AOM

Best Practices

Issue	01
Date	2020-08-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Creating Threshold Rules

The alarm function is a basic function of Application Operations Management (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 Short Message Service (SMS) message or email.

AOM provides both multi- and single-resource static threshold rules. The former threshold rules are supported only in CN North-Beijing1 and CN East-Shanghai2.

- Multi-resource static threshold rules: You can set threshold rules in batches. After a threshold rule is set, it can be applied to all services or hosts of a tenant. You can set threshold rules with a few clicks for six types of common metrics, including host and component metrics.
- Single-resource static threshold rules: You can set threshold conditions for application metrics (resource usage, latency, throughput, and errors) and resource metrics by setting single-resource static threshold rules. If a metric value meets a threshold condition, a threshold alarm is generated. If no metric data is reported, an insufficient data event is generated.

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	Downlink rate (BPS), downlink error rate, uplink error 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

Category	Example
Application performance metrics	Average latency, error calls, and throughput

For more information, see section "Metric Overview" in *AOM Service Overview*.

Procedure

Step 1 Create multi-resource static threshold rules with a few clicks.

1. Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**.
2. On the **Rule List** tab page, click **Create Default Threshold**.

   AOM will automatically create six static threshold templates. You can click the **Static Threshold Template** tab to view the templates. In addition, AOM will automatically create six default static threshold rules based on these templates. The monitored objects are all hosts or components. For example, click next to **[node:default-static-rule] CPU Usage** to monitor the CPU usage of all hosts.

   If you add hosts or components later, AOM automatically applies the rules to them.

Figure 1-1 Creating default multi-resource static threshold rules

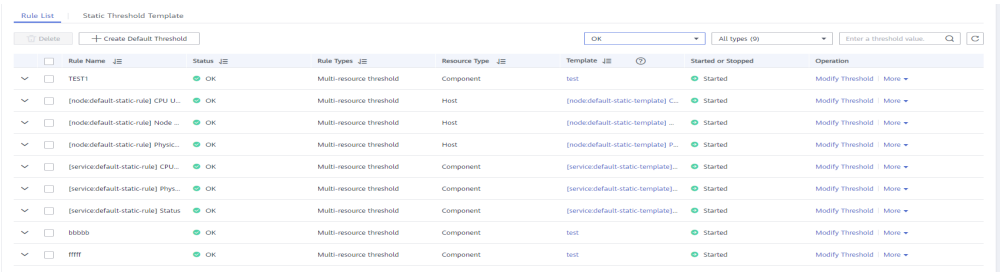


Table 1-1 Description of default multi-resource static threshold rules

Rule/Template	Resource	Metric	Default Configuration
– Rule: [node: default-static-rule] CPU Usage – Template: [node: default-static-template] CPU Usage	Host	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No

Rule/Template	Resource	Metric	Default Configuration
– Rule: [node: default-static-rule] Physical Memory Usage – Template: [node: default-static-template] Physical Memory Usage		Physical memory usage	
– Rule: [node: default-static-rule] Node Status – Template: [node: default-static-template] Node Status		Host status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
– Rule: [service: default-static-rule] CPU Usage – Template: [service: default-static-template] CPU Usage	Component	CPU usage	Statistic Method: Average; Threshold Condition: > 90%; Consecutive Periods: 3; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No
– Rule: [service: default-static-rule] Physical Memory Usage – Template: [service: default-static-template] Physical Memory Usage		Physical memory usage	
– Rule: [service: default-static-rule] Status – Template: [service: default-static-template] Status		Component status	Statistic Method: Average; Threshold Condition: > 0; Consecutive Periods: 1; Statistical Cycle: 1 minute; Alarm Severity: Major; Send Notification: No

Step 2 Create a multi-resource static threshold rule by using a custom static template.

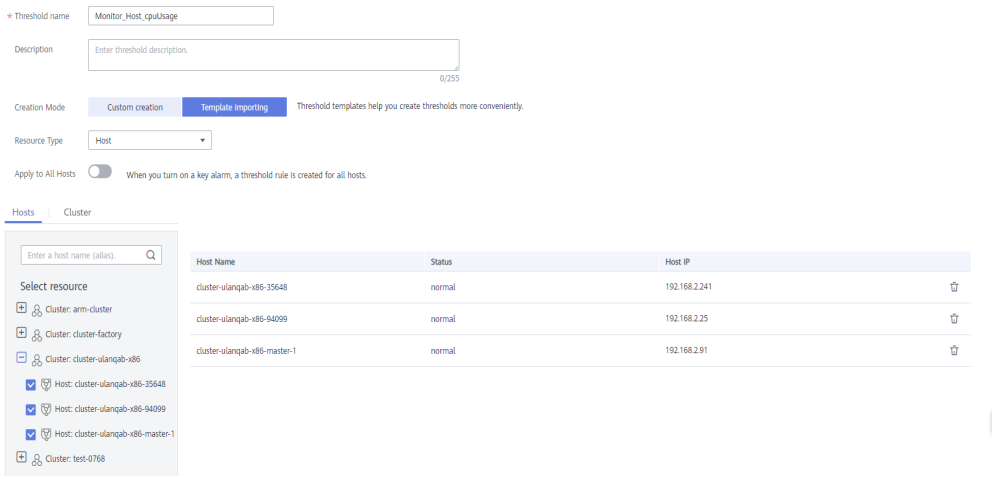
To create multi-resource static threshold rules for metrics excluding those listed in step 1, perform the following operations:

1. Before creating a static threshold rule, **create a static threshold template**.
2. Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**. Then, click **Add Threshold** in the upper right corner.
3. Select a resource. Specifically, enter a threshold rule name, select **Template importing** for **Creation Mode**, select a resource type, select the resource to be monitored from the resource tree, and click **Next**.

NOTE

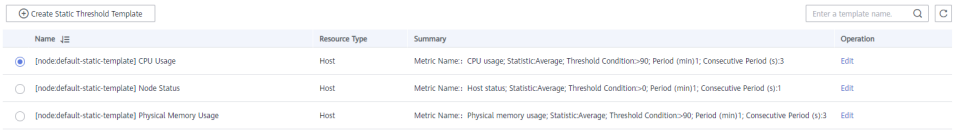
- When the option below **Resource Type** is disabled: You need to select one or more resources from the resource tree. A maximum of 100 resources can be selected.
- When the option below **Resource Type** is enabled: If **Resource Type** is **Host**, all hosts will be monitored. If **Resource Type** is **Component**, all components will be monitored. This function also takes effect for hosts or components added later.

Figure 1-2 Selecting the resource to be monitored



4. Select the created static threshold template.

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



5. Click **Submit** to create a multi-resource static threshold rule. Then click ⌄ to monitor the same metric of multiple resources.

   When a threshold alarm is generated, 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.

Step 3 Customize a single-resource static threshold rule.

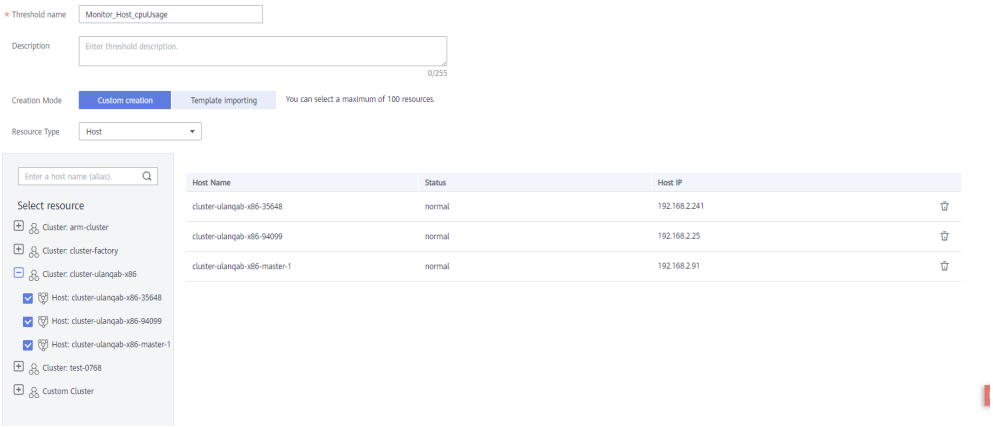
To create single-resource static threshold rules for metrics excluding those listed in step 1, perform the following operations:

1. Log in to the AOM console. In the navigation pane, choose **Alarm Center** > **Threshold Rules**. Then, click **Add Threshold** in the upper right corner.
2. Select a resource. Specifically, enter a threshold name, select **Custom creation** for **Creation Mode**, select a resource type, select the resource 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 1-4 Selecting resources



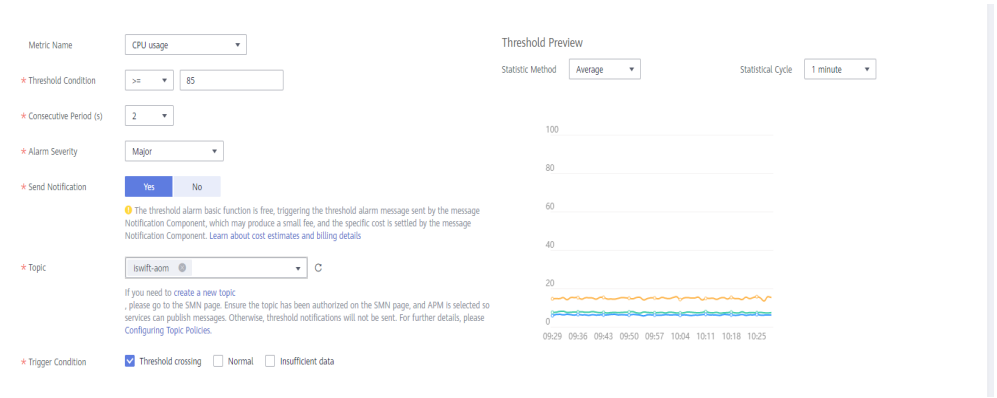
3. Customize a threshold. Specifically, select the metric to be monitored, and set parameters such as **Threshold Condition**, **Consecutive Period (s)**, **Alarm Severity**, **Statistic Method**, and **Send Notification**.

NOTE

- **Threshold Condition**: Trigger condition of a threshold alarm. A threshold condition consists of two parts: determination condition (≥, ≤, >, 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.

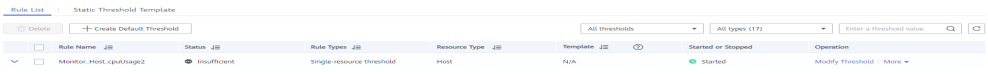
Figure 1-5 Customizing a threshold



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 1-6 Creating a single-resource static threshold rule



----End

2 Discovering Applications

Overview

Application Operations Management (AOM) can discover applications deployed on HUAWEI CLOUD hosts and collect their metrics based on configured rules. You can view the discovered applications on the **Application Monitoring** page and their metrics on the **O&M** page.

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.

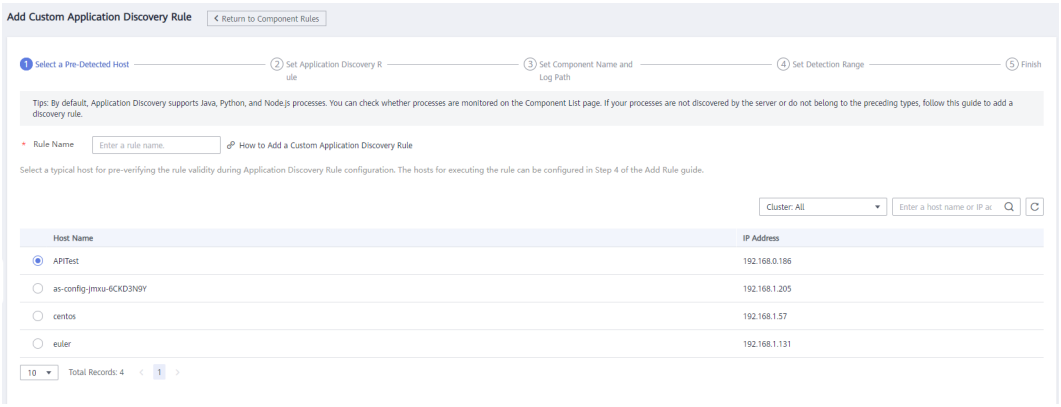
After application discovery is configured, you can use AOM to monitor application metrics and associate related alarms. Mainly, AOM can:

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).

Procedure

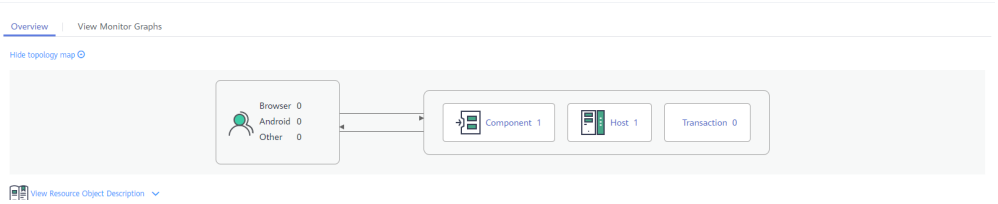
Step 1 Log in to AOM, choose **Configuration Management** > **Service Discovery** in the navigation pane, and then **configure an application discovery rule**.

You need to configure a log path associated with the target component.

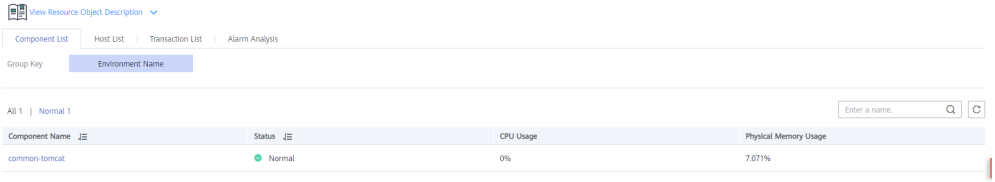


Step 2 View the application status.

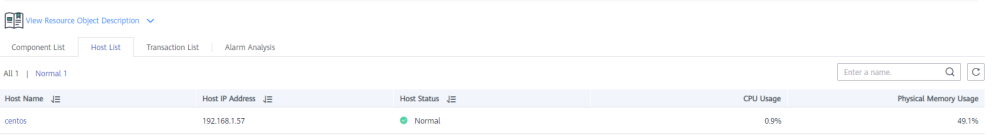
1. In the navigation pane, choose **Monitoring** > **Application Monitoring**.
2. Click an application to view its components and other resources.



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



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



5. Click the **Alarm Analysis** tab to view alarms.

----End

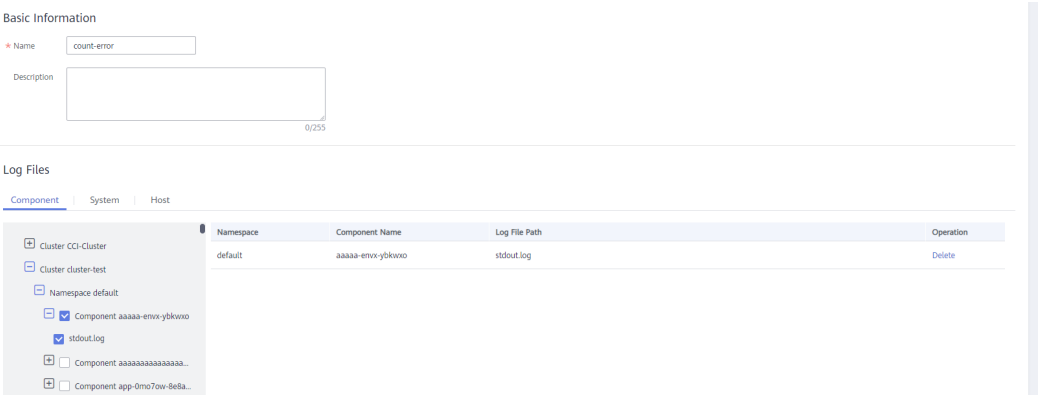
3 Counting Log Keywords

Scenario

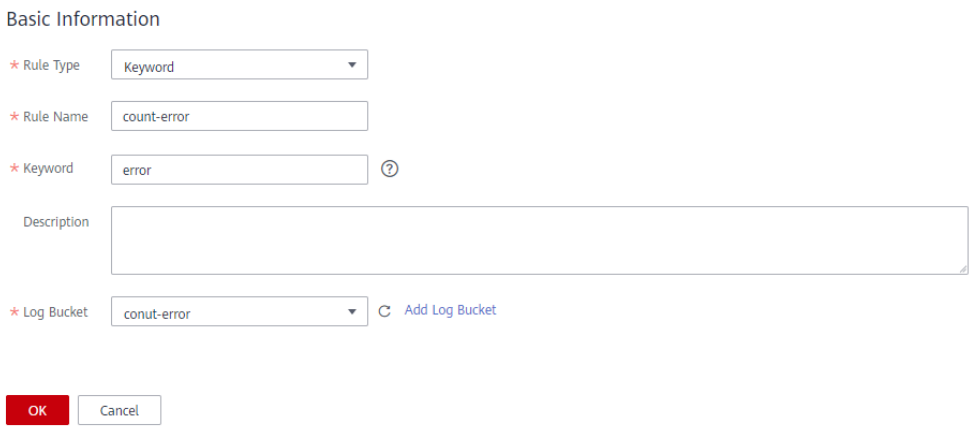
When an application is normal, its log file contains fewer than 10 error keywords every 10 minutes. However, when the application becomes abnormal, the number of error keywords increases rapidly. To identify an exception in a timely manner, you can use Application Operations Management (AOM) to count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

Procedure

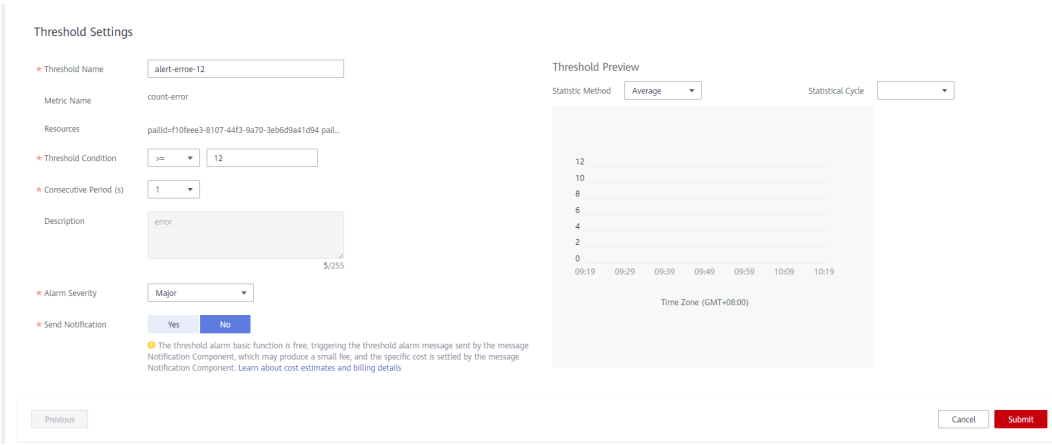
Step 1 Create a log bucket and store log files of the target application to the bucket.



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



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.



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. Then, locate and rectify the fault as soon as possible.

----End

