Application Operations Management

Getting Started

Issue	01
Date	2024-05-27

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Subscribing to AOM 2.0 1
2 Managing Applications 3
3 Managing Containers 18
4 Getting Started with Common Practices 29

1 Subscribing to AOM 2.0

Before subscribing to AOM, register **a HUAWEI ID**.

AOM resources are region-specific and cannot be used across regions. Select a region (such as CN-Hong Kong and AP-Bangkok) before enabling AOM.

NOTE

Currently, AOM 2.0 is available in ME-Riyadh, CN North-Beijing1, CN North-Beijing4, CN North-Beijing2, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, AF-Johannesburg, TR-Istanbul, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

Procedure

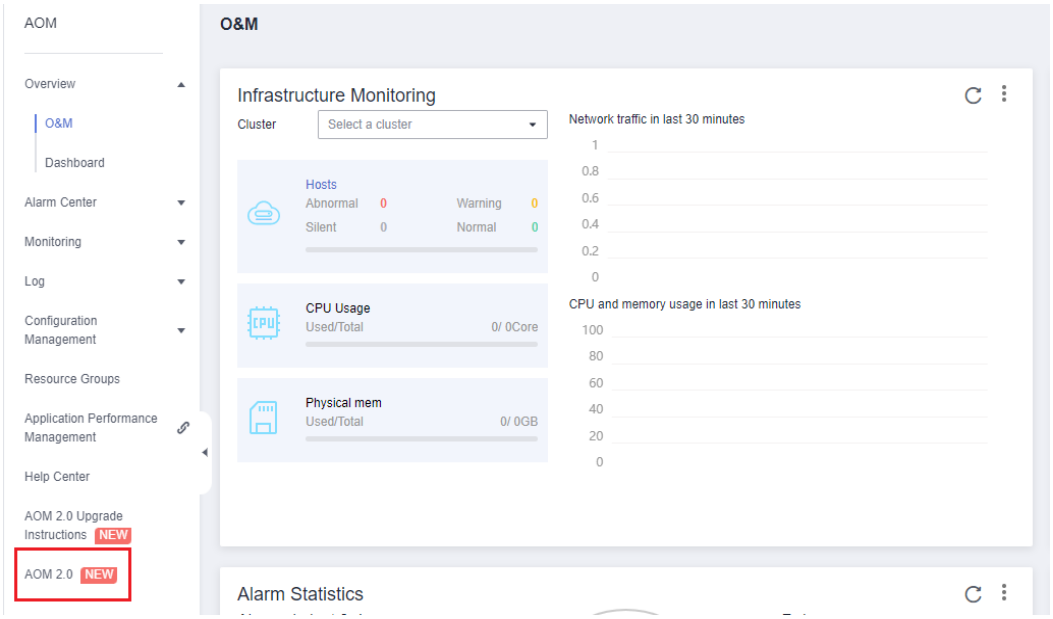
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner and select your desired region from the drop-down list.

Step 3 Click on the left and choose **Application** > **Application Operations Management**.

Step 4 In the navigation pane on the left, choose **AOM 2.0**. The AOM 2.0 page is displayed.

Figure 1-1 Going to the AOM 2.0 console



Step 5 On the notice dialog box that is displayed, read the billing changes for switching AOM 1.0 to AOM 2.0.

Step 6 Click **Authorize**. On the **Service Authorization** page that is displayed, read the *Authorization Statement* and select "I have read and agreed to the *Authorization Statement*".

Step 7 Click **Subscribe and Authorize for Free** for AOM 2.0.

Step 8 In the navigation tree on the left, click a function, for example, **Dashboard**.

----End

2 Managing Applications

This section describes how to use AOM to manage applications on the **Overview** page, including application creation, discovery, and monitoring. The procedure is as follows:

1. **Adding an Application**: Create an application and resource relationship tree on CMDB and install collectors on the hosts where the application is located.
2. **Setting an Alarm Rule**: Create metric alarm rules to ensure that notifications are sent when applications become abnormal.
3. **Setting an Alarm Action Rule**: Configure alarm action rules, for example, applications automatically restart when they become abnormal.

NOTE

The **Overview** option is disabled by default. If you need this option, enable it on the **Menu Settings** page. For details, see **Menu Settings**.

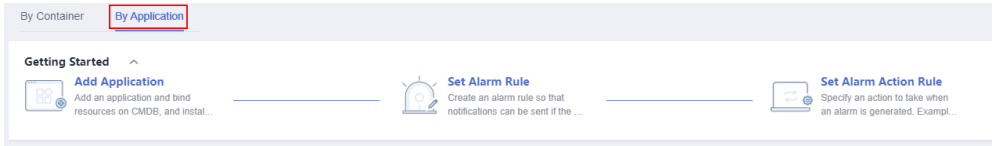
Adding an Application

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Overview**.

Step 3 On the displayed page, switch to **By Application**.

Figure 2-1 Switching the perspective



Step 4 In the **Getting Started** area, click **Add Application**. The **Application Management** page is displayed.

Step 5 Add an application.

1. Click **Add Application** in the upper right corner. On the displayed page, set parameters for adding an application.

Figure 2-2 Adding an application

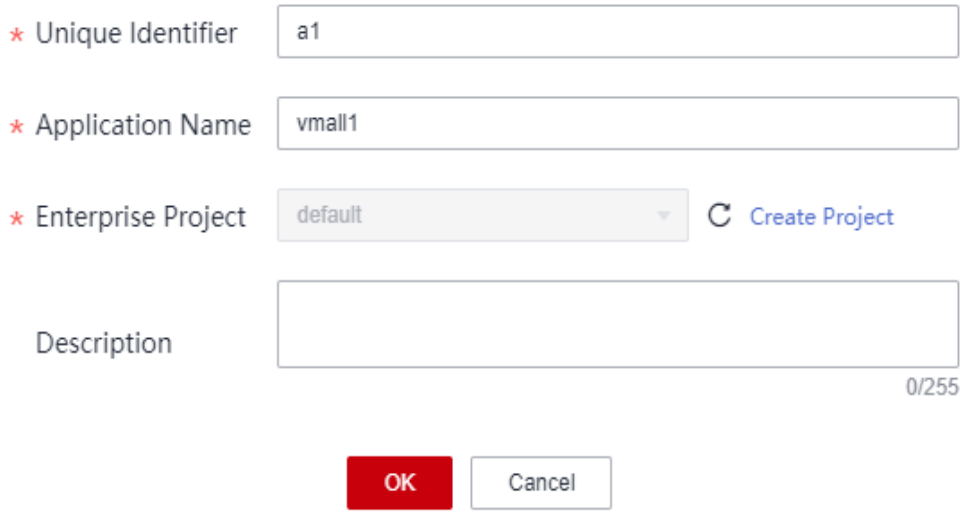


Table 2-1 Parameters for adding an application

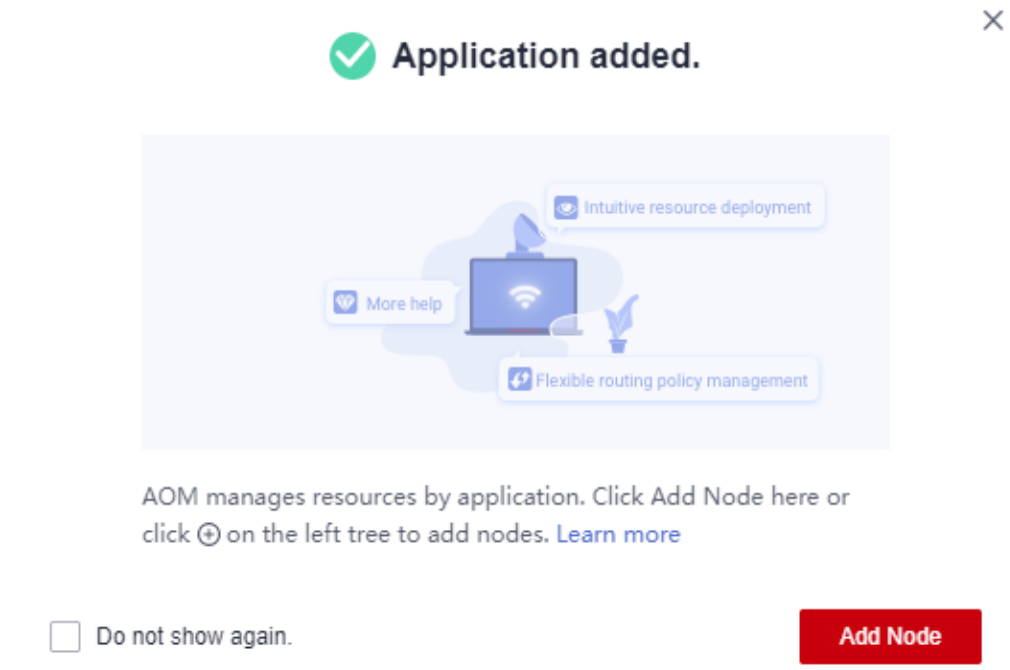
Parameter	Description
Unique Identifier	Unique identifier of an application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Application Name	Name of an application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project	Huawei Cloud enterprise project. Select a project from the drop-down list. If there is no project you want to select, click **Create Project** to create one.
Description	Description of the application. Enter up to 255 characters.

2. Click **OK**.

Step 6 Add nodes for the created application, including components and sub-applications. Use either of the following methods:

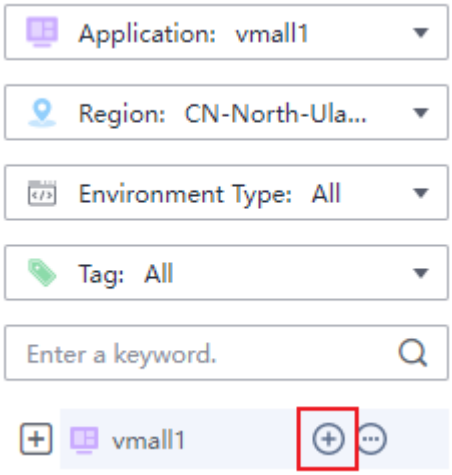
- After an application is created, click **Add Node**.

Figure 2-3 Adding a sub-application



- In the navigation pane, choose **Application Management**. Click ⊕ next to the application in the tree on the left.

  Figure 2-4 Application tree

1. Configure node information, including the node type and name.

Figure 2-5 Adding a node

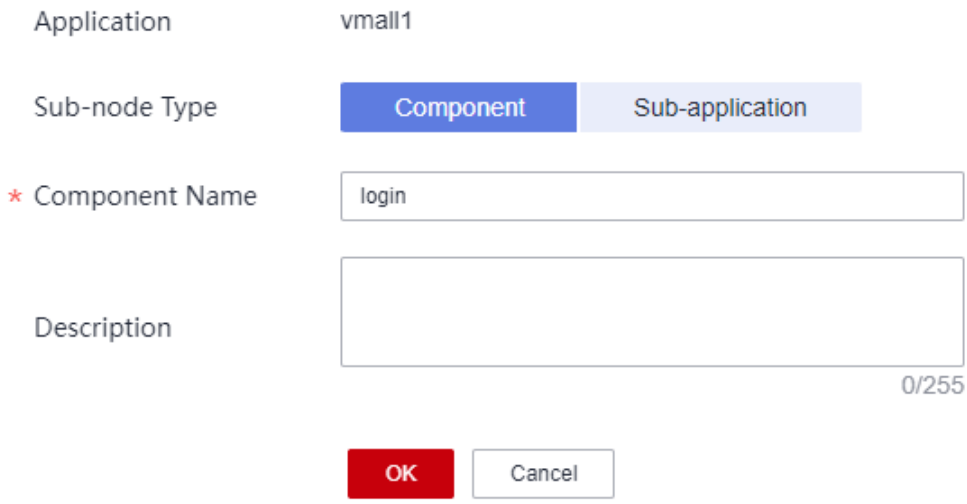


Table 2-2 Parameters for adding a node

Category	Parameter	Description
Component parameters	Component Name	Name of a component. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
	Description	Description of the component. Enter up to 255 characters.
Sub-application parameters	Unique Identifier	Unique identifier of a sub-application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
	Sub-application Name	Name of a sub-application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
	Description	Description of the sub-application. Enter up to 255 characters.

NOTE

- Up to three levels of sub-applications can be created under an application.
- Up to 50 sub-applications can be created under an application.
- Up to 50 components can be created under an application.

2. Click **OK**.

Step 7 Add different environments for the component based on information such as hosts and regions for easier resource and application management.

1. In the tree on the left, move the cursor to the name of the target component and click  .
2. On the **Add Environment** page, set information such as the environment type and host type.

Figure 2-6 Adding an environment

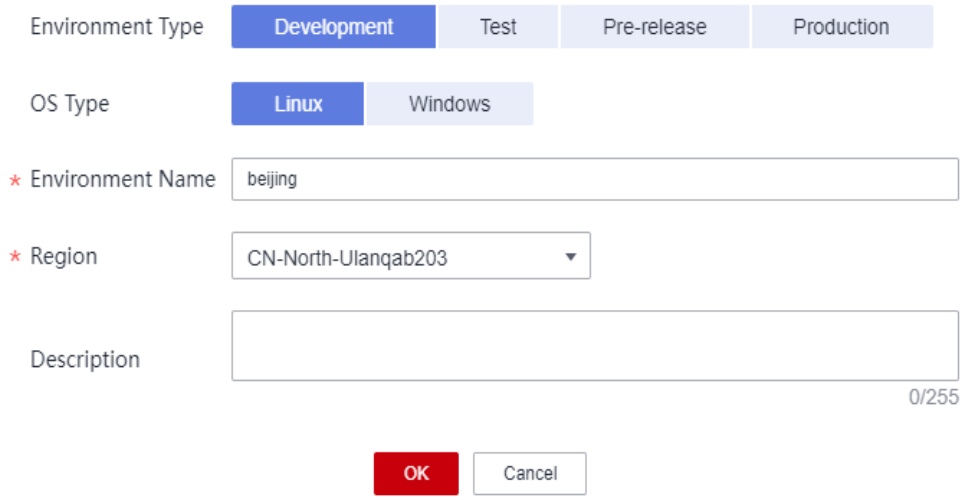


Table 2-3 Parameters for adding an environment

Parameter	Description
Environment Type	Type of an environment. Options: **Development**, **Test**, **Pre-release**, and **Production**.
OS Type	OS type of a host. Options: **Linux** and **Windows**.
Environment Name	Name of an environment. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Region	Region where the environment is located. Select a value from the drop-down list.
Description	Description of the environment. Enter up to 255 characters.

NOTE

A maximum of 20 environments can be created under a component.

3. Click **OK**.

After creating an environment for a component, you can bind resources to this environment. Then, you can monitor the resource usage in real time through application monitoring.

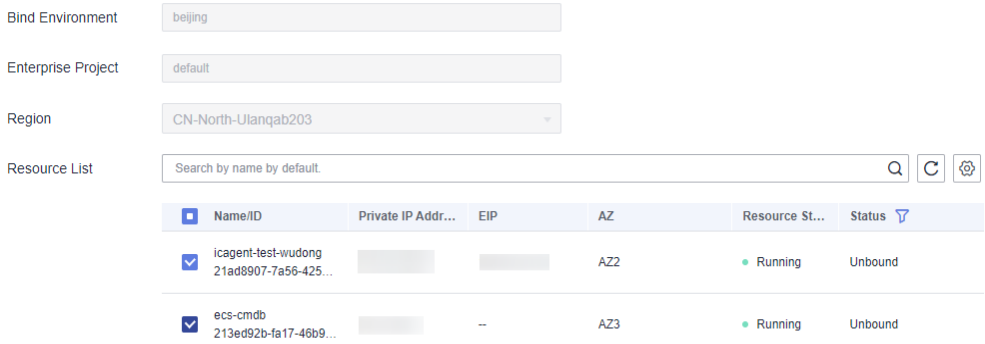
Step 8 Select the required resource on the right and bind it to the application.

1. In the tree on the left, select a target environment, click a resource tab in the right pane, and click **Bind Resource** in the lower pane.
2. Select your target resource from the resource list.

   NOTE

   The resource list displays only the resources under the enterprise project that you have selected.

   Figure 2-7 Binding resources



3. Click **Bind**.

   NOTE

   In the case of an ECS, click **Bind Resource & Install Agent** to bind the ECS and install an Agent.

----End

Setting an Alarm Rule

Metric alarm rules can be created in three modes: **Select by resource type**, **Select from all metrics**, and **PromQL**.

The following uses **Select from all metrics** as an example.

Step 1 On the **Overview** page, switch to **By Application**.

Step 2 In the **Getting Started** area, click **Set Alarm Rule**. The **Alarm Rules** page is displayed.

Step 3 Click **Create Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to **Table 2-4**.

Table 2-4 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Parameter	Description
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Description	Description of the rule. Enter up to 1024 characters.

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **Metric alarm rule**.
2. Set **Configuration Mode** to **Select from all metrics**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. **Table 2-5** describes the parameters.

   After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. A maximum of 50 metric data records can be displayed. Click the line icon before each metric data record to hide the metric data in the graph. You can click **Add Metric** to add metrics and set the statistical period and detection rules for the metrics.

   After moving the cursor to the metric data and the corresponding alarm condition, you can perform the following operations as required:

   - Click next to an alarm condition to hide the corresponding metric data record in the graph.
   - Click next to an alarm condition to convert the metric data and alarm condition into a Prometheus command.
   - Click next to an alarm condition to quickly copy the metric data and alarm condition and modify them as required.
   - Click next to an alarm condition to remove a metric data record from monitoring.

Figure 2-8 Setting alarm rule details

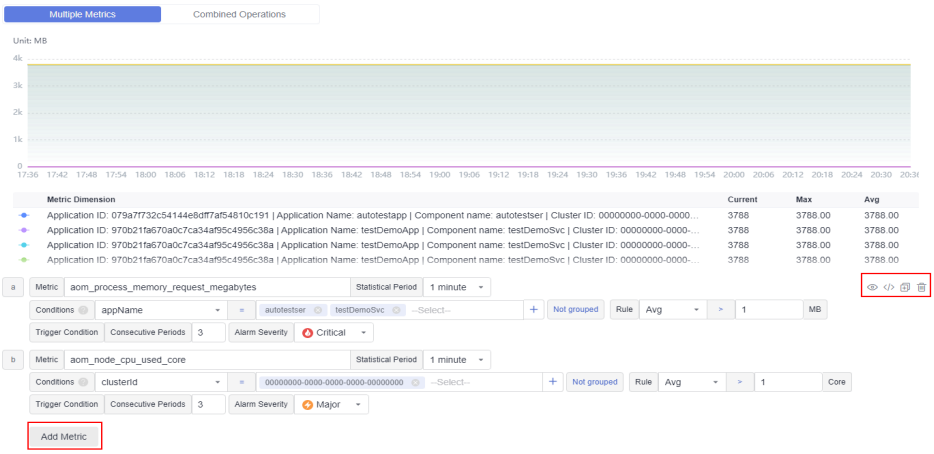


Table 2-5 Alarm rule details

Parameter	Description
Multiple Metrics	Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met. For example, if three alarm conditions are set, the system performs calculation respectively. If any of the conditions is met, an alarm will be triggered.
Combined Operations	The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered. For example, if there is no metric showing the CPU core usage of a host, do as follows: – Set the metric of alarm condition "a" to **aom_node_cpu_used_core** and retain the default values for other parameters. This metric is used to count the number of CPU cores used by a measured object. – Set the metric of alarm condition "b" to **aom_node_cpu_limit_core** and retain the default values for other parameters. This metric is used to count the total number of CPU cores that have been applied for a measured object. – If the expression is set to "a/b", the CPU core usage of the host can be obtained. – Set **Rule** to **Max > 0.2**. – In the trigger condition, set **Consecutive Periods** to **3**. – Set **Alarm Severity** to **Critical**. If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.
Metric	Metric to be monitored. When **Select from all metrics** is selected, enter keywords to search for metrics. Click the **Metric** text box. In the resource tree on the right, you can also select a target metric by resource type.
Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.

Parameter	Description
Condition	Metric monitoring scope. If this parameter is left blank, all resources are covered. Each condition is in a key-value pair. You can select a dimension name from the drop-down list. The dimension value varies according to the matching mode. – **=**: Select a dimension value from the drop-down list. For example, if **Dimension Name** is set to **Host name** and **Dimension Value** is set to **192.168.16.4**, only host **192.168.16.4** will be monitored. – **!=**: Select a dimension value from the drop-down list. For example, if **Dimension Name** is set to **Host name** and **Dimension Value** is set to **192.168.16.4**, all hosts excluding host **192.168.16.4** will be monitored. – **=~**: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (|). For example, if **Dimension Name** is set to **Host name** and **Regular Expression** is set to **192.*|172.***, only hosts whose names are **192.*** and **172.*** will be monitored. – **!~**: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (|). For example, if **Dimension Name** is set to **Host name** and **Regular Expression** is set to **192.*|172.***, all hosts excluding hosts **192.*** and **172.*** will be monitored. For details about how to enter a regular expression, see **Regular Expression Examples**. You can also click  and select **AND** or **OR** to add more conditions for the metric.
Grouping Condition	Aggregate metric data by the specified field and calculate the aggregation result. Options: **Not grouped**, **avg by**, **max by**, **min by**, and **sum by**. For example, **avg by clusterName** indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.
Rule	Detection rule of a metric alarm, which consists of the statistical mode (**Avg**, **Min**, **Max**, **Sum**, and **Samples**), determination criterion (≥, ≤, >, and <), and threshold value. For example, if the detection rule is set to **Avg >10**, a metric alarm will be generated if the average metric value is greater than 10.

Parameter	Description
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. For example, if **Consecutive Periods** is set to **2**, a metric alarm will be triggered if the trigger condition is met for two consecutive periods.
Alarm Severity	Severity of a metric alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see **Table 2-6**.

Table 2-6 Advanced settings

Parameter	Description
Check Interval	Interval at which metric query and analysis results are checked. • **Hourly**: Query and analysis results are checked every hour. • **Daily**: Query and analysis results are checked at a fixed time every day. • **Weekly**: Query and analysis results are checked at a fixed time point on a specified day of a week. • **Custom interval**: The query and analysis results are checked at a fixed interval. • **Cron**: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: **0/5 * * * ***, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods. For example, if **Consecutive Periods** is set to **2**, the alarm will be cleared when the alarm condition is not met for two consecutive periods.

Parameter	Description
Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods. The system supports the following actions: changing the status to **Exceeded** and sending an alarm, changing the status to **Insufficient data** and sending an event, maintaining **Previous status**, and changing the status to **Normal** and sending an alarm clearance notification.
Alarm Tag	Click + Tag to add an alarm tag. Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value". For details, see **Alarm Tags and Annotations**. **NOTE** If **tag policies** related to AOM have already been set, add alarm tags based on these policies. If a tag does not comply with the policies, tag addition may fail. Contact your organization administrator to learn more about tag policies.
Alarm Annotation	Click + Tag to add an alarm annotation. Alarm non-identification attribute. It is used in alarm notification and message template scenarios. It is in the format of "key:value". For details, see **Alarm Tags and Annotations**.

Step 7 Set an alarm notification policy. For details, see **Table 2-7**.

Figure 2-9 Setting an alarm notification policy

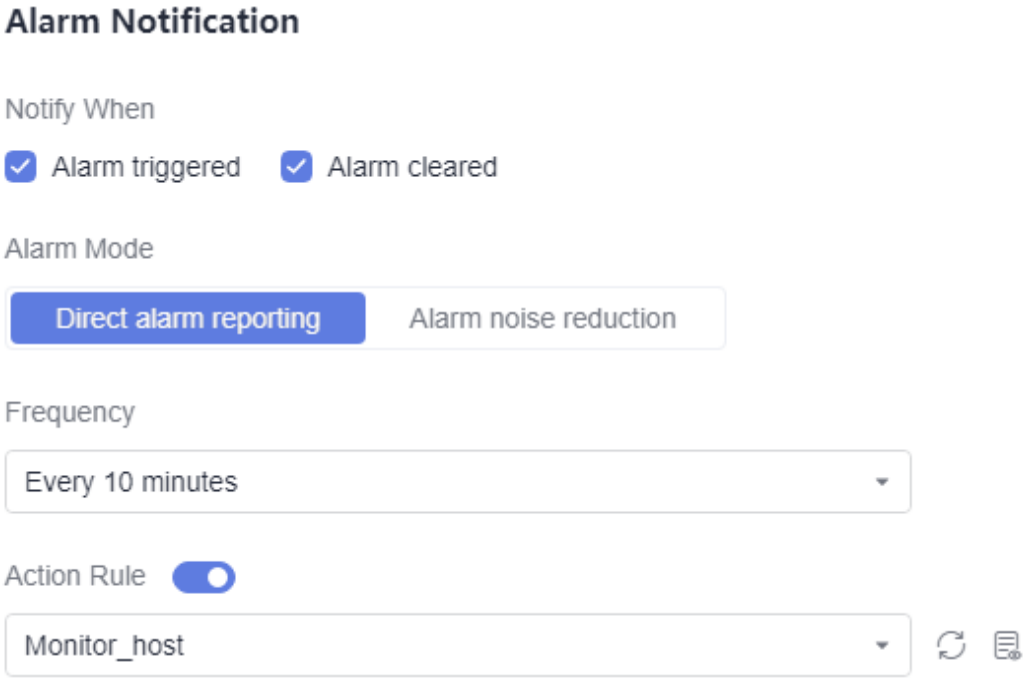


Table 2-7 Parameters for setting an alarm notification policy

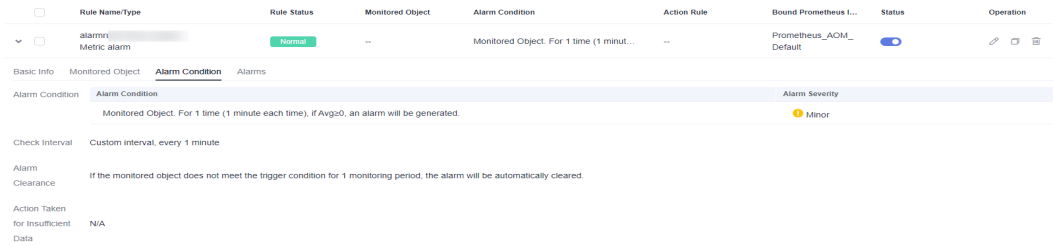
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: frequency for sending alarm notifications. Select a desire value from the drop-down list. If you enable this function, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details about how to set alarm action rules, see **Setting an Alarm Action Rule**. • **Alarm noise reduction**: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. If you select this mode, the silence rule is enabled by default. You can determine whether to enable **Grouping Rule** as required. If you enable this function, select a grouping rule from the drop-down list. If the existing grouping rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details, see **Creating a Grouping Rule**.

Step 8 Click **Confirm**. Then click **View Rule** to view the created alarm rule.

In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management** > **Alarm List** in the navigation pane. If a metric value meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

Figure 2-10 Created metric alarm rule



----End

Setting an Alarm Action Rule

Step 1 On the **Overview** page, switch to **By Application**.

Step 2 In the **Getting Started** area, click **Set Alarm Action Rule**. The **Alarm Action Rules** page is displayed.

Step 3 On the **Action Rules** tab page, click **Create**.

Step 4 Set parameters such as **Rule Name** and **Action Type** by referring to **Table 2-8**.

Figure 2-11 Creating an alarm action rule

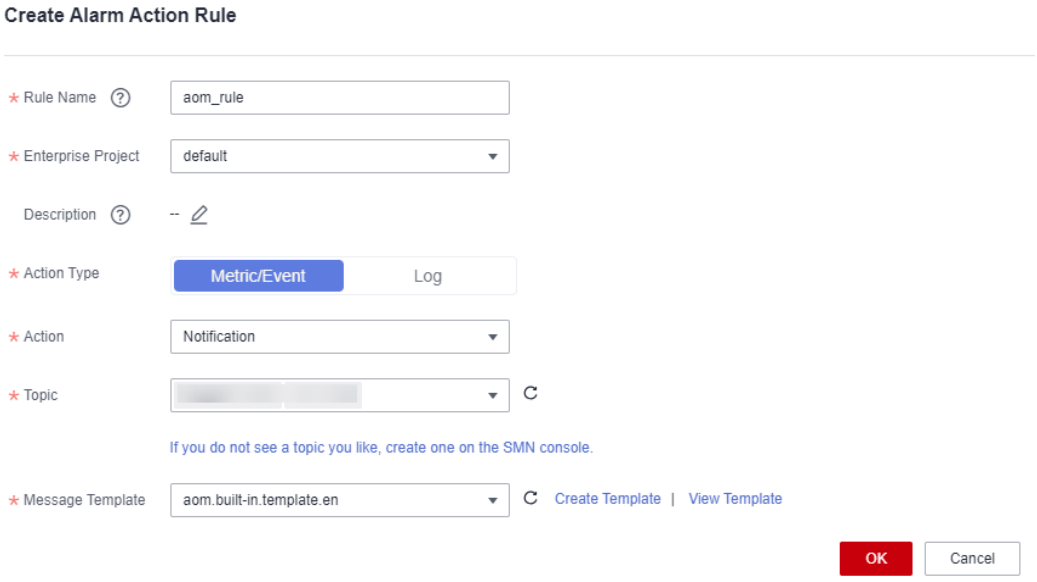


Table 2-8 Parameters for creating an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter up to 200 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, underscores, and hyphens are allowed.
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Description	Description of the action rule. Enter up to 1024 characters.
Action Type	Type of an alarm action rule. • Metric/Event If a metric or an event meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template. • Log If the log data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.
Action	Type of action that is associated with the SMN topic and message template. Select your desired action from the drop-down list. Only **Notification** is supported.

Parameter	Description
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If no proper message template is available, click **Create Template** to create a message template.

Step 5 Click **OK**.

----End

3 Managing Containers

This section describes how to use AOM to quickly manage containers on the **Overview** page, including container monitoring and alarm rule creation. The procedure is as follows:

1. **Monitoring Containers**: AOM is compatible with Kubernetes and automatically collects and reports container information, without the need to configure CMDB.
2. **Setting an Alarm Rule**: Create metric alarm rules to ensure that notifications are sent when containers are abnormal.
3. **Setting an Alarm Action Rule**: Configure alarm action rules, for example, containers automatically restart when they become abnormal.

NOTE

The **Overview** option is disabled by default. If you need this option, enable it on the **Menu Settings** page. For details, see **Menu Settings**.

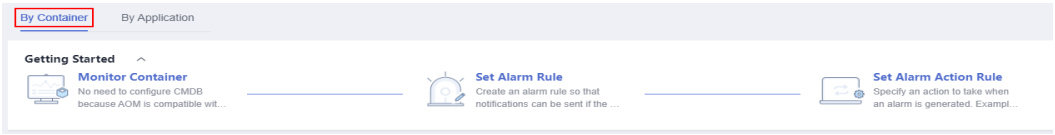
Monitoring Containers

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Overview**.

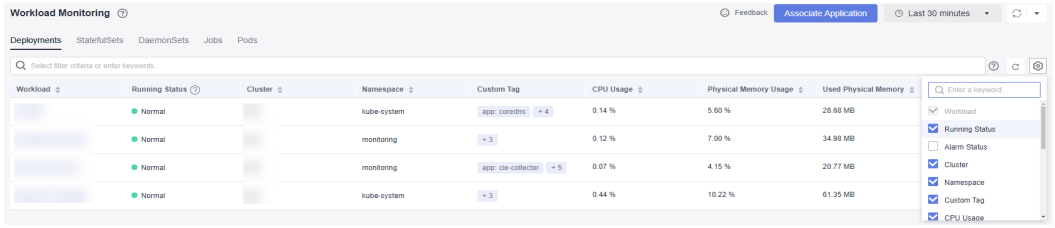
Step 3 On the displayed page, switch to **By Container**.

Figure 3-1 Switching the perspective



Step 4 In the **Getting Started** area, click **Monitor Container**. The **Workload Monitoring** page is displayed.

Figure 3-2 Workload monitoring



Step 5 In the upper right corner of the page, set filter criteria.

1. Set a time range to view the workloads reported. There are two methods to set a time range:

   Method 1: Use a predefined time label, such as **Last hour**, **Last 6 hours**, or **Last day**. Select one as required.

   Method 2: Specify the start time and end time (max. 30 days).

2. Set the interval for refreshing information. Click  and select a desired value from the drop-down list.

Step 6 Click any workload tab to view information, such as workload name, status, cluster, and namespace.

- In the upper part of the workload list, filter workloads by cluster, namespace, or pod name.
- Click  in the upper right corner to obtain the latest workload information.
- Click  in the upper right corner and select or deselect the columns to display.
- Click the name of a workload to view its details.
  - On the **Pods** tab page, view all pod conditions of the workload. Click a pod name to view the resource usage and health status of the pod's containers.
  - On the **Monitoring Views** tab page, view the resource usage of the workload.
  - On the **Logs** tab page, view the raw logs and real-time logs of the workload and analyze them as required.
  - On the **Alarms** tab page, view the alarm details of the workload.
  - On the **Events** tab page, view the event details of the workload.

----End

Setting an Alarm Rule

Metric alarm rules can be created in three modes: **Select by resource type**, **Select from all metrics**, and **PromQL**.

The following uses **Select from all metrics** as an example.

Step 1 On the **Overview** page, switch to **By Container**.

Step 2 In the **Getting Started** area, click **Set Alarm Rule**. The **Alarm Rules** page is displayed.

Step 3 Click **Create Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to **Table 3-1**.

Table 3-1 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Description	Description of the rule. Enter up to 1024 characters.

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **Metric alarm rule**.
2. Set **Configuration Mode** to **Select from all metrics**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. **Table 3-2** describes the parameters.

   After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. A maximum of 50 metric data records can be displayed. Click the line icon before each metric data record to hide the metric data in the graph. You can click **Add Metric** to add metrics and set the statistical period and detection rules for the metrics.

   After moving the cursor to the metric data and the corresponding alarm condition, you can perform the following operations as required:

   - Click next to an alarm condition to hide the corresponding metric data record in the graph.
   - Click next to an alarm condition to convert the metric data and alarm condition into a Prometheus command.
   - Click next to an alarm condition to quickly copy the metric data and alarm condition and modify them as required.
   - Click next to an alarm condition to remove a metric data record from monitoring.

Figure 3-3 Setting alarm rule details

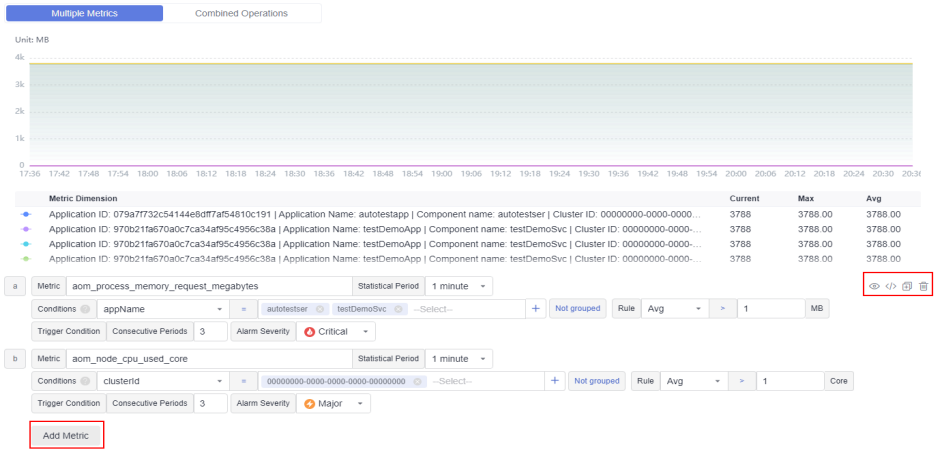


Table 3-2 Alarm rule details

Parameter	Description
Multiple Metrics	Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met. For example, if three alarm conditions are set, the system performs calculation respectively. If any of the conditions is met, an alarm will be triggered.
Combined Operations	The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered. For example, if there is no metric showing the CPU core usage of a host, do as follows: – Set the metric of alarm condition "a" to **aom_node_cpu_used_core** and retain the default values for other parameters. This metric is used to count the number of CPU cores used by a measured object. – Set the metric of alarm condition "b" to **aom_node_cpu_limit_core** and retain the default values for other parameters. This metric is used to count the total number of CPU cores that have been applied for a measured object. – If the expression is set to "a/b", the CPU core usage of the host can be obtained. – Set **Rule** to **Max > 0.2**. – In the trigger condition, set **Consecutive Periods** to **3**. – Set **Alarm Severity** to **Critical**. If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.

Parameter	Description
Metric	Metric to be monitored. When **Select from all metrics** is selected, enter keywords to search for metrics. Click the **Metric** text box. In the resource tree on the right, you can also select a target metric by resource type.
Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.
Condition	Metric monitoring scope. If this parameter is left blank, all resources are covered. Each condition is in a key-value pair. You can select a dimension name from the drop-down list. The dimension value varies according to the matching mode. – **=**: Select a dimension value from the drop-down list. For example, if **Dimension Name** is set to **Host name** and **Dimension Value** is set to **192.168.16.4**, only host **192.168.16.4** will be monitored. – **!=**: Select a dimension value from the drop-down list. For example, if **Dimension Name** is set to **Host name** and **Dimension Value** is set to **192.168.16.4**, all hosts excluding host **192.168.16.4** will be monitored. – **=~**: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (|). For example, if **Dimension Name** is set to **Host name** and **Regular Expression** is set to **192.*|172.***, only hosts whose names are **192.*** and **172.*** will be monitored. – **!~**: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (|). For example, if **Dimension Name** is set to **Host name** and **Regular Expression** is set to **192.*|172.***, all hosts excluding hosts **192.*** and **172.*** will be monitored. For details about how to enter a regular expression, see **Regular Expression Examples**. You can also click  and select **AND** or **OR** to add more conditions for the metric.
Grouping Condition	Aggregate metric data by the specified field and calculate the aggregation result. Options: **Not grouped**, **avg by**, **max by**, **min by**, and **sum by**. For example, **avg by clusterName** indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.

Parameter	Description
Rule	Detection rule of a metric alarm, which consists of the statistical mode (**Avg**, **Min**, **Max**, **Sum**, and **Samples**), determination criterion (≥, ≤, >, and <), and threshold value. For example, if the detection rule is set to **Avg >10**, a metric alarm will be generated if the average metric value is greater than 10.
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. For example, if **Consecutive Periods** is set to **2**, a metric alarm will be triggered if the trigger condition is met for two consecutive periods.
Alarm Severity	Severity of a metric alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see **Table 3-3**.

Table 3-3 Advanced settings

Parameter	Description
Check Interval	Interval at which metric query and analysis results are checked. • **Hourly**: Query and analysis results are checked every hour. • **Daily**: Query and analysis results are checked at a fixed time every day. • **Weekly**: Query and analysis results are checked at a fixed time point on a specified day of a week. • **Custom interval**: The query and analysis results are checked at a fixed interval. • **Cron**: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: **0/5 * * * ***, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods. For example, if **Consecutive Periods** is set to **2**, the alarm will be cleared when the alarm condition is not met for two consecutive periods.

Parameter	Description
Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods. The system supports the following actions: changing the status to **Exceeded** and sending an alarm, changing the status to **Insufficient data** and sending an event, maintaining **Previous status**, and changing the status to **Normal** and sending an alarm clearance notification.
Alarm Tag	Click + Tag to add an alarm tag. Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value". For details, see **Alarm Tags and Annotations**. **NOTE** If **tag policies** related to AOM have already been set, add alarm tags based on these policies. If a tag does not comply with the policies, tag addition may fail. Contact your organization administrator to learn more about tag policies.
Alarm Annotation	Click + Tag to add an alarm annotation. Alarm non-identification attribute. It is used in alarm notification and message template scenarios. It is in the format of "key:value". For details, see **Alarm Tags and Annotations**.

Step 7 Set an alarm notification policy. For details, see **Table 3-4**.

Figure 3-4 Setting an alarm notification policy

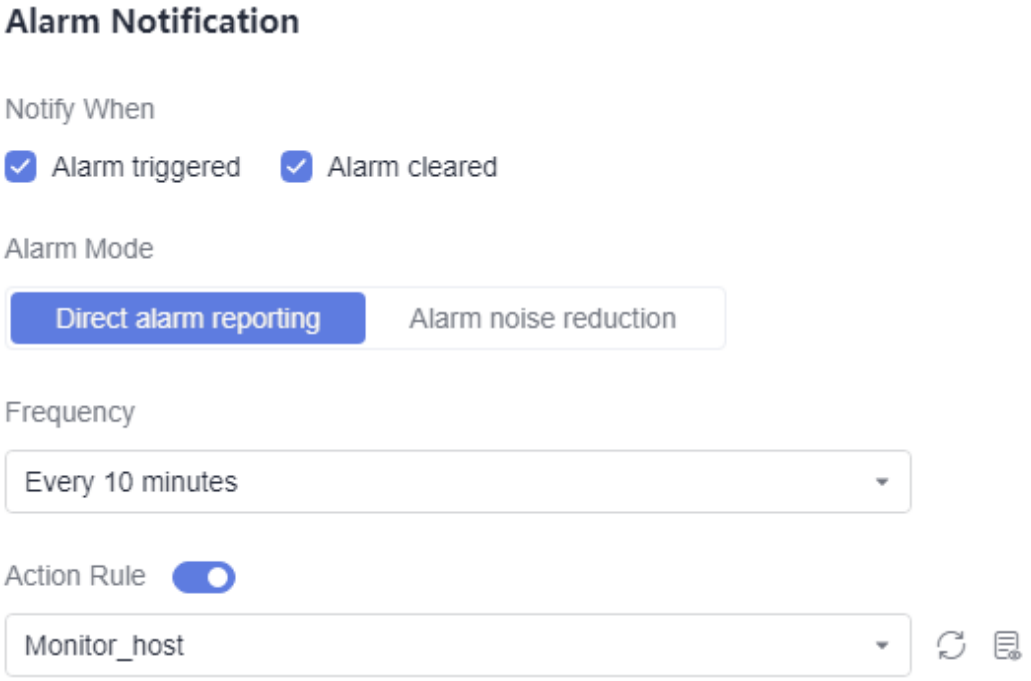


Table 3-4 Parameters for setting an alarm notification policy

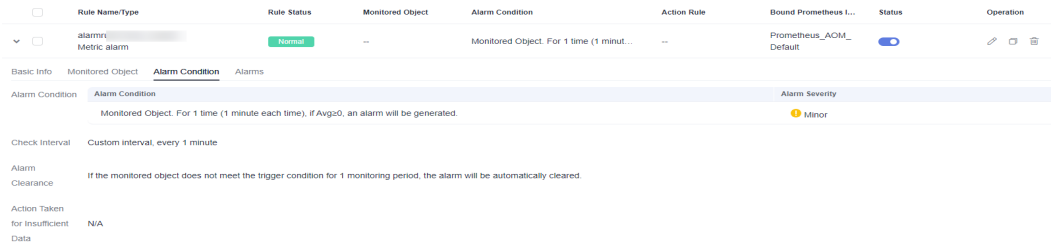
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: frequency for sending alarm notifications. Select a desire value from the drop-down list. If you enable this function, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details about how to set alarm action rules, see **Setting an Alarm Action Rule**. • **Alarm noise reduction**: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. If you select this mode, the silence rule is enabled by default. You can determine whether to enable **Grouping Rule** as required. If you enable this function, select a grouping rule from the drop-down list. If the existing grouping rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details, see **Creating a Grouping Rule**.

Step 8 Click **Confirm**. Then click **View Rule** to view the created alarm rule.

In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management** > **Alarm List** in the navigation pane. If a metric value meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

Figure 3-5 Created metric alarm rule



----End

Setting an Alarm Action Rule

Step 1 Go to the **Dashboard** page and switch to **By Container**.

Step 2 In the **Getting Started** area, click **Set Alarm Action Rule**. The **Alarm Action Rules** page is displayed.

Step 3 On the **Action Rules** tab page, click **Create**.

Step 4 Set parameters such as **Rule Name** and **Action Type** by referring to **Table 3-5**.

Figure 3-6 Creating an alarm action rule

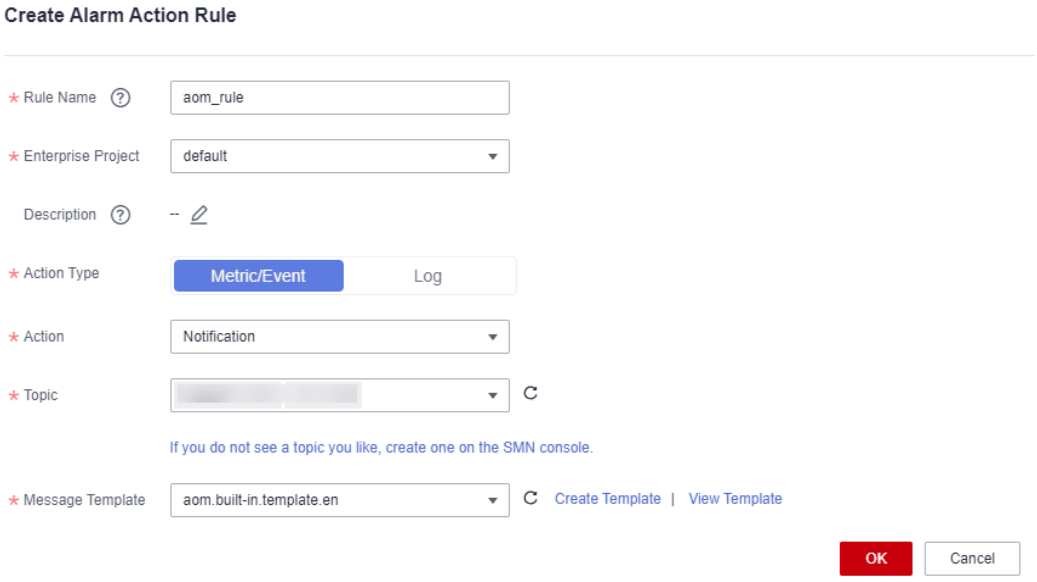


Table 3-5 Parameters for creating an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter up to 200 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, underscores, and hyphens are allowed.
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Description	Description of the action rule. Enter up to 1024 characters.
Action Type	Type of an alarm action rule. • Metric/Event If a metric or an event meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template. • Log If the log data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.
Action	Type of action that is associated with the SMN topic and message template. Select your desired action from the drop-down list. Only **Notification** is supported.

Parameter	Description
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If no proper message template is available, click **Create Template** to create a message template.

Step 5 Click **OK**.

----End

4 Getting Started with Common Practices

After completing basic operations such as managing applications and containers, you can implement common practices based on this section.

Table 4-1 Common practices

Practice	Description
Preventing Alarm Storms Through Noise Reduction	Set alarm noise reduction, so AOM processes alarms based on noise reduction rules to prevent alarm storms.

