Cloud Eye

Best Practices

Issue	01
Date	2026-11-20



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. 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


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 Alarm Notification Methods....1
1.1 Receiving Alarm Notifications via HTTP/HTTPS....1
1.2 Receiving Alarm Notifications Through WeCom....11
1.3 Receiving Alarm Notifications in a DingTalk Group....12
1.4 Receiving Alarm Notifications in a Lark Group....13
1.5 Receiving Alarm Notifications Using Functions....15
1.6 Applying for SMN New Protocol OBT....21
2 Alarm Configuration Method....23
2.1 Configuring Alarm Notifications by Severity....23
2.2 Masking Alarms by Multiple Metrics or Objects....24
3 Cloud Resource Monitoring....26
3.1 Installing the Agent on Servers....26
3.2 Creating Alarm Rules By Associating Resource Groups with Alarm Templates....32
3.3 Configuring Alarm Rules for Resources by Matching Tags....35
3.4 Recommended Metrics and Alarm Policies for Each Cloud Service....42
4 Cloud Eye Resource Group Configuration....88
4.1 Resource Group Overview....88
4.2 Configuring Resource Groups for Metric Alarms....90
4.3 Configuring Resource Groups for Event Alarms....100
5 Scenario-specific Cases....103
5.1 Service Monitoring on E-Commerce Platforms....103
5.1.1 Overview....103
5.1.2 Server Monitoring....103
5.1.3 Cloud Service Monitoring....105
5.1.4 Resource Groups....106
5.2 Live Streaming Monitoring....107
5.2.1 Overview....107
5.2.2 Server Monitoring....107
5.2.3 ELB Monitoring....110
5.2.4 Network Monitoring....112
5.3 Crowdsourcing Platforms....114
5.3.1 Overview....114

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.3.2 Server Monitoring 115
5.3.3 Network Monitoring 115
5.3.4 Event Monitoring 116
5.4 Best Practices of Event Monitoring 117
5.4.1 ECS Events 117
5.4.2 RDS Events 119
5.4.3 EIP Events 121
5.5 Resource Group Monitoring 123
5.6 Configuring an Alarm Rule for the Disk Usage of All Mount Points on an ECS 125
6 Suggestions on Cloud Eye Security Configuration 126

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Alarm Notification Methods

1.1 Receiving Alarm Notifications via HTTP/HTTPS

In enterprise O&M environments, alarm notifications need to be sent to multiple third-party systems, such as service ticket platforms and in-house monitoring centers. Traditional email and SMS channels are limited in flexibility, allowing only manual message notification. They lack structured parsing, automated transfer, and custom processing capabilities. Alarm notifications can be received through HTTP/HTTPS channels. When an alarm is triggered, the notification is received in JSON format. The notification can be parsed and subsequent logic can be executed as needed, enabling seamless integration of alarms with HTTP-compliant systems and enhancing O&M automation and response efficiency.

When you configure an alarm contact, if you select HTTP or HTTPS as the notification channel and enter a public HTTP/HTTPS address, an alarm notification will be sent to that address when the resource metric reaches the alarm condition.

Procedure

For details about the process and description of receiving alarm notifications through HTTP or HTTPS, see **Table 1-1**.

Table 1-1 Process of receiving alarm notifications through HTTP or HTTPS

No.	Step	Description
1	**Adding an HTTP/HTTPS Public Address for a Contact**	Configure a public address for receiving alarm notifications. When an alarm is triggered, an HTTP/HTTPS request is sent to this address to push structured alarm data.
2	**Creating an Alarm Contact Group and Adding Alarm Contacts**	Define an alarm contact group and add HTTP/HTTPS contacts to the group so that the group can be referenced in alarm rules.

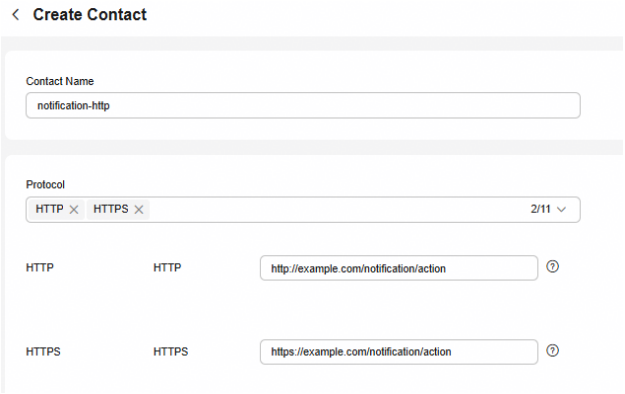
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No.	Step	Description
3	Creating a Notification Template	Create a notification template to ensure that the recipient can parse key fields as required and meet the requirements for structured alarm messages.
4	Creating an Alarm Rule	Set monitoring metrics and alarm policies for triggering alarms, and bind the alarm rules to the contact group and notification template.
5	Viewing Alarm Notifications	Verify that alarms are sent and received as expected.

Adding an HTTP/HTTPS Public Address for a Contact

1. Log in to the Cloud Eye console.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. Click the **Contacts** tab.
4. Click **Create**. The **Create Contact** page is displayed.

Figure 1-1 Creating a contact



5. Configure contact information as prompted, as shown in Table 1-2.

Table 1-2 Parameters for creating a contact

Parameter	Example Value	Description
Contact Name	**notification-http**	Contact name. Enter 1 to 42 characters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

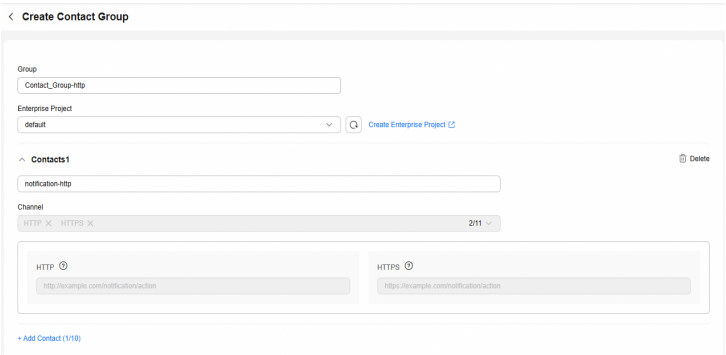
Parameter	Example Value	Description
Protocol	• Select **HTTP** and enter the public network address in the text box of the selected protocol. Example: **http://example.com/notification/action** • Select **HTTPS** and enter the public network address in the text box of the selected protocol. Example: **https://example.com/notification/action** **NOTE** The HTTP/HTTPS address you provide is an accessible public address.	Over which protocol alarm notifications will be sent. Only one object can be added for each protocol.

6. Click **Create**.

Creating an Alarm Contact Group and Adding Alarm Contacts

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. Click the **Contact Groups** tab.
4. Click **Create**. The **Create Contact Group** page is displayed.

Figure 1-2 Creating a contact group



5. Configure contact group information as prompted, as shown in **Table 1-3**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 1-3 Parameters for creating a contact group

Parameter	Example Value	Description
Group	**Contact_Group-http**	Contact group name. Enter 1 to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Enterprise Project	**default**	Enterprise project to which the contact group belongs. Only users with the enterprise project permissions can view and manage the contact group.
Contact	**notification-http**	Click the name text box and select the contact created in **Adding an HTTP/HTTPS Public Address for a Contact** from the drop-down list. The notification protocols configured for the contact are automatically filled in.

6. On the **Create Contact Group** page, click **Create**.

   After the contact is added to the contact group, the corresponding subscription endpoint will receive a subscription notification. The contact should access the link through the corresponding program or copy the link to a web browser to confirm the subscription. Then the contact can receive alarm notifications.

Creating a Notification Template

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. Click the **Notification Templates** tab.
4. Click **Create**. The **Create Notification Template** page is displayed.
5. Configure the notification template information as prompted, as shown in **Table 1-4**.

Table 1-4 Parameters for creating a notification template

Parameter	Example Value	Description
Name	**noticeTemplate-http(s)**	Name of the notification template. The system generates a random name, but you can change it. Enter 1 to 200 characters.
Description	-	(Optional) Description of the alarm notification template.
Protocol	**HTTP/HTTPS**	Select a notification method from the drop-down list.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Notification Type	**Metric** or **Event**	Notification type of the notification content template. When you are configuring an alarm rule, the alarm type of the alarm rule determines the alarm type of the notification template. For example, for a metric alarm rule, you can select only **Metric** for this parameter. For more information about alarm types, see **Overview**.
Format	**JSON**	Data format of the alarm notification content.

6. Click **Create**. On the **Notification Templates** tab, you can view the new notification template whose **Template Type** is **Custom**.

Creating an Alarm Rule

Set monitoring metrics and alarm policies for target resources, and bind the alarm rules to the contact group and notification template.

Configure alarm rule parameters by referring to **Creating an Alarm Rule and Notifications**. The following table lists the alarm notification parameters.

Table 1-5 Alarm notification parameters

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send alarm notifications.
Notified By	**Contact groups** / **Notification_Group-http**	Notification method. You can select notification policies, contact groups, or topic subscriptions.
Notification Window	00:00–23:59 every day	Cloud Eye sends notifications only within the notification window.
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala Lumpur, Singapore, Perth, Taipei, Irkutsk, Ulaanbaatar	Time zone for the alarm notification window. By default, it matches the time zone of the client, but can be manually configured.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Trigger Condition	**Generated alarm** and **Cleared alarm**	If you select a contact group or topic subscription for **Notified By**, you need to select the conditions for triggering alarm notifications. • If the alarm type is metric, you can select **Generated alarm** and **Cleared alarm** as the trigger conditions. • If the alarm type is event, you can only select **Generated alarm**.
Notification Template	**noticeTemplate-http(s)**	Notification content format. Alarm notifications are sent to contacts in the target format.

Viewing Alarm Notifications

When a metric or event triggers an alarm rule, the HTTP/HTTPS public address will receive an alarm notification encapsulated by SMN.

The following describes the fields in metric and event alarm notifications.

Metric Alarm Notification Fields

The following is an example of an alarm notification sent based on a custom metric notification template:


```
{
  "version": "v1",
  "data": {
    "Namespace": "Elastic Cloud Server",
    "DimensionName": "ECSs",
    "MetricName": "CPU Usage",
    "IsAlarm": true,
    "AlarmLevel": "Major",
    "Region": "CN North-Beijing4",
    "RegionId": "cn-north-4",
    "AlarmRuleName": "test-zcy",
    "AccountName": "RDS_test",
    "LastAlarmLevel": "Warning",
    "ResourceID": "853f8ead-428e-4c54-babc-f1bdae6d34a0",
    "PrivateIP": "10.0.0.39",
    "EPName": "default",
    "ResourceName": "ecs-hce330-test",
    "PrivateIPV6": "2407:c080:11f0:1115:490e:36fe:ba94:a410",
    "PublicIP": "100.85.113.106",
    "CurrentData": "100.00 %",
    "Count": 1,
    "IsOriginalValue": true,
    "Filter": "Raw data",
    "ComparisonOperator": ">=",
    "Value": "0%",
    "AlarmTime": "2025/11/17 16:39:42 GMT+08:00",
    "AlarmDesc": "test",
    "AlarmRecordID": "ah17223968140068KqpEA3NP",
    "ResourceDimensionInfos": [
      {
        "MetricName": "CPU Usage",
        "DimensionInfos": [
```

```
        {
          "Name": " ECS,"
          "Value": "853f8ead-428e-4c54-babc-f1bdae6d34a0"
        }
      ]
    }
  ],
  "AlarmNotificationType": "Metric",
  "Unit": "%",
  "ResourceTags": "_sys_type_hcss_x,test=test",
  "AlarmDurationTime": "0"
 }
}
```

Table 1-6 Metric alarm notification fields

Field	Type	Description
Namespace	String	Cloud service name.
DimensionName	String	Dimension name.
MetricName	String	Metric name.
IsAlarm	Boolean	Alarm triggering condition, indicating whether an alarm is generated. • **true**: An alarm is generated. • **false**: No alarm is generated.
AlarmLevel	String	Alarm severity. The value can be **Critical**, **Major**, **Minor**, or **Warning**.
Region	String	Region name, for example, **CN North-Beijing4**.
RegionId	String	Region ID, for example, **cn-north-4**.
AlarmRuleName	String	Alarm rule name.
AccountName	String	Account name.
LastAlarmLevel	String	Severity of the last alarm. The value can be **Critical**, **Major**, **Minor**, or **Warning**. When a metric has several thresholds and the metric data triggers them, the alarm severity updates and this parameter appears in the notification.
ResourceID	String	Resource ID, that is, the dimension value. If there are multiple levels of dimensions, the names and values of all dimensions are displayed.
PrivateIP	String	Private IP address.
EPName	String	Name of the enterprise project to which the resource belongs.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Field	Type	Description
ResourceName	String	Resource name.
PrivateIPV6	String	Private IPv6 address. Currently, only ECSs support this field.
PublicIP	String	Public IP address.
CurrentData	String	Metric value that triggers the alarm.
Count	Integer	Number of consecutive alarm triggers.
IsOriginalValue	Boolean	Whether the metric configured in the alarm policy uses the raw data. • **true**: The metric data is the raw data. • **false**: The metric data is the aggregated data.
Filter	String	Metric value type. The options are average value, variance value, minimum value, maximum value, sum value, and raw data.
ComparisonOperator	String	Comparison between the metric value and the threshold. The comparison operators include **>**, **>=**, **<**, **<=**, **=**, **!=**, **cycle_increase** (period-on-period increase), **cycle_decrease** (period-on-period decrease), and **cycle_wave** (period-on-period fluctuation).
Value	String	Value defined in the alarm rule.
AlarmTime	String	Time when the alarm is generated.
AlarmDesc	String	Description of the alarm rule.
AlarmRecordID	String	Alarm record ID.
ResourceDimensionInfos	Array of objects	Resource dimension information. For details, see **Table 1-7**.
AlarmNotificationType	String	Alarm notification type. The value can be **Metric** or **Event**.
Unit	String	Original unit of the metric.
ResourceTags	String	Resource tags.
AlarmDurationTime	String	Alarm duration.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 1-7 Resource dimension information

Field	Type	Description
MetricName	String	Metric name.
DimensionInfos	Array of objects	Dimension information. For details, see **Table 1-8**.

Table 1-8 Dimension information

Field	Type	Description
Name	String	Dimension name.
Value	String	Dimension value.

Event Alarm Notification Fields

The following is an example of an alarm notification sent based on a custom event notification template:

```
{
  "version": "v1",
  "data": {
    "PrivateIPV6": "2407:c080:11f0:1115:490e:36fe:ba94:a410",
    "AlarmNotificationType": "Event",
    "AccountName": "RDS_test",
    "Namespace": "Elastic Cloud Server",
    "ResourceName": "ecs-abc-test",
    "ResourceTags": "_sys_type_hcss_x,test=test",
    "MetricName": "VM Restart",
    "IsAlarm": true,
    "IsCycleTrigger": false,
    "AlarmLevel": "Major",
    "Region": "CN North-Beijing4",
    "RegionId": "cn-north-4",
    "ResourceID": "7eb14e5d-8a79-4c94-8f8e-8f5467142490",
    "PrivateIP": "172.20.1.188",
    "PublicIP": "100.85.113.106",
    "EPName": "default",
    "AlarmRecordID": "ah260110T172316SmCFRcx7X",
    "AlarmRuleName": "alarm-VM Restart-abc-adafhads",
    "Filter": "Avg.",
    "ComparisonOperator": ">=",
    "AlarmDesc": "desc-test",
    "IsOriginalValue": false,
    "Count": 1,
    "AlarmTime": "2025/11/17 17:28:37 GMT+08:00",
    "ShowImpactAndSolution": true,
    "ImpactScope": "The VM is restarted.",
    "RecommendedSolution": "Check whether services are recovered."
    "DataPointTime": [
      "2025/11/17 17:28:35 GMT+08:00"
    ],
    "MonitoringRange": "Specified resources"
  }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 1-9 Event alarm notification fields

Field	Type	Description
PrivateIPV6	String	Private IPv6 address. Currently, only ECSs support this field.
AlarmNotificationType	String	Alarm notification type. The value can be **Metric** or **Event**.
AccountName	String	Account name.
Namespace	String	Cloud service name.
ResourceName	String	Resource name.
ResourceTags	String	Resource tags.
MetricName	String	Event name.
IsAlarm	Boolean	Alarm triggering condition, indicating whether an alarm is generated. • **true**: An alarm is generated. • **false**: No alarm is generated.
IsCycleTrigger	Boolean	Whether to continuously trigger alarms.
AlarmLevel	String	Alarm severity, which can be critical, major, minor, or warning.
Region	String	Region name, for example, **CN North-Beijing4**.
RegionId	String	Region ID, for example, **cn-north-4**.
ResourceID	String	Resource ID, that is, the dimension value. If there are multiple levels of dimensions, the names and values of all dimensions are displayed.
PrivateIP	String	Private IP address.
PublicIP	String	Public IP address.
EPName	String	Name of the enterprise project to which the resource belongs.
AlarmRecordID	String	Alarm record ID.
AlarmRuleName	String	Alarm rule name.
Filter	String	This field has no actual meaning for event alarms.
ComparisonOperator	String	This field has no actual meaning for event alarms. The default value is **>=**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Field	Type	Description
AlarmDesc	String	Description of the alarm rule.
IsOriginalValue	Boolean	Whether the metric configured in the alarm policy uses the raw data. • **true**: The metric data is the raw data. • **false**: The metric data is the aggregated data.
Count	Integer	Number of consecutive alarm triggers.
AlarmTime	String	Time when the alarm is generated.
ShowImpactAndSolution	Boolean	Whether the event impact and solution have values. • **true**: The event impact and solution have values. • **false**: The event impact and solution are empty.
ImpactScope	String	Event impact. Currently, only some interconnected cloud services support this field.
RecommendedSolution	String	Solution. Currently, only some interconnected cloud services support this field.
DataPointTime	Array of strings	Time when the event occurred. If the trigger type of the alarm policy in the event alarm rule is cumulative, the time of each event occurrence is displayed.
MonitoringRange	String	Monitoring scope. The value can be **Specific resources**, **All resources**, or **Resource groups**.

1.2 Receiving Alarm Notifications Through WeCom

After you select WeCom as the notification protocol and enter the webhook URL of a WeCom chatbot, if the resource metrics meet the alarm conditions, you can receive alarm notifications in a WeCom group.

Prerequisites

You have created a contact and enabled the WeCom notification protocol whitelist. For details, see **Applying for SMN New Protocol OBT**.

Creating a WeCom Chatbot

This section uses the WeCom mobile app as an example to describe how to create a WeCom chatbot.

1. Open the WeCom group that will receive alarm notifications on the WeCom mobile app.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. Touch in the upper right corner.
3. Touch next to **Group Robots**.
4. Click **Add Robot**.
5. Click **New**.
6. Enter a chatbot name, for example, **Cloud Eye Alarms**.
7. Click **Add**.
8. Click **Copy** to copy the webhook URL.

Adding a WeCom Chatbot as a Contact

Add the webhook URL of the WeCom chatbot as a contact.

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. On the **Recipients** tab page, click **Create** or click **Modify** in the row containing an existing contact.
4. Select **WeCom** for **Protocol**.
5. Enter the webhook URL of the WeCom chatbot in the text box, confirm the information, and click **Create**.

Creating an Alarm Contact Group and Adding Alarm Contacts

Create an alarm contact group and add contacts to the group.

For details, see **Creating a Contact/Contact Group**.

Creating an Alarm Rule

Create an alarm rule. You can configure a notification policy or directly select a contact group or contact to receive notifications.

For details about how to create an alarm rule, see **Creating an Alarm Rule**. For details about how to create a notification policy, see **Creating, Modifying, or Deleting a Notification Policy**.

Viewing Alarm Notifications

When a metric triggers the alarm rule, the WeCom group will receive an alarm notification.

1.3 Receiving Alarm Notifications in a DingTalk Group

After you select DingTalk as the notification protocol and enter the webhook URL of a DingTalk chatbot, if the resource metrics meet the alarm conditions, you can receive alarm notifications in a DingTalk group.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

You have created a contact and enabled the DingTalk notification protocol whitelist. For details, see **Applying for SMN New Protocol OBT**.

Creating a DingTalk Chatbot

For details about how to create a DingTalk chatbot, see **Creating a DingTalk Chatbot**. Pay attention to DingTalk's **Notice on Transition from Free Use to Commercial Use**.

Adding a DingTalk Chatbot as a Contact

Add the webhook URL of a DingTalk chatbot as a contact.

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. On the **Recipients** tab page, click **Create** or click **Modify** in the row containing an existing contact.
4. Select **DingTalk** for **Protocol**.
5. Enter the webhook URL of the DingTalk chatbot in the text box, confirm the information, and click **Create**.

Creating an Alarm Contact Group and Adding Alarm Contacts

Create an alarm contact group and add contacts to the group.

For details, see **Creating a Contact/Contact Group**.

Creating an Alarm Rule

Create an alarm rule. You can configure a notification policy or directly select a contact group or contact to receive notifications.

For details about how to create an alarm rule, see **Creating an Alarm Rule**. For details about how to create a notification policy, see **Creating, Modifying, or Deleting a Notification Policy**.

Viewing Alarm Notifications

When a metric triggers the alarm rule, the DingTalk group will receive an alarm notification.

1.4 Receiving Alarm Notifications in a Lark Group

After you select Lark as the notification protocol and enter a webhook URL, key, or custom keyword, if the resource metrics meet the alarm conditions, you can receive alarm notifications through a Lark group.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

You have created a contact and enabled the Lark notification protocol whitelist. For details, see **Applying for SMN New Protocol OBT**.

Creating a Lark Chatbot

This section uses the Lark PC client as an example to describe how to create a Lark chatbot.

1. Open the Lark group that will receive alarm notifications on the Lark PC client.
2. Click ··· in the upper right corner.
3. On the **Settings** page, click **Bot**.
4. Click **Add Bot** and select **Custom Bot**.
5. Enter a chatbot name, for example, **Cloud Eye Notification**, and click **Add**.
6. Click **Copy** to copy the webhook URL.
7. Click **Set Keywords** to add a custom keyword, confirm the information, and click **Finish**.

Adding a Lark Chatbot as a Contact

Add the webhook URL of a Lark chatbot as a contact.

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. On the **Recipients** tab page, click **Create** or click **Modify** in the row containing an existing contact.
4. Select **Lark** for **Protocol**.
5. Enter the webhook URL of the Lark robot in the text box.
6. Enter the key or custom keyword in the text box, confirm the information, and save the configuration.

Creating an Alarm Contact Group and Adding Alarm Contacts

Create an alarm contact group and add contacts to the group.

For details, see **Creating a Contact/Contact Group**.

Creating an Alarm Rule

Create an alarm rule. You can configure a notification policy or directly select a contact group or contact to receive notifications.

For details about how to create an alarm rule, see **Creating an Alarm Rule**. For details about how to create a notification policy, see **Creating, Modifying, or Deleting a Notification Policy**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Viewing Alarm Notifications

When a metric triggers the alarm rule, the Lark group will receive an alarm notification.

1.5 Receiving Alarm Notifications Using Functions

If existing notification channels (email, SMS, voice notification, Lark, DingTalk, and WeCom) of Cloud Eye cannot meet your requirements, you can use FunctionGraph to compile code for more customized requirements.

Prerequisites

You have enabled FunctionGraph. For details, see **Process of Using FunctionGraph**.

Scenarios

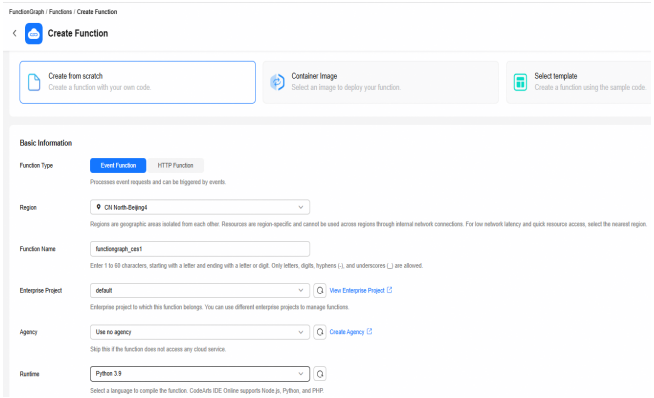
- Use FunctionGraph to process the format of alarm notifications so that tools other than Cloud Eye notification channels can receive alarm notifications.
- Use FunctionGraph to customize the alarm notification content of Cloud Eye.

Creating a Function with FunctionGraph

1. Log in to the **FunctionGraph console**.
2. In the navigation pane, choose **Functions** > **Function List**.
3. In the upper right corner, click **Create Function**.
4. On the displayed page, set **Create With** to **Create from scratch** and **Function Type** to **Event Function**, and enter a function name. Select **Python 3.9** for **Runtime**, and retain the default values for other parameters.

   For details about the parameters for creating a function, see **Creating an Event Function**.

   Figure 1-3 Creating a function

5. After the configuration is complete, click **Create Function**.

   The function details page is displayed, and a new function is added.

6. On the function details page, insert the required custom fields and other parameters in the code source. The following is an example:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- The notification type of the alarm notification template is metric.
- The alarm receiving mode is URL, and the URL is **http://10.181.139.219:5000/callback**.
- Notification content fields include **AlarmRecordID**, **AlarmTime**, and **AlarmLevel**. Fields in alarm notifications received through functions are defined by system templates. For details about the supported field structures, see **Notification Content Supported by Metric Alarms** and **Notification Content Supported by Event Alarms**. You can adjust the fields as required.

```
# -*- coding:utf-8 -*-
import json
import requests
def handler(event, context):
    record = event["record"][0]
    smn = record['smn']
    message_str = smn['message']
    message = json.loads(message_str)
    template_variable = message['template_variable']
    AlarmRecordID = message['AlarmRecordID']
    AlarmTime = template_variable['AlarmTime']
    AlarmLevel = template_variable['AlarmLevel']
    Source = 'Huawei'
    NewEvent = {
        "AlarmRecordID": AlarmRecordID,
        "AlarmTime": AlarmTime,
        "AlarmLevel": AlarmLevel,
        "Source": Source
    }
    print(NewEvent)
    URL = 'http://10.181.139.219:5000/callback'
    r = requests.post(URL, json=NewEvent)
    return {
        "statusCode": 200,
        "isBase64Encoded": False,
        "body": json.dumps(NewEvent),
        "headers": {
            "Content-Type": "application/json"
        }
    }
```

7. Click **Deploy** to complete the deployment.

Creating a Contact

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. Click the **Contacts** tab, click **Create**, and set parameters as prompted.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 1-4 Creating a contact

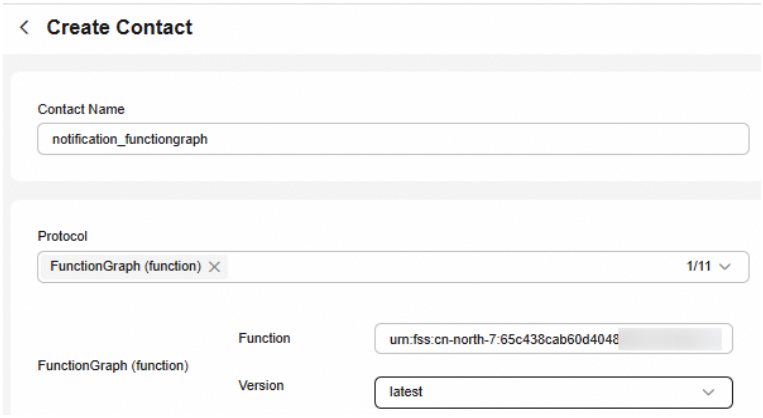


Table 1-10 Creating a contact

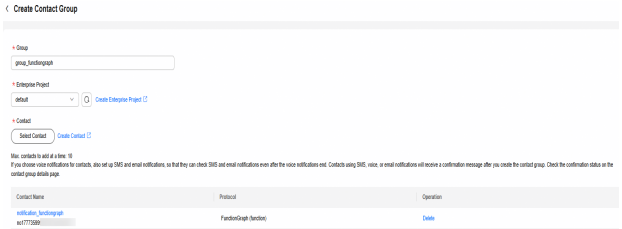
Parameter	Example Value	Description
Contact Name	notification_functiongraph	Contact name. Enter 1 to 42 characters.
Protocol	FunctionGraph (function)	Channel through which the contact receives alarm notifications. If you select **FunctionGraph (function)**, select the corresponding function and version. • **Function**: Click the function text box. In the displayed dialog box, select the function configured in **Creating a Function with FunctionGraph**. • **Version**: After you select a function, the function endpoint address and version numbers are displayed on the page. Manually select a version.

4. Click **Create**.
   A contact named **notification_functiongraph** is added to the contact list.

Creating a Contact Group

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. Click the **Contact Groups** tab, click **Create**, and set parameters as prompted.

Figure 1-5 Creating a contact group



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 1-11

Parameter	Example Value	Definition
Group	group_functiongraph	Contact group name. Use only letters, digits, underscores (_), and hyphens (-). Enter up to 64 characters.
Enterprise Project	default	Enterprise project to which the contact group belongs. Only users with the enterprise project permissions can view and manage the contact group. For details about how to create an enterprise project, see **Creating an Enterprise Project**.
Contact	notification_functiongraph	Select the contacts you have added. A maximum of 10 contacts can be added at a time. Click **Select Contact**. On the displayed page, select the created contact and click  to add it to the selected list. Then, click **OK**.

4. Click **Create**.

   A contact group named **group_functiongraph** is added to the contact group list.

You can also add the contact to a created contact group. For details, see **Adding Contacts to a Contact Group**. If you want to receive alarm notifications through an alarm policy, you can select the contact group as the recipient when configuring the alarm policy. For details, see **Creating a Notification Policy**.

Creating an Alarm Rule

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click **Create Alarm Rule**.
4. On the displayed page, configure the basic information, alarm content, alarm policy, and alarm notification for the alarm rule. Set **Notified By** to **Contact groups** and select **group_functiongraph** created in **Creating a Contact Group**.

   For details about alarm rule parameters, see **Creating an Alarm Rule and Notifications**.
5. Click **Create**.

Viewing Alarm Notifications

When a monitored metric triggers the alarm rule, the target function is called to send an alarm notification to the notification recipient.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

You can also view the call logs of the target function on the FunctionGraph console and check whether the logs meet your expectations. For details, see **Configuring and Viewing Function Invocation Logs**.

Notification Content Supported by Metric Alarms

The following uses the CPU usage of an ECS as an example to describe the field structure supported by metric alarms.

NOTE

If you have any questions about the fields in the alarm notification content, **create a service ticket** to contact technical support.


```
{
   "message_type": "alarm",
   "alarm_id": "al260512T094501SwVt7****",
   "alarm_name": "alarm-****",
   "alarm_status": "alarm",
   "time": 1778550457194,
   "namespace": "SYS.ECS",
   "metric_name": "cpu_util",
   "dimension": "instance_id:6b42c3f4-666d-409c-afe7-c16268d7****",
   "period": 1,
   "filter": "Raw data",
   "comparison_operator": "\u003e=",
   "value": 10,
   "unit": "%",
   "count": 1,
   "alarmValue": [{
      "time": 1778550457000,
      "value": 0.037267080745341616
   }],
   "sms_content": "[CN North-Beijing4 (cn-north-4)][Enterprise Project: default][Major alarm] ***, the raw data of the CPU usage of ECS as-config-**** (private IP address: 192.168.X.X; resource ID: 6b42c3f4-666d-409c-afe7-c16268d7****) is greater than or equal to 10% for one consecutive time.\nDimension Details: CPU usage: ECS: 6b42c3f4-666d-409c-afe7-c16268d70da1\nCurrent Data: 0.04% \nAn alarm was triggered on May 12, 2026 09:47:37 (GMT+08:00). Alarm Record ID: ah260512T094737SSSej****. Alarm Rule Name: alarm-****. Alarm Type: Metric. For details, visit the Cloud Eye console.\n",
   "default_content": "[CN North-Beijing4 (cn-north-4)][Enterprise Project: default][Major alarm] ***, the raw data of the CPU usage of ECS as-config-**** (private IP address: 192.168.X.X; resource ID: 6b42c3f4-666d-409c-afe7-c16268d7****) is greater than or equal to 10% for one consecutive time.\nDimension Details: CPU usage: ECS: 6b42c3f4-666d-409c-afe7-c16268d7****\nCurrent Data: 10.04% \nAn alarm was triggered on May 12, 2026 09:47:37 (GMT+08:00). Alarm Record ID: ah260512T094737SSSe****. Alarm Rule Name: alarm-****. Alarm Type: Metric. For details, visit the Cloud Eye console.\n",
   "template_variable": {
      "AlarmNotificationType": "Metric",
      "AccountName": "***",
      "Namespace": "Elastic Cloud Server",
      "DimensionName": "ECSs,"
      "ResourceName": "as-config-****",
      "ResourceTags": "11=22",
      "MetricName": "CPU Usage",
      "IsAlarm": true,
      "IsCycleTrigger": false,
      "AlarmLevel": "Major",
      "Region": "CN North-Beijing4",
      "RegionId": "cn-north-4",
      "ResourceId": "6b42c3f4-666d-409c-afe7-c16268d7****",
      "PrivateIp": "192.168.X.X",
      "CurrentData": "10.04 %",
      "AlarmTime": "2026/05/12 09:47:37 GMT+08:00",
      "DataPoint": {
         "2026/05/12 09:47:37 GMT+08:00": "10.04 %"
      },
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
      "DataPointTime": ["2026/05/12 09:47:37 GMT+08:00"],
      "AlarmDurationTime": "0",
      "AlarmRecordID": "ah260512T094737SSSej****",
      "AlarmRuleName": "alarm-****",
      "AlarmId": "al260512T094501SwVt7****",
      "MonitoringRange": "All resources",
      "IsOriginalValue": true,
      "Filter": "Raw data",
      "ComparisonOperator": "\u003e=",
      "Value": "10 %",
      "Unit": "%",
      "Count": 1,
      "Link": "https://console.huaweicloud.com/ces/?region=cn-north-4#/alarm/histories?
alarmRecordId=ah260512T094737SSSej****",
      "EpName": "default",
      "IsIEC": false,
      "IsAgentEvent": false,
      "ShowImpactAndSolution": false,
      "ResourceDimensionInfos": [{
         "MetricName": "CPU Usage",
         "DimensionInfos": [{
            "Name": "ECS,"
            "Value": "6b42c3f4-666d-409c-afe7-c16268d7****"
         }]
      }]
   },
   "AlarmRecordID": "ah260512T094737SSSej****"
}
```


Notification Content Supported by Event Alarms

The following uses restarting an ECS as an example to describe the field structure supported by event alarms:

NOTE

If you have any questions about the fields in the alarm notification content, **create a service ticket** to contact technical support.


```
{
   "message_type": "alarm",
   "alarm_id": "al260514T104252SVeqi****",
   "alarm_name": "alarm-8***",
   "alarm_status": "alarm",
   "time": 1778726924655,
   "namespace": "SYS.ECS",
   "metric_name": "rebootServer",
   "dimension": "instance_id:095b058c-ae86-4544-b3b9-6dd4583a****",
   "period": 0,
   "filter": "average",
   "comparison_operator": "\\u003e=",
   "value": 1,
   "unit": "count",
   "count": 1,
   "alarmValue": [{
      "time": 1778726607943,
      "value": 1
   }],
   "sms_content": "[CN North-Beijing4 (cn-north-4)][Enterprise Project: default][Major alarm] ***, an alarm
was triggered on May 14, 2026 10:48:44 (GMT+08:00) for the VM restart of ECS ecs-*** (private IP address:
192.168.X.X; ID: 095b058c-ae86-4544-b3b9-6dd4583a****). Alarm Record ID: ah260514T104844Shz0J****;
Alarm Rule Name: alarm-8***; Alarm Type: Event; Impact: The VM is restarted. Solution: Check whether
services are recovered. For details, visit the Cloud Eye console."
   "default_content": "[CN North-Beijing4 (cn-north-4)][Enterprise Project: default][Major alarm] ***, an
alarm was triggered on May 14, 2026 10:48:44 (GMT+08:00) for the VM restart of ECS ecs-*** (private IP
address: 192.168.X.X; ID: 095b058c-ae86-4544-b3b9-6dd4583a****). Alarm Record ID:
ah260514T104844Shz0J****; Alarm Rule Name: alarm-8***; Alarm Type: Event; Impact: The VM is restarted.
Solution: Check whether services are recovered. For details, visit the Cloud Eye console."
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "template_variable": {
     "PrivateIPV6": "XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX",
     "AlarmNotificationType": "Event",
     "AccountName": "***",
     "Namespace": "Elastic Cloud Server",
     "ResourceName": "ecs-****",
     "ResourceTags": "CES_TAG_XXX",
     "MetricName": "VM Restart",
     "IsAlarm": true,
     "IsCycleTrigger": false,
     "AlarmLevel": "Major",
     "Region": "CN North-Beijing4",
     "RegionId": "cn-north-4",
     "ResourceId": "095b058c-ae86-4544-b3b9-6dd4583a****",
     "PrivateIp": "192.168.X.X",
     "CurrentData": "1.00 ",
     "AlarmTime": "2026/05/14 10:48:44 GMT+08:00",
     "DataPoint": {
        "2026/05/14 10:43:27 GMT+08:00": "1.00"
     },
     "DataPointTime": ["2026/05/14 10:43:27 GMT+08:00"],
     "AlarmRecordID": "ah260514T104844Shz0J****",
     "AlarmRuleName": "alarm-8***",
     "AlarmId": "al260514T104252SVeqi****",
     "MonitoringRange": "All resources",
     "IsOriginalValue": false,
     "Filter": "Avg.",
     "ComparisonOperator": "\\u003e=",
     "Count": 1,
     "Link": "https://console.huaweicloud.com/ces/?region=cn-north-4#/alarm/histories?
alarmRecordId=ah260514T104844Shz0J****",
     "EpName": "default",
     "IsIEC": false,
     "IsAgentEvent": false,
     "ShowImpactAndSolution": true,
     "ImpactScope": "The VM is restarted.",
     "RecommendedSolution": "Check whether services are recovered."
  },
  "AlarmRecordID": "ah260514T104844Shz0J****"
}
```


1.6 Applying for SMN New Protocol OBT

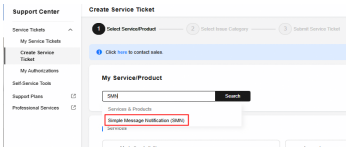
Currently, the voice notifications, DingTalk group messages, WeCom group messages, and Lark group messages are in the open beta test (OBT) phase. To use these protocols, you need to submit a service ticket to apply for the OBT. This section describes how to request them.

Scenarios

Configure notification protocols when creating contacts and alarm rules.

Procedure

1. Access the **Create Service Ticket** page.
2. Enter **SMN** in the **My Service/Product** text box and click **Simple Message Notification (SMN)**.

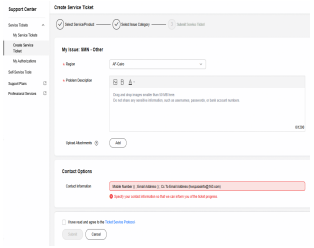


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

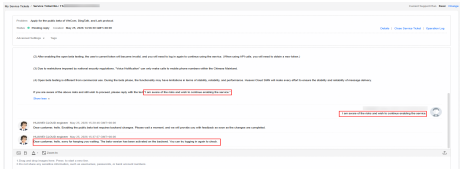
3. Select **Other** for **Issue Categories** and click **Create Now**.



4. Select the region where your cloud resources are located, enter **Apply for the OBT of the WeCom, DingTalk, and Lark protocols** in the issue description, enter your contact information (mobile number or email address), and click **Submit**.



5. Wait for the system to reply. When a message from a Huawei Cloud engineer is displayed asking you to confirm the risks, reply with **I am aware of the risks and wish to continue enabling the service.** Wait for the system to reply and enable the protocols for you.



NOTE

The number of WeCom, DingTalk, and Lark group messages that can be sent is limited, and the recipient system may be faulty. As a result, messages may fail to be sent. In this case, SMN does not ensure successful message delivery.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Alarm Configuration Method

2.1 Configuring Alarm Notifications by Severity

You can set up alarms using Cloud Eye's notification policies for tiered alerts. This feature will send alarm notifications by severity, channel, and time frame to different recipients.

Scenarios

When creating an alarm policy, you can notify contacts in contact groups or topic subscriptions of alarms by severity. This helps reduce repeated alarms and ensures important ones are not missed.

Prerequisites

You have added contacts for receiving alarms with different severities, channels, and time frames to different contact groups or topic subscriptions. For details about how to configure a contact group, see **Creating a Contact/Contact Group**. For details about how to configure a topic subscription, see **Creating a Topic**.

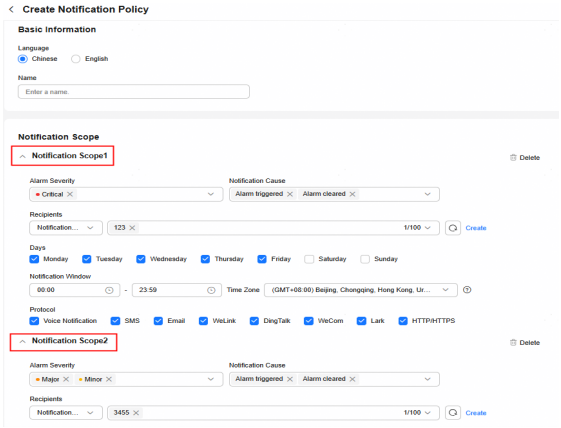
Creating a Notification Policy

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Notifications**.
3. On the **Notification Policies** tab, click **Create** and set the parameters as prompted. For details, see **Creating a Notification Policy**.

   Click **Add Scope** and configure multiple notification scopes in a notification policy. For each scope, specify the alarm severities, notification channels, time frames, and choose either specific contact groups or subscription topics to receive alarms. This setup allows sending notifications based on severity, channel, timing, and contacts.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-1 Creating a notification policy



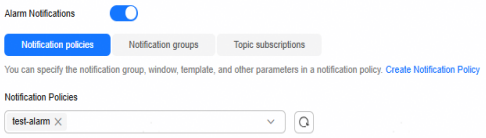
4. After the parameters are configured, click **OK**.

Creating an Alarm Rule

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click **Create Alarm Rule** and set the parameters as prompted. For details, see **Creating an Alarm Rule and Notifications**.

   After enabling **Alarm Notifications**, set **Notified By** to **Notification policies** and select the configured notification policy.

Figure 2-2 Configuring alarm notifications



In this way, you can send different alarms to different recipients based on different severities, channels, and time frames.

2.2 Masking Alarms by Multiple Metrics or Objects

You can configure masking rules to minimize invalid and non-urgent alarms for O&M personnel, improving alarm validity.

Scenarios

If you have configured alarm rules to monitor various metrics of both production and test resources on the cloud, you can set up masking rules for test resources to avoid receiving alarms for such resources.

Creating an Alarm Masking Rule

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Handling**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

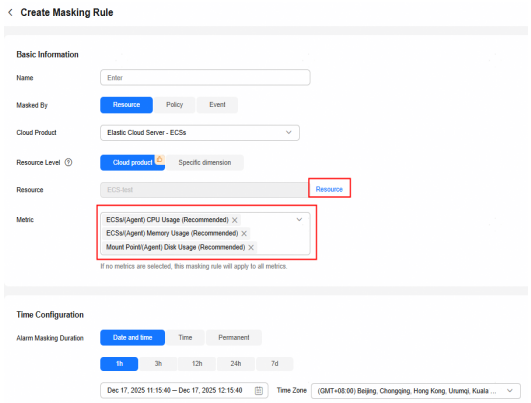
3. Click the **Alarm Masking** tab.

   NOTE

   In some regions, the path is **Alarm Management** > **Alarm Masking**.

4. In the upper right corner of the page, click **Create Masking Rule**.
5. On the **Create Masking Rule** page, set parameters as prompted. For details, see **Creating a Masking Rule**.
   a. Set **Masked By** to **Resource**.
   b. Set **Cloud Product** to the name of the target cloud service.
   c. Click **Resource**. On the displayed page, select one or more resources to be masked.
   d. In the drop-down list next to **Metric**, select one or more metrics to be masked. Leaving this blank applies the masking rule to all metrics.

Figure 2-3 Creating an alarm masking rule



6. Click **Create**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Cloud Resource Monitoring

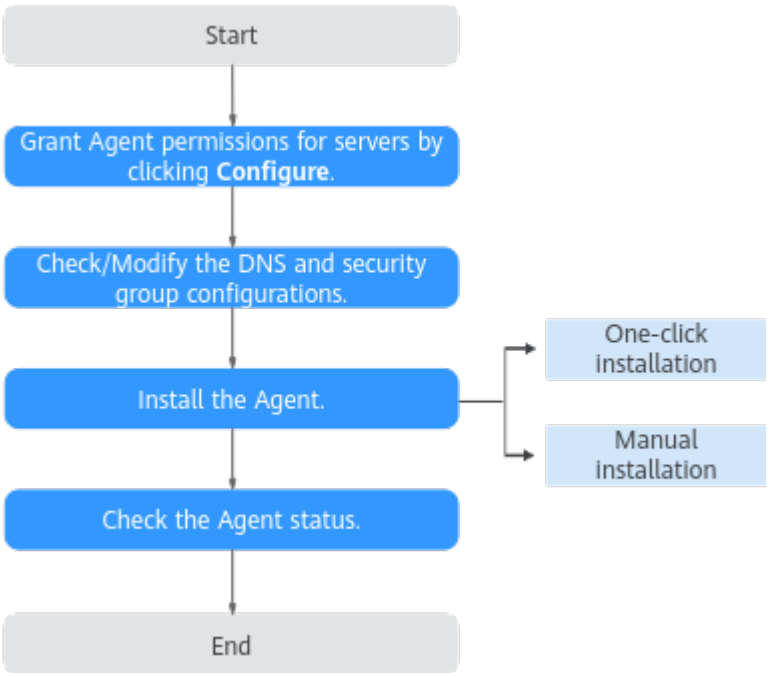
3.1 Installing the Agent on Servers

Servers are the most important cloud resources. It is crucial to monitor and set alarms for servers during actual O&M. After purchasing a server, you can configure an alarm rule to monitor its key service metrics.

Basic metrics and OS metrics are reported. Basic metrics are reported by ECS, and most of these metrics are collected at an interval of 5 minutes. OS metrics are reported by the Cloud Eye Agent installed on the OS. These metrics are more accurate, precise, and comprehensive, with a collection interval of 1 minute.

This section describes how to install the Agent on a server.

Figure 3-1 Agent installation process



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

You have purchased an ECS. After the ECS reports monitoring data to Cloud Eye, the ECS is displayed on the **Server Monitoring** page on the Cloud Eye console.

Granting Agent Permissions for Servers by Clicking Configure

The 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. Then, you can query the ECS or BMS metric data on the Cloud Eye console or by calling the Cloud Eye APIs.

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.

Checking/Modifying the DNS and Security Group Configurations

When installing the Cloud Eye Agent, you need to configure Huawei Cloud DNS to resolve the OBS domain name. The Agent also uses Huawei Cloud DNS to resolve the Cloud Eye backend domain name, allowing intranet access for reporting metrics and its status. Before installing the Agent, check your DNS and security group configurations to avoid exceptions when downloading the installation package or collecting monitoring data.

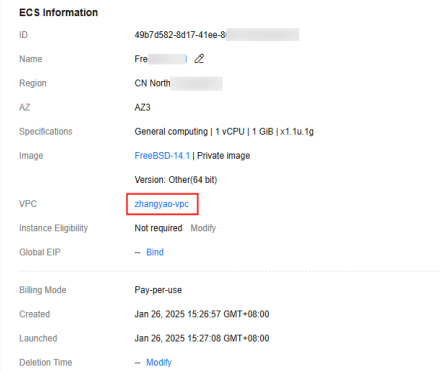
Viewing/Modifying the DNS Configuration

The following describes how to check the DNS configuration of an ECS in CN North-Beijing1. The operations for BMSs are similar.

1. Log in to the **ECS console**.
2. On the ECS console, click the name of an ECS to view its details.
3. In the ECS information area, click the VPC name.

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

   Figure 3-2 ECS information



4. Locate the target VPC and click the number of subnets.
5. In the subnet list, click the name of the target subnet.

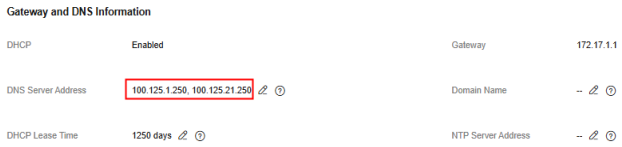
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6. In the **Gateway and DNS Information** area, check whether the DNS server address is the same as the private DNS server address provided by Huawei Cloud.

   For details about how to obtain the DNS server addresses of different regions, see **What Are Huawei Cloud Private DNS Server Addresses?**

   - If they are the same, as shown in **Figure 3-3**, you do not need to change the DNS server addresses.

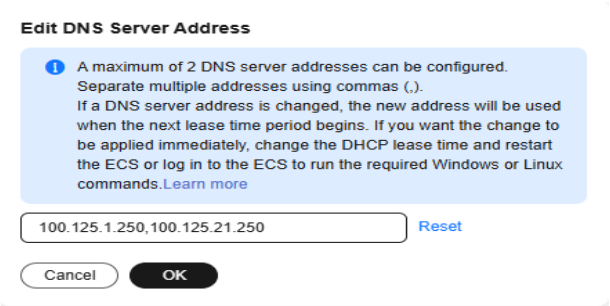
     Figure 3-3 Viewing the DNS server address

   - If they are different, perform steps **7** to **10** to change the DNS server address.

7. Click  next to **DNS Server Address**.
8. Enter the DNS server address. Use commas (,) to separate multiple IP addresses.

   Figure 3-4 Changing DNS server addresses

9. Click **OK**.
10. Restart the ECS or BMS. For details, see **Restarting an ECS** or **Restarting a BMS**.

Viewing and Adding Security Group Rules

1. Log in to the **ECS console**.
2. On the ECS console, click the name of an ECS to view its details.
3. On the ECS details page, click the **Security Groups** tab.
4. In the **Security Group Rules** area, click **Outbound Rules**.
5. Check whether the outbound rules contain the security group rules listed in **Table 3-1**.
   - If yes, no more security group rules need to be added.

     NOTE

     If **Protocol & Port** of an outbound rule is set to **All**, all traffic is allowed to pass through. You do not need to add new security group rules.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If not, go to the next step to add security group rules.

6. Click the security group name to go to its details page.
7. In the **Outbound Rules** tab, click **Add Rule**.
8. Add rules based on **Table 3-1**.

Table 3-1 Security group rules

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

Installing the Agent

The Agent can be automatically installed on mainstream OSs. You can click **Install & Upgrade the Agent** on the **Server Monitoring** page to install the Agent. You can also select **Detailed monitoring** to install the Agent when you buy an ECS. All OSs that support one-click installation support automatic Agent installation.

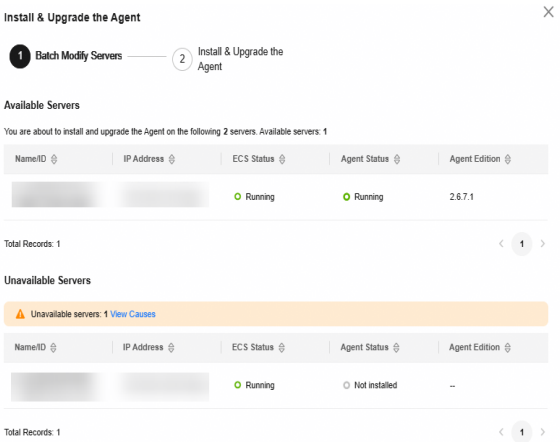
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If your OS does not support one-click installation or one-click installation fails, you can manually install the Agent.

Installing the Agent in One-Click Mode

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Select the target servers and choose **Install & Upgrade the Agent** > **Batch Install and Upgrade Agent**. The Agent installation and upgrade guide will be displayed on the right.

Figure 3-5 Batch installing and upgrading the Agent



4. On the displayed page, check the servers with ongoing tasks. If any inoperable servers are identified, rectify the fault by referring to **Why Can't I Install or Upgrade the Agent for Servers in Batches?**
5. Click **Next**. The page for installing and upgrading the Agent is displayed.
6. Select the Agent installation mode and edition.

Table 3-2 Installing and upgrading the Agent

Parameter	Example Value	Description
Select an installation and upgrade option.	Install the Agent	• **Install or upgrade the Agent to the latest version on all ECSs**: Install the Agent for all ECSs that support one-click installation but without the Agent installed, and upgrade the Agent for all ECSs with the Agent installed. • **Install the Agent**: Install the Agent on all ECSs that support one-click installation but without the Agent installed. • **Upgrade the Agent**: Upgrade the Agent for all ECSs with the Agent installed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Agent Edition	Latest Version	Select the Agent edition. Currently, only **Latest Version** is available.

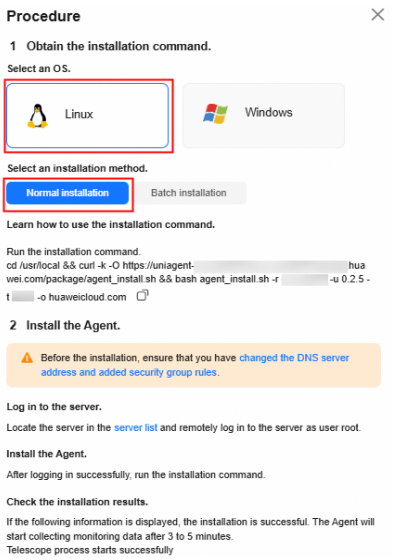
7. Click **OK**.
8. Check the Agent installation results.
   a. In the navigation pane, choose **Task Center**.
   b. Click the **Agent Maintenance** tab to view the task status.
      - If the status is **Succeeded**, the Agent is installed. On the **Server Monitoring** page, the Agent status is running and the Agent version is the latest.
      - If the status is **Timed out**, click **Retry** in the **Operation** column.

Installing the Agent on a Single Server

This section uses a Linux server as an example to describe how to manually install the Agent on a single server. For details about how to install the Agent on a Windows server, see **Windows**.

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Click **Install Manually** above the server list. The installation guide is displayed on the right.

Figure 3-6 Agent installation guide



4. Obtain the installation command.
   a. Select **Linux**.
   b. Select **Normal installation**.

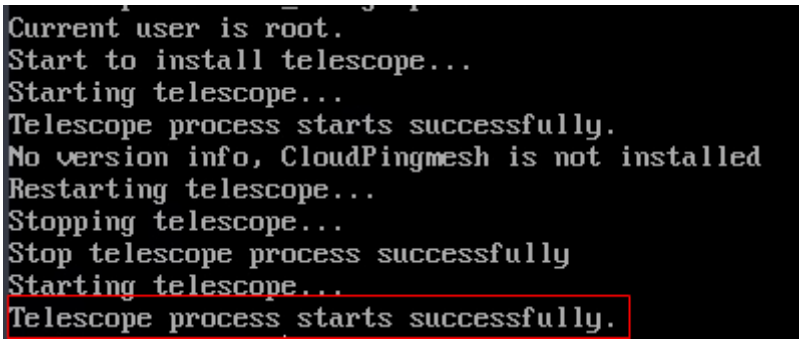
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

c. Click next to the installation command to copy the command.

5. Log in to the server as user **root**. For details, see **Logging In to a Linux ECS**.
6. Run the installation command obtained in **4**.

   Check whether **Telescope process starts successfully.** is displayed. If yes, the installation is successful. Wait for 3 to 5 minutes until the Agent starts collecting monitoring data.

Figure 3-7 Successful installation



Checking the Agent Status

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Check the Agent status of the target server.
   - If the Agent status is **Running**, the Agent has been installed and started.
   - If the Agent status is not running, see **What Are Agent Statuses and Troubleshooting Methods? (New Version)** for troubleshooting.

Helpful Links

- For more information about how to install the Agent, see **Installing the Agent**.
- After the Agent is installed, you can create alarm rules for metrics. If resource metric data reaches the specified threshold, Cloud Eye will notify you of the exception in real time through SMN to avoid service loss. For details, see **Creating an Alarm Rule to Monitor a Server**.

3.2 Creating Alarm Rules By Associating Resource Groups with Alarm Templates

If you have purchased a large number of cloud service resources under your account, you can create resource groups to manage these resources in batches. When you need to configure alarms for these resources in batches, you can create alarm rules by associating resource groups with custom alarm templates.

Scenarios

You need to create alarm rules for multiple cloud services in batches.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

You have multiple resources in your account.

Constraints

For details about the cloud services supported by resource groups, see **Cloud Services Supported by Resource Groups**.

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, set the following parameters:
   a. Enter a resource group name, for example, **Key_Service_Resource_Management**.
   b. Set **Add Resources** to **Automatically**.
   c. Set **Match Resources By** to **Enterprise project**.
   d. Set **Resource Level** to **Cloud product** and select the cloud service to which the resources belong.
   e. Select an enterprise project that the resources belong to.

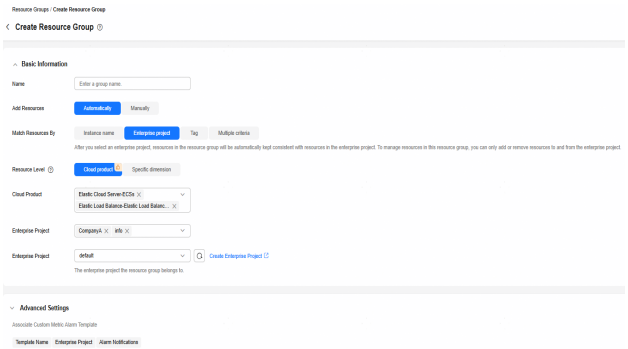
      NOTE

      - You can set **Add Resources** to **Automatically** or **Manually**. The **Automatically** option is recommended because resources in the group can update dynamically based on set rules.
      - You can set **Resource Level** to **Cloud product** or **Specific dimension**. The **Cloud product** option is recommended.

   f. Configure alarm notification parameters.
   g. Click **Create**.

      The created resource group appears in the resource group list.

Figure 3-8 Matching resources by enterprise project



Creating a Custom Alarm Template

1. Log in to the **Cloud Eye console**.

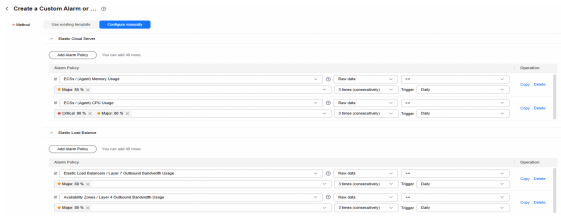
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click the **Alarm Templates** tab.

   NOTE

   In some regions, the path is **Alarm Management** > **Alarm Templates**.
4. Click **Create Custom Template** in the upper right corner.
5. On the displayed page, set the template parameters as follows:
   a. Enter a template name, for example, **Key_Service_Resource_Alarm_Template**.
   b. Set **Alarm Type** to **Metric**.
   c. Set **Method** to **Configure manually**.
   d. Click **Add Resource Type**, select the cloud service to which your resources belong, and configure alarm policies.

      Figure 3-9 Creating a custom alarm template

   e. Click **Create**.

      The created alarm template appears in the custom metric alarm template list.

Associating a Custom Alarm Template with a Resource Group

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click the **Alarm Templates** tab.

   NOTE

   In some regions, the path is **Alarm Management** > **Alarm Templates**.
4. Click the **Custom Metric Templates** tab.
5. Locate the row that contains the target alarm template and click **Associate with Resource Group** in the **Operation** column.
6. On the **Associate with Resource Group** page, select the created resource group and determine whether to inherit the notification type configured for the resource group.
   - If **Inherit Notification Settings from the Resource Group** is set to **Yes**, the alarm rules will inherit the notification type from the resource group. If the resource group has no notification type configured, the alarm rules will not have one either.
   - If it is set to **No**, all associated alarm rules will not inherit the notification type from the resource group. **Alarm Notifications** in new alarm rules will be disabled, and the associated alarm rules will use existing alarm notification settings.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7. Click **OK**.

   NOTE

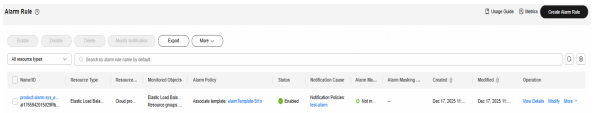
   This operation requires asynchronous creation, modification, and deletion of alarm rules, which takes 5 to 10 minutes. If there are multiple association tasks, this process takes longer.

8. In the **Modified** dialog box, view the names of updated alarm rules and click **OK**.
9. After the association is successful, you can view the alarm rules created for different cloud services on the alarm rule list page.

   NOTE

   For alarm rules created by associating a custom alarm template with a resource group, you cannot directly modify the policies in the alarm rules. Instead, you need to modify the policies in the custom alarm template.

Figure 3-10 Alarm rules



3.3 Configuring Alarm Rules for Resources by Matching Tags

If you have configured alarm rules for all resources of a cloud product but later need to adjust thresholds for specific resources, creating new rules can take too much effort. You can group resources of specific tags and link these groups to alarm templates to generate rules automatically. To update thresholds of resources, simply change their tags.

Prerequisites

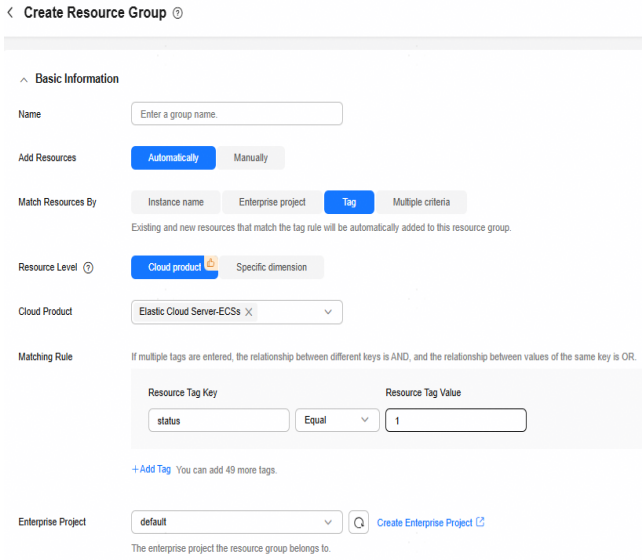
- You have configured a tag for all resources of a cloud product.
- You have configured another tag for the resources whose thresholds need to be adjusted.

Creating a Resource Group for All Resources

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Resource Groups**.
3. On the **Resource Groups** page, click **Create Resource Group**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-11 Creating a resource group for all resources



4. Set parameters according to **Table 3-3**.

Table 3-3 Creating a resource group for all resources

Parameter	Example Value	Description
Name	ECS-All-Resources	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Tag	How resources are added to a resource group.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Cloud Product	Elastic Cloud Server-ECSs	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instances belong 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.
Matching Rule	status Equal 1	Tag matching rule. You can add up to 50 tags. Tags are key-value pairs that you can use to easily categorize and search for cloud resources. • **Tag key**: A tag key cannot start or end with a space, or start with **_sys_**. It can contain up to 128 characters and contain letters, digits, spaces, and these special characters: _.:=+-@ • **Tag value**: A tag value consists of the matching method and value. The matching method can be **Equal**, **All**, **Include**, **Prefix**, **Suffix**, or **Not include**. A tag value can contain up to 255 characters and contain letters, digits, spaces, and these 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.
Enterprise Project	default	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Configure alarm notification parameters.
6. Click **Create**.

Creating a Resource Group for Resources Whose Thresholds Need to Be Adjusted

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Resource Groups**.
3. On the **Resource Groups** page, click **Create Resource Group**.
4. Set parameters according to **Table 3-4**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-4 Creating a resource group by matching resources by tag

Parameter	Example Value	Description
Name	**ECS-Threshold-Adjustment**	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Tag	How resources are added to a resource group.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.
Cloud Product	Elastic Cloud Server-ECSs	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instances belong 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Matching Rule	status Equal 0	Tag matching rule. You can add up to 50 tags. Tags are key-value pairs that you can use to easily categorize and search for cloud resources. • **Tag key**: A tag key cannot start or end with a space, or start with _**sys**_. It can contain up to 128 characters and contain letters, digits, spaces, and these special characters: _.:=+-@ • **Tag value**: A tag value consists of the matching method and value. The matching method can be **Equal**, **All**, **Include**, **Prefix**, **Suffix**, or **Not include**. A tag value can contain up to 255 characters and contain letters, digits, spaces, and these 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.
Enterprise Project	default	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Configure alarm notification parameters.
6. Click **Create**.

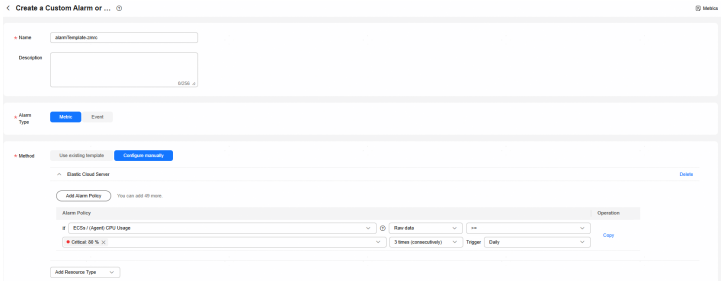
Creating a Custom Alarm Template

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click the **Alarm Templates** tab.

   NOTE

   In some regions, the path is **Alarm Management** > **Alarm Templates**.
4. Click **Create Custom Template** and set parameters according to **Table 3-5**.

Figure 3-12 Setting alarm template parameters



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-5 Setting alarm template parameters

Parameter	Example Value	Description
Name	ECS-General-Alarm	Custom template name. The system generates a random name, which you can modify.
Description	Alarm template applicable to all ECS resources	(Optional) Description of the custom alarm template.
Alarm Type	Metric	Alarm type to which the alarm template applies.
Method	Configure manually	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.
Add Resource Type	Elastic Cloud Server	Type of the resources the alarm template is created for. **NOTE** Up to 50 resource types can be added for each service.
Alarm Policy	If the raw data of CPU usage in three consecutive periods is 80% or more, Cloud Eye triggers a critical alarm once a day.	Policy for triggering an alarm. When you set **Alarm Type** to **Metric**, whether to trigger an alarm depends on whether the data in consecutive periods reaches the threshold. For details, see **Alarm Policies**. **NOTE** You can add up to 50 alarm policies to an alarm rule. If any of these alarm policies are met, an alarm will be triggered.
Operation	Copy	You can copy or delete an added alarm policy.

5. Click **Create**.
6. In the custom metric template list, locate the alarm template created in the preceding steps, and choose **More** > **Copy** in the **Operation** column.
7. On the **Copy Template** page, enter the template name and description.
   - **Template Name**: **ECS-Threshold-Adjustment**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **Description**: **Alarm template for adjusted ECS resource thresholds**

8. Click **OK**.
9. Locate the copied alarm template and click **Modify** in the **Operation** column.
10. On the **Modify Custom Metric Template** page, modify the thresholds in the alarm policy.
11. Click **Modify**.

Associating an Alarm Template with a Resource Group

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. Click the **Alarm Templates** tab.

   NOTE

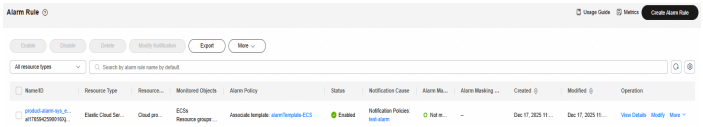
   In some regions, the path is **Alarm Management** > **Alarm Templates**.
4. Click the **Custom Metric Templates** tab.
5. Locate the template **ECS-General-Alarm** and click **Associate with Resource Group** in the **Operation** column.
6. Set **Resource Groups** to the resource group **ECS-All-Resources** and determine whether to inherit the notification type configured for the resource group.
   - If **Inherit Notification Settings from the Resource Group** is set to **Yes**, the alarm rules will inherit the notification type from the resource group. If the resource group has no notification type configured, the alarm rules will not have one either.
   - If it is set to **No**, all associated alarm rules will not inherit the notification type from the resource group. **Alarm Notifications** in new alarm rules will be disabled, and the associated alarm rules will use existing alarm notification settings.
7. 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.
8. In the **Modified** dialog box, view the names of updated alarm rules and click **OK**.
9. Repeat steps **5** to **8** to associate the alarm template **ECS-Threshold-Adjustment** with the resource group **ECS-Threshold-Adjustment**.

   After the association, you can view the created alarm rules in the alarm rule list.

Figure 3-13 Alarm rules



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Managing Resource Tags

After creating alarm rules, if you want to adjust the alarm threshold of a resource, you only need to modify its tag to match it to the alarm rule with the new threshold. For details about how to modify resource tags, see .

3.4 Recommended Metrics and Alarm Policies for Each Cloud Service

This section recommends metrics and alarm policies for configuring alarms for specific cloud services. Alarm policies change based on cloud services. This section is for reference only. Adjust your alarm settings as required.

Elastic Cloud Server

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.ECS	CPU Usage	cpu_util	Raw data	3	>	80	90	%	Hourly
	(Windows) Memory Usage	mem_util	Raw data	3	>	80	90	%	Hourly
	(Windows) Disk Usage	disk_util_inband	Raw data	3	>	80	90	%	Hourly
AGT.ECS	(Agent) CPU Usage	cpu_usage	Raw data	3	>	80	90	%	Hourly
	(Agent) Memory Usage	mem_usedPercent	Raw data	1	>	80	90	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(Agent) Receive Error Rate	net_errin	Raw data	5	>	0	-	%	Every 5 minutes
	(Agent) Transmit Error Rate	net_errout	Raw data	5	>	0	-	%	Every 5 minutes
	(Agent) Received Packet Drop Rate	net_dropin	Raw data	5	>	0	-	%	Every 5 minutes
	(Agent) Transmitted Packet Drop Rate	net_dropout	Raw data	5	>	0	-	%	Every 5 minutes
	(Agent) Blocked Processes	proc_blocked_count	Raw data	5	>	0	-	count	Hourly
	(Agent) NTP Offset	ntp_offset	Raw data	3	>=	5000	10000	ms	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(Agent) Disk I/O Usage	disk_ioUtils	Raw data	3	>	80	90	%	Hourly
	(Agent) Disk Usage	disk_usedPercent	Raw data	3	>	80	90	%	Hourly
	(Agent) Percentage of Total inode Used	disk_inodesUsedPercent	Raw data	3	>	80	90	%	Hourly
	(Agent) File System Read/Write Status	disk_fs_rwstate	Raw data	2	=	-	1	N/A	Hourly
	(Agent) NPU Device Health	npu_device_health	Raw data	1	=	2	3	N/A	Hourly
	(Agent) NPU Driver Health	npu_driver_health	Raw data	5	!=	-	0	N/A	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(Agent) NPU Memory Usage	npu_util_rate_mem	Raw data	5	>	98	-	%	Once
	(Agent) NPU AI Core Usage	npu_util_rate_ai_core	Raw data	10	>	98	-	%	Once
	(Agent) NPU Control CPU Usage	npu_util_rate_ctrl_cpu	Raw data	10	>	98	-	%	Once
	(Agent) Average NPU AI CPU Usage	npu_aicpu_avg_util_rate	Raw data	10	>	98	-	%	Once
	(Agent) HBM ECC Check Status	npu_hbm_ecc_enable	Raw data	5	=	0	-	N/A	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(Agent) Isolated Memory Pages with HBM Double-Bit Errors	npu_hbm_double_bit_isolated_pages_cnt	Raw data	5	>=	64	-	count	Once
	(Agent) NPU HBM Usage	npu_util_rate_hbm	Raw data	5	>	95	98	%	Once
	(Agent) NPU Optical Module Case Temperature	npu_opt_temperature	Raw data	5	> <	-	80 -10	°C	Once
	NPU Vector Core Usage	npu_util_rate_vector_core	Raw data	10	>	98	-	%	Once
	NPU Macro1 SerDes Lane0 SNR	npu_macro1_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro1 SerDes Lane1 SNR	npu_macro1_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro1 SerDes Lane2 SNR	npu_macro1_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro1 SerDes Lane3 SNR	npu_macro1_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane0 SNR	npu_macro2_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane1 SNR	npu_macro2_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro2 SerDes Lane2 SNR	npu_macro2_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane3 SNR	npu_macro2_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane0 SNR	npu_macro3_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane1 SNR	npu_macro3_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane2 SNR	npu_macro3_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro3 SerDes Lane 3 SNR	npu_macro3_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro4 SerDes Lane 0 SNR	npu_macro4_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro4 SerDes Lane 1 SNR	npu_macro4_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro4 SerDes Lane 2 SNR	npu_macro4_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro4 SerDes Lane 3 SNR	npu_macro4_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro5 SerDes Lane0 SNR	npu_macro5_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro5 SerDes Lane1 SNR	npu_macro5_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro5 SerDes Lane2 SNR	npu_macro5_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro5 SerDes Lane3 SNR	npu_macro5_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane0 SNR	npu_macro6_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro6 SerDes Lane1 SNR	npu_macro6_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane2 SNR	npu_macro6_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane3 SNR	npu_macro6_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane0 SNR	npu_macro7_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane1 SNR	npu_macro7_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro7 SerDes Lane2 SNR	npu_macro7_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane3 SNR	npu_macro7_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	Packets Retransmitted by NPU RoCE	npu_roce_new_pkt_rty_num	Raw data	5	Increase compared with last period	1	-	%	Once
	Abnormal PSN Packets Received by NPU RoCE	npu_roce_out_of_order_num	Raw data	5	Increase compared with last period	1	-	%	Once

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API Gateway (Dedicated)

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.APIC	5xx Responses	req_count_5xx	Raw data	1	Increase compared with last period	20	30	%	Hourly
	Average Latency	avg_latency	Raw data	3	>=	3000	5000	ms	Hourly
	Node System Load	node_system_load	Raw data	3	=	2	3	count	Hourly
	Node CPU Usage	node_cpu_usage	Raw data	3	>	30	60	%	Hourly
	Node Memory Usage	node_memory_usage	Raw data	3	>	30	60	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Throttled API Calls	throttled_calls	Raw data	1	Increase compared with last period	50	70	%	Hourly

NAT Gateway

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.NAT	Inbound PPS	inbound_pps	Raw data	3	>	-	800000	Count	Hourly
	Inbound PPS	inbound_pps	Raw data	3	Increase or decrease compared with last period	20	-	%	Hourly
	Outbound PPS	outbound_pps	Raw data	3	>	-	> 800000	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Outbound PPS	outbound_pps	Raw data	3	Increase or decrease compared with last period	20	-	%	Hourly
	SNAT Connection Usage Rate	snat_connection_ratio	Raw data	3	>	-	80	%	Hourly
	Packets Dropped (Excessive SNAT Connections)	packets_drop_count_snat_connection_beyond	Raw data	3	>	-	0	Count	Hourly
	Packets Dropped (Excessive PPS)	packets_drop_count_pps_beyond	Raw data	3	>	-	0	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Packets Dropped (When All EIP Ports Allocated)	packets_drop_count_eip_port_alloc_beyond	Raw data	3	>	-	0	Count	Hourly
	Total PPS Usage	total_pps_ratio	Raw data	3	>	-	80	%	Hourly

Web Application Firewall

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.WAF	CPU Usage	cpu_util	Raw data	3	>	80	90	%	Hourly
	Memory Usage	mem_util	Raw data	3	>	80	90	%	Hourly
	Disk Usage	disk_util	Raw data	3	>	80	-	%	Hourly
	Active Connections	active_connections	Raw data	3	>	40000	-	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	WAF Status Code (5XX)	waf_http_5xx	Raw data	1	Increase compared with last period	10	15	%	Hourly
	Status Code Returned by the Origin Server (5XX)	upstream_code_5xx	Raw data	3	>	15	20	Count	Hourly

Elastic Load Balance

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.ELB	Concurrent Connections	m1_cps	Raw data	3	>	40000	45000	Count	Hourly
	New Connections	m4_ncps	Raw data	3	>	4000	4500	Count/s	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Unhealthy Servers	m9_abnormal_servers	Raw data	3	>	-	0	Count	Hourly
	Dropped Connections	dropped_connections	Raw data	3	>	-	0	Count/s	Hourly
	Dropped Packets	dropped_packets	Raw data	3	>	-	0	Count/s	Hourly
	Bandwidth for Dropping Packets	dropped_traffic	Raw data	3	>	-	0	bit/s	Hourly
	Layer 4 New Connection Usage	l4_ncps_usage	Raw data	3	>	80	90	%	Hourly
	Layer 4 Concurrent Connection Usage	l4_con_usage	Raw data	3	>	80	90	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Layer 4 Inbound Bandwidth Usage	l4_in_bps_usage	Raw data	3	>	80	90	%	Hourly
	Layer 4 Outbound Bandwidth Usage	l4_out_bps_usage	Raw data	3	>	80	90	%	Hourly
	Layer 7 New Connection Usage	l7_ncps_usage	Raw data	3	>	80	90	%	Hourly
	Layer 7 Concurrent Connection Usage	l7_con_usage	Raw data	3	>	80	90	%	Hourly
	Layer 7 Inbound Bandwidth Usage	l7_in_bps_usage	Raw data	3	>	80	90	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Layer 7 Outbound Bandwidth Usage	l7_out_bps_usage	Raw data	3	>	80	90	%	Hourly
	Layer 7 QPS Usage	l7_qps_usage	Raw data	3	>	80	90	%	Hourly
	Concurrent Connections	m1_cps	Raw data	1	Decrease compared with previous period	-	80	%	Hourly
	New Connections	m4_ncps	Raw data	1	Decrease compared with previous period	-	80	%	Hourly
	5xx Status Codes (Total)	mf_l7_http_5xx	Raw data	1	Increase compared with last period	-	50	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Average Layer 7 Response Time	m14_l7_rt	Raw data	1	Increase compared with last period	-	50	%	Hourly
	5xx Status Codes (Load Balancer)	elb_http_5xx	Raw data	1	Increase compared with last period	-	50	%	Hourly
	5xx Status Codes Percentage	l7_5xx_ratio	Raw data	3	>=	-	5	%	Hourly
	2xx Status Codes Percentage	l7_2xx_ratio	Raw data	3	<=	-	95	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Scalable File Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.SFS	File System Read Bandwidth	read_bytes_intranet	Raw data	1	Decrease compared with previous period	100	-	%	Every 3 hours
	File System Write Bandwidth	write_bytes_intranet	Raw data	1	Decrease compared with previous period	100	-	%	Every 3 hours
	File System Read TPS	read_tps	Raw data	1	Decrease compared with previous period	100	-	%	Every 3 hours
	File System Write TPS	write_tps	Raw data	1	Decrease compared with previous period	100	-	%	Every 3 hours

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Scalable File Service Turbo

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.EFS	Capacity Usage	used_capacity_percent	Raw data	5	>	90	95	%	Hourly
	Inode Usage	used_inode_percent	Raw data	5	>	90	95	%	Hourly

Object Storage Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.OBS	Request Success Rate	request_success_rate	Raw data	2	<	-	99.97	%	Hourly

Distributed Cache Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DCS	Memory Usage	memory_usage	Raw data	2	>	70	80	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	CPU Usage	cpu_usage	Raw data	2	Decrease compared with previous period	-	100	%	Hourly
	Proxy Status	node_status	Raw data	2	=	-	1	N/A	Hourly
	Average CPU Usage	cpu_avg_usage	Raw data	2	>	70	80	%	Hourly
	Maximum Latency	command_max_rt	Raw data	2	>	-	900000	µs	Hourly
	Average Latency	command_avg_rt	Raw data	2	>	-	150000	µs	Hourly
	Connection Usage	connections_usage	Raw data	2	>	70	80	%	Hourly
	CPU Usage	cpu_usage	Raw data	2	>	70	80	%	Hourly
	Slow Query Logs	mc_is_slow_log_exist	Raw data	1	>	-	0	N/A	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Distributed Database Middleware

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DDMS	CPU Usage	ddm_cpu_util	Raw data	3	>	80	90	%	Hourly
	Memory Usage	ddm_mem_util	Raw data	3	>	85	90	%	Hourly
	Slow SQL Logs	ddm_slow_log	Raw data	3	>	50	100	Piece	Daily
	Connection Usage	ddm_connection_util	Raw data	2	>=	80	85	%	Hourly
	DDM Node Connectivity	ddm_node_status_alarm_code	Raw data	1	=	-	1	N/A	Hourly

Distributed Message Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DMS	Consumers	consumers	Raw data	2	>	3600	-	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	RabbitMQ Instance Available Messages	messages_ready	Raw data	1	>	10000	-	Count	Hourly
	Unacknowledged Messages	messages_unacknowledged	Raw data	1	>	10000	-	Count	Hourly
	Instance Disk Usage	instance_disk_usage	Raw data	3	>	80	90	%	Hourly
	Disk Capacity Usage	broker_disk_usage	Raw data	3	>	80	90	%	Hourly
	Memory Usage	broker_memory_usage	Raw data	3	>	80	90	%	Hourly
	Broker Alive	broker_alive	Raw data	1	=	-	0	N/A	Hourly
	Connections	broker_connections	Raw data	3	>	-	2000	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	CPU Usage	broker_cpu_usage	Raw data	3	Decrease compared with previous period	-	100	%	Hourly
	Average Disk Read Time	broker_disk_read_await	Raw data	3	>	-	5000	ms	Hourly
	Average Disk Write Time	broker_disk_write_await	Raw data	3	>	-	5000	ms	Hourly
	Message Creation Processing (99th Percentile)	broker_produce_p99	Raw data	3	>	50	-	ms	Hourly
	Message Creation Processing (99.9th Percentile)	broker_produce_p999	Raw data	3	>	50	-	ms	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Creation Success Rate	broker_produce_success_rate	Raw data	1	<	-	90	%	Hourly
	Messages in the Dead Letter Queue	dlq_accumulation	Raw data	3	>	0	-	Count	Hourly
	Dead Letter Message Increase	dlq_increase	Raw data	3	>	0	-	Count	Hourly
	Topic Available Messages	topic_messages_remained	Raw data	1	>	10000	-	Count	Hourly
	Consumer Available Messages	consumer_messages_remained	Raw data	1	>	10000	-	Count	Hourly
	Socket Connections	socket_used	Raw data	3	>	2500	-	Count	Hourly
	Node Alive	rabbitmq_alive	Raw data	1	=	-	0	N/A	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Disk Capacity Usage	rabbitmq_disk_usage	Raw data	3	>	80	85	%	Hourly
	CPU Usage	rabbitmq_cpu_usage	Raw data	3	-	> 80	> 90% Or Decreased by 100% compared with the last period	%	Hourly
	Memory Usage	rabbitmq_memory_usage	Raw data	3	>	-	30	%	Hourly
	Memory High Watermark	rabbitmq_memory_high_watermark	Raw data	1	>	-	0	N/A	Hourly
	Disk High Watermark	rabbitmq_disk_insufficient	Raw data	1	>	-	0	N/A	Hourly
	Connection Usage	connections_usage	Raw data	1	>	-	80	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Accumulated Messages	instance_accumulation	Raw data	1	>	10000	Increased by 50% compared with the last period	Count	Hourly
	Production Rate Limits	instance_produce_ratelimit_times	Raw data	1	>=	-	1	Count	Hourly
	Group Available Messages	group_accumulation	Raw data	1	>	10000	-	Count	Hourly
	Task Status	task_status	Raw data	1	=	0	-	N/A	Hourly
	Message Delay	message_delay	Raw data	3	>	1000	-	ms	Hourly
	Partitions	current_partitions	Raw data	3	>	90	-	Count	Hourly
	Accumulated Messages	group_msgs	Raw data	1	>	10000	-	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Queue Available Messages	queue_messages_ready	Raw data	1	>	10000	-	Count	Hourly
	Average Message Creation Processing Duration	broker_produce_mean	Raw data	3	>	-	50	ms	Hourly
	JVM Heap Memory Usage	broker_heap_usage	Raw data	3	>	80	90	%	Hourly
	Connections	broker_connections	Raw data	1	>	-	4000	Count	Hourly
	CPU Usage	broker_cpu_usage	Raw data	3	>	80	90	%	Hourly
	Network Bandwidth Usage	network_bandwidth_usage	Raw data	3	>	70	80	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Relational Database Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.RDS	CPU Usage	rds001_cpu_util	Raw data	3	>=	80	90	%	Hourly
	Memory Usage	rds002_mem_util	Raw data	3	>=	90	95	%	Hourly
	Disk Usage	rds039_disk_util	Raw data	3	>=	80	95	%	Hourly
	Connection Usage	rds072_conn_usage	Raw data	3	>=	80	90	%	Hourly
	Real-Time Replication Delay	rds073_replication_delay	Raw data	3	>=	300	600	s	Hourly
	Active Connection Usage	rds_conn_active_usage	Raw data	3	>=	80	95	%	Hourly
	Stream Replication Status of Standby Instance or Read Replica	slave_replication_status	Raw data	3	=	-	0	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	ReplicationLag	rds046_replication_lag	Raw data	3	>=	300000	600000	ms	Hourly
	Connection Usage	rds083_conn_usage	Raw data	3	>=	80	90	%	Hourly

Relational Database Service Cluster

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.RDS_MYSQL_CLUSTER	Active Connection Usage	rds_conn_active_usage	Raw data	3	>=	80	95	%	Hourly
	CPU Usage	rds001_cpu_util	Raw data	3	>=	80	90	%	Hourly
	Memory Usage	rds002_mem_util	Raw data	3	>=	90	95	%	Hourly
	Storage Space Usage	rds039_disk_util	Raw data	3	>=	80	95	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Connection Usage	rds072_conn_usage	Raw data	3	>=	80	90	%	Hourly
	Real-Time Replication Delay	rds073_replication_delay	Raw data	3	>=	300	600	s	Hourly

Content Delivery Network

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.CDN	Bandwidth	bw	Raw data	3	Increase or decrease compared with last period	10	20	%	Hourly
	Retrieval Failure Rate	bs_fail_rate	Raw data	3	>	3	10	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Status Codes 4xx	http_code_4xx	Raw data	3	Increase compared with last period	60	80	%	Hourly
	4xx Status Code Ratio	http_code_4xx_rate	Raw data	3	>=	10	30	%	Hourly
	Status Codes 5xx	http_code_5xx	Raw data	3	Increase compared with last period	60	80	%	Hourly
	5xx Status Code Ratio	http_code_5xx_rate	Raw data	3	>	1	5	%	Hourly
	Traffic Hit Ratio	hit_flux_rate	Raw data	3	<	80	50	%	Hourly
	5xx Origin Status Code Ratio	bs_http_code_5xx_rate	Raw data	3	>	1	5	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Live

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.LIVE	5xx Status Code Proportion	http_5xx_proportion	Raw data	1	>	0	1	%	Hourly

Data Warehouse Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DWS	CPU Usage	dws010_cpu_usage	Raw data	3	>	85	90	%	Daily
	Memory Usage	dws011_mem_usage	Raw data	3	>	90	95	%	Daily
	Disk Usage	dws015_disk_usage	Raw data	3	>	80	90	%	Daily
	Disk Read Throughput	dws018_disk_read_throughput	Raw data	5	>	-	30000000	Byte/s	6 hours

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Disk Write Throughput	dws019_disk_write_throughput	Raw data	5	>	-	30000000	Byte/s	6 hours

Data Replication Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DRS	CPU Usage	cpu_util	Raw data	3	>	80	90	%	Hourly
	Memory Usage	mem_util	Raw data	3	>	85	90	%	Hourly
	Storage Space Usage	disk_util	Raw data	3	>	80	90	%	Hourly
	Source Database WAL Extract Lag	extract_latency	Raw data	3	>	300000	600000	ms	Hourly
	Data Synchronization Latency	apply_latency	Raw data	3	>	300000	600000	ms	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Synchronization Status	apply_current_state	Raw data	3	=	-	10	N/A	Hourly
	Task Status	apply_job_status	Raw data	3	=	-	1	N/A	Hourly

Database Security Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DBSS	CPU Usage	cpu_util	Raw data	3	>	80	85	%	Hourly
	Memory Usage	mem_util	Raw data	3	>	80	85	%	Hourly
	Disk Usage	disk_util	Raw data	3	>	80	85	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Database Proxy

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DBPROXY	CPU Usage	rds001_cpu_util	Raw data	3	>	80	90	%	Hourly
	Memory Usage	rds002_mem_util	Raw data	3	>	90	95	%	Hourly
	Intranet Outbound Bandwidth Usage (%)	l4_out_bps_usage	Raw data	2	>	90	95	%	Hourly
	Intranet Inbound Bandwidth Usage (%)	l4_in_bps_usage	Raw data	2	>	90	95	%	Hourly
	Abnormal ELB Backend Proxy Nodes	m9_abnormal_servers	Raw data	1	>	-	0	Count	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Document Database Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DDS	Replication Lag	mongo026_repl_lag	Raw data	3	>=	300	600	s	Hourly
	CPU Usage	mongo031_cpu_usage	Raw data	3	>=	80	98	%	Hourly
	Memory Usage	mongo032_mem_usage	Raw data	3	>=	90	98	%	Hourly
	Storage Space Usage	mongo035_disk_usage	Raw data	3	>=	80	95	%	Hourly
	Disk Read Time	mongo039_avg_disk_sec_per_read	Raw data	3	>=	0.05	0.1	s	Hourly
	Disk Write Time	mongo040_avg_disk_sec_per_write	Raw data	3	>=	0.05	0.1	s	Hourly
	Percentage of Active Node Connections	mongo007_connections_usage	Raw data	3	>=	80	95	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	WiredTiger Cache Percentage	mongo054_wt_cache_used_percent	Raw data	3	>=	85	95	%	Hourly
	WiredTiger Dirty Data Cache Percentage	mongo055_wt_cache_dirty_percent	Raw data	3	>=	20	25	%	Hourly

Virtual Private Cloud

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.VPC	Outbound Bandwidth Usage	upstream_bandwidth_usage	Raw data	3	>	-	80	%	Hourly
	Inbound Bandwidth Usage	downstream_bandwidth_usage	Raw data	3	>	-	80	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Outbound Bandwidth Usage	upstream_bandwidth_usage	Raw data	3	Increase or decrease compared with last period	20	-	%	Hourly
	Inbound Bandwidth Usage	downstream_bandwidth_usage	Raw data	3	Increase or decrease compared with last period	20	-	%	Hourly

Cloud Firewall

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.CFW	Protection Bandwidth Usage Rate	protection_bandwidth_usage	Raw data	3	>	85	95	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Internet Boundary Protection Bandwidth Usage (%)	internet_protection_bandwidth_usage_rate	Raw data	3	>	85	95	%	Hourly
	Inter-VPC Protection Bandwidth Usage (%)	vpc_protection_bandwidth_usage_rate	Raw data	3	>	85	95	%	Hourly

Cloud Connect

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.CC	Network Bandwidth Usage	network_bandwidth_usage	Raw data	3	>	-	80	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

TaurusDB

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.GAUSSDB	CPU Usage	gaussdb_mysql001_cpu_util	Raw data	3	>	80	90	%	Hourly
	Memory Usage	gaussdb_mysql002_mem_util	Raw data	3	>	-	90	%	Hourly
	Connection Usage	gaussdb_mysql072_conn_usage	Raw data	3	>	80	90	%	Hourly
	Data Disk Usage	gaussdb_mysql113_data_disk_used_ratio	Raw data	3	>	80	90	%	Hourly

Cloud Search Service

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.ES	Max. Disk Usage	disk_util	Raw data	5	>=	85	90	%	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Cluster Health Status	status	Raw data	5	>=	1	2	N/A	Hourly
	Max. JVM Heap Usage	max_jvm_heap_usage	Raw data	1	>	80	85	%	Hourly
	Max. CPU Usage	max_cpu_usage	Raw data	2	>	80	85	%	Hourly
	Nodes	nodes_count	Raw data	3	Decrease compared with previous period	-	10	%	Hourly
	Tasks in Write Queue	sum_thread_pool_write_queue	Raw data	5	>=	500	1000	N/A	Hourly
	Tasks in Search Queue	sum_thread_pool_search_queue	Raw data	5	>=	500	800	N/A	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Rejected Tasks in Write Queue	sum_thread_pool_write_rejected	Raw data	5	>=	10	20	N/A	Hourly
	Rejected Tasks in Search Queue	sum_thread_pool_search_rejected	Raw data	5	>=	10	20	N/A	Hourly
	Max. Task Runtime	task_max_running_time	Raw data	1	>=	-	60000	ms	Hourly

Direct Connect

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
SYS.DCAAS	Port Status	network_status	Raw data	1	!=	-	1	N/A	Every 5 minutes
	Inbound Error Packets	in_errors	Raw data	1	>	-	0	Packet	Every 5 minutes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Latency	latency	Raw data	3	Increase compared with last period	-	20	%	Hourly
	Packet Loss Rate	packet_loss_rate	Raw data	3	>	5	10	%	Hourly
	IPv4 Peer Status	bgp_peer_status_v4	Raw data	1	!=	-	1	N/A	Hourly
	IPv6 Peer Status	bgp_peer_status_v6	Raw data	1	!=	-	1	N/A	Hourly

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Cloud Eye Resource Group Configuration

4.1 Resource Group Overview

A typical e-commerce project includes several connected subsystems. Each handles specific functions and collaborates to deliver the full service experience. If the customer's e-commerce project uses systems developed by various suppliers, each system owner must be responsible for receiving and handling resource alarms for their respective systems.

This practice describes how to use resource groups in Cloud Eye to send alarms to the correct O&M personnel, thereby avoiding alarm flooding and invalid notifications.

What Is a Resource Group?

Resource groups allow you to centrally manage services involved in your businesses. You can manage different types of resources, alarm rules, and alarm records by business, which quickly improves O&M efficiency.

Metric and Event Notification Solutions for Cloud Eye

Table 4-1 Metric and event notification solutions

Alarm Type	Configuration	Scenario	Remarks/Risk Point
Metric	Create a resource group and set **Add Resources** to **Automatically** and **Match Resources By** to **Tag**.	Tags have been added for resources and the tags are complete.	This solution depends on the accuracy of tags added for resources.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Type	Configuration	Scenario	Remarks/Risk Point
	Create a resource group and set **Add Resources** to **Automatically** and **Match Resources By** to **Enterprise project**.	No tag is added for the resources of the account.	This solution only allows you to select enterprise projects. It is suitable for accounts with only one environment.
	Create a resource group and set **Add Resources** to **Automatically** and **Match Resources By** to **Multiple criteria**.	Enterprise projects have been configured for resources, and no tag related to rights- and domain-based management has been added.	This solution allows you to match resources by enterprise project, tag, and instance name. It is suitable for accounts with a small number of tags. If a large number of tags are added for resources, the matching will be complex.
	Create a resource group and set **Add Resources** to **Automatically** and **Match Resources By** to **Instance name**.	The account's resources have no tags and are not bound to any enterprise project.	The solution relies on resource naming rules, making it hard to execute. Therefore, it is not recommended.
	Create a resource group and set **Add Resources** to **Manually** and **Resource Level** to **Cloud product**.	Cloud services that do not support automatic resource addition or resource matching by tag.	For details about these services, see **Cloud Services Supported by Resource Groups**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Alarm Type	Configuration	Scenario	Remarks/Risk Point
	Create a resource group and set **Add Resources** to **Manually** and **Resource Level** to **Specific dimension**.	Other scenarios where you need to manually create a resource group. For example, some resources require specific thresholds.	If you only want to monitor metrics of a specific dimension, set **Resource Level** to **Specific dimension**.
Event	Create an alarm rule of the event type. Set the monitoring scope to specified resources.	Event alarms require rights- and domain-based management.	When you select specified resources, you can filter resources by resource group. Each alarm rule applies to only one cloud service for which event-based alarms are generated. Therefore, you need to create an alarm rule for each group within that cloud service. If resources are added to a resource group, you need to manually add the resources to the event alarm rule.
	Create an event alarm rule and set the monitoring scope to all resources.	Event alarms do not require rights- and domain-based management.	-

4.2 Configuring Resource Groups for Metric Alarms

When creating a resource group, you are advised to set **Add Resources** to **Automatically**. Resource groups created with **Add Resources** set to **Automatically** can be updated dynamically. When you add resources that meet the required conditions, the system automatically adds the resources to the group. Supported cloud services vary with how resources are added. For details, see **Cloud Services Supported by Resource Groups**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Creating a Resource Group by Matching Resources by Tag

When you need to group services of different owners, you are advised to set **Add Resources** to **Tag**. This matching rule relies on the accuracy of resource tags. For example, the tag **env=pro,business=***xxx* indicates resources of the *xxx* service in the production environment.

1. Log in to the **Cloud Eye console**.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, choose **Resource Groups**.
5. In the upper right corner, click **Create Resource Group**.
6. On the **Create Resource Group** page, set parameters.

Figure 4-1 Matching resources by tag

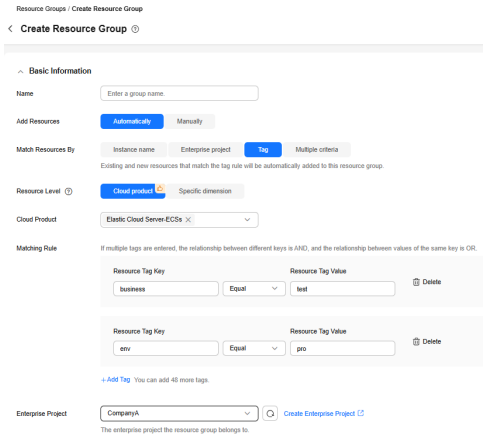


Table 4-2 Creating a resource group by matching resources by tag

Parameter	Example Value	Description
Name	Production_Business_xxx	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Tag	How resources are added to a resource group.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.
Cloud Product	Elastic Cloud Server-ECSs	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instances belong 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.
Matching Rule	Tag 1: env=pro, Tag 2: business=xxx	Tag matching rule. You can add up to 50 tags. Tags are key-value pairs that you can use to easily categorize and search for cloud resources. • **Tag key**: A tag key cannot start or end with a space, or start with **_sys_**. It can contain up to 128 characters and contain letters, digits, spaces, and these special characters: _.:=+-@ • **Tag value**: A tag value consists of the matching method and value. The matching method can be **Equal**, **All**, **Include**, **Prefix**, **Suffix**, or **Not include**. The value can contain up to 255 characters and contain letters, digits, spaces, and these 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.
Enterprise Project	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

7. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

8. Click **Create**.
9. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

Creating a Resource Group by Matching Resources by Enterprise Project

When you create a resource group with **Match Resources By** set to **Enterprise Project**, you can only select a specific enterprise project to match resources, which is not flexible. This method is applicable to accounts with only one environment.

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, set parameters.

Figure 4-2 Matching resources by enterprise project

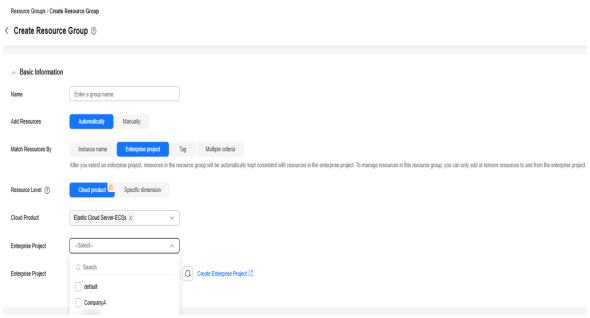


Table 4-3 Creating a resource group by matching resources by enterprise project

Parameter	Example Value	Description
Name	Enterprise_Project_B	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Enterprise project	How resources are added to a resource group.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.
Cloud Product	Elastic Cloud Server-ECSs	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instances belong 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.
Enterprise Project	Enterprise Project B	Enterprise project for matching resources. You can select multiple enterprise projects.
Enterprise Project	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.
6. Click **Create**.
7. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

Creating a Resource Group by Matching Resources by Multiple Criteria

When you create a resource group with **Match Resources By** set to **Multiple Criteria**, you can choose to match resources by enterprise project and tag. This method is similar to matching resources by tag. If a large number of tags are added for resources, the matching will be complex. This method is suitable for accounts with fewer tags.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4. On the **Create Resource Group** page, set parameters.

Figure 4-3 Matching resources by multiple criteria

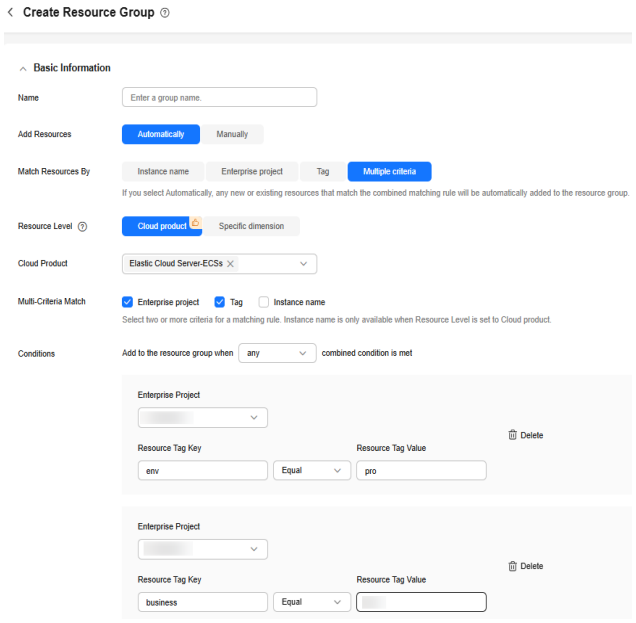


Table 4-4 Creating a resource group by matching resources by multiple criteria

Parameter	Example Value	Description
Name	Production_Business_XXX_Enterprise_Project_B	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Multiple criteria	How resources are added to a resource group.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Cloud Product	Elastic Cloud Server-ECSs	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instances belong 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.
Multi-Criteria Match	**Enterprise project** and **Tag** Combination method 1: Enterprise Project B and resource tag **env=pro** Combination method 2: Enterprise Project B and resource tag **business=xxx**	Combination method for matching resources by multiple criteria. After selecting a combination method, you need to set the corresponding matching rule. Each rule allows 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	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.
6. Click **Create**.
7. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

Creating a Resource Group by Matching Resources by Instance Name

When you create a resource group with **Match Resources By** set to **Multiple Criteria**, resources are added or matched based on the resource naming rule, which can be difficult to manage. Therefore, it is not recommended.

1. Log in to the **Cloud Eye console**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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, set parameters.

Figure 4-4 Matching resources by instance name

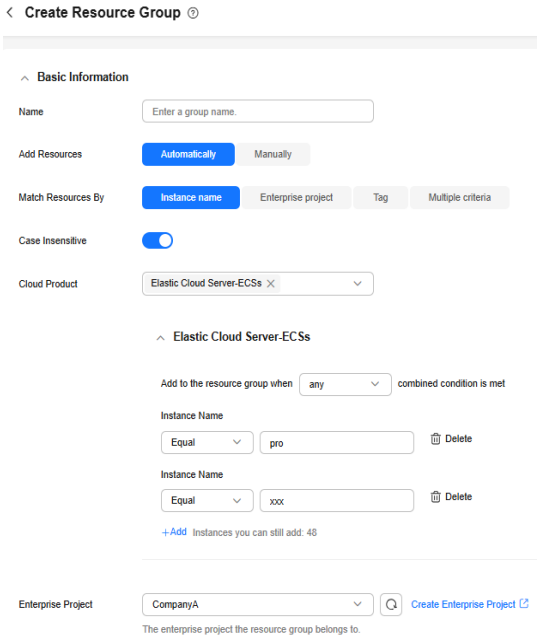


Table 4-5 Parameters for creating a resource group by matching resources by instance name

Parameter	Example Value	Description
Name	Resource_Group_test1	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Automatically	Method of adding or matching resources to a resource group.
Match Resources By	Instance name	How resources are added to a resource group.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If you select **Cloud product**, you need to select a cloud product. If you select **Specific dimension**, some dimensions of the cloud service are automatically selected. For details, click **View monitored dimensions**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Cloud Product	Elastic Cloud Server-ECSs Add to the resource group when any combined condition is met The instance name contains test1.	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. 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. It can contain only letters, digits, underscores (_), periods (.), and hyphens (-). The relationship between different cloud products is OR.
Enterprise Project	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.
6. Click **Create**.
7. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

Creating a Resource Group by Manually Selecting Cloud Products

Some services do not support automatic resource addition or resource match by tag for a resource group. For details about these services, see **Cloud Services Supported by Resource Groups**. To perform rights- and domain-based configuration for resources of these services, you need to manually select resources, which is complex.

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, set parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-6 Parameters for creating a resource group for services that do not support automatically adding resources

Parameter	Example Value	Description
Name	Resource_Group_Manual	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Manually	Method of adding or matching resources to a resource group.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**.
Cloud Product	NAT Gateway - Private NAT Gateway, Web Application Firewall - Dedicated WAF Instance, NAT Gateway - Public NAT Gateway	If **Resource Level** is set to **Cloud product**, you need to select the cloud product that the instance belongs to and select specified resources. You can select one or more cloud products.
Enterprise Project	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.
6. Click **Create**.
7. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

Creating a Resource Group by Manually Selecting Dimensions

- You created a resource group for which resources are added automatically and set **Resource Level** to **Specific dimension**, but resources of the selected dimension cannot be tagged for some reasons.

  For example, when you create a service in CCE, the listener created in ELB is automatically called. In this case, you need to set **Resource Level** to **Specific dimension** because only one type of resource (listener) needs to be added.
- Some resources require specific thresholds.

  For example, the message stacking threshold of a queue in a RabbitMQ instance needs to be lowered.

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Resource Groups**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3. In the upper right corner, click **Create Resource Group**.
4. On the **Create Resource Group** page, set parameters.

   Name: Name of a resource group. The value can contain 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

   Add Resources: Select **Manually**.

   Resource Level: Select **Specific dimension**.

   Table 4-7 Parameters for creating a resource group for services that do not support automatically adding resources

Parameter	Example Value	Description
Name	Resource_Group_Manual	Name of the resource group. The value can contain 1 to 128 characters and can only contain letters, digits, underscores (_), and hyphens (-).
Add Resources	Manually	Method of adding or matching resources to a resource group.
Resource Level	Specific dimension	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If this parameter is set to **Specific dimension**, you can manually select resources for the resource group.
Enterprise Project	Enterprise Project A	Enterprise project to which the resource group belongs, not the enterprise project to which the instance belongs.

5. Set alarm notification parameters as prompted. For details about alarm notification parameters, see **Creating an Alarm Rule**.
6. Click **Create**.
7. After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

4.3 Configuring Resource Groups for Event Alarms

When configuring alarm rules for events, you cannot select resource groups for some services. Currently, you can select resource groups only for event alarms of ECS (only supported in some regions; subject to the console), DDS, RDS, DCS, and GeminiDB. In this case, you are advised to configure alarm rules by setting **Monitoring Scope** to **Specified resources** or **All resources**. When selecting **Specified resources**, you can select specified resources from existing resource groups for better efficiency.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

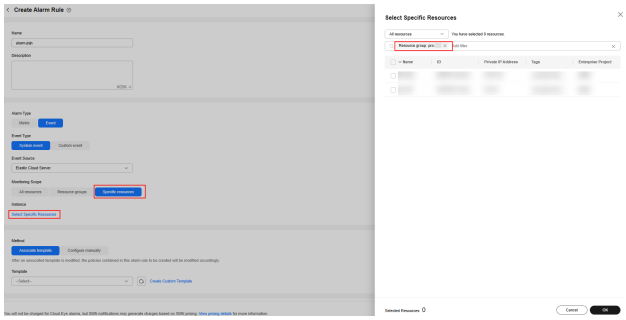
Before creating an alarm rule for specified resources, ensure that the resources have been added to a resource group. For details, see **Creating a Resource Group**.

Creating an Alarm Rule for Specified Resources

1. Log in to the **Cloud Eye console**.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, choose **Event Monitoring**.
5. Click **Create Alarm Rule** in the upper right corner and set parameters.
   a. Set **Monitoring Scope** to **Specified Resources** and click **Select Specified Resources** next to **Instance**.
   b. In the resource list, filter resources by resource group and select resources as needed.

   For parameter details, see **Creating an Alarm Rule and Notification for Event Monitoring**.

   Figure 4-5 Creating an alarm rule



6. Click **Create**.

If the resources in a resource group change, you need to manually update the resources for the event alarm rule. For details, see **Modifying an Alarm Rule**.

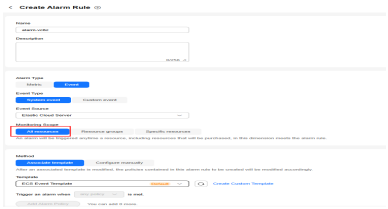
Creating an Alarm Rule for All Resources

1. Log in to the **Cloud Eye console**.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, choose **Event Monitoring**.
5. Click **Create Alarm Rule** in the upper right corner and set parameters.

   If **Monitoring Scope** is set to **All resources**, an alarm will be triggered if any resource of the current cloud product meets the alarm policy. For parameter details, see **Creating an Alarm Rule and Notification for Event Monitoring**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-6 Creating an alarm rule



6. Click **Create**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Scenario-specific Cases

5.1 Service Monitoring on E-Commerce Platforms

5.1.1 Overview

E-commerce services feature large data volume and large data access, which requires large memory, fast data exchange and processing, and extremely strict monitoring.

Elastic Cloud Servers (ECSs) is a core service in the e-commerce scenarios. Therefore, a comprehensive and three-dimensional ECS monitoring system plays an important role in service stability. **Server Monitoring** provides system-wide, active, and fine-grained ECS monitoring to ensure smooth service running.

People access the websites of e-commerce platforms and make transactions. During grand annual shopping festivals such as Double 12 and 618 shopping festivals , the websites are often hit by various problems like slow page loading and long network latency when people access from different networks.

For services used by an e-commerce platform, such as Relational Database Service (RDS), Elastic Load Balance (ELB), and Virtual Private Cloud (VPC), you can use the **Cloud Service Monitoring** function. On the **Cloud Service Monitoring** page, you can gain visibility into the running status of each cloud service and usage of each metric. After setting alarm rules for cloud service metrics, you can get a more accurate picture of the health of cloud services.

An e-commerce platform involves many cloud services, such as ECS, Content Delivery Network (CDN), Auto Scaling (AS), security services, RDS, ELB, and Object Storage Service (OBS). With **resource groups**, you can view resource usages, alarms, and health status from the service perspective and manage alarm rules. This greatly reduces O&M complexity and improves O&M efficiency.

5.1.2 Server Monitoring

ECSs are the cores of an e-commerce platform. Slight changes in ECS performance may cause dramatic fluctuation of e-commerce services or even service interruptions, resulting in huge losses.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Server Monitoring provides **Basic Monitoring** and **OS Monitoring** of different monitoring granularities. **Basic Monitoring** monitors metrics reported by ECSs. **OS Monitoring** provides system-wide, active, and fine-grained server monitoring after the Agent is installed on an ECS.

This section takes **(Agent) CPU Usage** as an example to describe how to use server monitoring. To reserve some processing performance for proper server running, you are advised to set its threshold to 80% and let Cloud Eye generate an alarm when the usage exceeds the threshold for three consecutive times.

Scenarios

In e-commerce scenarios such as promotions, flash sales, and red-hot sellers, the number of instantaneous visits multiplies to tens to hundreds of times than that in days without activities, which results in heavy server load and slow system response.

You can configure alarm rules for ECS metrics, for example, CPU usage. When the CPU usage reaches the threshold, an alarm notification is sent to remind you to handle the exception promptly.

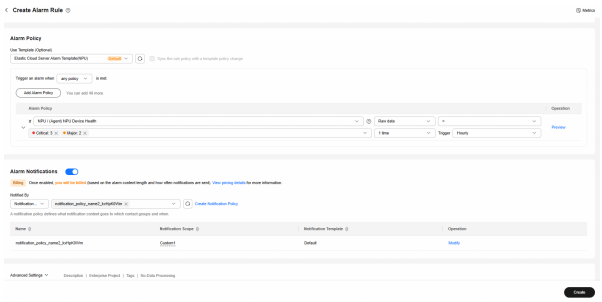
Prerequisites

The Agent has been installed. For details, see **Agent Installation and Configuration**.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring**.
3. Locate the target ECS. In the **Operation** column, click **More** and select **Create Alarm Rule**.
4. On the **Create Alarm Rule** page, the basic information is pre-filled by default. Set alarm policy parameters as prompted. For details about alarm policy parameters, see **Creating an Alarm Rule**.

   Figure 5-1 Creating an alarm rule

5. Configure alarm notification parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-1 Alarm notification parameters

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Select **Topic subscriptions** from the first drop-down list and **Account contact** from the second drop-down list.	Select a notification method and recipients. You can select notification policies, contact groups, or topic subscriptions. If you select **Account contact**, notifications will be sent to the mobile number and email address specified during registration.
Notification Window	00:00–23:59	If you select **Contact groups** or **Topic subscriptions** for **Notified By**, you need to set the notification window. The system sends notifications only within the notification window.
Trigger Condition	**Generated alarm** and **Cleared alarm**	If you set **Alarm Type** to **Contact groups** or **Topic subscriptions**, select **Generated alarm**, **Cleared alarm**, or both for this parameter.
Notification Template	System template	This parameter is only available if you set **Notified By** to **Contact groups** or **Topic subscriptions**. You can select an existing template or create one to send alarm notifications.

After the alarm rule is created, when the service volume surges and the metric data reaches the threshold, Cloud Eye notifies you of the cloud resource exception in real time.

5.1.3 Cloud Service Monitoring

For the RDS, ELB, and VPC services used by an e-commerce platform, you can use the **Cloud Service Monitoring** function. On the **Cloud Service Monitoring** page, you can accurately master the status of each cloud service and usage of each metric by setting alarm rules.

Prerequisites

Ensure that the cloud service for which you want to create an alarm rule has uploaded monitoring data to Cloud Eye. You can query the monitoring data on the **Cloud Service Monitoring** page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Cloud Service Monitoring**.
3. On the **Cloud Service Monitoring** page, click the dashboard named **Elastic Load Balance ELB**.
4. Locate the target load balancer and click **Create Alarm Rule** in the **Operation** column.

   The **Create Alarm Rule** page is displayed.

   NOTE

   To create an alarm rule for RDS or VPC, choose **Relational Database Service** or **Virtual Private Cloud** on the **Cloud Service Monitoring** page.

   For details about other parameters, see **Creating an Alarm Rule**.

   NOTE

   - To better monitor the ELB service, you need to enable the ELB health check first. For details, see **How Do I Troubleshoot an Unhealthy Backend Server of a Dedicated Load Balancer?** You are advised to set the outbound rate threshold to 80%.
   - You are advised to set the CPU usage threshold of the RDS instance to 80% and configure alarm triggering if the threshold is exceeded for three consecutive times. Set thresholds for other RDS metrics, such as disk usage, IOPS, and database connections in use as required.
   - You are advised to set the outbound bandwidth usage threshold of VPC to 80% and trigger an alarm if the threshold is exceeded for three consecutive times. Set thresholds for other Elastic IP and Bandwidth metrics as required.
5. Click **Create**.

   If the service volume soars and the specified RDS, VPC, or ELB threshold is reached, Cloud Eye immediately informs you of the resource exception. This helps you handle the exceptions in a timely manner to prevent business loss.

5.1.4 Resource Groups

A complete e-commerce platform uses a number of cloud services, such as ECS, CDN, AS, security services, RDS, OBS, and VPC. You can create resource groups and divide resources into different groups. You can accurately view resource usages, alarms, and health status, and manage alarm rules from the service perspective on the **Resource Groups** page. This greatly reduces O&M complexity and improves O&M efficiency.

This section describes how to create a resource group.

Procedure

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. Specify a name for the group.
5. Select a method for adding resources. For details about the parameters for creating a resource group, see **Creating a Resource Group**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6. Configure alarm notification parameters.
7. Click **Create**.

   After creating a resource group, you need to associate a custom metric alarm template with it to create alarm rules in batches. For details, see **Associating a Resource Group with an Alarm Template**.

5.2 Live Streaming Monitoring

5.2.1 Overview

In the era of rapid Internet development, the demand for live streaming is increasing. Services on Huawei Cloud, such as ECS, VPC, and ELB, provide stable resources to ensure convenient access, low latency, high concurrency, high definition, and smoothness of live streaming services. This solves the poor user experience caused by video freeze and blurring.

ECSs are the basis of live streaming services, VPCs provide networks, and ELBs are used for traffic distribution. Subtle ECS performance changes and sudden increase of network access traffic will cause service instability. In this regard, real-time monitoring of cloud resources and timely notification of resource exceptions become increasingly important. Cloud Eye monitors ECS, VPC, and ELB resources, detects exceptions in a timely manner, and notifies users of the exceptions.

5.2.2 Server Monitoring

ECSs are the core of live video streaming. Slight changes in ECS performance may greatly affect other cloud services. To monitor more fine-grained metrics, you can install the Agents on ECSs. For details, see **Agent Installation and Configuration**.

This section describes how to create alarm rules for ECS CPU usage, memory usage, and disk usage. It also includes how to configure an AS policy. When the ECS CPU usage reaches 90% for five consecutive times within 5 minutes, AS automatically adds an ECS to ensure stable service running.

After the alarm rule and AS policy are created, if the service volume soars and the specified threshold is reached, AS automatically adds an ECS and Cloud Eye immediately informs you of the resource exception.

Background

CPU Usage, Memory Usage, and Disk Usage are metrics for basic ECS monitoring. (Agent) CPU Usage, (Agent) Memory Usage, and (Agent) Disk Usage are metrics for fine-grained minute-level monitoring.

Creating an Alarm Rule

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Locate the target ECS. In the **Operation** column, choose **More** > **Create Alarm Rule**.
4. On the **Create Alarm Rule** page, set **Method** to **Configure manually** and configure alarm policies for the monitored instance.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 5-2 Creating an alarm rule

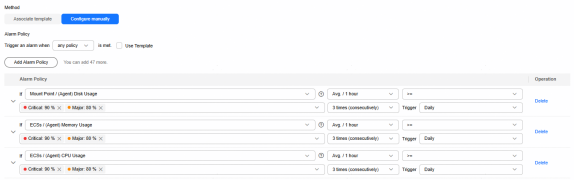


Table 5-2 Alarm policy description

Parameter	Example Value	Description
Metric Name	Alarm policy 1: **ECSs / (Agent) CPU Usage** Alarm policy 2: **ECSs / (Agent) Memory Usage** Alarm policy 3: **Mount Point / (Agent) Disk Usage**	Metric for triggering alarms.
Statistic	**Avg.** > **1 hour**	Metric value type. Cloud Eye supports the following statistics for metrics: **Raw data**, **Avg.**, **Max.**, **Min.**, **Variance**, and **Sum**.
Consecutive Triggers	3 times (consecutively)	Number of consecutive times that an alarm is triggered.
Operator	>=	Operator used to compare metric value and the threshold.
Threshold	**Major: 80%**; **Critical: 90%**	Alarm threshold and unit.
Frequency	Daily	How often alarms are repeatedly notified when there is already an alarm.

5. Configure alarm notification parameters. For details, see **Creating an Alarm Rule and Notifications**.

Table 5-3 Alarm notification parameters

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.

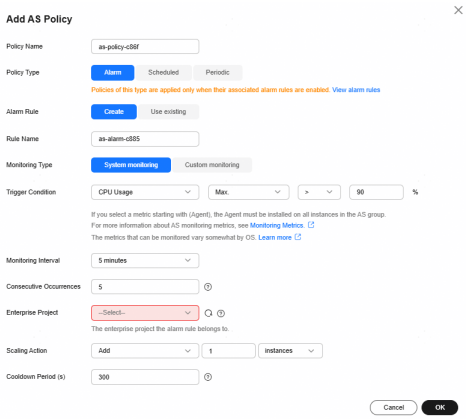
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value	Description
Notified By	Select **Topic subscriptions** from the first drop-down list and **Account contact** from the second drop-down list.	Select a notification method and recipients. You can select notification policies, contact groups, or topic subscriptions. If you select **Account contact**, notifications will be sent to the mobile number and email address specified during registration.
Notification Window	00:00–23:59	If you select **Contact groups** or **Topic subscriptions** for **Notified By**, you need to set the notification window. The system sends notifications only within the notification window.
Trigger Condition	**Generated alarm** and **Cleared alarm**	If you set **Alarm Type** to **Contact groups** or **Topic subscriptions**, select **Generated alarm**, **Cleared alarm**, or both for this parameter.
Notification Template	System template	This parameter is only available if you set **Notified By** to **Contact groups** or **Topic subscriptions**. You can select an existing template or create one to send alarm notifications.

Configuring an AS Policy

1. Choose **Computing** > **Auto Scaling**.
2. Click **Create AS Group**. For details, see **Creating an AS Group**.
3. In the AS group list, locate the created AS group and click **View AS Policy** in the **Operation** column.
4. On the **AS Policies** tab page, click **Add**. In the displayed **Add AS Policy** dialog box, set parameters based on **Figure 5-3**.

Figure 5-3 Adding an AS policy



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.2.3 ELB Monitoring

In live video streaming, sudden increase of network access traffic may cause service instability. Therefore, most live video streaming platforms use ELB to automatically distribute traffic to multiple ECSs.

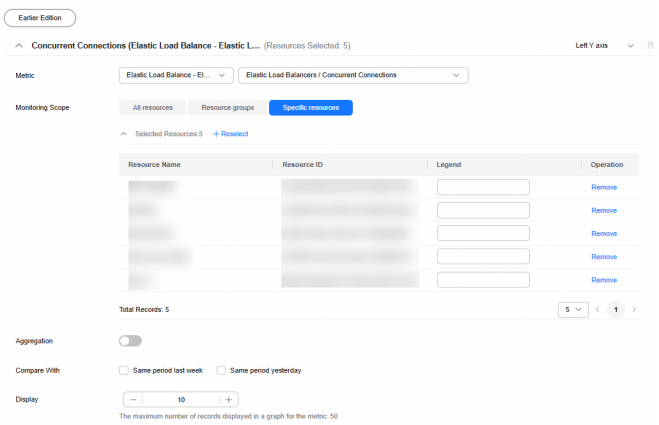
Stable and reliable load balancing is critical to the proper running of live video streaming. Cloud Eye can monitor unhealthy backend servers and concurrent connections of load balancers to ensure proper running of your services.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, click **My Dashboards** > **Custom Dashboards**.
3. Locate the dashboard for which you want to add a graph and click its name.
4. In the upper part of the page, click **Create** and then **Create Graph**.

   In the **Add Graph** dialog box, add the concurrent connections of all enhanced elastic load balancers involved in live video streaming to the same graph.

   Figure 5-4 Adding a graph

   NOTE

   The running trends of all concurrent connections in the same live video streaming must be consistent. If the trend of one or more concurrent connections is inconsistent with other trends, an exception occurs. In this case, locate the cause and rectify the fault immediately.

5. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
6. Click **Create Alarm Rule** in the upper right corner of the page.
7. On the displayed page, set the parameters as prompted. For details about alarm rule parameters, see **Creating an Alarm Rule and Notifications**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 5-5 Creating an alarm rule

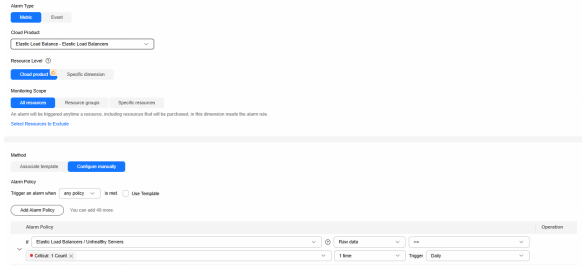


Table 5-4 Alarm content parameters

Parameter	Example Value	Description
Alarm Type	Metric	Alarm type that the alarm rule applies to.
Cloud Product	Elastic Load Balance - Elastic Load Balancers	Name of the monitored service.
Resource Level	Cloud product	A cloud product has many specific dimensions. If you set this parameter to **Cloud product**, metrics across dimensions can be configured in the same alarm rule. If you set it to **Specific dimension**, only metrics of the specified dimension can be configured in the same alarm rule.
Monitoring Scope	All resources	Monitoring scope the alarm rule applies to.
Method	Configure manually	Method of triggering the rule.
Metric Name	**Elastic Load Balances** > **Unhealthy Servers**	Metric for triggering alarms.
Alarm Policy	If **Raw data** of the metric **>= 1** for **1 time**, a **Critical** alarm is triggered **Daily**.	Policy for triggering an alarm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-5 Alarm notification parameters

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Alarm notification mode.
Recipient	Account contact	• If **Notified By** is set to **Topic subscriptions**, you need to select the recipients. • If **Recipient** is set to **Account contact**, notifications will be sent to the registered mobile number and email address.
Notification Window	00:00–23:59	• If **Notified By** is set to **Topic subscriptions**, you need to set the notification window. • Cloud Eye sends notifications only within the specified time period.
Trigger Condition	**Generated alarm** and **Cleared alarm**	If you set **Alarm Type** to **Contact groups** or **Topic subscriptions**, select **Generated alarm**, **Cleared alarm**, or both for this parameter.

8. Click **Create**.

   When ELB is abnormal, Cloud Eye interworks with SMN to notify you of the resource exception in real time.

5.2.4 Network Monitoring

In live video streaming, random packet loss occurs when the outbound bandwidth reaches the upper limit. Therefore, attention must be paid to this metric of Elastic IP and Bandwidth.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

This section describes how to set alarm rules for the outbound bandwidth usage of Elastic IP and Bandwidth.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Cloud Service Monitoring**.
3. On the displayed page, click the VPC dashboard name.
4. Locate the row that contains the target VPC and choose **More** > **Create Alarm Rule** in the **Operation** column.
5. On the **Create Alarm Rule** page, set **Method** to **Configure manually** and configure alarm policies for the monitored instance.

   You are advised to configure alarm rules for the EIPs and bandwidths involved in the service. Set the threshold of **Outbound Bandwidth Usage** to **Raw data ≥ 90%** of the purchased bandwidth.

   Table 5-6 Alarm policy description

Parameter	Example Value	Description
Metric Name	Alarm policy 1: **Bandwidths** > **Outbound Bandwidth Usage** Alarm policy 2: **Bandwidths** > **Inbound Bandwidth Usage**	Metric for triggering alarms.
Statistic	Raw data	Metric value type. Cloud Eye supports the following statistics for metrics: **Raw data**, **Avg.**, **Max.**, **Min.**, **Variance**, and **Sum**.
Consecutive Triggers	3 times (consecutively)	Number of consecutive times that an alarm is triggered.
Operator	>=	Operator used to compare metric value and the threshold.
Threshold	Critical: 90%	Alarm threshold and unit.
Frequency	Daily	How often alarms are repeatedly notified when there is already an alarm.

6. Configure alarm notification parameters. For details, see **Creating an Alarm Rule and Notifications**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-7 Alarm notification parameters

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Select **Topic subscriptions** from the first drop-down list and **Account contact** from the second drop-down list.	Select a notification method and recipients. You can select notification policies, contact groups, or topic subscriptions. If you select **Account contact**, notifications will be sent to the mobile number and email address specified during registration.
Notification Window	00:00–23:59	If you select **Contact groups** or **Topic subscriptions** for **Notified By**, you need to set the notification window. The system sends notifications only within the notification window.
Trigger Condition	**Generated alarm** and **Cleared alarm**	If you set **Alarm Type** to **Contact groups** or **Topic subscriptions**, select **Generated alarm**, **Cleared alarm**, or both for this parameter.
Notification Template	System template	This parameter is only available if you set **Notified By** to **Contact groups** or **Topic subscriptions**. You can select an existing template or create one to send alarm notifications.

7. Click **Create**.

   When the bandwidth is abnormal, Cloud Eye sends real-time alerts via the SMN service.

5.3 Crowdsourcing Platforms

5.3.1 Overview

Crowdsourcing platforms, as knowledge worker sharing platforms, use the Internet to allocate jobs and connect employers with service providers. Many service providers provide customized solutions for enterprises, public institutions, and individuals to transform ideas, wisdom, and skills into business value and social value.

Core databases of a crowdsourcing platform deployed on Huawei Cloud use BMS clusters. The web servers and API servers are deployed on ECSs. The web servers provide website search, category, store, and transaction services. The API servers

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

provide basic APIs for connecting services to the databases. The running statuses of BMSs and ECSs are critical to the entire service. CPU, memory, and disk usages affect the overall service status. Therefore, you need to use the server monitoring and event monitoring functions to monitor the running statuses of ECSs and BMSs at any time. For details, see **Server Monitoring** and **Event Monitoring**.

Services like VPC, NAT Gateway, and ELB provide basic network support. The network status affects the connectivity between services. Therefore, you need to use **Network Monitoring** to monitor the running status of each service system at any time.

5.3.2 Server Monitoring

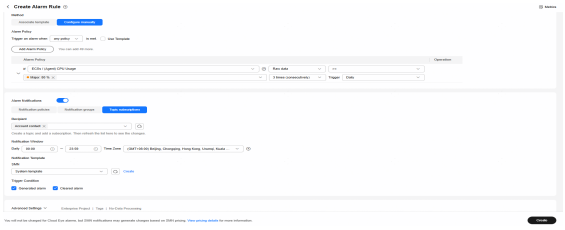
On crowdsourcing platforms, ECSs provide computing resources, and databases are deployed on BMSs. Therefore, BMS disk read and write rates affect the database operation speed. ECS memory and CPU usages affect the service execution speed. To monitor more fine-grained metrics, you can **install and configure the Agent** on ECSs.

You can set the thresholds of CPU usage, memory usage, and disk usage to 80%, respectively. The following procedure uses CPU usage as an example.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**.
3. Locate the target ECS. In the **Operation** column, choose **More** > **Create Alarm Rule**.
4. On the displayed page, set **Method** to **Configure manually** and configure alarm policies for the monitored instance. For details, see **Creating an Alarm Rule and Notifications**.

   Figure 5-6 Creating an alarm rule

   After the alarm rule is created, when the service volume surges and the metric data reaches the threshold, the system notifies you of the resource exception in real time.

5.3.3 Network Monitoring

During activities on a crowdsourcing platform, traffic to the website homepage, login page, and store details page increases instantaneously. The outbound bandwidth needs to be monitored at any time.

In addition, if the number of connections increases sharply due to DDoS attacks or heavy traffic, service access becomes slow. The number of SNAT connections on

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

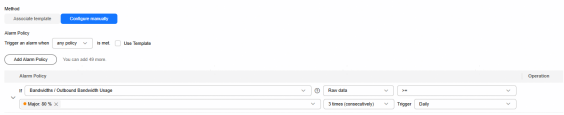
days with activities is expected to be two to three times higher. Therefore, you need to monitor the number of SNAT connections at any time.

Procedure

1. Log in to the **Cloud Eye console**.
2. Choose **Cloud Service Monitoring**.
3. Click the name of the VPC dashboard to access its details page.
   a. Locate the row that contains the target VPC and choose **More** > **Create Alarm Rule** in the **Operation** column.
   b. On the **Create Alarm Rule** page, set parameters as shown in **Figure 5-7**.

      You are advised to set the threshold of the outbound bandwidth usage to 80%.

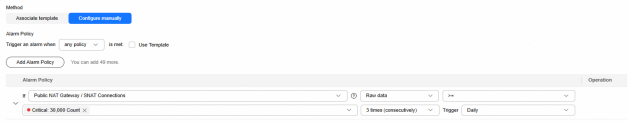
      Figure 5-7 Creating an alarm rule (for a VPC)

   c. Click **Create**.
4. Click the NAT Gateway dashboard to access its details page.
   a. Locate the row that contains the target NAT gateway and choose **More** > **Create Alarm Rule** in the **Operation** column.
   b. On the **Create Alarm Rule** page, set parameters as shown in **Figure 5-8**.

      In this example, the number of SNAT connections is 10,000 in normal days, and that number is two to three times in peak hours. Therefore, you are advised to set the threshold of SNAT connections to 30,000.

      Figure 5-8 Creating an alarm rule (for a NAT gateway)

   c. Click **Create**.

When the bandwidth is abnormal, Cloud Eye sends real-time alerts via the SMN service.

5.3.4 Event Monitoring

During service running, you can delete, reboot, or stop ECSs and BMSs, and delete NICs or security group rules for the ECSs and BMSs at any time as required. You can use the event monitoring function to monitor the running status of ECSs and BMSs at any time.

Procedure

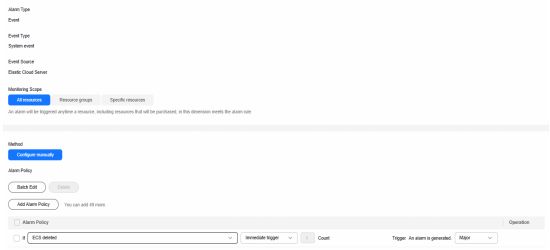
1. Log in to the **Cloud Eye console**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. In the navigation pane, choose **Event Monitoring**. Locate an event and click **Create Alarm Rule** in the **Operation** column.

   This section uses ECS deletion as an example. You can also create alarm rules for other events, such as rebooting ECSs, stopping ECSs, and deleting NICs.

   Figure 5-9 Creating an alarm rule

   When the ECSs or BMSs are abnormal, Cloud Eye notifies you of the resource exception in real time through the SMN service.

5.4 Best Practices of Event Monitoring

5.4.1 ECS Events

Elastic Cloud Server (ECS) is a cloud server that provides scalable, on-demand computing resources for secure, flexible, and efficient applications. ECSs are the core of various services. Slight changes in ECS performance, abnormal running, and automatic recovery, may greatly affect cloud services.

Therefore, elastic load balancers are required to distribute access traffic to multiple backend ECSs based on forwarding policies. Traffic distribution expands the external service capability of the application system. This eliminates single point of failures (SPOFs), thereby improving the application system availability. The event monitoring function of Cloud Eye can monitor ECS running exceptions and automatic recovery. You can subscribe to the ECS event notification when changes occur.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-8 Key ECS events

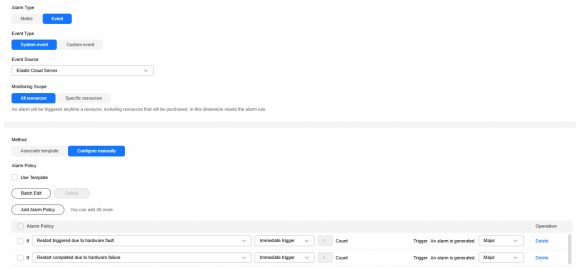
Event Name	Event ID	Event Severity	Event Description	Solution	Impact
Redeployment triggered by system faults	startAutoRecovery	Major	ECSs on a faulty host were automatically migrated to another properly-running host. During the migration, the ECSs were restarted.	Wait until the migration is successful and the ECS status is normal.	ECSs are redeployed.
Redeployment triggered by system faults completed	endAutoRecovery	Major	ECSs are recovered after the automatic migration is complete.	Check whether services are restored.	The ECS redeployment is complete.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   In this example, values of **Event Name** of two alarm policies are set to **Restart triggered due to hardware fault** and **Restart completed due to hardware failure**, respectively. For details about the parameters, see **Creating an Alarm Rule and Notification for Event Monitoring**.

   Figure 5-10 Creating an alarm rule

3. Click **Create**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

When abnormal ECS events occur, Cloud Eye notifies you in real time through the SMN service.

5.4.2 RDS Events

RDS is an online relational database service based on the cloud computing platform. RDS is reliable, scalable, and easy to manage, and immediately ready for use. When using relational databases, you need to pay attention to the database status. You can use event monitoring to track abnormal events to ensure stable service running.

Table 5-9 Key RDS events

Event Name	Event Description	Handling Method
DB instance creation failure	Generally, DB instances fail to be created because the number and quota of disks are small, and the underlying resources are exhausted.	Check the number and quota of disks. Release resources and create DB instances again.
Full backup failure	A single full backup failure does not affect the files that have been successfully backed up, but prolongs the incremental backup time during the point-in-time restore (PITR).	Create a manual backup again.
Primary/standby switchover failure	The standby DB instance does not take over services from the primary DB instance due to some network or server failures. The original primary DB instance continues to provide services within a short time.	Check whether the connection between the application and the database is re-established.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Event Name	Event Description	Handling Method
Replication status abnormal	The replication delay between the primary and standby DB instances is too long (usually occurs when a large amount of data is written to databases or a large transaction is performed). During off-peak hours, the replication delay between the primary and standby DB instances gradually decreases. Another possible cause is that the network between the primary and standby DB instances is interrupted. However, the network interruption does not interrupt data read and write of a single DB instance, and customers' applications are unaware of the interruption.	Submit a service ticket for processing.
DB instance faulty	A single or primary DB instance is faulty due to a disaster or a server failure. This event is critical and may cause database service unavailability.	Check whether an automated backup policy has been configured for the DB instance and submit a service ticket for processing.
Failure of changing single DB instance to primary/standby	During the standby DB instance creation or after the standby DB instance is created, the configuration synchronization between the primary DB instance and the standby DB instance is faulty. Generally, the fault is caused by insufficient resources of the data center where the standby DB instance is located. This event does not cause the data read and write interruption of the original single DB instance, and customers' applications are unaware of this event.	Submit a service ticket for processing.
Replication status recovered	The replication delay between the primary and standby DB instances is within the normal range, or the network connection between the two is restored.	No action is required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

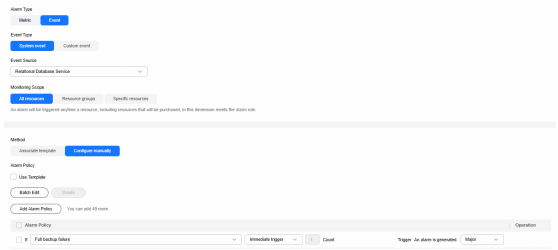
Event Name	Event Description	Handling Method
DB instance recovered	RDS uses high availability tools to rebuild the standby DB instance for disaster recovery.	No action is required.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   In this example, **Event Name** is set to **Full backup failure**. Set the event name as required. For details about other parameters, see **Creating an Alarm Rule and Notification for Event Monitoring**.

   Figure 5-11 Creating an alarm rule

3. Click **Create**.

When abnormal DB instance events occur, Cloud Eye notifies you in real time through the SMN service.

5.4.3 EIP Events

VPC enables you to build isolated, configurable, and manageable virtual networks for ECSs, improving the security of your resources on the cloud and simplifying network deployment.

You can bind an EIP assigned in a VPC to your ECS to access the Internet. Different EIPs can share a bandwidth, reducing your bandwidth costs.

With the event monitoring function, Cloud Eye monitors the EIP status. This prevents abnormal events and packet loss that affect your services. You can subscribe to the EIP event notification when changes occur.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-10 Key EIP events

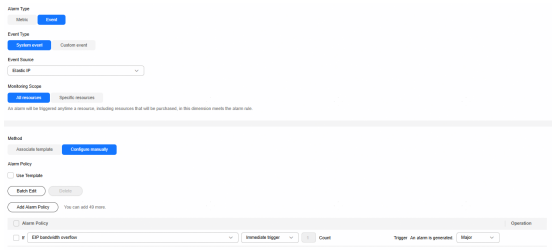
Event Name	Event Description	Handling Method
EIP bandwidth overflow	If this event is reported, the bandwidth exceeds the purchased bandwidth, which may slow down the network or cause packet loss. **NOTE** This event is available only in certain regions. You can check the regions on the console.	Check whether the EIP bandwidth keeps increasing and whether services are normal. Expand capacity if required.
EIP blocked	If the bandwidth exceeds 5 Gbit/s, the traffic is blocked. That is, the traffic is directly discarded. This indicates that the bandwidth exceeds the threshold or the system suffers from attacks (generally DDoS attacks). If the EIP unblocked event is reported, the blocking has been resolved.	Replace the EIP to prevent services from being affected. In addition, check the blocking cause and rectify the fault.
EIP unblocked		Use the unblocked EIP again to avoid resource waste.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   In this example, **Event Name** is set to **EIP bandwidth overflow**. For details about other parameters, see **Creating an Alarm Rule and Notification for Event Monitoring**.

   Figure 5-12 Creating an alarm rule

3. Click **Create**.

When abnormal EIP events occur, Cloud Eye notifies you in real time through the SMN service.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.5 Resource Group Monitoring

Scenarios

Cloud Eye provides the resource group and alarm functions. With it, you can group and monitor resources and receive alarm notifications of the resources in different groups.

This section describes how to do this.

Assume that there are four ECSs, namely ECS-01, ECS-02, ECS-03, and ECS-04. ECS-01 and ECS-02 are used by the development team. ECS-03 and ECS-04 are used by the test team. You need to obtain the running status of the two ECSs in the development team in a timely manner, including their CPU usage, idle CPU usage, average load, I/O usage, disk usage, memory usage, and percentage of total inode used.

Table 5-11 ECS list and group planning

ECS Name	Group	Whether to Install the Agent	Department
ECS-01	Development team resources	Yes	Development team
ECS-02	Development team resources	Yes	Development team
ECS-03	N/A	No	Test team
ECS-04	N/A	No	Test team

Prerequisites

The Agent has been installed on ECS-01 and ECS-02. For details, see **Agent Installation and Configuration**.

Step 1 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. Enter the group name as prompted. In this example, enter **Development-group-resources**.
5. Select the target cloud service resources.
6. Click **Create**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 2 Creating a Topic and Configuring the Notification Object

When resource exceptions occur, an alarm notification can be sent to the configured topic subscribers.

1. Log in to the **SMN console**.
2. In the navigation pane, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.
3. In the upper right corner, click **Create Topic**.

   The **Create Topic** dialog box is displayed.
4. Set the parameters as prompted. For details about the parameters, see **Creating a Topic**.
5. Click **OK.**

   The topic you created is displayed in the topic list.

   NOTE

   Click the topic name to view the topic details and the total number of topic subscriptions.
6. In the topic list, locate the new topic. In the **Operation** column, click **More** and select **Add Subscription**.
7. Specify the subscription protocol and endpoints.
8. Click **OK**.

   The subscriptions you added are displayed in the subscription list.

Step 3 Creating an Alarm Rule

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Rule Settings**.
3. In the upper right corner, click **Create Alarm Rule**.
4. On the displayed page, set parameters as prompted. For details about the parameters, see **Creating an Alarm Rule and Notifications**.

   NOTE

   Set the monitoring scope to **Resource groups** and select the **Development team resources** group created in **Step 1 Creating a Resource Group**.

   a. Set **Alarm Notification** parameters.

      NOTE

      - Select **Topic subscriptions** for **Notified By** and select the **Mytopic** topic created in **Step 2 Creating a Topic and Configuring the Notification Object**.
      - Alarm notifications sent by SMN will be billed. For details, see **Product Pricing Details**.

   b. Click **Create**.

After the alarm rule is added, if the metric data reaches the threshold, Cloud Eye immediately informs you that the metric data of group **Development group resources** (ECS-01 and ECS-02) is abnormal through SMN.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.6 Configuring an Alarm Rule for the Disk Usage of All Mount Points on an ECS

Scenarios

Cloud Eye allows you to configure alarm rules for all mount points of an ECS. This section describes how to configure alarm rules for the disk usage of all mount points on an ECS.

- The disk usage metric has been adjusted to a mount point dimension. When you configure a new alarm rule for the disk usage, you need to select the **ECS - Mount Point** dimension.
- If you have configured an alarm rule for **Any mount point** of an ECS, the alarm rule will automatically apply to new mount points of the ECS.
- If you have configured an alarm rule for the disk usage of the mount point, when you modify the alarm rule, the system prompts you to split the alarm rule into multiple rules in different dimensions. You are advised to select all mount points for the new alarm rules.

Prerequisites

The Agent has been installed on the ECS.

Procedure

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**, and click **Create Alarm Rule** in the upper right corner.
3. On the displayed page, enter the rule name and description, and set the following parameters as prompted.
   - **Alarm Type**: **Metric**
   - **Cloud Product**: **Elastic Cloud Server - ECSs**
   - **Resource Level**: **Specific dimension**. Select **ECSs - Mount Point** from the drop-down list next to this option.
   - **Monitoring Scope**: **Specific resources**
   - **Instance**: Click **Select Specific Resources**. On the displayed page, select all resources, that is, all mount points of all ECSs of the current account.
   - **Method**: **Configure manually**
   - **Alarm Policy**: If **Raw data** of **(Agent) Disk Usage >= 80%** for **3 times (consecutively)**, a **Major** alarm is triggered **Daily**.
4. If you want to receive alarm notifications, enable **Alarm Notification** and select a notification method.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Suggestions on Cloud Eye Security Configuration

This section provides actionable guidance for enhancing the overall security of Cloud Eye. You can continuously evaluate the security of Cloud Eye and combine different security capabilities to enhance overall defense. By doing this, stored data can be protected from leakage and tampering both at rest and in transit.

Consider the security configurations from the following aspects:

- **Granting User Permissions Using Access Control Capabilities**
- **Protecting Privacy and Sensitive Information Through Data Masking**
- **Enabling CTS to Record All Cloud Eye Access Operations**

Granting User Permissions Using Access Control Capabilities

You need to grant necessary permissions to IAM users with different roles to prevent data leakage or misoperations caused by excessive permissions

To better isolate and manage permissions, you are advised to configure independent IAM administrators and grant them privileges to manage IAM policies. An IAM administrator can create different user groups based on your service requirements. User groups correspond to different data access scenarios. By adding users to user groups and binding IAM policies to user groups, the IAM administrator can grant different data access permissions to employees in different departments based on the principle of least privilege. For details, see **Login Protection** and **Login Authentication Policy**.

Protecting Privacy and Sensitive Information Through Data Masking

When a service request includes sensitive information, you are advised to use the data masking function. On the data masking page, create masking configurations for your components. The platform will then replace sensitive information in traces with a globally unique random character string (**Hash code** mode) or a fixed number of asterisks (*) (**Mask** mode). After the configuration is applied, you can go to the tracing page to view the trace details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Enabling CTS to Record All Cloud Eye Access Operations

Cloud Trace Service (CTS) is a log audit service intended for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to track resource changes, analyze security compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record Cloud Eye operations for auditing. For details, see **Overview**. For details about the Cloud Eye operations that can be recorded, see **Operations That Can Be Recorded by CTS**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.