Best Practices

Best Practices

Issue 05

Date 2025-12-22

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Configuration Method

1.1 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 recipients in notification groups or topic subscriptions of alarms by severity. This helps reduce repeated alarms and ensures important ones are not missed.

Prerequisites

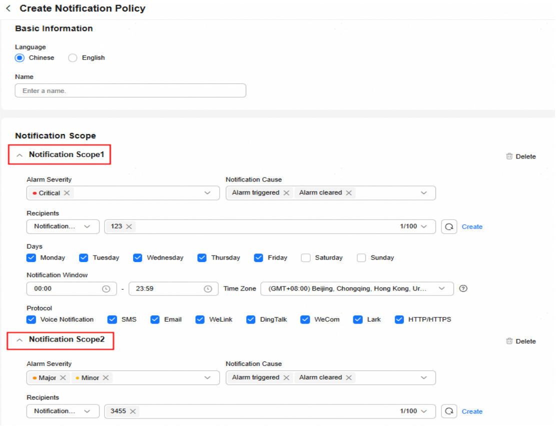
You have added recipients for receiving alarms with different severities, channels, and time frames to different notification groups or topic subscriptions. For details about how to configure a notification group, see **Creating a Recipient and Notification Group**. For details about how to configure 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 notification groups or subscription topics receive alarms. This setup allows sending notifications based on severity, channel, timing, and recipients.

Figure 1-1 Creating a notification policy



< Create Notification Policy

Basic Information

Language
● Chinese ○ English

Name
Enter a name.

Notification Scope

Notification Scope1 Delete

Alarm Severity: Critical
Notification Cause: Alarm triggered, Alarm cleared

Recipients: Notification... 123 1/100 Create

Days
☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Notification Window: 00:00 - 23:59 Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Ur...

Protocol
☑ Voice Notification ☑ SMS ☑ Email ☑ WeLink ☑ DingTalk ☑ WeCom ☑ Lark ☑ HTTP/HTTPS

Notification Scope2 Delete

Alarm Severity: Major, Minor
Notification Cause: Alarm triggered, Alarm cleared

Recipients: Notification... 3455 1/100 Create

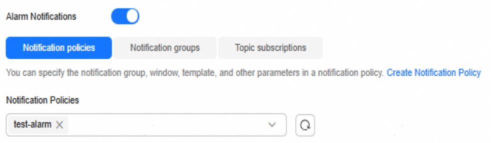
4. After the parameters are configured, click **OK**.

Creating an Alarm Rule

1. Log in to the Cloud Eye console.
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
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 1-2 Configuring alarm notifications



Alarm Notifications: on

Notification policies | Notification groups | Topic subscriptions

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

Notification Policies: test-alarm

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

1.2 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

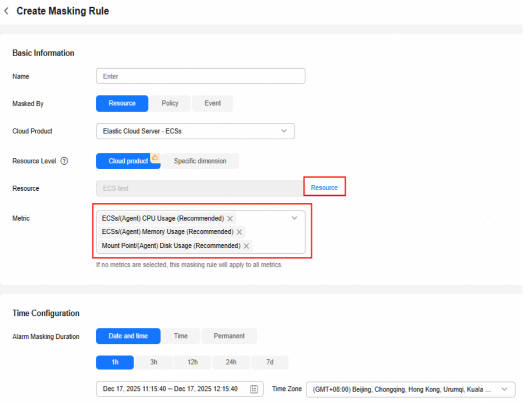
If you have configured alarm rules to monitor various metrics of both production and test resources on the cloud, you can set up masking rules for test resources to avoid receiving alarms for such resources.

Creating an Alarm Masking Rule

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

3. In the upper right corner of the page, click **Create Masking Rule**.
4. On the **Create Masking Rule** page, set parameters as prompted. For details, see **Creating a Masking Rule**.
   1. Set **Masked By** to **Resource**.
   2. Set **Cloud Product** to the name of the target cloud service.
   3. Click **Resource**. On the displayed page, select one or more resources to be masked.
   4. 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 1-3 Creating an alarm masking rule



Create Masking Rule

Basic Information

Name: Enter

Masked By: Resource

Cloud Product: Elastic Cloud Server - ECSs

Resource Level: Cloud product

Resource: ECS-test

Metric: ECSs/(Agent) CPU Usage (Recommended), ECSs/(Agent) Memory Usage (Recommended), Mount Point/(Agent) Disk Usage (Recommended)

If no metrics are selected, this masking rule will apply to all metrics.

Time Configuration

Alarm Masking Duration: Date and time

1h

Dec 17, 2025 11:15:40 – Dec 17, 2025 12:15:40

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala ...

5. Click **Create**.

2 Cloud Resource Monitoring

2.1 Creating Alarm Rules By Associating Resource Groups with Alarm Templates

When your account buys many cloud services, organize them efficiently by creating resource groups. 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.

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.

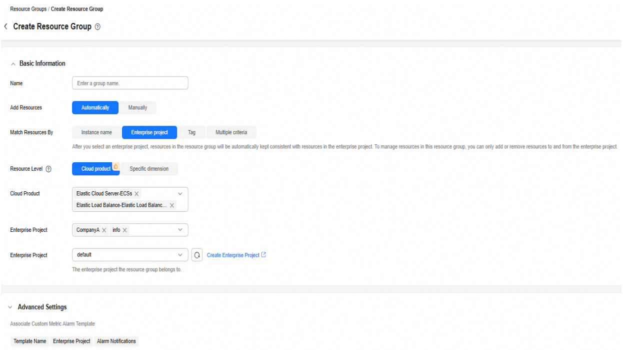
e. Select an enterprise project that the resources belongs to.

> 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. Click **Create**.

The created resource group appears in the resource group list.

Figure 2-1 Matching resources by enterprise project



Resource Groups / Create Resource Group

Create Resource Group

Basic Information

Name: Enter a group name.

Add Resources: Automatically | Manually

Match Resources By: Instance name | Enterprise project | Tag | Multiple criteria

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

Resource Level: Cloud product | Specific dimension

Cloud Product: Elastic Cloud Server-ECSs; Elastic Load Balance-Elastic Load Balanc...

Enterprise Project: CompanyA; info

Enterprise Project: default

The enterprise project the resource group belongs to.

Advanced Settings

Associate Custom Metric Alarm Template

Template Name	Enterprise Project	Alarm Notifications

Creating a Custom Alarm Template

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click **Create Custom Template** in the upper right corner.
4. On the displayed page, set the template parameters as follows:

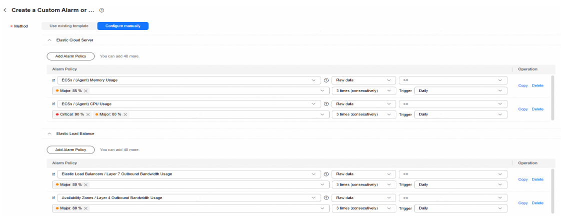
a. Enter a template name, for example, **Key_Service_Resource_Alarm_Template**.

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 2-2 Creating a custom alarm template



Create a Custom Alarm or ...

* Method: Use existing template | Configure manually

Elastic Cloud Server

You can add 48 more.

Alarm Policy	Operation
If ECSs / (Agent) Memory Usage, Raw data, >= Major: 85 %, 3 times (consecutively), Trigger Daily	Copy Delete
If ECSs / (Agent) CPU Usage, Raw data, >= Critical: 90 %, Major: 80 %, 3 times (consecutively), Trigger Daily	Copy Delete

Elastic Load Balance

You can add 48 more.

Alarm Policy	Operation
If Elastic Load Balancers / Layer 7 Outbound Bandwidth Usage, Raw data, >= Major: 80 %, 3 times (consecutively), Trigger Daily	Copy Delete
If Availability Zones / Layer 4 Outbound Bandwidth Usage, Raw data, >= Major: 80 %, 3 times (consecutively), Trigger Daily	Copy Delete

e. Click **Create**.

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

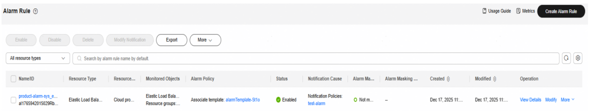
Associating a Custom Metric Alarm Template with a Resource Group

1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Templates**.
3. Click the **Custom Metric Templates** tab.
4. Locate the row that contains the target alarm template and click **Associate with Resource Group** in the **Operation** column.
5. In the **Associate with Resource Group** dialog box, select the created resource group and set alarm notification parameters. For details about alarm notification parameters, see **Configuring alarm notifications**.
6. Click **OK** to deliver the association task.
7. 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 2-3 Alarm rules



Name/ID	Resource Type	Resource...	Monitored Objects	Alarm Policy	Status	Notification Cause	Alarm Ma...	Alarm Masking ...	Created	Modified	Operation
product-alarm-sys_e... al1765942015029Rb...	Elastic Load Bala...	Cloud pro...	Elastic Load Bala... Resource groups:...	Associate template: alarmTemplate-5t1o	Enabled	Notification Policies: test-alarm	Not m...	--	Dec 17, 2025 11:...	Dec 17, 2025 11:...	View Details Modify More

2.2 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

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(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
	(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

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(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
	(Agent) Disk I/O Usage	disk_ioUtils	Raw data	3	>	80	90	%	Hourly
	(Agent) Disk Usage	disk_usedPercent	Raw data	3	>	80	90	%	Hourly

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(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
	(Agent) NPU Memory Usage	npu_util_rate_mem	Raw data	5	>	98	-	%	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(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
	(Agent) Isolated Memory Pages with HBM Double-Bit Errors	npu_hbm_double_bit_isolated_pages_cnt	Raw data	5	>=	64	-	count	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	(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 Lane 0 SNR	npu_macro1_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro1 SerDes Lane 1 SNR	npu_macro1_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro1 SerDes Lane 2 SNR	npu_macro1_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro1 SerDes Lane 3 SNR	npu_macro1_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane 0 SNR	npu_macro2_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane 1 SNR	npu_macro2_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro2 SerDes Lane 2 SNR	npu_macro2_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro2 SerDes Lane 3 SNR	npu_macro2_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane 0 SNR	npu_macro3_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane 1 SNR	npu_macro3_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane 2 SNR	npu_macro3_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro3 SerDes Lane 3 SNR	npu_macro3_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	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
	NPU Macro5 SerDes Lane 0 SNR	npu_macro5_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro5 SerDes Lane 1 SNR	npu_macro5_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro5 SerDes Lane 2 SNR	npu_macro5_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro5 SerDes Lane 3 SNR	npu_macro5_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane 0 SNR	npu_macro6_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane 1 SNR	npu_macro6_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro6 SerDes Lane 2 SNR	npu_macro6_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro6 SerDes Lane 3 SNR	npu_macro6_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane 0 SNR	npu_macro7_serdes_lane0_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane 1 SNR	npu_macro7_serdes_lane1_snr	Raw data	5	<	-	500000	db	Once
	NPU Macro7 SerDes Lane 2 SNR	npu_macro7_serdes_lane2_snr	Raw data	5	<	-	500000	db	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro7 SerDes Lane 3 SNR	npu_macro7_serdes_lane3_snr	Raw data	5	<	-	500000	db	Once
	Packets Retransmitted by NPU Macro1	npu_macro1_retry_cnt	Raw data	5	>	0	-	count	Once
	Packets Retransmitted by NPU Macro2	npu_macro2_retry_cnt	Raw data	5	>	0	-	count	Once
	Packets Retransmitted by NPU Macro3	npu_macro3_retry_cnt	Raw data	5	>	0	-	count	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Packets Retransmitted by NPU Macro4	npu_macro4_retry_cnt	Raw data	5	>	0	-	count	Once
	Packets Retransmitted by NPU Macro5	npu_macro5_retry_cnt	Raw data	5	>	0	-	count	Once
	Packets Retransmitted by NPU Macro6	npu_macro6_retry_cnt	Raw data	5	>	0	-	count	Once
	Packets Retransmitted by NPU Macro7	npu_macro7_retry_cnt	Raw data	5	>	0	-	count	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Invalid Packets Received by NPU Macro1	npu_macro1_crc_error_cnt	Raw data	5	>	0	-	count	Once
	Invalid Packets Received by NPU Macro2	npu_macro2_crc_error_cnt	Raw data	5	>	0	-	count	Once
	Invalid Packets Received by NPU Macro3	npu_macro3_crc_error_cnt	Raw data	5	>	0	-	count	Once
	Invalid Packets Received by NPU Macro4	npu_macro4_crc_error_cnt	Raw data	5	>	0	-	count	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Invalid Packets Received by NPU Macro5	npu_macro5_crc_error_cnt	Raw data	5	>	0	-	count	Once
	Invalid Packets Received by NPU Macro6	npu_macro6_crc_error_cnt	Raw data	5	>	0	-	count	Once
	Invalid Packets Received by NPU Macro7	npu_macro7_crc_error_cnt	Raw data	5	>	0	-	count	Once
	NPU Macro1 BER	npu_macro1_crc_error_rate	Raw data	5	>	0	-	count	Once
	NPU Macro2 BER	npu_macro2_crc_error_rate	Raw data	5	>	0	-	%	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	NPU Macro3 BER	npu_macro3_crc_error_rate	Raw data	5	>	0	-	%	Once
	NPU Macro4 BER	npu_macro4_crc_error_rate	Raw data	5	>	0	-	%	Once
	NPU Macro5 BER	npu_macro5_crc_error_rate	Raw data	5	>	0	-	%	Once
	NPU Macro6 BER	npu_macro6_crc_error_rate	Raw data	5	>	0	-	%	Once
	NPU Macro7 BER	npu_macro7_crc_error_rate	Raw data	5	>	0	-	%	Once
	Maximum Duration of NPU Macro1 in Lane 0 Mode	npu_macro1_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Maximum Duration of NPU Macro2 in Lane 0 Mode	npu_macro2_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once
	Maximum Duration of NPU Macro3 in Lane 0 Mode	npu_macro3_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once
	Maximum Duration of NPU Macro4 in Lane 0 Mode	npu_macro4_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once
	Maximum Duration of NPU Macro5 in Lane 0 Mode	npu_macro5_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Maximum Duration of NPU Macro6 in Lane 0 Mode	npu_macro6_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once
	Maximum Duration of NPU Macro7 in Lane 0 Mode	npu_macro7_0lane_max_consec_sec	Raw data	1	>	-	5	s	Once
	Total Duration of NPU Macro1 in Lane 0 Mode	npu_macro1_0lane_total_sec	Raw data	1	>	-	20	s	Once
	Total Duration of NPU Macro2 in Lane 0 Mode	npu_macro2_0lane_total_sec	Raw data	1	>	-	20	s	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Total Duration of NPU Macro3 in Lane 0 Mode	npu_macro3_0lane_total_sec	Raw data	1	>	-	20	s	Once
	Total Duration of NPU Macro4 in Lane 0 Mode	npu_macro4_0lane_total_sec	Raw data	1	>	-	20	s	Once
	Total Duration of NPU Macro5 in Lane 0 Mode	npu_macro5_0lane_total_sec	Raw data	1	>	-	20	s	Once
	Total Duration of NPU Macro6 in Lane 0 Mode	npu_macro6_0lane_total_sec	Raw data	1	>	-	20	s	Once

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Total Duration of NPU Macro7 in Lane 0 Mode	npu_macro7_0lane_total_sec	Raw data	1	>	-	20	s	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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Namespace	Metric Name	Metric ID	Statistic	Consecutive Triggers	Operator	Major Alarm Threshold	Critical Alarm Threshold	Unit	Frequency
	Replication Lag	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

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

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

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

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	>	-	300000000	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

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

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

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

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

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

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

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

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

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

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

3 Cloud Eye Resource Group Configuration

3.1 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 from various suppliers, each system owner must handle alarms for their specific resources.

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 3-1 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.
	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.

Alarm Type	Configuration	Scenario	Remarks/Risk Point
	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 match by tag.	For details about these services, see **Cloud Services Supported by Resource Groups**.
	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.	-

3.2 Configuring Resource Groups for Metric Alarms

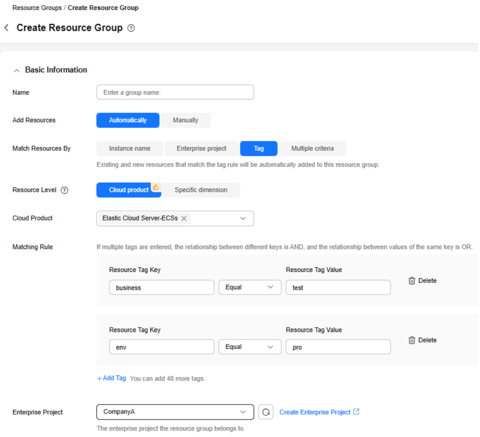
When creating a resource group, you are advised to set **Add Resources** to **Automatically**. Resource groups created with **Add Resources** set to **Automatically** can be updated dynamically. When you add resources that meet the required conditions, the system automatically adds the resources to the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

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 management 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 3-1 Matching resources by tag



Resource Groups / Create Resource Group

Create Resource Group

Basic Information

Name: Enter a group name.

Add Resources: ● Automatically ○ Manually

Match Resources By: ○ Instance name ○ Enterprise project ● Tag ○ Multiple criteria

Existing and new resources that match the tag rule will be automatically added to this resource group.

Resource Level: ● Cloud product ○ Specific dimension

Cloud Product: Elastic Cloud Server-ECSs

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

Resource Tag Key		Resource Tag Value	
business	Equal	test	Delete
env	Equal	pro	Delete

+Add Tag You can add 48 more tags.

Enterprise Project: CompanyA

Create Enterprise Project

The enterprise project the resource group belongs to.

Table 3-2 Parameters for 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 (-).

Parameter	Example Value	Description
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 **Resource Level** is set to **Cloud product**, you need to select a cloud product. If **Resource Level** is set to **Specific dimension**, all available resources in the selected dimensions will be automatically added to this resource group. For details, click **View Types of Resources That Can Be Added Automatically**.
Cloud Product	Elastic Cloud Server - ECSs	If **Resource Level** is set to **Cloud service**, you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If **Cloud Product** is set to **All**, all cloud products that are interconnected with Cloud Eye will be selected.

Parameter	Example Value	Description
Matching Rule	Tag 1: env=pro, Tag 2: business=xxx	Tag matching rule. You can add up to 50 tags. Key-value pairs that you can use to easily categorize and search for cloud resources. ● Resource 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: _.:=+-@ ● Resource tag value: A tag value consists of the matching method and value. The matching method can be set to **Equal**, **All**, **Include**, **Prefix**, **Suffix**, or **Not include**. The value can contain 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 that the resource group belongs to

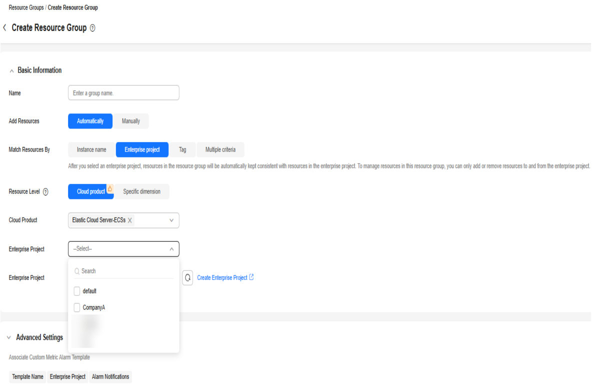
7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

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 management 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 3-2 Matching resources by enterprise project



Resource Groups / Create Resource Group

Create Resource Group

Basic Information

Name: Enter a group name.

Add Resources: Automatically | Manually

Match Resources By: Instance name | Enterprise project | Tag | Multiple criteria

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

Resource Level: Cloud product | Specific dimension

Cloud Product: Elastic Cloud Server-ECSs

Enterprise Project: --Select--

Enterprise Project

Table 3-3 Parameters for 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.
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If **Resource Level** is set to **Cloud product**, you need to select a cloud product. If **Resource Level** is set to **Specific dimension**, all available resources in the selected dimensions will be automatically added to this resource group. For details, click **View Types of Resources That Can Be Added Automatically**.

Parameter	Example Value	Description
Cloud Product	Elastic Cloud Server - ECSs	If **Resource Level** is set to **Cloud service**, you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If **Cloud Product** is set to **All**, all cloud products that are interconnected with Cloud Eye will be selected.
Enterprise Project	Enterprise project B	Enterprise project for matching resources. You can select multiple enterprise projects.
Enterprise Project	Enterprise Project A	Enterprise project that the resource group belongs to

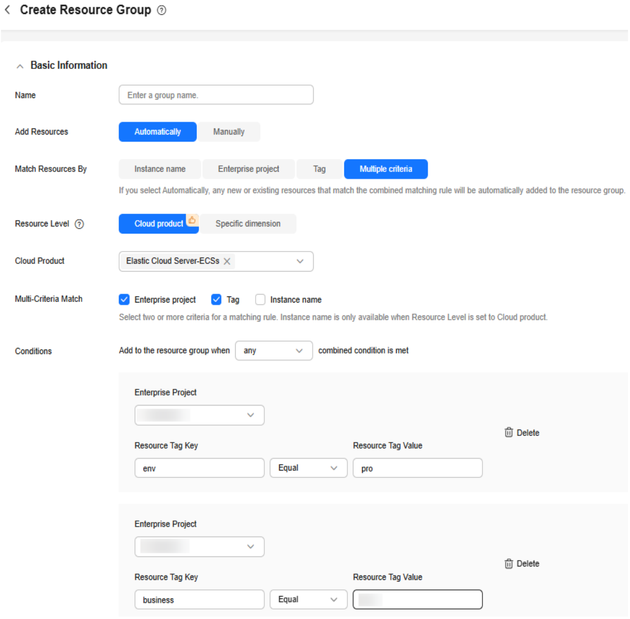
7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

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 management 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 3-3 Matching resources by multiple criteria



Create Resource Group

Basic Information

Name: Enter a group name.

Add Resources: [✓ Automatically] Manually

Match Resources By: Instance name Enterprise project Tag [✓ Multiple criteria]

If you select Automatically, any new or existing resources that match the combined matching rule will be automatically added to the resource group.

Resource Level: [✓ Cloud product] Specific dimension

Cloud Product: Elastic Cloud Server-ECSs

Multi-Criteria Match: ☑ Enterprise project ☑ Tag □ Instance name

Select two or more criteria for a matching rule. Instance name is only available when Resource Level is set to Cloud product.

Conditions: Add to the resource group when any combined condition is met

Enterprise Project: [redacted]
Resource Tag Key: env Equal Resource Tag Value: pro
Delete

Enterprise Project: [redacted]
Resource Tag Key: business Equal Resource Tag Value: [redacted]
Delete

Table 3-4 Parameters for 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 **Resource Level** is set to **Cloud product**, you need to select a cloud product. If **Resource Level** is set to **Specific dimension**, all available resources in the selected dimensions will be automatically added to this resource group. For details, click **View Types of Resources That Can Be Added Automatically**.

Parameter	Example Value	Description
Cloud Product	Elastic Cloud Server - ECSs	If **Resource Level** is set to **Cloud service**, you need to select the cloud service that the instance belongs to. You can select one or more cloud services. If **Cloud Product** is set to **All**, all cloud products that are interconnected with Cloud Eye will be selected.
Multi-Criteria Match	**Enterprise project** and **Tag** Combination method 1: env=pro,enterprise project B Combination method 2: business=xxx,enterprise project B	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 that the resource group belongs to

7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

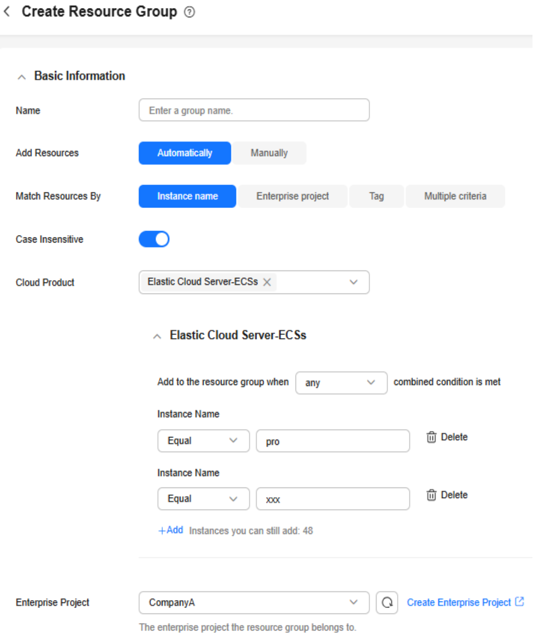
Creating a Resource Group by Matching Resources by Instance Name

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 management 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 3-4 Matching resources by instance name



Create Resource Group

Basic Information

Name: Enter a group name.

Add Resources: Automatically

Match Resources By: Instance name

Case Insensitive: on

Cloud Product: Elastic Cloud Server-ECSs

Elastic Cloud Server-ECSs

Add to the resource group when any combined condition is met

Instance Name: Equal pro

Instance Name: Equal xxx

Instances you can still add: 48

Enterprise Project: CompanyA

The enterprise project the resource group belongs to.

Table 3-5 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.

Parameter	Example Value	Description
Resource Level	Cloud product	Resource level of the monitored object. You can select **Cloud product** or **Specific dimension**. If **Resource Level** is set to **Cloud product**, you need to select a cloud product. If **Resource Level** is set to **Specific dimension**, all available resources in the selected dimensions will be automatically added to this resource group. For details, click **View Types of Resources That Can Be Added Automatically**.
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 that the resource group belongs to

7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

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 management 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.

Table 3-6 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 that the resource group belongs to

7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

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 management 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.

   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 3-7 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 that the resource group belongs to

7. In the **Advanced Settings** area, select an alarm template and configure alarm notifications to create an alarm rule. For details about parameters, see **(Optional) Advanced Configurations**.
8. Click **Create**.

3.3 Configuring Resource Groups for Event Alarms

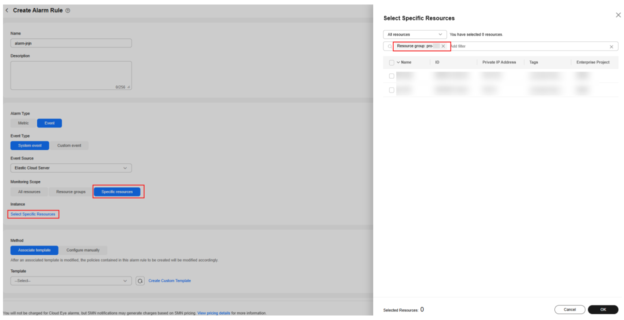
When configuring event alarm rules, you can only configure resource groups for DDS, RDS, DCS, and GeminiDB. In this case, you are advised to configure alarm rules by setting **Monitoring Scope** to **Specified resources** or **All resources**. When selecting **Specified resources**, you can select specified resources from existing resource groups for better efficiency.

Creating an Alarm Rule for Specified Resources

1. Log in to the management 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 3-5 Creating an alarm rule

   Create Alarm Rule

   Name: alarm-jnjn

   Description: 0/256

   Alarm Type: Metric | Event

   Event Type: System event | Custom event

   Event Source: Elastic Cloud Server

   Monitoring Scope: All resources | Resource groups | Specific resources

   Instance: Select Specific Resources

   Method: Associate template | Configure manually

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

   Template: --Select-- Create Custom Template

   You will not be charged for Cloud Eye alarms, but SMN notifications may generate charges based on SMN pricing. View pricing details for more information.

   Select Specific Resources

   All resources You have selected 0 resources.

   Resource group: pro- Add filter

Name	ID	Private IP Address	Tags	Enterprise Project

   Selected Resources: 0

6. Click **Create**.

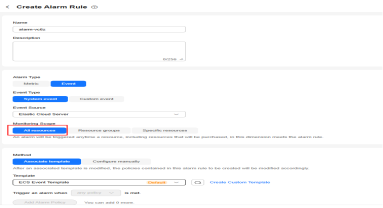
If the resources in a resource group change, you need to manually update the resources for the event alarm rule. For details, see **Modifying an Alarm Rule**.

Creating an Alarm Rule for All Resources

1. Log in to the management 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**.

   Figure 3-6 Creating an alarm rule

   Create Alarm Rule

   Name: alarm-vc6z

   Description: 0/256

   Alarm Type: Metric | Event

   Event Type: System event | Custom event

   Event Source: Elastic Cloud Server

   Monitoring Scope: All resources | Resource groups | Specific resources

   An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

   Method: Associate template | Configure manually

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

   Template: ECS Event Template Default Create Custom Template

   Trigger an alarm when any policy is met.

   Add Alarm Policy You can add 0 more.

6. Click **Create**.

4 Scenario-specific Cases

4.1 Service Monitoring on E-Commerce Platforms

4.1.1 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.

4.1.2 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.

Server Monitoring provides **Basic Monitoring** and **OS Monitoring** of different monitoring granularities. **Basic Monitoring** monitors metrics reported by ECSs. **OS Monitoring** provides server monitoring that is system-wide, active, and fine-grained 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 management 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 **Server Monitoring**.
5. Locate the target ECS. In the **Operation** column, click **More** and select **Create Alarm Rule**.
6. On the **Create Alarm Rule** page, set the alarm parameters as prompted. **Alarm Type**, **Cloud Product**, **Resource Level**, **Monitoring Scope**, and **Instance** are preset by default.

Table 4-1 Parameters for configuring an alarm rule for an ECS

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

7. Configure alarm notification parameters.

Table 4-2 Parameters for configuring alarm notifications

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Select an alarm notification mode.

Parameter	Example Value	Description
Recipient	Account contact	- If you select **Topic subscriptions** for **Notified By**, select one or more notification recipients. - If **Recipient** is set to **Account contact**, notifications will be sent to the registered phone 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, Cleared alarm	This parameter is available when **Notified By** is set to **Topic subscriptions** or **Notification groups**. You can select **Generated alarm**, **Cleared alarm**, or both.

After the alarm rule is created, once the service volume soars and the specified threshold is reached, Cloud Eye immediately informs you of the resource exception.

4.1.3 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.

Procedure

1. Log in to the management 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 **Cloud Service Monitoring** > **Elastic Load Balance**.
5. Locate the target load balancer and click **Create Alarm Rule** in the **Operation** column.

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

   NOTE

   > To create alarm rules for RDS and EIP and bandwidth metrics, choose **Relational Database Service** and **Elastic IP and Bandwidth**, respectively.

   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 set to trigger an alarm 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 Elastic IP and Bandwidth 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.

6. Click **Create**.

   If the service volume soars and the specified RDS, Elastic IP, and Bandwidth, or ELB threshold is reached, Cloud Eye immediately informs you of the resource exception.

4.1.4 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 management 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. Specify a name for the group.
7. Select a method for adding resources. For details about the parameters for creating a resource group, see **Creating a Resource Group**.
8. Click **Create**.

   After the group is created, you can view the resource usage, alarms, and health status of the group in **Resource Groups**.

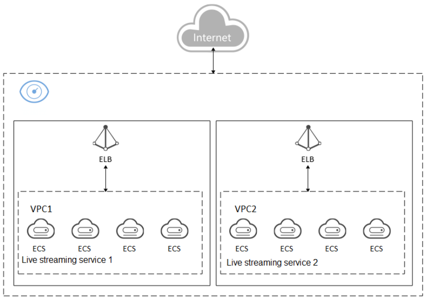
4.2 Live Streaming Monitoring

4.2.1 Overview

In the era of rapid Internet development, the demand for live video 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.

Figure 4-1 shows the typical architecture of live video streaming deployed on Huawei Cloud. Multiple ECSs, VPCs, and load balancers are used. ECSs are the basis of live video streaming, VPCs provide networks, and load balancers 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.

Figure 4-1 Service architecture of live streaming services



4.2.2 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.

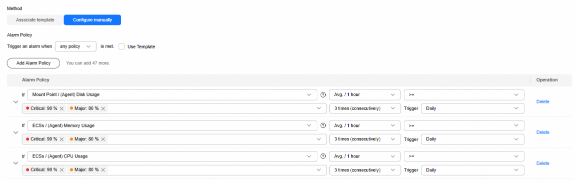
Creating an Alarm Rule

1. Log in to the management 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 **Server Monitoring** > **Elastic Cloud Server**.

5. Locate the target ECS. In the **Operation** column, choose **More** > **Create Alarm Rule**.

6. On the **Create Alarm Rule** page, set **Method** to **Configure manually** and configure alarm policies for the monitored instance.

Figure 4-2 Creating an alarm rule



Method: Associate template | **Configure manually**

Alarm Policy

Trigger an alarm when any policy is met. □ Use Template

Alarm Policy				Operation
If Mount Point / (Agent) Disk Usage	Avg. / 1 hour	>=		Delete
● Critical: 90 % ● Major: 80 %	3 times (consecutively)	Trigger	Daily	
If ECSs / (Agent) Memory Usage	Avg. / 1 hour	>=		Delete
● Critical: 90 % ● Major: 80 %	3 times (consecutively)	Trigger	Daily	
If ECSs / (Agent) CPU Usage	Avg. / 1 hour	>=		Delete
● Critical: 90 % ● Major: 80 %	3 times (consecutively)	Trigger	Daily	

Table 4-3 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.

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

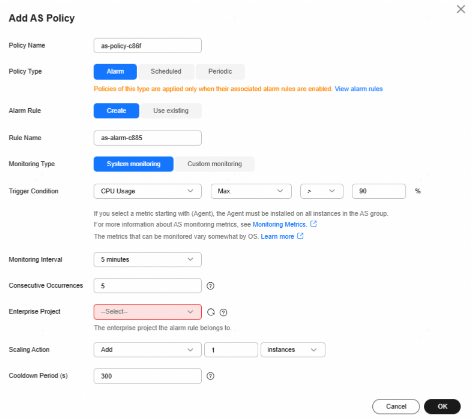
Table 4-4 Parameters for configuring alarm notifications

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Select an alarm notification mode.
Recipient	Account contact	● If you select **Topic subscriptions** for **Notified By**, select one or more notification recipients. ● If **Recipient** is set to **Account contact**, notifications will be sent to the registered phone 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, Cleared alarm	This parameter is available when **Notified By** is set to **Topic subscriptions** or **Notification groups**. You can select **Generated alarm**, **Cleared alarm**, or both.

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 4-3**.

Figure 4-3 Adding an AS policy



Add AS Policy

Policy Name: as-policy-c86f

Policy Type: Alarm

Policies of this type are applied only when their associated alarm rules are enabled. View alarm rules

Alarm Rule: Create

Rule Name: as-alarm-c885

Monitoring Type: System monitoring

Trigger Condition: CPU Usage Max. > 90 %

If you select a metric starting with (Agent), the Agent must be installed on all instances in the AS group.
For more information about AS monitoring metrics, see Monitoring Metrics.
The metrics that can be monitored vary somewhat by OS. Learn more

Monitoring Interval: 5 minutes

Consecutive Occurrences: 5

Enterprise Project: --Select--

The enterprise project the alarm rule belongs to.

Scaling Action: Add 1 instances

Cooldown Period (s): 300

4.2.3 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.

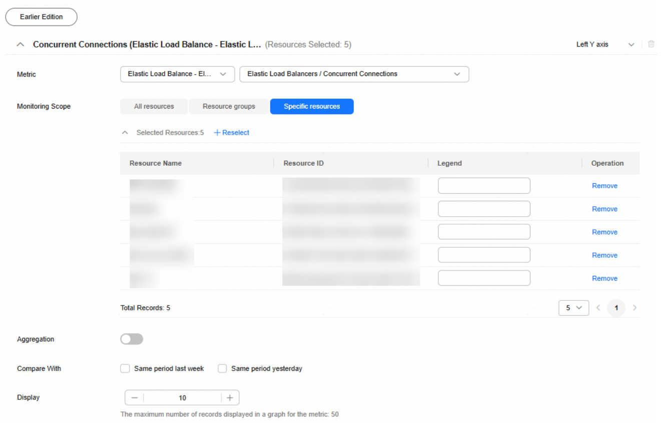
Stable and reliable load balancing is critical to the proper running of live video streaming. Cloud Eye can monitor unhealthy backend servers and concurrent connections of load balancers to ensure proper running of your services.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane, click **My Dashboards** > **Custom Dashboards**.
5. Locate the dashboard for which you want to add a graph and click its name.
6. 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 4-4 Adding a graph



Concurrent Connections (Elastic Load Balance - Elastic L... (Resources Selected: 5)

Metric: Elastic Load Balance - El... | Elastic Load Balancers / Concurrent Connections

Monitoring Scope: Specific resources

Selected Resources:5

Resource Name	Resource ID	Legend	Operation
[redacted]	[redacted]		Remove
[redacted]	[redacted]		Remove
[redacted]	[redacted]		Remove
[redacted]	[redacted]		Remove
[redacted]	[redacted]		Remove

Total Records: 5 5 < 1 >

Aggregation

Compare With □ Same period last week □ Same period yesterday

Display − 10 +

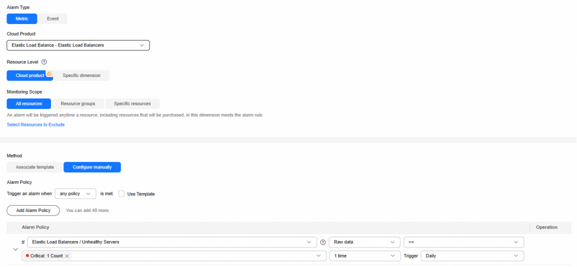
The maximum number of records displayed in a graph for the metric: 50

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.

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

Figure 4-5 Creating an alarm rule



Alarm Type: Metric

Cloud Product: Elastic Load Balance - Elastic Load Balancers

Resource Level: Cloud product

Monitoring Scope: All resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Method: Configure manually

Alarm Policy

Trigger an alarm when any policy is met. □ Use Template

You can add 49 more.

Alarm Policy	Operation
If Elastic Load Balancers / Unhealthy Servers, Raw data, >= Critical: 1 Count, 1 time, Trigger Daily	

Table 4-5 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.

Table 4-6 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 **Notification groups** or **Topic subscriptions**, select **Generated alarm**, **Cleared alarm**, or both for this parameter.

10. Click **Create**.

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

4.2.4 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.

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

Procedure

1. Log in to the management 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 **Cloud Service Monitoring**.
5. On the displayed page, click the VPC dashboard name.
6. Locate the row that contains the target VPC and choose **More** > **Create Alarm Rule** in the **Operation** column.
7. 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 4-7 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.

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

Table 4-8 Parameters for configuring alarm notifications

Parameter	Example Value	Description
Alarm Notifications	Enabled	Whether to send an alarm notification when an alarm is triggered.
Notified By	Topic subscriptions	Select an alarm notification mode.
Recipient	Account contact	● If you select **Topic subscriptions** for **Notified By**, select one or more notification recipients. ● If **Recipient** is set to **Account contact**, notifications will be sent to the registered phone 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, Cleared alarm	This parameter is available when **Notified By** is set to **Topic subscriptions** or **Notification groups**. You can select **Generated alarm**, **Cleared alarm**, or both.

9. Click **Create**.

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

4.3 Crowdsourcing Platforms

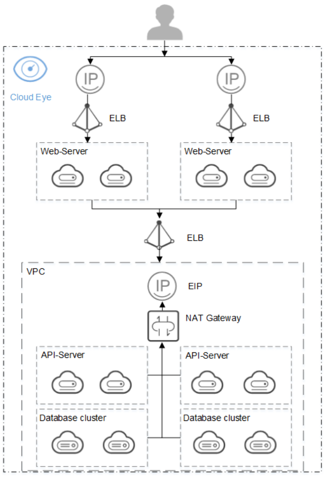
4.3.1 Overview

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.

Figure 4-6 shows the typical architecture of the crowdsourcing platform deployed on Huawei Cloud. The core databases use the BMS clusters to deploy the database clusters. Web-Servers and API-Servers are deployed on ECSs. Web-Servers provide website search, category, store, and transaction services, and API-Servers are basic interfaces for connecting services with 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 **4.3.2 Server Monitoring** and **4.3.4 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 the cloud service monitoring function to monitor the running status of each service system at any time. For details, see **4.3.3 Network Monitoring**.

Figure 4-6 Crowdsourcing platform architecture



4.3.2 Server Monitoring

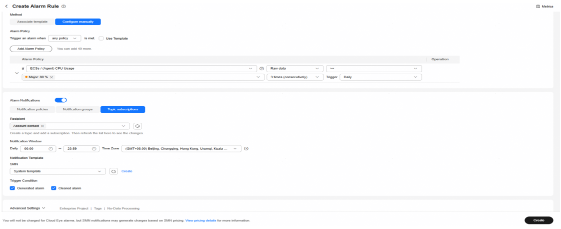
On crowdsourcing platforms, ECSs provide computing resources, and databases are deployed on BMSs. Therefore, BMS disk read and write rates affect the database operation speed. ECS memory and CPU usages affect the service execution speed. To monitor more fine-grained metrics, you can **install and configure 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 management 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 **Server Monitoring** > **Elastic Cloud Server**.
5. Locate the target ECS. In the **Operation** column, choose **More** > **Create Alarm Rule**.
6. 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 4-7 Creating an alarm rule



Create Alarm Rule

Metrics

Method: Associate template | Configure manually

Alarm Policy

Trigger an alarm when any policy is met. ☐ Use Template

Add Alarm Policy You can add 49 more.

Alarm Policy				Operation
If ECSs / (Agent) CPU Usage	Raw data	>=		
Major: 80 %	3 times (consecutively)	Trigger	Daily	

Alarm Notifications

Notification policies | Notification groups | Topic subscriptions

Recipient: Account contact

Create a topic and add a subscription. Then refresh the list here to see the changes.

Notification Window: Daily 00:00 – 23:59 Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala ...

Notification Template

SMN: System template Create

Trigger Condition: ☑ Generated alarm ☑ Cleared alarm

Advanced Settings Enterprise Project | Tags | No-Data Processing

You will not be charged for Cloud Eye alarms, but SMN notifications may generate charges based on SMN pricing. View pricing details for more information.

Create

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.

4.3.3 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.

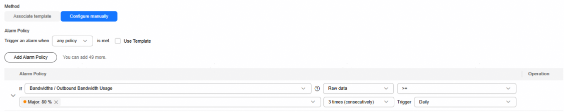
In addition, if the number of connections increases sharply due to DDoS attacks or heavy traffic, service access becomes slow. The number of SNAT connections on days with activities is expected to be two to three times higher. Therefore, you need to monitor the number of SNAT connections at any time.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. Choose **Cloud Service Monitoring**.
5. 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 4-8**.

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

      Figure 4-8 Creating an alarm rule (for a VPC)

      Method: Associate template | Configure manually

      Alarm Policy

      Trigger an alarm when any policy is met. ☐ Use Template

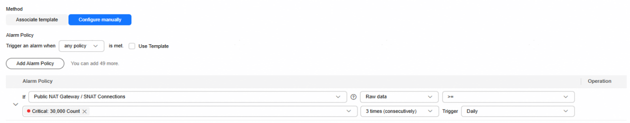
      Add Alarm Policy You can add 49 more.

Alarm Policy				Operation
If Bandwidths / Outbound Bandwidth Usage	Raw data	>=		
Major: 80 %	3 times (consecutively)	Trigger	Daily	

   c. Click **Create**.
6. 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 4-9**.

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 4-9 Creating an alarm rule (for a NAT gateway)



Method: Configure manually

Alarm Policy

Trigger an alarm when any policy is met. □ Use Template

Alarm Policy	Operation
If Public NAT Gateway / SNAT Connections · Raw data · >= · Critical: 30,000 Count · 3 times (consecutively) · Trigger Daily	

c. Click **Create**.

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

4.3.4 Event Monitoring

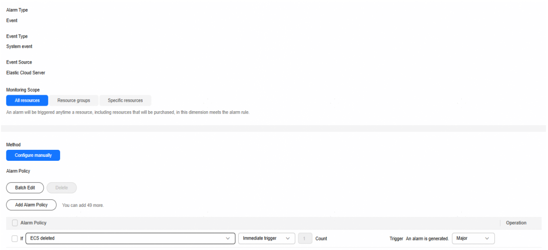
During service running, you can delete, reboot, or stop ECSs and BMSs, and delete NICs or security group rules for the ECSs and BMSs at any time as required. You can use the event monitoring function to monitor the running status of ECSs and BMSs at any time.

Procedure

1. Log in to the management 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**. 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 4-10 Creating an alarm rule



Alarm Type
Event

Event Type
System event

Event Source
Elastic Cloud Server

Monitoring Scope: All resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Method: Configure manually

Alarm Policy

□ Alarm Policy	Operation
□ If ECS deleted · Immediate trigger · 1 Count · Trigger An alarm is generated. Major	

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

4.4 Best Practices of Event Monitoring

4.4.1 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 the applications that run on the ECS.

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.

Table 4-9 Key ECS events

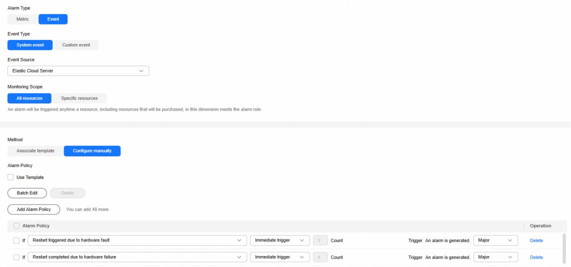
Event Name	Event Description	Handling Method
Restart triggered due to hardware fault	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs were restarted and Cloud Eye sent an event Restart triggered due to hardware fault. After the migration is complete, Cloud Eye sent an event Restart completed due to hardware failure.	This event indicates that a fault has occurred and the ECS cannot be used. In this case, you need to replace the ECS or direct traffic to other ECSs.
Restart completed due to hardware failure		This event indicates that the ECS is working properly and can be used again.

Procedure

1. Log in to the management 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**. 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 4-11 Creating an alarm rule



Alarm Type: Metric | **Event**

Event Type: **System event** | Custom event

Event Source: Elastic Cloud Server

Monitoring Scope: **All resources** | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Method: Associate template | **Configure manually**

Alarm Policy

□ Use Template

Batch Edit | Delete

Add Alarm Policy You can add 48 more.

□ Alarm Policy						Operation
□ If	Restart triggered due to hardware fault	Immediate trigger	1	Count	Trigger An alarm is generated. Major	Delete
□ If	Restart completed due to hardware failure	Immediate trigger	1	Count	Trigger An alarm is generated. Major	Delete

5. Click **Create**.

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

4.4.2 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 4-10 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.

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.

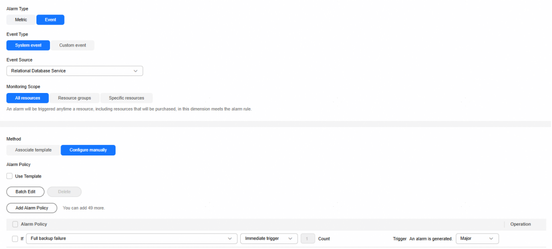
Event Name	Event Description	Handling Method
DB instance recovered	RDS uses high availability tools to rebuild the standby DB instance for disaster recovery.	No action is required.

Procedure

1. Log in to the management 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**. 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 4-12 Creating an alarm rule

   Alarm Type: Metric / **Event**
   Event Type: **System event** / Custom event
   Event Source: Relational Database Service
   Monitoring Scope: **All resources** / Resource groups / Specific resources
   An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

   Method: Associate template / **Configure manually**
   Alarm Policy
   □ Use Template
   Batch Edit | Delete
   Add Alarm Policy — You can add 49 more.

□ Alarm Policy	Operation
□ If Full backup failure, Immediate trigger, 1 Count, Trigger An alarm is generated. Major	

5. Click **Create**.

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

4.4.3 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.

Table 4-11 Key EIP events

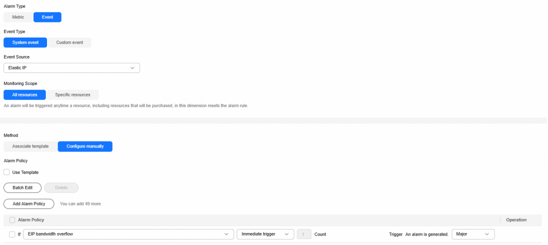
Event Name	Event Description	Handling Method
EIP bandwidth overflow	If this event is reported, the bandwidth exceeds the purchased bandwidth, which may slow down the network or cause packet loss. **NOTE** This event is available only in certain regions. You can check the regions on the console.	Check 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 management 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**. 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 4-13 Creating an alarm rule

   Alarm Type: Metric / [✓ Event]

   Event Type: [✓ System event] / Custom event

   Event Source: Elastic IP

   Monitoring Scope: [✓ All resources] / Specific resources

   An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

   Method: Associate template / [✓ Configure manually]

   Alarm Policy

   □ Use Template

   Batch Edit Delete

   Add Alarm Policy You can add 49 more.

□ Alarm Policy	Operation
□ If EIP bandwidth overflow Immediate trigger 1 Count Trigger An alarm is generated. Major	

5. Click **Create**.

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

4.5 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 4-12 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

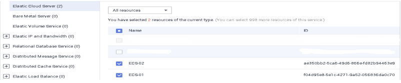
Prerequisites

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 management 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. Enter the group name as prompted. In this example, enter **Development-group-resources**.
7. Select the target cloud service resources.

Figure 4-14 Selecting cloud service resources



Elastic Cloud Server (2)
Bare Metal Server (0)
Elastic Volume Service (0)
Elastic IP and Bandwidth (0)
Relational Database Service (0)
Distributed Message Service (0)
Distributed Cache Service (0)
Elastic Load Balance (0)

All resources

You have selected 2 resources of the current type. (You can select 998 more resources of this service.)

	Name	ID
□		
□		
☑	ECS-02	ae350bb2-5ca6-49d6-866e-fd82b94463e9
☑	ECS-01	f04d95e8-5e1c-4271-9a52-056836da0c70

8. Click **Create**.

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.

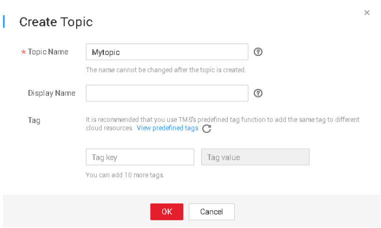
1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Application**, select **Simple Message Notification**.

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

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

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

Figure 4-15 Creating a topic



Create Topic

* Topic Name: Mytopic

The name cannot be changed after the topic is created.

Display Name:

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

Tag key | Tag value

You can add 10 more tags.

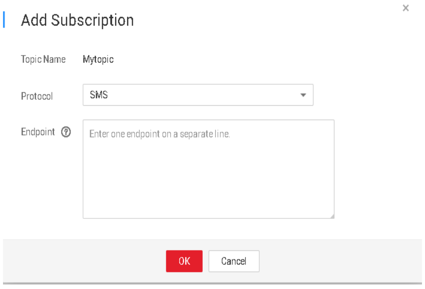
6. Enter a topic name and display name.
7. Click **OK.**

   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.
8. In the topic list, locate the new topic. In the **Operation** column, click **More** and select **Add Subscription**.

Figure 4-16 Adding a subscription



Add Subscription

Topic Name: Mytopic

Protocol: SMS

Endpoint: Enter one endpoint on a separate line

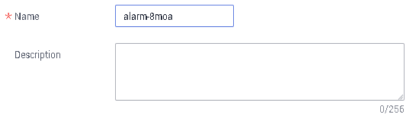
9. Specify the subscription protocol and endpoints.
10. Click **OK**.

    The subscriptions you added are displayed in the subscription list.

Step 3 Creating an Alarm Rule

1. Log in to the management 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 **Alarm Management** > **Alarm Rules**.
5. In the upper right corner, click **Create Alarm Rule**.
6. On the **Create Alarm Rule** page, follow the prompts to set the parameters.
   a. Set the alarm rule name.

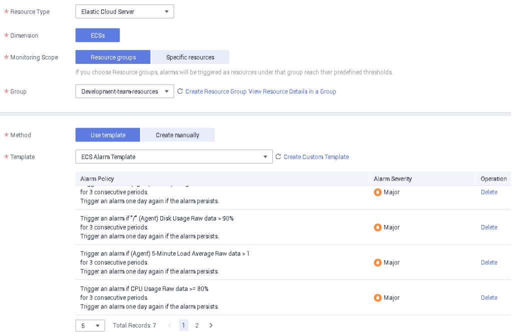
Figure 4-17 Setting an alarm rule name



* Name	alarm-8moa
Description	0/256

   b. Set the monitored object and alarm triggering conditions.

Figure 4-18 Configuring an alarm rule



* Resource Type	Elastic Cloud Server
* Dimension	ECSs
* Monitoring Scope	Resource groups
* Group	Development-team-resources
* Method	Use template
* Template	ECS Alarm Template

If you choose Resource groups, alarms will be triggered as resources under that group reach their predefined thresholds.

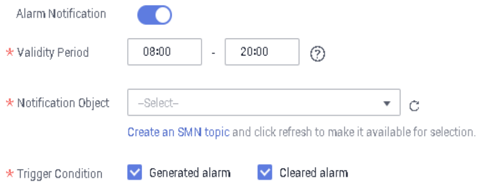
Alarm Policy	Alarm Severity	Operation
for 3 consecutive periods. Trigger an alarm one day again if the alarm persists.	Major	Delete
Trigger an alarm if "/" (Agent) Disk Usage Raw data > 90% for 3 consecutive periods. Trigger an alarm one day again if the alarm persists.	Major	Delete
Trigger an alarm if (Agent) 5-Minute Load Average Raw data > 1 for 3 consecutive periods. Trigger an alarm one day again if the alarm persists.	Major	Delete
Trigger an alarm if CPU Usage Raw data >= 80% for 3 consecutive periods. Trigger an alarm one day again if the alarm persists.	Major	Delete

NOTE

Set **Group** to **Development-group-resources** created in **Step 1 Creating a Resource Group**.

   c. Set **Alarm Notification** parameters.

Figure 4-19 Configuring alarm notifications



Alarm Notification	on
* Validity Period	08:00 - 20:00
* Notification Object	--Select--
* Trigger Condition	☑ Generated alarm ☑ Cleared alarm

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

NOTE

- Note: When configuring **Notification Object**, select **Mytopic** created in **Step 2 Creating a Topic and Configuring the Notification Object**.

d. 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.

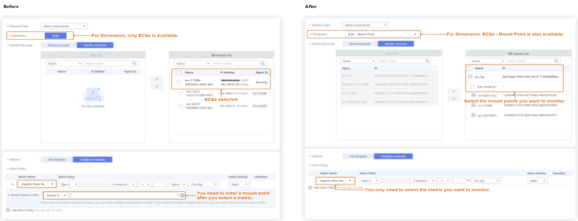
4.6 Configuring an Alarm Rule for the Disk Usage of All Mount Points on an ECS

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 mount point dimension is added to metric disk usage. 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.

Figure 4-20 Alarm rule configuration before and after optimization


Before
After
For Dimension, only ECSs is available.
ECSs selected
You need to enter a mount point after you select a metric.
For Dimension, ECSs - Mount Point is also available.
Select the mount points you want to monitor.
You only need to select the metric you want to monitor.

Prerequisites

The Agent has been installed on the ECS.

Procedure

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane, choose **Alarm Management** > **Alarm Rules**, and click **Create Alarm Rule** in the upper right corner.
4. 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**.

5. If you want to receive alarm notifications, enable **Alarm Notification** and select the notification object and method.

5 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.

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 records management traces of Cloud Eye for auditing. For details about Cloud Eye operations recorded by CTS, see **Key Cloud Eye Operations**.