph Group** to create one.
 - c. In the **Monitoring Item Configuration** area, set the monitoring scope, set **Order**, and set **Quantity**.

 NOTE

For **Bar chart**, **Horizontal bar chart**, **Table chart**, and **Donut chart**, set **Quantity** to an integer from 3 to 10. For **Line chart** and **Stacked area line chart**, set **Quantity** to an integer from 1 to 50.

- d. In the monitoring scope area, select **Left Y axis** or **Right Y axis**. View the configured chart in the **Preview** area.
 - e. In the **Graph Settings** area, set **Remarks (Optional)**. Select an option from **Location** and an option from **Legend Value**. Set **Threshold** and select a color.
4. Click **Finish**.

4.4 Viewing a Graph

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

Constraints

CDN monitoring data is sent to Cloud Eye with a 5-minute delay. So, you cannot see the latest 5 minutes of data on the graph.

Viewing All Graphs on a Dashboard

You can view all graphs on a dashboard on its details page.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Click the name of a dashboard and view all graphs on it.
4. In the upper right corner of the page, select a default or custom time range from the drop-down list in the upper right corner to view metrics of a cloud service.

After selecting the monitoring period and aggregation type, click **Save** in the upper part of the page to save the configuration. When you access the dashboard again, the data trends of the configured period and type will be displayed by default.

5. Select a graph layout from the third drop-down list in the upper right corner of the page. The options are **Auto-adaptive**, **1 per row**, **2 per row**, **3 per row**, and **4 per row**.

You can also drag and drop graphs to sort graphs.

6. Select a graph refresh interval from the fourth drop-down list in the upper right corner of the page. The options are **Turn off refresh**, **Refresh every 10 seconds**, **Refresh every 1 minute**, **Refresh every 5 minutes**, and **Refresh every 20 minutes**.

Click **Save** in the upper part of the page to save the configuration. When you access the dashboard again, the monitoring data is refreshed at the selected interval by default.

7. Click  in the upper right corner of the page to refresh all graphs on the dashboard.
8. Check graphs on the full screen for clearer visibility.
 - To enter the full screen, click **Full Screen** in the upper part of the page.
 - To exit the full screen, press **Esc**.

Viewing a Single Graph

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Click the name of a dashboard and view all graphs on it.
4. Move the cursor to the target graph. Click  in the upper right corner of the graph to refresh the data.
5. Click  in the upper right corner of the graph to view monitoring data details in a table.

NOTE

You can view monitoring data directly in a graph of the donut chart or table type. Tables show specific values in columns. Donut charts display specific values on the right.

6. Click  in the upper right corner of the graph to set the number of metrics displayed and the sorting rule. This updates the metric sequence.

NOTE

Line charts and stacked area line charts show data trends over time. Sorting by metric does not reveal these trends, so this feature is not available for those charts.

7. Click  in the upper right corner of the graph to go to its details page.
 - In the upper right corner of the details page, select a default time range or customize one to view the metrics.

The time granularity varies depending on the monitoring period and . For details, see [Aggregation Types and Time Granularities for Different Monitoring Periods](#). For details about the aggregation methods supported by Cloud Eye, see
 - You can click and drag on a line chart or stacked area line chart to check data in a specified period.
 - i. Click the start time and drag to the end time. The system automatically displays the monitoring data within the selected time range.
 - ii. Click  in the upper right corner to reset the time range.

Aggregation Types and Time Granularities for Different Monitoring Periods

Table 4-1 Time granularities for different aggregation types in different monitoring periods

Monitoring Period	Aggregation Type	Time Granularity
Last 15 min	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 30 min	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 1h	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 2h	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 3h	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 12h	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	

Monitoring Period	Aggregation Type	Time Granularity
Last 1d	Avg.	• 1 minute • 5 minutes • 20 minutes • 1 hour
	Max.	
	Min.	
	Sum	
Last 7d	Avg.	• 20 minutes • 1 hour • 4 hours • 24 hours
	Max.	
	Min.	
	Sum	
Last 30d	Avg.	• 1 hour • 4 hours • 24 hours
	Max.	
	Min.	
	Sum	

4.5 Configuring a Graph

If the existing metrics do not meet your requirements, you can add, modify, and delete metrics on a line chart or bar chart.

Copying a Graph

You can copy an existing graph to quickly create one.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Locate the dashboard for which you want to copy a graph and click its name.
4. Move the cursor to the target graph, click *** in the upper right corner of the graph, and click **Copy**.
5. In the **Copy** dialog box, set the parameters.

Table 4-2 Copying a monitoring graph

Parameter	Description	Example Value
From	Target location of the new graph. You can select Current dashboard or Other dashboards .	Other dashboards

Parameter	Description	Example Value
Enterprise Project	Enterprise project to which the target dashboard belongs. This parameter is required when you set From to Other dashboards .	default
Target Dashboard	Target dashboard. This parameter is required when you set From to Other dashboards . All dashboards in the selected enterprise project are displayed.	--
Graph Group (Optional)	Group the new graph belongs to.	--

6. Click **OK**. The page for editing the graph is displayed.
7. Modify the parameters as required and click **Save**.
The graph is added to the selected dashboard.

Editing a Graph

You can edit a graph if it cannot meet your needs.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Locate the dashboard for which you want to edit a graph and click its name.
4. Move the cursor to the target graph, click ******* in the upper right corner of the graph, and click **Edit**.
5. On the **Edit Graph** page, modify parameters as required.
6. Click **Save**. The graph is edited.

Moving a Graph to Another Group

To compare graphs across different groups on a dashboard, you can move one graph to other groups for better comparison.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Locate the dashboard for which you want to move a graph and click its name.
4. Move the cursor to the target graph, click ******* in the upper right corner of the graph, and click **Move to Another Group**.
5. In the **Select Group** dialog box, select the target graph group.
6. Click **OK**.
The graph is moved to the selected group.

Changing Legend Names

You can change legend names for a graph only when **Monitoring Scope** of the graph is set to **Specific resources** and **Aggregation** is disabled or **Aggregation Settings** is not set to **All resources of the current user**.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Locate the dashboard with the graph for which you want to change legend names and click the dashboard name.
4. Move the cursor to the target graph, click *** in the upper right corner of the graph, and click **Change Legend Name**.
5. In the **Change Legend Name** dialog box, enter legend names.
6. Click **OK**.

The legend names of the graph are changed.

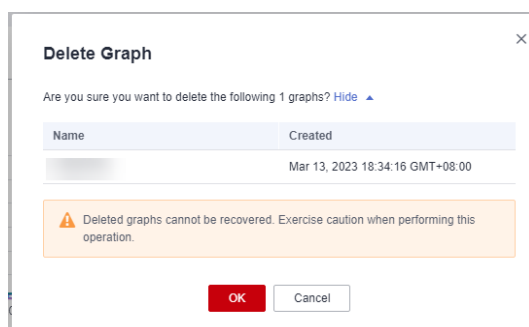
4.6 Deleting a Graph

If there are service changes or you need to replan parameters for a graph, you can delete the graph.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
3. Locate the dashboard from which you want to delete a graph and click the dashboard name.
4. Click *** and choose **Delete**.
5. In the displayed **Delete Graph** dialog box, click **OK**.

Figure 4-1 Deleting a graph



4.7 Deleting a Dashboard

If an existing dashboard cannot meet your requirements, you can delete it and replan 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 [Cloud Eye console](#).
2. In the navigation pane, choose **My Dashboards**.
 - To delete a single dashboard, click **Delete** in the **Operation** column of the dashboard.
 - To delete multiple dashboards, select the check boxes of the dashboards and click **Delete** above the list.
3. In the displayed **Delete Dashboard** dialog box, click **OK**.

5 Alarm Management

[5.1 Overview](#)

[5.2 Alarm Rules](#)

[5.3 Alarm Records](#)

[5.4 Alarm Templates](#)

[5.5 Alarm Notifications](#)

[5.6 One-Click Monitoring](#)

[5.7 Alarm Masking](#)

5.1 Overview

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

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

NOTE

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

5.2 Alarm Rules

5.2.1 Overview

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

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.

You can enable **Alarm Notifications** when creating alarm rules. When a metric reaches the threshold specified in an alarm rule, Cloud Eye will notify you by email, HTTP or HTTPS message. You can track the service status and establish programs accordingly to handle the alarms.

Table 5-1 Applicable scenarios

Alarm Type	Scenario
Metric	Cloud Eye can collect metric data of cloud services, such as CPU usage and memory usage. You can monitor metrics to track the status of cloud services. You can set alarm rules and notifications for core service metrics. When a metric triggers the preset threshold, Cloud Eye sends you a notification. This helps you identify and handle abnormal monitoring data in real time.
Event	Events are key operations or statuses of a cloud service, for example, restarting a VM. You can set event alarm rules for key business events or cloud resource operations. When a specified event occurs, Cloud Eye automatically sends an alarm notification. This helps you quickly identify and address issues.

5.2.2 Creating an Alarm Rule and Notifications

To monitor the usage of cloud service resources or key operations on them, you can create an alarm rule. After the alarm rule is created, if a metric reaches the specified threshold or the specified event occurs, Cloud Eye immediately informs you of the exception through SMN.

This topic describes how to create an alarm rule.

Prerequisites

Alarm Type	Prerequisites
Metric	- Before creating a metric alarm rule for a cloud service, ensure that its instances have automatically reported monitoring data to Cloud Eye. - Before creating an alarm rule for Agent metrics, ensure that Agent has been installed on the server. For details, see 3.2.2.3 Installing the Agent. - Before creating an alarm rule for process monitoring metrics, ensure that you have added custom processes for monitoring. For details, see Adding Processes for Monitoring.
Event	Before creating an alarm rule for a custom event, ensure that the event source is the same as that specified in Reporting Events .

Creating an Alarm Rule

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
3. Click **Create Alarm Rule** in the upper right corner.
4. On the **Create Alarm Rule** page, configure parameters.
5. Configure basic information about the alarm rule.

Figure 5-1 Basic information

The screenshot shows a form with two fields. The first field is labeled '★ Name' and contains the text 'alarm-a8tc'. The second field is labeled 'Description' and is empty, with a character count '0/256' and a refresh icon at the bottom right.

Table 5-2 Parameter description

Parameter	Description
Name	Name of the alarm rule. The name is automatically generated, but you can change it to a custom one. The rule name cannot exceed 128 characters and can contain only letters, digits, underscores (_), and hyphens (-).
Description	(Optional) Alarm rule description. It can contain up to 256 characters.

6. Select monitored objects and configure alarm parameters.

Figure 5-2 Configuring an alarm rule

★ Alarm Type: **Metric** (selected) | Event

★ Cloud Product: Elastic Cloud Server - ECSs

★ Resource Level: Cloud product (selected) | Specific dimension

★ Monitoring Scope: All resources (selected) | Resource groups | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.
[Select Resources to Exclude](#)

★ Method: Associate template (selected) | Configure manually

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

★ Template: --Select-- | [Create Custom Template](#)

Table 5-3 Alarm rule parameters

Parameter	Description	Example Value
Alarm Type	Alarm type to which the alarm rule will apply. The type can be Metric or Event . For details about how to select an alarm type, see Table 5-1 .	Metric
Cloud Product	Select the cloud product you want to monitor. This parameter is only available if you select Metric for Alarm Type . For details about supported cloud products and their metrics, see 10 Cloud Product Metrics .	Elastic Cloud Server - ECSs
Resource Level	Resource level of the monitored object. This parameter is only available if Alarm Type is set to Metric . The value can be Cloud product (recommended) or Specific dimension . Take ECS as an example. ECS is the cloud product. Specific dimensions are disks, mount points, processes, and more. NOTE If you select Cloud product , metrics across dimensions (such as Disk Usage and CPU Usage) can be configured in the same alarm rule. If you select Specific dimension , only metrics of the specified dimension can be configured for the same alarm rule.	Cloud product

Parameter	Description	Example Value
Monitoring Scope	Monitoring scope the alarm rule applies to. • All resources: An alarm will be triggered if any resource of the selected cloud product meets the alarm policy. To exclude resources that do not need to be monitored, click Select Resources to Exclude. • Resource groups: An alarm will be triggered if any resource in the selected resource group meets the alarm policy. To exclude resources that do not need to be monitored, click Select Resources to Exclude. • Specific resources: Click Select Specific Resources to select resources. NOTE • If Alarm Type is set to Metric, you can select Resource groups, All resources, or Specific resources. • If Alarm Type is set to Event and Event Type is set to System event, you can configure the monitoring scope. Currently, Resource groups is only available for DDS, RDS, and DCS event alarms.	Specific resources
Group	When Monitoring Scope is set to Resource groups, you need to select a group. If no resource group meets your needs, click Create Resource Group to create one. After selecting a resource group from the drop-down list, you can click View Resources in a Group to view the details of resources in the group. After an alarm rule is configured, the group cannot be modified. NOTE If the resource group contains an EVS resource with the type in the format of <i>ECS instance ID-volume-Volume ID</i>, the instance cannot report monitoring data after the alarm rule is created. As a result, no alarm can be triggered.	-
Instance	When Monitoring Scope is set to Specific resources, you need to select the monitored objects for the alarm rule. Click Select Specific Resources to select desired resources.	-
Event Type	This parameter is only available if Alarm Type is set to Event. You can select either System event or Custom event. For details about the events supported by each cloud service, see 6.4 Events Supported by Event Monitoring.	System event

Parameter	Description	Example Value
Event Source	This parameter is only available if Alarm Type is set to Event. • If Event Type is set to System event, select the cloud service from which the event comes. • If Event Type is set to Custom event, the event source must be the same as that of the reported source and written in the <i>service.item</i> format. For details about how to report an event, see Reporting Events.	Elastic Cloud Server
Method	Select a method for configuring an alarm rule. For metric alarm rules or system event alarm rules, you can customize a policy or use a preset template to create one. For custom event alarm rules, you can only customize a policy. • Configure manually: You can create a custom alarm policy as needed. • Associate template: If you need to configure the same alarm rule for multiple groups of resources under the same cloud product, you can use an alarm template to simplify operations.	Configure manually
Template	When you set Method to Associate template, you need to select a template. You can select a default or custom template. NOTE An alarm template may contain alarm policies of multiple cloud products or different dimensions of the same cloud product. When you create an alarm rule, the alarm policies vary according to the resource level. • When you set Resource Level to Cloud product, all alarm policies of the cloud product in the alarm template will be synchronized to the alarm rule. • When you set Resource Level to Specific dimension, only alarm policies of the same dimension as the current resource in the alarm template will be added to the alarm rule.	-

Parameter	Description	Example Value
Alarm Policy	When you set Method to Configure manually, you need to configure alarm policies. - When you set Alarm Type to Metric, whether to trigger an alarm depends on whether the data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. - If Alarm Type is set to Event and a specified event occurs, an alarm is triggered. For example, an alarm is triggered if a VM is restarted. For details about alarm policy parameters, see 5.2.3 Alarm Policies. You can add up to 50 alarm policies for a single alarm rule. You can choose to send alarm notifications when any of the policies is met or when all policies are met.	-
Alarm Severity	Alarm severity, which can be Critical , Major , Minor , or Warning .	Major

7. Configure alarm notifications.

Table 5-4 Parameters for configuring alarm notifications

Parameter	Description
Alarm Notifications	Whether to send alarm notifications by SMS, email, HTTP, or HTTPS. This parameter is enabled by default.
Recipient	Target recipient of alarm notifications. You can select the account contact or a topic. This parameter is available only if Notified By is set to Topic subscriptions. If there is a display name of a topic, the format is <i>Topic name (Display name)</i>, and you can search for a topic by name or display name. If no display name is set for a topic, only the topic name will be displayed. - The account contact is the mobile number and email address of the registered account. - A topic is used to publish messages and subscribe to notifications. If there is no topic you need, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.

Parameter	Description
Notification Window	If Notified By is set to Notification groups or Topic subscriptions, you need to set the notification window. Cloud Eye sends notifications only within the validity period specified in the alarm rule. For example, if the notification window is set to 08:00:00 to 20:00:00, notifications are sent only within this specified time range when a metric reaches the specified threshold or a specified event occurs.
Time Zone	Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured.
Trigger Condition	This parameter is required when you set Notified By to Notification groups or Topic subscriptions. • If you set Alarm Type to Metric, select Generated alarm, Cleared alarm, or both for this parameter. • If you set Alarm Type to Event, you can only select Generated alarm for this parameter.

8. Set parameters in **Advanced Settings**.

Figure 5-3 Advanced settings

Advanced Settings • Enterprise Project | Tag

Enterprise Project **default** Create Enterprise Project

The enterprise project the alarm rule belongs to.

Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

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

Enter a tag key Enter a tag value Add

20 tags available for addition.

Table 5-5 Parameter description

Parameter	Description
Enterprise Project	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 .
Tag	Key-value pairs that you can use to easily categorize and search for cloud resources. You are advised to create predefined tags in TMS. For details, see Creating Predefined Tags. • A key can contain up to 128 characters, and a value can contain up to 225 characters. • You can create up to 20 tags.

9. Click **Create**.

After the alarm rule is created, if a metric reaches the specified threshold, Cloud Eye immediately informs you of the exception through SMN.

5.2.3 Alarm Policies

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

Configuring Alarm Policies for Metrics

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

Table 5-6 Parameters for metric alarm policies

Parameter	Description	Example Value
Metric Name	Metric name. After selecting a metric, move the cursor to  on the right of the metric to view its description. For details about the monitoring metrics supported by cloud products, see 10 Cloud Product Metrics .	CPU Usage

Parameter	Description	Example Value
Statistic	Metric value type. Cloud Eye supports the following statistics for metrics: Raw data, Avg., Max., Min., Variance, and Sum. • Raw data indicates the metric data that is not processed or converted. • Avg. is the value calculated by averaging raw data during a rollup period. • Max. is the highest value observed during a rollup period. • Min. is the lowest value observed during a rollup period. • Variance: indicates the difference between each data point in the original value and the average value within a rollup period. • Sum is the sum of raw data during a rollup period. NOTE • An aggregation period can be 5 minutes, 20 minutes, 1 hour, 4 hours, or 24 hours. Select an aggregation period based on your service requirements. • If you set a rollup period, alarm notifications will be delayed. If you set the rollup period to 5 minutes, alarm notifications will be delayed for 10 to 15 minutes. If you set the rollup period to 20 minutes, alarm notifications will be delayed for 20 minutes. If you set the rollup period to 1 hour, alarm notifications will be delayed for 1 hour and 20 minutes. If you set the rollup period to 4 hours, alarm notifications will be delayed for 4 hours and 40 minutes. If you set the rollup period to 24 hours, alarm notifications will be delayed for 25 hours. • When selecting a rollup period, make sure it's longer than the metric reporting period. Otherwise, alarms may not be generated. For example, if the metric reporting period is 10 minutes, you cannot create an alarm policy with a 5-minute rollup period.	Raw data
Consecutive Triggering Times	Number of consecutive times that an alarm is triggered. The value can be set to 1, 2, 3, 4, 5, 10, 15, 30, 60, 90, 120, or 180 times (consecutively).	2 times (consecutively)

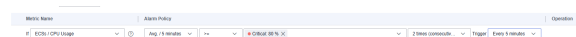
Parameter	Description	Example Value
Operator	Operator used to compare metric value and the threshold. Cloud Eye supports >, >=, <, <=, =, !=, Increase compared with last period, Decrease compared with last period, and Increase or decrease compared with last period. NOTE • Increase compared with last period: The metric data reported in the current monitoring period increases sharply when compared with that in the previous monitoring period. • Decrease compared with last period: The metric data reported in the current monitoring period decreases sharply when compared with that in the previous monitoring period. • Increase or decrease compared with last period: The metric data in the current monitoring period increases or decreases sharply when compared with that in the previous monitoring period.	=
Threshold and Alarm Severity	Threshold for triggering an alarm and alarm severity.	Critical: 22 Byte/s
Frequency	How often alarms are repeatedly notified when there is already an alarm. The following options are available: Trigger only one alarm, Every 5 minutes, Every 10 minutes, Every 15 minutes, Every 30 minutes, Every 1 hour, Every 3 hours, Every 6 hours, Every 12 hours, and One day. NOTE If the alarm is not cleared after it is generated, an alarm notification is sent, once every hour.	Every 5 minutes

Example of configuring an alarm policy for a metric

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

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

Figure 5-4 Alarm policy



Configuring Alarm Policies for Events

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

Table 5-7 Parameters of event alarm policies

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

Example of configuring an alarm policy for an event

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

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

Figure 5-5 Alarm policy for an event

Event Name	Alarm Policy
If ECS stopped	Accumulative trigger 2 Count Within 5 minutes Then Every 5 minutes

5.2.4 Modifying an Alarm Rule

If there are service changes or you need to replan an alarm rule, you can modify the alarm rule.

CAUTION

If an alarm policy in the alarm rule has already been used to create an alarm masking rule, changing or deleting the policy will invalidate it within the masking rule. If all policies in a masking rule become invalid, the alarm masking rule will be automatically deleted. If needed, you can reconfigure the alarm masking rule after modifying the alarm rule.

Procedure

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Rules**.
3. On the displayed **Alarm Rules** page, use either of the following methods to modify an alarm rule:
 - Locate the alarm rule and 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.
4. On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

When you modify an alarm rule, the default values of **Alarm Type**, **Cloud Product**, **Resource Level**, and **Monitoring Scope** are used and cannot be changed. If **All resources** is selected for **Monitoring Scope**, you can click **Select Resources to Exclude** to not monitor specified resources. For details about how to set other parameters, see [5.2.2 Creating an Alarm Rule and Notifications](#).
5. Click **Modify**.

5.2.5 Disabling Alarm Rules

The new alarm rule is enabled by default. If you need to stop a cloud service for maintenance or upgrade, you can disable the alarm rule avoid receiving unnecessary alarm notifications because of manual changes.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management > Alarm Rules**.
 - On the **Alarm Rules** page, locate an enabled alarm rule, click **More > Disable** in the **Operation** column. In the displayed **Disable Alarm Rule** dialog box, click OK.
 - On the **Alarm Rules** page, select multiple enabled alarm rules and click **Disable** above the list. In the displayed **Disable Alarm Rule** dialog box, click OK.
3. Check the status of an alarm rule.
On the **Alarm Rules** page, the status of the alarm rule changes to **Disabled**.

5.2.6 Enabling Alarm Rules

After maintaining or upgrading a cloud product, you can enable the alarm rule for that product again. This will automatically restore the alarm notifications.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management > Alarm Rules**.
 - On the **Alarm Rules** page, locate a disabled alarm rule, click **More > Enable** in the **Operation** column. In the displayed **Enable Alarm Rule** dialog box, click **OK**.
 - On the **Alarm Rules** page, select multiple disabled alarm rules and click **Enable** above the list. In the displayed **Enable Alarm Rule** dialog box, click **OK**.
3. Check the alarm rule status.
On the **Alarm Rules** page, the status of the alarm rule changes to **Enabled**.

5.2.7 Deleting Alarm Rules

If an alarm rule does not meet your needs, you can delete it. Once a rule is deleted, you will not receive notifications from it anymore.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management > Alarm Rules**.
 - On the **Alarm Rules** page, locate the alarm rule to be deleted and choose **More > Delete** in the **Operation** column. In the displayed **Delete Alarm Rule** dialog box, click OK.
 - On the **Alarm Rules** page, select multiple alarm rules to be deleted and click **Delete** above the list. In the displayed **Delete Alarm Rule** dialog box, click OK.
3. Confirm that the alarm rule has been deleted.
On the **Alarm Rules** page, the alarm rule is deleted from the list.

5.2.8 Exporting Alarm Rules

You can export alarm rules configured for resources under your account. This topic describes how to export alarm rules.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
3. Click **Export** in the upper left corner of the alarm rule list.
4. In the displayed **Export Alarm Rules** dialog box, enter a task name, select required fields, determine whether to export the specific resource list, and click **OK**.

NOTE

The data to be exported contains specific resources monitored by Cloud Eye. You can choose whether to export the specified resource list as needed.

In the exported alarm rule details, only the first 30,000 characters of the resource information (resource name or resource ID) can be displayed due to cell limits.

5. After the export task is submitted, go to **Task Center**. On the **Alarm Data Export Tasks** page, click **Alarm Rule Export Tasks**. View the task details and download the task.

5.2.9 Filtering Alarm Rules

The alarm rule list displays all alarm rules you created. You can filter desired alarm rules.

Filtering Alarm Rules

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
3. On the **Alarm Rules** page, search for an alarm rule by specifying an API filter or resource tag. An API filter can be an alarm rule name, alarm rule ID, status, resource type, resource level, enterprise project, resource ID, resource group name, or resource group ID. Resource tags can be any tags configured when you create an alarm rule.

NOTE

To search for an alarm rule by resource ID, you are advised to select a resource type first.

5.3 Alarm Records

5.3.1 Viewing Alarm Records

When a metric reaches the threshold set for an alarm rule or an event occurs, you can check the monitoring details on the **Alarm Records** page. By default, alarm

records from the last seven days are displayed. You can select a time range to view alarm records from up to the last 30 days. When an alarm is generated, you can filter desired alarm records of a cloud resource and view their details.

Viewing Alarm Details

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Records**.
On the **Alarm Records** page, you can view information about alarms triggered in the last seven days by default.
3. Locate a record and 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

On the **Alarm Records** page, you can click **Export** in the upper left corner to export desired alarm records.

Filtering Alarm Records

You can filter alarm records by time range, resource type/dimension/metric, alarm type, or property type.

- By **time range**: In the upper right corner of the alarm records, select **Alarm Generated** or **Last Updated** from the drop-down list and select a time range in the calendar. You can view alarm records of any time range within the last 30 days.
- On the **Alarm Records** page, you can select a property type and enter a value to filter alarm records by record ID, status, alarm severity, alarm rule name, resource type, resource ID, or alarm rule ID.

Different alarm types have different states. Metric alarms may be in the **Alarm**, **Insufficient data**, **Expired**, **Resolved**, or **Resolved (forcible clear)** state. Event alarms may be in the **Triggered**, **Resolved**, **Expired**, or **Resolved (forcible clear)** state. For details, see [What Alarm Status Does Cloud Eye Support?](#) **Triggered** and **Alarm** indicate that there are active event and metric alarms. When you filter alarms by either of the two states, alarms in both states are displayed.

5.3.2 Forcibly Clearing an Alarm

To forcibly clear an alarm, confirm that the problem has been resolved on the console and then change the alarm status to **Resolved (forcible clear)**. This operation is not recommended because it is risky and used only in special scenarios.

Constraints

You can forcibly clear alarms only in the **Alarm**, **Alarm (triggered)**, or **Insufficient data** state.

Procedure

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Records**.
On the **Alarm Records** page, you can view information about alarms triggered in the last seven days.
3. Click **Forcibly Clear Alarm** in the **Operation** column.
The **Forcibly Clear the Alarm** dialog box is displayed.

Figure 5-6 Forcibly Clear the Alarm



4. In the displayed **Forcibly Clear the Alarm** dialog box, click **OK**.

NOTE

If a resource is still in the **Alarm** state, you are not advised to forcibly clear the alarm, or the alarm will be triggered again in the next alarm triggering period.

For example, if the alarm triggering frequency is set to once a day and the resource remains in the **Alarm** state, the alarm will be triggered again one day after it is forcibly cleared.

5.4 Alarm Templates

5.4.1 Overview

You can configure metrics in an alarm policy template in advance so that they can be referenced when you create different alarm rules for a cloud service resource.

When there are multiple cloud service resources, you can configure alarm policies for these resources in one or more alarm templates beforehand. Then, you can use these templates when configuring alarm rules. For alarm rules created using a template, you can modify the alarm policy in the template. The changes will be applied to all alarm rules created using the template. This helps you create and manage alarm rules with ease.

You can also create a custom metric or event template as needed.

5.4.2 Viewing Alarm Templates

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

Procedure

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Templates**.

On this page, you can view the created alarm templates, create a custom metric or event template, or change or delete an existing template.

5.4.3 Creating a Custom Metric or Event Template

You can select a default template or create a custom one as needed. This topic describes how to create a custom metric or event template.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. On the **Alarm Templates** page, click **Create Custom Template**.
4. On the **Create a Custom Alarm or Event Template** page, configure parameters by referring to [Table 5-8](#).

Table 5-8 Parameters for creating a template

Parameter	Description
Name	Custom template name. The system generates a random name, which you can modify. Example value: alarmTemplate-c6ft
Description	(Optional) Provides supplementary information about the custom template.
Alarm Type	Alarm type to which the alarm template applies. The value can be Metric or Event .
Event Type	Event type when you set Alarm Type to Event . The default value is System Event .
Method	You can select Use existing template or Configure manually . • Use existing template: You can select one or more existing templates. If you select multiple existing templates, the metric information is distinguished by resource type. • Configure manually: You can customize alarm policies as required.

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

5. Click **Create**.

5.4.4 Modifying a Custom Metric or Event Template

You can modify a custom metric or event template when there are service changes or you need to replan a custom template. If the template is associated with a resource group or alarm rule, the policies in the alarm rule will also change. This topic describes how to modify a custom metric or event template.

CAUTION

If you modify an alarm policy in an alarm template, the policy in the associated alarm masking rule will become invalid. If all policies in the alarm masking rule become invalid, the alarm masking rule will be automatically deleted. If needed, you can reconfigure the alarm masking rule after modifying the alarm template.

Modifying a Custom Metric or Event Template

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metric Templates** or **Custom Event Templates** tab.
4. Locate the template and click **Modify** in the **Operation** column.
5. Modify the configured parameters by referring to [Table 5-8](#).
6. Click **Modify**.

5.4.5 Deleting a Custom Metric or Event Template

You can delete a custom alarm or event template that is no longer used. The deletion operation cannot be undone.

Deleting a Custom Metric Template

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metrics Templates** tab and delete desired templates.
 - Deleting a template
 - Locate the metric template to be deleted, and choose **More** > **Delete** in the **Operation** column.

- In the **Delete Custom Metric Template** dialog box, select a deletion method and click **OK**.
- Batch deleting templates
 - Select multiple metric templates to be deleted and click **Delete** above the list.
 - In the **Delete Custom Metric Template** dialog box, click **OK**.

Deleting Custom Event Templates

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Event Templates** tab.
 - Locate the event template to be deleted, and choose **More** > **Delete** in the **Operation** column.
 - Select multiple event templates to be deleted and click **Delete** above the list.
4. In the displayed dialog box, click **OK**.

5.4.6 Copying a Custom Metric or Event Template

If you need to create an alarm template or event template with the same configurations as an existing one, you can simply copy the template.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
 - On the **Default Metric Templates** or **Default Event Templates** page, locate the desired template and click **Copy** in the **Operation** column.
 - Click the **Custom Metric Templates** or **Custom Event Templates** tab, locate the desired template, and choose **More** > **Copy** in the **Operation** column.
3. In the **Copy Template** dialog box, set **Template Name** and **Description**.
4. Click **OK**.

5.4.7 Associating a Custom Metric Template with a Resource Group

By associating a custom metric template with a resource group, you can create alarm rules for different resources in batches. If you have many cloud resources, you are advised to create resource groups by service application, create alarm templates, and associate resource groups with the alarm templates to create alarm rules in batches. This simplifies and speeds up rule creation and maintenance. After the association, corresponding alarm rules will be generated. Any changes to the templates will update all related alarm policies.

Prerequisites

- You have created a resource group by referring to [3.1.2 Creating a Resource Group](#).
- You have created a custom metric template by referring to [5.4.3 Creating a Custom Metric or Event Template](#).

Associating a Custom Metric Template with a Resource Group

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metric Templates** tab.
4. Locate the target template and click **Associate with Resource Group** in the **Operation** column.
5. On the **Associate with Resource Group** page, select the target resource group.
6. Configure alarm notifications.

Table 5-9 Configuring alarm notifications

Parameter	Description	Example Value
Alarm Notifications	Whether to send alarm notifications by SMS, email, HTTP, or HTTPS. This parameter is enabled by default.	Enabled
Recipient	Target recipient of alarm notifications. You can select the account contact or a topic. This parameter is available only if Notified By is set to Topic subscriptions . If there is a display name of a topic, the format is <i>Topic name (Display name)</i> , and you can search for a topic by name or display name. If no display name is set for a topic, only the topic name will be displayed. • The account contact is the mobile number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If there is no topic you need, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.	Account contact
Notification Window	If Notified By is set to Notification groups or Topic subscriptions , you need to set the notification window. Cloud Eye sends notifications only within the validity period specified in the alarm rule. If you set Notification Window to 08:00 to 20:00, Cloud Eye only sends notifications within this period.	08:00-20:00

Parameter	Description	Example Value
Time Zone	Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured.	(GMT +08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala Lumpur, Singapore, Perth, Taipei, Irkutsk, Ulaanbaatar
Trigger Condition	This parameter is required when you set Notified By to Notification groups or Topic subscriptions . Condition that will trigger an alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.	Generated alarm

7. Select an enterprise project.

Figure 5-7 Advanced settings

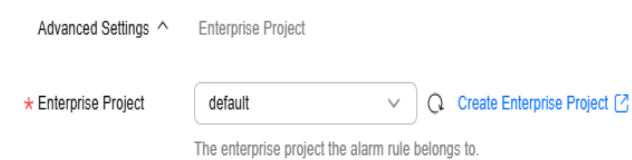


Table 5-10 Parameter of Advanced Settings

Parameter	Description	Example Value
Enterprise Project	Enterprise project that the alarm template belongs to. Only users who have all permissions for the enterprise project can manage the alarm template.	default

8. Click **OK**.

 NOTE

This operation requires asynchronous creation, modification, and deletion of alarm rules, which takes 5 to 10 minutes. If there are multiple association tasks, this process takes longer.

5.4.8 Importing and Exporting Custom Metric or Event Templates

If you want to quickly create a metric or event template using an existing custom template, you can export your desired template, modify it as needed, and then import the template. This section describes how to import or export custom metric or event templates.

Constraints

Monitoring metrics and events vary by Cloud Eye version. Importing custom alarm or event templates across regions with different versions may result in errors.

Importing a Custom Template

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metric Templates** or **Custom Event Templates** tab.
4. Click **Import**.
5. Upload a JSON file, enter a template name, and click **OK**.

Exporting a Custom Template

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metric Templates** or **Custom Event Templates** tab.
4. Locate the template and choose **More** > **Export** in the **Operation** column.

5.5 Alarm Notifications

5.5.1 Creating Alarm Notification Topics

5.5.1.1 Creating a Topic

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 [SMN console](#).

2. In the navigation pane, choose **Topic Management > Topics**.
The **Topics** page is displayed.
3. Click **Create Topic**.
The **Create Topic** dialog box is displayed.
4. Enter a topic name and display name (topic description).

Table 5-11 Parameters required for creating a topic

Parameter	Description
Topic Name	Topic name, which: • Contains only letters, digits, hyphens (-), and underscores (_) and must start with a letter or digit. • Must contain 1 to 255 characters. • Must be unique and cannot be modified after the topic is created.
Display Name	Display name, which can contain up to 192 bytes. NOTE After you specify a display name, the sender will be presented in <i>Display name<username@example.com></i> format, or the sender will be <i><username@example.com></i> .
Enterprise Project	Enterprise project. It centrally manages cloud resources and members by project.
CTS Log	Whether to enable CTS logging.
Log Group	Select a log group. A log group is a group of log streams which share the same log retention settings.
Log Stream	Select a log stream in the specified log group. A log stream is the basic unit for reading and writing logs. Sorting logs into different log streams makes it easier to find specific logs when you need them.
Tag	Tags identify cloud resources so that you can categorize and search for your resources easily and quickly. • For each resource, each tag key must be unique, and can have only one tag value. • A tag key can contain a maximum of 36 characters. It can only include 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 for each topic.

5. 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.

6. Click the name of the topic you created to view the topic its details.

Follow-up Operations

After you create a topic, add subscriptions to the topic by referring to [add subscriptions](#). After the subscriptions have been confirmed, alarm notifications will be sent to the subscription endpoints via SMN.

5.5.1.2 Adding Subscriptions

A topic is a channel used by SMN to broadcast messages. To receive messages published to a topic, you must subscribe to the topic. In this way, when an alarm is reported, Cloud Eye will notify you of the alarm information.

Procedure

1. Log in to the [SMN console](#).
2. In the navigation pane, choose **Topic Management > Topics**.
The **Topics** page is displayed.
3. Locate the topic you want to add subscriptions to and click **Add Subscription** in the **Operation** column.
The **Add Subscription** dialog box is displayed.
4. Specify the subscription protocol and endpoints.
If you enter multiple endpoints, enter each endpoint on a separate line.
5. Click **OK**. The new subscription is displayed in the subscription list.

NOTE

After the subscription is added, each subscription endpoint will receive a subscription confirmation. They need to confirm their subscriptions so that they can receive alarm notifications. If no subscription or notification message is received, rectify the fault by referring to

5.6 One-Click Monitoring

One-click monitoring enables you to quickly and easily enable or disable monitoring for cloud service resources. This topic describes how to use the one-click monitoring function to monitor key metrics.

[Table 5-12](#) describes differences between one-click monitoring and common monitoring.

Table 5-12 Differences between one-click monitoring and common monitoring

Alarm Type	How It Works	Scope	Monitoring	Trigger
One-click monitoring	When an event occurs, Cloud Eye triggers alarms immediately. Advantages: The configuration is simple.	For details about services supported by Cloud Eye, see Cloud Services That Support One-Click Monitoring .	Event Monitoring Metric Monitoring	Immediate trigger
Common monitoring	Cloud Eye triggers alarms based on the preset alarm policies. For example, Cloud Eye triggers an alarm if the average CPU usage is 80% or more for five consecutive times within 5 minutes. Advantages: Alarm policies are flexible and can be configured based on service requirements.	All services supported by Cloud Eye	• Server Monitoring • Cloud Service Monitoring • Custom Monitoring	Accumulative trigger
	When an event occurs, Cloud Eye triggers alarms based on the alarm policy. Advantages: The configuration is flexible. Only event alarms are supported.	For detailed events, see 6.4 Events Supported by Event Monitoring .	Event Monitoring	Immediate trigger or accumulative trigger

Constraints

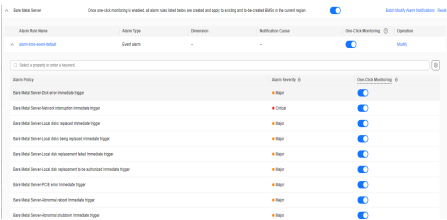
Once the alarm conditions specified in one-click monitoring are reached, Cloud Eye will trigger alarms immediately.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management > One-Click Monitoring**.

- 3. Locate the cloud service you want to enable one-click monitoring and toggle on the button in the **One-Click Monitoring** column.
- 4. On the **Enable Alarm Rule** page, check that one-click monitoring is enabled for all alarm rules by default. Locate the alarm rule for which one-click monitoring is unnecessary and toggle off the button in the **One-Click Monitoring** column.
- 5. Set alarm notification parameters. For details, see [Table 5-4](#).
- 6. Click **OK**. One-click monitoring is enabled. The alarm rule is added to the list.
- 7. Click the arrow on the left of a cloud service name to view or modify the built-in alarm rules, or reset the built-in alarm rules after modification.
 - Locate an alarm rule and click **Modify** in the **Operation** column to delete or add alarm policies. Set **Alarm Notification** as needed. For details, see [Table 5-4](#).
 - Locate a cloud service and click **Reset** in the **Operation** column to restore the default alarm rules. If one-click monitoring is disabled, resetting one-click monitoring will restore the changed alarm policy and clear the configured notification method. If one-click monitoring is enabled, resetting it only restores the changed alarm policy but keeps the notification settings.

Figure 5-8 Viewing alarm rules or modifying an alarm rule



Cloud Services That Support One-Click Monitoring

Cloud Service	Metric Monitoring	Event Monitoring
Auto Scaling	Supported	Not supported
Cloud Search Service	Supported	Not supported
API Gateway	Supported	Not supported
Data Ingestion Service	Supported	Not supported
Database Security Service	Supported	Not supported
Distributed Database Middleware	Supported	Not supported
ROMA	Supported	Not supported
Direct Connect	Supported	Not supported

Cloud Service	Metric Monitoring	Event Monitoring
GeminiDB	Supported	Supported
TaurusDB	Supported	Supported
DataArts Studio	Supported	Not supported
Prediction Service	Supported	Not supported
GaussDB	Supported	Supported
ModelArts	Supported	Not supported
Workspace	Supported	Not supported
CloudTable	Supported	Not supported
Content Moderation	Supported	Not supported
Bare Metal Server	Supported	Supported
Cloud Bastion Host	Supported	Not supported
Cloud Backup and Recovery	Supported	Supported
Cloud Data Migration	Supported	Not supported
Content Delivery Network	Supported	Not supported
Cloud Firewall	Supported	Not supported
Cloud Phone	Supported	Not supported
Cloud Storage Gateway	Supported	Supported
Distributed Cache Service	Supported	Supported
Document Database Service	Supported	Supported
Data Lake Insight	Supported	Not supported
Distributed Message Service	Supported	Not supported
Data Replication Service	Supported	Not supported
Data Warehouse Service	Supported	Not supported
Elastic Cloud Server	Supported	Supported
SFS Turbo	Supported	Not supported
Elastic Load Balance	Supported	Not supported
Elastic Volume Service	Supported	Supported
Face Recognition	Supported	Not supported

Cloud Service	Metric Monitoring	Event Monitoring
Graph Engine Service	Supported	Not supported
Image Recognition	Supported	Not supported
Identity Verification Solution	Supported	Not supported
NAT Gateway	Supported	Not supported
Natural Language Processing	Supported	Not supported
Object Storage Service	Supported	Supported
Optical Character Recognition	Supported	Not supported
Relational Database Service	Supported	Supported
Speech Interaction Service	Supported	Not supported
Virtual Private Cloud	Supported	Not supported
Virtual Private Network	Supported	Not supported
Web Application Firewall	Supported	Not supported
Elastic IP	Not supported	Supported

5.7 Alarm Masking

5.7.1 Introduction

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

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.

5.7.2 Creating a Masking Rule

You can create a masking rule to mask alarm notifications once alarms are triggered. After the masking rule is applied, only alarm records will be generated, and alarm notifications will no longer be sent. This section describes how to create a masking rule.

**CAUTION**

- If you set **Masked By** to **Resource**, all alarm notifications will be masked for the selected resource. Exercise caution.
- If **Masked By** is set to **Policy**, changing or deleting the policy of the alarm rule will invalidate it within the masking rule. If all policies in a masking rule become invalid, the alarm masking rule will be automatically deleted. If needed, you can reconfigure the alarm masking rule after modifying the alarm rule.

Prerequisites

Ensure that an alarm rule has been created before creating a policy-specific masking rule. For details, see [5.2.2 Creating an Alarm Rule and Notifications](#).

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Masking**.
3. In the upper right corner of the page, click **Create Masking Rule**.
4. On the displayed **Create Masking Rule** page, configure parameters.

Figure 5-9 Creating an alarm masking rule

Table 5-13 Parameters for configuring a masking rule

Parameter	Description
Name	Name of the alarm masking rule. The name allows 1 to 64 characters and can only contain letters, digits, hyphens (-), and underscores (_).
Masked By	Masking method of the alarm masking rule. Set this parameter to Resource , Policy , or Event .
Cloud product	Cloud product that the alarm masking rule applies to. This parameter is mandatory when Masked By is set to Resource or Policy .

Parameter	Description
Resource Level	When Masked By is set to Resource or Policy, you need to select a resource level, either Cloud product or Specific dimension. Take ECS as an example. ECS is the cloud product. Specific dimensions are disks, mount points, processes, and more. If Cloud product is selected, metrics across sub-dimensions are supported. If Specific dimension is selected and a sub-dimension is specified, only metrics of the specified dimension can be selected.
Select Rule	If Masked By is set to Policy , select an alarm rule.
Select Policies	If Masked By is set to Policy, select alarm policies in an alarm rule. You can associate the selected alarm policies with the selected alarm rule. You can select one or more alarm policies to mask alarms. NOTE If an alarm policy has been configured in an alarm rule in which an alarm will be generated only when all alarm policies are met, the alarm policy cannot be selected.
Resource	Resource for which alarm notifications need to be masked. You can add up to 100 resources at a time. • If Masked By is set to Resource, select specific resources. • If Masked By is set to Policy, select an alarm rule, and specify policies as well as resources. You can select All resources or Specific resources. • If Masked By is set to Event and Monitoring Scope is set to Specific resources, select specific resources.
Metric	If Masked By is set to Resource, select specific metrics. You can select up to 50 metrics at a time. CAUTION If you do not select any metrics, this masking rule will apply to all metrics.
Event Source	Name of the cloud service that triggers the event. This parameter is only available if Masked By is set to Event.

Parameter	Description
Monitoring Scope	Resources for which the event masking rule is applied. If Masked By is set to Event , you need to set the monitoring scope. The value can be All resources or Specific resources based on the event source.
Select Event	Name of the event to be masked. You need to select an event only if Masked By is set to Event . If no event is selected, this making rule will apply to all events.
Alarm Masking Duration	Time or duration when the masking rule is applied. • Date and time: The masking rule is applied within a specified time range. After specifying a time range, you need to select the effective time. The options are 1 hour, 3 hours, 12 hours, 24 hours, and 7 days. • Time: The masking rule takes effect in a fixed time range every day. You can also configure the effective date range when the masking rule takes effect. For example, if the effective date is 2022-12-01 to 2022-12-31 and the effective time is 08:00 to 20:00, the masking rule will apply during this time window every day from December 1, 2022 to December 31, 2022. • Permanent: The masking rule will always take effect.
Time Zone	Time zone of the alarm notification window in the masking rule. The default value is the time zone where the client browser is located. The value can be configured.

5. Click **Create**.

5.7.3 Modify a Masking Rule

This section describes how you can modify a masking rule.

Modifying a Masking Rule

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Masking**.
3. On the displayed page, locate the masking rule and click **Modify** in the **Operation** column.
4. On the displayed **Modify Masking Rule** page, configure parameters.

Table 5-14 Parameters for configuring a masking rule

Parameter	Description
Name	Name of the masking rule. The name allows 1 to 64 characters and can only contain letters, digits, hyphens (-), and underscores (_).
Resource	Resource for which alarm notifications need to be masked. You can add up to 100 resources at a time. • If Masked By is set to Resource, select specific resources. • If Masked By is set to Policy, select an alarm rule, and specify policies as well as resources. You can select All resources or Specific resources. • If Masked By is set to Event and Monitoring Scope is set to Specific resources, select specific resources.
Metric	If Masked By is set to Resource , select specific metrics. You can select up to 50 metrics at a time. CAUTION If you do not select any metrics, this masking rule will apply to all metrics.
Select Rule	If you select Policy for Masked By , select an alarm rule.
Select Policies	If Masked By is set to Policy , select alarm policies in an alarm rule. You can associate the selected alarm policies with the selected alarm rule. You can select one or more alarm policies to mask alarms. NOTE If an alarm policy has been configured in an alarm rule in which an alarm will be generated only when all alarm policies are met, the alarm policy cannot be selected.
Monitoring Scope	Resources for which the event masking rule is applied. If Masked By is set to Event , you need to set the monitoring scope. The value can be All resources or Specific resources based on the event source.
Select Event	Name of the event to be masked. You need to select an event only if Masked By is set to Event . If no event is selected, this making rule will apply to all events.

Parameter	Description
Alarm Masking Duration	Time or duration when the masking rule is applied. • Date and time: The masking rule is applied within a specified time range. • Time: The masking rule takes effect in a fixed time range every day. You can also configure the effective date range when the masking rule takes effect. For example, if the effective date is 2022-12-01 to 2022-12-31 and the effective time is 08:00 to 20:00, the masking rule will apply during this time window every day from December 1, 2022 to December 31, 2022. • Permanent: The masking rule always takes effect. NOTE To change Alarm Masking Duration in batches, select multiple masking rules on the Alarm Masking page and click Modify Alarm Masking Duration above the list.
Time Zone	Time zone of the alarm notification window in the masking rule. The default value is the time zone where the client browser is located. The value can be configured.

5. Click **OK**.

Modifying the Masking Duration for a Masking Rule

You can batch modify the masking duration for masking rules, replacing the existing time with the new one.

1. Log in to the [Cloud Eye console](#).
2. Choose **Alarm Management** > **Alarm Masking**.
3. On the **Alarm Masking** page, select the masking rules and click **Modify Alarm Masking Duration** above the list.
4. On the **Modify Alarm Masking Duration** page, set the masking duration and click **OK**.

5.7.4 Deleting a Masking Rule

If a masking rule is no longer used, you can delete it. After a masking rule is removed, the alarm notification can be sent normally.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Masking**.
3. On the **Alarm Masking** page, locate the masking rule and click **Delete** in the **Operation** column. Alternatively, select one or more masking rules and click **Delete** above the list.

4. Click **OK**.

5.7.5 Masking an Alarm Rule

Cloud Eye can not only mask alarm notifications based on masking rules you configure, but also mask an alarm rule. This section describes how to mask an alarm rule.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
3. Select the alarm rule to be masked and choose **More** > **Mask Alarm** above the alarm rule list.
4. On the displayed page, set **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.
5. Check the masking status of the alarm rule.
On the **Alarm Rules** page, the masking status of the alarm rule changes to **Applied**.

6 Event Monitoring

[6.1 Overview](#)

[6.2 Viewing Events](#)

[6.3 Creating an Alarm Rule and Notification for Event Monitoring](#)

[6.4 Events Supported by Event Monitoring](#)

6.1 Overview

What Is an Event?

Events are key operations or statuses of a cloud service that are stored and monitored by Cloud Eye. By reviewing these events, you can learn who performed specific actions on which resources at what time, such as VM deletion or restart, along with other resource status changes.

Event Monitoring

You can query system events and custom events reported to Cloud Eye through APIs. You can collect all critical events from your services or operations on cloud resources to Cloud Eye to track the cloud service status. You can also set event alarm rules for these events or operations. When a specified event occurs, Cloud Eye automatically sends an alarm notification. This helps you quickly identify and address issues.

Event monitoring is enabled by default, regardless of whether the Agent is installed.

Event Monitoring Type

You can view monitoring details about system events and custom events.

Event Type	Description
System events	For details about supported system events, see 6.4 Events Supported by Event Monitoring .
Custom events	Event monitoring provides an API for reporting custom events, which helps you collect and report abnormal events or important change events from services to Cloud Eye. For details, see Reporting Events .

6.2 Viewing Events

Cloud Eye monitors system events and custom events of cloud services. This helps you quickly analyze and locate faults if any. This section describes how to view event monitoring data.

Viewing Event Monitoring Data

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Event Monitoring**.
3. On the displayed page, view all system events and custom events over the last 24 hours.
You can view events in the last 1 hour, last 3 hours, last 12 hours, last 1 day, last 7 days, or last 30 days. Alternatively, you can set a custom time range to view events triggered within that period.
4. Locate the event type to be viewed and click **View Graph** in the **Operation** column.
5. Locate a specific event and click **View Event** in the **Operation** column.

6.3 Creating an Alarm Rule and Notification for Event Monitoring

You can create alarm rules and notifications for events of concern to receive timely alarm notifications. This topic describes how to create an alarm rule for event monitoring.

If you disable **Alarm Notifications** when creating an alarm rule, no notifications will be sent. You can check the alarm rule statuses on the **Alarm Records** page.

Creating an Alarm Rule and Notification for Event Monitoring

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Event Monitoring**.
3. Click **Create Alarm Rule** in the upper right corner to go to the **Create Alarm Rule** page.

 NOTE

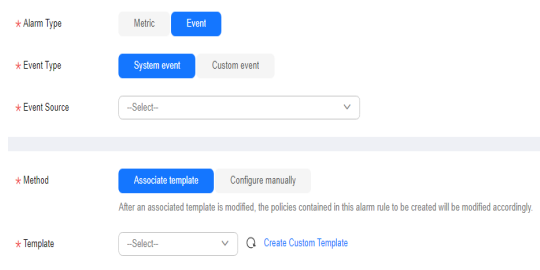
If you want to create an alarm rule for a specific event, locate the event in the event list and click **Create Alarm Rule** in the **Operation** column. On the displayed **Create Alarm Rule** page, required parameters have been configured for that event.

4. Configure basic information about the alarm rule.

Table 6-1 Basic parameters

Parameter	Description
Name	Name of the alarm rule. The system generates a random name, which you can modify. The rule name cannot exceed 128 characters and can contain only letters, digits, underscores (_), and hyphens (-).
Description	(Optional) Alarm rule description. It can contain up to 256 characters.

5. Select monitored objects and configure alarm parameters.

Figure 6-1 Configuring parameters**Table 6-2** Parameter description

Parameter	Description
Alarm Type	Alarm type that the alarm rule applies to. The default value is Event .
Event Type	Event type, which can be System event or Custom event . For details, see Event Monitoring Type .
Event Source	The service the event is generated for. For a custom event, set Event Source to the value of event_source .
Monitoring Scope	Monitoring scope the alarm rule applies to. You can select Resource groups , All resources , or Specific resources . If Event Type is set to System event , you can configure the monitoring scope. Currently, Resource groups is only available for DDS, RDS, and DCS event alarms.

Parameter	Description
Method	Select a mode for configuring an alarm policy. If you select System event for Event Type , Method can be Associate template or Configure manually . If you select Custom event for Event Type , only Configure manually is supported. • Configure manually: You can create a custom alarm policy as needed. • Associate template: If you need to configure the same alarm rule for multiple groups of resources under the same cloud product, you can use an alarm template to simplify operations.
Template	If you set Method to Associate template , you need to select a template. You can select a default or custom template.
Event Name	Instantaneous operations users performed on resources, such as login and logout. • For supported system events, see 6.4 Events Supported by Event Monitoring. • For a custom event, the event name is the value of event_name when the custom event is reported.
Alarm Policy	Policy for triggering an alarm. For details about alarm policy parameters, see Configuring Alarm Policies for Events .
Alarm Severity	Alarm severity, which can be Critical , Major , Minor , or Warning .
Operation	You can click Delete to delete the alarm policy.

6. Configure alarm notifications.

Table 6-3 Parameter description

Parameter	Description
Alarm Notifications	Whether to send alarm notifications by SMS, email, HTTP, or HTTPS. This parameter is enabled by default.

Parameter	Description
Recipient	Target recipient of alarm notifications. You can select the account contact or a topic. This parameter is available only if Notified By is set to Topic subscriptions. If there is a display name of a topic, the format is <i>Topic name (Display name)</i>, and you can search for a topic by name or display name. If no display name is set for a topic, only the topic name will be displayed. • The account contact is the mobile number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If there is no topic you need, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.
Notification Window	Notification window during which Cloud Eye only sends notifications. If you set Notification Window to 08:00 to 20:00, Cloud Eye only sends notifications within this period.
Time Zone	Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured.
Trigger Condition	When the alarm type is Event, you can select Generated alarm for Trigger Condition.

7. Select an enterprise project.

Figure 6-2 Advanced settings

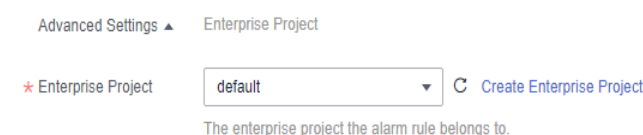


Table 6-4 Parameter description

Parameter	Description
Enterprise Project	Enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can manage the alarm rule. To create an enterprise project, see Creating an Enterprise Project.

8. Click **Create**.

You can go to the **Alarm Rules** page and check the alarm rule you created. You can filter the new alarm rule by its name.

6.4 Events Supported by Event Monitoring

 NOTE

The name of a resource that supports event reporting can contain a maximum of 128 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). If it contains other characters, the event may fail to be reported to Cloud Eye.

Table 6-5 Elastic Cloud Server (ECS)

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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU link fault	GPULinkFault	Critical	The GPU of the host running the ECS was faulty or 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.
	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.

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

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 SRAM is faulty, and services exit abnormally.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host running the ECS was faulty or 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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Local disk replacement to be executed	localdisk_recovery_scheduled	Major	Local disk failure	Clarify the impact on services during the execution window.	None
	Xid event alarm generated on GPU	commonXidError	Major	A Xid event alarm was generated on the GPU.	If services are affected, submit a service ticket.	The GPU hardware, driver, and application problems lead to Xid events, which may interrupt services.
	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 on the NPU.	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 disks are faulty.	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU throttle alarm	gpuClocksThrottleReasonsAlarm	Informational	1. The GPU power may exceed the maximum operating power threshold (continuous full load). The clock frequency automatically decreases to prevent the GPU from being damaged. 2. The GPU temperature may exceed the maximum operating temperature threshold (continuous full load). The clock frequency automatically decreases to reduce heat. 3. The GPU may remain idle, with the clock frequency automatically decreasing to reduce power consumption.	Check whether the clock frequency decrease is caused by hardware faults. If yes, transfer it to the hardware team.	The GPU slows down, resulting in less powerful compute .

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				4. Hardware faults may cause a decrease in clock frequency.		
	Pending page retirement for GPU DRAM ECC	gpuRetiredPagesPendingAlarm	Major	1. An ECC error occurred on the hardware. DRAM pages need to be retired. 2. An uncorrectable ECC error occurred on the GPU memory page and the page needs to be retired. However, the page is suspended and has not been retired yet.	1. View the event details and check whether the value of retired_pages.pending is yes. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Pending row remapping for GPU DRAM ECC	gpuRemappedRows Alarm	Major	Some rows in the GPU memory have errors and need to be remapped. The faulty rows must be mapped to standby resources.	1. View the event metric "RemappedRow" to check if there are any rows that have been remapped. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.
	Insufficient resources for GPU DRAM ECC row remapping	gpuRowRemapperResource Alarm	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. The standby GPU memory row resources are exhausted, so row remapping cannot be continued.	Transfer the issue to the hardware team.	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Correctable GPU DRAM ECC error	gpuDRAMCorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. A correctable ECC error occurs in the DRAM of the GPU. However, the ECC mechanism can automatically rectify the error and programs are not affected.	1. View the event metric "ecc.errors.corrected.volatile" to check whether there are any correctable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Uncorrectable GPU DRAM ECC error	gpuDRAMUncorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. An uncorrectable ECC error occurs in the DRAM of the GPU. This error cannot be automatically corrected using the ECC mechanism. The verification process affects system stability and may cause program crashes.	1. View the event metric "ecc.errors.uncorrected.volatile" to check whether there are any uncorrectable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Inconsistent GPU kernel versions	gpuKernelVersionInconsistencyAlarm	Major	Inconsistent GPU kernel versions. During driver installation, the GPU driver is compiled based on the kernel at that time. If the kernel versions are identified inconsistent, the kernel has been customized after the driver installation. In this case, the driver would become unavailable and needs to be reinstalled.	1. Run the following commands to rectify the issue: rmmod nvidia_drm rmmod nvidia_modeset rmmod nvidia Then, run nvidia-smi. If the command output is normal, the issue has been rectified. 2. If the preceding solution does not work, rectify the fault by referring to Why Is the GPU Driver	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					Unavailable?	
	GPU monitoring dependency not met	gpuCheckEnvFailedAlarm	Major	The plug-in cannot identify the GPU driver library path.	1. Check whether the driver is installed . 2. Check whether the driver installation directory has been customized. The driver needs to be installed in the default installation directory <code>/usr/bin/</code>.	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Initialization failure of the GPU monitoring driver library	gpuDriverInitFailedAlarm	Major	The GPU driver is unavailable.	Run nvidia-smi to check whether the driver is unavailable. If the driver is unavailable, reinstall the driver by referring to Manually Installing a Tesla Driver on a GPU-accelerated ECS .	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Initialization timeout of the GPU monitoring driver library	gpuDriverInitAlarm	Major	The GPU driver initialization timed out (exceeding 10s).	1. If the driver is not installed, install it by referring to Manually Installing a Tesla Driver on a GPU-accelerated ECS. 2. If the driver is installed, run nvidia-smi to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to Manually Installing a Tesla Driver on a GPU-	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					accelerated ECS. 3. If the driver is properly installed , check whether the high-performance mode is enabled. If not, run nvidia-smi -pm 1 to enable it. P0 indicates the high-performance mode.	

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU metric collection timeout	gpuCollectMetricTimeoutAlarm	Major	The GPU metric collection timed out (exceeding 10s).	1. If the library API timed out, run nvidia-smi to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to Manually Installing a Tesla Driver on a GPU-accelerated ECS. 2. If the command execution timed out, check the system logs and determine whether there is an issue.	GPU monitoring metric data is missing. As a result, subsequent metrics may fail to be collected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					with the system.	
	GPU handle lost	gpuDeviceHandleLost	Major	The GPU metric information cannot be obtained, and the GPU may be lost.	1. Run nvidia-smi to check whether there are any errors reported. 2. Run nvidia-smi -L to check whether the number of GPUs is the same as the server specifications. 3. Submit a service ticket to contact on-call support.	All metrics of the GPU are lost.
	Failed to listen to the XID of the GPU.	gpuDeviceXidLost	Major	Failed to listen to the XID metric.	1. Check whether the GPU is lost or damaged. 2. Submit a service ticket to contact on-call support.	Failed to obtain XID-related metrics of the GPU.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ReadOnly issues in OS	ReadOnlyFileSystem	Critical	The file system %s is read-only.	Check the disk health status.	The files cannot be written.
	NPU: driver and firmware not matching	NpuDriverFirmwareMismatch	Major	The NPU's driver and firmware do not match.	Obtain the matched version from the Ascend official website and reinstall it.	NPUs cannot be used.
	NPU: Docker container environment check	NpuContainerEnvironment	Major	Docker was unavailable.	Check if Docker is normal.	Docker cannot be used.
			Major	The container plug-in Ascend-Docker-Runtime was not installed.	Install the container plug-in Ascend-Docker-Runtime. Or, the container cannot use Ascend cards.	NPUs cannot be attached to Docker containers.
			Major	IP forwarding was not enabled in the OS.	Check the net.ipv4.ip_forward configuration in the /etc/sysctl.conf file.	Docker containers experience network communication problems.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
			Major	The shared memory of the container was too small.	The default shared memory is 64 MB, which can be modified as needed. Method 1 Modify the default-shm-size field in the /etc/docker/daemon.json configuration file. Method 2 Use the --shm-size parameter in the docker run command to set the shared memory size of a container.	Distributed training will fail due to insufficient shared memory.
	NPU: RoCE NIC down	RoCELinkStatusDown	Major	The RoCE link of NPU card %d was down.	Check the NPU RoCE network port status.	The NPU NIC becomes unavailable.
	NPU: RoCE NIC health status abnormal	RoCEHealthStatusError	Major	The RoCE network health status of NPU %d was abnormal.	Check the health status of the NPU RoCE NIC.	The NPU NIC becomes unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NPU: RoCE NIC configuration file /etc/hccn.conf not found	HccnConfNotExist	Major	The RoCE NIC configuration file /etc/hccn.conf was not found.	Check whether the /etc/hccn.conf NIC configuration file can be found.	The RoCE NIC is unavailable.
	GPU: basic components abnormal	GpuEnvironmentSystem	Major	The nvidia-smi command was abnormal.	Check whether the GPU driver is normal.	The GPU driver is unavailable.
			Major	The nvidia-fabricmanager version was inconsistent with the GPU driver version.	Check the GPU driver version and nvidia-fabricmanager version.	The nvidia-fabricmanager cannot work properly, affecting GPU usage.
			Major	The container plug-in nvidia-container-toolkit was not installed.	Install the container plug-in nvidia-container-toolkit.	GPUs cannot be attached to Docker containers.
	Local disk attachment inspection	MountDiskSystem	Major	The /etc/fstab file contains invalid UUIDs.	Ensure that the UUIDs in the /etc/fstab configuration file are correct. Or, the server may fail to be restarted.	The disk attachment process fails, preventing the server from restarting.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU: incorrectly configured dynamic route for Ant series server	GpuRouteConfigError	Major	The dynamic route of the NIC %s of an Ant series server was not configured or was incorrectly configured. CMD [ip route]: %s CMD [ip route show table all]: %s.	Configure the RoCE NIC route correctly.	The NPU network communication will be interrupted.
	NPU: RoCE port not split	RoCEUDPConfigError	Major	The RoCE UDP port was not split.	Check the RoCE UDP port configuration on the NPU.	The communication performance of NPUs is affected.
	Warning of automatic system kernel upgrade	KernelUpgradeWarning	Major	Warning of automatic system kernel upgrade. Old version: %s; new version: %s.	System kernel upgrade may cause AI software exceptions. Check the system update logs and prevent the server from restarting.	The AI software may be unavailable.
	NPU environment command detection	NpuToolsWarning	Major	The hccn_tool was unavailable.	Check whether the NPU driver is normal.	The IP address and gateway of the RoCE NIC cannot be configured.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
			Major	The npu-smi was unavailable.	Check whether the NPU driver is normal.	NPUs cannot be used.
			Major	The ascend-dmi was unavailable.	Check whether ToolBox is properly installed.	ascend-dmi cannot be used for performance analysis.
	Warning of an NPU driver exception	NpuDriverAbnormal Warning	Major	The NPU driver was abnormal.	Reinstall the NPU driver.	NPUs cannot be used.

 NOTE

Automatic recovery: If the hardware where an ECS is located is faulty, the system automatically migrates it to a normal physical host. The ECS will restart during the migration.

Table 6-6 Bare metal server (BMS)

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	SYS.BMS	ECC uncorrectable error alarm generated on GPU SRAM	SRAM Uncorrectable EccError	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 SRAM is faulty, and services exit abnormally.
		BMS restarted	osReboot	Major	The BMS instance is 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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BMS unexpected restart	serverReboot	Major	The BMS instance restarts unexpectedly. • OS faults. • hardware faults.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
		BMS stopped	osShutdown	Major	The BMS instance is stopped. • 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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BMS unexpected shutdown	serverShutdown	Major	The BMS stops unexpectedly due to: - unexpected power-off. - hardware faults.	- Deploy service applications in HA mode. - After the BMS is restarted, check whether services recover.	Services are interrupted.
		Network disconnection	linkDown	Major	The BMS network is disconnected. Possible causes are as follows: - The BMS was stopped or restarted unexpectedly. - The switch was faulty. - The gateway was faulty.	- 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
		PCIe error	pcieError	Major	The PCIe device or main board on the BMS is faulty. Possible causes are as follows: - main board faults. - PCIe device faults.	- Deploy service applications in HA mode. - After the BMS is started, check whether services recover.	The network or disk read/write services are affected.
		Disk fault	diskError	Major	The disk of the BMS is faulty. Possible causes are as follows: - 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
		EVS error	storage Error	Major	The BMS failed to connect to EVS disks. Possible causes are as follows: • The SDI card was faulty. • Remote storage devices were faulty.	• Deploy service applications in HA mode. • After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Inforom alarm generated on GPU	gpuInfoROM Alarm	Major	The infoROM of the GPU is abnormal. ROM is an important storage area of the GPU firmware and stores key data loaded during startup.	Non-critical services can continue to use the GPU. For critical services, submit a service ticket to resolve this issue. 1. Restart the VM and check that the issue is not caused by a temporary cache or communication error. 2. If the fault persists after the restart, the hardware may be faulty. Submit	Services will not be affected. If ECC errors are reported on a GPU, faulty pages may not be automatically retired and services are affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						a service ticket to check whether the GPU needs to be replaced.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Double-bit ECC alarm generated on GPU	doubleBitEccError	Major	A double-bit error occurs in the ECC memory of the GPU. The ECC cannot correct the error, which may cause program breakdown.	1. If services are interrupted, restart the services. 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 can continue to be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Too many retired pages	gpuTooManyRetiredPagesAlarm	Major	An ECC page retirement error occurred on the GPU. When an uncorrectable ECC error occurs on a GPU memory page, the GPU marks the page as retired.	If services are affected, submit a service ticket.	If there are too many ECC errors, services may be affected. 1. If there are too many retired pages and the GPU memory capacity decreases too much, the system performance ma

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
							y deteriorate. 2. If there are too many retired pages and the GPU memory capacity decreases too much, the system may run unstably.

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

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 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.

Event Source	Name space	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. 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 errors occurring in the ECC memory of the 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.	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 it cannot be found by the NVIDIA driver.	1. You are advised to try restarting the VM to restore your services. 2. If services still cannot be restored, submit a service ticket.	The GPU 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 the GPU.
		VM GPU lost	vmLostGpuAlarm	Major	The number of GPUs on the VM is less than the number specified in the specifications.	If services are affected, submit a service ticket.	GPUs 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	Name space	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.	None
		System maintenance canceled	system_maintenance_cancelled	Major	The scheduled BMS maintenance is canceled.	None	None

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

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

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: request for BMS restart	Reboot Virtual Machine	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	ResetS OC	Informational	A fault occurs and the SoC needs to be reset.	Collect the fault information, and reset the SoC.	Services may be interrupted.
		NPU: request for restart AI process	Restart AIProcess	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	NPUErrorCode Warning	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 <i>Black Box Error Code Information List</i> and <i>Health Management Error Definition</i> .	Services may be interrupted.
		nvidia-smi suspended	nvidiaSmiHangEvent	Major	nvidia-smi timed out.	If services are affected, submit a service ticket.	The driver may report an error during service running.

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

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU throttle alarm	gpuClocksThrottleReasonsAlarm	Informational	1. The GPU power may exceed the maximum operating power threshold (continuous full load). The clock frequency automatically decreases to prevent the GPU from being damaged. 2. The GPU temperature may exceed the maximum operating temperature threshold (continuous full load). The clock frequency automatically decreases to reduce heat. 3. The GPU may remain	Check whether the clock frequency decrease is caused by hardware faults. If yes, transfer it to the hardware team.	The GPU slows down, resulting in less powerful compute.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					idle, with the clock frequency automatically decreasing to reduce power consumption. 4. Hardware faults may cause a decrease in clock frequency.		

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Pending page retirement for GPU DRAM ECC	gpuRetiredPagesPendingAlarm	Major	1. An ECC error occurred on the hardware. DRAM pages need to be retired. 2. An uncorrectable ECC error occurred on the GPU memory page and the page needs to be retired. However, the page is suspended and has not been retired yet.	1. View the event details and check whether the value of retired_pages_pending is yes. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Pending row remapping for GPU DRAM ECC	gpuRemappedRows Alarm	Major	Some rows in the GPU memory have errors and need to be remapped. The faulty rows must be mapped to standby resources.	1. View the event metric "RemappedRow" to check if there are any rows that have been remapped. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.
		Insufficient resources for GPU DRAM ECC row remapping	gpuRowRemapperResource Alarm	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. The standby GPU memory row resources are exhausted, so row remapping cannot be continued.	Transfer the issue to the hardware team.	The GPU cannot work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Correctable GPU DRAM ECC error	gpuDRAMCorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. A correctable ECC error occurs in the DRAM of the GPU. However, the ECC mechanism can automatically rectify the error and programs are not affected.	1. View the event metric "ecc.errors.corrected.volatile" to check whether there are any correctable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Uncorrectable GPU DRAM ECC error	gpuDRAMUncorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. An uncorrectable ECC error occurs in the DRAM of the GPU. This error cannot be automatically corrected using the ECC mechanism. The verification process affects system stability and may cause program crashes.	1. View the event metric "ecc.errors.uncorrected.volatile" to check whether there are any uncorrectable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Inconsistent GPU kernel versions	gpuKernelVersionInconsistencyAlarm	Major	Inconsistent GPU kernel versions. During driver installation, the GPU driver is compiled based on the kernel at that time. If the kernel versions are identified inconsistent, the kernel has been customized after the driver installation. In this case, the driver would become unavailable and needs to be reinstalled.	1. Run the following commands to rectify the issue: rmmod nvidia_drm rmmod nvidia_mode set rmmod nvidia Then, run nvidia-smi. If the command output is normal, the issue has been rectified. 2. If the preceding solution does not work, rectify	The GPU cannot work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						the fault by referring to	
		GPU monitoring dependency not met	gpuCheckEnvFailedAlarm	Major	The plug-in cannot identify the GPU driver library path.	1. Check whether the driver is installed. 2. Check whether the driver installation directory has been customized. The driver needs to be installed in the default installation directory <code>/usr/bin/</code>.	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Initialization failure of the GPU monitoring driver library	gpuDriverInitFailedAlarm	Major	The GPU driver is unavailable.	Run nvidia-smi to check whether the driver is unavailable. If the driver is unavailable, reinstall the driver by referring to .	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Initialization timeout of the GPU monitoring driver library	gpuDriverInitTAlarm	Major	The GPU driver initialization timed out (exceeding 10s).	1. If the driver is not installed, install it by referring to . 2. If the driver is installed, run nvidia-smi to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to . 3. If the driver is properly installed, check whether the high-	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						performance mode is enabled. If not, run nvidia-smi -pm 1 to enable it. P0 indicates the high-performance mode.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU metric collection timeout	gpuCollectMetricTimeoutAlarm	Major	The GPU metric collection timed out (exceeding 10s).	1. If the library API timed out, run nvidia-smi to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to . 2. If the command execution timed out, check the system logs and determine whether there is an issue with	GPU monitoring metric data is missing. As a result, subsequent metrics may fail to be collected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						the system .	
		GPU handle lost	gpuDeviceHandleLost	Major	The GPU metric information cannot be obtained, and the GPU may be lost.	1. Run nvidia-smi to check whether there are any errors reported. 2. Run nvidia-smi -L to check whether the number of GPUs is the same as the server specifications. 3. Submit a service ticket to contact on-call support.	All metrics of the GPU are lost.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to listen to the XID of the GPU.	gpuDeviceXidLost	Major	Failed to listen to the XID metric.	1. Check whether the GPU is lost or damaged. 2. Submit a service ticket to contact on-call support.	Failed to obtain XID-related metrics of the GPU.
		Multiple NPU HBM ECC errors	NpuHbmMultiEccInfo	Informational	There are NPU HBM ECC errors.	This event is only a reference for other events. You do not need to handle it separately.	The NPU may not work properly.
		ReadOnly issues in OS	ReadOnlyFileSystem	Critical	The file system %s is read-only.	Check the disk health status.	The files cannot be written.
		NPU: driver and firmware not matching	NpuDriverFirmwareMismatch	Major	The NPU's driver and firmware do not match.	Obtain the matched version from the Ascend official website and reinstall it.	NPUs cannot be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: Docker container environment check	NpuContainerEnvSystem	Major	Docker was unavailable.	Check if Docker is normal.	Docker cannot be used.
				Major	The container plug-in Ascend-Docker-Runtime was not installed.	Install the container plug-in Ascend-Docker-Runtime. Or, the container cannot use Ascend cards.	NPUs cannot be attached to Docker containers.
				Major	IP forwarding was not enabled in the OS.	Check the net.ipv4.ip_forward configuration in the /etc/sysctl.conf file.	Docker containers experience network communication problems.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
				Major	The shared memory of the container was too small.	The default shared memory is 64 MB, which can be modified as needed. Method 1 Modify the default-shm-size field in the /etc/docker/daemon.json configuration file. Method 2 Use the --shm-size parameter in the docker run command to set the shared memory size of a container.	Distributed training will fail due to insufficient shared memory.
		NPU: RoCE NIC down	RoCELinkStatusDown	Major	The RoCE link of NPU card %d was down.	Check the NPU RoCE network port status.	The NPU NIC becomes unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: RoCE NIC health status abnormal	RoCEHealthStatusError	Major	The RoCE network health status of NPU %d was abnormal.	Check the health status of the NPU RoCE NIC.	The NPU NIC becomes unavailable.
		NPU: RoCE NIC configuration file <code>/etc/hccn.conf</code> not found	HccnConfNotExisted	Major	The RoCE NIC configuration file <code>/etc/hccn.conf</code> was not found.	Check whether the <code>/etc/hccn.conf</code> NIC configuration file can be found.	The RoCE NIC becomes unavailable.
		GPU: basic components abnormal	GpuEnvironmentSystem	Major	The nvidia-smi command was abnormal.	Check whether the GPU driver is normal.	The GPU driver is unavailable.
				Major	The nvidia-fabricmanager version was inconsistent with the GPU driver version.	Check the GPU driver version and nvidia-fabricmanager version.	The nvidia-fabricmanager cannot work properly, affecting GPU usage.
				Major	The container plug-in nvidia-container-toolkit was not installed.	Install the container plug-in nvidia-container-toolkit.	GPUs cannot be attached to Docker containers.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Local disk attachment inspection	Mount DiskSystem	Major	The /etc/fstab file contains invalid UUIDs.	Ensure that the UUIDs in the /etc/fstab configuration file are correct. Or, the server may fail to be restarted.	The disk attachment process fails, preventing the server from restarting.
		GPU: incorrectly configured dynamic route for Ant series server	GpuRouteConfigError	Major	The dynamic route of the NIC %s of an Ant series server was not configured or was incorrectly configured. CMD [ip route]: %s CMD [ip route show table all]: %s.	Configure the RoCE NIC route correctly.	The NPU network communication will be interrupted.
		NPU: RoCE port not split	RoCEUdpConfigError	Major	The RoCE UDP port was not split.	Check the RoCE UDP port configuration on the NPU.	The communication performance of NPUs is affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Warning of automatic system kernel upgrade	Kernel UpgradeWarning	Major	Warning of automatic system kernel upgrade. Old version: %s; new version: %s.	System kernel upgrade may cause AI software exceptions. Check the system update logs and prevent the server from restarting.	The AI software may be unavailable.
		NPU environment command detection	NpuToolsWarning	Major	The hcn_tool was unavailable.	Check whether the NPU driver is normal.	The IP address and gateway of the RoCE NIC cannot be configured.
				Major	The npu-smi was unavailable.	Check whether the NPU driver is normal.	NPUs cannot be used.
				Major	The ascend-dmi was unavailable.	Check whether ToolBox is properly installed.	ascend-dmi cannot be used for performance analysis.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Warning of an NPU driver exception	NpuDriverAbnormalWarning	Major	The NPU driver was abnormal.	Reinstall the NPU driver.	NPUs cannot be used.
		GPU: invalid RoCE NIC configuration	GpuRoceNicConfigurationCorrect	Major	The RoCE NIC of the GPU is incorrectly configured.	Contact O&M personnel.	The parameter plane network is abnormal, preventing the execution of the multi-node task.
		Local disk replacement to be authorized	localdisk_recovery_inquiring	Major	The local disk is faulty. Local disk replacement authorization is in progress.	Authorize local disk replacement.	Local disks are unavailable.
		Local disks being replaced	localdisk_recovery_executing	Major	The local disk is faulty and is being replaced.	When the replacement is complete, check whether the local disks are available.	Local disks are unavailable.

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

Table 6-7 Elastic IP (EIP)

Event Source	Name space	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 released 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 was 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)		
		EIP unbound with resources	EipNot Bound Status	Major	The EIP is unbound with instance resources.	None	When an EIP is unbound, you will be billed for IP reservation fees and bandwidth fees (billed by bandwidth).

Table 6-8 Advanced Anti-DDoS (AAD)

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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Blackhole event	blackHoleEvents	Major	The attack traffic exceeds the purchased AAD protection threshold.	A blackhole is canceled after 30 minutes by default. The actual blackhole duration is related to the blackhole triggering times and peak attack traffic on the current day. The maximum duration is 24 hours. If you need to permit access before a blackhole becomes ineffective, contact technical support.	Services may be interrupted.
		Cancel Blackhole	cancelBlackHole	Informational	The customer's AAD instance recovers from the black hole state.	This is only a prompt and no action is required.	Customer services recover.
		IP address scheduling triggered	ipDispatchEvents	Major	IP route changed	Check the workloads of the IP address.	Services are not affected.

Table 6-9 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 6-10 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	Name space	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 6-11 Relational Database Service (RDS) — resource exception

Event Source	Name Space	Event Name	Event ID	Event Severity	Description	Solution	Impact
RDS	SYS.RDS	DB instance creation failure	createInstanceFailed	Major	Generally, the cause is that the number of disks is insufficient due to quota limits, or underlying resources are exhausted.	The selected resource specifications are insufficient. Select other available specifications and try again.	DB instances cannot be created.
		Full backup failure	fullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Try again.	Full backup failed.
		Read replica promotion failure	activeStandbySwitchFailed	Major	The standby DB instance does not take over workloads from the primary DB instance due to network or server failures. The original primary DB instance continues to provide services within a short time.	Perform the switchover again during off-peak hours.	The primary/standby switchover will fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication status abnormal	abnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	Database replication is being repaired. You will be notified immediately after the repair.	The replication status is abnormal.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication status recovered	replicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	Check whether services are running properly.	Replication status is recovered.
		DB instance faulty	faultyDBInstance	Major	A single or primary DB instance was faulty due to a catastrophic failure, for example, server failure.	Instance status is being repaired. You will be notified immediately after the repair.	The instance status is abnormal.
		DB instance recovered	DBInstanceRecovered	Major	RDS rebuilds the standby DB instance with its high availability. After the instance is rebuilt, this event will be reported.	The DB instance status is normal. Check whether services are running properly.	The instance is recovered.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of changing single DB instance to primary/standby	singleToHaFailed	Major	A fault occurs when RDS is creating the standby DB instance or configuring replication between the primary and standby DB instances. The fault may occur because resources are insufficient in the data center where the standby DB instance is located.	Automatic retry is in progress.	Changing a single DB instance to primary/standby failed.
		Database process restarted	DatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Check whether services are running properly.	The primary instance is restarted. Services are interrupted for a short period of time.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance storage full	instanceDiskFull	Major	Generally, the cause is that the data space usage is too high.	Scale up the storage.	The instance storage is used up. No data can be written into databases.
		Instance storage full recovered	instanceDiskFullRecovered	Major	The instance disk is recovered.	Check whether services are running properly.	The instance has available storage.
		Kafka connection failed	kafkaConnectionFailed	Major	The network is unstable or the Kafka server does not work properly.	Check whether services are affected.	None

Table 6-12 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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description
		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 6-13 Document Database Service (DDS)

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	SYS.DDS	DB instance creation failure	DDSCreatelInstanceFailed	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: 1. 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. 2. The network between the primary instance and the standby instance or a read replica is	Submit a service ticket.	1. Read and write operations on the original instance are not interrupted, but data updates on the standby instance may experience delays. 2. The replication delay keeps growing between the primary and standby instances, and the standby instance may be disconnected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					disconnected.		
		Replication status recovered	DDSR eplica tionSt atusR ecove red	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	DDSF aulty DBIns tance	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	DDS DBIns tance Recov ered	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	DDSPPrimaryStandbySwitchover	Major	This event is reported when a primary/standby switchover or a failover is triggered.	No action is required.	None

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Insufficient storage space	DDSRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
		Data disk expanded and being writable	DDSDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No further action is required.	No adverse impact.
		Schedule for deleting a KMS key	planDeleteKmsKey	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
		Full backup failure	DDSFullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Try again.	Full backup fail.

Table 6-14 GeminiDB

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GeminiDB	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	NoSQL ResizeInstanceFailed	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	NoSQL AddNodesFailed	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	NoSQL DeleteNodesFailed	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	NoSQL ScaleUpStorageFailed	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	NoSQL ResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
		Parameter group change failed	NoSQL UpdateInstanceParameterGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
		Backup policy configuration failed	NoSQL SetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
		Manual backup creation failed	NoSQL CreateManualBackupFailed	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	NoSQL CreateAutomatedBackupFailed	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	NoSQL Faulty DBInstance	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	NoSQL DBInstanceRecovered	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	NoSQL Faulty DBNode	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	NoSQL DBNodeRecovered	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	NoSQL PrimaryStandbySwitched	Major	This event is reported when a primary/secondary switchover or 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	BigKey Occurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	1. Choose a proper partition key. 2. Add a new partition key for hashing data.	As the data in the large partition increases, the cluster stability deteriorates.
		Insufficient storage space	NoSQL RiskyDataDiskUsage	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	NoSQL DataDiskUsageRecovered	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	NoSQL CreateIndexFailed	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	NoSQL StallingsOccurs	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	NoSQL StoppingOccurs	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	NoSQL Restart DBFailed	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	NoSQL RestoreToNewInstanceFailed	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	NoSQL RestoreToExistingInstanceFailed	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	NoSQL DeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
		Failed to enable Show Original Log	NoSQL SwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the <i>GaussDB NoSQL User Guide</i> to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None
		EIP binding failed	NoSQL BindEIPFailed	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	NoSQL UnbindEipFailed	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	NoSQL ModifyParameterFailed	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	NoSQL ApplyParameterGroupFailed	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	NoSQL SwitchSSLFailed	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	planDeleteKmsKey	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GeminiDB Influx instance connection limit reached	InfluxDBConnectionFull	Major	The connections on the instance node reach the upper limit.	1. Upgrade specifications if they cannot meet service requirements. 2. Check whether the client properly manages connections, for example, whether there are unreleased or long connections.	If no new connection can be created on a node, the client may fail to connect to a GeminiDB Influx instance. As a result, services may become unstable.
		High availability switchover	nodeHaSwitch	Major	The high availability switchover is triggered by underlying network jitters.	Check whether the business is normal and it can be restored automatically.	The network jitter causes a few seconds of delay.

Table 6-15 TaurusDB

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
TaurusDB	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	Taurus DeleteReadOnlyNodeFailed	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	Taurus ResetInstancePasswordFailed	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	Taurus RestartInstanceFailed	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.	Backup data fails to be restored to new instances.
		EIP binding failure	TaurusBindingEIPToInstanceFailed	Major	The binding task fails.	Submit a service ticket.	EIPs fail to be bound to instances.
		EIP unbinding failure	TaurusUnbindingEIPFromInstanceFailed	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.	Backup jobs fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Primary / standby failover	Taurus ActiveStandby Switched	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	NodeReadOnly Mode	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	NodeReadWrite Mode	Major	The database supports both write and read operations.	Submit a service ticket.	None
		Instance DR switchover	DisasterSwitch Over	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	Taurus DatabaseProcessRestarted	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 6-16 GaussDB

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	SYS.GAUSSDB.V5	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 faulty, 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	Other Abnormal Alarm	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.
		DB instance creation failure	Gauss DBV5 Create Instance Failed	Major	Instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.
		Node adding failure	Gauss DBV5 Expand Cluster Failed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Storage scale-up failure	GaussDBV5EnlargeVolumeFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
		Reboot failure	GaussDBV5RestartInstanceFailed	Major	The network is abnormal.	Retry the reboot operation or submit a service ticket to the O&M personnel.	The database service may be unavailable.
		Full backup failure	GaussDBV5FullBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
		Differential backup failure	GaussDBV5DifferentialBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
		Backup deletion failure	GaussDBV5DeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		EIP binding failure	GaussDBV5 BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the public network.
		EIP unbinding failure	GaussDBV5 UnbindEIPFailed	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	GaussDBV5 ApplyParameterFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
		Parameter modification failure	GaussDBV5 UpdateInstanceParameterGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
		Backup and restoration failure	GaussDBV5 RestoreFromBackupFailed	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to upgrade the hot patch	GaussDBV5 UpgradeHotfixFailed	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
		DB instance faulty	GaussDBV5 FaultyDBInstance	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	GaussDBV5 InstanceRecovered	Major	GaussDB provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No action is required.	None
		Faulty node	GaussDBV5 FaultyDBNode	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.	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	The database service may be unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Node recovered	GaussDBV5 FaultyDBNodeRecovered	Major	GaussDB provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No action is required.	None

Table 6-17 Distributed Database Middleware (DDM)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDM	SYS.DDM (DDM 1.0)	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.
	SYS.DDMS (DDM 2.0)	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 6-18 Cloud Phone Server

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	SYS.CPH	Server shutdown	cloudPhoneServerShutdown	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	cp hS erv erS hut do wn	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	cp hS erv er Os Re boot	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	cp hS erv erR eb oot	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	cp hS erv link Down	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	cp hS erv PCIe Error	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 services are affected.
		Disk error	cp hS erv DiskError	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	cp hS erv erS tor ag eEr ror	Major	The cloud phone server could not 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.
		GPU offline	cp hS erv er Gp uOff lin e	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	cp hS erv er Gp uTi me Ou t	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	cp hS erv er Dis kF ull	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 read only	cp hS erv er Dis kR ea dO nly	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	cpHPoneMetaDamage	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.	None
		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	pciError	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 /.sharepath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.sharepath/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 6-19 Layer 2 Connection Gateway (L2CG)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	SYS.ESW	IP addresses conflicted	IPC onflict	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 6-20 Virtual Private Cloud (VPC)

Event Source	Namespace	Event Name	Event ID	Event Severity
VPC	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 6-21 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 NOTE This event is no longer supported for EVS and will be removed from Cloud Eye.	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 6-22 Identity and Access Management (IAM)

Event Source	Na me spa ce	Event Name	Event ID	Event Severity
IAM	SYS .IA M	Login	login	Minor
		Logout	logout	Minor
		Password changed	changePasswor d	Major
		User created	createUser	Minor
		User deleted	deleteUser	Major
		User updated	updateUser	Minor
		User group created	createUserGro up	Minor
		User group deleted	deleteUserGro up	Major
		User group updated	updateUserGro up	Minor
		Identity provider created	createIdentityP rovider	Minor
		Identity provider deleted	deleteIdentityP rovider	Major
		Identity provider updated	updateIdentity Provider	Minor
		Metadata updated	updateMetada ta	Minor
		Security policy updated	updateSecurity Policies	Major
		Credential added	addCredential	Major
		Credential deleted	deleteCredenti al	Major
		Project created	createProject	Minor
		Project updated	updateProject	Minor
		Project suspended	suspendProject	Major

Table 6-23 Key Management Service (KMS)

Event Source	N a m e s p a c e	Event Name	Event ID	Even t S e v e r i t y	Descrip tion	Solutio n	Impact
KMS	SY S. K M S	Key disabled	disableKey	Maj or	A key is disable d and cannot be used.	If the custom er needs to disable the key, no action is require d. Howev er, if the key is disable d by mistak e, the custom er needs to log in to the DEW console and enable it again.	Services may be affected if the key is being used.

Event Source	N a m e s p a c e	Event Name	Event ID	Even t Seve rity	Descrip tion	Solutio n	Impact
		Key deletion scheduled	scheduleKey Deletion	Minor	A key is scheduled to be deleted and cannot be used.	If the customer needs to delete the key, no action is required. However, if the deletion of the key is scheduled by mistake, the customer needs to log in to the DEW console , cancel the scheduled deletion, and enable the key again.	Services may be affected if the key is being used.

Event Source	N a m e s p a c e	Event Name	Event ID	Even t Seve rity	Descrip tion	Solutio n	Impact
		Grant retired	retireGrant	Maj or	A grant is retired and the key cannot be used.	If the custom er needs to cancel the key grant, no action is require d. Howev er, if the grant is canceled by mistak e, the custom er needs to log in to the DEW console and create the grant again.	Services may be affected if the key is being used.

Event Source	N a m e s p a c e	Event Name	Event ID	Even t Seve rity	Descrip tion	Solutio n	Impact
		Grant revoked	revokeGrant	Maj or	A grant is revoked and the key cannot be used.	If the custom er needs to cancel the key grant, no action is require d. Howev er, if the grant is canceled by mistak e, the custom er needs to log in to the DEW console and create the grant again.	Services may be affected if the key is being used.

Table 6-24 Object Storage Service (OBS)

Event Source	Na me spa ce	Event Name	Event ID	Event Severity
OBS	SYS .OB S	Bucket deleted	deleteBucket	Major
		Bucket policy deleted	deleteBucketP olicy	Major
		Bucket ACL configured	setBucketAcl	Minor
		Bucket policy configured	setBucketPolic y	Minor

Table 6-25 Cloud Eye

Event Source	Name Space	Event Name	Event ID	Event Severity	Description	Solution	Impact
Cloud Eye	SY S.C ES	Agent heartbeat interruption	agentHeartbeatInterrupted	Major	The collecting process of the Agent is 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.	The Agent will stop collecting and reporting metrics.

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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Agent back to normal	agentResumed	Informational	The Agent was back to normal.	No action is required.	None
		Agent faulty	agentFaulted	Major	The Agent was faulty and this status was reported to Cloud Eye.	The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. Update the Agent to the latest version.	The Agent will stop collecting and reporting metrics.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Agent disconnected	agentDisconnected	Major	The communication process of the Agent is 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	The Agent will stop collecting and reporting metrics.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
						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 6-26 Enterprise Switch

Event Source	Name space	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 6-27 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	operateDeleteSecret	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 6-28 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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Automatic failover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check whether services can recover by themselves. If applications are not recovered, restart them.	Persistent connections to the instance are interrupted.
		Memcached master/standby switchover	memcachedMasterStandbyFailover	Minor	The master node was abnormal, promoting the standby node to master.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance will be interrupted.

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

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance will be interrupted.
		Long-running Lua scripts stopped	scriptStopped	Informational	Lua scripts that had timed out automatically stopped running.	Optimize Lua scripts to prevent execution timeout.	The execution of the lua scripts takes a long time and is forcibly interrupted. If the execution of the lua scripts takes a long time, the entire instance will be blocked.
		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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Bandwidth scaling	bandwidthAutoScalingTriggered	Informational	Instance bandwidth used up.	Check the services on this instance.	A bandwidth increase incurs fees.
		Specification auto scaling triggered	specAutoScalingTriggered	Informational	Instance specifications auto scaling was triggered.	Check the services on this instance.	The instance specifications were used up, triggering auto scaling. The billing will be changed if the instance specifications are changed.
		Instance specifications scaled	specAutoScalingTriggeredSuccess	Informational	The instance specifications were scaled successfully.	Check the services on this instance.	Instance scaled up. Check its information.
		Instance specifications failed	specAutoScalingTriggeredFail	Critical	The instance specifications fail to be scaled.	Contact technical support.	Instance scaling failed. Log in to the console to check whether services are affected.

Table 6-29 Intelligent Cloud Access (ICA)

Event Source	Name space	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	Na me spa ce	Event Name	Event ID	Eve nt Seve rity	Descriptio n	Solution	Impact
		Intelligen t enterprise gateway going offline	Intelli gentE nterpr iseGat eway Going Offlin e	Maj or	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 6-30 Host Security Service (HSS)

Event Source	Na me spa ce	Event Name	Event ID	Eve nt Seve rity	Descriptio n	Solution	Impact
HSS	SYS .HS S	HSS agent disconnec ted	hssAg entAb norm alOffli ne	Maj or	The communica tion between the agent and the server is abnormal, or the agent process on the server is abnormal.	Fix your network connection . If the agent is still offline for a long time after the network recovers, the agent process may be abnormal. In this case, log in to the server and restart the agent process.	Services are interrupte d.

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

Table 6-31 Cloud Storage Gateway (CSG)

Event Source	Na me spa ce	Event Name	Event ID	Event Severity	Description
CSG	SYS .CS G	Abnormal CSG process status	gatewayProcessStatusAbnormal	Major	This event is triggered when an exception occurs in the CSG process status.

Event Source	Na me spa ce	Event Name	Event ID	Event Severity	Description
		Abnormal CSG connection status	gatewayT oServiceC onnectAb normal	Major	This event is triggered when no CSG status report is returned for five consecutive periods.
		Abnormal connection status between CSG and OBS	gatewayT oObsConn ectAbnor mal	Major	This event is triggered when CSG cannot connect to OBS.
		Read-only file system	gatewayFi leSystemR eadOnly	Major	This event is triggered when the partition file system on CSG becomes read-only.
		Read-only file share	gatewayFi leShareRe adOnly	Major	This event is triggered when the file share becomes read-only due to insufficient cache disk storage space.

Table 6-32 Enterprise connection

Event Source	Na me spa ce	Event Name	Event ID	Event Severity	Description	Solution	Impact
EC	SYS .EC	WAN interface goes up	Equipm entWan GoesOn line	Major	The WAN interface goes online.	None	None

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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 6-33 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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Certificate auto-deployment failure	CCMAutoDeploymentFailure	Major	The certificate fails to be automatically deployed.	Check service resources whose certificates need to be replaced.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.
		Certificate expiration	CCMCertificateExpiration	Major	An SSL certificate has expired.	Purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Certificate about to expire	CCMCertificateAboutToExpiration	Major	This alarm is generated when an SSL certificate is about to expire in one week, one month, and two months.	Renew or purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.
		Private certificate is about to expire	CCMPrivateCertificateAboutToExpiration	Major	A private certificate is considered about to expire if it is within 7 or 30 days of its expiration date.	Purchase a new private certificate in a timely manner.	If no new private certificate has been deployed before certificate expires, services may be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Private CA is about to expire	CCMPrivateCAAboutToExpiration	Major	A private CA is considered about to expire if it is within one month, three months, or six months of its expiration date.	Purchase a new private CA in a timely manner.	If no new CA has been deployed before a private CA expires, services may be interrupted.

Table 6-34 Workspace

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
Workspace	SYS.Workspace	Abnormal desktop heartbeat	desktopStatusAbnormal	Major	The network is disconnected or the key is lost.	1. Restart the desktop. 2. Check whether the desktop time is the current time. If not, change the desktop time to the current time. 3. Check whether special security software or network connection	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						software is installed on the desktop. If so, uninstall the software and restart the system. Alternatively, uninstall the software, reinstall the HDC Agent, and restart the system.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of assigning desktops in a desktop pool	desktopPoolAssignFailed	Major	This fault is caused by policies.	1. Adjust the desktop pool policy to ensure that there are idle desktops in the desktop pool or desktops can be automatically created. 2. If Linux desktops cannot be assigned to users with digit-only usernames, enable	New desktops cannot be assigned.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						Use the username prefix function.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Desktop access failure	desktopAccessFailed	Major	This fault is caused by VM stopping and restart, access gateway exceptions, or network faults.	1. If you stop or restart a VM, wait for a period of time and try again when the desktop status is normal. 2. Check the network environment and reconnect to the network when the network is normal.	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Desktop startup failure	desktopStartFailed	Major	The underlying resources are insufficient.	Wait for a while and try again.	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of automatic desktop pool capacity expansion	desktopPoolExpandFailed	Major	The instance quota or underlying resources are insufficient.	1. If the quota is insufficient, request a higher quota (such as the number of desktops, CPUs, memory, and VPCs). 2. If underlying resources are insufficient, make purchases in the next capacity expansion period.	Desktop capacity cannot be expanded.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						3. If automatic desktop capacity expansion is not required, disable the function of automatic desktop pool capacity expansion.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of migrating a desktop running on a dedicated host	desktopMigrateFailed	Major	The host malfunctions.	1. Replace the faulty host with a normal one. 2. Contact technical support to rectify the host fault.	No dedicated host is available for desktop scheduling.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		User login failure	userLoginFailed	Major	The client network is disconnected, or the enterprise ID, username, or password is incorrect.	1. Check the network environment and reconnect to the network when the network is normal. 2. Check whether the enterprise ID, username, and password are valid.	Desktops or applications are unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Screen recording failure	screenRecordFailed	Major	An unknown exception occurred on the desktop.	1. Try reconnecting to the desktop. 2. Check whether special security software is installed on the desktop. If it is, uninstall the software and restart the system.	Screen recording malfunctions and the desktop is disconnected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Screen recording upload failure	screenRecordUploadFailed	Major	The network between the desktop and OBS malfunctions.	1. Check whether the desktop network is normal. 2. Check whether security group interception has been configured. 3. Check whether interception on access control with VPCEP and OBS has been configured.	Screen recording file upload failed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Damaged screen recording file	screenRecordFileDamaged	Major	The screen recording file was maliciously damaged.	1. Wait until the screen recording function is automatically restored. 2. Check whether malicious damage occurs.	The screen recording file is abnormal.
		Abnormal agent process	agentAbnormal	Major	The agent process has been killed or reset.	The agent process can be automatically restarted after being killed.	Functions such as application control and upgrade will be affected.
		Bypassing controlled applications	appRestrictFailed	Major	The application control agent was continuously killed.	Check whether a script is used to continuously kill the application control agent.	Application control will fail.

7 Access Center

7.1 Custom Monitoring

7.1 Custom Monitoring

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

Prerequisites

You have added monitoring data using APIs, which will be displayed on the Cloud Eye console. For details about how to add monitoring data, see [Adding Monitoring Data](#).

Viewing Custom Monitoring

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Custom Monitoring**.
3. On the **Custom Monitoring** page, view the data reported by yourself through API requests, including custom services and metrics.
4. Locate the row that contains the cloud resource to be viewed, and click **View Metric**.

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

Creating an Alarm Rule

You can create an alarm rule for a custom metric. If the metric surpasses its limit, Cloud Eye alerts you immediately, keeping you informed in real time.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Custom Monitoring**.

3. On the **Custom Monitoring** page, locate the resource and click **Create Alarm Rule** in the **Operation** column.
4. On the **Create Alarm Rule** page, configure parameters. For details, see [Table 5-2](#) and [Table 5-4](#).
5. Click **Create**.

8 Data Dump

[8.1 Overview](#)

[8.2 Dumping Data](#)

[8.3 Modifying, Deleting, Enabling, or Disabling a Dump Task](#)

8.1 Overview

You can dump key metric data to DMS for Kafka in real time for further analysis or other data consumption.

You can use the data dump function to query metrics on the DMS for Kafka console or on an open-source Kafka client.

8.2 Dumping Data

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.

Constraints

- You can create a maximum of 20 data dump tasks per account.
- Data dump is available only for whitelisted customers.

Procedure

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Data Dump**.
3. Click **Add Dump Task** in the upper right corner.
4. On the **Add Dump Task** page, configure parameters by referring to [Table 8-1](#).

Table 8-1 Parameters for configuring a dump task

Parameter	Description	Example Value
Name	Name of the data dump task. The system generates a name randomly, and you can change it as you want. The name can include 1 to 64 characters and contain only letters, digits, underscores (_), and hyphens (-).	dataShareJob-ECSMetric
Resource Type	Type of resources monitored by Cloud Eye.	Elastic Cloud Server
Dimension	This parameter is used to filter specified monitoring data. For details about the dimensions of monitored objects of each service, see 10 Cloud Product Metrics . For example, if Resource Type is set to Elastic Cloud Server , the dimensions can be: • If All is selected, all metrics of the selected service will be dumped to DMS for Kafka. • If ECSs is selected, ECS metrics will be dumped to DMS for Kafka.	All
Monitoring Scope	Dimension of the monitored object. The scope can only be All resources , indicating that all metrics of the specified monitored object will be dumped to DMS for Kafka.	All resources
Resource Type	Destination cloud service of the dumped data. Currently, data can be dumped only to DMS for Kafka.	DMS for Kafka
Project Name	IAM project name of the account for saving dumped data.	-
Destination	Kafka instance and topic where the metric data is to be dumped. If no Kafka instance is available, see Buying a Kafka Instance and Creating a Kafka Topic .	-

5. Click **Add** after the configuration is complete.

 NOTE

You can query the dumped data in Kafka. For details, see [Viewing Kafka Messages](#).

8.3 Modifying, Deleting, Enabling, or Disabling a Dump Task

If the service changes or the previously configured data dump settings do not meet your requirements, you can modify, disable, enable, or delete the dump tasks as needed.

Modifying a Dump Task

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Data Dump**.
3. Locate the target dump task and click **Modify** in the **Operation** column.
4. Modify the task settings by referring to [Table 8-1](#).
5. Click **Modify**.

Disabling a Dump Task

NOTE

Once you disable a dump task, collected monitoring data will not be dumped but existing data is still saved.

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Data Dump**.
3. On the **Data Dump** page, perform the following operations to disable a data dump task.
 - Locate the dump task and click **Disable** in the **Operation** column. In the displayed **Disable Dump Task** dialog box, click **OK**.
 - Select one or more dump tasks to be disabled and click **Disable** above the list. In the displayed dialog box, click **OK**.

Enabling a Dump Task

NOTE

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

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Data Dump**.
3. On the **Data Dump** page, perform the following operations to enable a data dump task:
 - Locate a disabled dump task and click **Enable** in the **Operation** column. In the displayed **Enable Dump Task** dialog box, click **OK**.
 - Select the dump task to be enabled and click **Enable** above the list. In the displayed dialog box, click **OK**.

Deleting a Dump Task

NOTE

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

1. Log in to the [Cloud Eye console](#).
2. In the navigation pane, choose **Data Dump**.
3. On the **Data Dump** page, locate the target dump task and click **Delete** in the **Operation** column.
4. In the **Delete Dump Task** dialog box, click **OK**.

9 Quotas

What Are Quotas?

Quotas are used to control service resources and avoid unexpected surges in usage. Quotas can limit the quantity and capacity of resources available to users, such as the maximum number of ECSs or EVS disks they can create.

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 **Quotas** 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.

How Do I Apply for a Higher Quota?

1. Log in to the [management console](#).
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Quotas** page is displayed.
3. Click **Increase Quota** in the upper right corner of the page.
4. On the **Create Service Ticket** page, configure parameters as required.
In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

10 Cloud Product Metrics

Category	Service	Namespace	Dimension	Reference
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECSs	ECS metrics
	Elastic Cloud Server – OS Monitoring	AGT.ECS	• Key: instance_id Value: ECSs • Key: roce Value: RoCE • Key: disk Value: Disk • Key: mount_point Value: Mount Point • Key: gpu Value: GPU • Key: npu Value: NPU • Key: davn Value: DAVP • Key: network_interface_card Value: NICs • Key: proc Value: Process	OS monitoring metrics supported by ECSs with the Agent installed

Category	Service	Namespace	Dimension	Reference
	Elastic Cloud Server – Process Monitoring	AGT.ECS	• Key: instance_id Value: ECSs • Key: pname Value: Process • Key: pid Value: ProcessIDs	Process monitoring metrics supported by ECSs with the Agent installed
	Bare Metal Server	SERVICE.BMS	• Key: instance_id Value: ECSs • Key: disk_error_monitor Value: Disk Error Monitor • Key: proc Value: Process • Key: pname Value: Process • Key: pid Value: ProcessIDs • Key: disk Value: Disk • Key: mount_point Value: Mount Point • Key: gpu Value: GPU • Key: npu Value: NPU • Key: roce Value: RoCE • Key: network_interface_card Value: NICs	OS monitoring metrics supported by BMSs with the Agent installed

Category	Service	Namespace	Dimension	Reference
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: AS group ID	AS metrics
	FunctionGraph	SYS.FunctionGraph	Key: package-functionname Value: <i>App name-Function name</i>	FunctionGraph metrics
Storage	Elastic Volume Service (attached to an ECS or BMS)	SYS.EVS	Key: disk_name Value: server ID-drive letter (sda is the drive letter.)	EVS metrics
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name	OBS metrics
	Scalable File Service Turbo	SYS.EFS	Key: efs_instance_id Value: Instances	SFS Turbo metrics
	Cloud Backup and Recovery	SYS.CBR	Key: instance_id Vault: vault name/ID	CBR metrics
Networking	Virtual Private Cloud	SYS.VPC	- Key: publicip_id Value: EIP ID - Key: bandwidth_id Value: bandwidth ID	VPC metrics

Category	Service	Namespace	Dimension	Reference
	Elastic Load Balance	SYS.ELB	- Key: lb_instance_id Value: ID of a classic load balancer - Key: lbaas_instance_id Value: ID of a shared load balancer - Key: lbaas_listener_id Value: ID of a shared load balancer listener	ELB metrics
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID	NAT Gateway metrics
	Enterprise Router	SYS.ER	- Key: er_instance_id Value: enterprise router - Key: er_attachment_id Value: Enterprise router attachment	ER metrics
	Virtual Private Network	SYS.VPN	Key: evpn_connection_id Value: S2C VPN Connection	VPN metrics

Category	Service	Namespace	Dimension	Reference
	Direct Connect	SYS.DCAAS	- Key: direct_connect_id Value: connection - Key: history_direct_connect_id Value: historical connection	Direct Connect metrics
	Global Accelerator	SYS.GA	- Key: ga_accelerator_id Value: ID of the global accelerator - Key: ga_listener_id Value: ID of a listener added to the global accelerator	Global Accelerator metrics
App middle ware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.	DMS for Kafka metrics RabbitMQ metrics DMS for RocketMQ metrics
	API Gateway	SYS.APIC	For details, see the information in the right column.	API Gateway metrics

Category	Service	Namespace	Dimension	Reference
	Distributed Cache Service	SYS.DCS	• Key: dcs_instance_id Value: DCS Redis instance • Key: dcs_cluster_redis_node Value: Redis Server • Key: dcs_cluster_proxy_node Value: Proxy in a Proxy Cluster DCS Redis 3.0 instance • Key: dcs_cluster_proxy2_node Value: Proxies (4.0 and later) • Key: dcs_memcached_instance_id Value: DCS Memcached instance	DCS metrics
Databases	Relational Database Service	SYS.RDS	For details, see the information in the right column.	RDS for MySQL metrics RDS for PostgreSQL metrics RDS for MariaDB metrics

Category	Service	Namespace	Dimension	Reference
	Document Database Service	SYS.DDS	- Key: mongodb_node_id Value: DDS node ID - Key: mongodb_instance_id Value: DDS DB instance ID	DDS metrics
	Distributed Database Middleware	SYS.DDMS	Key: node_id Value: DDM Nodes	DDM metrics
	GeminiDB	SYS.NoSQL	For details, see the information in the right column.	GeminiDB Cassandra metrics GeminiDB Influx metrics GeminiDB Redis metrics

Category	Service	Namespace	Dimension	Reference
	TaurusDB	SYS.GAUSSDB	• Key: gaussdb_mysql_instance_id Value: TaurusDB Instances • Key: gaussdb_mysql_node_id Value: TaurusDB Nodes • Key: dbproxy_instance_id Value: Database Proxy Instance • Key: dbproxy_node_id Value: Database Proxy Node	TaurusDB metrics
	Data Replication Service	SYS.DRS	Key: instance_id Value: DRS instance ID	DRS metrics
Migration	Cloud Data Migration	SYS.CDM	Key: instance_id Value: Instances	CDM metrics
Enterprise Intelligence	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster	CSS metrics

Category	Service	Namespace	Dimension	Reference
	ModelArts	SYS.ModelArts	- Key: service_id Value: real-time service ID - Key: model_id Value: model ID	ModelArts metrics
	Data Lake Insight	SYS.DLI	- Key: queue_id Value: queue instance - Key: flink_job_id Value: Flink job	DLI metrics
	Data Warehouse Service	SYS.DWS	- Key: datastore_id Value: data warehouse cluster ID - Key: dws_instance_id Value: data warehouse node ID	DWS metrics
Security and Compliance	Web Application Firewall	SYS.WAF	- Key: instance_id Value: dedicated WAF instance - Key: waf_instance_id Value: cloud WAF instance	WAF metrics
	Database Security Service	SYS.DBSS	Key: audit_id Value: Instances	DBSS metrics

Category	Service	Namespace	Dimension	Reference
	Cloud Bastion Host	SYS.CBH	Key: server_id Value: CBH instance ID	CBH metrics
	Host Security Service	SYS.HSS	Key: host_id Value: host instance	HSS metrics
	Cloud Firewall	SYS.CFW	Key: fw_instance_id Value: CFW Instances	CFW metrics
Business Applications	Workspace	SYS.Workspace	Key: instance_id Value: Workspace	Workspace metrics