

Application Operations Management

Getting Started

Issue 01
Date 2025-03-03



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



HUAWEI 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 Monitoring CCE Metrics..... | 1 |
| 2 Using Prometheus to Monitor ECS Metrics..... | 9 |
| 3 (New) Using Prometheus to Monitor ECS Metrics..... | 18 |
| 4 Getting Started with Common Practices..... | 28 |

1 Monitoring CCE Metrics

Cloud Container Engine (CCE) is an enterprise-level cluster hosting service. It allows you to quickly build reliable container clusters based on cloud servers, and easily create and manage different containerized workloads. AOM is a one-stop, multi-dimensional O&M platform for cloud applications. It enables you to monitor real-time running of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency. After CCE is interconnected with AOM, CCE cluster information can be reported to AOM. AOM can monitor the status and performance of CCE clusters and provide alarm notifications in real time.

You can set alarm rules in AOM to check whether resources in CCE clusters are normal and learn about real-time cluster running. This section uses **aom_container_cpu_usage** as an example to describe how to set an alarm rule.

Procedure

1. [Subscribing to AOM 2.0 for the First Time and Granting Permissions](#)
2. **Monitoring Containers:** Purchase a cluster and node on CCE. The ICAgent is then automatically installed to report cluster metrics to AOM.
3. **Setting an Alarm Action Rule:** Create an alarm action rule and associate it with an SMN topic and a message template. If the CCE metric data meets the alarm condition, the system sends an alarm notification accordingly. If you do not want to receive alarm notifications by email or SMS, there is no need to set alarm action rules.
4. **Setting an Alarm Rule:** Create an alarm rule for the CCE metric. If the metric data meets the alarm condition, an alarm is generated.

Preparation

This section uses a CCE metric as an example. You need to purchase a cluster and node in CCE in advance. For details, see [Buying a CCE Standard/Turbo Cluster](#) and [Creating a Node](#). If you already have a cluster and node, skip this step.

Subscribing to AOM 2.0 for the First Time and Granting Permissions

1. Register an account and perform real-name authentication.

Before using AOM 2.0, register a HUAWEI ID and perform real-name authentication. If you already have a HUAWEI ID, skip the following operations.

- a. Go to the [Huawei Cloud](#) official website, and click **Sign Up** in the upper right corner.
 - b. Complete registration by referring to [Signing up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
 - c. Complete real-name authentication by referring to [Real-Name Authentication](#).
2. Subscribe to AOM 2.0.
- Before using AOM 2.0, subscribe to it. If you have subscribed to AOM 2.0, skip the following operations.
- a. Go to the [AOM official website](#).
 - b. Click **AOM 2.0 Console** under the AOM introduction.
 - c. On the displayed dialog box, read the billing changes for switching AOM 1.0 to AOM 2.0.
 - d. Click **Authorize**. On the displayed **Service Authorization** page, read the *Authorization Statement* and select "I have read and agreed to the *Authorization Statement*".
 - e. Click **Subscribe and Authorize for Free** for AOM 2.0.
3. Grant the AOM and CCE permissions to the user.

You must have the **AOM FullAccess** and **CCE FullAccess** permissions. For details, see [Creating a User and Granting Permissions](#) and [Granting Cluster Permissions to an IAM User](#).

Monitoring Containers

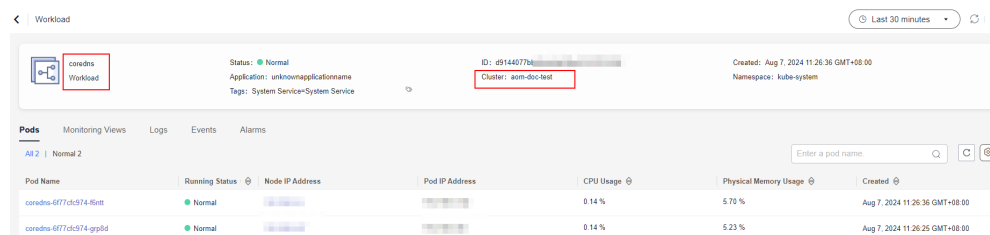
Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Infrastructure Monitoring > Workload Monitoring**.

Step 3 Click a workload on any workload tab page. The workload details such as the name, status, cluster, and namespace are displayed. [Figure 1-1](#) shows the details about the **coredns** workload in the **aom-doc-test** cluster.

You can also create more workloads to monitor by referring to [Creating a Workload](#).

Figure 1-1 Workload details



----End

Setting an Alarm Action Rule

Step 1 In the navigation pane, choose **Alarm Management > Alarm Action Rules**.

Step 2 On the **Action Rules** tab page, click **Create** and set parameters by referring to [Table 1-1](#).

Table 1-1 Alarm action rule parameters

| Parameter | Description | Example |
|--------------------|--|--------------|
| 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. | Mon_aom |
| Enterprise Project | Select the required enterprise project. The default value is default . | default |
| Description | Description of the action rule. Enter up to 1,024 characters. In this example, leave this parameter blank. | - |
| Rule Type | Type of an alarm action rule. Select Metric/Event . 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. | Metric/Event |
| Action | Type of action that is associated with the SMN topic and message template. Select a desired action from the drop-down list. Only Notification is supported. | Notification |
| Topic | SMN topic. Select a 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 a desired template from the drop-down list. If there is no message template you want to select, create one . | - |

Step 3 Click **OK**.

----End

Setting an Alarm Rule

Metric alarm rules can be created using the following modes: **Select from all metrics**, and **PromQL**.

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

Step 1 In the navigation pane, choose **Alarm Management > Alarm Rules**. Then, click **Create**.

Step 2 Set basic information about the alarm rule by referring to [Table 1-2](#).

Table 1-2 Basic information

| Parameter | Description | Example |
|--------------------|---|-----------------|
| Rule Name | Name of the 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. | monitor_cc e |
| Enterprise Project | Select the required enterprise project. The default value is default . | default |
| Description | Description of the rule. Enter up to 1,024 characters. In this example, leave this parameter blank. | - |

Step 3 Set the detailed information about the alarm rule.

- Rule Type: Metric alarm rule.**
- Configuration Mode: Select from all metrics.** Then you can set alarm conditions for different types of resources.
- Select a target Prometheus instance from the drop-down list. In this example, select **Prometheus_AOM_Default**.
- Set alarm rule details by referring to [Table 1-3](#).

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm conditions. You can click **Add Metric** to add more metrics and set the statistical period and detection rules for them.

Figure 1-2 Setting alarm rule details

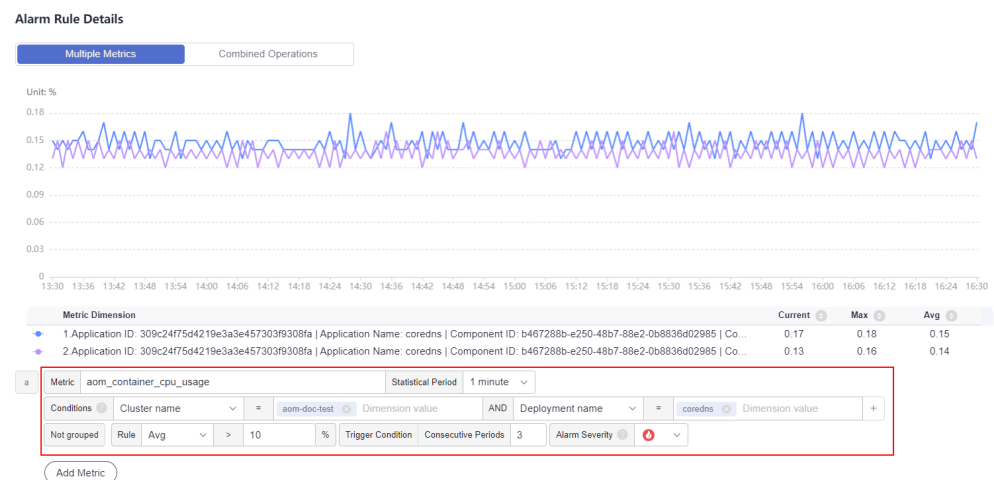





Table 1-3 Alarm rule details

| Parameter | Description | Example |
|--------------------|--|---|
| 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. | Multiple Metrics |
| Metric | Metric to be monitored. Click the Metric text box. In the resource tree on the right, you can select a target metric by resource type. | aom_container_cpu_usage |
| Statistical Period | Interval at which metric data is collected. | 1 minute |
| Conditions | Metric monitoring scope. If this parameter is left blank, all resources are covered. Set the condition based on the workload mentioned in 3 . | Cluster name=aom-doc-test AND Workload name=coredns |
| Grouping Condition | Aggregate metric data by the specified field and calculate the aggregation result. | Not grouped |
| Rule | Detection rule of a metric alarm, which consists of the statistical mode (Avg , Min , Max , Sum , and Samples), determination criterion (\geq , \leq , $>$, and $<$), and threshold value. | Avg > 10 |
| Trigger Condition | When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. | 3 |
| Alarm Severity | Severity of a metric alarm. |  |

Step 4 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 1-4](#).

Table 1-4 Advanced settings

| Parameter | Description | Example |
|-----------------|--|---------------------------|
| Check Interval | Interval at which metric query and analysis results are checked. | Custom interval: 1 minute |
| Alarm Clearance | The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. | 1 |

| Parameter | Description | Example |
|------------------------------------|--|---|
| Action Taken for Insufficient Data | Action to be taken if there is no or insufficient metric data within the monitoring period. Enable this option if needed. | Enabled: If the data is insufficient for 1 period, the status will change to Insufficient data and an alarm will be sent. |
| Alarm Tag | Click  to add an alarm tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |
| Alarm Annotation | Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |

Step 5 Set an alarm notification policy. For details, see [Table 1-5](#).

Figure 1-3 Setting an alarm notification policy

Alarm Notification

Notify When

- Alarm triggered Alarm cleared

Alarm Mode

Direct alarm reporting Alarm noise reduction

Frequency

Once

Action Rule

Mon_aom



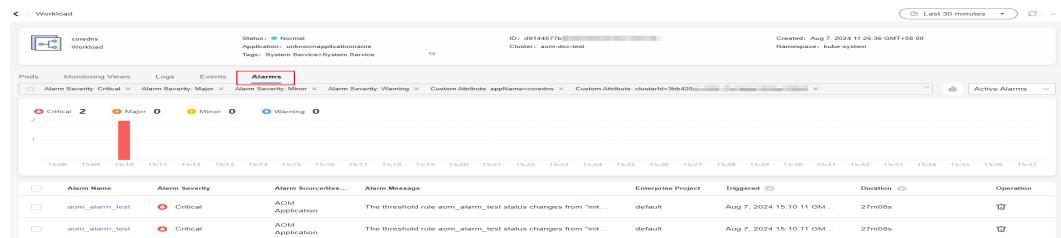
Table 1-5 Alarm notification policy parameters

| Parameter | Description | Example |
|-------------|---|--|
| Notify When | <p>Set the scenario for sending alarm notifications. By default, Alarm triggered and Alarm cleared are selected.</p> <ul style="list-style-type: none"> • 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. | Retain the default value. |
| Alarm Mode | <ul style="list-style-type: none"> • 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. • Action Rule: If you enable this function, the system sends notifications based on the associated SMN topic and message template. If there is no alarm action rule you want to select, 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. | <p>Alarm Mode: Select Direct alarm reporting.</p> <p>Frequency: Select Once.</p> <p>Action Rule: Select Mon_aom.</p> |

Step 6 Click **Confirm**. Then click **View Rule** to view the created 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 the alarm, 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 1-4 Creating a metric alarm rule



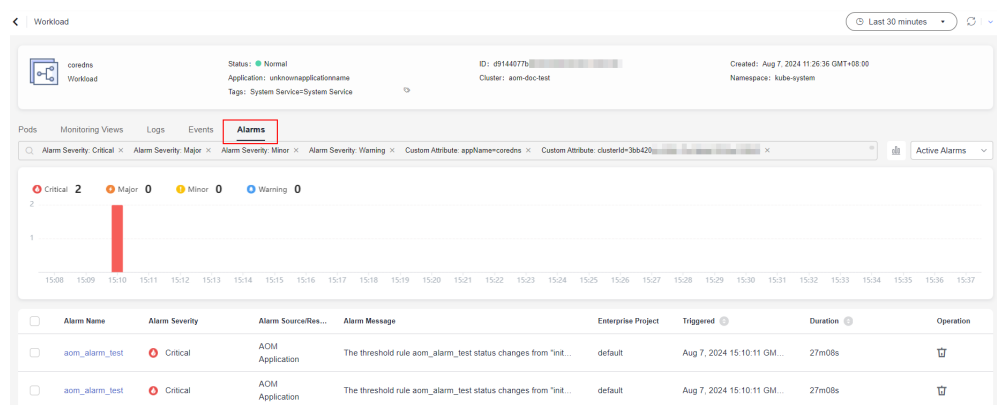
----End

Related Information

After an alarm rule is configured, you can perform the following operations if needed:

- On the workload details page, click the **Alarms** tab to check alarms. Alternatively, choose **Alarm Management > Alarm List** to check alarms. For details, see [Checking Alarms](#).

Figure 1-5 Checking alarms



- Create metric alarm rules using other methods. For details, see [Creating a Metric Alarm Rule](#).

2 Using Prometheus to Monitor ECS Metrics

An Elastic Cloud Server (ECS) is a computing server consisting of the CPU, memory, OS, and Elastic Volume Service (EVS) disk. It supports on-demand allocation and auto scaling. ECSs integrate Virtual Private Cloud (VPC), security group, and Cloud Firewall (CFW) capabilities to create an efficient, reliable, and secure computing environment. This ensures stable and uninterrupted running of services. AOM is a one-stop, multi-dimensional O&M platform for cloud applications. It enables you to monitor real-time running of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency. After an ECS is connected to AOM, AOM can monitor the ECS in real time and send alarm notifications.

This section uses the **node_network_up** metric of an ECS as an example to describe how to use AOM.

Procedure

1. **Manually Installing UniAgent on the ECS:** Manually install UniAgent on the ECS to centrally manage metric collection plug-ins.
2. **Connecting the ECS to AOM:** Collect the ECS metric to AOM through Node Exporter and store it in the Prometheus instance for ECS.
3. **Setting a Metric Alarm Rule:** Create an alarm rule for the ECS metric. If the metric data meets the alarm condition, an alarm will be generated.

Preparation

- You have purchased an ECS. For details, see [Purchasing and Using a Linux ECS](#). If you already have an ECS, skip this step.
- You have [subscribed to AOM 2.0 and granted permissions](#).

Manually Installing UniAgent on the ECS

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Settings**. The **Global Configuration** page is displayed.

- Step 3** Choose **Collection Settings > UniAgent Installation and Configuration** to view the UniAgent status of the host.
- If the UniAgent status is **Running**, UniAgent has been installed. In this case, go to **Connecting the ECS to AOM**.
 - If the UniAgent status is **Abnormal**, UniAgent is abnormal. In this case, contact technical support.
 - If the UniAgent status is **Installing**, UniAgent is being installed. Wait until the UniAgent is installed.
 - If the UniAgent status is **Installation failed** or **Not installed**, UniAgent fails to be installed or is not installed on the host. In this case, install it.
- Step 4** Select the host where UniAgent is to be installed, click **Install UniAgent** in the upper right corner, and then select **Manual**.
- (When you install UniAgent for the first time, the **Manual** page is displayed by default.)
- Step 5** On the **Install UniAgent** page, set parameters.

Figure 2-1 Manually installing UniAgent

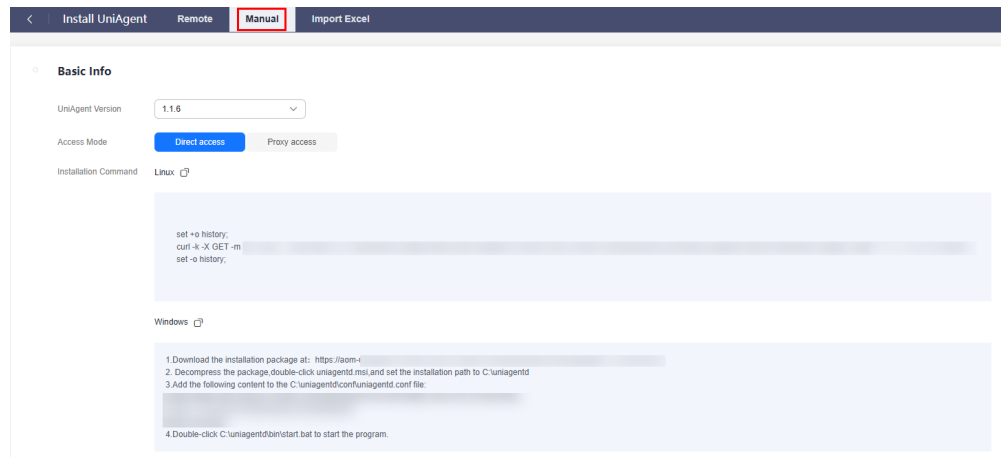



Table 2-1 Parameters for manual installation

| Parameter | Description | Example |
|------------------|---|---------------|
| UniAgent Version | (Mandatory) UniAgent version. | 1.1.6 |
| Access Mode | Mode for connecting to UniAgent. Select Direct access . Direct access : intended for Huawei Cloud hosts. | Direct access |

| Parameter | Description | Example |
|----------------------|--|--------------------------------------|
| Installation Command | <p>Command for installing UniAgent. In this example, copy the Linux installation command.</p> <p>Click  to copy the installation command.</p> <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/ install_uniagent https://aom-uniagent-xxxxxx/ install_uniagent.sh;bash /tmp/install_uniagent -a xxxxxxxx -s xxxxxxxxxxx -p xxxxxx -d https://aom-uniagent- xxxxxx -m https://uniagent.master.cnxxxxxx,https:// xx.xx.xx.xx:xxxx -v 1.x.x -q false set -o history;</pre> | Copy the Linux installation command. |

Step 6 [Log in to the ECS](#) and run the Linux installation command copied in [Step 5](#) as the **root** user.

Step 7 Check the UniAgent status in the UniAgent list. If the UniAgent status is **Running**, the installation is successful.

----End

Connecting the ECS to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation tree on the left, choose **Access > Access Center**.

Step 3 On the **Prometheus Running Environments** panel, click the **Elastic Cloud Server (ECS)** card.

Step 4 On the **Procedure** tab page of the ECS dialog box, perform operations as prompted.

1. Create a Prometheus instance for ECS: Click **Create Instance**. In the displayed dialog box, set related parameters.

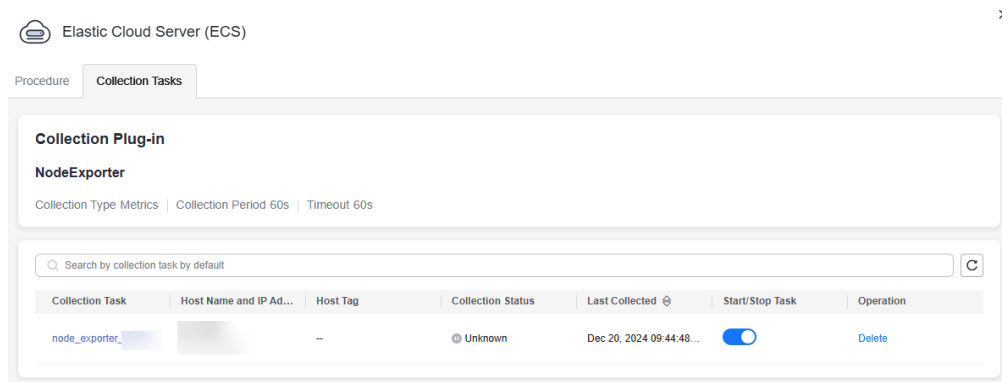
Table 2-2 Parameters for creating a Prometheus instance for ECS

| Parameter | Description | Example |
|---------------|---|---------|
| Instance Name | <p>Prometheus instance name.</p> <p>Enter a maximum of 100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.</p> | mon_ECS |

| Parameter | Description | Example |
|--------------------|---|--------------------|
| Enterprise Project | Enterprise project. - If Enterprise Project is set to All on the global settings page, select an enterprise project from the drop-down list here. - If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. | default |
| Instance Type | Type of a Prometheus instance. | Prometheus for ECS |

2. Select the Prometheus instance for ECS created in [Step 4.1](#) from the drop-down list.
3. Install Node Exporter. Select the target host from the host list and click **Install Exporter**.
4. After the installation is complete, Node Exporter can collect metrics. Click the **Collection Tasks** tab in the ECS dialog box to check the collection task.

Figure 2-2 Checking the collection task



----End

Setting a Metric Alarm Rule

Metric alarm rules can be created in the following modes: **Select from all metrics** and **PromQL**.

The following describes how to create an alarm rule when **Configuration Mode** is set to **Select from all metrics**.

Step 1 In the navigation pane, choose **Alarm Management > Alarm Rules**. Then, click **Create**.

Step 2 Set basic information about the alarm rule by referring to [Table 2-3](#).

Table 2-3 Basic information

| Parameter | Description | Example |
|--------------------|---|-------------|
| Rule Name | Name of the 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. | monitor_ecs |
| Enterprise Project | Select the required enterprise project. The default value is default . | default |
| Description | Description of the rule. Enter up to 1,024 characters. In this example, leave this parameter blank. | - |

Step 3 Set the detailed information about the alarm rule.

1. **Rule Type: Metric alarm rule.**
2. **Configuration Mode: Select from all metrics.** Then you can set alarm conditions for different types of resources.
3. Select the target Prometheus instance from the drop-down list. In this example, select the instance created in **Step 4.1**.
4. Set alarm rule details. **Table 2-4** describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm conditions. You can click **Add Metric** to add more metrics and set the statistical period and detection rules for them.

Figure 2-3 Setting alarm rule details

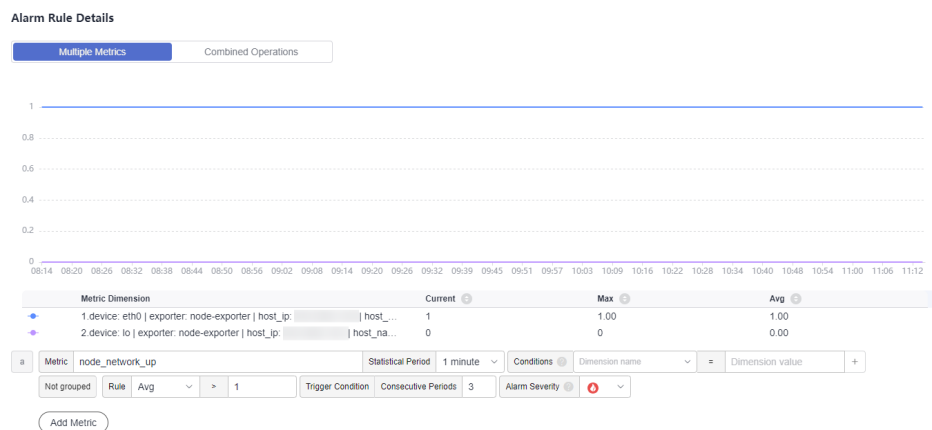







Table 2-4 Alarm rule details



| Parameter | Description | Example |
|------------------|--|------------------|
| 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. | Multiple Metrics |

| Parameter | Description | Example |
|--------------------|--|---|
| Metric | Metric to be monitored. Click the Metric text box. In the resource tree on the right, select a target metric by resource type. | node_net work_up |
| Statistical Period | Interval at which metric data is collected. | 1 minute |
| Conditions | Metric monitoring scope. If this parameter is left blank, all resources are covered. In this example, leave this parameter blank. | - |
| Grouping Condition | Aggregate metric data by the specified field and calculate the aggregation result. | Not grouped |
| Rule | Detection rule of a metric alarm, which consists of the statistical mode (Avg , Min , Max , Sum , and Samples), determination criterion (\geq , \leq , $>$, and $<$), and threshold value. | Avg > 1 |
| Trigger Condition | When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. | 3 |
| Alarm Severity | Severity of a metric alarm. <ul style="list-style-type: none"> - : a critical alarm. - : a major alarm. - : a minor alarm. - : a warning. |  |

Step 4 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 2-5](#).

Table 2-5 Advanced settings

| Parameter | Description | Example |
|-----------------|--|---------------------------|
| Check Interval | Interval at which metric query and analysis results are checked. | Custom interval: 1 minute |
| Alarm Clearance | The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. | 1 |

| Parameter | Description | Example |
|------------------------------------|--|---|
| Action Taken for Insufficient Data | Action to be taken if there is no or insufficient metric data within the monitoring period. Enable this option if needed. | Enabled: If the data is insufficient for 1 period, the status will change to Insufficient data and an alarm will be sent. |
| Alarm Tag | Click  to add an alarm tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |
| Alarm Annotation | Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |

Step 5 Set an alarm notification policy. For details, see [Table 2-6](#).

Figure 2-4 Setting an alarm notification policy

Alarm Notification

Notify When

Alarm triggered Alarm cleared

Alarm Mode

Direct alarm reporting Alarm noise reduction

Frequency

Once

Action Rule

Mon_aom

Table 2-6 Alarm notification policy parameters

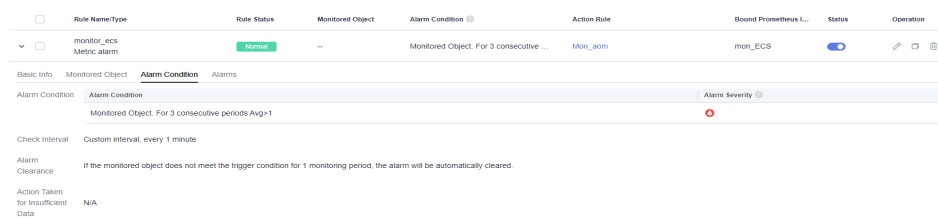
| Parameter | Description | Example |
|-------------|---|---------------------------|
| Notify When | <p>Set the scenario for sending alarm notifications. By default, Alarm triggered and Alarm cleared are selected.</p> <ul style="list-style-type: none"> • Alarm triggered: If the alarm trigger condition 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. | Retain the default value. |

| Parameter | Description | Example |
|------------|--|---|
| Alarm Mode | <ul style="list-style-type: none"> ● 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 desired value from the drop-down list. ● Action Rule: If you enable this function, the system sends notifications based on the associated SMN topic and message template. If there is no alarm action rule you want to select, click Create Rule in the drop-down list to create one. For details, see Setting an Alarm Action Rule. | <ul style="list-style-type: none"> ● Alarm Mode: Select Direct alarm reporting. ● Frequency: Select Once. ● Action Rule: Select Mon_aom. |

Step 6 Click **Confirm**. Then click **View Rule** to view the created 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 the alarm, 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 2-5 Creating a metric alarm rule



----End

Related Information

After an alarm rule is configured, you can perform the following operations if needed:

- Choose **Alarm Management > Alarm List** to check alarms. For details, see [Checking Alarms](#).
- Create metric alarm rules using other methods. For details, see [Creating a Metric Alarm Rule](#).

3 (New) Using Prometheus to Monitor ECS Metrics

An Elastic Cloud Server (ECS) is a computing server consisting of the CPU, memory, OS, and Elastic Volume Service (EVS) disk. It supports on-demand allocation and auto scaling. ECSs integrate Virtual Private Cloud (VPC), security group, and Cloud Firewall (CFW) capabilities to create an efficient, reliable, and secure computing environment. This ensures stable and uninterrupted running of services. AOM is a one-stop, multi-dimensional O&M platform for cloud applications. It enables you to monitor real-time running of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency. After an ECS is connected to AOM, AOM can monitor the ECS in real time and send alarm notifications.

This section uses the `node_network_up` metric of an ECS as an example to describe how to use AOM.

Constraints

The ECS must be in the same region as the AOM console.

Procedure

1. **Installing UniAgent on the ECS:** Install UniAgent on the host in the region where the AOM console is located to centrally manage metric collection plugins.
2. **Creating a Host Group:** Create a host group for better host management and more efficient data collection.
3. **Connecting the ECS to AOM:** Connect an ECS to AOM. Then you can install Node Exporter and configure collection tasks for the host group. The collected metrics will be stored in the Prometheus instance for ECS for easy management.
4. **Setting a Metric Alarm Rule:** Create an alarm rule for the ECS metric. If the metric data meets the alarm condition, an alarm will be generated.

Preparation

- You have purchased an ECS. For details, see [Purchasing and Using a Linux ECS](#). If you already have an ECS, skip this step.

- You have [subscribed to AOM 2.0 and granted permissions](#).

Installing UniAgent on the ECS

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Settings > Collection Settings > UniAgent Installation and Configuration**, and click **Go to New Version** in the upper right corner.

Step 3 On the displayed page, check the UniAgent status of the ECS.

- If the UniAgent status is **Running**, UniAgent has been installed. In this case, go to [Creating a Host Group](#).
- If the UniAgent status is **Abnormal**, UniAgent is abnormal. In this case, contact technical support.
- If the UniAgent status is **Installing**, UniAgent is being installed. Wait until the UniAgent is installed.
- If the UniAgent status is **Installation failed** or **Not installed**, UniAgent fails to be installed or is not installed on the host. In this case, install it.

Step 4 Click **Install UniAgent**. On the displayed page, set related parameters.

Figure 3-1 Installing UniAgent

Select Installation Mode

Server Location

Current region

Outside current region

The network between AOM and the server in the current region is connected.

Server Type

ECSs

Other Servers

Cloud hosts managed by the ECS service.

Installation Mode

CLI

Remotely log in to the server to run the installation command.

OS

Linux

Table 3-1 Installation parameters

| Parameter | Description | Example |
|-----------------------------------|--|--------------------------------------|
| Server Region | Options: Current region and Outside current region . In this example, select Current region . Current region : The network between AOM and the server in the current region is connected. | Current region |
| Server Type | Options: ECSs and Other Servers . Select ECSs . ECSs : hosts managed by the ECS service. | ECSs |
| Installation Mode | Option: CLI . You need to remotely log in to the server to run the installation command provided on the console. | CLI |
| OS | Option: Linux . | Linux |
| UniAgent Version | Select a UniAgent version. The latest version is selected by default. | Latest version |
| Copy and Run Installation Command | Click Copy to copy the installation command. | Copy the Linux installation command. |

Step 5 [Log in to the ECS](#) and run the Linux installation command copied in [Step 4](#) as the **root** user.

Step 6 Check the UniAgent status in the UniAgent list. If the UniAgent status is **Running**, the installation is successful.

----End

Creating a Host Group

You can create host groups of the IP address and custom identifier types. In this example, select the IP address type.

Step 1 In the navigation pane, choose **Settings > Collection Settings > Host Groups** and click **Create Host Group**.

Step 2 On the displayed page, set related parameters.

Table 3-2 Parameters

| Parameter | Description | Example |
|-----------------|---|---------|
| Host Group | Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed. | aom-ecs |
| Host Group Type | Type of the host group. Options: IP and Custom identifier . In this example, select IP . | IP |
| Host Type | Host type. Default: Linux . | Linux |
| Remark | Host group remarks. Enter up to 1,024 characters. In this example, leave this parameter blank. | - |

Step 3 In the host list, select one or more hosts to add to the group and click **OK**.

----End

Connecting the ECS to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access > Access Center**. Click **Experience the new version** in the upper right corner of the page.

Step 3 Locate the **Elastic Cloud Server (ECS)** card under **Running environments** and click **Ingest Metric (AOM)** on the card.

Step 4 Set parameters for connecting to the ECS.

1. Select a Prometheus instance.
 - a. **Instance Type: Prometheus for ECS** is selected by default and cannot be changed.
 - b. **Instance Name:** Click **Create Instance** to create an instance by referring to [Table 3-3](#). Then select the created instance from the drop-down list.

Table 3-3 Parameters for creating a Prometheus instance for ECS

| Parameter | Description | Example |
|---------------|--|---------|
| Instance Name | Prometheus instance name. Enter a maximum of 100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed. | mon_ECS |

| Parameter | Description | Example |
|--------------------|--|--------------------|
| Enterprise Project | Enterprise project. <ul style="list-style-type: none"> ▪ If Enterprise Project is set to All on the global settings page, select an enterprise project from the drop-down list here. ▪ If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. | default |
| Instance Type | Type of a Prometheus instance. | Prometheus for ECS |

2. Select a host group.

In the host group list, select the host group created in [Creating a Host Group](#).

3. Configure the collection.

Under **Configure Collection**, set parameters by referring to the following table.

Table 3-4 Collection configuration

| Category | Parameter | Description | Example |
|------------------------|--------------------------------|--|----------|
| Basic Settings | Configuration Name | Name of a metric ingestion rule. Enter up to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed. | ecs-rule |
| Metric Collection Rule | Metric Collection Interval (s) | Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default). | 60 |
| | Metric Collection Timeout (s) | Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval. | 60 |
| | Executor | User who executes the metric ingestion rule, that is, the user of the selected host group. Default: root . | root |
| Other | Custom Dimensions | Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs). In this example, leave this parameter blank. | - |

| Category | Parameter | Description | Example |
|----------|-------------------------------|--|---------|
| | Import ECS Tags as Dimensions | This function is disabled by default. If it is enabled, ECS tags (key-value pairs) will be written to metric dimensions and tag changes will be synchronized to AOM. | Disable |

Step 5 After the configuration is complete, click **Next**. The ECS is then connected.

----End

Setting a Metric Alarm Rule

Metric alarm rules can be created in the following modes: **Select from all metrics** and **PromQL**.

The following describes how to create an alarm rule when **Configuration Mode** is set to **Select from all metrics**.

Step 1 In the navigation pane, choose **Alarm Management > Alarm Rules**. Then, click **Create**.

Step 2 Set basic information about the alarm rule by referring to [Table 3-5](#).

Table 3-5 Basic information

| Parameter | Description | Example |
|--------------------|---|-------------|
| Rule Name | Name of the 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. | monitor_ecs |
| Enterprise Project | Select the required enterprise project. The default value is default . | default |
| Description | Description of the rule. Enter up to 1,024 characters. In this example, leave this parameter blank. | - |

Step 3 Set the detailed information about the alarm rule.

- Rule Type: Metric alarm rule.**
- Configuration Mode: Select from all metrics.** Then you can set alarm conditions for different types of resources.
- Select the target Prometheus instance from the drop-down list. In this example, select the instance created in [Step 4.1.b](#).
- Set alarm rule details. [Table 3-6](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm conditions. You can click **Add Metric** to add more metrics and set the statistical period and detection rules for them.

Figure 3-2 Setting alarm rule details

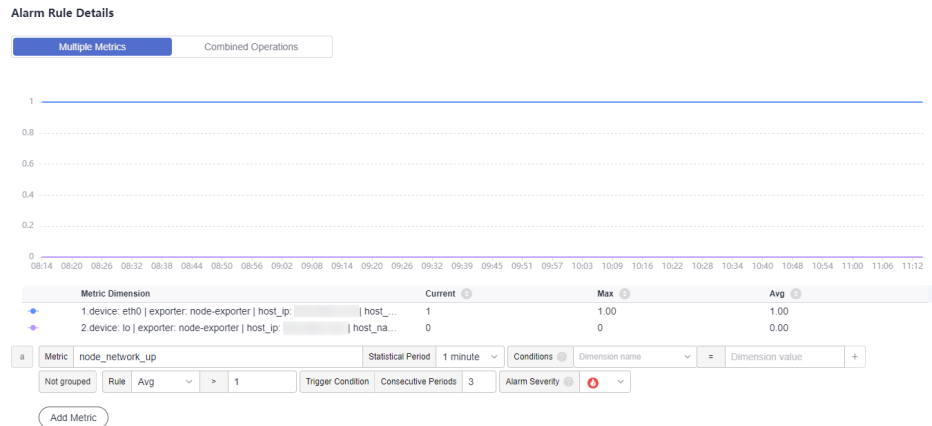









Table 3-6 Alarm rule details

| Parameter | Description | Example |
|--------------------|--|---|
| 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. | Multiple Metrics |
| Metric | Metric to be monitored. Click the Metric text box. In the resource tree on the right, select a target metric by resource type. | node_net work_up |
| Statistical Period | Interval at which metric data is collected. | 1 minute |
| Conditions | Metric monitoring scope. If this parameter is left blank, all resources are covered. In this example, leave this parameter blank. | - |
| Grouping Condition | Aggregate metric data by the specified field and calculate the aggregation result. | Not grouped |
| Rule | Detection rule of a metric alarm, which consists of the statistical mode (Avg , Min , Max , Sum , and Samples), determination criterion (\geq , \leq , $>$, and $<$), and threshold value. | Avg > 1 |
| Trigger Condition | When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. | 3 |
| Alarm Severity | Severity of a metric alarm. <ul style="list-style-type: none"> - : a critical alarm. - : a major alarm. - : a minor alarm. - : a warning. |  |

Step 4 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 3-7](#).

Table 3-7 Advanced settings

| Parameter | Description | Example |
|------------------------------------|---|---|
| Check Interval | Interval at which metric query and analysis results are checked. | Custom interval: 1 minute |
| Alarm Clearance | The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. | 1 |
| Action Taken for Insufficient Data | Action to be taken if there is no or insufficient metric data within the monitoring period. Enable this option if needed. | Enabled: If the data is insufficient for 1 period, the status will change to Insufficient data and an alarm will be sent. |
| Alarm Tag | Click  to add an alarm tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |
| Alarm Annotation | Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations . | - |

Step 5 Set an alarm notification policy. For details, see [Table 3-8](#).

Figure 3-3 Setting an alarm notification policy

Alarm Notification

Notify When

Alarm triggered Alarm cleared

Alarm Mode

Direct alarm reporting Alarm noise reduction

Frequency

Once

Action Rule

Mon_aom  

Table 3-8 Alarm notification policy parameters

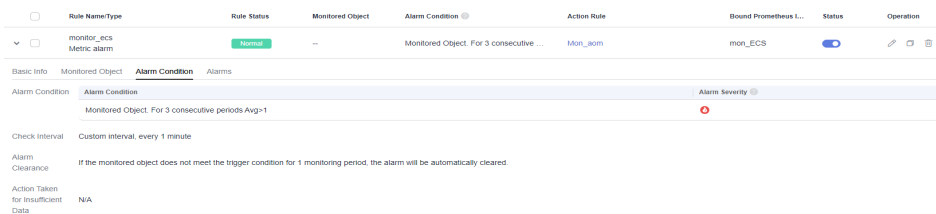
| Parameter | Description | Example |
|-------------|---|---------------------------|
| Notify When | <p>Set the scenario for sending alarm notifications. By default, Alarm triggered and Alarm cleared are selected.</p> <ul style="list-style-type: none"> • Alarm triggered: If the alarm trigger condition 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. | Retain the default value. |

| Parameter | Description | Example |
|------------|--|---|
| Alarm Mode | <ul style="list-style-type: none"> • 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 desired value from the drop-down list. • Action Rule: If you enable this function, the system sends notifications based on the associated SMN topic and message template. If there is no alarm action rule you want to select, click Create Rule in the drop-down list to create one. For details, see Setting an Alarm Action Rule. | <ul style="list-style-type: none"> • Alarm Mode: Select Direct alarm reporting. • Frequency: Select Once. • Action Rule: Select Mon_aom. |

Step 6 Click **Confirm**. Then click **View Rule** to view the created 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 the alarm, 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 3-4 Creating a metric alarm rule



----End

Related Information

After an alarm rule is configured, you can perform the following operations if needed:

- Choose **Alarm Management > Alarm List** to check alarms. For details, see [Checking Alarms](#).
- Create metric alarm rules using other methods. For details, see [Creating a Metric Alarm Rule](#).

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. |