

AOM

Best Practices

Issue 01
Date 2023-01-03



Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Contents

| | |
|---|-----------|
| 1 Threshold Alarms (Old) | 1 |
| 2 Threshold Alarms (New) | 4 |
| 3 Discovering Applications | 9 |
| 4 Counting Log Keywords | 13 |

1 Threshold Alarms (Old)

This function is available in AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

Alarm is a basic function of AOM and plays an important role in routine O&M. AOM can interconnect with dozens of VM and component metrics, and notify customers of system problems by SMS message or email.

Supported Metrics

AOM allows you to set threshold alarms for the following types of metrics:

| Category | Example |
|-----------------------------------|---|
| Component (process) | Total CPU cores, used CPU cores, and CPU usage |
| Host network metrics | Receive rate (BPS), receive error packet rate, send error packet rate, and total rate (BPS) |
| Host disk and file system metrics | Disk read rate, disk write rate, and disk usage |
| Host metrics | Total CPU cores, physical memory usage, host status, and NTP offset |
| Application performance metrics | Average latency, error calls, and throughput |

For more information, see [Metric Overview](#) in *AOM Service Overview*.

Procedure

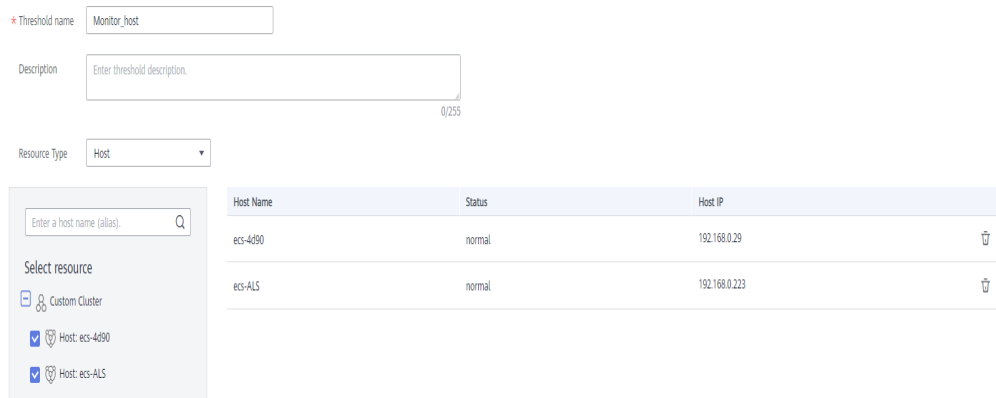
- Step 1** Log in to the AOM console. In the navigation pane, choose **Alarm Center > Alarm Rule**. Then, click **Add Threshold** in the upper right corner.

Step 2 Select resources: Enter a threshold name, select a resource type, select the resources to be monitored from the resource tree, and click **Next**.

NOTE

- You can select a maximum of 100 resources from the resource tree.
- When multiple resources are selected, multiple single-resource static threshold rules will be created after the creation is complete. Each resource is monitored by a single-resource static threshold rule. A rule name consists of the threshold rule name you enter in the **Threshold name** text box, and a sequence number ranging from 0 to 9. The resource which is selected earlier has a smaller number.

Figure 1-1 Selecting resources

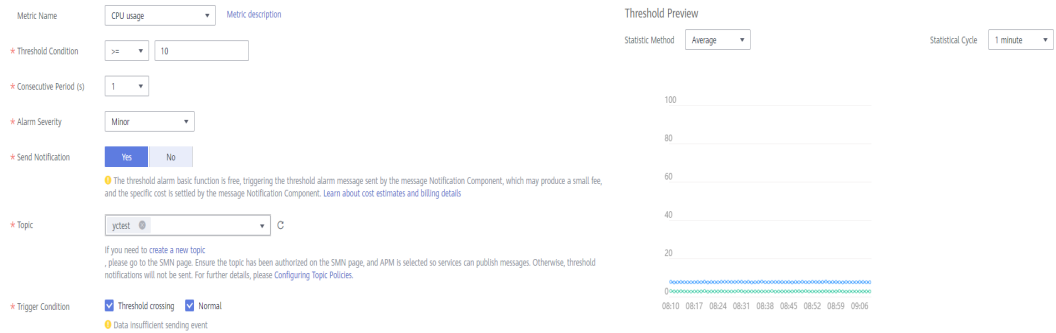


Step 3 Customize a threshold: Select the metric to be monitored, and set parameters such as **Threshold Condition**, **Consecutive Period (s)**, **Alarm Severity**, **Statistic Method**, and **Send Notification**.

NOTE

- **Threshold Condition:** Trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (\geq , \leq , $>$, or $<$) and threshold value. For example, if **Threshold Condition** is set to > 85 and an actual metric value exceeds 85, a threshold alarm will be generated.
- **Consecutive Period (s):** If the metric value meets the threshold condition for a specified number of consecutive periods, a threshold alarm will be generated.
- **Statistic Method:** Method used to measure metrics.
- **Statistical Cycle:** Interval at which metric data is collected.
- **Send Notification:** Whether to send notifications by email or SMS message when the static threshold rule status (**Exceeded**, **OK**, or **Insufficient**) changes.
 - If you want to receive notifications by email or SMS message, select **Yes**, set a notification policy, select a created topic, and select a trigger condition.
 - If you do not need to receive notifications by email or SMS message, select **No**.
- **Trigger Condition:** Condition for sending a notification. You can select multiple trigger conditions. For example, to receive notifications if the threshold status changes to **Exceeded**, select **Threshold crossing**. To receive notifications upon any threshold status change, select all trigger conditions.

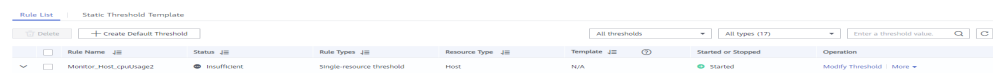
Figure 1-2 Customizing a threshold



Step 4 Click **Submit** to create multiple single-resource static threshold rules. Each resource is monitored by an independent rule.

If a single-resource static threshold rule monitors a host and the CPU usage of the host exceeds the threshold, a threshold alarm will be generated on the alarm page. You can choose **Alarm Center > Alarm List** in the navigation pane and view the alarm in the alarm list. If any host meets the preset notification policy, an email or SMS message will be sent.

Figure 1-3 Creating a single-resource static threshold rule



----End

2 Threshold Alarms (New)

This function is available in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, CN South-Shenzhen, CN South-Guangzhou-InvitationOnly, CN North-Ulanqab1, AP-Bangkok, and AP-Singapore.

Alarm is a basic function of AOM and plays an important role in routine O&M. AOM can interconnect with dozens of VM and component metrics, and notify customers of system problems by SMS message or email.

Supported Metrics

AOM allows you to set threshold rules for metrics of various resources such as hosts and components. You can view the supported metric types on the threshold rule creation page.

For more information about metrics, see [Metric Overview](#).

Creation Methods

You can **customize threshold rules** or **use templates to create threshold rules**. Only one rule is generated at a time. All resources are monitored using the same rule.

To use the second method to create a static threshold rule, ensure that a static threshold template has been created.

You are advised to customize threshold rules.

Customizing a Threshold Rule

Step 1 Log in to the AOM console. In the navigation pane, choose **Alarm Center > Alarm Rules**. Then, click **Add Alarm** in the upper right corner.

Step 2 Customize a threshold rule.

1. Set basic information such as the rule name and description.

Figure 2-1 Setting basic information

Basic Information


* Rule Name

Description

0/1000


2. Set rule details.
 - a. Set **Rule Type** to **Threshold alarm**.
 - b. Select monitored objects. Use either of the following methods:
 - Select resource objects: Click **Select Resource Object**, add objects by dimension or resource, and click **Confirm**.

 **NOTE**


- A threshold rule can monitor up to 100 pieces of metric data.
- If you enable **Apply to All** () when selecting objects to monitor, an alarm rule will be created for all metrics of the type you select under an application or service. For example, if you select **CCE/Host/Host/CPU Usage** and enable **Apply to All**, an alarm rule will be created for all hosts in CCE.
- Click **Edit resource objects** to modify the selected resource object.

- Command input: Both manual and auto inputs are supported.
 - Manual input: used when you know the metric name and IP address, and you are familiar with the Prometheus format. For example, to query the CPU usage of the host, run the `avg(label_replace(avg_over_time(aom_node_cpu_usage{hostID="81010a40-1682-41c1-9645-f0588ff9c0cf",nodeIP="192.168.1.210",clusterId='00000000-0000-0000-0000-00000000'}[59999ms]), "__name__","aom_node_cpu_usage","", "")) by(__name__,hostID,nodeIP)` command.

 **NOTE**

For details about Prometheus commands, move the cursor to  next to the search box and click [Learn more](#).

- Auto input: used when you do not know the metric information or are unfamiliar with the Prometheus format. The command can only be automatically filled when you switch from the **Metric Monitoring** page. Specifically, choose **Monitoring > Metric Monitoring** in the navigation pane. Then, click **Add Metric** and select **Dimension** or **Resource** for **Add By**. Select up to 12 metrics to monitor.

Next, click  in the **Operation** column. The system automatically switches to the threshold rule creation page and fills the Prometheus command for your metric.

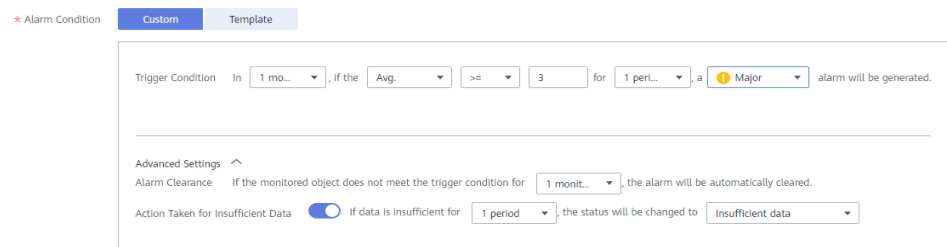
- c. Set an alarm condition. Click **Custom** and set information such as statistical periods, consecutive periods, and threshold condition. [Table 2-1](#) describes the parameters.

Table 2-1 Alarm condition parameters

| Category | Parameter | Description |
|-------------------|---------------------|--|
| Trigger Condition | Statistical Period | Interval at which metric data is collected. By default, only one period is measured. A maximum of five periods can be measured. |
| | Consecutive Periods | When the metric value meets the threshold condition for a specified number of consecutive periods, a threshold-crossing alarm will be generated. |
| | Statistic | Method used to measure metrics. Options: Avg., Min., Max., Sum, and Samples. |
| | Threshold Condition | Trigger condition of a threshold alarm. A threshold condition consists of two parts: operators (\geq , \leq , $>$, and $<$) and threshold value. For example, after Threshold Condition is set to > 85 , if the actual metric value exceeds 85, a threshold alarm is generated. Move the cursor to the graph area above the alarm condition. The ID, IP address, and unit of the current metric are displayed. |
| | Alarm Severity | Severity of a threshold alarm. Options: Critical, Major, Minor, and Warning. |
| Advanced Settings | Alarm Clearance | An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods. |

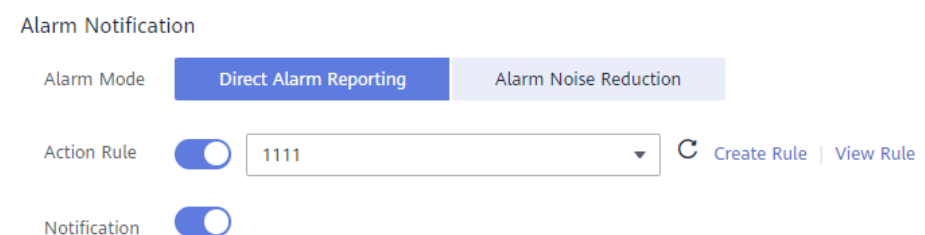
| Category | Parameter | Description |
|----------|------------------------------------|---|
| | Action Taken for Insufficient Data | <p>Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can configure this option based on your requirements.</p> <p>By default, metrics in only one period are monitored. You can set up to five monitoring periods.</p> <p>Options: Alarm, Insufficient data, Keep previous status, and Normal.</p> |

Figure 2-2 Setting an alarm condition



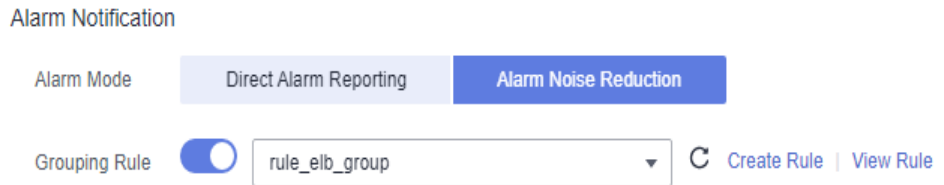
- d. Set alarm tags and annotations to group alarms. They can be associated with alarm noise reduction policies for sending notifications.
Click **Add Tag** or **Add Annotation**.
- 3. Set an alarm notification policy. There are two alarm notification modes.
 - **Direct Alarm Reporting:** An alarm is directly sent when the alarm condition is met.
 - i. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Creating an Alarm Action Rule](#).
 - ii. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in [Advanced Settings > Alarm Clearance](#) is met, alarm clearance notifications are sent based on the selected action rule.

Figure 2-3 Selecting the direct alarm reporting mode



- **Alarm Noise Reduction:** Alarms are sent only after being processed based on alarm action rules, preventing alarm storms.
Select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Grouping Rules](#).

Figure 2-4 Selecting the alarm noise reduction mode



Step 3 Click **Create Now** to complete the creation. As shown in the following figure, a threshold rule is created. Click to monitor the same metric of multiple resources.

In the expanded list, if the metric data of a host meets the preset alarm condition, a threshold alarm is generated on the alarm page. To view the alarm, go to the AOM console and choose **Alarm Center** > **Alarm List** in the navigation pane. If a host meets the preset notification policy, the system sends an alarm notification to the specified personnel by WeCom, email, or SMS.

Figure 2-5 Creating threshold rules

| Alarm Name | Status | Rule Type | Resource Type | Template | Started or Stopped | Operation |
|-------------|--------|--------------------------------|---------------|----------|--------------------|------------------------|
| Host_CPU_ph | Normal | Multi-resource threshold rules | Host | N/A | Started | Modify Delete More |

| Name | Status | Cluster Name | Physical memory usage (%) | Status Change Description |
|---------------|----------|--------------|---------------------------|---|
| 192.168.0.204 | Exceeded | -- | 37.1 | Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 37.1 Status Update: from "L..." |
| 10.2.0.99 | Exceeded | -- | 28.3 | Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 28.3 Status Update: from "L..." |
| 172.16.10.177 | Exceeded | -- | 31.2 | Time: 2022-03-08 11:15:33 GMT+08:00 Threshold Condition: >=10 Latest Value: 31.2 Status Update: from "L..." |

----End

3 Discovering Applications

Overview

AOM can discover applications deployed on hosts and collects their metrics based on preset rules. The discovered applications and their metric data will be displayed on the **Application Monitoring** and **O&M** pages.

The relationship between applications and components is as follows:

- Component refers to the smallest unit for completing a task. It can be a microservice, container process, or common process.
- Application refers to a complete service module and consists of multiple components.

After application discovery is configured, you can use AOM to monitor application metrics and associate related alarms. Mainly, AOM can:

1. Provide association relationships between applications and components, between components and component instances, and between applications and hosts.
2. Enable you to search for associated components and logs.
3. Aggregate component metrics (so that you can obtain aggregated results of all component instances).

Configuring Application Discovery Rules

Step 1 In the navigation pane, choose **Configuration Management > Application Discovery**.

Step 2 Click **Add Custom Application Discovery Rule** and configure an application discovery rule.

Step 3 Select a host for pre-detection.

1. Customize a rule name, for example, **rule-test**.
2. Select a typical host, for example, **host-test**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in **Step 6**. Then, click **Next**.

Step 4 Set an application discovery rule.

1. Click **Add Check Items**. AOM can discover processes that meet the conditions of check items.

For example, AOM can detect the processes whose command parameters contain **ovs-vswitchd unix:** and environment variables contain **SUDO_USER=paas**.

 **NOTE**

- To precisely detect processes, you are advised to add check items about unique features of the processes.
 - You must add at least one check item and can add up to five check items. If there are multiple check items, AOM only discovers the processes that meet the conditions of all check items.
2. After adding check items, click **Detect** to search for the processes that meet the conditions.
If no process is detected within 20s, modify the discovery rule and detect processes again. Only when at least one process is detected can you proceed to the next step.

Step 5 Set an application name and component name.

Set an application name.

1. Set an application name.

In the **Application Name Settings** area, click **Add Naming Rule** to set an application name for the detected process.


 **NOTE**

- If you do not set an application name, the default name **unknownapplicationname** is used.
 - When you add multiple naming rules, all the naming rules are combined as the application name of the process. Metrics of the same application are aggregated.
2. Set a component name.

In the **Component Name Settings** area, specify an application type and click **Add Naming Rule** to set a component name for the discovered process. For example, add the text **app-test** as a component name.

 **NOTE**

- Application types are specified to identify application categories. They are used only for better rule classification and console display. You can enter any field. For example, you can enter **Java** or **Python** to categorize applications by technology stack or enter **collector** or **database** to categorize applications by function.
 - If you do not set a component name, the default name **unknownapplicationname** is used.
 - When you add multiple naming rules, all the naming rules are combined as the component name of the process. Metrics of the same component are aggregated.
3. Preview the component name.

If the name does not meet your requirements, click  in the **Preview Component Name** table to rename the component.

Step 6 Set a priority and detection range.

1. Set a priority: When there are multiple rules, set priorities. Enter 1 to 9999. A smaller value indicates a higher priority. For example, **1** indicates the highest priority and **9999** indicates the lowest priority.
2. Set a detection range: Select a host to be detected. That is, select the host to which the configured rule is applied. If no host is selected, this rule will be executed on all hosts, including hosts added later.

Step 7 Click **Add** to complete the configuration. AOM collects metrics of the process.

Step 8 After about two minutes, choose **Monitoring > Component Monitoring** in the navigation pane, select the target host from the cluster drop-down list, and find out the monitored component.

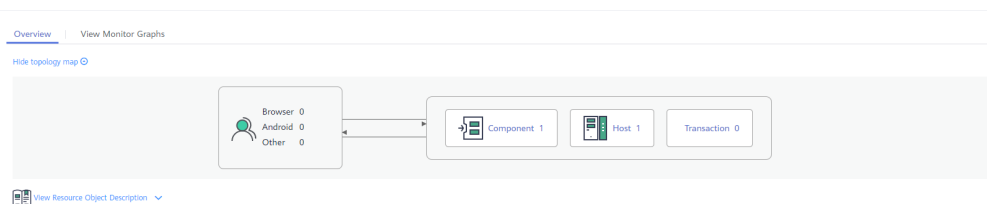
----End

Viewing the Application Status

Step 1 In the navigation pane, choose **Monitoring > Application Monitoring**.

Step 2 Click an application to view its components and other resources.

Figure 3-1 Viewing the application status



Step 3 Click the **Component List** tab and view the component information.

Figure 3-2 Viewing components

| Component Name | Status | CPU Usage | Physical Memory Usage |
|----------------|--------|-----------|-----------------------|
| common-tomcat | Normal | 0% | 7.071% |

Step 4 Click the **Host List** tab to view the host information.

Figure 3-3 Viewing hosts

| Host Name | Host IP Address | Host Status | CPU Usage | Physical Memory Usage |
|-----------|-----------------|-------------|-----------|-----------------------|
| centos | 192.168.1.57 | Normal | 0.9% | 49.1% |

- Step 5** Click the **Alarm Analysis** tab to view alarms.
----End

4 Counting Log Keywords

Scenario

When an application is normal, its log file contains fewer than 10 error keywords every 10 minutes. However, when the application becomes abnormal, the number of error keywords increases rapidly. To identify an exception in a timely manner, you can use AOM to count the number of errors in logs and set threshold rules.

Procedure

Step 1 Log in to the AOM console. In the navigation pane, choose **Log > Statistical Rules** and click **Create Statistical Rule**.

Step 2 Create a statistical rule for the log bucket and set the keyword **error**.

Basic Information

* Rule Type

* Rule Name

* Keyword ?

Description

* Log Bucket [Add Log Bucket](#)

Step 3 Create a threshold rule for the statistical rule and set the trigger condition as follows: if the number of errors is greater than 12 within 5 minutes, an alarm will be reported.

Threshold Settings

- * Threshold Name: alert-erroe-12
- Metric Name: count-error
- Resources: pailld-f10fee3-8107-44f3-9a70-3eb6d9a1d94 paill...
- * Threshold Condition: >= 12
- * Consecutive Period (s): 1
- Description: error
- * Alarm Severity: Major
- * Send Notification: Yes

Threshold Preview

Statistic Method: Average Statistical Cycle: [dropdown]

Graph showing values over time (Time Zone: GMT+08:00):

| Time | Value |
|-------|-------|
| 09:19 | 12 |
| 09:29 | 0 |
| 09:39 | 0 |
| 09:49 | 0 |
| 09:59 | 0 |
| 10:09 | 0 |
| 10:19 | 0 |

Buttons: Previous, Cancel, Submit

Step 4 After the threshold rule is created, if the statistical result exceeds the threshold, a Short Message Service (SMS) message or email will be sent immediately, informing you that the threshold has been exceeded and your service may be abnormal. The fault can then be located and rectified at the earliest time.

----End