

Application Operations Management

User Guide

Issue 01
Date 2025-01-08



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 Introduction.....	1
2 Access Center.....	7
2.1 Access Center Overview.....	7
3 Dashboard.....	10
3.1 Creating a Dashboard.....	10
3.2 Setting the Full-Screen Online Duration.....	18
3.3 Adding Variables.....	21
3.4 Graph Description.....	22
4 Alarm Management.....	37
4.1 Usage Description.....	37
4.2 Alarm Rules.....	37
4.2.1 Overview.....	37
4.2.2 Creating a Metric Alarm Rule.....	38
4.2.3 Creating an Event Alarm Rule.....	51
4.2.4 Creating a Log Alarm Rule.....	55
4.2.5 Managing Alarm Rules.....	58
4.3 Alarm Templates.....	62
4.4 Checking Alarms.....	72
4.5 Viewing Events.....	74
4.6 Alarm Action Rules.....	74
4.6.1 Overview.....	75
4.6.2 Creating an Alarm Action Rule.....	75
4.6.3 Creating a Message Template.....	77
4.7 Alarm Noise Reduction.....	83
4.7.1 Overview.....	83
4.7.2 Creating a Grouping Rule.....	85
4.7.3 Creating a Suppression Rule.....	89
4.7.4 Creating a Silence Rule.....	92
5 Metric Browsing.....	96
6 Log Analysis.....	101
6.1 Searching for Logs.....	101

6.2 Checking Log Files.....	103
6.3 Configuring VM Log Collection Paths.....	104
6.4 Adding Log Dumps.....	106
6.5 Log Streams.....	110
6.5.1 Searching for Logs.....	110
6.5.2 Quickly Analyzing Logs.....	116
6.5.3 Quickly Querying Logs.....	118
6.5.4 Viewing the Context.....	119
7 Prometheus Monitoring.....	120
7.1 Prometheus Monitoring.....	120
7.1.1 Prometheus Monitoring Overview.....	120
7.1.2 Functions.....	122
7.1.3 Advantages.....	123
7.1.4 Basic Concepts.....	124
7.2 Creating Prometheus Instances.....	126
7.2.1 Prometheus Instance for Cloud Services.....	126
7.2.2 Prometheus Instance for ECS.....	128
7.2.3 Prometheus Instance for CCE.....	129
7.2.4 Common Prometheus Instance.....	131
7.3 Managing Prometheus Instances.....	131
7.4 Configuring a Recording Rule.....	134
7.5 Metric Management.....	136
7.5.1 Configuring Metrics.....	136
7.5.2 Configuring Metric Management for CCE Clusters.....	140
7.6 Dashboard Monitoring.....	143
7.7 Access Guide.....	145
7.7.1 Connecting Node Exporter.....	145
7.7.2 Exporter Access in the VM Scenario.....	147
7.7.2.1 Access Overview.....	147
7.7.2.2 MySQL Component Access.....	147
7.7.2.3 Redis Component Access.....	151
7.7.2.4 Kafka Component Access.....	155
7.7.2.5 Nginx Component Access.....	160
7.7.2.6 MongoDB Component Access.....	164
7.7.2.7 Consul Component Access.....	168
7.7.2.8 HAProxy Component Access.....	172
7.7.2.9 PostgreSQL Component Access.....	176
7.7.2.10 Elasticsearch Component Access.....	180
7.7.2.11 RabbitMQ Component Access.....	184
7.7.2.12 Access of Other Components.....	188
7.7.2.13 Custom Plug-in Access.....	193
7.7.2.14 Other Operations.....	198

7.8 Obtaining the Service Address of a Prometheus Instance.....	199
7.9 Viewing Prometheus Instance Data Through Grafana.....	200
7.10 Reading Prometheus Instance Data Through Remote Read.....	204
7.11 Reporting Self-Built Prometheus Instance Data to AOM.....	206
7.12 Resource Usage Statistics.....	208
8 Business Monitoring (Beta).....	210
8.1 Creating a Log Metric Rule.....	210
9 Infrastructure Monitoring.....	215
9.1 Workload Monitoring.....	215
9.2 Cluster Monitoring.....	217
9.3 Host Monitoring.....	220
9.4 Process Monitoring.....	222
9.4.1 Application Monitoring.....	222
9.4.2 Component Monitoring.....	223
9.4.3 Application Discovery.....	225
10 Settings.....	230
10.1 Cloud Service Authorization.....	230
10.2 Access Management.....	230
10.3 Global Settings.....	231
10.4 Collection Settings.....	232
10.4.1 Overview.....	232
10.4.2 Connecting VMs.....	232
10.4.2.1 Installing a UniAgent.....	232
10.4.2.2 Operating UniAgents in Batches.....	239
10.4.2.3 Operating ICAgent Plug-ins in Batches.....	240
10.4.2.4 Other Operations.....	241
10.4.3 CCE Access.....	242
10.4.4 Managing Host Groups.....	243
10.4.5 Proxy Area Management.....	244
10.4.5.1 Proxy Area.....	244
10.4.5.2 Proxy.....	245
10.4.6 Operation Logs.....	247
10.5 Log Settings.....	248
10.6 Menu Settings.....	250
11 Remarks.....	251
11.1 Alarm Tags and Annotations.....	251
11.2 Prometheus Statements.....	252
11.3 What Is the Relationship Between the Time Range and Statistical Period?.....	256
12 Permissions Management.....	258
12.1 Creating a User and Granting Permissions.....	258

12.2 Creating a Custom Policy.....	259
13 Auditing.....	261
13.1 Operations Logged by CTS.....	261
13.2 Viewing CTS Traces in the Trace List.....	263
14 Subscribing to AOM 2.0.....	267
15 Upgrading to AOM 2.0.....	269
15.1 Manual Upgrade.....	269
15.2 One-click Migration.....	270

1 Introduction

Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform for cloud applications. It provides one-stop observability analysis and automated O&M solutions. By collecting metrics, logs, and performance data from the cloud and local devices, AOM enables you to monitor real-time running status of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency.

Table 1-1 Function description

Category	Description
Overview	Provides quick entries to common services or functions from the container perspective, and monitors and displays key resource or application data in real time.
Access center	At the access center, you can quickly connect multi-dimensional metrics at different layers to AOM in various scenarios. After the connection is complete, you can view the usage of metrics and status of related resources or applications on the Metric Browsing page.
Dashboard	With a dashboard, different resource data graphs can be displayed on the same screen. Various graphs (such as line graphs, digit graphs, and status graphs) help you monitor data comprehensively.

Category	Description
Alarm management	<p>Provides the alarm list, event list, alarm rules, alarm templates, and alarm notifications.</p> <ul style="list-style-type: none"> ● Alarm list Alarms are reported when AOM or an external service is abnormal or may cause exceptions. You need to take measures accordingly. Otherwise, service exceptions may occur. The alarm list displays the alarms generated within a specified time range. ● Event list Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. The event list displays the events generated within a specified time range. ● Alarm rules By setting alarms rules, you can define event conditions for services or threshold conditions for resource metrics. An event alarm is generated when the resource data meets the event condition. A threshold-crossing alarm is generated when the metric data of a resource meets the threshold condition and an insufficient data event is generated when no metric data is reported, so that you can discover and handle exceptions at the earliest time. ● Alarm templates An alarm template is a combination of alarm rules based on cloud services. You can use an alarm template to create threshold alarm rules, event alarm rules, or PromQL alarm rules for multiple metrics of one cloud service in batches. ● Alarm notification AOM supports alarm notification. You can configure alarm notification by creating alarm action rules and noise reduction rules. When an alarm is generated due to an exception in AOM or an external service, the alarm information is sent to specified personnel by email, WeCom, or Short Message Service (SMS). In this way, related personnel can take measures to rectify faults in a timely manner to avoid service loss.
Metric browsing	<p>The Metric Browsing page displays metric data of each resource. You can check metric values and trends, and create alarm rules for desired metrics for real-time monitoring and data correlation analysis.</p>

Category	Description
Log analysis	<p>AOM allows you to search for logs, view log files, set log paths, dump logs, and use log streams.</p> <ul style="list-style-type: none"> • Log search AOM enables you to quickly query logs, and locate faults based on log sources and contexts. • Log files You can quickly view log files of component instances or hosts to locate faults. • Log paths AOM can collect and display VM logs. A VM refers to an Elastic Cloud Server (ECS) running Linux. • Log dumps AOM enables you to dump logs to Object Storage Service (OBS) buckets for long-term storage. • Log streams Supports log search.
Prometheus monitoring	<p>Provides Prometheus instances and resource usage statistics.</p> <ul style="list-style-type: none"> • Instances AOM is fully connected with the open-source Prometheus ecosystem. It monitors many types of components, provides multiple ready-to-use dashboards, and supports flexible expansion of cloud-native component metric plug-ins. • Resource usage After metric data is reported to AOM through Prometheus monitoring, you can view the number of reported basic and custom metric samples on the Resource Usage page.
Business monitoring (beta)	<p>Enables you to create log metric rules.</p>

Category	Description
Infrastructure monitoring	<p>Monitors workloads, clusters, processes, and hosts.</p> <ul style="list-style-type: none"> ● Workload monitoring Workloads deployed on CCE are monitored. Therefore, you can understand the resource usage, status, and alarms of workloads in a timely manner. ● Cluster monitoring Clusters deployed using CCE are monitored. The Cluster Monitoring page displays the pod status and CPU usage of the clusters in real time. ● Host monitoring Host monitoring displays resource usage, trends, and alarms, so that you can quickly respond to malfunctioning hosts and handle errors to ensure smooth host running. ● Process monitoring Provides application and component monitoring, and application discovery. <ul style="list-style-type: none"> - Application monitoring An application groups identical or similar components based on service requirements. - Component monitoring Components refer to the services that you deploy, including containers and common processes. - Application discovery AOM can discover applications and collect their metrics based on configured rules.

Category	Description
Settings	<p>Provides service authorization, authentication, global settings, log settings, collection settings, and menu settings.</p> <ul style="list-style-type: none">• Service authorization Grant the permissions to access multiple cloud services in one click.• Authentication Create an access code for setting API call permissions.• Global settings Determine whether to enable Metric Collection to collect metrics (excluding SLA and custom metrics), and TMS Tag Display to display cloud resource tags in alarm notifications to facilitate fault locating.• Log settings You can set log quotas and ICAgent collection.• Menu settings You can choose to show or hide Overview, Log Stream, and Business Monitoring in the navigation pane of the console.• Collection settings You can install and manage the UniAgent, manage the ICAgent in CCE clusters in a unified manner, manage host groups and proxy areas, and check operation logs of the UniAgent and ICAgent.

Going Back to AOM 1.0

Log in to the AOM 2.0 console and click **Back to 1.0** in the navigation pane to go back to AOM 1.0. For details about AOM 1.0, see [AOM 1.0 User Guide](#).

Enterprise Project

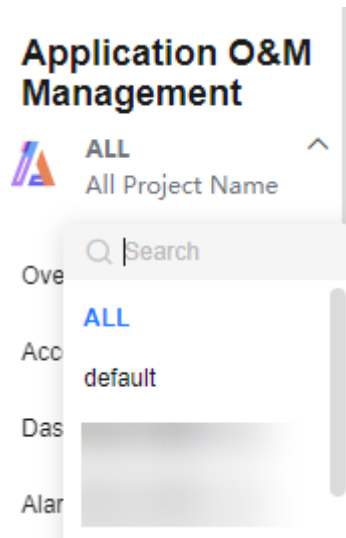
An enterprise project can contain one or more applications.

Log in to the AOM 2.0 console. In the enterprise project drop-down list in the navigation pane, select a desired enterprise project.

NOTE

To use the enterprise project function, contact engineers.

Figure 1-1 Enterprise project



2 Access Center

2.1 Access Center Overview

AOM monitors metric and log data from multiple dimensions at different layers in multiple scenarios. At the access center, you can quickly connect metrics to monitor. After the connection is complete, you can view the metrics and statuses of related resources or applications on the [Metric Browsing](#) page.

Prerequisites

[ELB logs have been ingested to LTS.](#)

Business Access

Obtain extracted ELB logs, transaction monitoring data, or reported custom metrics, such as the number of users and the number of orders.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Business** panel, click a target card.

- Click the **ELB Logs** card. On the displayed page, connect related ELB log metrics. For details, see [8.1 Creating a Log Metric Rule](#).

----End

Prometheus Middleware Access

Connect native or cloud middleware metrics, such as cluster index status, or file system capacity or usage.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Prometheus Middleware** panel, click a target card.

- On the **Procedure** tab page, configure a collection task and install Exporter. For details, see [7.7.2.1 Access Overview](#).

- On the **Collection Tasks** tab page, check, start, stop, edit, and delete the collection tasks of the middleware. For details, see [7.7.2.14 Other Operations](#).

----End

Prometheus Running Environments

This function enables CCE container metrics and ECS metrics to be reported to AOM.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Prometheus Running Environments** panel, click a target card.

- By default, an ICAgent is installed when you purchase a CCE cluster. The ICAgent automatically reports CCE cluster metrics to AOM.

Click the **Cloud Container Engine (CCE) (ICAgent)** card to view the connected CCE cluster metrics. For details about the CCE cluster metrics that are automatically reported to AOM, see [Basic Metrics - VM Metrics](#).

- Click the **ECS ICAgent (Old)** card. In the displayed dialog box, click **Learn more**. On the displayed **VM Access** page, click [Install UniAgent](#) to install a UniAgent on the ECS.

After the UniAgent is installed, ECS metrics are automatically reported to AOM. For details about ECS metrics, see [Basic Metrics - VM Metrics](#).

- Click the **ECS Node Exporter** card. On the displayed page, install Node Exporter. For details, see [7.7.1 Connecting Node Exporter](#).

----End

Prometheus Cloud Services

Connect cloud service metrics, such as the CPU usage, memory usage, and health status.

- ModelArts automatically reports metrics to AOM as ready-to-use data. For details about ModelArts metrics, see [Basic Metrics - ModelArts Metrics](#).
- For details about metrics of other cloud services, such as FunctionGraph, Elastic Volume Service (EVS), Cloud Backup and Recovery (CBR), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Direct Connect, NAT Gateway, Distributed Message Service (DMS), Distributed Cache Service (DCS), Relational Database Service (RDS), Document Database Service (DDS), Data Replication Service (DRS), LakeFormation, MapReduce Service (MRS), GaussDB(DWS), Cloud Search Service (CSS), and Web Application Firewall (WAF), see [Cloud Service Metrics](#).

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Prometheus Cloud Services** panel, click a target cloud service card.

Step 4 In the displayed dialog box, connect the cloud service. For details, see [Connecting Cloud Services](#).

After the cloud service is connected, you can click **View Details** to go to the Prometheus instance details page.

----End

Open-Source Monitoring System Access

This function is suitable for customers who have self-built Prometheus servers, but need Prometheus storage availability and scalability through remote write.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Open-Source Monitoring** panel, click the **Common Prometheus instance** card.

Step 4 In the displayed dialog box, [create a common Prometheus instance](#).

----End

Prometheus API/SDK Access

Connect metric data using APIs.

Custom Prometheus Plug-in Access

Use a custom plug-in to create a collection task to monitor metrics of the component. In addition, use Exporter to report database metrics for exception detection and Grafana dashboard display.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Custom Prometheus Plug-in Access** panel, click **Custom Plug-in**.

Step 4 Set plug-in parameters. For details, see [Creating a Custom Plug-in](#).

Step 5 Click the card of the custom plug-in to be connected.

- Go to the **Create Collection Task** tab page to create a collection task. For details, see [Custom Plug-in Access](#).
- On the **Collection Tasks** tab page, check, start, stop, edit, and delete the collection tasks of the custom plug-in. For details, see [7.7.2.14 Other Operations](#).

----End

3 Dashboard

3.1 Creating a Dashboard

With a dashboard, different graphs (such as line graphs and digit graphs) are displayed on the same screen, so you can view metric data or log data comprehensively.

You can add key resource metrics to a dashboard and monitor them in real time. You can also compare the same metric of different resources on one screen. In addition, you can add routine O&M metrics to a dashboard so that you can perform routine checks without re-selecting metrics when you open AOM again.

Precautions

- Preset dashboard templates are listed under **System**, including the container, native middleware, and application templates. Preset dashboards cannot be deleted. Their groups cannot be changed. Dashboard templates cannot be created.
- Up to 1000 dashboard groups can be created in a region.
- Up to 1000 dashboards can be created in a region.
- A maximum of 30 graphs can be added to a dashboard.
- A maximum of 200 metric data records can be displayed in a line graph.
- A maximum of 12 resources can be added to a digit graph. Only one resource can be displayed. By default, the first resource is displayed.

Creating a Dashboard

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click  next to **Dashboard** to create a dashboard group.

Step 4 Click **Add Dashboard** in the upper left corner of the list.

Step 5 In the displayed dialog box, set parameters.

Table 3-1 Parameters for creating a dashboard

Parameter	Description
Dashboard Name	Name of a dashboard. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'+'<=>?\\"
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • 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.
Group Type	Options: Existing and New . <ul style="list-style-type: none"> • Existing: Select an existing dashboard group from the drop-down list. • New: Enter a dashboard group name to create one. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'+'<=>?\\"

Step 6 Click **OK**.

----End

Adding a Graph to a Dashboard

After a dashboard is created, you can add graphs to the dashboard:

Step 1 In the dashboard list, locate the target dashboard.

Step 2 Go to the dashboard page, and select the Prometheus instance for which you want to add a graph from the drop-down list.

Step 3 Go to the dashboard page. Click **Add Graph** or  in the upper right corner to add a graph to the dashboard. For details about the graphs that can be added to the dashboard, see [3.4 Graph Description](#). The data can be metric, log,. Select a graph as required.

Table 3-2 Parameters for adding a graph

Data Source	How to Add	Scenario
Metric Sources	See Add a metric graph .	Monitors metrics of the business layer, Prometheus middleware, Prometheus running environments, open-source monitoring systems, Prometheus APIs/ SDKs, and custom Prometheus plug-ins.
Log Sources	See Add a log graph .	Monitors business metrics or other log metrics, such as latency, throughput, and errors cleaned based on ELB logs.

- Add a metric graph. Set parameters by referring to [Table 3-3](#). Then click **Save**.

Figure 3-1 Adding a metric graph

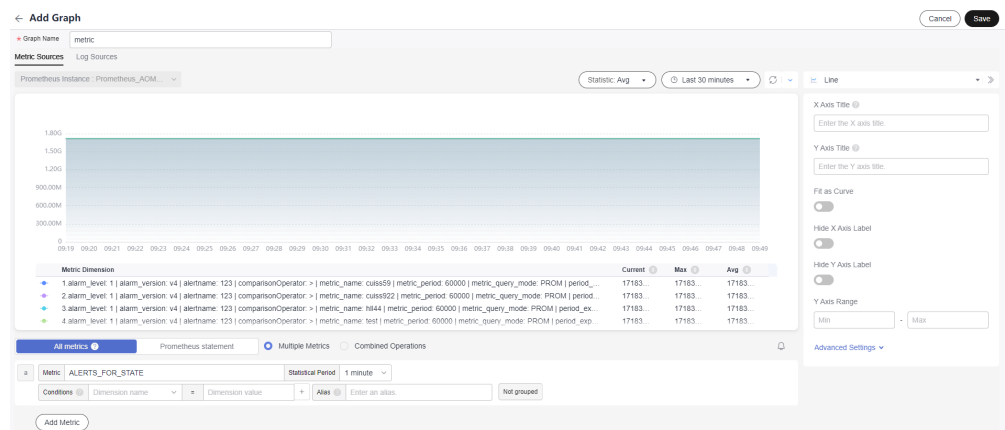










Table 3-3 Adding a metric graph


Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Data Source	Click Metric Sources and select metric data as the source.
Graph Type	Options: line, digit, top N, table, bar, and digital line.

Parameter	Description
Metric List	<p>Add metrics as required. There are the following ways to add metrics:</p> <ul style="list-style-type: none"> – All metrics: Select desire metrics from all metrics. When you select metrics in this mode, you can only enter English keywords to search and only English content is displayed. – Prometheus statement: Enter a Prometheus command and select your target metric. For details, see 11.2 Prometheus Statements. <p>Click Add Metric to add up to 100 metric data records.</p> <p>NOTE</p> <ul style="list-style-type: none"> – When All metrics is selected, enter keywords to search for metrics. – Condition: Metric monitoring scope. The condition is in the key-value pair format. Directly select an option from the drop-down list or use AND and OR to specify conditions for metrics. – Group 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. – Alias: Use a fixed name or variable to display. An alias must be in the format of "<code>{{variable}}</code>". For example, <code>{{host name}}</code>. (Digit graphs, tables, and line graphs do not support aliases.)
Graph Settings	<p>On the right of the page, click the down arrow, select a desired graph type from the drop-down list, and set graph parameters (such as the X axis title, Y axis title, and displayed value). For details about the parameters, see Metric Data Graphs (Line/Digit/Top N/Table/Bar/Digital Line Graphs).</p>
Statistic	<p>Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples.</p>
Statistical Period	<p>Interval at which metric data is collected.</p> <p>The available statistical period options vary according to the time range you select. For details, see What Is the Relationship Between the Time Range and Statistical Period.</p>
Time Range	<p>Time range in which metric data is collected. Options: Last 30 minutes, Last hour, Last 6 hours, Last day, Last week, and Custom.</p>
Refresh Frequency	<p>Interval at which the metric data is refreshed. Options: Refresh manually, 30 seconds auto refresh, 1 minute auto refresh, and 5 minutes auto refresh.</p>

- Add a log graph. Set parameters by referring to [Table 3-4](#). Then click **Save**.

Table 3-4 Log graph parameters

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'+';<=>?\\"
Data Source	Click Log Sources .
Log Group	Select a proper log group from the drop-down list box. If there is no log group you want to select, click Add Log Group to create one. For details, see Table 3-6 .
Log Stream	Select a proper log stream from the drop-down list. If there is no log stream you want to select, click Add Log Stream to create one. For details, see Table 3-6 .
Graph Settings	<ol style="list-style-type: none"> 1. Select the required field from the structured field list and click  next to the field name. 2. Use the default SQL statements in the log graph or enter related query statements in the SQL statement query area as required. 3. Specify the statistical period of log data. Options: Last minute, Last 5 minutes, Last 15 minutes, Last hour, Last 6 hours, Last day, Last week, or Custom. 4. Click Execute Query to query related logs. 5. By default, log data is displayed based on the graph type you set. You can select a graph type as required. <ul style="list-style-type: none"> ▪ Click  to display the current log data in a table. ▪ Click  to display the current log data in a bar graph. ▪ Click  to display the current log data in a line graph. ▪ Click  to display the current log data in a pie graph. ▪ Click  to display the current log data in a number graph. ▪ Click  to display the current log data in a digital line graph. ▪ Click  to display the current log data in a national or provincial map. ▪ You can set the display parameters under a graph. For details, see Log Graphs (Table/Bar/Line/Pie/Number/Digital Line/Map Graphs).








Step 4 Click . The graph is successfully added to the dashboard.














----End













More Operations

After a dashboard is created, you can also perform the operations listed in [Table 3-5](#).

Table 3-5 Related operations

Operation	Description
Setting column display	Click  in the upper right corner of the dashboard list and select or deselect the columns to display.
Adding dashboards to favorites	Locate a dashboard and click  in the Operation column.
Moving dashboards to another group	<ul style="list-style-type: none"> • Moving a dashboard: Locate a dashboard and choose  > Move Group in the Operation column. • Moving dashboards in batches: Select dashboards to move. In the displayed dialog box, click Move Group.
Deleting a dashboard	<ul style="list-style-type: none"> • Deleting a dashboard: Locate a dashboard and choose  > Delete in the Operation column. • Deleting dashboards in batches: Select dashboards to delete. In the displayed dialog box, click Delete.
Changing a dashboard group name	<ol style="list-style-type: none"> 1. In the dashboard list, click a dashboard name. 2. Go to the dashboard page and click a dashboard name in the upper left corner. 3. Move the cursor to the target dashboard group and choose  > Modify to change the group name.
Deleting a dashboard group	<p>You can delete a dashboard using either of the following methods:</p> <p>Method 1:</p> <ol style="list-style-type: none"> 1. In the dashboard list, click a dashboard name. 2. Go to the dashboard page and click a dashboard name in the upper left corner. 3. Move the cursor to the target dashboard group and choose  > Delete. 4. In the displayed dialog box, click OK. <p>Method 2: In the dashboard group list, locate the target dashboard group and choose  > Delete. In the displayed dialog box, click Yes to delete the dashboard group.</p>

Operation	Description
Deleting a graph from a dashboard	<ol style="list-style-type: none"> 1. Click the target dashboard, click  in the upper right corner of the dashboard page, move the cursor to the upper right corner of a graph, and choose  > Delete. 2. Click  to save the setting.
Relocating a graph on a dashboard	<ol style="list-style-type: none"> 1. Click the target dashboard, click  in the upper right corner of the dashboard page, move the cursor to the target graph, and move it to any position in the dashboard. 2. Click  to save the setting.
Full-screen display	Click the target dashboard and click  in the upper right corner of the dashboard page to view the dashboard in full screen.
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  or  , or press Esc on the keyboard.
Manual refresh	Click the target dashboard and click  in the upper right corner of the dashboard page and manually refresh the current page.
Auto refresh	Click the target dashboard and click the arrow next to  in the upper right corner of the dashboard page and enable auto refresh.
Manually refreshing a graph	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Refresh to manually refresh the graph.
Modifying a graph	<ol style="list-style-type: none"> 1. Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Modify to modify the graph. For details, see Adding a Graph to a Dashboard. 2. Modify parameters and click OK. 3. Click  in the upper right corner of the dashboard page to save the setting.

Operation	Description
Adding alarm rules	<ul style="list-style-type: none"> Adding an alarm rule when adding a graph <ol style="list-style-type: none"> Click Add Graph on the page or click  in the upper right corner of the page. After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. For details, see 4.2.2 Creating a Metric Alarm Rule. Adding an alarm rule when modifying a graph <ol style="list-style-type: none"> Locate a target dashboard, move the cursor to the upper right corner of a graph, and choose  > Modify. After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. For details, see 4.2.2 Creating a Metric Alarm Rule.
Displaying a graph in full screen	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Full Screen .
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  , or choose  > Exit Full Screen , or press Esc on the keyboard to exit the full-screen mode.
Rotating dashboards	Click a target dashboard and click  in the upper right corner of the dashboard details page. Set full-screen display by referring to 3.2 Setting the Full-Screen Online Duration .
Setting a dashboard	Click a target dashboard and click  in the upper right corner of the dashboard details page. For details, see 3.3 Adding Variables .
Setting the query time	Select the target dashboard. In the upper right corner of the dashboard page, click the time range next to  and select Last 30 minutes , Last hour , Last 6 hours , Last day , Last week , or Custom from the drop-down list. If you select Custom , select a time range in the calendar that is displayed. The time can be accurate to seconds. Then click OK , so that you can query data in the dashboard based on the selected time range.
Exporting a dashboard	Export the metric graph data of a dashboard in JSON format and save it to your local PC for further analysis. You can export a dashboard using either of the following methods: Method 1: In the dashboard list, locate a dashboard, and choose  > Export Dashboard in the Operation column. Method 2: Click a dashboard to go to its details page and choose  > Export Dashboard in the upper right corner.


Operation	Description
Importing a dashboard	<p>Import the dashboard data in JSON format from a local PC to AOM for analysis. You can import a dashboard using either of the following methods:</p> <p>Method 1: On the Dashboard page, click Import Dashboard.</p> <p>Method 2: In the dashboard group list, locate the group to which the dashboard is to be imported, and choose ... > Import Dashboard.</p> <p>Procedure:</p> <ol style="list-style-type: none"> 1. Select the JSON dashboard file to be imported, upload it or drag it to the upload area in the Import Dashboard dialog box, and then click OK. 2. In the dialog box that is displayed, set information such as the dashboard name by referring to Table 3-1. 3. Click OK.
Exporting a monitoring report	<p>Select the target dashboard, click  in the upper right corner of the Dashboard page, and click Export Line Graph Report to export the line graph as a CSV file for local storage and further analysis..</p>

Table 3-6 Operations related to log graphs

Operation	Description
Creating a log group	<ol style="list-style-type: none"> 1. Enter a log group name. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. Do not start with a period or underscore, or end with a period. 2. Set the log retention duration. The default duration is 7 days. You can set it to up to 30 days. The logs that exceed the retention period will be deleted automatically. You can dump logs to OBS buckets for long-term storage. 3. Click OK.
Creating a log stream	<ol style="list-style-type: none"> 1. Enter a log stream name. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. Do not start with a period or underscore, or end with a period. 2. Click OK.

3.2 Setting the Full-Screen Online Duration

AOM provides an automatic logout mechanism to secure customer information. Specifically, after you access a page on the console but do not perform any operations within 1 hour, the console automatically logs you out.

When an AOM dashboard is used for monitoring in full-screen mode, the full-screen mode will exit when your account logs out. As a result, real-time monitoring cannot be performed. To prevent this, AOM allows you to customize full-screen online duration.

Precautions

- For security purposes, exit the full-screen view when it is not required.
- The full-screen online duration is irrelevant to operations. If the preset duration times out, the login page is automatically displayed.
- The full-screen online duration takes precedence over the automatic logout mechanism of the cloud.

For example, if you log in to the console, set the full-screen online duration to 2 hours on AOM pages, and then open other pages, your setting on the AOM pages also takes effect on other pages. That is, the login page will be automatically displayed 2 hours later.

- If you leave all full-screen views, the default automatic logout mechanism is used.

For example, if you log in to the console, set the full-screen online duration to 2 hours on AOM pages, open other pages, and then leave all full-screen views of AOM, the default logout mechanism will be used. That is, if you do not perform any operations within 1 hour, the login page will be automatically displayed.

Procedure


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Dashboard**.
- Step 3** Click a target dashboard and click  in the upper right corner of the dashboard details page.
- Step 4** In the dialogue box that is displayed, set the full-screen online duration. For details, see [Table 3-7](#).

Figure 3-2 Setting the online duration

Set Full Screen

Online Setting: **Custom** (Always online)

1 hours

Dashboard Rotation:

Rotation Period: 10 s

Dashboard: [i] x [v]

OK Cancel

Table 3-7 Online duration parameters

Parameter	Description
Online Setting	Mode of setting the online duration. Options: <ul style="list-style-type: none"> Custom: After the specified duration expires, the login page will be automatically displayed. Always online: The full-screen online duration is not restricted. That is, you can always implement full-screen monitoring and the login page will never be displayed.
Duration	Full-screen online duration. The duration varies according to the setting mode. <ul style="list-style-type: none"> Custom: The default duration is 1 hour. Range: 1 to 24 hours. For example, if you enter 2 in the text box, the login page will be automatically displayed 2 hours later. Always online: The default value is Always online and cannot be changed.
Dashboard Rotation	Specifies whether to enable dashboard rotation. If this function is enabled, you need to set Rotation Period and Dashboard .
Rotation Period	Period for rotating dashboards. Range: 10s to 120s. Default: 10s.
Dashboard	Dashboard to be rotated. Select one or more dashboards from the drop-down list.

Step 5 Click **OK** to enter the full-screen mode.

----End


3.3 Adding Variables

You can add variables to customize filters when viewing or adding graphs on the **Dashboard** page.

Procedure

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Select a desired dashboard and click  in the upper right corner of the **Dashboard** page. The **Variable Settings** page is displayed.

Step 4 Click **Add Variable** and set parameters by referring to [Table 3-8](#).

Table 3-8 Parameters for adding variables

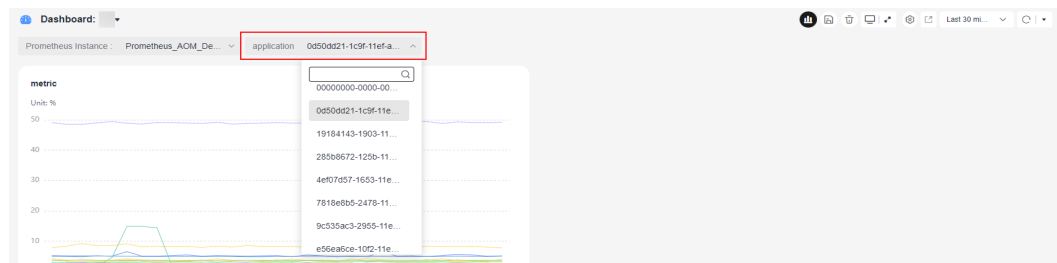
Parameter	Description
Variable Name	Name of a variable. Enter up to 255 characters and do not start or end with an underscore (_). Only digits, letters, and underscores are allowed.
Type	Type of the variable. Only Query is supported.
Alias	Alias of the variable. Enter up to 255 characters and do not start or end with an underscore (_) or hyphens (-). Only digits, letters, hyphens, and underscores are allowed. If you set an alias, it will be preferentially displayed.
Description	Description of the variable.
Data Source	Source of the data. Select a data source on the Dashboard page. It is dimmed here and cannot be selected. You can select a default or custom Prometheus instance. By default, the default Prometheus instance is selected.
Refresh Mode	Filter refresh mode. Only On dashboard load is supported, which means refreshing filters when your dashboard is refreshed.
Metric	Name of a metric. You can select metrics of the selected Prometheus instance.
Display Field	Displayed in a filter drop-down list on a dashboard.
Value	Value of the display field.
Conditions	Dimension name and value. You can set multiple conditions for the same metric.

Parameter	Description
Allow multiple values	Whether multiple values can be selected. By default, this function is disabled. If it is enabled, you can select multiple values for your custom filter.
Include "All"	Whether the All option is available. By default, this function is disabled. If it is enabled, the All option will be added for your custom filter.

Step 5 Click **Save** to add the variable.

The new variable will be displayed as a filter on the dashboard page and the page for adding a graph. You can click the filter and select a desired value from the drop-down list.

Figure 3-3 Checking filters






----End

More Operations

After the variable is added, you can perform the operations listed in [Table 3-9](#) if needed.

Table 3-9 Related operations

Parameter	Description
Searching for a variable	You can search for variables by name. Enter a keyword in the search box above the variable list and click  to search.
Editing a variable	Click  in the Operation column of the target variable. For details, see Table 3-8 .
Deleting a variable	Click  in the Operation column of the target variable. In the displayed dialog box, click Yes .

3.4 Graph Description

The dashboard displays the query and analysis results of metric, log, data in graphs (such as line/digit/status graphs).

Metric Data Graphs (Line/Digit/Top N/Table/Bar/Digital Line Graphs)

- Line graph:** used to analyze the data change trend in a certain period. Use this type of graph when you need to monitor the metric data trend of one or more resources within a period.

You can use a line graph to compare the same metric of different resources. The following figure shows the CPU usage of different hosts.

Figure 3-4 Line graph



Table 3-10 Line graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Fit as Curve	Whether to fit a smooth curve.
	Hide X Axis Label	Whether to hide the X axis label.
	Hide Y Axis Label	Whether to hide the Y axis label.
	Y Axis Range	Value range of the Y axis.
Advanced Settings	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.

Category	Parameter	Description
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- Digit Graph:** used to highlight a single value. Use this type of graph to monitor the latest value of a metric in real time.
 In the following figure, you can view the CPU usage of a host in real time.

Figure 3-5 Digit graph

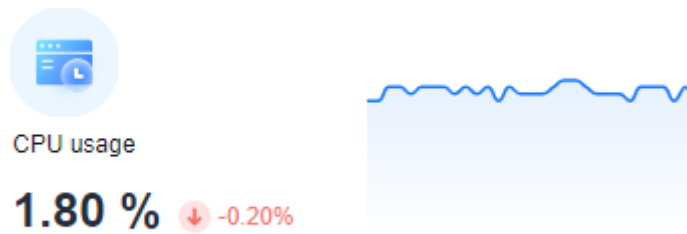


Table 3-11 Digit graph parameters

Parameter	Description
Show Miniature	After this function is enabled, the icon will be zoomed out based on a certain proportion. Also, a line graph is added.

- Top N:** The statistical unit is a cluster and statistical objects are resources such as hosts, components, or instances in the cluster. The top N graph displays top N resources in a cluster. By default, top 5 resources are displayed.
 To view the top N resources, add a top N graph to the dashboard. You only need to select resources and metrics, for example, host CPU usage. AOM then automatically singles out top N hosts for display. If the number of resources is less than N, actual resources are displayed.
 In the following graph, the top 5 hosts with the highest CPU usage are displayed.

Figure 3-6 Top N graph

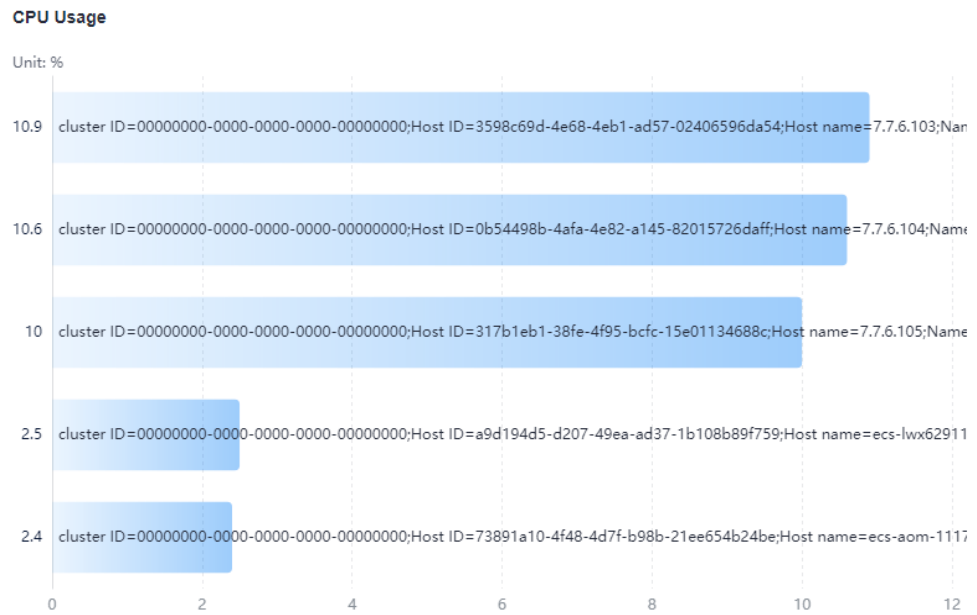


Table 3-12 Top N graph parameters

Category	Parameter	Description
-	Sorting Order	Sorting order of data. Default: Descending .
	Upper Limit	The maximum number of resources to be displayed in the top N graph. Default: 5 .
	Dimension	Metric dimensions to be displayed in the top N graph.
	Column Width	Column width. Options: auto (default), 16 , 22 , 32 , 48 , and 60 .
	Unit	Unit of the data to be displayed. Default: % .
	Display X-Axis Scale	After this function is enabled, the scale of the X axis is displayed.
	Show Value	After this function is enabled, the value on the Y axis is displayed.
Advanced Settings	Display Y-Axis Line	After this function is enabled, the line on the Y axis is displayed.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.

Category	Parameter	Description
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- Table:** A table lists content in a systematic, concise, centralized, and comparative manner, and intuitively shows the relationship between different categories or makes comparison, ensuring accurate display of data.

In the following figure, you can view the CPU usage of different hosts in a table.

Figure 3-7 Table

CPU Usage

Metric Na...	cluster ID	Host ID	Host name	Namespace	Host IP	Node Name	Value
CPU us...	000000...	0b5449...		default			10.3
CPU us...	000000...	195e90...		default			1.6
CPU us...	000000...	317b1e...		default			9.7
CPU us...	000000...	3598c6...		default			10.5

Table 3-13 Table parameters

Parameter	Description
Field Name	Name of a field.
Field Rename	Rename a table header field when necessary.

- Bar graph:** A vertical or horizontal bar graph compares values between categories. It shows the data of different categories and counts the number of elements in each category. You can also draw multiple rectangles for the same type of attributes. Grouping and cascading modes are available so that you can analyze data from different dimensions.

In the following figure, you can view the CPU usage of different hosts.

Figure 3-8 Bar graph

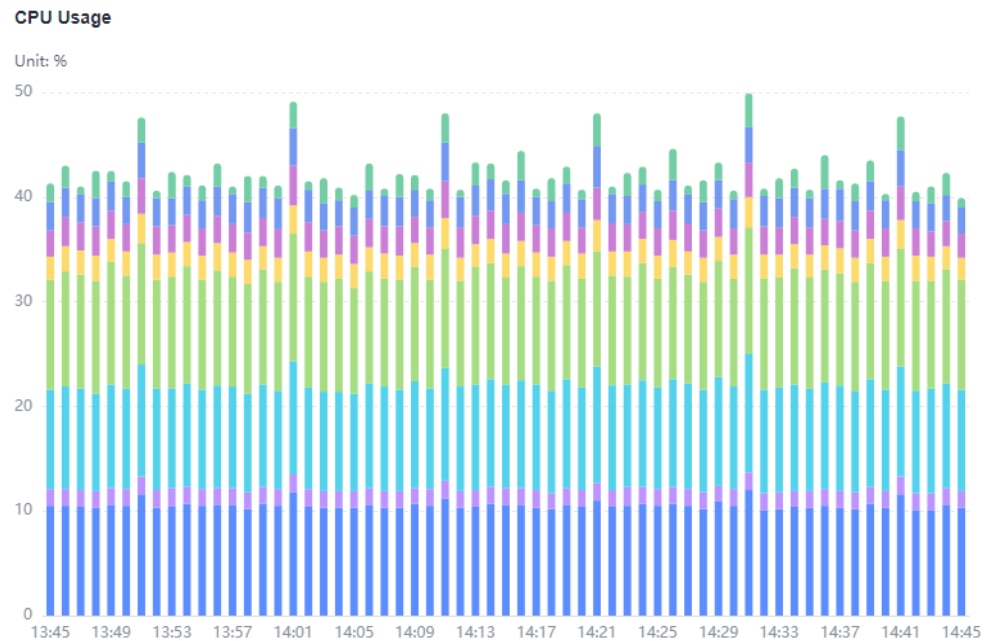


Table 3-14 Bar graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.
	Hide X Axis Label	Whether to hide the X axis label.
	Hide Y Axis Label	Whether to hide the Y axis label.
Advanced Settings	Top Margin	Distance between the axis and the upper boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Digital line graph:** used to analyze the data change trend in a certain period and intuitively display related data. Use this type of graph when you need to monitor the metric data trend of one or more resources within a period.

In the following figure, you can view the CPU usage in different periods in a graph.

Figure 3-9 Digital line graph

CPU

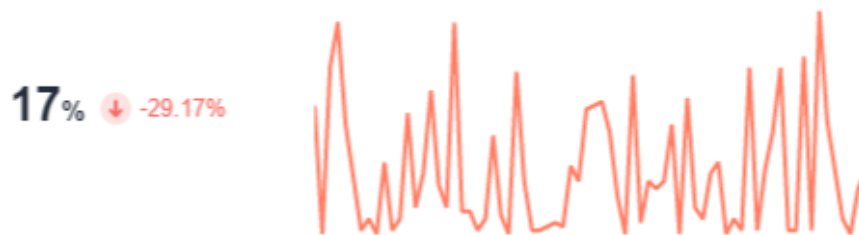


Table 3-15 Digital line graph parameters

Parameter	Description
Fit as Curve	Whether to fit a smooth curve.
Show Legend	Whether to display legends.
Hide X Axis Label	Whether to hide the X axis label.
Hide Y Axis Background Line	Whether to hide the Y axis background line.
Show Data Markers	Whether to display the connection points.

Log Graphs (Table/Bar/Line/Pie/Number/Digital Line/Map Graphs)

- Table:** A table lists content in a systematic, concise, centralized, and comparative manner, and intuitively shows the relationship between different categories or makes comparison, ensuring accurate display of data. In the following figure, you can view the CFW traffic log data in different periods.

Figure 3-10 CFW traffic log table

__time	index_traffic	storage	write_traffic
2023-05-24T12:25:27.168Z	44467383	2527038132	8883476
2023-05-24T11:24:47.157Z	44358652	2488844672	8871730
2023-05-24T10:25:09.668Z	44330367	2452837903	8866073
2023-05-24T09:24:05.031Z	44296782	2415832130	8859356
2023-05-24T08:25:37.788Z	44324126	2378812284	8864825
2023-05-24T07:24:26.084Z	44618146	2341880807	8923829
2023-05-24T06:23:59.712Z	44218670	2304205483	8843714
2023-05-24T05:24:29.515Z	44384107	2267197473	8878821
2023-05-24T04:24:17.947Z	44220921	2230070342	8844184

Table 3-16 Table parameters

Parameter	Description
Records per Page	Number of log events displayed per page. Options: 10 (default), 20 , 30 , and 50 .
Filtering	Filtering allows you to select specific data.
Sorting	Sorting allows you to sort data in ascending or descending order.

- Bar graph:** A vertical or horizontal bar graph compares values between categories. It shows the data of different categories and counts the number of elements in each category. You can also draw multiple rectangles for the same type of attributes. Grouping and cascading modes are available so that you can analyze data from different dimensions.

In the following figure, you can view the average used CPU cores.

Figure 3-11 Bar graph

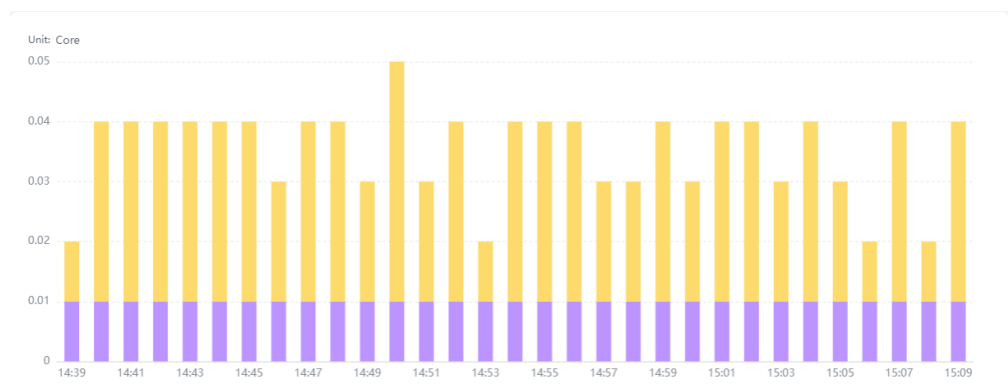


Table 3-17 Bar graph parameters

Category	Parameter	Description
-	X Axis	Select a value from the drop-down list. Generally, a categorical field is used.
	Y Axis	Select a value from the drop-down list. Generally, one or more numbers are selected.
	Graph Type	Both basic and horizontal bar graphs are supported.
	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Hide Legend	After this function is enabled, legends are hidden.
	Show Labels	After this function is enabled, labels are displayed.
	Stacked	After this function is enabled, the Y axis data is displayed in stack mode and labels cannot be shown.
	Sorting Dialog Boxes	Set the sorting order of data. When you move the cursor on the target bar, the data is displayed according to the configured sorting order.
Advanced Settings	Legend Position	Position of a legend in a graph. It can be on the top, bottom, left, or right.
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Line graph:** used to analyze the data change trend in a certain period. Use this type of graph when you need to monitor the log data trend of one or more resources within a period.

In the following graph, you can view the CPU usage.

Figure 3-12 Line graph

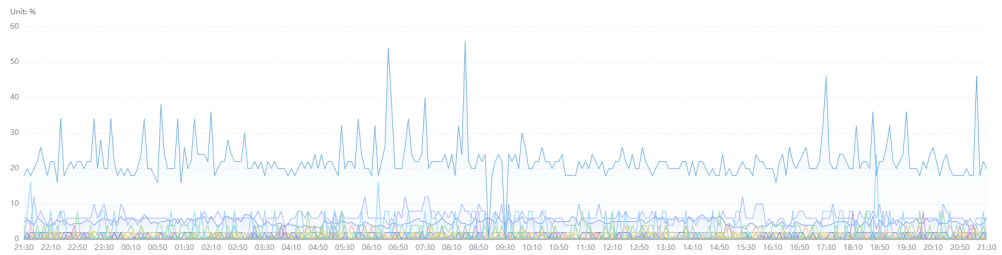


Table 3-18 Line graph parameters

Category	Parameter	Description
-	X Axis	Select a value from the drop-down list. Generally, it is an ordinal variable (time series).
	Y Axis	Select a value from the drop-down list. Generally, one or more numbers are selected.
	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Line Shape	Line type. Options: Straight and Curved .
	Hide Legend	After this function is enabled, legends are hidden.
	Show Data Markers	Whether to display the connection points.
	Dimension	Select a value from the drop-down list. Generally, it is an ordinal variable.
Advanced Settings	Sorting Dialog Boxes	Set the sorting order of data. When you move the cursor on the target bar, the data is displayed according to the configured sorting order.
	Legend Position	Position of a legend in a graph. It can be on the top, bottom, left, or right.
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- Pie graph:** used to show the proportion of different categories. Different categories are compared by radian. A pie is divided into multiple blocks based on the proportion of each category. The entire pie indicates the total volume. Each block indicates the proportion of the category to the total amount. The sum of all blocks is 100%.

As shown in the following figure, you can view the log data of different places.

Figure 3-13 Pie graph

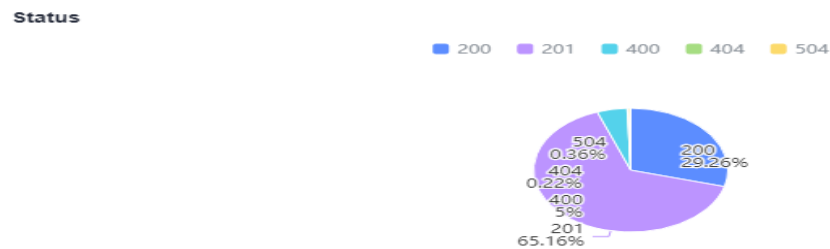


Table 3-19 Pie graph parameters

Category	Parameter	Description
-	Category	Select a value from the drop-down list. Generally, a number or string is selected.
	Value	Select a value from the drop-down list. Generally, a number is selected.
	Label Position	Options: Outside and Inside . This parameter can be set only after you enable Show Labels .
	Shown Categories	Number of data records displayed in the pie graph.
	Coxcomb Chart	After this function is enabled, a Coxcomb chart is displayed.
	Hide Legend	After this function is enabled, the legends on the pie graph are hidden.
	Show Labels	After this function is enabled, the labels on the pie graph are displayed.
Advanced Settings	Legend Position	Position of a legend in a graph. It can be on the top, bottom, left, or right.
	Outer Radius	Outer radius of the pie graph.
	Inner Radius	Inner radius of the pie graph. If the inner radius is not 0 , the pie graph is displayed as a doughnut graph.

Category	Parameter	Description
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Number graph:** used to highlight a single value. Use this type of graph to monitor the latest value of a metric in real time.

As shown in the following figure, the CFW traffic log data is displayed in real time.

Figure 3-14 Number graph

CFW
2023-04-10T07:22:00.000Z **2023-04-10T07:22:00.000Z**

Table 3-20 Number graph parameters

Category	Parameter	Description
-	Data Column	Select a value from the drop-down list. Generally, a number or string is selected.
	Add Comparison Data	After this function is enabled, the comparison data will be displayed.
	Comparison Data	Select a value from the drop-down list. Generally, a number is selected.
	Description	The description of related information can be displayed in the graph.
	Data Unit	Enter a unit based on the selected data column.
	Comparison Data Unit	Set a unit based on the selected comparison data.

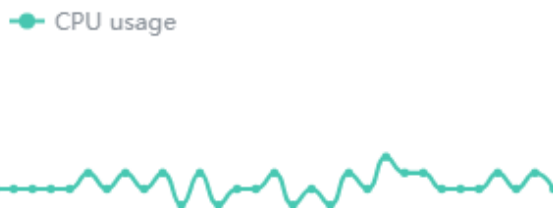
Category	Parameter	Description
Advanced Settings	Number Format	The value of number format can be Number , Percent (%) , or Value + KB, MB , or GB . When a number is greater than or equal to 100,000,000, it will be written in scientific notation and rounded to two digits after the decimal point. For example, if the number is 100,000,000 , it will be written as 10e8 .
	Data Text Size	Set the text size based on your requirements.
	Comparison Data Text Size	Set the text size based on your requirements.
	Unit Text Size	Set the text size based on your requirements.
	Comparison Data Unit Text Size	Set the text size based on your requirements.

- Digital line graph:** used to analyze the data change trend in a certain period and intuitively display related data. Use this type of graph when you need to monitor the log data trend of one or more resources within a period.

In the following figure, you can view the CPU usage in different periods in a graph.

Figure 3-15 Digital line graph

CPU usage



1.5% ↑ 0.00%

Table 3-21 Digital line graph parameters

Category	Parameter	Description
Basic	Data Unit	Select a unit based on the data on the Y axis.
	Number Format	The value of number format can be Number , Percent (%) , or Value + KB , MB , or GB . When a number is greater than or equal to 100,000,000, it will be written in scientific notation and rounded to two digits after the decimal point. For example, if the number is 100,000,000 , it will be written as 10e8 .
	Data Text Size	Set the text size based on your requirements.
	Unit Text Size	Set the text size based on your requirements.
	Background	The background color can be dark or light.
Data	X Axis	Select a value from the drop-down list. Generally, a number or string is selected.
	Y Axis	Select a value from the drop-down list. Generally, a number or string is selected.
Interactions	Line Shape	Line type. Options: Straight and Curved .

- Map:** Log data is displayed by city, state/province, or country. You can compare the same type of logs of different countries, states/provinces, and cities on a map. The following figure shows the log statistics of users in different provinces.

Figure 3-16 Map

PV Distribution (Global)

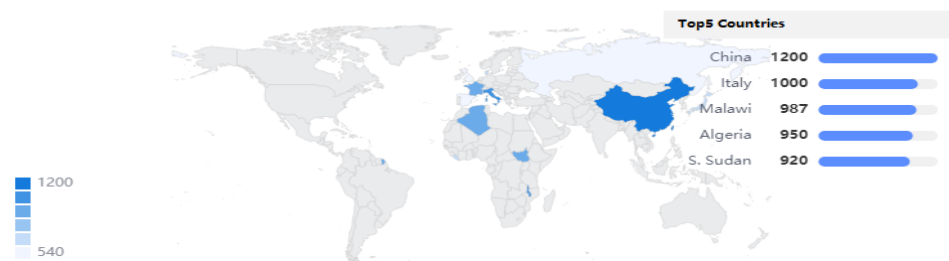


Table 3-22 Map graph parameters

Parameter	Description
Map Type	Select a value from the drop-down list. You can select a provincial map of China, municipal map of China, or world map.
Province	If the map type is set to the provincial map of China, you need to set province information.
City	If the map type is set to the municipal map of China, you need to set city information.
Country/ Region	If the map type is set to the world map, you need to set country or region information.
Data Column	Data corresponding to the location information.

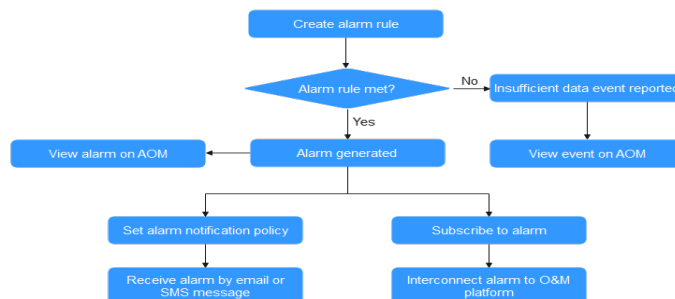
4 Alarm Management

4.1 Usage Description

Alarms are reported when AOM or an external service is abnormal or may cause exceptions. You need to take measures accordingly. Otherwise, service exceptions may occur.

Before using alarm management, ensure that you have installed a UniAgent on your host according to [10.4.2.1 Installing a UniAgent](#). [Figure 4-1](#) shows how to use this function.

Figure 4-1 Process of using alarm management



4.2 Alarm Rules

4.2.1 Overview

AOM allows you to set alarm rules. With alarm rules, you can set event conditions for services, set search analysis, keyword counting, and SQL query for resource

logs, or set threshold conditions for resource metrics. An event alarm is generated when the resource data meets the event condition. If a metric value meets a threshold condition, a threshold alarm will be reported. If there is no metric data, an insufficient data event will be reported. When the log data of a resource meets the preset alarm condition, a log alarm is generated.

Alarm rules are classified into metric alarm rules, event alarm rules, and log alarm rules. Generally, metric/log alarm rules monitor the real-time usage of resources (such as hosts and components) in the environment. When there are too many resource usage alarms and alarm notifications are sent too frequently, you can use event alarm rules to simplify alarm notifications, quickly identify a type of resource usage problems of a service, and resolve the problems in a timely manner.

The total number of alarm rules is 3000. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

4.2.2 Creating a Metric Alarm Rule

You can set threshold conditions in metric alarm rules for resource metrics. If a metric value meets a threshold condition, a threshold alarm will be reported. If there is no metric data, an insufficient data event will be reported.

Function Introduction

- You can set the statistical period, detection rules, and trigger conditions for alarm rules. For details, see [Step 5.4](#).
- You can configure alarm notifications. For details, see [Step 7](#).
- Two alarm notification modes are supported: direct alarm reporting and noise reduction. For details, see [Setting an Alarm Notification Policy](#).

Creation Mode

You can create metric alarm rules in the following ways: [Select from all metrics](#) and [PromQL](#).

Precautions

- If you need AOM to send email or SMS notifications when the metric alarm rule status (**Exceeded**, **Normal**, **Effective**, or **Disabled**) changes, set an alarm action rule according to [4.6.2 Creating an Alarm Action Rule](#).
- Second-level monitoring is supported when you create metric alarm rules by selecting metrics from all metrics or using PromQL. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time.

Creating Metric Alarm Rules by Selecting Metrics from All Metrics

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Rules**.

Step 3 Click **Create Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to [Table 4-1](#).

Table 4-1 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. <ul style="list-style-type: none">• 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 4-2](#) 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 4-2 Setting alarm rule details



Table 4-2 Alarm rule details


Parameter	Description
Multiple Metrics	<p>Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met.</p> <p>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.</p>
Combined Operations	<p>The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered.</p> <p>For example, if there is no metric showing the CPU core usage of a host, do as follows:</p> <ul style="list-style-type: none"> – 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. <p>If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.</p>



Parameter	Description
Metric	<p>Metric to be monitored. When Select from all metrics is selected, enter keywords to search for metrics.</p> <p>Click the Metric text box. In the resource tree on the right, you can also select a target metric by resource type.</p>
Statistical Period	<p>Metric data is aggregated based on the configured statistical period, which can be 15 seconds, 30 seconds, 1 minute, 5 minutes, 15 minutes, or 1 hour.</p>
Condition	<p>Metric monitoring scope. If this parameter is left blank, all resources are covered.</p> <p>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.</p> <ul style="list-style-type: none"> - =: 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. <p>For details about how to enter a regular expression, see Regular Expression Examples.</p> <p>You can also click  and select AND or OR to add more conditions for the metric.</p>
Grouping Condition	<p>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.</p>

Parameter	Description
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. 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	Metric alarm severity. Options: <ul style="list-style-type: none">- : critical alarm.- : major alarm.- : minor alarm.- : warning.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 4-3](#).

Table 4-3 Advanced settings

Parameter	Description
Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <ul style="list-style-type: none"> ● 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. <p>NOTE You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time. For example, if the metric reporting period is 5 seconds, rule check interval is 30 seconds, and notification send time is 1 second, an alarm can be detected and an alarm notification can be sent within 36 seconds.</p> <ul style="list-style-type: none"> ● 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	<p>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 30 consecutive monitoring periods.</p> <p>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.</p>
Action Taken for Insufficient Data	<p>Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements.</p> <p>By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods.</p> <p>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.</p>
Alarm Tag	<p>Click  to add an alarm tag. Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value".</p> <p>For details, see Alarm Tags and Annotations.</p>

Parameter	Description
Alarm Annotation	 Click  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 4-4](#).

Figure 4-3 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

Monitor_host



Table 4-4 Parameters for setting an alarm notification policy

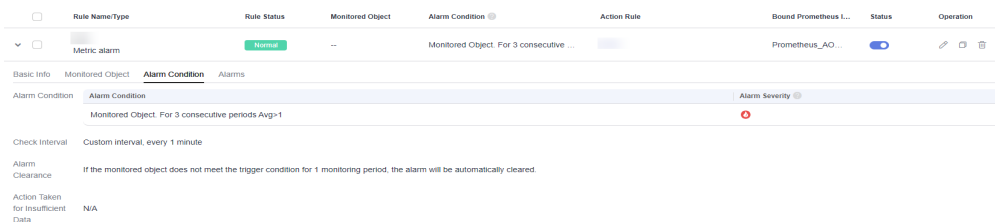
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. <ul style="list-style-type: none"> ● Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. ● Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
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: interval for sending alarm notifications. Select a desired value from the drop-down list. After an alarm action rule is enabled, 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, see Creating 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. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 4.7.2 Creating a Grouping Rule. <p>NOTE The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.</p>

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 4-4 Created metric alarm rule



----End

Creating Metric Alarm Rules by Running Prometheus Statements

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Rules**.

Step 3 Click **Create**.

Step 4 Set basic information about the alarm rule by referring to [Table 4-5](#).

Table 4-5 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. <ul style="list-style-type: none"> 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 **PromQL**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. [Table 4-6](#) 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.

Figure 4-5 Setting alarm rule details

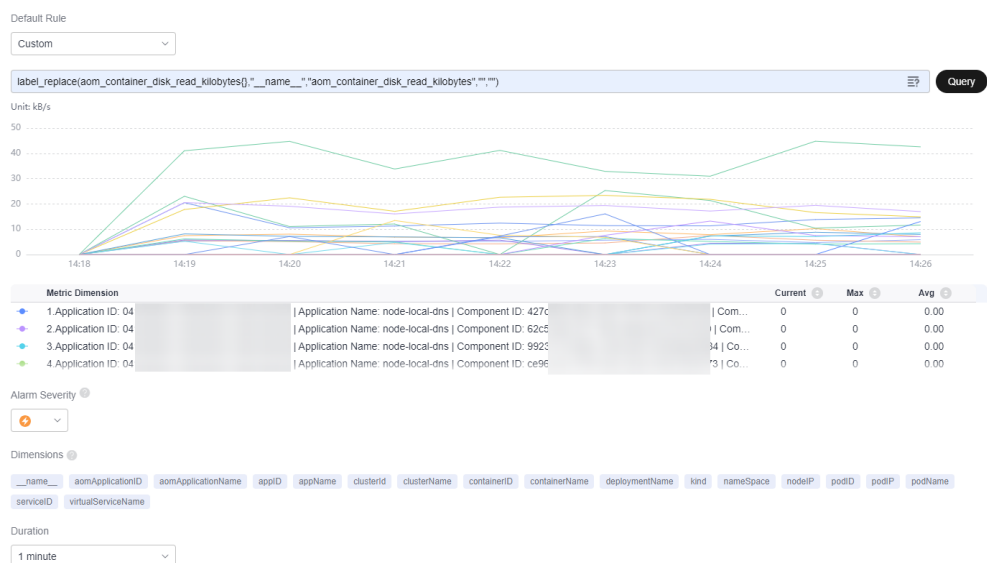









Table 4-6 Alarm rule details

Parameter	Description
Default Rule	<p>Detection rule generated based on Prometheus statements. The system provides two input modes: Custom and CCEFromProm. After the input is complete, click Query. The corresponding graph will be displayed in the lower part of the page in real time.</p> <ul style="list-style-type: none"> - Custom: If you have known the metric name and IP address and are familiar with the Prometheus statement format, select Custom from the drop-down list and manually enter a Prometheus command. - CCEFromProm: used when you do not know the metric information or are unfamiliar with the Prometheus format. Select CCEFromProm from the drop-down list and then select a desired template from the CCE templates. The system then automatically fills in the Prometheus command based on the selected template. <p>You can click  to view examples. For details, see 11.2 Prometheus Statements.</p>
Alarm Severity	<p>Metric alarm severity. Options:</p> <ul style="list-style-type: none"> - : critical alarm. - : major alarm. - : minor alarm. - : warning.
Dimensions	<p>Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.</p>
Duration	<p>A metric alarm will be triggered when the alarm condition is met for the specified duration. Options: Immediate, 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, and 10 minutes. For example, if Duration is set to 2 minutes, a metric alarm is triggered when the default rule condition is met for 2 minutes.</p>

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 4-7](#).

Table 4-7 Advanced settings

Parameter	Description
Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <ul style="list-style-type: none"> • XX hours: Check the query and analysis results every XX hours. • XX minutes: Check the query and analysis results every XX minutes. • XX seconds: Check the query and analysis results every XX seconds. <p>NOTE You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time. For example, if the metric reporting period is 15 seconds, rule check interval is 15 seconds, and notification send time is 3 seconds, an alarm can be detected and an alarm notification can be sent within 33 seconds.</p>
Alarm Tag	<p>Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value".</p> <p>It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click . For details, see 11.1 Alarm Tags and Annotations.</p>
Alarm Annotation	<p>Click  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 11.1 Alarm Tags and Annotations.</p>

Step 7 Set an alarm notification policy. For details, see [Table 4-8](#).

Figure 4-6 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

action-wudong ▼ ↻ 📄

Notification Template ?

Cluster \${cluster_name}/namespace \${namespace}/pod \${pod} has been in the \${phase} status for more than 10 minutes.

Table 4-8 Parameters for setting an alarm notification policy

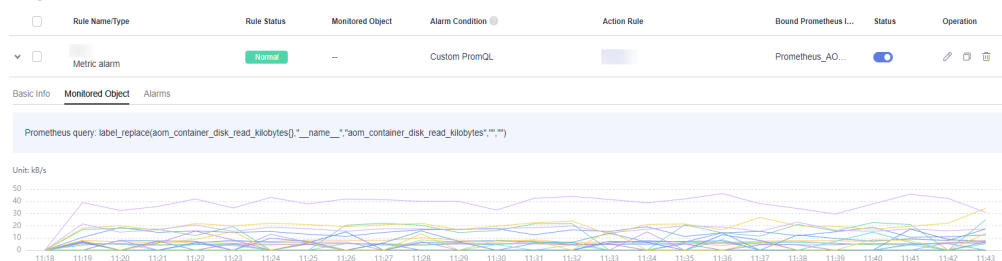
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. <ul style="list-style-type: none"> ● Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. ● Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
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: interval for sending alarm notifications. Select a desired value from the drop-down list. <p>After an alarm action rule is enabled, 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, see Creating an Alarm Action Rule.</p> Alarm noise reduction: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. <p>If you select this mode, the silence rule is enabled by default. You can determine whether to enable Grouping Rule as required. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 4.7.2 Creating a Grouping Rule.</p> <p>NOTE The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.</p>
Notification Template	<p>Template for sending alarm notifications. It is automatically generated based on the Prometheus statement you set.</p> <p>NOTE You can use variables (that is, dimensions) in a notification template. The format is "\$\${Dimension}".</p>

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 4-7 Created metric alarm rule



----End

4.2.3 Creating an Event Alarm Rule

You can set event conditions for services by setting event alarm rules. When the resource data meets an event condition, an event alarm is generated.

Precautions

- If you want to receive email or SMS notifications when the resource data meets the event condition, set an alarm action rule by referring to [4.6.2 Creating an Alarm Action Rule](#).

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** Click **Create**.
- Step 4** Set basic information about the alarm rule by referring to [Table 4-9](#).

Table 4-9 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. <ul style="list-style-type: none">• 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 **Event alarm rule**.
 2. Specify an event type and source.
 - If **Event Type** is set to **System**, **Event Source** can only be **CCE** or **ModelArts**.
 - If **Event Type** to set to **Custom**, select an event source from the existing service list.
 3. Set alarm rule details.

Figure 4-8 Setting alarm rule details

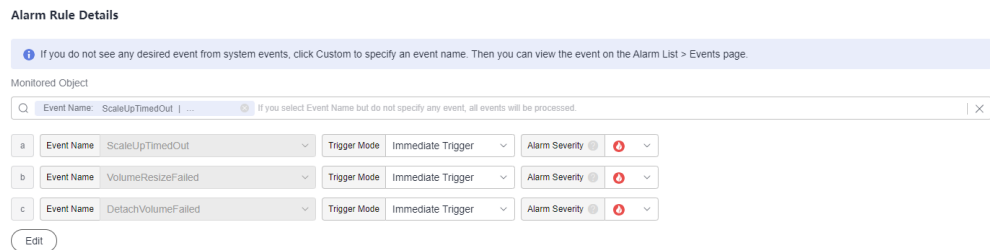






Table 4-10 Alarm rule parameters

Parameter	Description
Monitored Object	<p>Select criteria to filter service events. You can select Notification Type, Event Name, Alarm Severity, Custom Attributes, Namespace, or Cluster Name as the filter criterion. One or more criteria can be selected.</p> <p>NOTE Set Event Name as the filter criterion. If no event name is selected, all events are selected by default.</p>

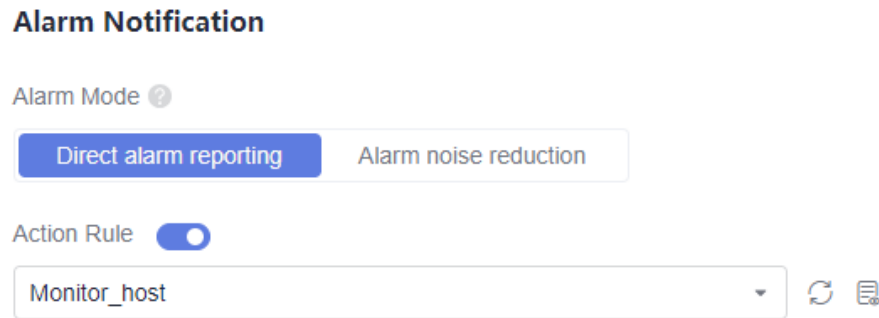
Parameter	Description
Alarm Condition	<p>Condition for triggering event alarms. It contains:</p> <ul style="list-style-type: none"> - Event Name: The value varies depending on Monitored Object. If you do not specify any event for Monitored Object, all events are displayed here and cannot be changed. - Trigger Mode: trigger mode of an event alarm. <ul style="list-style-type: none"> ▪ Accumulated Trigger: When the trigger condition is met for a specified number of times in a monitoring period, alarm notifications are sent based on the preset interval. Assume that you set Event Name to VolumeResizeFailed, Monitoring Period to 20 minutes, Cumulative Times to ≥ 3, and Alarm Frequency to Every 5 minutes. If data volume scale-out fails for 3 or more times within 20 minutes, an alarm notification will be sent every 5 minutes unless the alarm is cleared. NOTICE If you have selected Alarm noise reduction when setting the alarm notification policy, the alarm frequency set here does not take effect. Alarm notifications are sent at the frequency set during noise reduction configuration. ▪ Immediate Trigger: An alarm is immediately generated when the trigger condition is met. - Alarm Severity: Severity of an alarm. <ul style="list-style-type: none"> ▪ : critical alarm. ▪ : major alarm. ▪ : minor alarm. ▪ : warning. <p>In case of multiple events, click Batch Set to set alarm conditions for these events in batches.</p>

Step 6 Set an alarm notification policy. There are two alarm notification modes. Select one as required.

- **Direct alarm reporting:** An alarm is directly sent when the alarm condition is met.

Set whether to enable the alarm action rule as required. The system sends alarm 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 an alarm action rule, see [4.6.2 Creating an Alarm Action Rule](#).

Figure 4-9 Selecting the direct alarm reporting mode



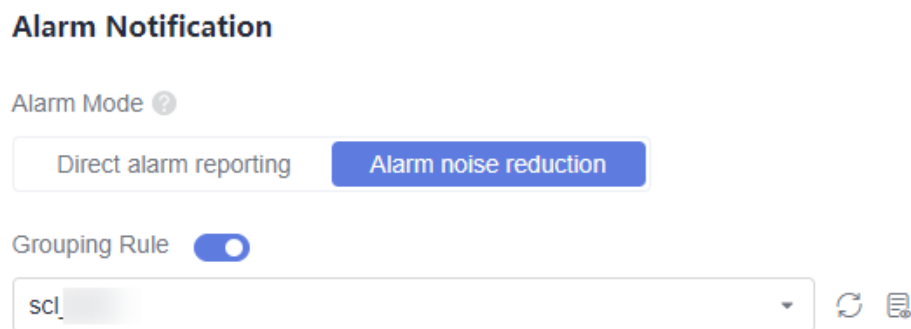
- **Alarm noise reduction:** Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms.

Select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details, see [4.7.2 Creating a Grouping Rule](#).

NOTE

The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.

Figure 4-10 Selecting the alarm noise reduction mode



Step 7 Click **Confirm**. Then click **Back to Alarm Rule List** to view the created alarm rule.

When CCE resources meet the configured event alarm conditions, an event alarm will be generated on the alarm page. To view the alarm, choose **Alarm Management > Alarm List** in the navigation pane. The system also sends alarm notifications to specified personnel by email or SMS.

Figure 4-11 Created event alarm rule

Rule Name/Type	Rule Status	Monitored Object	Alarm Condition	Action Rule	Bound Prometheus L...	Status	Operation
Event alarm	Effective	LTS	All events. An action rule will be imm...		--	On	[Edit] [Copy] [Delete]

Basic info				
Alarm Condition				
Alarm Condition	Event Name	Trigger Mode	Trigger Condition	Alarm Severity
All events		Immediate Trigger	--	0

----End

4.2.4 Creating a Log Alarm Rule

You can create alarm rules based on keyword statistics so that AOM can monitor log data in real time and report alarms if there are any.

Prerequisites

- You have created a log group and log stream. For details, see [Creating Log Groups and Log Streams](#).
- You have structured logs using the new edition of log structuring. For details, see [Log Structuring](#).

Creation Mode

Log alarm rules can be created by referring to [Creating Log Alarm Rules by Keyword](#).

Creating Log Alarm Rules by Keyword

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** In the right pane, click the **Log Alarm Rules** tab and click **Add Log Alarm Rule**.
- Step 4** On the displayed page, set alarm rule parameters by referring to [Table 4-11](#).

Table 4-11 Alarm condition parameters

Category	Parameter	Description
Basic Info	Rule Name	Name of a rule. Enter 1 to 64 characters and do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed. NOTE After an alarm rule is created, the rule name can be modified. After the modification, move the cursor over the rule name to view both new and original rule names.
	Description	Description of the rule. Enter up to 64 characters.
Statistical Analysis	Statistics	By keyword: applicable to scenarios where log alarm rules are created based on the counted keywords.
	Query Condition	Log Group Name: Select a log group. Log Stream Name: Select a log stream. NOTE If a log group contains more than one log stream, you can select multiple log streams when creating a log alarm rule by keyword.

Category	Parameter	Description
		<p>Query Time Range: Specify the statement query period. It is one period earlier than the current time. For example, if Query Time Range is set to one hour and the current time is 9:00, the query statement period is 8:00–9:00.</p> <ul style="list-style-type: none"> • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours. <p>Keywords: Enter keywords that you want AOM to monitor in logs. Exact and fuzzy matches are supported. A keyword is case-sensitive and contains up to 1024 characters.</p>
	Check Rule	<p>Configure a condition that will trigger the alarm.</p> <p>Matching Log Events: When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered.</p> <p>Four comparison operators are supported: greater than (>), greater than or equal to (>=), less than (<), and less than or equal to (<=).</p> <p>Specify the number of queries and the number of times the condition (keyword contained in log events) must be met to trigger an alarm. The number of queries must be greater than or equal to the number of times the condition must be met.</p> <p>NOTE</p> <ul style="list-style-type: none"> • The alarm severity can be Critical (default), Major, Minor, or Info. • Number of queries: 1–10

Category	Parameter	Description
Advanced Settings	Query Frequency	<p>Options:</p> <ul style="list-style-type: none">• Hourly: The query is performed at the top of each hour.• Daily: The query is performed at a specific time every day.• Weekly: The query is performed at a specific time on a specific day every week.• Custom interval: You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the Custom interval is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on. <p>NOTE When the query time range is larger than 1 hour, the interval must be at least 5 minutes.</p> <ul style="list-style-type: none">• CRON: Cron expressions use the 24-hour format and are precise down to the minute. Examples:<ul style="list-style-type: none">- 0/10 * * * *: The query starts from 00:00 and is performed every 10 minutes at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50.- 0 0/5 * * * *: The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00.- 0 14 * * * *: The query is performed at 14:00 every day.- 0 0 10 * *: The query is performed at 00:00 on the 10th day of every month.
	Restores	<p>Configure a policy for sending an alarm clearance notification.</p> <p>If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification will be sent.</p> <p>Number of last queries: 1–10</p>

Category	Parameter	Description
	Notify When	<ul style="list-style-type: none"> • Alarm triggered: Specify whether to send a notification when an alarm is triggered. If this option is enabled, a notification will be sent when the trigger condition is met. • Alarm cleared: Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.
	Frequency	<p>You can select Once, Every 5 minutes, Every 10 minutes, Every 15 minutes, Every 30 minutes, Every hour, Every 3 hours, or Every 6 hours to send alarms.</p> <p>Once indicates that a notification is sent once an alarm is generated. Every 10 minutes indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.</p>
	Alarm Action Rules	<p>Select a desired rule from the drop-down list.</p> <p>If no rule is available, click Create Alarm Action Rule on the right. For details, see 4.6.2 Creating an Alarm Action Rule.</p>
	Languages	Specify the language (English) in which alarms are sent.

Step 5 Click **Confirm**. The alarm rule is created.

----End

4.2.5 Managing Alarm Rules

After an alarm rule is created, you can view the rule name, type, status, and monitored object of the alarm rule in the rule list. You can also modify, enable, or disable the alarm rule as required.

Managing Metric/Event Alarm Rules

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Rules**. The **Metric/Event Alarm Rules** page is displayed.


Step 3 In the rule list, view all created alarm rules and perform the following operations as required. For details, see [Table 4-12](#).

Figure 4-12 Checking alarm rules

Rule Name/Type	Rule Status	Monitored Object	Alarm Condition	Action Rule	Bound Prometheus L...	Status	Operation
> <input type="checkbox"/> Event alarm	Effective	LTS	All events. An action rule will be imm...		--	<input checked="" type="checkbox"/>	
> <input type="checkbox"/> Metric alarm	Normal	--	Monitored Object. For 3 consecutive...		Prometheus_AO...	<input checked="" type="checkbox"/>	
> <input type="checkbox"/> Event alarm	Effective	ACM	All events. If the alarm condition is ...		--	<input checked="" type="checkbox"/>	
> <input type="checkbox"/> Metric alarm	Exceeded	Host 1 monitored object	Current threads number For 1 perio...		Prometheus_AO...	<input type="checkbox"/>	
> <input type="checkbox"/> Metric alarm	Exceeded	--	Monitored Object. For 1 period AvgE...		Prometheus_AO...	<input checked="" type="checkbox"/>	

Table 4-12 Operations related to alarm rules

Operation	Description
Filtering and displaying alarm rules	In the rule list, filter alarm rules by rule name, type, status, or other criteria.
Refreshing alarm rules	Click in the upper right corner of the rule list to obtain the latest information about all alarm rules.
Customizing columns to display	Click in the upper right corner of the rule list and select or deselect the columns to display.
Modifying alarm rules	Click in the Operation column. For details, see 4.2.2 Creating a Metric Alarm Rule and 4.2.3 Creating an Event Alarm Rule .
Copying an alarm rule	Click in the Operation column. For details, see 4.2.2 Creating a Metric Alarm Rule and 4.2.3 Creating an Event Alarm Rule .
Deleting alarm rules	<ul style="list-style-type: none"> To delete an alarm rule, click in the Operation column. To delete one or more alarm rules, select them and click Delete in the displayed dialog box.
Enabling or disabling alarm rules	<ul style="list-style-type: none"> To enable or disable an alarm rule, turn on or off the button in the Status column. To enable or disable one or more alarm rules, select them and click Enable or Disable in the displayed dialog box.
Setting alarm notification policies in batches	Select one or more alarm rules of the same type. In the displayed dialog box, click Alarm Notification to set alarm notification policies in batches. Alarm notification policies vary depending on alarm rule types. For details, see Setting Alarm Notification Policies (1) or Setting Alarm Notification Policies (2) .
Searching for alarm rules	You can search for alarm rules by rule names. Enter a keyword in the search box in the upper right corner and click to search.

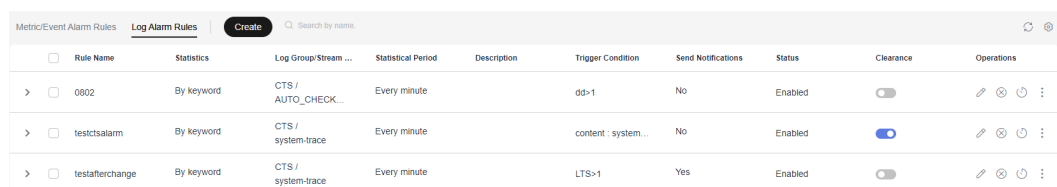
Operation	Description
Viewing detailed alarm information	Click  before a rule name to view rule details, including the basic information and alarm conditions. You can also view the monitored objects and the list of triggered alarms.
Viewing alarms	When the metric value of a resource meets threshold conditions during the configured consecutive periods, the system reports a threshold alarm. In the navigation pane, choose Alarm Management > Alarm List . On the Alarms tab page, view alarms. For details, see 4.4 Checking Alarms .
Viewing events	When no metric data is reported during the configured consecutive periods, the system reports an insufficient data event. In the navigation pane, choose Alarm Management > Alarm List . On the Events tab page, view events. For details, see 4.5 Viewing Events .

----End

Managing Log Alarm Rules


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** Click the **Log Alarm Rules** tab.
- Step 4** In the rule list, view all created alarm rules and perform the operations listed in [Table 4-13](#) if needed.









Figure 4-13 Checking alarm rules



Rule Name	Statistics	Log Group/Stream ...	Statistical Period	Description	Trigger Condition	Send Notifications	Status	Clearance	Operations
> 0802	By keyword	CTS / AUTO_CHECK...	Every minute		dd>1	No	Enabled		
> testctsalarm	By keyword	CTS / system-trace	Every minute		content: system...	No	Enabled		
> testafterchange	By keyword	CTS / system-trace	Every minute		LTS>1	Yes	Enabled		

Table 4-13 Operations related to log alarm rules

Operation	Description
Searching for alarm rules	Enter an alarm rule name to search.
Refreshing alarm rules	Click  in the upper right corner of the rule list to obtain the latest information about all alarm rules.

Operation	Description
Customizing columns to display	Click  in the upper right corner of the rule list and select or deselect the columns to display.
Modifying alarm rules	Click  in the Operation column. For details, see 4.2.4 Creating a Log Alarm Rule . NOTE A rule name can be changed. After they are changed, you can move the cursor to the rule name. Both the new and original names can be viewed.
Disabling alarm rules	<ul style="list-style-type: none"> To disable an alarm rule, click  in the Operation column. To disable one or more alarm rules, select them and click Disable in the displayed dialog box.
Enabling alarm rules	<ul style="list-style-type: none"> To enable an alarm rule, click  in the Operation column. To enable one or more alarm rules, select them and click Enable in the displayed dialog box.
Disabling an alarm rule temporarily	<ul style="list-style-type: none"> For an alarm rule, click  in the Operation column. In the displayed dialog box, set the expiration date. For one or more alarm rules, select them. In the displayed dialog box, click Disable Temporarily.
Re-enabling an alarm rule	Select one or more alarm rules. In the displayed dialog box, click Re-enable .
Copying an alarm rule	To copy an alarm rule, choose  > Copy in the Operation column. For details, see 4.2.4 Creating a Log Alarm Rule .
Deleting alarm rules	<ul style="list-style-type: none"> To delete an alarm rule, choose  > Delete in the Operation column. In the displayed dialog box, click Yes. To delete one or more alarm rules, select them and click Delete in the displayed dialog box.
Enabling/Disabling alarm clearance	<ul style="list-style-type: none"> For an alarm rule, enable or disable the option in the Clearance column. For one or more alarm rules, select them. In the displayed dialog box, click Enable Alarm Clearance or Disable Alarm Clearance.
Viewing detailed alarm information	Click  next to a rule name to view details.

Operation	Description
Viewing alarms	During the configured consecutive periods, if a log data record meets the preset condition, an alarm will be generated. In the navigation pane, choose Alarm Management > Alarm List . On the Alarms tab page, view alarms. For details, see 4.4 Checking Alarms .

----End


4.3 Alarm Templates

An alarm template is a combination of alarm rules based on cloud services. You can use an alarm template to create threshold alarm rules, event alarm rules, or PromQL alarm rules for multiple metrics of one cloud service in batches.

Precautions

You can create up to 150 alarm templates. If the number of alarm templates reaches 150, delete unnecessary templates and create new ones.

Background

AOM presets default alarm templates for key metrics (including CPU usage, physical memory usage, host status, and service status) of all hosts and services. They are displayed on the **Alarm Templates > Default** page. You can locate the desired default alarm template and click  in the **Operation** column to quickly customize your own alarm template.

Creating an Alarm Template

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Templates**.
- Step 3** Click **Create Alarm Template**.
- Step 4** Set the basic information about an alarm template. [Table 4-14](#) describes the parameters.

Table 4-14 Basic information

Parameter	Description
Template Name	Name of an alarm template. 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.

Parameter	Description
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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 template. Enter up to 1024 characters.

Step 5 Add a cloud service to be monitored and an alarm rule to the template.

1. Select a desired cloud service from the drop-down list.
2. Switch to your desired cloud service tab. Then add an alarm rule for the cloud service. For details, see [Table 4-15](#).

Figure 4-14 Adding an alarm rule for the cloud service

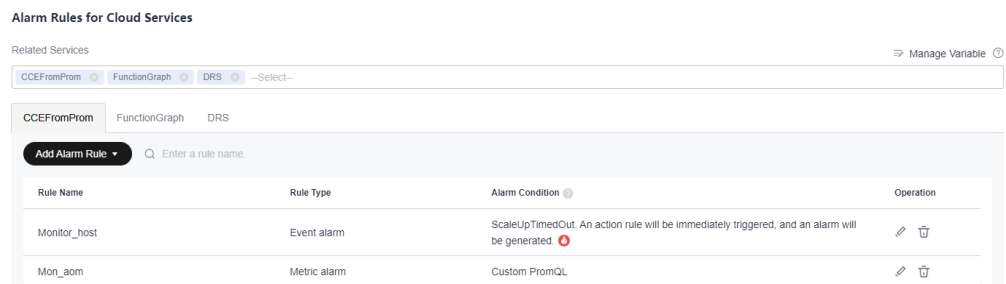


Table 4-15 Parameters for adding an alarm rule for the cloud service

Cloud Service	Alarm Rule Type	Method
FunctionGraph, DRS, RDS, NAT, VPC, DCS, CSS, DC, CBR, DMS, ELB, EVS, OBS, DDS, and WAF	Metric alarm rule	<ol style="list-style-type: none"> 1. Click Add Threshold Alarm Rule. 2. In the displayed Create Rule dialog box, set a rule name, metric, and alarm condition. For details, see Step 5.4 and Step 6 in Creating Metric Alarm Rules by Selecting Metrics from All Metrics. 3. Click OK.
CCEFromProm	Event alarm rule	See Step 6 .
	PromQL alarm rule	See Step 7 .

Step 6 (Optional) Add an event alarm rule for the CCEFromProm service.

1. Choose **Add Alarm Rule > Add Event Alarm Rule**.


2. In the displayed dialog box, set the rule name and event rule details. For details, see [Table 4-16](#).
 - You can click **Add Event** to add more events and set information such as the trigger mode and alarm severity for the events.
 - In case of multiple events, click **Batch Set** to set alarm conditions for these events in batches.
 - Click  next to the event details to copy them and then modify them as required.

Figure 4-15 Adding an event alarm rule

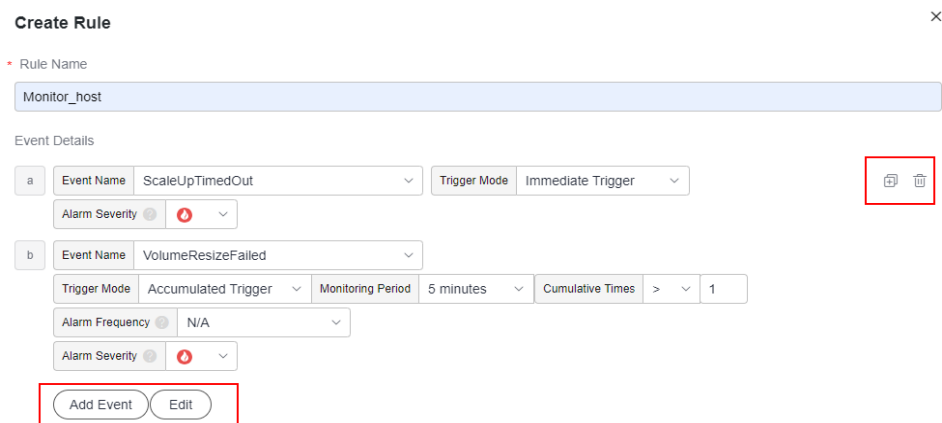






Table 4-16 Event rule parameters

Parameter	Description
Rule Name	Enter a maximum of 256 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Event Name	Select a value from the drop-down list. By default, all events are selected.
Trigger Mode	Trigger mode of an event alarm. <ul style="list-style-type: none"> - Accumulated Trigger: When the trigger condition is met for a specified number of times in a monitoring period, alarm notifications are sent based on the preset interval. Assume that you set Event Name to VolumeResizeFailed, Monitoring Period to 20 minutes, Cumulative Times to 3, and Alarm Frequency to Every 5 minutes. If data volume scale-out fails three times within 20 minutes, an alarm notification will be sent every five minutes unless the alarm is cleared. - Immediate Trigger: An alarm is immediately generated when the trigger condition is met.

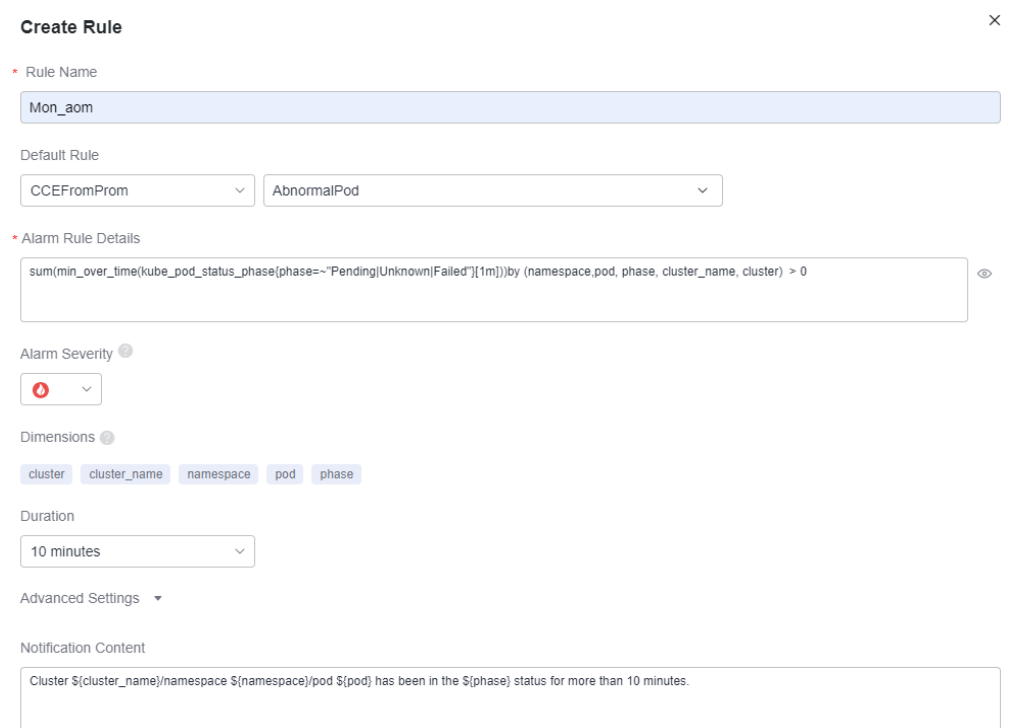
Parameter	Description
Alarm Severity	Severity of an event alarm. <ul style="list-style-type: none"> - : critical alarm. - : major alarm. - : minor alarm. - : warning.

3. Click **OK**.

Step 7 (Optional) Add a PromQL alarm rule for the CCEFromProm service.

1. Choose **Add Alarm Rule > Add PromQL Alarm Rule**.
2. In the displayed dialog box, set the rule name, default rule, and alarm severity. For details, see [Table 4-17](#).

Figure 4-16 Adding a PromQL alarm rule



Create Rule ×

* Rule Name

Default Rule

* Alarm Rule Details

Alarm Severity ?

Dimensions ?








Duration



Advanced Settings ▼

Notification Content

Table 4-17 PromQL alarm rule parameters

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

Parameter	Description
Default Rule	<p>Detection rule generated based on Prometheus statements. The system provides two input modes: Custom and CCEFromProm.</p> <ul style="list-style-type: none"> - Custom: If you have known the metric name and IP address and are familiar with the Prometheus statement format, select Custom from the drop-down list and manually enter a Prometheus command. - CCEFromProm: used when you do not know the metric information or are unfamiliar with the Prometheus format. Select CCEFromProm from the drop-down list and then select a desired template from the CCE templates. The system then automatically fills in the Prometheus command based on the selected template. <p>NOTE</p> <p>Click  next to the alarm rule details to lock the content. Then you can perform the following operations:</p> <ul style="list-style-type: none"> - Click  next to the alarm rule details to unlock the content. - Click  next to the alarm rule details to copy the Prometheus statement. <p>For details, see 11.2 Prometheus Statements.</p>
Alarm Severity	<p>Severity of a metric alarm.</p> <ul style="list-style-type: none"> - : critical alarm. - : major alarm. - : minor alarm. - : warning.
Dimensions	<p>Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.</p>
Duration	<p>A metric alarm will be triggered when the alarm condition is met for the specified duration. Options: Immediate, 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, and 10 minutes. For example, if Duration is set to 2 minutes, a metric alarm is triggered when the default rule condition is met for 2 minutes.</p>

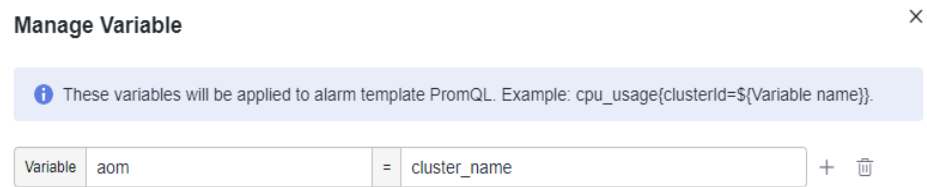
Parameter		Description
Advanced Settings	Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <ul style="list-style-type: none"> - XX hours: Check the query and analysis results every XX hours. - XX minutes: Check the query and analysis results every XX minutes. - XX seconds: Check the query and analysis results every XX seconds. <p>NOTE You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time.</p> <p>For example, if the metric reporting period is 15 seconds, rule check interval is 15 seconds, and notification send time is 3 seconds, an alarm can be detected and an alarm notification can be sent within 33 seconds.</p>
	Alarm Tag	<p>Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value".</p> <p>It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click . For details, see 11.1 Alarm Tags and Annotations.</p> <p>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.</p>
	Alarm Annotation	<p>Click  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 11.1 Alarm Tags and Annotations.</p>
Notification Content		Alarm notification content. It is automatically generated based on the Prometheus statement you set.

3. Click **OK**.

Step 8 (Optional) Manage variables. When adding a PromQL alarm rule to the CCEFromProm service, manage variables and apply them to the alarm template PromQL.

1. Click **Manage Variable**.
2. In the displayed dialog box, set variable names and values. A maximum of 50 variables can be added.

Figure 4-17 Managing variables



3. Click **OK**.

Step 9 Click **OK** to create the alarm template.

Step 10 (Optional) In the displayed **Bind Alarm Template with Prometheus Instance/Cluster** dialog box, set the cluster or Prometheus instance to be bound with the alarm template. For details about the parameters, see [Table 4-18](#). After the setting is complete, click **OK**.

Figure 4-18 Binding an alarm template with a Prometheus instance or cluster

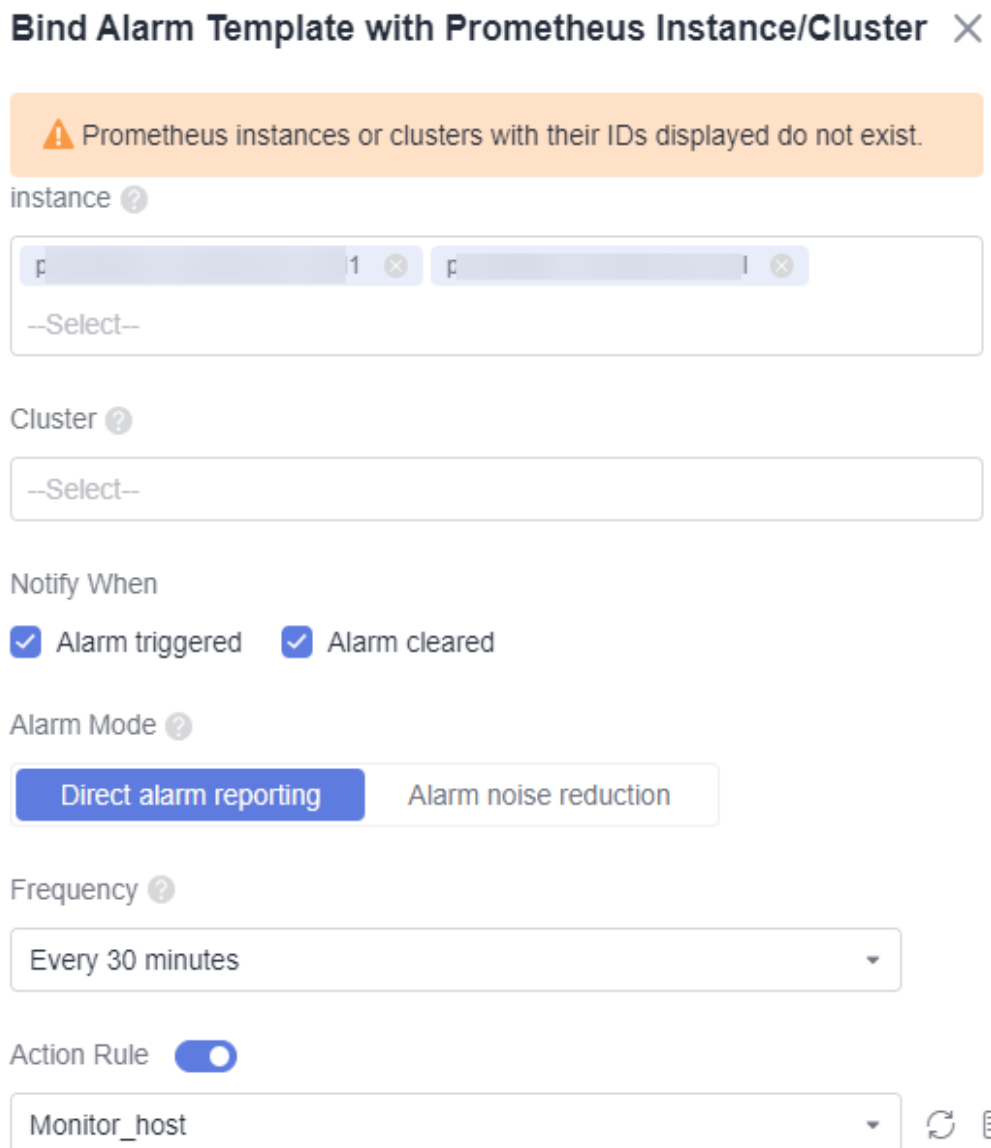


Table 4-18 Parameters for binding an alarm template

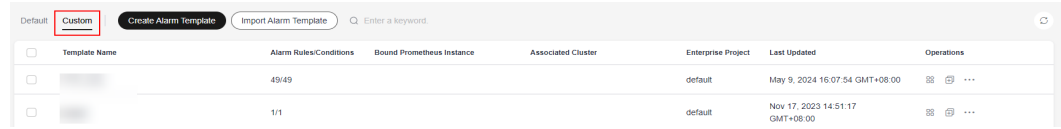
Parameter	Description
Instance	<p>This parameter is optional. If the cloud services selected in Step 5.1 contain services other than CCEFromProm, this parameter will be displayed.</p> <p>The drop-down list displays all Prometheus instances for cloud services under your account. Select your desired instance.</p>
Cluster	<p>This parameter is optional. If the cloud services selected in Step 5.1 contain CCEFromProm, this parameter will be displayed.</p> <p>The drop-down list displays all CCE clusters of your account. Select your desired cluster.</p>
Notify When	<p>Set the scenario for sending alarm notifications.</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.
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: interval for sending alarm notifications. Select a desired value from the drop-down list. After an alarm action rule is enabled, 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, see Creating 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. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 4.7.2 Creating a Grouping Rule. <p>NOTE The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.</p>

Step 11 View the created alarm template on the **Custom** tab page.

If a resource or metric meets the alarm condition set in the alarm template, an alarm will be triggered. In the navigation pane, choose **Alarm Management** >

Alarm List to view the alarm. The system also sends alarm notifications to specified personnel by email or SMS.

Figure 4-19 Creating an alarm template



Template Name	Alarm Rules/Conditions	Bound Prometheus Instance	Associated Cluster	Enterprise Project	Last Updated	Operations
	49/49			default	May 9, 2024 16:07:54 GMT+08:00	⊞ ⊞ ...
	1/1			default	Nov 17, 2023 14:51:17 GMT+08:00	⊞ ⊞ ...

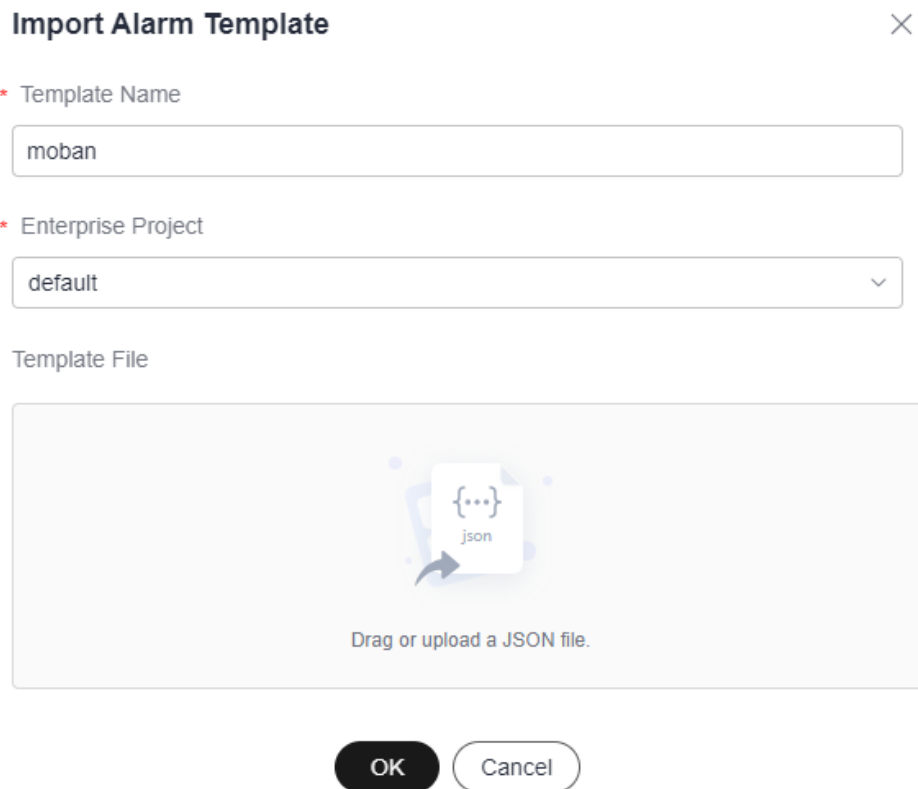
----End

Importing an Alarm Template

You can quickly create an alarm template by importing a template file.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Templates**.
- Step 3** Click **Import Alarm Template**.
- Step 4** In the displayed dialog box, set parameters. For details, see [Table 4-19](#). Click **OK**.

Figure 4-20 Importing an alarm template

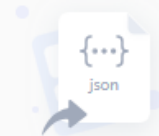


Import Alarm Template ✕

* Template Name

* Enterprise Project

Template File



Drag or upload a JSON file.

Table 4-19 Parameters for importing an alarm template

Parameter	Description
Template Name	Name of an alarm template. 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.
Enterprise Project	Enterprise project. Select a value from the drop-down list.
Template File	Directly upload or drag a JSON file to the box to upload.



Step 5 View the created alarm template on the **Custom** tab page.



----End

More Operations

After the alarm template is created, you can also perform the operations listed in [Table 4-20](#).

Table 4-20 Related operations

Operation	Description
Checking an alarm template	In the template list, check the information such as Template Name , Alarm Rules/Conditions , Associated Cluster , and Enterprise Project .
Binding an alarm template with a Prometheus instance or cluster	Click  in the Operation column. For details, see Step 10 .
Modifying an alarm template	Choose ... > Edit in the Operation column. For details, see Creating an Alarm Template .
Exporting a custom alarm template	Choose ... > Export in the Operation column.
Copying an alarm template	Click  in the Operation column.
Deleting an alarm template	<ul style="list-style-type: none"> To delete an alarm template, choose ... > Delete in the Operation column. To delete one or more alarm templates, select them and click Delete in the displayed dialog box.

Operation	Description
Searching for an alarm template	Enter a template name in the search box in the upper right corner and click  .
Viewing alarm rules created using a template	In the navigation pane on the left, choose Alarm Management > Alarm Rules . Enter a template name keyword in the search box above the alarm rule list and click  . If an alarm template has been bound with a Prometheus instance or cluster, you can also search for the alarm rule by the bound Prometheus instance or cluster name.
Viewing alarms	When the metric value of a resource meets an alarm condition, an alarm will be generated. In the navigation pane, choose Alarm Management > Alarm List . On the Alarms tab page, view alarms. For details, see 4.4 Checking Alarms .
Viewing events	When no metric data is reported during the configured consecutive periods, the system reports an insufficient data event. In the navigation pane, choose Alarm Management > Alarm List . On the Events tab page, view events. For details, see 4.5 Viewing Events .

4.4 Checking Alarms

Alarms are reported when AOM or an external service is abnormal or may cause exceptions. You need to take measures accordingly. Otherwise, service exceptions may occur. The **Alarms** tab page allows you to query and handle alarms, so that you can quickly detect, locate, and rectify faults.

Function Introduction

The alarm list provides the following key functions:

- Alarm list: View alarm information by alarm severity in a graph.
- Advanced filtering: You can filter alarms by alarm severity, source, or keyword in the search box. By default, alarms are filtered by alarm severity.
- Alarm clearance: Clear alarms one by one or in batches.
- Alarm details: View the alarm object and handling suggestions in the alarm details. Handling suggestions are provided for all alarms.

Procedure


Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Alarm Management > Alarm List**.

Step 3 Click the **Alarms** tab to view the alarm information.

1. Set a time range to view alarms. There are two methods to set a time range:
Method 1: Use a predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.

Method 2: Specify the start time and end time (max. 31 days).



2. Set the interval for refreshing alarms. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

3. Set filter criteria and click  to check the alarms generated in the period. You can filter alarms by alarm severity, source, or keyword in the search box. By default, alarms are filtered by alarm severity.

If you want to filter alarms by custom attribute, select **Custom Attribute** and enter "custom attribute name=custom attribute value". For example, you specify custom attribute **nodeIP=192.168.0.106**, the alarms of the host whose IP address is **192.168.0.106** within the specified time range will be filtered.

Step 4 Perform the operations listed in [Table 4-21](#) as required:

Table 4-21 Operations

Operation	Description
Viewing alarm statistics	Click  , and view alarm statistics that meet filter criteria within a specific time range on a bar graph.
Clearing alarms	<ul style="list-style-type: none"> • To clear an alarm, click  in the Operation column of the target alarm. • To clear one or more alarms, select them and click Clear in the displayed dialog box. <p>NOTE You can clear alarms after the problems that cause them are resolved.</p>
Viewing alarm details	<p>Click an alarm name to view alarm details, including alarm information and handling suggestions. You can also view a bound alarm action rule or alarm noise reduction rule if there is any.</p> <p>NOTE</p> <ul style="list-style-type: none"> • On the Alarm Info tab page, click the alarm rule, log group, or log stream in blue to drill down to check details.
Viewing cleared alarms	Click Active Alarms in the upper right corner and select Historical Alarms from the drop-down list to view alarms that have been cleared.

----End

4.5 Viewing Events



Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. You can handle events as required. The **Events** tab page allows you to quickly search for events and monitor your system.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm List**.


Step 3 Click the **Events** tab to view the event information.

1. Set a time range to view events. There are two methods to set a time range:
 - Method 1: Use the predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.
 - Method 2: Specify the start time and end time to customize a time range. You can specify 31 days at most.
2. Set the event refresh interval. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
3. Set filter criteria and click  to check the events generated in the period. You can filter events by event severity, resource type, or event source in the search box. By default, events are filtered by event severity.

If you want to filter alarms by custom attribute, select **Custom Attribute** and enter "custom attribute name=custom attribute value". For example, if you specify custom attribute **clusterId=ee-643f-XXXX-XXXX-XXXXXXXX**, the events of the cluster whose ID is *ee-643f-XXXX-XXXX-XXXXXXXX* within the specified time range will be filtered.

Step 4 Perform the operations listed in [Table 4-22](#) as required:

Table 4-22 Operations

Operation	Description
Viewing event statistics	Click  , and view event statistics that meet filter criteria within a specific time range on a bar graph.
Viewing event details	Click an event name to view event details and handling suggestions.

----End

4.6 Alarm Action Rules

4.6.1 Overview

AOM allows you to customize alarm action rules. When log, resource or metric data meets alarm conditions, the system sends notifications based on the associated Simple Message Notification (SMN) topic and message template.

- Create an alarm action rule to associate an SMN topic and message template.
- Create a message template to customize notification.

After an alarm action rule is created, choose **Alarm Center > Alarm Noise Reduction** in the navigation pane. Then, click the **Grouping Rules** tab and click **Create**. On the displayed page, specify an alarm action rule.

4.6.2 Creating an Alarm Action Rule

You can create an alarm action rule and associate it with an SMN topic and a message template. If the log, resource or metric data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.

Prerequisites

- A topic has been created according to [Creating a Topic](#).
- A topic policy has been set according to [Configuring Topic Policies](#).
- A subscriber, that is, an email or SMS message recipient has been added for the topic according to [Adding a Subscription](#).

Precautions

You can create a maximum of 1000 alarm action rules. If this number has been reached, delete unnecessary rules.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Action Rules**.
- 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 4-23](#).

Figure 4-21 Creating an alarm action rule

Create Alarm Action Rule

* Rule Name ⓘ

* Enterprise Project

Description ⓘ -- [✍](#)

* Rule Type Metric/Event Log

* Action

* Topic

If you do not see a topic you like, create one on the SMN console.

* Message Template [Create Template](#) | [View Template](#)

Table 4-23 Parameters of an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter up to 100 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, hyphens, and underscores are allowed.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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 the action. Select one from the drop-down list. <ul style="list-style-type: none"> Metric/Event If a metric or 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 one from the drop-down list. Currently, 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 there is no message template you want to select, create one by referring to 4.6.3 Creating a Message Template .


Step 5 Click **OK**.

----End

More Operations

After an alarm action rule is created, you can perform operations described in [Table 4-24](#).

Table 4-24 Related operations

Operation	Description
Modifying an alarm action rule	Click Modify in the Operation column.
Deleting an alarm action rule	<ul style="list-style-type: none"> To delete a single rule, click Delete in the Operation column in the row that contains the rule, and then click Yes on the displayed page. To delete one or more rules, select them, click Delete above the rule list, and then click Yes on the displayed page. <p>NOTE Before deleting an alarm action rule, you need to delete the alarm rule or grouping rule bound to the action rule.</p>
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click  .

4.6.3 Creating a Message Template

In AOM, you can create message templates to customize notifications. When a preset notification rule is triggered, notifications can be sent to specified personnel by email, SMS, Lark, WeCom, DingTalk, voice call, WeLink, HTTP, or HTTPS. If no message template is created, the default message template will be used.

Function Introduction

- Message templates for emails, SMS, WeCom, DingTalk, Lark, voice calls, WeLink, HTTP, and HTTPS are supported.

NOTE

- WeLink message templates are not yet generally available. If you need this function, [submit a service ticket](#).
- Message templates can be customized. For details, see [Step 3.3](#).

Precautions

- You can create a maximum of 100 metric/event or log message templates. If the number of message templates of a certain type reaches 100, delete unnecessary ones.
- By default, six message templates are preset and cannot be deleted or edited. If there is no custom message template, notifications are sent based on a preset message template by default.

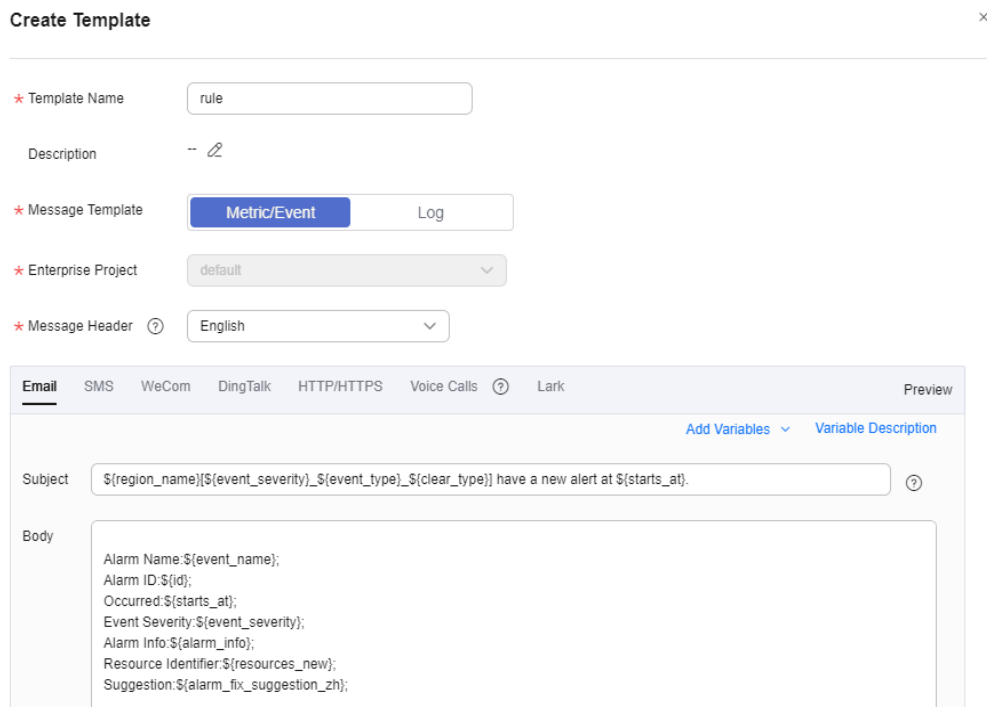
Creating a Message Template

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Action Rules**.

Step 3 On the **Message Templates** tab page, click **Create**.

Figure 4-22 Creating a message template



The screenshot shows the 'Create Template' interface. It has a title bar 'Create Template' with a close button. Below the title bar are several form fields:

- Template Name:** A text input field containing 'rule'.
- Description:** A text input field with a clear icon.
- Message Template:** A dropdown menu with 'Metric/Event' selected and 'Log' as an alternative option.
- Enterprise Project:** A dropdown menu with 'default' selected.
- Message Header:** A dropdown menu with 'English' selected.

Below these fields is a preview section for the message template. It has tabs for 'Email', 'SMS', 'WeCom', 'DingTalk', 'HTTP/HTTPS', 'Voice Calls', and 'Lark'. The 'Email' tab is active. The preview shows the following content:

Subject: `${region_name}[${event_severity}_${event_type}_${clear_type}] have a new alert at ${starts_at}.`

Body:

```
Alarm Name: ${event_name};
Alarm ID: ${id};
Occurred: ${starts_at};
Event Severity: ${event_severity};
Alarm Info: ${alarm_info};
Resource Identifier: ${resources_new};
Suggestion: ${alarm_fix_suggestion_zh};
```

1. Enter a template name, message template type, and description, and specify an enterprise project.

Table 4-25 Parameter description

Parameter	Description
Template Name	Name of a message template. Enter up to 100 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, underscores, and hyphens are allowed.
Description	Description of the template. Enter up to 1024 characters.
Message Template	Type of the message template. Option: Metric/Event or Log .
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> - 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.

2. Select a language (for example, English).
3. Customize the template content (default fields are automatically filled in when a metric/event message template is created). There are templates for emails, WeCom, DingTalk, and SMS. For details about metric/event templates, see [Table 4-26](#). For details about log templates, see [Table 4-27](#).

 **NOTE**

- In addition to the message fields in the default template, the message template also supports custom fields. You need to specify the fields when reporting event alarms. For details, see the alarm reporting structs in the following message template.
- Custom fields support the JSONPath format. Example: `$event.metadata.case1` or `$event.metadata.case[0]`.
- In the upper right corner of the **Body** area, click **Add Variables** to add required variables.
- If you select **Emails**, you can click **Preview** to view the final effect. On the **Preview** page, change the message topic if necessary.

Table 4-26 Variables in the default message template

Variable	Description	Definition
Alarm Name	Name of the alarm rule that is triggered.	<code>\${event_name}</code>
Alarm ID	ID of the alarm rule that is triggered.	<code>\${id}</code>
Action Rule	Name of the alarm action rule that triggers notification.	<code>\${action_rule}</code>

Variable	Description	Definition
Occurred	Time when the alarm or event is triggered.	<code>\${starts_at}</code>
Event Severity	Alarm or event severity. Options: Critical , Major , Minor , and Warning .	<code>\${event_severity}</code>
Alarm Info	Detailed alarm information.	<code>\${alarm_info}</code>
Resource Identifier	Resource for which the alarm or event is triggered.	<code>\${resources}</code>
Custom tag	Extended tag.	<code>\$event.metadata.key1</code>
Suggestion	Suggestion about handling the alarm. For non-custom reporting, "NA" is displayed.	<code>\${alarm_fix_suggestion_zh}</code>
Custom annotation	Extended annotation.	<code>\$event.annotations.key2</code>

Table 4-27 Log message template parameters

Parameter	Description	Check Rule	Example
Topic	Message topic.	Customize the topic name or use variables. (Max. 512 characters) Only email templates need a topic name.	test

Parameter	Description	Check Rule	Example
Body	Message content.	<p>Add variables:</p> <ul style="list-style-type: none"> - Original rule name: <i>\${event_name}</i> - Alarm severity: <i>\${event_severity}</i> - Occurrence time: <i>\${starts_at}</i> - Occurrence region: <i>\${region_name}</i> - Huawei Cloud account: <i>\${domain_name}</i> - Alarm source: <i>\${event.metadata.resource_provider}</i> - Resource type: <i>\${event.metadata.resource_type}</i> - Resource ID: <i>\${resources}</i> - Alarm status: <i>\${event.annotations.alarm_status}</i> - Expression: <i>\${event.annotations.condition_expression}</i> - Current value: <i>\${event.annotations.current_value}</i> - Statistical period: <i>\${event.annotations.frequency}</i> - Rule name: <i>\${event.annotations.alarm_rule_alias}</i> - Keyword variables <ol style="list-style-type: none"> 1. Query time: <i>\${event.annotations.results[0].time}</i> 2. Query logs: <i>\${event.annotations.results[0].raw_results}</i> 3. Query URL: <i>\${event.annotations.results[0].url}</i> 	<p><i>\${event_name}</i> <i>\${event_severity}</i> <i>\${starts_at}</i> <i>\${region_name}</i></p>

Parameter	Description	Check Rule	Example
		<p>4. Log group/stream name: <i>\$event.annotations.results[0].resource_id</i></p> <p>NOTE Only the original name of the log group or stream created for the first time can be added.</p> <p>- SQL variables</p> <p>1. Log group/stream names of chart 0: <i>\$event.annotations.results[0].resource_id</i></p> <p>NOTE Only the original name of the log group or stream created for the first time can be added.</p> <p>2. Query statement of chart 0: <i>\$event.annotations.results[0].sql</i></p> <p>3. Query time of chart 0: <i>\$event.annotations.results[0].time</i></p> <p>4. Query URL of chart 0: <i>\$event.annotations.results[0].url</i></p> <p>5. Query logs of chart 0: <i>\$event.annotations.results[0].raw_results</i></p>	


4. Click **Confirm**. The message template is created.

----End

More Operations

After creating a message template, you can perform the operations listed in [Table 4-28](#).

Table 4-28 Related operations

Operation	Description
Editing a message template	Click Edit in the Operation column.
Copying a message template	Click Copy in the Operation column.
Deleting a message template	<ul style="list-style-type: none">To delete a single message template, click Delete in the Operation column in the row that contains the template, and then click Yes on the displayed page.To delete one or more message templates, select them, click Delete above the template list, and then click Yes on the displayed page. <p>NOTE Before deleting a message template, delete the alarm action rules bound to it.</p>
Searching for a message template	Enter a template name in the search box in the upper right corner and click  .

4.7 Alarm Noise Reduction

4.7.1 Overview

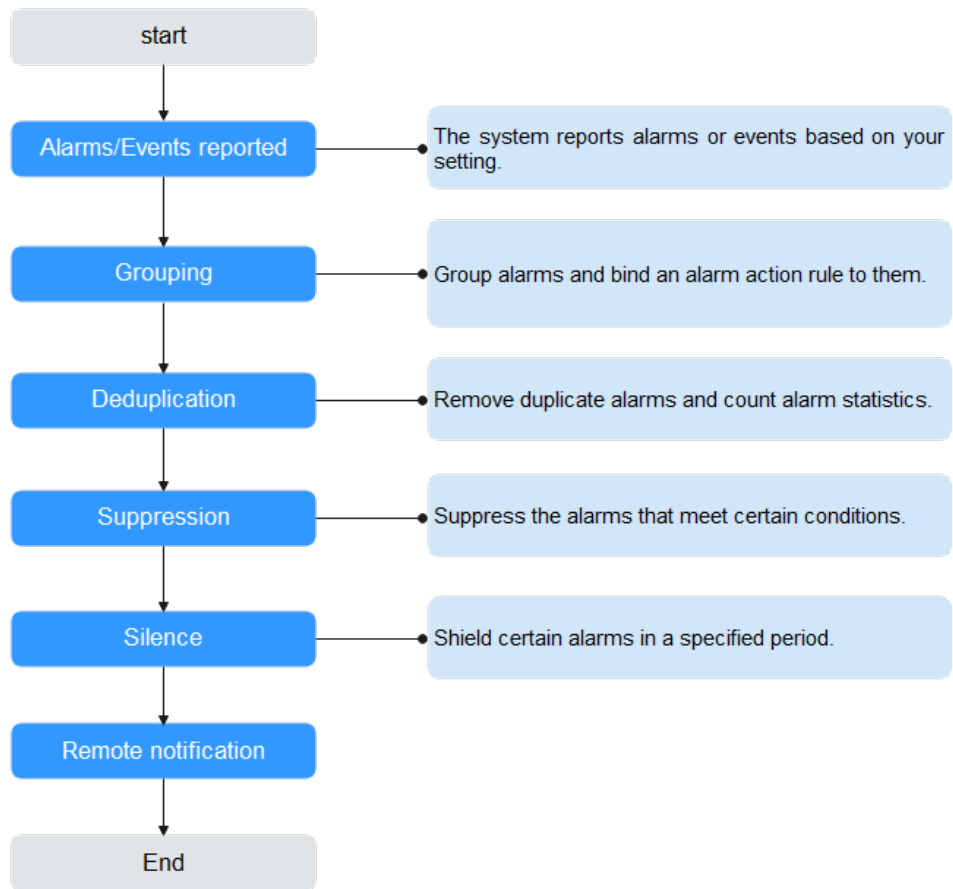
AOM supports alarm noise reduction. Alarms can be processed based on the alarm noise reduction rules to prevent notification storms.

Alarm noise reduction consists of four parts: grouping, deduplication, suppression, and silence.

AOM uses built-in deduplication rules. The service backend automatically deduplicates alarms. You do not need to manually create rules.

You need to manually create grouping, suppression, and silence rules. For details, see [4.7.2 Creating a Grouping Rule](#), [4.7.3 Creating a Suppression Rule](#), and [4.7.4 Creating a Silence Rule](#).

Figure 4-23 Alarm noise reduction process



NOTE

1. This module is used only for message notification. All triggered alarms and events can be viewed on the [alarm list](#) page.
2. All conditions of alarm noise reduction rules are obtained from **metadata** in alarm structs. You can use the default fields or customize your own fields.

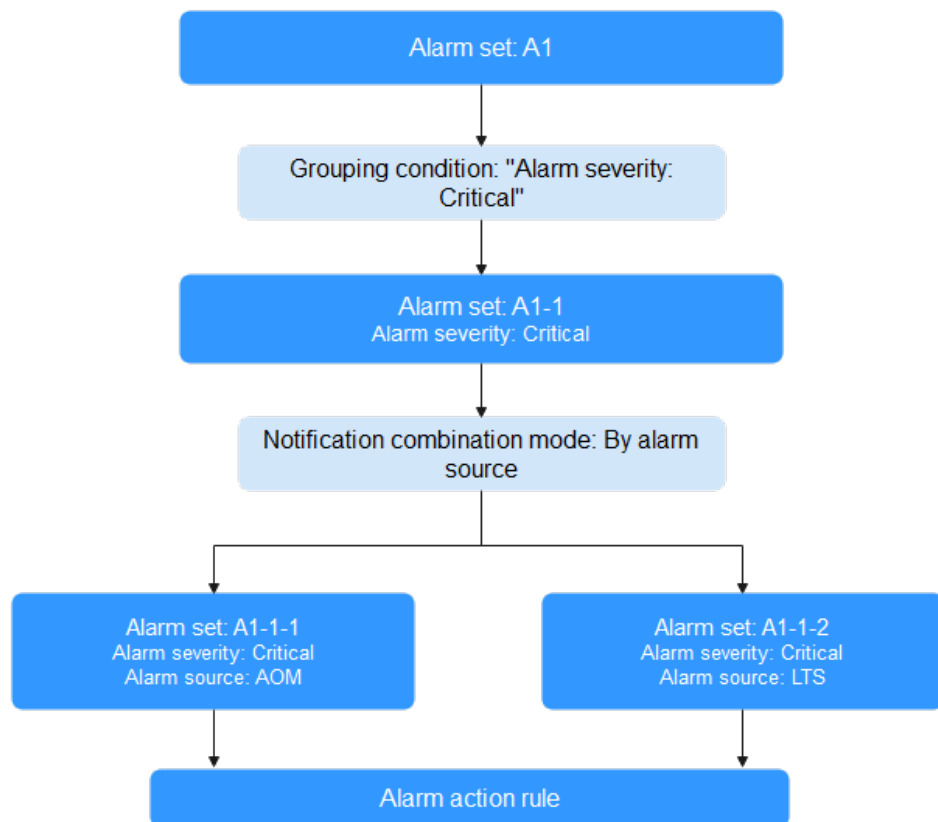
```
{
  "starts_at" : 1579420868000,
  "ends_at" : 1579420868000,
  "timeout" : 60000,
  "resource_group_id" : "5680587ab6*****755c543c1f",
  "metadata" : {
    "event_name" : "test",
    "event_severity" : "Major",
    "event_type" : "alarm",
    "resource_provider" : "ecs",
    "resource_type" : "vm",
    "resource_id" : "ecs123",
    "key1" : "value1" // Alarm tag configured when the alarm rule is created
  },
  "annotations" : {
    "alarm_probableCause_en_us": " Possible causes",
    "alarm_fix_suggestion_en_us": "Handling suggestion"
  }
}
```

4.7.2 Creating a Grouping Rule

You can filter alarm subsets and then group them based on the grouping conditions. Alarms in the same group are aggregated to trigger one notification.

As shown in [Figure 4-24](#), when **Alarm Severity** under **Grouping Condition** is set to **Critical**, the system filters out the critical alarms, and then combines these alarms based on the specified mode. The combined alarms can then be associated with an action rule for sending notifications.

Figure 4-24 Grouping process



Procedure

You can create up to 100 grouping rules.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Grouping Rules** tab page, click **Create** and set parameters such as the rule name and grouping condition. For details, see [Table 4-29](#).

Figure 4-25 Creating a grouping rule

* Rule Name

* Enterprise Project

Description

Grouping Rule

Grouping Condition

Alarm Severity Equals To

Alarm Source Equals To

Action Rule

Combination Rule

* Combine Notifications

* Initial Wait Time Range: 0s to 10 mins.

* Batch Processing Interval Range: 5s to 30 mins.

Table 4-29 Grouping rule parameters

Category	Parameter	Description
-	Rule Name	Name of a grouping rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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 a grouping rule. Enter up to 1024 characters.

Category	Parameter	Description
Grouping Rule	Grouping Condition	<p>Conditions set to filter alarms. After alarms are filtered out, you can set alarm action rules for them.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> ● Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical ● Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: host, container, process, and so on. Example: Resource Type Equals to container ● Alarm Source: name of the service that triggers the alarm or event. Options: AOM, LTS, CCE, and so on. Example: Alarm Source Equals to AOM ● Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure ● Notify When: scenario when notifications are triggered. Options: Alarm triggered and Alarm cleared. For example, select Notify When and then select Alarm triggered. ● XX Exists: indicates the alarm whose metadata contains parameter <i>XX</i>. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. ● XX Regular Expression: indicates the alarm whose parameter <i>XX</i> matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <ul style="list-style-type: none"> ● You can create a maximum of 10 parallel conditions, each of which can contain up to 10 serial conditions. One or more alarm action rules can be set for each parallel condition. ● Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions. <p>For example, if two serial conditions (that is, Alarm Severity = Critical and Provider = AOM) are set under a parallel condition, critical AOM alarms are filtered out, and notification actions are performed based on the alarm action rule you set.</p>

Category	Parameter	Description
Combination Rule	Combine Notifications	<p>Combines grouped alarms based on specified fields. Alarms in the same group are aggregated for sending one notification.</p> <p>Notifications can be combined:</p> <ul style="list-style-type: none">• By alarm source: Alarms triggered by the same alarm source are combined into one group for sending notifications.• By alarm source + severity: Alarms triggered by the same alarm source and of the same severity are combined into one group for sending notifications.• By alarm source + all tags: Alarms triggered by the same alarm source and with the same tag are combined into one group for sending notifications.
	Initial Wait Time	<p>Interval for sending an alarm notification after alarms are combined for the first time. It is recommended that the time be set to seconds to prevent alarm storms.</p> <p>Value range: 0s to 10 minutes. Recommended: 15s.</p>
	Batch Processing Interval	<p>Waiting time for sending an alarm notification after the combined alarm data changes. It is recommended that the time be set to minutes. If you want to receive alarm notifications as soon as possible, set the time to seconds.</p> <p>The change here refers to a new alarm or an alarm status change.</p> <p>Value range: 5s to 30 minutes. Recommended: 60s.</p>
	Repeat Interval	<p>Waiting time for sending an alarm notification after the combined alarm data becomes duplicate. It is recommended that the time be set to hours.</p> <p>Duplication means that no new alarm is generated and no alarm status is changed while other attributes (such as titles and content) are changed.</p> <p>Value range: 0 minutes to 15 days. Recommended: 1 hour.</p>


Step 4 Click **Confirm**.

----End

More Operations

After creating a grouping rule, perform the operations listed in [Table 4-30](#) if needed.

Table 4-30 Related operations

Operation	Description
Modifying a grouping rule	Click Modify in the Operation column.
Deleting a grouping rule	<ul style="list-style-type: none">To delete a single rule, click Delete in the Operation column in the row that contains the rule.To delete one or more rules, select them and click Delete above the rule list.
Searching for a grouping rule	Enter a rule name in the search box in the upper right corner and click  .

4.7.3 Creating a Suppression Rule

By using suppression rules, you can suppress or block notifications related to specific alarms. For example, when a major alarm is generated, less severe alarms can be suppressed. Another example, when a node is faulty, all other alarms of the processes or containers on this node can be suppressed.

Precautions

If the source alarm corresponding to the suppression condition is cleared before the alarm notification is sent, the suppression rule becomes invalid. For the suppressed object (alarm suppressed by the source alarm), the alarm notification can still be sent as usual.

You can create up to 100 suppression rules.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Suppression Rules** tab page, click **Create** and set parameters such as the rule name and source alarm.

Figure 4-26 Creating a suppression rule

The screenshot displays the configuration interface for a suppression rule. At the top, there are three main fields: 'Rule Name' with the value 'rule', 'Enterprise Project' with a dropdown set to 'default', and 'Description' with an edit icon. Below this is the 'Suppression Rule' section, which is divided into two main parts: 'Source Alarm' and 'Suppressed Alarm'. The 'Source Alarm' part includes a dropdown for 'Alarm Severity', a text input for 'event_severity', a dropdown for 'Equals To', and a dropdown for 'Critical'. Below these are options to 'Add Serial Condition' and 'Add Parallel Condition'. The 'Suppressed Alarm' part includes a dropdown for 'Resource Type', a text input for 'resource_type', a dropdown for 'Equals To', and a dropdown for 'service'. Similar to the source alarm, it has options to 'Add Serial Condition' and 'Add Parallel Condition'.

Table 4-31 Setting a suppression rule

Category	Parameter	Description
-	Rule Name	Name of a suppression rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • 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 a suppression rule. Enter up to 1024 characters.

Category	Parameter	Description
Suppression Rule	Source Alarm	<p>Alarm that triggers suppression.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> • Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical • Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: include host, container, and process. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: include AOM, LTS, and CCE. Example: Alarm Source Equals to AOM • Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure • XX Exists: indicates the alarm whose metadata contains parameter XX. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. • XX Regular Expression: indicates the alarm whose parameter XX matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <p>A maximum of 10 parallel conditions can be set for root alarms, and a maximum of 10 serial conditions can be set for each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions.</p> <p>Example: For a serial condition, if Alarm Severity is set to Critical, critical alarms are filtered out as the root alarms.</p>
	Suppressed Alarm	<p>Alarm that is suppressed by the root alarm.</p> <p>Set parameters for the suppressed alarm in the same way that you set parameters for the source alarm.</p> <p>If Alarm Severity is set to Critical in the source alarm's serial condition and set to Warning in the suppressed alarm's serial condition, warnings will be suppressed when critical alarms are generated.</p>

Step 4 Click **Confirm**.


After a suppression rule is created, it will take effect for all alarms that are grouped.

----End

More Operations

After creating a suppression rule, perform the operations listed in [Table 4-32](#) if needed.

Table 4-32 Related operations

Operation	Description
Modifying a suppression rule	Click Modify in the Operation column.
Deleting a suppression rule	<ul style="list-style-type: none"> To delete a single rule, click Delete in the Operation column in the row that contains the rule. To delete one or more rules, select them and click Delete above the rule list.
Searching for a suppression rule	Enter a rule name in the search box in the upper right corner and click  .

4.7.4 Creating a Silence Rule

You can shield alarm notifications in a specified period. A silence rule takes effect immediately after it is created.

Procedure

You can create up to 100 silence rules.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Silence Rules** tab page, click **Create** and set parameters such as the rule name and silence condition.

Figure 4-27 Creating a silence rule

* Rule Name

* Enterprise Project

Description

Silence Rule

* Silence Condition

Alarm Severity Equals To

* Silence Time

Time Zone/Language (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi /

To change the time zone/language, [go to the user center](#).

Table 4-33 Setting a silence rule

Category	Parameter	Description
-	Rule Name	Name of a silence rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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 a silence rule. Enter up to 1024 characters.

Category	Parameter	Description
Silence Rule	Silence Condition	<p>Any alarm notifications that meet the silence condition will be shielded.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> • Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical • Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: include host, container, and process. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: include AOM, LTS, and CCE. Example: Alarm Source Equals to AOM • Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure • XX Exists: indicates the alarm whose metadata contains parameter XX. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. • XX Regular Expression: indicates the alarm whose parameter XX matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <p>You can create up to 10 parallel conditions under Silence Condition, and up to 10 serial conditions under each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions.</p> <p>Example: If Alarm Severity is set to Warning in a serial condition, warnings will be shielded.</p>
	Silence Time	<p>Time when alarm notifications are shielded. There are two options:</p> <ul style="list-style-type: none"> • Fixed time: Alarm notifications are shielded only in a specified period. • Cycle time: Alarm notifications are shielded periodically.

Category	Parameter	Description
	Time Zone/ Language	Time zone and language for which alarm notifications are shielded. The time zone and language configured in Preferences are selected by default. You can change them as required.


Step 4 Click **Confirm**.

----End

More Operations

After creating a silence rule, you can also perform the operations listed in [Table 4-34](#).

Table 4-34 Related operations

Operation	Description
Modifying a silence rule	Click Modify in the Operation column.
Deleting a silence rule	<ul style="list-style-type: none">To delete a single rule, click Delete in the Operation column in the row that contains the rule.To delete one or more rules, select them and click Delete above the rule list.
Searching for a silence rule	Enter a rule name in the search box in the upper right corner and click  .

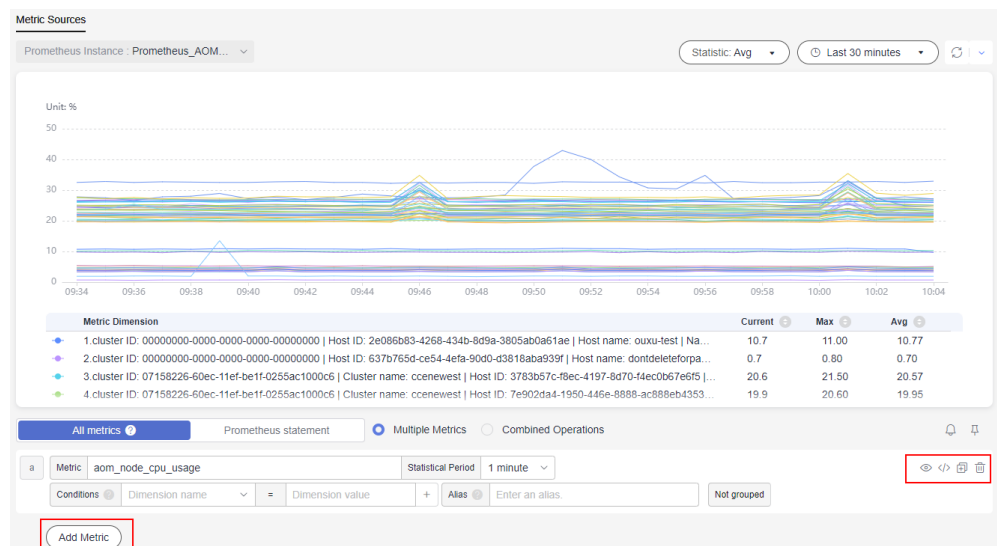
5 Metric Browsing

The **Metric Browsing** page displays metric data of each resource. You can monitor metric values and trends in real time, and create alarm rules for real-time service data monitoring and analysis.

Monitoring Metrics

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Metric Browsing**.
- Step 3** Select a target Prometheus instance from the drop-down list.
- Step 4** Select one or more metrics from all metrics or by running Prometheus statements.
 - Select metrics from all metrics.

Figure 5-1 Selecting metrics from all metrics



For details about how to set monitoring conditions, see [Table 4-2](#).

After selecting a target metric, you can set condition attributes to filter information.

You can click **Add Metric** to add metrics and set information such as statistical period for the metrics. After moving the cursor to the metric data and monitoring condition, you can perform the following operations as required:





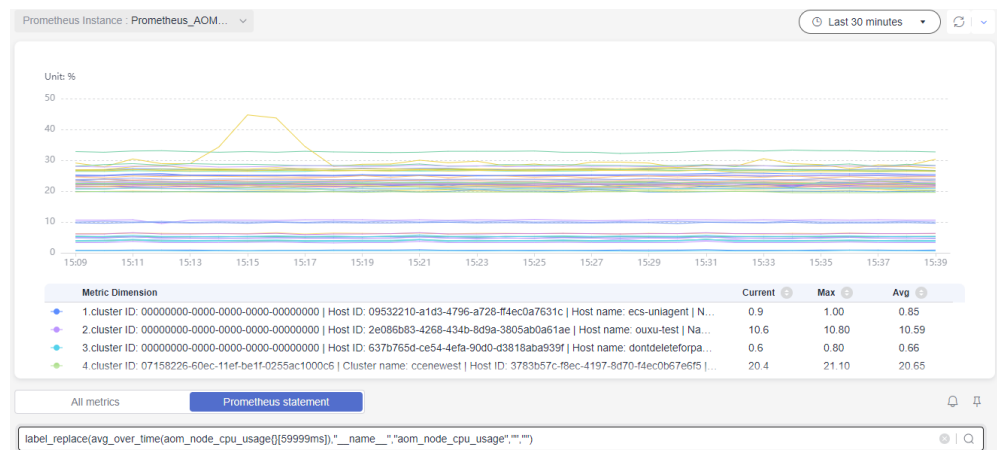
- Click  next to a monitoring condition to hide the corresponding metric data record in the graph.
 - Click  next to a monitoring condition to convert the metric data and monitoring condition into a Prometheus command.
 - Click  next to a monitoring condition to quickly copy the metric data and monitoring condition and modify them as required.
 - Click  next to a monitoring condition to remove a metric data record from monitoring.
- Select metrics by running Prometheus statements. For details about Prometheus statements, see [11.2 Prometheus Statements](#).

Figure 5-2 Selecting metrics by running Prometheus statements



Step 5 Set metric parameters by referring to [Table 5-1](#), view the metric graph in the upper part of the page, and analyze metric data from multiple perspectives.

Table 5-1 Metric parameters

Parameter	Description
Statistic	Method used to measure metrics. Options: Avg , Min , Max , Sum , and Samples . NOTE Samples : the number of data points.
Time Range	Time range in which metric data is collected. Options: Last 30 minutes , Last hour , Last 6 hours , Last day , Last week , and Custom .
Refresh Frequency	Interval at which the metric data is refreshed. Options: Refresh manually , 30 seconds auto refresh , 1 minute auto refresh , and 5 minutes auto refresh .

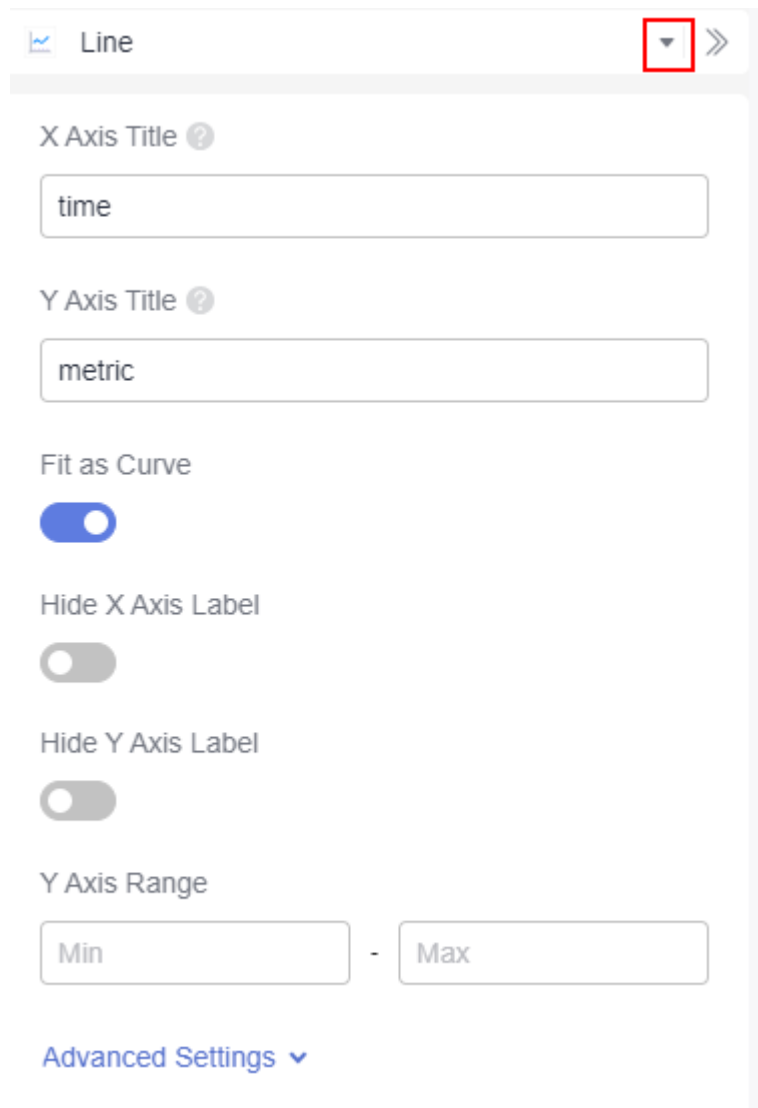
Step 6 (Optional) Set the display layout of metric data.

On the right of the page, click the arrow next to the graph type, select your target graph type from the drop-down list, and set graph parameters, such as the X-axis name, Y-axis name, and displayed value. For details about the parameters, see [Metric Data Graphs \(Line/Digit/Top N/Table/Bar/Digital Line Graphs\)](#).

 **NOTE**

A maximum of 200 metric data records can be displayed in a line graph.

Figure 5-3 Selecting a graph type






----End

More Operations








You can also perform the operations listed in [Table 5-2](#).

Table 5-2 Related operations

Operation	Description
Adding an alarm rule for a metric	After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. NOTE When you are redirected to the Create Alarm Rule page, your settings made on the Metric Browsing page will be automatically applied to Alarm Rule Settings and Alarm Rule Details areas.
Deleting a metric	Click  next to the target metric.
Adding a metric graph to a dashboard	After selecting a metric, click  in the upper right corner of the metric list.
Display Background	If this option is enabled, the background will be displayed in the line graph.

Monitoring Logs

AOM can monitor and analyze log data. However, you need to structure logs first. For details, see [Log Structuring](#).

- Step 1** In the navigation pane, choose **Metric Browsing**.
- Step 2** On the displayed page, click the **Log Sources** tab.
- Step 3** Select a log group name and a log stream name from the drop-down lists.
- Step 4** In the search box, enter an SQL statement, and click **Search** to view the log data analysis of the log stream.
- Step 5** Select a graph or table to display the query result. For details about graph types and configurations, see [Log Graphs \(Table/Bar/Line/Pie/Number/Digital Line/Map Graphs\)](#).
- Click  to display the current log data in a table.
 - Click  to display the current log data in a line graph.
 - Click  to display the current log data in a bar graph.
 - Click  to display the current log data in a pie graph.
 - Click  to display the current log data in a number graph.
 - Click  to display the current log data in a digital line graph.
 - Click  to display the current log data in a national or provincial map.
- Step 6** Perform the following operations on the query result:
- Click **Create**. In the displayed dialog box, set **Chart Name** and **SQL Statement**, select a chart type, and click **OK**.

- Click **Save**. In the displayed dialog box, set **Chart Name**, and click **OK** to save the visual chart. You can also select a chart, click **Save**, and modify it as required.
- Click **Save As**. In the displayed dialog box, set **Chart Name**, and click **OK** to copy the existing visual chart.

 **NOTE**

You must save a chart before saving it as a visual chart.

- Click **Download** to download the visual data of the current SQL query result. The file is in **.csv** format.
- Click **Show Chart** to expand the charts of the current log stream.
- Click **Hide Chart** to collapse the expanded charts of the current log stream.

----End

6 Log Analysis

6.1 Searching for Logs

AOM enables you to quickly query logs, and locate faults based on log sources and contexts.

Step 1 Log in to the AOM 2.0 console.





Step 2 In the navigation pane, choose **Log Analysis > Log Search**.

Step 3 On the **Log Search** page, click the **Component**, **System**, or **Host** tab and set filter criteria as prompted.

NOTE

1. You can search for logs by component, system, or host.
 - For component logs, you can set filter criteria such as **Cluster**, **Namespace**, and **Component**. You can also click **Advanced Search** and set filter criteria such as **Instance**, **Host**, and **File**, and choose whether to enable **Hide System Component**.
 - For system logs, you can set filter criteria such as **Cluster** and **Host**.
 - For host logs, you can set filter criteria such as **Cluster** and **Host**.
2. Enter a keyword in the search box. Rules are as follows:
 - Enter keywords for exact search. A keyword is the word between two adjacent delimiters.
 - Use an asterisk (*) or question mark (?) for fuzzy search, for example, **ER?OR**, **ROR***, or **ER*R**.
 - Enter a phrase for exact search. For example, enter **Start to refresh** or **Start-to-refresh**. Note that hyphens (-) are delimiters.
 - Enter a keyword containing AND (&&) or OR (||) for search. For example, enter **query logs&&error*** or **query logs||error**.
 - If no log is returned, narrow down the search range, or add an asterisk (*) to the end of a keyword for fuzzy match.

Step 4 View the search result of logs.

The search results are sorted based on the log collection time, and keywords in them are highlighted. You can click  in the **Time** column to switch the sorting order.  indicates the default order.  indicates the ascending order by time (the latest log is displayed at the bottom).  indicates the descending order by time (the latest log is displayed at the top).

1. AOM allows you to view context. Click **Context** in the **Operation** column to view the previous or next logs of a log for fault locating.
 - In the **Display Rows** drop-down list, set the number of rows that display raw context data of the log.

 **NOTE**


For example, select **200** from the **Display Rows** drop-down list.

- If there are 100 logs or more printed before a log and 99 or more logs printed following the log, the preceding 100 logs and following 99 logs are displayed as the context.
 - If there are fewer than 100 logs (for example, 90) printed before a log and fewer than 99 logs (for example, 80) printed following the log, the preceding 90 logs and following 80 logs are displayed as the context.
- Click **Export Current Page** to export displayed raw context data of the log to a local PC.

 **NOTE**

To ensure that tenant hosts and services run properly, some components (for example, kube-dns) provided by the system will run on the tenant hosts. The logs of these components are also queried during tenant log query.

2. Click **View Details** on the left of the log list to view details such as host IP address and source.

Step 5 (Optional) Click  on the right of the **Log Search** page, select an export format, and export the search result to a local PC.

Logs are sorted according to the order set in [Step 4](#) and a maximum of 5000 logs can be exported. For example, when 6000 logs in the search result are sorted in descending order, only the first 5000 logs can be exported.

Logs can be exported in CSV or TXT format. You can select a format as required. If you select the CSV format, detailed information (such as the log content, host IP address, and source) can be exported, as shown in [Figure 6-1](#). Only log content will be exported when you select the TXT format (as shown in [Figure 6-2](#)). Each line indicates a log.

Figure 6-1 Exporting logs in CSV format

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Time	Type	Service Name	Instance/Process Name	Host IP Address	Namespace	Cluster Name	Source	Description											
2	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:14:09.089 (5397)[W]	ntp_linux.go:36 update ntpStatus: &{status:1 serverStatus:1 offset:}											
3	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:14:09.089 (5397)[W]	ntp_linux.go:107 NTPConfig has no set the main NTP_Server!											
4	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[evs-driver-fknbe] fail, podName2podInfoM: map[!]											
5	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[obs-driver-lfhjg] fail, podName2podInfoM: map[!]											
6	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[sfs-driver-f83hn] fail, podName2podInfoM: map[!]											
7	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[storage-driver-z5rv2] fail, podName2podInfoM: map[!]											
8	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[atps-7cc56659b-hvk57] fail, podName2podInfoM: map[!]											
9	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[atps-7cc56659b-mp8cm] fail, podName2podInfoM: map[!]											
10	2018-12-11	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/CAg/2018-12-18 16:13:58.626 (5397)[W]	container_watcher.go:359 get label by pod[atps-7cc56659b-qh47x] fail, podName2podInfoM: map[!]											

Figure 6-2 Exporting logs in TXT format

```
2023-01-19T16:30:38.783448+08:00 host-71-24-40-204 docker[1522]: time="2023-01-19T16:30:38.783401876+08:00" level=info msg="handled exit event processID=a9b55efe7ee83e4663a66c59795cafc65b0d3eaf593688199dbf4c3eed38aa6 containerID=32dcfcf3b782a32f55768dfbc7773eac862b0b66587103dd334bdab904157 pid=74026" module=libcontainerd namespace=moby
2023-01-19T16:30:38.750722+08:00 host-71-24-40-204 docker[1930]: time="2023-01-19T16:30:38+08:00" level=info msg="--try publish event(1) /tasks/exit &TaskExit (ContainerID:32dcfcf3b782a32f55768dfbc7773eac862b0b66587103dd334bdab904157, ID:a9b55efe7ee83e4663a66c59795cafc65b0d3eaf593688199dbf4c3eed38aa6, Pid:74026, ExitStatus:0, ExitedAt:2023-01-19 16:30:38.731935965 +0800 CST m="+794826.727765440.) <nil>"
2023-01-19T16:30:38.749258+08:00 host-71-24-40-204 docker[1522]: time="2023-01-19T16:30:38.749183798+08:00" level=info msg="event ExitStatus=0 ExitedAt="2023-01-19 08:30:38.731935965 +0000 UTC" Pid=74026 ProcessID=a9b55efe7ee83e4663a66c59795cafc65b0d3eaf593688199dbf4c3eed38aa6 containerID=32dcfcf3b782a32f55768dfbc7773eac862b0b66587103dd334bdab904157 module=libcontainerd namespace=moby topic=/tasks/exit
2023-01-19T16:30:38.749095+08:00 host-71-24-40-204 docker[1930]: time="2023-01-19T16:30:38.749010188+08:00" level=info msg="--exit-del moby/32dcfcf3b782a32f55768dfbc7773eac862b0b66587103dd334bdab904157.74026.0 error=<nil>"
2023-01-19T16:30:38.727852+08:00 host-71-24-40-204 docker[1522]: time="2023-01-19T16:30:38.727801764+08:00" level=info msg="handled exit event processID=df8fc094ea7e209119dfcac8c20ae56befd0e78ee1153b723ce3cba3c5c1abb9 containerID=38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35 pid=73999" module=libcontainerd namespace=moby
2023-01-19T16:30:38.692915+08:00 host-71-24-40-204 docker[1930]: time="2023-01-19T16:30:38+08:00" level=info msg="--try publish event(1) /tasks/exit &TaskExit (ContainerID:38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35, ID:df8fc094ea7e209119dfcac8c20ae56befd0e78ee1153b723ce3cba3c5c1abb9, Pid:73999, ExitStatus:0, ExitedAt:2023-01-19 16:30:38.674153885 +0800 CST m="+197458.957089482.) <nil>"
2023-01-19T16:30:38.691108+08:00 host-71-24-40-204 docker[1522]: time="2023-01-19T16:30:38.690862578+08:00" level=info msg="event ExitStatus=0 ExitedAt="2023-01-19 08:30:38.674153885 +0000 UTC" Pid=73999 ProcessID=df8fc094ea7e209119dfcac8c20ae56befd0e78ee1153b723ce3cba3c5c1abb9 containerID=38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35 module=libcontainerd namespace=moby topic=/tasks/exit
2023-01-19T16:30:38.690739+08:00 host-71-24-40-204 docker[1930]: time="2023-01-19T16:30:38.690699053+08:00" level=info msg="--exit-del moby/38b7025401d815a0e299a9dfce0e9e665ad34e25257fa64677e376f629971c35.73999.0 error=<nil>"
```

Step 6 (Optional) Click **Configure Dumps** to dump the searched logs to the same log file in the OBS bucket at a time. For details, see [Adding One-Off Dumps](#).

----End


6.2 Checking Log Files

You can quickly check log files of component instances or hosts to locate faults.

Procedure

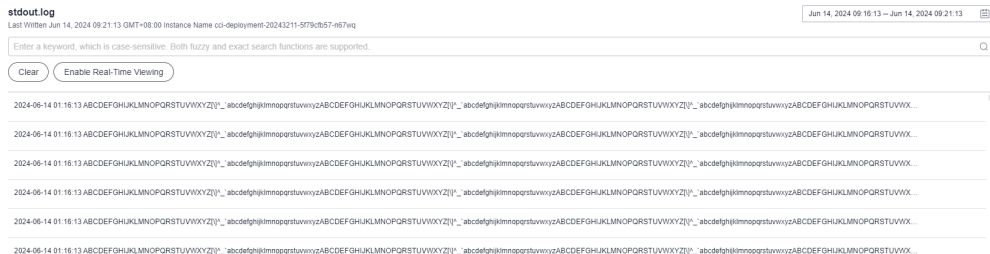
- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Analysis > Log Files**.
- Step 3** On the page that is displayed, click the **Component** or **Host** tab and click a name. Information such as the log file name and latest written time is displayed on the right of the page.
- Step 4** Click **View** in the **Operation** column of the desired instance. [Table 6-1](#) shows how to view log file details. [Figure 6-3](#) shows log file details.

Table 6-1 Operations

Operation	Settings	Description
Setting a time range	Date	Click  to select a date.
Viewing log files	Clear	Click Clear to clear the logs displayed on the screen. Logs displayed on the screen will be cleared, but will not be deleted.

Operation	Settings	Description
	Viewing logs in real time	<p>Real-time viewing is disabled by default. You can click Enable Real-Time Viewing as required. After this function is enabled, the latest written logs can be viewed. Logs can be searched only when real-time viewing is disabled.</p> <p>For real-time log viewing, AOM automatically highlights exception keywords in logs, facilitating fault locating. Such keywords are case-sensitive. For example, when you enter format to search, format in logs will be highlighted, but Format and FORMAT will not.</p>

Figure 6-3 Log file details



Step 5 (Optional) Click **Configure Dumps** in the **Operation** column of the target instance to dump its logs to the same log file in the OBS bucket at a time. For details, see [Adding One-Off Dumps](#).

----End

6.3 Configuring VM Log Collection Paths

AOM can collect and display VM logs. A VM refers to an Elastic Cloud Server (ECS) running Linux. Before collecting logs, ensure that you have set a log collection path.

Prerequisites

You need to install an ICAgent on your VM. About five minutes after the ICAgent is installed, you can view your VM in the VM list on the **Log Analysis > Log Paths** page.

Precautions


- An ICAgent collects ***.log**, ***.trace**, and ***.out** log files only. For example, **/opt/yilu/work/xig/debug_cpu.log**.
- Ensure that an absolute path of a log directory or file is configured and the path exists. For example, **/opt/yilu/work/xig** or **/opt/yilu/work/xig/debug_cpu.log**.

- The ICAgent does not collect log files from subdirectories. For example, the ICAgent does not collect log files from the `/opt/yilu/work/xig/debug` subdirectory of `/opt/yilu/work/xig`.
- A maximum of 20 log collection paths can be configured for a VM.
- For ECSs in the same resource space, only the latest log collection configuration in the system will be used. AOM and LTS log collection configurations cannot take effect at the same time. For example, if you configure log collection paths in AOM for ECSs, the previous collection configurations you made in LTS for these ECSs become invalid.

Configuring Log Collection Paths

Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Log Analysis > Log Paths**.

Step 3 In the VM list, click  in the **Operation** column to configure one or more log collection paths for a VM.

You can use the paths automatically identified by the ICAgent or manually configure paths.

- **Using the Paths Automatically Identified by the ICAgent**

The ICAgent automatically scans the log files of your VM, and displays all the `.log`, `.trace`, or `.out` log files with handles and their paths on the page.

You can click  in the **Operation** column to add a path automatically identified by the ICAgent to the configured log collection path list. To configure multiple paths, repeat this operation.

- **Manual configuration**

If the paths automatically identified by the ICAgent cannot meet your requirements, enter a log directory or file (for example, `/usr/local/uniagentd/log/agent.log`) in the **Collection Path** text box, and then add the path to the configured log collection path list. To configure multiple paths, repeat this operation.

Step 4 Click **Confirm**.

----End

Viewing VM Logs

After the log collection paths are configured, the ICAgent collects log files from them. This operation takes about 1 minute to complete. After collecting logs, you can perform the following operations:

- **Viewing VM Log Files**

In the navigation pane, choose **Log Analysis > Log Files**. Click the **Host** tab to view the collected log files. For details, see [6.2 Checking Log Files](#).

- **Viewing and Analyzing VM logs**

In the navigation pane, choose **Log Analysis > Log Search**. Click the **Host** tab to view and analyze the collected logs by time range, keyword, and context. For details, see [6.1 Searching for Logs](#).

6.4 Adding Log Dumps

AOM enables you to dump logs to Object Storage Service (OBS) buckets for long-term storage. To store logs for a longer time, add log dumps.

AOM offers both periodic and one-off dump modes. You can choose one of them as required.

- **Periodic dump:** Current logs are dumped in real time into an OBS bucket and 1-day logs are divided based on the dump cycle.

To periodically store logs for a long period, add periodic dumps. For details, see [Adding Periodical Dumps](#).

- **One-off dump:** Dump historical logs to a log file of an OBS bucket at one time.

One-off dump is similar to the export function on the **Log Search** page. You can export up to 5000 logs on that page. When you need to export more logs but the export function cannot meet your needs, dump the logs at a time according to [Adding One-Off Dumps](#).

NOTE

- To add a log dump, you must have OBS administrator permissions in addition to AOM and LTS permissions.
- If you need to dump logs to OBS buckets in real time for long-term storage, use the log dump function of LTS.

Adding Periodical Dumps

Assume that you need to dump the logs of the **als0320a** component into files in the **/home/Periodical Dump** directory of the **obs-store-test** OBS bucket in real time, and the dump cycle is 3 hours, perform the following steps:

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Dumps**.

Step 3 Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 6-2](#) and click **OK**.

Table 6-2 Periodical dump parameters

Parameter	Description	Example
Dump Mode	Select Periodic dump .	Periodic dump
Filter Criteria	Logs can be filtered by multiple criteria such as log type, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Select the Component log type and select the als0320a component.

Parameter	Description	Example
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups.	log-group1
Dump Cycle	<p>You can divide 1-day logs based on the dump cycle. There are "N" time segments in a day (Number of time segments = 24 hours/Dump cycle). The logs of the same time segment are dumped into the same log file.</p> <p>For example, if the dump cycle is set to 3 hours, there are 8 time segments in a day. The logs generated at 00:00–03:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 00 path, and the logs generated at 03:00–06:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 03 path. Other time segments can be deduced by analogy.</p>	3 hours
Target OBS Bucket	<p>OBS bucket for storing logs.</p> <p>NOTE You must create an OBS bucket first. Click View OBS to create a bucket on the OBS console.</p>	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs.	/home/ Periodical Dump

After the periodical dump is added, the new logs of the specified resource will be dumped into the OBS bucket in real time.

In the preceding example, the logs of **als0320a** will be dumped into log files in the **/home/Periodical Dump** directory of the **obs-store-test** OBS bucket in real time, and the dump cycle is 3 hours.

 **NOTE**

Periodical dump is a near-real-time dump but has latency in minutes. The latency varies depending on the number of logs and log size. Details are as follows:

- If the number of logs generated within 5 minutes exceeds 1000 or the log size exceeds 2 MB, the logs are dumped in real time.
- If the number of logs generated within 5 minutes is less than 1000 or the log size is less than 2 MB, the logs are dumped every 5 minutes.

Step 4 Download the log files in the OBS bucket to a local host for locating faults.

1. In the periodical dump list, click the target OBS bucket to go to the **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log files stored in OBS, such as **192.168.0.74_var-paas-sys-log-apm-count_warn.log** and **192.168.0.74_var-paas-sys-log-apm-debug_erro.trace**.

Paths of the log files dumped to the OBS bucket: Log file paths are related to the selected log types, as shown in the following table.

Table 6-3 Paths of the log files dumped to the OBS bucket

Log Type	Log File Path
Component	Bucket directory > Log group name > Cluster name > Component name > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X) For example, obs-store-test > home > Periodical Dump > log-group1 > zhqtest0112n > als0320a > 2019-03-22 > 03 .
Host	Belong bucket directory > Log group name > CONFIG_FILE > default_appname > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X)
OS	Belong bucket directory > Log group name > Cluster name > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X)

Names of the log files dumped to the OBS bucket: Host IPv4 address_Log file source_Log file name. Note that slashes (/) in a log file source must be replaced with hyphens (-). For example, **192.168.0.74_var-paas-sys-log-apm-count_warn.log** or **192.168.0.74_var-paas-sys-log-apm-debug_errro.trace**.

3. Select the required log file and click **Download** to download it to the default download path. To save the log file to a custom path, choose **More > Download As**.

----End

Adding One-Off Dumps

For example, to dump the logs that contain the **warn** keyword in the last 30 minutes of **als0320a** to the **/home/One-off Dump** directory of the **obs-store-test** OBS bucket, perform the following steps:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Analysis > Log Dumps**.
- Step 3** Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 6-4](#) and click **OK**.

Table 6-4 One-off dump parameters

Parameter	Description	Example
Dump Mode	Select One-off dump .	One-off dump

Parameter	Description	Example
Filter Criteria	Logs can be filtered by multiple criteria such as log collection time, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Set the log collection time to Last 30 minutes , select the als0320a component, and set the keyword to warn .
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups. NOTE After a dump task is deleted, log groups will also be deleted.	log-group2
Target OBS Bucket	OBS bucket for storing logs. NOTE <ul style="list-style-type: none"> If no OBS bucket is available, click View OBS to create a bucket on the OBS console. If you select an unauthorized OBS bucket, AOM will take 15 minutes to authorize the ACL for the bucket. If your configuration fails, try again 15 minutes later. Data cannot be dumped to an OBS bucket whose storage class is Archive or for which cross-region replication has been configured. 	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs. NOTE If this parameter is left blank, logs are stored in the root directory of the OBS bucket by default.	/home/One-off Dump

After the one-off dump is added and the dump status changes to **Dumped**, the historical logs that meet criteria are dumped into the same log file of the OBS bucket at one time.

For example, the historical logs that contain the **warn** keyword in the last 30 minutes of **als0320a** will be dumped to the **log-group2_shard_0(custom).log** file in the **/home/One-off Dump** directory of the **obs-store-test** OBS bucket at one time.

Step 4 Download the log files in the OBS bucket to a local host for locating faults.

1. In the one-off dump list, click the target OBS bucket to go to the **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log file stored in OBS, for example, **/home/One-off Dump/log-group2_shard_0(custom).log**.

Paths of the log files dumped to the OBS bucket: OBS bucket > Belong bucket directory For example, **obs-store-test/home/One-off Dump**.

Names of the log files dumped to the OBS bucket: Log file names are related to dump file formats, as shown in the following table.

Table 6-5 Names of the log files dumped to the OBS bucket

Log File Name
- Log group name_shard_0(custom), for example, log-group2_shard_0(custom).log
- Log group name_shard_1(custom)

3. Select the required log file and click **Download** to download it to the default download path. To save the log file to a custom path, choose **More > Download As**.

----End

6.5 Log Streams

6.5.1 Searching for Logs

AOM enables you to quickly query logs, and locate faults based on log sources and contexts.

Precaution

- To use log streams, enable this function in **Menu Settings**. For details, see [10.6 Menu Settings](#).

Setting a Filter

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.

Step 3 In the filter area of the **Log Stream** page, filter logs by setting different perspectives (such as cloud log) and parameters. Set log search criteria as prompted.

Step 4 Click **Search**.

If a message indicating that no logs found is displayed, ingest logs by referring to [Log Ingestion](#).

----End

Searching for Raw Logs

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.

Step 3 Set filters by referring to [Setting a Filter](#).

Step 4 In the upper right corner of the **Raw Logs** tab page, select a time range.

Step 5 Search for raw logs in the following ways:

- In the search area, enter a keyword or select a keyword from the drop-down list, and click **Search**.

 **NOTE**

- After you set log structuring, the drop-down list displays both the built-in fields and fields configured for structuring.
- Built-in fields include **appName**, **category**, **clusterId**, **clusterName**, **collectTime**, **containerName**, **hostIP**, **hostIPv6**, **hostId**, **hostName**, **nameSpace**, **pathFile**, **podName** and **serviceID**. By default, the fields are displayed in simplified mode, and **hostIP**, **hostName**, and **pathFile** are displayed at the beginning.
- The structured fields are displayed in **key:value** format.
- Click a field in blue in the log content and the field will be used as a filter. All logs that meet the filtering criteria are displayed.
- Click a field for which quick analysis has been created to add it to the search box.

 **NOTE**

If the field you click already exists in the search box, it will be replaced by this newly added one. If the field is added the first time, fields in the search box are searched using the AND operator.

- In the search area, press the up and down arrows on the keyboard to select a keyword or search syntax from the drop-down list, press **Tab** or **Enter** to select a keyword or syntax, and click **Search**.

----End

Visualized Log Analysis

You can query and analyze structured log fields using SQL statements. After log structuring, wait about 1–2 minutes for SQL query and analysis.

Before visualized analysis, [structure raw logs first](#).

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.

Step 3 Set filters by referring to [Setting a Filter](#).

Step 4 Click the **Visualization** tab, select a time range, enter an SQL statement, and click **Search**.

 NOTE

- SQL query constraints:
 - A maximum of 100,000 records can be returned for each query.
 - If there are more than 100,000 aggregation results, they may be inaccurate.
- There are some restrictions when you use a string in a WHERE clause.
 - The value should be enclosed by single quotation marks (') for exact match, and by single or double quotation marks (") for fuzzy search. If the key has the same name with one of the SQL reserved fields, enclose the key with double quotation marks (").
 - Recommended formats: WHERE "Key"='Value' and WHERE "Key" like ' %Value%'
- There are no restrictions on **float** and **long** types in WHERE clauses. You are advised to use the formats described above to avoid query exceptions caused by keyword conflicts.

If the number of logs generated within the specified time range exceeds 1 billion, iterative query is triggered so you can view all logs in multiple queries. The message **Query status: Results are accurate** is displayed.

Step 5 Select a graph to display the query result. For details about graph types and configurations, see [Log Graphs \(Table/Bar/Line/Pie/Number/Digital Line/Map Graphs\)](#).

Step 6 Perform the following operations on the query result:

- Click **Create**. In the displayed dialog box, set **Chart Name** and **SQL Statement**, select a chart type, and click **OK**.
- Click **Save**. In the displayed dialog box, set **Chart Name**, and click **OK** to save the visual chart. You can also select a chart, click **Save**, and modify it as required.
- Click **Save As**. In the displayed dialog box, set **Chart Name**, and click **OK** to copy the existing visual chart.

 NOTE

You must save a chart before saving it as a visual chart.

- Click **Download** to download the visual data of the current SQL query result. The file is in **.csv** format.
- Click **Show Chart** to expand the charts of the current log stream.
- Click **Hide Chart** to collapse the expanded charts of the current log stream.

----End

Analyzing Real-Time Logs

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.

Step 3 Set filters by referring to [Setting a Filter](#).

Step 4 Click the **Real-Time Logs** tab to view the corresponding real-time logs.

Logs are refreshed every 5s. You may wait for up to 1 minute before the logs are displayed.

You can also customize log display by clicking **Clear** or **Pause** in the upper right corner.

- **Clear:** Displayed logs will be cleared from the real-time view.
- **Pause:** Loading of new logs to the real-time view will be paused.
After you click **Pause**, the button changes to **Continue**. You can click **Continue** to resume the log loading to the real-time view.

 **NOTE**







Stay on the **Real-Time Logs** tab to keep updating them in real time. If you leave the **Real-Time Logs** tab, logs will not be loaded in real time. The next time you access the tab, the logs that were shown before you left the tab will not be displayed.





----End

Common Log Search Operations

These operations include adding alarms, selecting a time range to display logs, and refreshing logs. For details, see [Table 6-6](#).

Table 6-6 Common operations

Operation	Description
Configuring quick search	Click  and configure quick search .
Refreshing logs	Click  to refresh logs. There are two refresh modes: manual and automatic. <ul style="list-style-type: none"> • Manual refresh: Click Refresh Now to refresh logs. • Automatic refresh: Select an interval from the drop-down list to automatically refresh logs. The interval can be 15 seconds, 30 seconds, 1 minute, or 5 minutes.
Copying logs	Click  to copy log content.
Viewing the context	Click  to view the log context.
Simplifying field details	Click  to view the simplified field details.
Unfolding	Click  to unfold log content. They will be displayed in multiple lines. NOTE By default, log content is unfolded and two lines are displayed.

Operation	Description
Downloading logs	<p>Click . On the page that is displayed, download logs to the local host.</p> <p>Direct Download: Download log files to the local PC. Up to 5000 logs can be downloaded at a time.</p> <p>Select .csv or .txt from the drop-down list and click Download to export logs to the local PC.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If you select .csv, logs are exported as a table. • If you select .txt, logs are exported as a .txt file.
JSON	<p>Move the cursor over , click JSON, and set JSON formatting.</p> <p>NOTE</p> <p>Formatting is enabled by default. The default number of expanded levels is 2.</p> <ul style="list-style-type: none"> • Formatting enabled: Set the default number of expanded levels. Maximum value: 10. • Formatting disabled: JSON logs will not be formatted for display.
Collapse configuration	<p>Move the cursor over , click Log Collapse, and set the maximum characters to display in a log.</p> <p>If the number of characters in a log exceeds the maximum, the extra characters will be hidden. Click Expand to view all.</p> <p>NOTE</p> <p>Logs are collapsed by default, with a default character limit of 400.</p>
Log time display	<p>Move the cursor over  and click Log time display. On the page that is displayed, set whether to display milliseconds and whether to display the time zone.</p> <p>NOTE</p> <p>By default, the function of displaying milliseconds is enabled.</p>

Syntax and Examples of Searching by Keyword

Search syntax:

Table 6-7 Search syntax

Condition	Description
Exact search by keyword	<p>Enter a keyword (case-sensitive) for exact search. A keyword is the word between two adjacent delimiters.</p> <p>You can add an asterisk (*) after a keyword, for example, error*, if you are not familiar with delimiters.</p>

Condition	Description
Exact search by phrase	Enter a phrase (case-sensitive) for exact search.
&&	Intersection of search results.
	Union of search results.
AND	Intersection of search results.
OR	Union of search results.
NOT	Logs that do not contain the keyword after NOT .
?	Fuzzy search. A question mark (?) can be put in the middle or at the end of a keyword to represent a character.
*	Fuzzy search. The asterisk (*) can only be after a keyword. It represents 0–N characters.

 **NOTE**

Operators (such as **&&**, **||**, **AND**, **OR**, **NOT**, *****, **?**, **:**, **>**, **<**, **=**, **>=**, and **<=**) contained in raw logs cannot be used to search for logs.

Search rules:

- Fuzzy search is supported.
For example, if you enter **error***, all logs containing **error** will be displayed and those start with **error** will be highlighted.
- You can use a combination of multiple search criteria in the key and value format: *key1:value1* **AND** *key2:value2* or *key1:value1* **OR** *key2:value2*. After entering or selecting *key1:value1*, you need to add **AND** or **OR** before entering or selecting *key2:value2* in the search box.
- Click a keyword and select one of the three operations from the displayed drop-down list: **Copy**, **Add To Search**, and **Exclude from Search**.
 - **Copy**: Copy the field.
 - **Add To Search**: Add **AND** *field: value* to the search statement.
 - **Exclude from Search**: Add **NOT** *field: value* to the query statement.

Search examples:

- Search for logs containing **start**: Enter **start**.
- Search for logs containing **start to refresh**: Enter **start to refresh**.
- Search for the logs containing both keyword **start** and **unexpected**: Enter **start && unexpected**.
- Search for logs containing both **start** and **unexpected**: Enter **start AND unexpected** or **start and unexpected**.
- Search for the logs containing keyword **start** or **unexpected**: Enter **start || unexpected**.

- Search for logs containing **start** or **unexpected**: Enter **start OR unexpected** or **start or unexpected**.
- Logs that do not contain *query1*: **NOT content: query1** or **not content: query1**.
- **error***: logs that contain **error**.
- **er?or**: logs that start with **er**, is followed by any single character, and end with **or**.
- If your keyword contains a colon (:), use the **content: Keyword** format. Example: **content: "120.46.138.115:80"** or **content: 120.46.138.115:80**.
- **query1 AND query2 AND NOT content: query3**: logs that contain both *query1* and *query2* but not *query3*.

 **NOTE**

- When you enter a keyword to query logs, the keyword is case-sensitive. Both the log contents you queried and the highlighted log contents are case-sensitive.
- The asterisk (*) and question mark (?) do not match special characters such as hyphens (-) and spaces.
- For fuzzy match, a keyword cannot start with a question mark (?) or an asterisk (*). For example, you can enter **ER?OR** or **ER*R**.

6.5.2 Quickly Analyzing Logs

Monitoring keywords in logs helps you trace system performance and services. For example, the number of **ERROR** keywords indicates the system health, and the number of **BUY** keywords indicates the sales volume. With AOM quick analysis, your specified keywords can be counted and metric data can be generated for real-time monitoring.

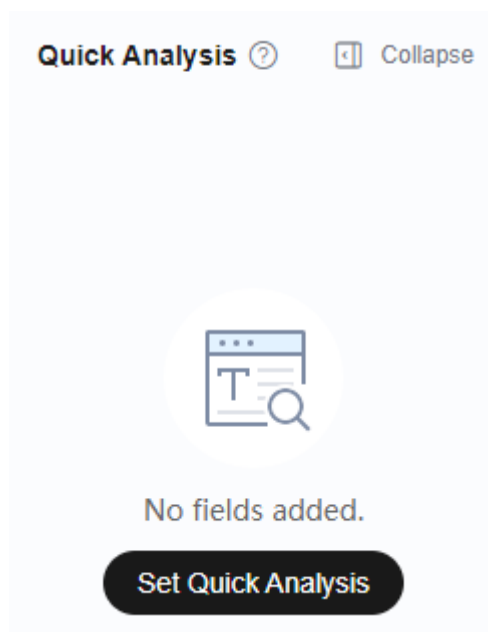
Precautions

Quick analysis is conducted on fields extracted from structured logs. [Structure raw logs](#) before you create a quick analysis task.

Creating a Quick Analysis Task

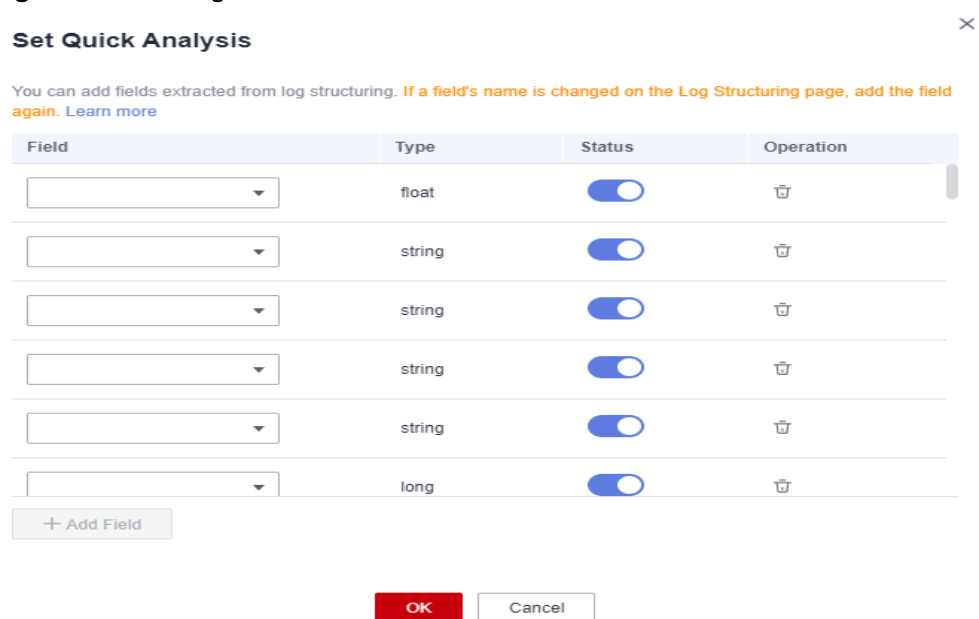
- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Analysis > Log Stream**.
- Step 3** On the **Raw Logs** page, click **Set Quick Analysis**, as shown in [Figure 6-4](#).

Figure 6-4 Creating a quick analysis task



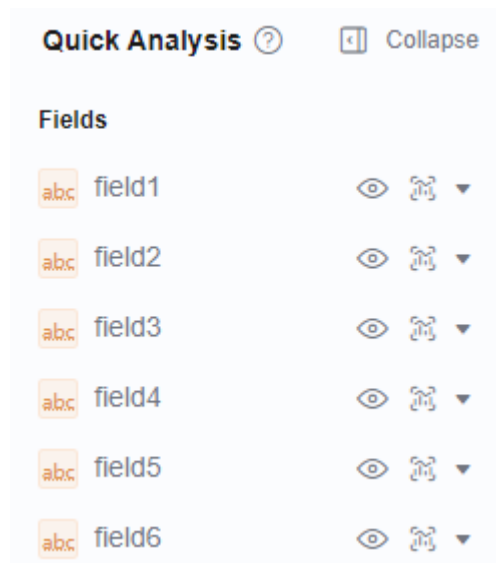
Step 4 On the displayed **Set Quick Analysis** page, select fields for quick analysis.

Figure 6-5 Adding fields







Step 5 Click **OK**. The quick analysis task is created.

Figure 6-6 Viewing quick analysis results



NOTE

-  indicates a field of the **string** type.
-  indicates a field of the **float** type.
-  indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.
- Click  in the upper right corner of the **Quick Analysis** area to modify or delete an existing field. If you delete a field or modify the name of a field on the **Log Structuring** page, the field will be updated in the quick analysis.
- If a structured field does not occur in logs during the specified time range, its occurrence percentage will be displayed as **null**.
 - When you click **null** to **add a float or long field to the search box**, *Field: 0 OR NOT Field: ** will be displayed.
 - When you click **null** to **add a string field to the search box**, *Field: null OR NOT Field: ** will be displayed.

----End

6.5.3 Quickly Querying Logs

To search for logs using a keyword repeatedly, perform the following operations to configure quick search.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.


Step 3 On the **Raw Logs** tab page, click  and configure quick search. For details, see [Table 6-8](#).

Figure 6-7 Configuring quick search

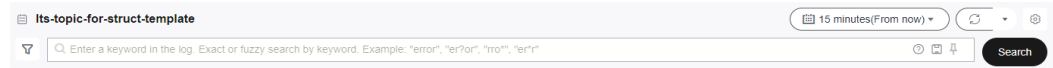


Table 6-8 Quick search parameters

Parameter	Description
Name	Quick search name, which is used to distinguish quick search statements. Enter 1 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. Do not start with a period (.) or underscore (_) or end with a period.
Keyword	Keyword that needs to be repeatedly used during log search, for example, error* .

Step 4 Click **OK**.

After the creation is complete, click the quick query name to quickly view log details.

----End

6.5.4 Viewing the Context

You can check the logs generated before and after a log for quick fault locating.

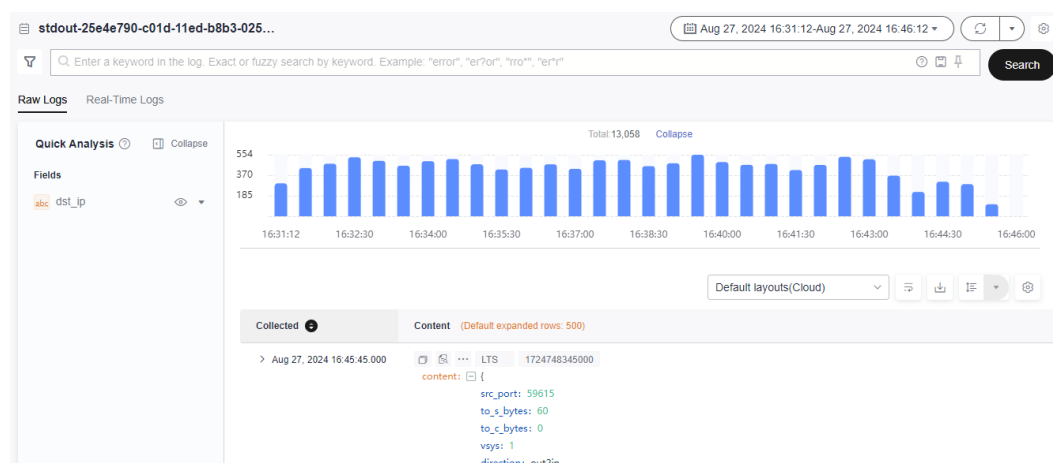
Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis > Log Stream**.

Step 3 On the **Raw Logs** tab page, click  to check the context.

The context of the log is displayed.

Figure 6-8 Checking the context



----End

7 Prometheus Monitoring

7.1 Prometheus Monitoring

7.1.1 Prometheus Monitoring Overview

Prometheus monitoring fully interconnects with the open-source Prometheus ecosystem. It monitors various components, and provides multiple out-of-the-box dashboards and fully hosted Prometheus services.

 **NOTE**

Prometheus is an open-source monitoring and alarm system. It features multi-dimensional data models, flexible PromQL statement query, and visualized data display. For more information, see [official Prometheus documents](#).

Prometheus Instance

Prometheus instances are logical units used to manage Prometheus data collection, storage, and analysis. [Table 7-1](#) lists different types of instances classified based on monitored objects and application scenarios.

Table 7-1 Prometheus instance description

Prometheus Instance Type	Monitored Object	Monitoring Capability	Application Scenario
Default Prometheus instance	<ul style="list-style-type: none"> Metrics reported using the API for adding monitoring data Metrics reported using ICAgents 	Monitors the metrics reported to AOM using APIs or ICAgents.	Default Prometheus instance. It is applicable to both the scenario where self-built Prometheus remote storage (remote write) is used and the scenario where container, cloud service, or host metrics are connected.
Prometheus instance for CCE	CCE	<ul style="list-style-type: none"> Provides native container service integration and container metric monitoring capabilities. By default, the following service discovery capabilities are enabled: Kubernetes SD, ServiceMonitor, and PodMonitor. 	Applicable when you need to monitor CCE clusters and applications running on them.
Prometheus instance for ECS	ECS	<ul style="list-style-type: none"> Provides integrated monitoring for ECS applications and components (such as databases and middleware) in a Virtual Private Cloud (VPC) using the UniAgent (Exporter) installed in this VPC. 	Applicable when you need to monitor application components running in a VPC (usually an ECS cluster) on the cloud. You can add middleware to monitor through the access center.
Prometheus instance for cloud services	Multiple cloud services	Monitors multiple cloud services. NOTE Only one Prometheus instance for cloud services can be created in an enterprise project.	Applicable when you need to centrally collect, store, and display monitoring data of cloud services.

Prometheus Instance Type	Monitored Object	Monitoring Capability	Application Scenario
Common Prometheus instance	Self-built Prometheus	<ul style="list-style-type: none"> Provides remote storage for Prometheus time series databases. Provides a self-developed monitoring dashboard to display data. <p>NOTE You maintain Prometheus servers. You need to configure metric management and data collection by yourselves.</p>	Applicable when you have your own Prometheus servers but need to ensure data storage availability and scalability through remote write.

7.1.2 Functions

Prometheus monitoring supports monitoring data collection, storage, computing, display, and alarm reporting. It monitors metrics of containers, cloud services, middleware, databases, applications, and services. This section describes the important functions of Prometheus monitoring.

Table 7-2 Monitored object access

Function	Description
7.2 Creating Prometheus Instances	Multiple types of Prometheus instances are supported. You can create Prometheus instances as required.
Connecting a CCE Cluster	An entry of Prometheus instances. It centrally displays associated data and high-frequency operations of container services, custom service discovery, and component monitoring. Only Prometheus instances for CCE support this function.

Table 7-3 Monitoring metric collection

Function	Description
7.5.2 Configuring Metric Management for CCE Clusters	By adding ServiceMonitor or PodMonitor, you can configure Prometheus collection rules to monitor the services deployed in CCE clusters. Only Prometheus instances for CCE support this function.

Function	Description
7.5.1 Configuring Metrics	You can check, add, and discard metrics. Only the default or common Prometheus instance and the Prometheus instances for CCE, cloud services, and ECS are supported.

Table 7-4 Data processing

Function	Description
7.8 Obtaining the Service Address of a Prometheus Instance	With the remote read and write addresses, you can store the monitoring data of self-built Prometheus to AOM Prometheus instances for remote storage.
7.4 Configuring a Recording Rule	By setting recording rules, you can move the computing process to the write end, reducing resource usage on the query end. Especially in large-scale clusters and complex service scenarios, recording rules can reduce PromQL complexity, thereby improving the query performance and preventing slow user configuration and queries. Only Prometheus instances for CCE support this function.

7.1.3 Advantages

Table 7-5 Advantages

<p>Out-of-the-box usability</p> <ul style="list-style-type: none"> • Installs and deploys Kubernetes and cloud products in a few clicks. • Connects to various application components and alarm tools in a few clicks. 	<p>Low cost</p> <ul style="list-style-type: none"> • Multiple metrics, including those of standard Kubernetes components, are free of charge. • Provides fully hosted services and eliminates the need to purchase additional resources, reducing monitoring costs and generating almost zero maintenance costs. • Integrates with CCE for monitoring services, reducing the time for creating a container monitoring system from 2 days to 10 minutes. A Prometheus instance for CCE can report the data of multiple CCE clusters.
---	---

<p>Open-source compatibility</p> <ul style="list-style-type: none"> • Supports custom multi-dimensional data models, HTTP API modules, and PromQL query. • Monitored objects can be discovered through static file configuration and dynamic discovery, facilitating migration and access. 	<p>Unlimited data</p> <ul style="list-style-type: none"> • Supports cloud storage. There is no limit on the data to store. Distributed storage on the cloud ensures data reliability. • Supports the Prometheus instance for multi-account aggregation. Therefore, metric data of multiple accounts can be aggregated for unified monitoring.
<p>High performance</p> <ul style="list-style-type: none"> • Is more lightweight and consumes fewer resources than open-source products. Uses single-process integrated Agents to monitor Kubernetes clusters, improving collection performance by 20 times. • Deploys Agents on the user side to retain the native collection capability and minimize resource usage. • Uses the collection-storage-separated architecture to improve the overall performance. • Optimizes the collection component to improve the single-replica collection capability and reduce resource consumption. • Balances collection tasks through multi-replica horizontal expansion to implement dynamic scaling and solve open-source horizontal expansion problems. 	<p>High availability</p> <ul style="list-style-type: none"> • Dual-replica: Data collection, processing, and storage components support multi-replica horizontal expansion, ensuring the high availability of core data links. • Horizontal expansion: Elastic scaling can be performed based on the cluster sca

7.1.4 Basic Concepts

This section describes the basic concepts about Prometheus monitoring.

Table 7-6 Basic concepts

Concept	Description
Exporter	Collects monitoring data and regulates the data provided for external systems using the Prometheus monitoring function. Hundreds of official or third-party exporters are available. For details, see Exporters .

Concept	Description
Target	Target to be captured by a Prometheus probe. A target either exposes its own operation and service metrics or serves as a proxy to expose the operation and service metrics of a monitored object.
Job	Configuration set for a group of targets. Jobs specify the capture interval, access limit, and other behavior for a group of targets.
Prometheus monitoring	Fully interconnects with the open-source Prometheus ecosystem. It monitors various components, and provides multiple out-of-the-box dashboards and fully hosted Prometheus services.
Prometheus instances	Logical units used to manage Prometheus data collection, storage, and analysis.
Prometheus probes	Deployed in the Kubernetes clusters on the user or cloud product side. Prometheus probes automatically discover targets, collect metrics, and remotely write data to databases.
PromQL	Prometheus query language. Supports both query based on specified time spans and instantaneous query, and provides multiple built-in functions and operators. Raw data can be aggregated, sliced, predicted, and combined.
Sample	Value corresponding to a time point in a timeline. For Prometheus monitoring, each sample consists of a value of the float64 data type and a timestamp with millisecond precision.
Alarm rule	Alarm configuration for Prometheus monitoring. An alarm rule can be specified using PromQL.
Tag	A key-value pair that describes a metric.
Metric management	Automatically discovers collection targets without static configuration. Supports multiple metric management modes (such as Kubernetes SD, Consul, and Eureka) and exposes collection targets through ServiceMonitor or PodMonitor.
Recording rules	With recording rules, raw data can be processed into new metrics using PromQL to improve query efficiency.
Time series	Consist of metric names and tags. Time series are streams of timestamped values belonging to the same metric and the same set of tagged dimensions.
Remote storage	Self-developed time series data storage component. It supports the remote write protocol related to Prometheus monitoring and is fully hosted by cloud products.
Cloud product monitoring	Seamlessly integrates monitoring data of multiple cloud products. To monitor cloud products, connect them first.

Concept	Description
Metrics	Labeled data exposed by targets, which can fully reflect the operation or service status of monitored objects. Prometheus monitoring uses the standard data format of OpenMetrics to describe metrics.

7.2 Creating Prometheus Instances

7.2.1 Prometheus Instance for Cloud Services

This type of instance is recommended when you need to monitor multiple metrics of cloud services.

Precautions

- Only one Prometheus instance for cloud services can be created in an enterprise project.

Creating a Prometheus Instance for Cloud Services

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.

Step 3 Set the instance name, enterprise project, and instance type.

Table 7-7 Parameters for creating a Prometheus instance

Parameter	Description
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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • 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.
Instance Type	Type of the Prometheus instance. Select Prometheus for Cloud Services .

Step 4 Click **OK**.

----End

Connecting Cloud Services

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** On the Prometheus instance list page, click a Prometheus instance for cloud services.
- Step 4** In the **Unconnected Cloud Services** area on the right, select a cloud service to connect.
- Step 5** In the displayed dialog box, set information about the cloud service.

Table 7-8 Connecting a cloud service

Parameter	Description
Select Prometheus Instance for Cloud Services	<p>Connect cloud service metrics to the Prometheus instance for cloud services.</p> <ul style="list-style-type: none"> • Enterprise Project By default, the value is the enterprise project selected in Step 3. This option is grayed and cannot be changed. <p>NOTE When connecting a cloud service through the access center, you can select the desired enterprise project from the drop-down list. If the existing enterprise projects cannot meet your requirements, create one by referring to Creating an Enterprise Project.</p> <ul style="list-style-type: none"> • Prometheus Instance for Cloud Services By default, the value is the Prometheus instance selected in Step 3. This option is grayed and cannot be changed. <p>NOTE By default, the value of this parameter is the Prometheus instance for cloud services under your selected enterprise project. If there is no such a Prometheus instance, create one.</p>
(Optional) Connect Cloud Service Tags	<p>Tags are used for aggregation and association. Select tag keys and their values will then be automatically synchronized. If the existing tags cannot meet your requirements, click Go to Tag Management Service (TMS) to add tags.</p>
Auto Sync	<p>If this function is enabled, tag changes will be synchronized.</p>

- Step 6** Click **Connect Now**.

----End

More Operations

You can also perform the operations listed in [Table 7-9](#) on the details page of the Prometheus instance for cloud services.

Table 7-9 Related operations

Operation	Description
Searching for cloud services	On the Cloud Service Connection page, enter a keyword in the search box to search for a cloud service.
Disconnecting cloud services	On the Cloud Service Connection page, click a target cloud service. In the displayed dialog box, click Disconnect Cloud Service .
Checking or modifying tag configurations of connected cloud services	On the Cloud Service Connection page, click a cloud service under Connected Cloud Services to change cloud service tag settings. For details, see Table 7-8 .

7.2.2 Prometheus Instance for ECS

This type of instance is recommended when you need Prometheus monitoring in a VPC (usually an ECS cluster) on the cloud. If needed, add Prometheus middleware monitoring at the access center.

Creating a Prometheus Instance for ECS

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.
- Step 3** Set an instance name, enterprise project, and instance type.

Table 7-10 Parameters for creating a Prometheus instance

Parameter	Description
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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none">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.
Instance Type	Type of the Prometheus instance. Select Prometheus for ECS .

Step 4 Click **OK**.

----End

Configuring a Collection Task

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.

Step 3 In the instance list, click the target Prometheus instance for ECS. The **Access Center** page is displayed.

Step 4 In the **Not Installed** panel on the right, locate the desired plug-in and click **Install**.

- Configure a collection task and install Exporter. For details, see [7.7.2.1 Access Overview](#).
- After the plug-in is installed, metrics can be reported to AOM. You can then check the metrics on the **Metric Management** page of the Prometheus instance.
- Click **Connected Collection Tasks** to check information about the connected collection tasks. You can also delete them if they are no longer needed.

Step 5 (Optional) In the **Installed** panel on the right, locate the target plug-in and click **Connect XX**, for example, **Connect MySQL**, and then configure collection tasks as required.

----End

7.2.3 Prometheus Instance for CCE

This type of instance is recommended when you need to monitor CCE clusters and applications running on them. By default, CCE clusters are monitored. If needed, add component monitoring through the access center.

Precautions

- You can connect clusters only when the kube-prometheus-stack add-on exists on the **Add-ons** page of CCE.
- Before installing the kube-prometheus-stack add-on, ensure that there are at least 4 vCPUs and 8 GiB memory. Otherwise, this add-on cannot work.

Creating a Prometheus Instance for CCE

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.

Step 3 Set the instance name, enterprise project, and instance type.

Table 7-11 Parameters for creating a Prometheus instance

Parameter	Description
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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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.
Instance Type	Type of the Prometheus instance. Select Prometheus for CCE .

Step 4 Click **OK**.

----End

Connecting a CCE Cluster

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.

Step 3 In the instance list, click a Prometheus instance for CCE.

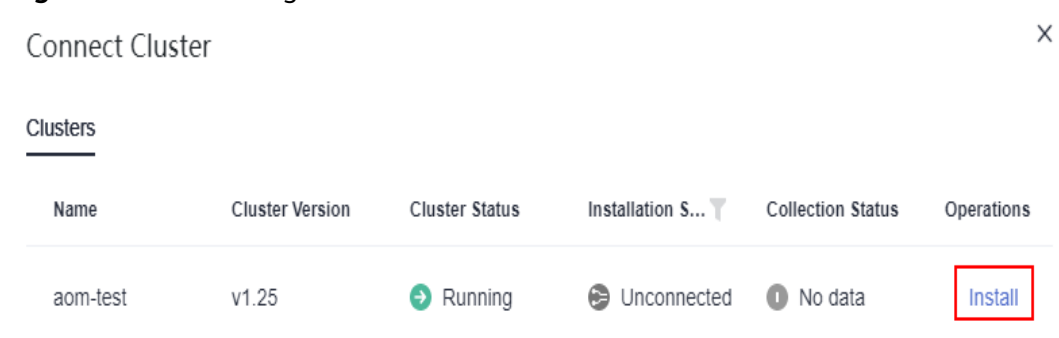
Step 4 On the **Integration Center** page, click **Connect Cluster**. In the cluster list, you can view the cluster information, installation status, and collection status.

Figure 7-1 Viewing cluster connection information



Step 5 Locate a target cluster and click **Install** in the **Operation** column to install the Prometheus add-on.

Figure 7-2 Connecting a CCE cluster



Step 6 After the installation is complete, click **Close** to connect the CCE cluster and bind it with the current Prometheus instance.

To disconnect the CCE cluster, click **Uninstall**.

----End

7.2.4 Common Prometheus Instance

This type of instance is recommended when you have built Prometheus servers and need to ensure the availability and scalability of Prometheus storage through remote write.

Creating a Common Prometheus Instance

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.

Step 3 Set the instance name, enterprise project, and instance type.

Table 7-12 Parameters for creating a Prometheus instance

Parameter	Description
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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> 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.
Instance Type	Type of the Prometheus instance. Select Common Prometheus Instance .

Step 4 Click **OK**.

----End

7.3 Managing Prometheus Instances

You can view the names, types, and enterprise projects of Prometheus instances in the instance list and modify and delete them as required.

Procedure







- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, view the created Prometheus instances and perform the operations listed in **Table 7-13** if needed.

Figure 7-3 Managing Prometheus instances

Prometheus Instance	Instance Type	Enterprise Project	Billing Mode	Operation
Prometheus_AOM_Default	default	default	Pay-per-Use Created on Aug 26, 2024 09:35:43 GMT+08:00	
	Prometheus for ECS	default	Pay-per-Use Created on Aug 26, 2024 16:12:37 GMT+08:00	
	Prometheus for CCE	default	Pay-per-Use Created on Aug 26, 2024 09:50:49 GMT+08:00	

Table 7-13 Related operations

Operation	Description
Searching for a Prometheus instance	Enter an instance name in the search box and click .
Filtering and displaying Prometheus instances	Click next to the Instance Type column to filter Prometheus instances.
Refreshing Prometheus instances	Click in the upper right corner of the Prometheus instance list to obtain their latest information in real time.

Operation	Description
Checking a Prometheus instance	<p>The Prometheus instance list displays information such as the instance name, instance type, billing mode, and enterprise project in real time.</p> <ul style="list-style-type: none"> ● When you have an access code: <p>Click an instance name. On the displayed instance details page, choose Settings and view the basic information and credential of the instance.</p> <ul style="list-style-type: none"> – By default, the AppSecret is hidden. To show it, click  or  reflects the status of the AppSecret. – In the Grafana Data Source Info area, obtain the Grafana data source configuration code in the private or public network of the desire Prometheus instance. Then click  on the right to copy the code to the corresponding file. – In the Service Addresses area, obtain the configuration code in the private or public network of the desire Prometheus instance. Then click  on the right to copy the code to the corresponding file. For details, see 7.8 Obtaining the Service Address of a Prometheus Instance. ● When you do not have an access code: <ol style="list-style-type: none"> 1. Click an instance name. On the displayed instance details page, choose Settings and view the basic information about the instance. The system displays a message indicating that there is no access code. 2. Click Add Access Code. In the displayed dialog box, click OK. Then, choose Settings in the navigation pane of the AOM 2.0 console. On the displayed page, choose Authentication in the navigation pane and manage access codes. For details, see More Operations.
Modifying a Prometheus instance	<ul style="list-style-type: none"> ● Modify a Prometheus instance name: <p>Click  in the Operation column that contains the target Prometheus instance. The name of each Prometheus instance in an enterprise project must be unique.</p> ● Modify Prometheus instance configurations: <p>In the Prometheus instance list, click the name of a Prometheus instance for cloud services/CCE and modify the cloud services/CCE clusters if needed.</p>
Deleting a Prometheus instance	<p>Click  in the Operation column that contains the target Prometheus instance.</p>

Operation	Description
Checking the billing information of a Prometheus instance	<p>In the Prometheus instance list, the Billing Mode column displays the billing mode and creation time of the Prometheus instance. Currently, only pay-per-use billing is supported.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If your account is frozen or restricted, you cannot add, delete, or modify Prometheus instances. • To continue using your cloud services, top up your account in time.

----End

7.4 Configuring a Recording Rule

Recording rules can be used for secondary development of metric data. Some queries may require a large amount of computing on the query end, resulting in high pressure on this end. By setting recording rules, you can move the computing process to the write end, reducing resource usage on the query end. Especially in large-scale clusters and complex service scenarios, recording rules can reduce PromQL complexity, thereby improving the query performance and preventing slow user configuration and queries.

Prerequisite

Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.3 Prometheus Instance for CCE](#).

Configuring a Recording Rule

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Settings**. In the **Recording Rules** area, click **Edit RecordingRule.yaml**.
- Step 5** In the dialog box that is displayed, delete the default content and enter a custom recording rule.

NOTE

Only one **RecordingRule.yaml** file needs to be configured for a cluster. Each rule group name must be unique.

Figure 7-4 Configuring a recording rule

Edit RecordingRule.yaml ✕

```

1 # groups:
2 #   - name: apiserver_request_total
3 #     interval: 60s
4 #     rules:
5 #       - record: job_instance_mode:apiserver_request_total:avg_rate5m
6 #         expr: avg by (job, instance, mode) (rate(apiserver_request_total[5m]))
7 #         labels:
8 #           team: operations
9 #       - record: job:apiserver_request_total:sum_rate10m
10 #        expr: sum by (job)(rate(apiserver_request_total[10m]))
11 #        labels:
12 #          team: operations
    
```

Table 7-14 Recording rule parameters

Parameter	Description
groups	Rule group. You can set multiple rule groups in one RecordingRule.yaml file.
name	Rule group name. Each rule group name must be unique.
interval	(Optional) Execution interval of a rule group. The default value is 60s .
rules	Rule. A rule group can contain multiple rules.
record	Name of a rule. The name must comply with Prometheus metric name specifications .
expr	Calculation expression. It is used to calculate metric values. It must comply with PromQL requirements .
labels	(Optional) Label of a metric.

Example of a recording rule:

```

groups:
- name: apiserver_request_total
  interval: 60s
  rules:
  - record: apiserver_request_rate
    expr: avg by (job, instance, mode) (rate(apiserver_request_total[5m]))
    labels:
      team: operations
  - record: job:apiserver_request_total:sum_rate10m
    expr: sum by (job)(rate(apiserver_request_total[10m]))
    labels:
      team: operations
    
```

Step 6 Click **OK**.

----End

Viewing Recording Rule Metrics

After a recording rule is configured, you can view its metrics on the [Metric Browsing](#) page of AOM or using Grafana.

Method 1: Viewing Metrics on the [Metric Browsing](#) Page of AOM

- Step 1** On the **Metric Browsing** page, select a Prometheus instance for which a recording rule has been configured from the drop-down list.
- Step 2** Click **All metrics** and enter the name of a recording rule metric in the search box to view its details.

----End

Method 2: Viewing Metrics Using Grafana

For details, see [7.9 Viewing Prometheus Instance Data Through Grafana](#).

7.5 Metric Management

7.5.1 Configuring Metrics

You can check the metrics of a default/common Prometheus instance, or a Prometheus instance for CCE/ECS/cloud services, and add or discard metrics.

Prerequisites

- Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.3 Prometheus Instance for CCE](#).
- Both your service and cloud services have been connected to a Prometheus instance for cloud services. For details, see [7.2.1 Prometheus Instance for Cloud Services](#).
- Both your service and plug-in have been connected to a Prometheus instance for ECS. For details, see [7.2.2 Prometheus Instance for ECS](#).
- Your service has been connected to a common Prometheus instance. For details, see [7.2.4 Common Prometheus Instance](#).

Precautions

- Only the default/common Prometheus instance, and Prometheus instance for CCE/ECS/cloud services support the functions of checking, adding, and discarding metrics.
- Default Prometheus instance: Metrics whose names start with **aom_** or **apm_** and resource type is **ICAgent** cannot be discarded.
- Prometheus instances for ECS: Only metrics collected by UniAgent can be displayed and configured.
- Prometheus instances for CCE:
Only the metrics reported by kube-prometheus-stack 3.9.0 or later installed on CCE **Add-ons** or AOM **Integration Center** can be discarded. Ensure that this add-on is running when discarding metrics.

 **NOTE**

To view the kube-prometheus-stack status, log in to the CCE console and access the cluster page, choose **Add-ons** in the navigation pane, and locate that add-on on the right.

Checking the Metrics of a Prometheus Instance for CCE

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Metric Management**. On the **Metrics** tab page, check the metric names and types of the current Prometheus instance.

You can also filter metrics by cluster name, job name, or metric type, or enter a metric name keyword to search.

Table 7-15 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

Checking the Metrics of a Prometheus Instance for Cloud Services

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for cloud services.
- Step 4** In the navigation pane on the left, choose **Metric Management**. Then check the metric names and types of the current Prometheus instance.

You can also filter metrics by metric or resource type, or enter a metric name keyword to search.

Table 7-16 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .

Parameter	Description
Resource Type	Type of a resource. That is, the type of the connected cloud service.

----End

Checking the Metrics of a Prometheus Instance for ECS

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for ECS.
- Step 4** In the navigation pane on the left, choose **Metric Management** and select a desired plug-in type and collection task. Then you can check all metric names and types of the Prometheus instance.

You can also specify a metric or resource type to filter metrics, or enter a metric name keyword to search.

Table 7-17 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Resource Type	Type of a resource, which is the cloud service to which the metric belongs.
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

Checking the Metrics of a Default Prometheus Instance

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a default Prometheus instance.
- Step 4** In the navigation pane on the left, choose **Metric Management**. Then check the metric names and types of the current Prometheus instance.

You can also filter metrics by metric or resource type, or enter a metric name keyword to search.

Table 7-18 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Resource Type	Type of a resource.
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

Checking the Metrics of a Common Prometheus Instance

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a common Prometheus instance.
- Step 4** In the navigation pane on the left, choose **Metric Management**. Then check the metric names and types of the current Prometheus instance.

You can also filter metrics by metric or resource type, or enter a metric name keyword to search.

Table 7-19 Metric parameters






Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Resource Type	Type of a resource.
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

More Operations

You can also perform the operations listed in [Table 7-20](#) if needed.

Table 7-20 Related operations

Operation	Description
Sorting metrics	Click  next to the Metrics in Last 10 Min or Proportion column to change the orders of metrics in the list.  indicates the default order.  indicates the ascending order (that is, the largest value is displayed at the bottom).  indicates the descending order (that is, the smallest value is displayed at the bottom).
Adding metrics	Click Add Metric , select desired metrics from the metric list, and click OK . NOTE A maximum of 100 metrics can be added each time.
Discarding metrics	<ul style="list-style-type: none"> To discard a metric, locate it and click  in the Operation column. To discard one or more metrics, select them and click Discard in the displayed dialog box. NOTE A maximum of 100 metrics can be discarded each time.

7.5.2 Configuring Metric Management for CCE Clusters

By adding ServiceMonitor or PodMonitor, you can configure Prometheus collection rules to monitor the applications deployed in CCE clusters.

Prerequisite

Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.3 Prometheus Instance for CCE](#).

Precautions

Only when kube-prometheus-stack installed on the **Add-ons** page of CCE or the **Integration Center** page of AOM is 3.9.0 or later and is still running, can you enable or disable collection rules.

NOTE

To view the kube-prometheus-stack status, log in to the CCE console and access the cluster page, choose **Add-ons** in the navigation pane, and locate that add-on on the right.

Adding ServiceMonitor

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.

- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Metric Management**. On the **Settings** tab page, click **ServiceMonitor**.
- Step 5** Click **Add ServiceMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 7-5 Adding ServiceMonitor

```

Create Prometheus.yaml
YAML
1 #apiVersion: monitoring.coreos.com/v1
2 #kind: ServiceMonitor
3 #metadata:
4 # name: go-demo # Enter a unique name.
5 # namespace: monitoring # Namespace cannot be changed.
6 #spec:
7 # endpoints:
8 # - interval: 30s
9 # Enter the port name of Prometheus Exporter in your service YAML.name: metric-port
10 # port: metric-port
11 # Enter the path of Prometheus Exporter. Default: /metrics
12 # path: /metrics
13 # relabelings:
14 # ** There must be at least one label named 'application'.
15 # Here, label 'app' was replaced with 'application'.
16 # - action: replace
17 # sourceLabels: [__meta_kubernetes_pod_label_app]
18 # targetLabel: application
19 # Enter the namespace of your service.
20 # namespaceSelector:
21 # matchNames:
22 # - golang-demo
23 # Enter the label of your service to monitor.
24 # selector:
25 # matchLabels:
26 # app: golang-app-demo
    
```

After the configuration is complete, the new collection rule is displayed in the list.

Figure 7-6 Configuring a collection rule

Name	Tag	Namespace	Configuration Mode	Created	Status	Operation
coredns	app:coredns	monitoring	Custom	Jun 13, 2024 15:28:46 GMT+08:00	On	(+) (-)
etcd-server	app:kubernetes.io/managed-by: Helm	monitoring	System	Jun 13, 2024 15:28:46 GMT+08:00	Off	(+) (-)
kube-apiserver	app:kubernetes.io/managed-by: Helm	monitoring	System	Jun 13, 2024 15:28:46 GMT+08:00	On	(+) (-)
kube-controller	app:kubernetes.io/managed-by: Helm	monitoring	System	Jun 13, 2024 15:28:46 GMT+08:00	Off	(+) (-)

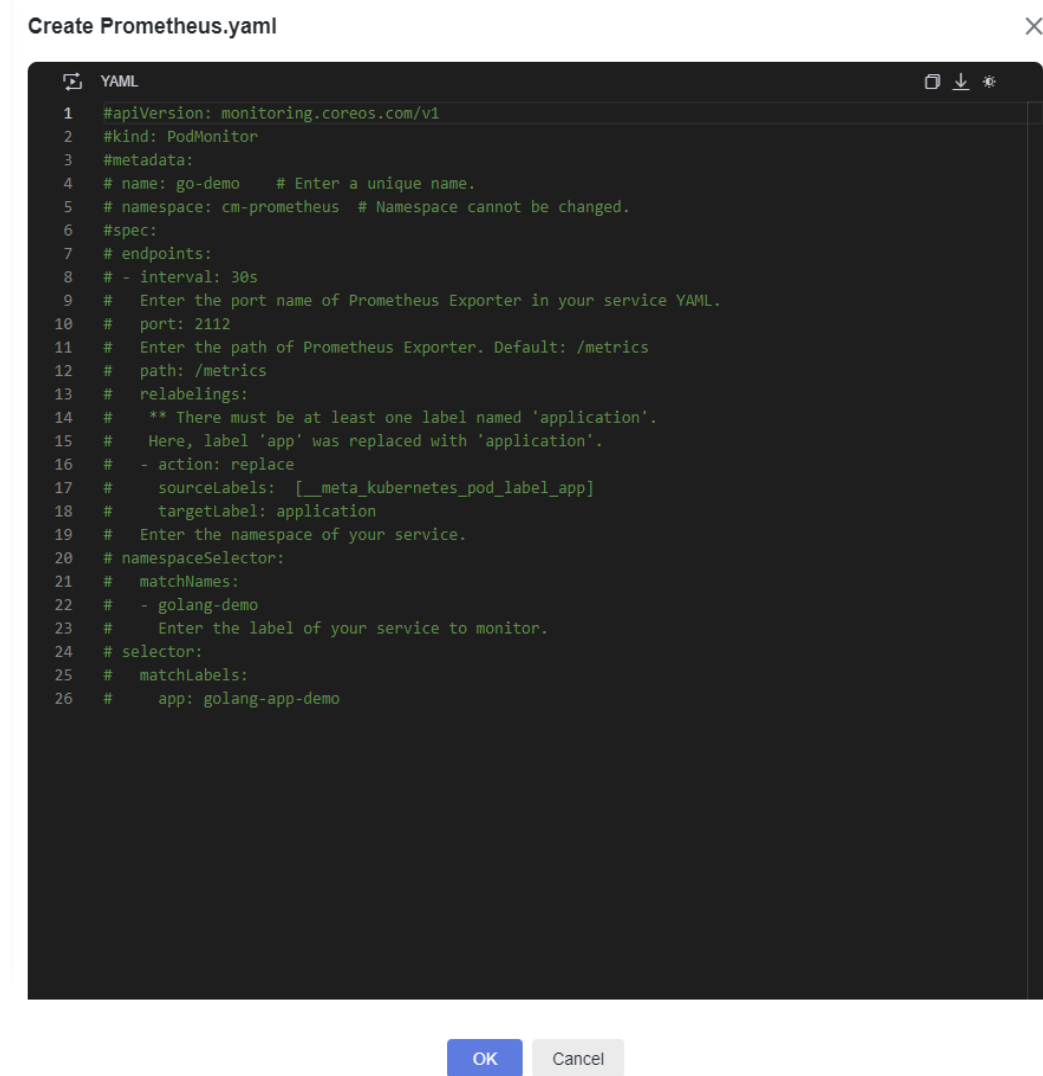
----End

Adding PodMonitor

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Metric Management**. On the **Settings** tab page, click **PodMonitor**.

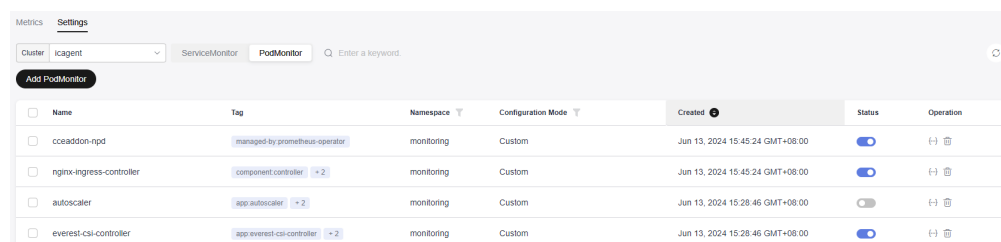
Step 5 Click **Add PodMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 7-7 Adding PodMonitor



After the configuration is complete, the new collection rule is displayed in the list.

Figure 7-8 Configuring a collection rule








----End

More Operations

Perform the operations listed in [Table 7-21](#) if needed.

Table 7-21 Related operations

Operation	Description
Checking metric management configuration	<ul style="list-style-type: none"> In the list, check information such as the name, tag, namespace, and configuration mode. You can filter information by cluster name, namespace, or configuration mode. Click  in the Operation column. In the displayed dialog box, view details about the ServiceMonitor or PodMonitor collection rule.
Enabling or disabling collection rules	<p>On the Settings tab page of the Metric Management page, click  in the Status column to enable or disable collection rules.  indicates that collection rules are disabled.  indicates that collection rules are enabled.</p>
Deleting metric management configuration	Click  in the Operation column.

7.6 Dashboard Monitoring

With preset dashboard templates, you can monitor the metrics of the default Prometheus instance or Prometheus instances for cloud services to locate and detect resource data problems and improve O&M efficiency.

Prerequisite

Both your service and cloud services have been connected to a Prometheus instance for cloud services. For details, see [7.2.1 Prometheus Instance for Cloud Services](#).

Precautions

Currently, only the default Prometheus instance or the Prometheus instance for cloud services supports metric monitoring using preset dashboard templates.

Monitoring the Metrics of a Default Prometheus Instance

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.

- Step 3** In the instance list, click a default Prometheus instance.
- Step 4** In the navigation pane, choose **Dashboards** to check all preset dashboard templates.
- Step 5** Click a desired dashboard template to monitor the metrics of the current Prometheus instance.

For example, to monitor the disk partition information of a host, click **disk-partition-template** and select the target host IP address and disk partition. You can also perform the operations listed in [Table 7-22](#).

----End

Monitoring the Metrics of a Prometheus Instance for Cloud Services






- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for cloud services.
- Step 4** In the navigation pane, choose **Dashboards** to check all preset dashboard templates.
- Step 5** Click a desired dashboard template to monitor the metrics of the current Prometheus instance.




For example, to monitor the CCE workload information, click **cce-workload-template** and select the target service ID. You can also perform the operations listed in [Table 7-22](#).

----End

More Operations

Table 7-22 Operations related to dashboards

Operation	Description
Full-screen display	Click the target dashboard and click  in the upper right corner of the dashboard page to view the dashboard in full screen.
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  or  , or press Esc on the keyboard.
Manual refresh	Click the target dashboard and click  in the upper right corner of the dashboard page and manually refresh the current page.
Auto refresh	Click the target dashboard and click the arrow next to  in the upper right corner of the dashboard page and enable auto refresh.

Operation	Description
Rotating dashboards	Click a target dashboard and click  in the upper right corner of the dashboard details page. Set full-screen display by referring to 3.2 Setting the Full-Screen Online Duration .
Setting the query time	Select the target dashboard. In the upper right corner of the dashboard page, click the time range next to  and select Last 30 minutes, Last hour, Last 6 hours, Last day, Last week, or Custom from the drop-down list. If you select Custom , select a time range in the calendar that is displayed. The time can be accurate to seconds. Then click OK , so that you can query data in the dashboard based on the selected time range.
Exporting a monitoring report	Click a dashboard to go to its details page. Then click  in the upper right corner, and choose Export Line Graph Report to export a CSV file to your local PC.

7.7 Access Guide

7.7.1 Connecting Node Exporter

Node Exporter is provided by Prometheus to collect information about Linux hosts, including the CPU, memory, load, file system, and network. After metrics are reported to AOM using Node Exporter, you can check the metrics on the **Metric Management** page of the Prometheus instance for ECS.

Prerequisite

The UniAgent has been installed on the host. For details, see [10.4.2.1 Installing a UniAgent](#).

Precaution

A host supports only one Node Exporter.

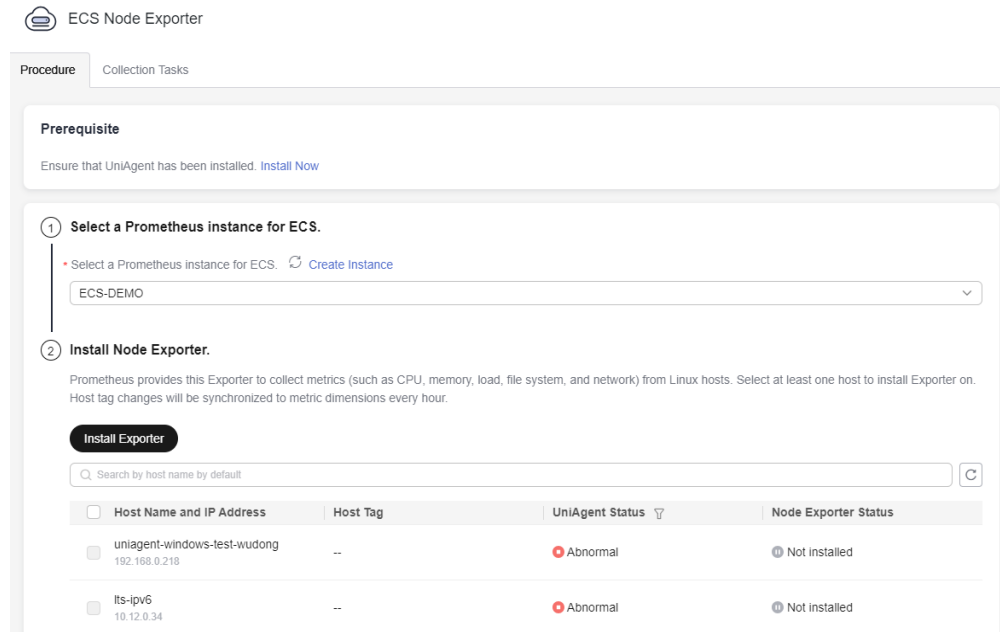
Installing Node Exporter

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Access Center**.
- Step 3** On the **Prometheus Running Environments** panel, click the **ECS Node Exporter** card.
- Step 4** On the **Procedure** tab page of the **ECS Node Exporter** dialog box, perform the installation as prompted.
 1. Select a target Prometheus instance for ECS from the drop-down list.
 2. Select one or more hosts to install Node Exporter.

Step 5 Click **Install** to complete the installation.

Upon installation, Node Exporter can collect metrics. By default, both the collection period and timeout period are 60s.

Figure 7-9 Installing Node Exporter




----End

Checking a Collection Task

After Node Exporter is installed, perform the operations listed in [Table 7-23](#) on the **Collection Tasks** tab page of the **ECS Node Exporter** dialog box.

Table 7-23 Related operations

Operation	Description
Searching for a collection task	You can search for collection tasks by collection task, collection status, host IP address, or host name.
Refreshing a collection task	Click  in the upper right corner of the collection task list to obtain the latest information.
Deleting a collection task	Click Delete in the Operation column.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.

7.7.2 Exporter Access in the VM Scenario

7.7.2.1 Access Overview

Prometheus monitoring integrates common infrastructure, custom components, and middleware. By creating collection tasks and executing plug-in scripts, it can monitor corresponding components. It works with AOM and open-source Grafana to provide one-stop, comprehensive monitoring, helping you quickly detect and locate faults and reduce their impact on services.

The connected components are displayed on the collection task page. You can set [dashboards](#) and [alarm rules](#) for the components.

There are two types of collection tasks: middleware and custom.

- Middleware collection tasks: created using [middleware plug-ins](#).
- Custom collection tasks: created using [custom plug-ins](#).

AOM allows you to quickly install middleware plug-ins and custom plug-ins and provides ready-to-use dashboards for Prometheus monitoring.

- **Middleware:** You can directly use built-in middleware plug-ins to create collection tasks. The built-in middleware plug-ins cannot be customized, modified, or deleted. The following middleware plug-ins are supported:
 - **MYSQL:** monitors MySQL metrics.
 - **REDIS:** monitors Redis metrics.
 - **KAFKA:** monitors Kafka metrics.
 - **NGINX:** monitors Nginx metrics.
 - **MONGODB:** monitors MongoDB metrics.
 - **CONSUL:** monitors Consul metrics.
 - **NODE:** monitors Node metrics.
 - **HAPROXY:** monitors HAProxy metrics.
 - **POSTGRESQL:** monitors PostgreSQL metrics.
 - **ELASTICSEARCH:** monitors Elasticsearch metrics.
 - **RABBITMQ:** monitors RabbitMQ metrics.
 - **CUSTOM_EXPORTER:** monitors custom component metrics.
- **Custom plug-ins:** user-defined.

7.7.2.2 MySQL Component Access

Application Scenario

Create collection tasks using the built-in MySQL plug-in. After installing this plug-in, you can monitor MySQL metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- [The UniAgent has been installed](#) and is running.

- **A Prometheus instance for ECS** has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click the **MySQL** card on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table.

Figure 7-10 Configuring a collection task

Collection Task

* Collection Task Name

* Host

Used for Exporter installation.

Metric Dimension (18metrics)


Advanced Settings ^


* Collection Period (s)

* Timeout Period (s)

* Executor

Table 7-24 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the MySQL plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is MYSQL .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-11 Installing Exporter

Install Exporter

• *mysql Username ?

• *mysql password ?

• *mysql address ?

Parameter	Description
MySQL Username	Username of MySQL.
MySQL Password	Password of MySQL.
MySQL Address	IP address and port number of MySQL, for example, 10.0.0.1:3306 .

Step 5 Click **Install** to connect the MySQL plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.3 Redis Component Access

Application Scenario

Create collection tasks using the built-in Redis plug-in. After installing this plug-in, you can monitor Redis metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click the **Redis** card on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-12 Configuring a collection task

Collection Task

* Collection Task Name

* Host

Used for Exporter installation.

Metric Dimension (28metrics)


Advanced Settings ^


* Collection Period (s)

* Timeout Period (s)

* Executor

Table 7-25 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the Redis plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is REDIS .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-13 Installing Exporter

Install Exporter

• *redis address ?

• redis password ?

Parameter	Description
Redis Address	IP address and port number of Redis, for example, 127.0.0.1:3306 .
Redis Password	Password for logging in to Redis.

Step 5 Click **Create** to connect the Redis plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.4 Kafka Component Access

Application Scenario

Create collection tasks using the built-in Kafka plug-in. After installing this plug-in, you can monitor Kafka metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click the **Kafka** card on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-14 Configuring a collection task

Collection Task

* Collection Task Name

* Host

+ Add Host ✓

i Used for Exporter installation.

Labels (15metrics)

job exporter instance target _app: ✕ +

Advanced Settings ^

* Collection Period (s)

10s ▾

* Timeout Period (s)


10s ▾


* Executor

root

Table 7-26 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .

Operation	Parameter	Description
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the Kafka plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is KAFKA .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-15 Installing Exporter

Parameter	Description
Kafka address	IP address and port number of Kafka, for example, 10.0.0.1:3306 .
SASL enabled	Enter enabled or disabled . By default, SASL is disabled. <ul style="list-style-type: none"> • enabled: Enable SASL. • disabled: Disable SASL.
SASL username	SASL username.
SASL password	SASL password.
SASL mechanism	Enter an SASL mechanism. Options: plain , scram-sha512 , and scram-sha256 . By default, this parameter is left blank.

Parameter	Description
TLS enabled	Enter enabled or disabled . By default, TLS is disabled. <ul style="list-style-type: none"> • enabled: Enable TLS. • disabled: Disable TLS.

Step 5 Click **Create** to connect the Kafka plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.5 Nginx Component Access

Application Scenario

Create collection tasks using the built-in Nginx plug-in. After installing this plug-in, you can monitor Nginx metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS](#) has been created.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center**. Then click the **Nginx** card on the **Prometheus Middleware** panel.

Step 3 On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-16 Configuring a collection task

Collection Task

★ Collection Task Name

★ Host

+ Add Host ✓

Used for Exporter installation.

Metric Dimension (9metrics)

job exporter instance target _env:"" × +

Advanced Settings ^

★ Collection Period (s)

10s ▼

★ Timeout Period (s)


10s ▼


★ Executor

root

Table 7-27 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the Nginx plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.

Operation	Parameter	Description
	Collection Plug-in	The default value is NGINX .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-17 Installing Exporter

Install Exporter

• *nginx url 

https://[redacted]/stub_status

Parameter	Description
Nginx URL	<p>Nginx URL, which is in the format of "Connection address of Nginx+Nginx service status path".</p> <ul style="list-style-type: none"> • Connection address of Nginx: IP address and listening port number of the Nginx service. The listening port is specified in the nginx.conf file. Example: 10.0.0.1:8080 • Nginx service status path: specified by the location parameter in the nginx.conf file, for example, /stub_status. <p>Example: https://10.0.0.1:8080/stub_status</p>

Step 5 Click **Create** to connect the Nginx plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.6 MongoDB Component Access

Application Scenario

Create collection tasks using the built-in MongoDB plug-in. After installing this plug-in, you can monitor MongoDB metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

Step 1 Log in to the AOM 2.0 console.

- Step 2** In the navigation pane on the left, choose **Access Center**. Then click the **MongoDB** card on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-18 Configuring a collection task

Collection Task

* Collection Task Name

* Host

+ Add Host ✔

Used for Exporter installation.

Metric Dimension (10metrics)

job exporter instance target _app:

Advanced Settings ^

* Collection Period (s)

10s

* Timeout Period (s)


10s


* Executor

root

Table 7-28 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .

Operation	Parameter	Description
Set Plug-in	OS	<p>Operating system of the host. Options: Linux and Windows. To use the MongoDB plug-in, select Linux.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If Linux is used, you can select a middleware or custom plug-in. • If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is MONGODB .
	Plug-in Version	<p>Select a plug-in version.</p> <p>NOTE</p> <p>Plug-in versions that have not been released are dimmed and cannot be selected.</p>
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host and select a running host for configuring the collection task and installing Exporter.</p> <p>Specify host: Select a host that has been connected.</p> <ul style="list-style-type: none"> • On the Specify host page, search for and select a host by the host name, IP address, or Agent status. • On the Specify host page, click  in the upper right corner to deselect the host if needed. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. <p>NOTE</p> <p>If you select a middleware plug-in, only one host can be selected.</p>

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-19 Installing Exporter

Install Exporter

• *mongodb address ?

• *mongodb port ?

• mongodb username ?

• mongodb password ?

Parameter	Description
MongoDB Address	IP address of MongoDB, for example, 10.0.0.1 .
MongoDB Port	Port number of MongoDB, for example, 3306 .
MongoDB Username	Username for logging in to MongoDB.
MongoDB Password	Password for logging in to MongoDB.

Step 5 Click **Create** to connect the MongoDB plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.7 Consul Component Access

Application Scenario

Create collection tasks using the built-in Consul plug-in. After installing this plug-in, you can monitor Consul metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS](#) has been created.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center**. Then click the **Consul** card on the **Prometheus Middleware** panel.

Step 3 On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-20 Configuring a collection task

Collection Task

* Collection Task Name

* Host

Used for Exporter installation.

Metric Dimension (7metrics)


Advanced Settings ^


* Collection Period (s)

* Timeout Period (s)

* Executor

Table 7-29 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the Consul plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is CONSUL .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.


Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-21 Installing Exporter

Install Exporter

• *consul address 

Parameter	Description
Consul Address	IP address and port number of Consul, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the Consul plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.8 HAProxy Component Access

Application Scenario

Create collection tasks using the built-in HAProxy plug-in. After installing this plug-in, you can monitor HAProxy metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS](#) has been created.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center**. Then click the **HAProxy** card on the **Prometheus Middleware** panel.

Step 3 On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-22 Configuring a collection task

Collection Task

* Collection Task Name

* Host

➕ Add Host ✔

Used for Exporter installation.

Metric Dimension (10metrics)

job exporter instance target _comp: [] +

Advanced Settings ^

* Collection Period (s)

10s

* Timeout Period (s)


10s


* Executor

root

Table 7-30 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the HAProxy plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is HAPROXY .

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> • On the Specify host page, search for and select a host by the host name, IP address, or Agent status. • On the Specify host page, click  in the upper right corner to deselect the host if needed. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

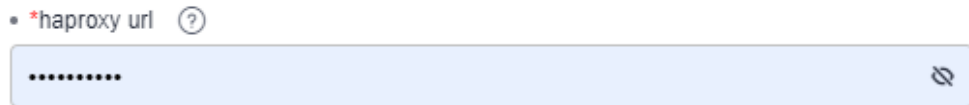
Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to check Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-23 Installing Exporter

Install Exporter



Parameter	Description
HAProxy URL	<p>HAProxy connection address, which must be in the format of "http://{username}:{password}@{IP address}:{port}/haproxy_stats;csv".</p> <ul style="list-style-type: none"> • <i>{username}</i>: username for logging in to HAProxy. • <i>{password}</i>: password for logging in to HAProxy. • <i>{IP}:{port}</i>: HAProxy IP address and port number, for example, 10.0.0.1:3306. <p>Example: http://admin:*****@10.0.0.1:3306/haproxy_stats;csv</p>

Step 5 Click **Install** to connect the HAProxy plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.9 PostgreSQL Component Access

Application Scenario

Create collection tasks using the built-in PostgreSQL plug-in. After installing this plug-in, you can monitor PostgreSQL metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center**. Then click the **PostgreSQL** card on the **Prometheus Middleware** panel.

Step 3 On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-24 Configuring a collection task

Collection Task

★ Collection Task Name

★ Host

+ Add Host ✔

Used for Exporter installation.

Metric Dimension (29metrics)

job exporter instance target _app: +

Advanced Settings ^

★ Collection Period (s)

10s ▼

★ Timeout Period (s)


10s ▼


★ Executor

root

Table 7-31 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .

Operation	Parameter	Description
Set Plug-in	OS	<p>Operating system of the host. Options: Linux and Windows. To use the PostgreSQL plug-in, select Linux.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If Linux is used, you can select a middleware or custom plug-in. • If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is POSTGRESQL .
	Plug-in Version	<p>Select a plug-in version.</p> <p>NOTE</p> <p>Plug-in versions that have not been released are dimmed and cannot be selected.</p>
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host and select a running host for configuring the collection task and installing Exporter.</p> <p>Specify host: Select a host that has been connected.</p> <ul style="list-style-type: none"> • On the Specify host page, search for and select a host by the host name, IP address, or Agent status. • On the Specify host page, click  in the upper right corner to deselect the host if needed. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. <p>NOTE</p> <p>If you select a middleware plug-in, only one host can be selected.</p>

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-25 Installing Exporter

Install Exporter

• *postgres Username ?

• *postgres password ?

• *postgres address ?

Parameter	Description
PostgreSQL Username	PostgreSQL username.
PostgreSQL Password	PostgreSQL password.
PostgreSQL Address	IP address and port number of PostgreSQL, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the PostgreSQL plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.10 Elasticsearch Component Access

Application Scenario

Create collection tasks using the built-in Elasticsearch plug-in. After installing this plug-in, you can monitor Elasticsearch metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click **Elasticsearch** on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-26 Configuring a collection task

Collection Task

* Collection Task Name

* Host

Used for Exporter installation.

Metric Dimension (176metrics)


Advanced Settings ^


* Collection Period (s)

* Timeout Period (s)

* Executor

Table 7-32 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use the Elasticsearch plug-in, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is ELASTICSEARCH .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host for configuring the collection task and installing Exporter. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-27 Installing Exporter

Install Exporter

• *elasticsearch url ?

Parameter	Description
Elasticsearch URL	IP address and port number of Elasticsearch, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the Elasticsearch plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.11 RabbitMQ Component Access

Application Scenario

Create collection tasks using the built-in RabbitMQ plug-in. After installing this plug-in, you can monitor RabbitMQ metrics and connect them to the ready-to-use Grafana dashboard.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS](#) has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click **RabbitMQ** on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table and click **Next**.

Figure 7-28 Configuring a collection task

Collection Task

* Collection Task Name

* Host

+ Add Host ✔

Used for Exporter installation.

Metric Dimension (23metrics)

job exporter instance target _app: +

Advanced Settings ^


* Collection Period (s)


* Timeout Period (s)

* Executor

Table 7-33 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .

Operation	Parameter	Description
Set Plug-in	OS	<p>Operating system of the host. Options: Linux and Windows. To use the RabbitMQ plug-in, select Linux.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If Linux is used, you can select a middleware or custom plug-in. • If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is RABBITMQ .
	Plug-in Version	<p>Select a plug-in version.</p> <p>NOTE</p> <p>Plug-in versions that have not been released are dimmed and cannot be selected.</p>
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host and select a running host for configuring the collection task and installing Exporter.</p> <p>Specify host: Select a host that has been connected.</p> <ul style="list-style-type: none"> • On the Specify host page, search for and select a host by the host name, IP address, or Agent status. • On the Specify host page, click  in the upper right corner to deselect the host if needed. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. <p>NOTE</p> <p>If you select a middleware plug-in, only one host can be selected.</p>

Operation	Parameter	Description
	Metric Dimension	<p>When Collection Plug-in is set to a middleware plug-in, the default metrics of the plug-in are displayed.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs if the installation fails.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Figure 7-29 Installing Exporter

Install Exporter

• *rabbitmq Username ?

• *rabbitmq password ?

• *rabbitmq address ?

Parameter	Description
RabbitMQ Username	RabbitMQ username.
RabbitMQ Password	RabbitMQ password.
RabbitMQ Address	IP address and port number of RabbitMQ, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the RabbitMQ plug-in. The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.12 Access of Other Components

Application Scenario

Use a custom Exporter to create a collection task to monitor metrics of the component. In addition, use Exporter to report database metrics for exception detection and Grafana dashboard display.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS** has been created.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Then click the **Other components** card on the **Prometheus Middleware** panel.
- Step 3** On the displayed page, set parameters by referring to the following table.

Figure 7-30 Configuring a collection task

Collection Task

* Collection Task Name

* Host

+ Add Host ✓

Used for Exporter installation.

Plug-in Collection Parameters

• *Exporter address ?

Metric Dimension

* Exporter Name

target job _app: × +

Advanced Settings ^

* Collection Period (s)

60s ▾

* Timeout Period (s)

60s ▾


* Executor


root

* Executor

root

Table 7-34 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . To use a custom exporter, select Linux . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	The default value is CUSTOM_EXPORTER .
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a running host. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host if needed. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a middleware plug-in, only one host can be selected.
	Plug-in Collection Parameters	Exporter Address: IP address and port number of the host where Exporter is installed. The format is "IP address:Port", for example, 10.0.0.1:9100

Operation	Parameter	Description
	Metric Dimension	<p>Exporter Name: Enter an exporter name.</p> <p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none"> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Includes Collection Period (s) and Timeout Period (s).</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). <p>NOTE The timeout period cannot exceed the collection period.</p> <ul style="list-style-type: none"> • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Click **Create**.

Step 5 The connected plug-in will be displayed on the collection task page. Click the name of a collection task. On the displayed page, you can check the configuration of the collection task.

----End

7.7.2.13 Custom Plug-in Access

Application Scenario

Use a custom plug-in to create a collection task to monitor specified metrics. In addition, use Exporter to report database metrics for exception detection and Grafana dashboard display.

Prerequisites

- [A UniAgent has been installed](#) on the host.
- [A Prometheus instance for ECS](#) has been created.
- [A custom plug-in](#) has been created.

Creating a Custom Plug-in

UniAgent allows you to create custom plug-ins. You can create a plug-in using scripts and create a collection task to use this plug-in by referring to [Custom Plug-in Access](#) to collect metrics.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Access Center**.
- Step 3** In the **Custom Prometheus Plug-in Access** panel, click **Custom Plug-in**.
- Step 4** On the displayed page, set related parameters.
 - Plug-in information

Table 7-35 Plug-in parameters

Parameter	Description
Plug-in Name	Name of a custom plug-in. Enter a maximum of 32 characters starting with a letter. Only letters, digits, and underscores (_) are allowed.
Plug-in Type	Type of a plug-in. The default value is Custom .
Description	Description of the plug-in to be created. Enter a maximum of 10,000 characters.

- Set Plug-in

Table 7-36 Plug-in configuration parameters





Parameter	Description
Plug-in Version	Version of the custom plug-in.

Parameter	Description
Plug-in Script	<p>Custom plug-in script. Options: Linux and Windows.</p> <p>Linux: Shell or Python script.</p> <p>Example:</p> <pre>#!/bin/bash #Examples echo "metric_name{label_name=\"label_value\"} 100"</pre> <p>Windows: BAT script</p> <p>Example:</p> <pre>::Examples @echo off echo metric_name{label_name="label_value"} 100</pre>
Default Script Parameter	<p>Custom script parameter template. Only letters, digits, and underscores (<code>_</code>) are allowed. Ensure that the following rules are met:</p> <ul style="list-style-type: none"> - Letter: For example, <code>-a</code>. - Character combination: For example, <code>http://127.0.0.1:80</code>. The following special characters are not allowed: <code>& ><;`!()\$-</code> - <code>\${Parameter}</code>: Enter a maximum of 64 characters starting with a letter. Only letters, digits, and underscores (<code>_</code>) are allowed. For example, <code>_\${a_b}</code>. <p>You can combine parameters as required and separate them with spaces. The total length of these parameters cannot exceed 250 characters.</p>
Script Parameter	<p>Parameters in the default script parameters. After you enter the default script parameters, the system automatically identifies script parameters based on your settings.</p> <p>Script parameter description:</p> <ul style="list-style-type: none"> - Mandatory: If this option is enabled, the parameter value in the plug-in debugging area is mandatory. If this option is disabled, the parameter value in the plug-in debugging area is optional. - Parameter: name of a script parameter. - Default Value: default value of the script parameter. - Description: description of the parameter.

Step 5 Click **Save**.

After a plug-in is created, you can modify it, create a version for it, or delete it.

Table 7-37 Related operations

Operation	Description
Checking the plug-in status	<p>Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Version. On the page that is displayed, check the plug-in status.</p> <ul style="list-style-type: none"> • Unreleased: When you create a plug-in or create a plug-in version, the plug-in status is Unreleased. You can click the version number to edit the plug-in. • Released: After you click Release in the Operation column, the plug-in status changes to Released. You can click the version number to view the plug-in details.
Creating a version	<p>Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Version. Click Create Version. On the displayed page, set the plug-in information.</p> <p>NOTE</p> <ul style="list-style-type: none"> • A maximum of five versions can be created for a plug-in. • If there is only one plug-in version, only Copy is available in the Operation column. If there is more than one plug-in, both Copy and Delete are available in the Operation column. You can click Delete to delete a plug-in version.
Modifying a plug-in	<p>Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Modify. On the displayed page, modify the plug-in information.</p>
Deleting a plug-in	<p>Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Delete. On the displayed page, click Yes to delete the plug-in.</p> <p>NOTE</p> <p>If a collection task has been configured for a plug-in, deleting the plug-in will also delete the collection task.</p>

----End

Custom Plug-in Access

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center**. Click the custom plug-in on the **Custom Prometheus Plug-in Access** panel.
- Step 3** On the collection task configuration page, set parameters by referring to the following table.

Figure 7-31 Configuring a collection task

Collection Task

* Collection Task Name

* Host

Tip: Hosts must be installed with UniAgents.

+ Add Host ✓

Advanced Settings ^


* Collection Period (s)

* Timeout Period (s)

* Executor

Table 7-38 Parameters for creating a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task will be associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . NOTE <ul style="list-style-type: none"> If Linux is used, you can select a middleware or custom plug-in. If Windows is used, you can only select a custom plug-in.
	Collection Plug-in	(Default) Created custom plug-in.

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. NOTE Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters and start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host and select a host. Specify host: Select a host that has been connected. <ul style="list-style-type: none"> On the Specify host page, search for and select a host by the host name, IP address, or Agent status. On the Specify host page, click  in the upper right corner to deselect the host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected. NOTE If you select a custom plug-in, you can select multiple hosts.
	Advanced Settings	Includes Collection Period (s) and Timeout Period (s) . <ul style="list-style-type: none"> Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). NOTE The timeout period cannot exceed the collection period. <ul style="list-style-type: none"> Executor: user who executes the collection task, that is, the user of the selected host. Default: root. Enter a username. Recommended: root.

Step 4 Click **Create**.








Step 5 On the displayed collection task page, click the target collection task to view its details.

----End

7.7.2.14 Other Operations

In the access center, click the middleware plug-in or custom plug-in of a created collection task. On the displayed page, click the **Collection Tasks** tab and perform the following operations as required.

Table 7-39 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click  in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. NOTE You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.  indicates the default order.  indicates the ascending order (that is, the maximum time is displayed at the bottom).  indicates the descending order (that is, the maximum time is displayed at the top).
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required. NOTE If no parameters need to be modified, skip this step.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required. NOTE <ul style="list-style-type: none"> Modifying a custom plug-in collection task: The plug-in version and collection task details can be modified. Modifying a middleware collection task: Only metric dimensions can be modified.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

7.8 Obtaining the Service Address of a Prometheus Instance

In the **Service Addresses** area on the **Settings** tab page of the default or common Prometheus instance or of the Prometheus instance for ECS, CCE, you can obtain the configuration code for Prometheus remote read and write. In the **Service Addresses** area on the **Settings** tab page of the Prometheus instance for cloud services, you can obtain the configuration code for Prometheus remote read.

Prerequisites

Your service has been connected for Prometheus monitoring. For more details, see:

- [Prometheus Instance for Cloud Services](#)
- [Prometheus Instance for ECS](#)
- [Prometheus Instance for CCE](#)
- [Common Prometheus Instance](#)

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the created Prometheus instance.
- Step 3** On the instance details page, choose **Settings** in the navigation pane to obtain the service address of the current instance.

The following describes how to obtain the service address of a Prometheus instance for CCE.


- Click the **Intranet** or **Public Network** tab to obtain the configuration code for Prometheus remote read and write in the intranet or public network. Click  on the right of the code to copy the code to the corresponding file.
- Obtain the configuration code for Prometheus remote read.

Figure 7-32 Configuration code for Prometheus remote read

```
Configuration Code for Prometheus Remote Read

remote_read:
  - url: 'https://aom
    tls_config:
      insecure_skip_verify: true
      bearer_token: '\N**aF'
      read_recent: true
    /api/v1/read'
```

Remote read address:

```
url: 'https://aom.{region_name}.{Site domain name suffix}/v1/{project_id}/api/v1/read'
```

Remote read address parameters:

- **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.
- **Site domain name suffix**: site domain name suffix, for example, **myhuaweicloud.com**.

- **project_id**: project ID.
- Obtain the configuration code for Prometheus remote write.

Figure 7-33 Configuration code for Prometheus remote write

Configuration Code for Prometheus Remote Write

```
remote_write:
- url: 'https://aom-internal-access.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/push'
  tls_config:
    insecure_skip_verify: true
  bearer_token: 'SE**IH'
```

Remote write address in the intranet:

url: 'https://aom-internal-access.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address in the public network:

url: 'https://aom-access.{region_name}.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address parameters:

- **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.
- **Site domain name suffix**: site domain name suffix, for example, **myhuaweicloud.com**.
- **project_id**: project ID.

----End

7.9 Viewing Prometheus Instance Data Through Grafana

After connecting a cloud service or CCE cluster to a Prometheus instance, you can use Grafana to view the metrics of the cloud service or cluster.

Prerequisites

- You have created an ECS. For details, see [Elastic Cloud Server \(ECS\) Getting Started](#).
- You have created an EIP and bound it to the created ECS. For details, see [Elastic Cloud Server \(ECS\) Getting Started](#).
- Your service has been connected for Prometheus monitoring. For more details, see:
 - [Prometheus Instance for Cloud Services](#)
 - [Prometheus Instance for ECS](#)
 - [Prometheus Instance for CCE](#)
 - [Common Prometheus Instance](#)

Procedure

Step 1 Install and start Grafana. For details, see the [Grafana official documentation](#).

Step 2 Add an access code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Settings**. The **Global Configuration** page is displayed.
3. In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

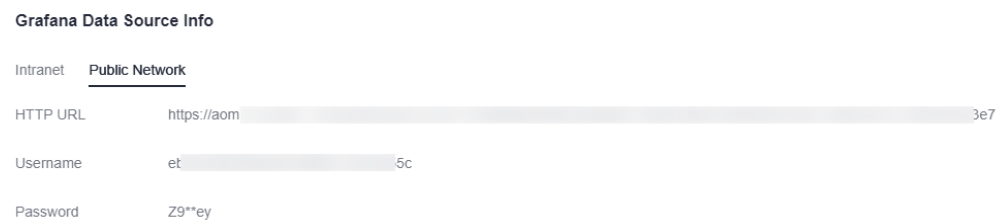
 **NOTE**

- You can create up to two access codes for each project.
- An access code is an identity credential for calling APIs. Keep your access code secure.

Step 3 Obtain the Grafana data source configuration code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the target Prometheus instance.
3. On the displayed page, choose **Settings** in the navigation pane and obtain the Grafana data source information from the **Grafana Data Source Info** area.

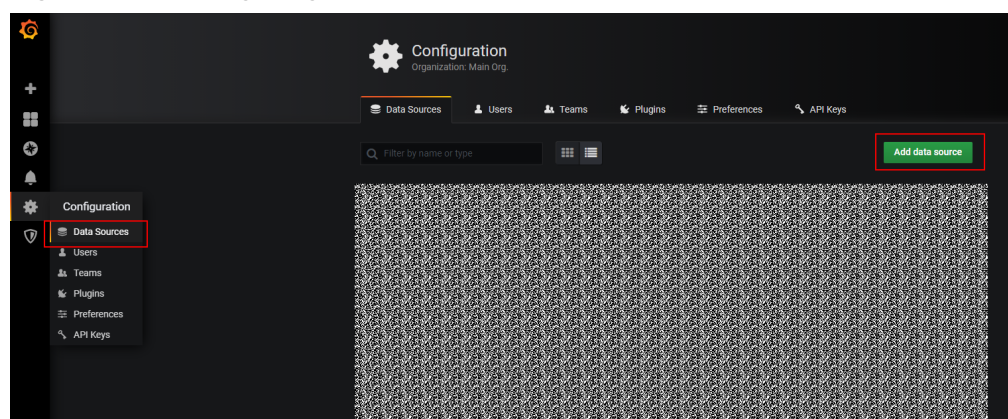
Figure 7-34 Grafana data source information



Step 4 Configure Grafana.

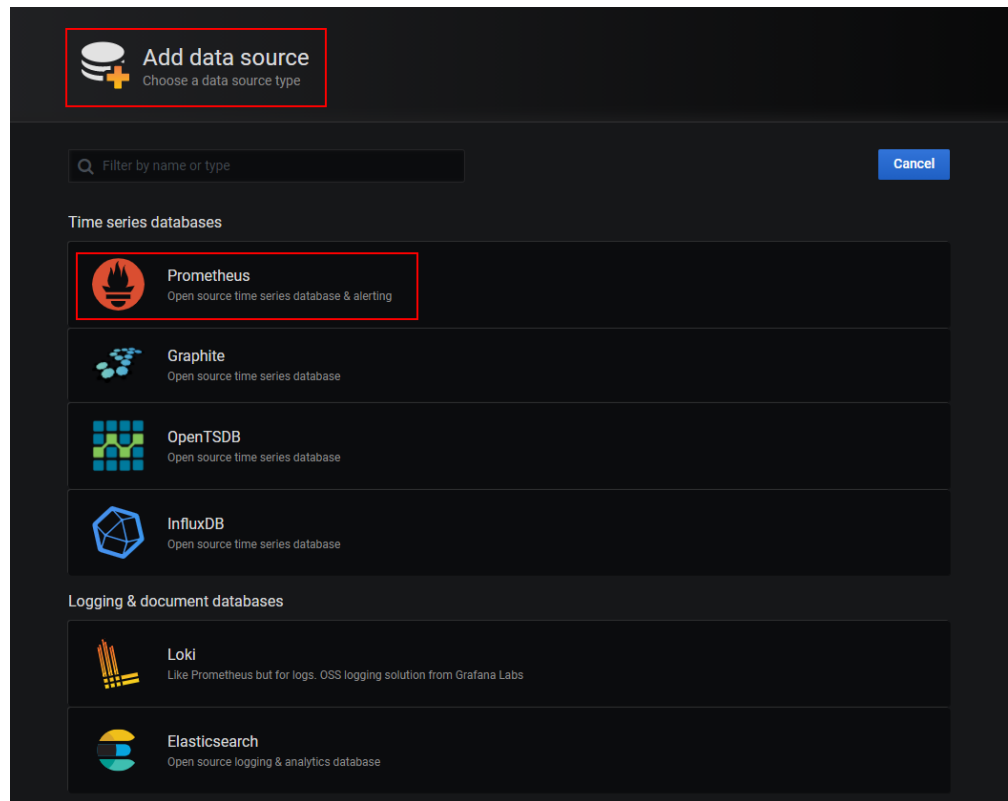
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration > Data Sources**. Then click **Add data source**.

Figure 7-35 Configuring Grafana



3. Click **Prometheus** to access the configuration page.

Figure 7-36 Prometheus configuration page

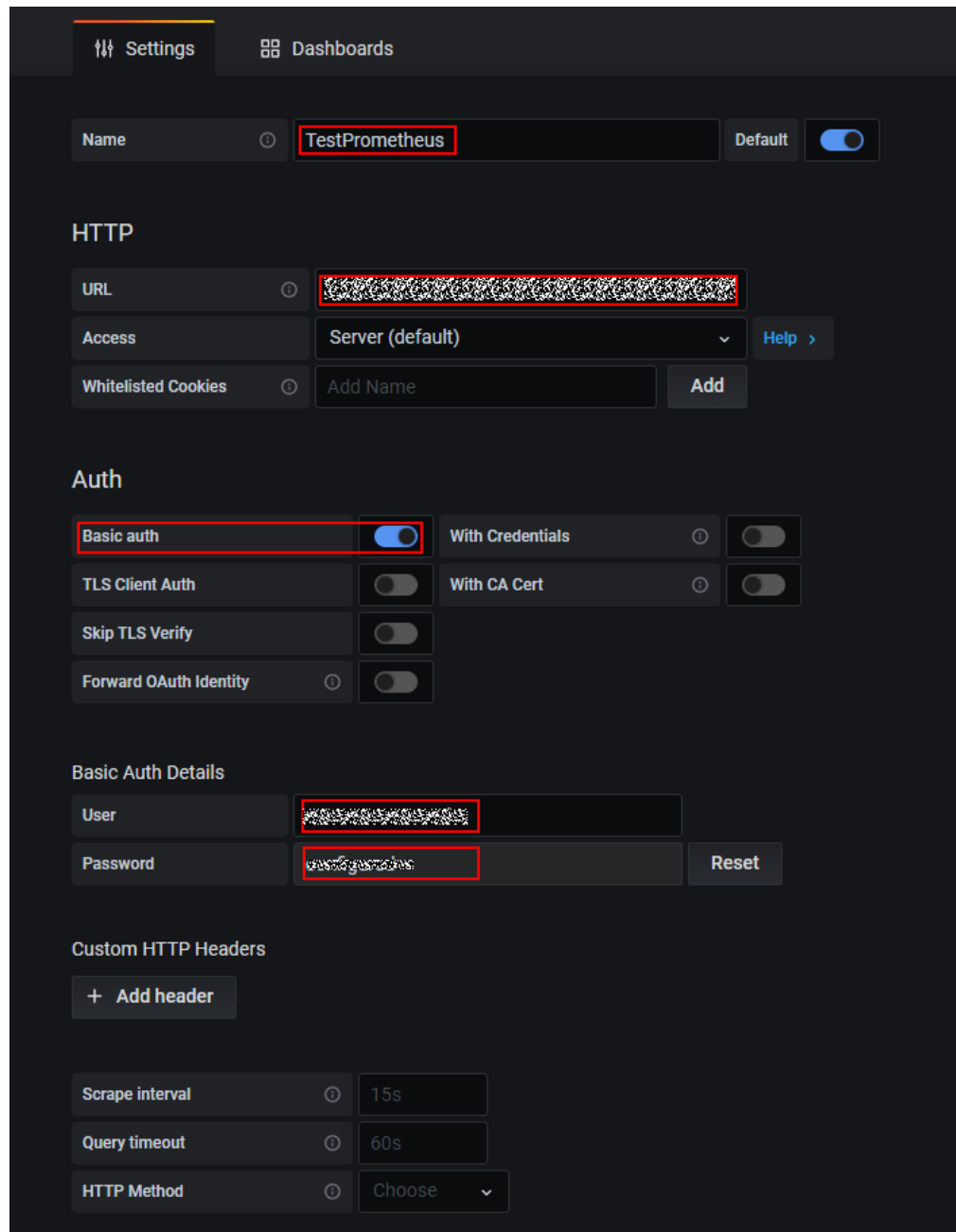


4. Set Grafana data source parameters.
 - **URL:** HTTP URL obtained in [Step 3](#).
 - **User:** username obtained in [Step 3](#).
 - **Password:** password obtained in [Step 3](#).

 **NOTE**

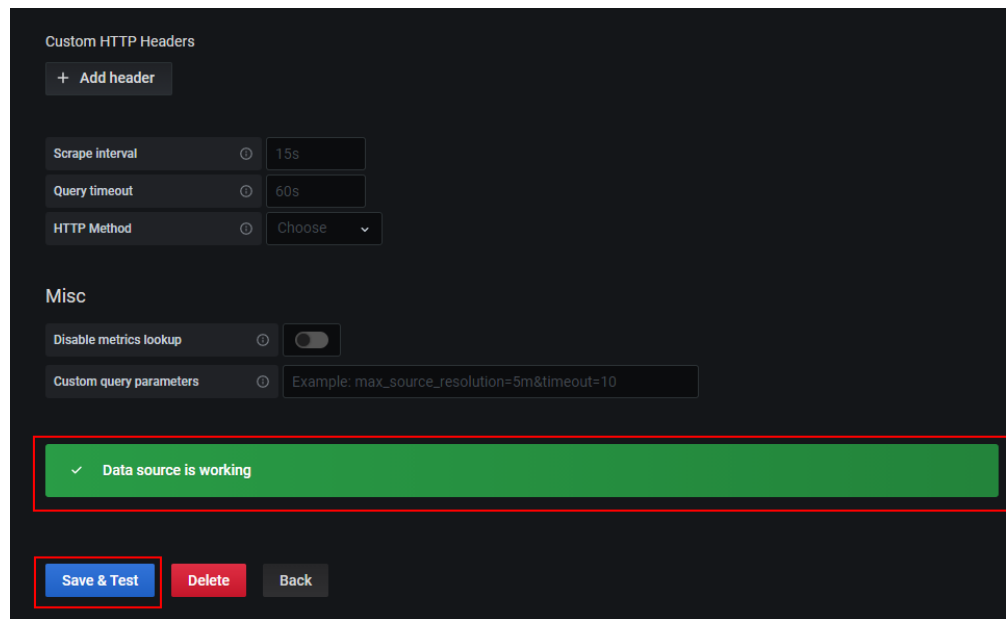
The **Basic auth** and **Skip TLS Verify** options under **Auth** must be enabled.

Figure 7-37 Setting parameters



5. Click **Save&Test** to check whether the configuration is successful. If the configuration is successful, you can use Grafana to configure dashboards and view metric data.

Figure 7-38 Checking whether the configuration is successful



----End

7.10 Reading Prometheus Instance Data Through Remote Read

Prometheus monitoring provides the remote read API, which can categorize a series of Prometheus protocol data sources into one single data source for query. This section describes how to read AOM Prometheus instance data through the remote read API when you are using self-built Prometheus.


Prerequisite

- Your service has been connected for Prometheus monitoring. For details, see:
 - [Prometheus Instance for Cloud Services](#)
 - [Prometheus Instance for ECS](#)
 - [Prometheus Instance for CCE](#)
 - [Common Prometheus Instance](#)

Remote Read Configuration

You are advised to set a **prometheus.yml** file. The following shows the procedure:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the target Prometheus instance.
- Step 3** On the instance details page, choose **Settings** in the navigation pane to obtain the service address of the current instance.

Click the **Intranet** or **Public Network** tab to obtain the configuration code for Prometheus remote read in the intranet or public network. Click  on the right of the code to copy the code to the corresponding file.

Remote read configuration:

```
remote_read:
  - url: 'https://aom.{region_name}-{Site domain name suffix}/v1/{project_id}/
    {prometheus_instance_id}/api/v1/read'
  tls_config:
    insecure_skip_verify: true
    bearer_token: '8H**LP'
    read_recent: true
```

----End

Complete Configuration Items of Remote Read

NOTE

The configuration items in brackets ([]) are optional. (The following lists the configurations of Prometheus v2.40. Some configuration items may be unavailable in earlier versions. For details, see [Prometheus official documents](#).)

```
# API URL of the target Prometheus instance for remote read
url: <string>

# Unique name of a configuration for remote read
[ name: <string> ]

# Filtering conditions that must be contained in PromQL for remote read
required_matchers:
  [ <labelname>: <labelvalue> ... ]

# Timeout for remote read query
[ remote_timeout: <duration> | default = 1m ]

# Custom headers attached to remote read requests, which cannot overwrite the headers added by
Prometheus
headers:
  [ <string>: <string> ... ]

# Whether to directly read metrics from the local storage during Prometheus remote read
[ read_recent: <boolean> | default = false ]

# Add an authorization header for each remote read request. Select either password or password_file.
basic_auth:
  [ username: <string> ]
  [ password: <secret> ]
  [ password_file: <string> ]

# Custom authorization header configuration
authorization:
  # Authentication type
  [ type: <string> | default: Bearer ]
  # Authentication key. Select either credentials or credentials_file.
  [ credentials: <secret> ]
# Obtain the key from a file.
  [ credentials_file: <filename> ]

# OAuth 2.0 authentication, which cannot be used together with basic_auth authorization
oauth2:
  [ <oauth2> ]

# TLS configuration
tls_config:
  [ <tls_config> ]
```

```
# Proxy URL
[ proxy_url: <string> ]

# Whether 3XX redirection is allowed
[ follow_redirects: <boolean> | default = true ]

# Whether to enable HTTP2
[ enable_http2: <bool> | default: true ]

# Whether to attach external_labels during remote read
[ filter_external_labels: <boolean> | default = true ]
```

7.11 Reporting Self-Built Prometheus Instance Data to AOM

On the **Settings** tab page of the default or common Prometheus instance or of the Prometheus instance for ECS, CCE, you can obtain the remote write address of the current Prometheus instance. Native Prometheus metrics can then be reported to AOM through remote write. In this way, time series data can be stored for long.

If the open-source Prometheus has been deployed and is being used, directly go to [Step 4](#).

Prerequisites

- You have created an ECS. For details, see [Elastic Cloud Server \(ECS\) Getting Started](#).
- Your service has been connected for Prometheus monitoring. For more details, see:
 - [Prometheus Instance for ECS](#)
 - [Prometheus Instance for CCE](#)
 - [Common Prometheus Instance](#)

Procedure

Step 1 Install and start Prometheus. For details, see [Prometheus official documentation](#).

Step 2 Add an access code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Settings**. The **Global Configuration** page is displayed.
3. In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

NOTE

- You can create up to two access codes for each project.
- An access code is an identity credential for calling APIs. Keep your access code secure.

Step 3 Obtain the configuration code for Prometheus remote write.

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**. In the instance list, click the target Prometheus instance.
3. On the displayed page, choose **Settings** in the navigation pane and obtain the configuration code for Prometheus remote write from the **Service Addresses** area.

Figure 7-39 Configuration code for Prometheus remote write

Configuration Code for Prometheus Remote Write

```
remote_write:
- url: 'https://aom-internal-access /push'
  tls_config:
    insecure_skip_verify: true
    bearer_token: 'Z9**ey'
```

Step 4 Log in to the target ECS and configure the **prometheus.yml** file.

Run the following command to find and start the **prometheus.yml** file:

```
./prometheus --config.file=prometheus.yml
```

Add the configuration code for Prometheus remote write obtained in [Step 3](#) to the end of the **prometheus.yml** file.

The following shows an example. You need to configure the italic part.

```
# my global config
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
        - targets:
            # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
# - "first_rules.yml"
# - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
# The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
- job_name: 'prometheus'

# metrics_path defaults to '/metrics'
# scheme defaults to 'http'.

static_configs:
- targets: ['localhost:9090']
# Replace the italic content with the configuration code for Prometheus remote write obtained in Step 3.
remote_write:
- url: 'https://aom-*.myhuaweicloud.com:8443/v1/6d6df***2ab7/58d6***c3d/push'
  tls_config:
    insecure_skip_verify: true
    bearer_token: 'SE**IH'
```

Step 5 Check the private domain name.

In the preceding example, data is reported through the intranet. Therefore, ensure that the host where Prometheus is located can resolve the private domain name. For details, see [Changing the DNS Server Addresses for a VPC Subnet](#).

Step 6 Restart Prometheus.

Step 7 [View metric data in AOM using Grafana](#) to check whether data is successfully reported after the preceding configurations are modified.

----End

7.12 Resource Usage Statistics

After metric data is reported to AOM through Prometheus monitoring, you can view the number of reported basic and custom metric samples on the **Resource Usage** page.

Prerequisites

- Your service has been connected for Prometheus monitoring. For more details, see:
 - [Prometheus Instance for ECS](#)
 - [Prometheus Instance for CCE](#)
 - [Common Prometheus Instance](#)

Precautions

- The **Resource Usage** page does not display the number of basic and custom metric samples reported by Prometheus instances for cloud services.
- Metric samples are reported every hour. If you specify a time range shorter than one hour, the query result of total metric samples may be 0.
- The number of metric samples displayed on the **Resource Usage** page may be different from the actual number.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Prometheus Monitoring > Resource Usage**.

Step 3 In the upper left corner of the page, select a desired Prometheus instance.


Step 4 In the upper right corner of the page, set filter criteria.

1. Set a time range in either of the following ways:

Method 1: Use a predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.

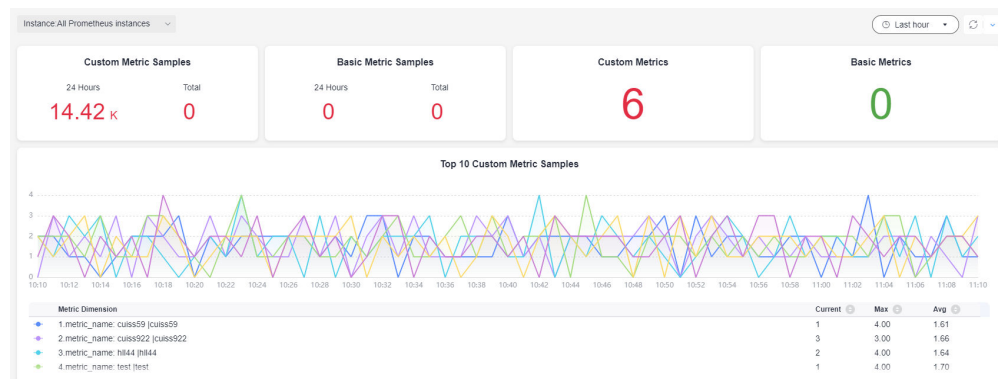
You are advised to select a time range longer than 1 hour.

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

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

- Step 5** View the number of basic metrics and that of custom metrics reported by the Prometheus instance.
- **Custom Metric Samples:** include the number of custom metric samples reported within 24 hours and that reported within a specified time range.
 - **Basic Metric Samples:** include the number of basic metric samples reported within 24 hours and that reported within a specified time range.
 - **Custom Metrics:** indicates the number of custom metric types reported within a specified time range.
 - **Basic Metrics:** indicates the number of basic metric types reported within a specified time range.
 - **Top 10 Custom Metric Samples:** displays the top 10 custom metric samples within a specified time range.

Figure 7-40 Viewing metric statistics



- Step 6** In the Instance Info area, view Total Custom Metric Samples (Million), Total Basic Metric Samples (Million), Custom Metric Samples in 24 Hours (Million), Basic Metric Samples in 24 Hours (Million), Custom Metrics, and Basic Metrics.

----End

8 Business Monitoring (Beta)

8.1 Creating a Log Metric Rule

You can create log metric rules to extract ELB log data reported to LTS as metrics and monitor them on the metric browsing and dashboard pages.

Precaution

- To use business monitoring, enable this function in **Menu Settings**. For details, see [10.6 Menu Settings](#).
- You can create a maximum of 100 log metric rules. The total number of metrics added to all rules cannot exceed 100.


Prerequisite

[ELB logs have been ingested to LTS.](#)

Creating a Log Metric Rule

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Business Monitoring (Beta) > Business Metrics**.

Step 3 Click  next to **Log Metric Rules**.

Step 4 Set parameters to ingest ELB logs reported to LTS to AOM. For details, see [Table 8-1](#).

Figure 8-1 Ingesting logs

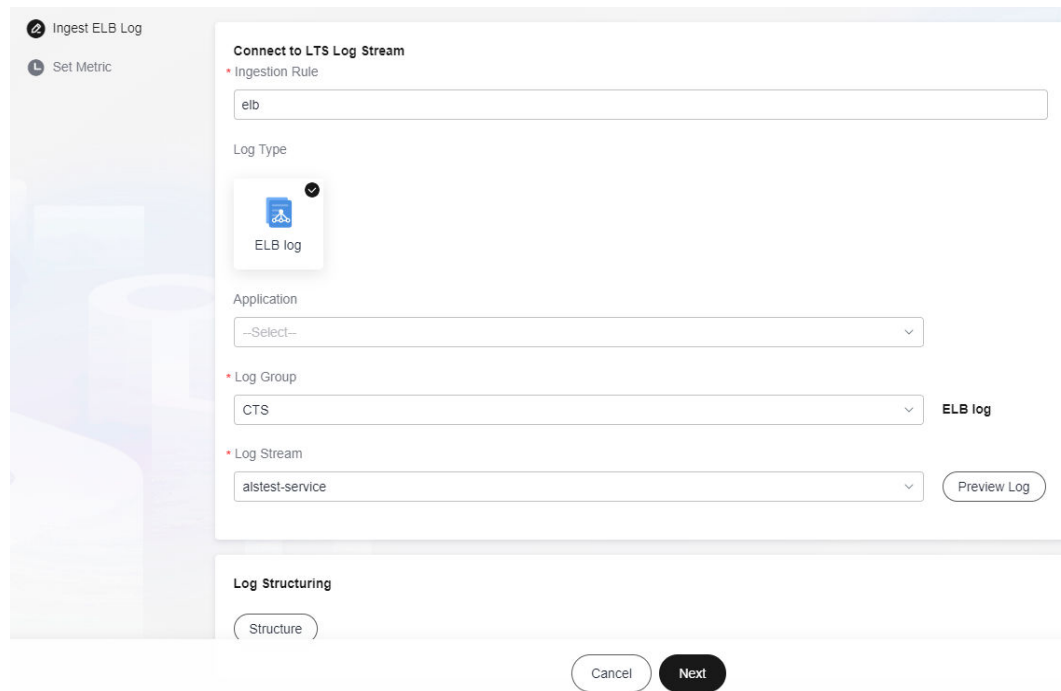


Table 8-1 Log ingestion parameters

Parameter	Description
Ingestion Rule	Enter 1 to 100 characters and do not start with an underscore (_) or hyphen (-). Only letters, digits, hyphens, and underscores are allowed.
Log Type	ELB log is selected by default and cannot be changed.
Application	Select a created application from the drop-down list.
Log Group	Select a created log group from the drop-down list. If no log group is available, create one by referring to Collecting Logs from ELB .
Log Stream	Select a created log stream from the drop-down list. Click Preview Log to view the log data contained in the log stream.
Log Structuring	Click Structure to structure the selected logs. By default, structured fields are displayed in the list below.

Step 5 Click **Next**.

Step 6 Set metric information.

1. Click **Add Metric** to add metrics for the log metric rule. For details, see [Table 8-2](#).

Figure 8-2 Adding a metric

Basic Info

* Metric Name

* Metric Alias

Query Metric

Search By
 Expression SQL

⚙️ 📄 ? Last hour ▾ Search

Result

__time	category	collectTime	field1	field2	field3	field4	field5
No data available.							

Define Metric

* Metric Value

Metric Dimension

Table 8-2 Metric configuration parameters

Category	Parameter	Description
Basic Info	Metric Name	The name consists of prefix aom_business_elb_ and custom content.
	Metric Alias	(Mandatory) Enter an alias.
Query Metric	Search By	Only SQL query is supported.
	Query Statement	Enter an SQL query statement in the text box and click ⚙️ to adjust the SQL statement format. Click ? to view the syntax of SQL statements.
	Query Period	Select a period from the drop-down list.

Category	Parameter	Description
Define Metric	Metric Value	Select a value from the drop-down list. Only numeric fields can be selected.
	Metric Dimension	Select a value from the drop-down list.

2. Click **OK**.
3. (Optional) Click **Add Metric** to add more metrics for the rule.

Step 7 Click **OK**.



The created log metric rule is displayed in the rule list on the left.


----End

More Operations

After creating a log metric rule, perform the operations listed in [Table 8-3](#) if needed.

Table 8-3 Related operations

Operation	Description
Querying a log metric rule	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the right pane, view the enabling status, log type, and metric of the rule.
Disabling a log metric rule	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the upper right corner of the page, click Disable.
Editing a log metric rule	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the upper right corner of the page, choose ... > Edit. For details, see Creating a Log Metric Rule.
Deleting a log metric rule	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the upper right corner of the page, choose ... > Delete.
Adding a metric	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the right pane, click Add Metric. For details, see Step 6.
Editing a metric	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select a metric access card and click . For details, see Step 6.
Deleting a metric	<ol style="list-style-type: none"> 1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select a metric access card and click .

Operation	Description
Searching for a metric	<ol style="list-style-type: none"><li data-bbox="603 297 1348 331">1. In the log metric rule list on the left, click a rule name.<li data-bbox="603 342 1406 421">2. On the right of the page, enter a rule name keyword in the search box next to Add Metric and click .

9 Infrastructure Monitoring

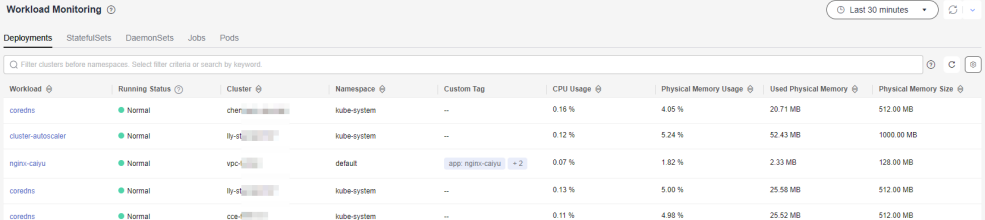
9.1 Workload Monitoring

Workload monitoring is for CCE workloads. It enables you to monitor the resource usage, status, and alarms of workloads in a timely manner so that you can quickly handle alarms or events to ensure smooth workload running. Workloads are classified into Deployments, StatefulSets, DaemonSets, Jobs, and Pods.

Function Introduction

- The workload monitoring solution is ready-to-use. After AOM is enabled, the workload status, CPU usage, and physical memory usage of CCE are displayed on the workload monitoring page by default.

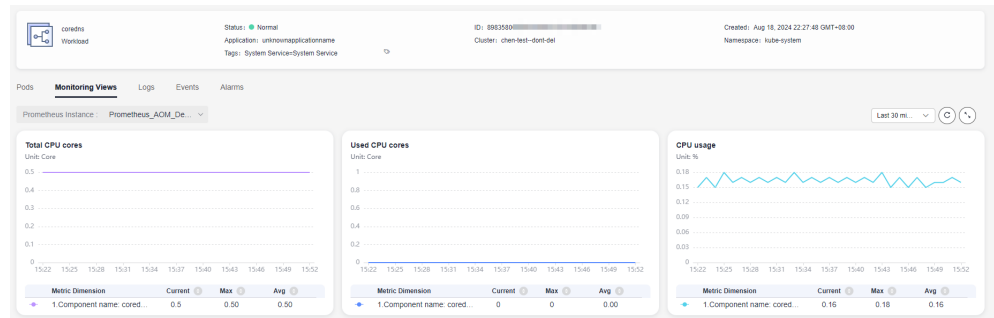
Figure 9-1 Workload monitoring



Workload	Running Status	Cluster	Namespace	Custom Tag	CPU Usage	Physical Memory Usage	Used Physical Memory	Physical Memory Size
coredns	Normal	che...	kube-system	--	0.16 %	4.05 %	20.71 MB	512.00 MB
cluster-autoscaler	Normal	by-d...	kube-system	--	0.12 %	5.24 %	52.43 MB	1000.00 MB
nginx-catsy	Normal	vpc-	default	app: nginx-catsy +2	0.07 %	1.82 %	2.33 MB	128.00 MB
coredns	Normal	by-d...	kube-system	--	0.13 %	5.00 %	25.58 MB	512.00 MB
coredns	Normal	cce-	kube-system	--	0.11 %	4.98 %	25.52 MB	512.00 MB

- For customer-built Kubernetes containers, only Prometheus remote write is supported. After container metrics are written into AOM's metric library, you can query metric data by following instructions listed in [5 Metric Browsing](#).
- Workload monitoring adopts the layer-by-layer drill-down design. The hierarchy is as follows: workload > Pod instance > container > process. You can view their relationships on the UI. Metrics and alarms are monitored at each layer.

Figure 9-2 Workload details



Procedure

Step 1 Log in to the AOM 2.0 console.


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

Step 3 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** or **Last 6 hours**. You can select a time range as required.

Method 2: Specify the start time and end time to customize a time range. You can specify 30 days at most.



2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 4 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 or namespace.

NOTE

To query namespaces, IAM users with the **AOM FullAccess** or **AOM ReadOnlyAccess** permission need to log in to the CCE console, choose **Permissions** in the navigation pane, and click **Add Permission** in the upper right corner of the page to add required permissions.

- Click  in the upper right corner to obtain the latest workload information within the time range specified in [Step 3.1](#).
- Click  in the upper right corner and select or deselect columns to display.
- Click the name of a workload to view its details.
 - On the **Pods** tab page, view the 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 **Alarms** tab page, view the alarm details of the workload. For details, see [4.4 Checking Alarms](#).
- On the **Events** tab page, view the event details of the workload. For details, see [4.5 Viewing Events](#).

----End

9.2 Cluster Monitoring

Clusters deployed using CCE are monitored. On the **Cluster Monitoring** page, you can view multiple basic metrics (such as cluster status, CPU usage, memory usage, and node status), and related alarms and events in real time. Based on them, you can monitor cluster statuses and handle risks in a timely manner, ensuring stable cluster running.

Precautions

- The host status can be **Normal**, **Abnormal**, **Warning**, **Silent**, or **Deleted**. The running status of a host is displayed as **Abnormal** when the host is faulty due to network failures or host power-off or shut-down, or when a threshold alarm is reported on the host.

Procedure

Step 1 Log in to the AOM 2.0 console.


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

Step 3 In the upper right corner of the page, set cluster filter criteria.

1. Set a time range to view the CCE clusters that report information. There are two methods to set a time range:

Method 1: Use a predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.


Method 2: Specify the start time and end time to customize a time range. You can specify 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 4 Set search criteria (such as the creation time, CPU usage, and cluster name) to find the target cluster.

Step 5 Click a cluster to go to its details page. In the navigation pane on the left, monitor cluster running conditions by cluster, on dashboards, or through **Alarm Management**.


- View information about nodes, workloads, pods (container groups), and containers by cluster.
 - In the navigation pane on the left, choose **Insights > Node** to view information about all nodes in the cluster in real time, including the status, IP address, pod status, CPU usage, and memory usage.


- In the upper part of the node list, filter nodes by node name.
- Click  in the upper right corner and select or deselect options as required.
- Click a node to view its related resources, alarms, and events, and common system devices such as GPUs and NICs.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and host status.


 **NOTE**


To use cloud-native monitoring, connect your cluster to a Prometheus instance for CCE first.


If there is no Prometheus instance for CCE, click **Prometheus Monitoring** to create a Prometheus instance by referring to [7.2.3 Prometheus Instance for CCE](#). After the instance is created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.



 Last 30 minutes ▾

Click  in the upper right corner and select a predefined time label or customize a time range from the drop-down list to view resource information.

Click  in the upper right corner to obtain the latest resource information in real time.

Click  in the upper right corner of the page to view resource information in full screen.

- On the **Related Resources** tab page, the pod (container group) to which the node belongs is displayed.
- In the navigation pane on the left, choose **Insights** > **Workload** to view the status and resource usage of all workloads in the cluster.
 - In the upper part of the workload list, filter workloads by workload type or name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a workload to view its related resources, alarms, events, and dashboards.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and file system.
 - On the **Related Resources** tab page, the pod (container group) to which the workload belongs is displayed.

- In the navigation pane on the left, choose **Insights** > **Pod** to view the status and resource usage of all pods in the cluster.
 - In the upper part of the container group list, filter container groups by name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a container group to view its related resources, alarms, events, and dashboards.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and file system.
 - On the **Related Resources** tab page, view nodes, workloads, and containers by name.
- In the navigation pane on the left, choose **Insights** > **Container** to view the status and resource usage of all containers in the cluster.
 - In the upper part of the container list, filter containers by name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a container to view its related resources, alarms, events, and dashboards. On the **Related Resources** tab page, the container group to which the container belongs is displayed by default. Check nodes, workloads, and container groups by name.
- Check the cluster running status through **Alarm Management**.
 - In the navigation pane on the left, choose **Alarm Management** > **Alarm List** to view alarm details of the cluster. For details, see [4.4 Checking Alarms](#).
 - In the navigation pane on the left, choose **Alarm Management** > **Event List** to view event details of the cluster. For details, see [4.5 Viewing Events](#).
 - In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules** to view the alarm rules related to the cluster. Modify the alarm rules as required. For details, see [4.2.5 Managing Alarm Rules](#).
- In the navigation pane on the left, choose **Dashboard** to view the running status of the current cluster.
 - A CCE Prometheus instance has been connected:
Select **Cluster View**, **Pod View**, **Host View**, or **Node View** from the drop-down list to view key metrics such as the CPU usage and physical memory usage.
 - No CCE Prometheus instance is connected:
Choose **Prometheus Monitoring** and then add a Prometheus instance. For details, see [7.2.3 Prometheus Instance for CCE](#) After the instance is

created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.

----End

9.3 Host Monitoring

Hosts include the Elastic Cloud Server (ECS) and Bare Metal Server (BMS). AOM can monitor the hosts purchased during CCE and ServiceStage cluster creation as well as those purchased in non-CCE and -ServiceStage environments. (The purchased hosts must meet the OS and version requirements, and ICAgents must be installed on them. Otherwise, AOM cannot monitor them.) In addition, hosts support IPv4 addresses.

Host monitoring displays resource usage, trends, and alarms, so that you can quickly respond to malfunctioning hosts and handle errors to ensure smooth host running.




Precautions

- A maximum of five tags can be added to a host, and each tag must be unique.
- The same tag can be added to different hosts.

Procedure

Step 1 Log in to the AOM 2.0 console.


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

- Set filter criteria (such as the running status, host type, host name, and IP address) above the host list.
- You can enable or disable **Hide master host**. By default, this option is enabled.
- Click  next to **Hide master host** to synchronize host information.
- In the upper right corner of the page, set filter criteria.
 - Set a time range to view the hosts reported. There are two methods to set a time range:
 - Method 1: Use a predefined time label, such as **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, or **Last week**. Select one as required.
 - Method 2: Specify the start time and end time (max. 30 days).
 - Set the interval for refreshing information. Click  and select a value from the drop-down list as required, such as **Refresh manually**, **30 seconds auto refresh**, **1 minute auto refresh**, or **5 minutes auto refresh**.
 - Click  in the upper right corner and select or deselect **Tags**.

Step 3 Perform the following operations if needed:



- **Adding an alias**

If a host name is too complex to identify, you can add an alias, which makes it easy to identify a host as required.


In the host list, click  in the **Operation** column of the target host, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted.

- **Adding a tag**

Tags are identifiers of hosts. You can manage hosts using tags. After a tag is added, you can quickly identify and select a host.

In the host list, click  in the **Operation** column of the target host. In the displayed dialog box, enter a tag key and value, and click  and **OK**.

- **Synchronizing host data**

In the host list, locate the target host and click  in the **Operation** column to synchronize host information.



Step 4 Set filter criteria to search for the desired host.


 **NOTE**

Hosts cannot be searched by alias.

Step 5 Click a host name. On the displayed host details page, you can view the running status and ID of the host.

Step 6 Click any tab. In the list, you can monitor the instance resource usage and health status, and information about common resources such as GPUs and NICs.

- On the **Process List** tab page of the ECS host, you can view the process status and IP address of the host.
 - In the search box in the upper right corner of the process list, you can set search criteria such as the process name to filter processes.
 - Click  in the upper right corner to obtain the latest process information within the specified time range.
- On the **Pods** tab page of the CCE host, you can view the pod status and node IP address.
 - Click a pod name to view details about the container and process of the pod.
 - In the search box in the upper right corner of the pod list, you can set search criteria such as pod names to filter pods.
 - Click  in the upper right corner to obtain the latest pod information within the specified time range.
- On the **Monitoring Views** tab page, view key metric graphs of the host.
- On the **File Systems** tab page, view the basic information about the file system of the host. Click a disk file partition to monitor its metrics on the **Monitoring Views** page.
- On the **Disks** tab page, view the basic information about the disks of the host. Click a disk to monitor its metrics on the **Monitoring Views** page.

- On the **Disk Partitions** tab page, view the disk partition information about the host. Click a disk partition to monitor its metrics on the **Monitoring Views** page.
- Click the **NICs** tab to view the basic information about the NICs of the host. Click a NIC to monitor its metrics on the **Monitoring Views** page.
- Click the **GPUs** tab to view the basic information about the GPUs of the host. Click a GPU to monitor its metrics on the **Monitoring Views** page.
- On the **Events** tab page, view the event details of the host. For details, see [4.5 Viewing Events](#).
- On the **Alarms** tab page, view the alarm details of the host. For details, see [4.4 Checking Alarms](#).
- On the **File Systems, Disks, Disk Partitions, NICs, or GPUs** tab page, click  in the upper right corner of the resource list and select or deselect items to display.

 **NOTE**

Disk partitions are supported by CentOS 7.x and EulerOS 2.5.

----End


9.4 Process Monitoring

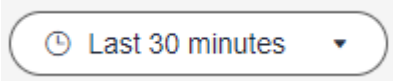
9.4.1 Application Monitoring

An application groups identical or similar components based on service requirements. Applications are classified into system applications and custom applications. System applications are discovered based on built-in discovery rules, and custom applications are discovered based on custom rules.

After application discovery rules are set, AOM automatically discovers applications that meet the rules and monitors related metrics. For details, see [9.4.3 Application Discovery](#).

Procedure


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Infrastructure Monitoring > Process Monitoring**. On the **Application Monitoring** page, view the application list.
- Set filter criteria in the search box to filter applications.
 - Click  in the upper right corner of the page and select or deselect the columns to display.


- Step 3** Click  in the upper right corner of the page and select a desired value from the drop-down list.

1. Set a time range to view applications. There are two methods to set a time range:

Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour** in the upper right corner of the page. You can select a time range as required.

Method 2: Specify the start time and end time to customize a time range. You can specify 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

- Step 4** Click an application name. On the page that is displayed, you can view the component list, host list, monitoring views, and alarms of the current application.
- On the **Component List** tab page, you can view the running status and resource usage of components.
 - On the **Host List** tab page, you can view the running status and resource usage of hosts.
 - On the **Monitoring Views** tab page, select a desired Prometheus instance to view the resource usage of the application. Click  in the upper right corner of the page to view resource information in full screen.
 - On the **Alarms** tab page, view the alarm details of the application. For details, see [4.4 Checking Alarms](#).


----End

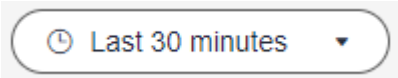
9.4.2 Component Monitoring

Components refer to the services that you deploy, including containers and common processes.

The component list displays the name, running status, and application of each component. AOM supports drill-down from a component to an instance, and then to a process. By viewing the status of each layer, you can implement dimensional monitoring for components.

Procedure


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Infrastructure Monitoring > Process Monitoring**. Next, click the **Component Monitoring** tab. Then you can view the component list.
 - The component list displays information such as **Component Name**, **Application**, **Deployment Mode**, and **Application Discovery Rules**.
 - To view target components, you can set filter criteria (such as the running status, application, cluster name, deployment mode, and component name) above the component list.
 - Enable or disable **Hide System Components** as required. By default, system components are hidden.
 - Click  in the upper right corner of the page and select or deselect the columns to display.

Step 3 Click  in the upper right corner of the page and select a desired value from the drop-down list.

1. Set a time range to view components. There are two methods to set a time range:

Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour** in the upper right corner of the page. You can select a time range as required.


Method 2: Specify the start time and end time to customize a time range. You can specify 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 4 Perform the following operations if needed:


- **Adding an alias**


If a component name is complex to identify, you can add an alias for the component.

In the component list, click  in the **Operation** column of the target component, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted.

- **Adding a tag**

Tags are identifiers of components. You can distinguish system components from non-system components based on tags. By default, AOM adds the **System Service** tag to system components (including icagent, css-defender, nvidia-driver-installer, nvidia-gpu-device-plugin, kube-dns, org.tanukisoftware.wrapper.WrapperSimpleApp, evs-driver, obs-driver, sfs-driver, icwatchdog, and sh).

In the component list, click  in the **Operation** column of the target component. In the displayed dialog box, enter a tag key and value, click

, select the **Mark as system component** check box, and click **OK**.

 **NOTE**

- A maximum of five tags can be created for each component.
- Tag key: max. 36 characters; tag value: max. 43 characters
- A tag value can contain only letters, digits, hyphens (-), and underscores (_).

Step 5 Set filter criteria to search for the desired component.

 **NOTE**

Components cannot be searched by alias.


Step 6 Click the component name. The component details page is displayed.

- On the **Instance List** tab page, view the instance details.

 NOTE

Click an instance name to view the monitoring view and alarm information.

- On the **Host List** tab page, view the host details.
- On the **Monitoring Views** tab page, select a desired Prometheus instance to

view the resource usage of the component. Click  in the upper right corner of the page to view resource information in full screen.

- On the **Alarms** tab page, view the alarm details of the component. For details, see [4.4 Checking Alarms](#).
- On the **Events** tab page, view the event details of the component. For details, see [4.5 Viewing Events](#).

----End

9.4.3 Application Discovery

AOM can discover applications and collect their metrics based on configured rules. There are two modes to configure application discovery: auto mode and manual mode. This section mainly describes the manual mode.

- **Auto mode**

After you install the ICAgent on a host, the ICAgent automatically discovers applications on the host based on [Built-in Discovery Rules](#) and displays them on the **Application Monitoring** page.

- **Manual mode**

If you customize an application discovery rule and apply it to the host where the ICAgent is installed, the ICAgent discovers applications on the host based on the custom rule and displays them on the **Application Monitoring** page.

Filtering Rules

The ICAgent periodically detects processes on the target host. The effect is similar to that of running the `ps -e -o pid,comm,lstart,cmd | grep -v defunct` command. Then, the ICAgent checks whether processes match the filtering rules in [Table 9-1](#). If a process meets a filtering rule, the process is filtered out and is not discovered by AOM. If a process does not meet any filtering rules, the process is not filtered and is discovered by AOM.

Information similar to the following is displayed:

PID	COMMAND	STARTED	CMD
1	systemd	Tue Oct 2 21:12:06 2018	/usr/lib/systemd/systemd --switched-root --system --deserialize 20
2	kthreadd	Tue Oct 2 21:12:06 2018	[kthreadd]
3	ksoftirqd/0	Tue Oct 2 21:12:06 2018	(ksoftirqd/0)
1140	tuned	Tue Oct 2 21:12:27 2018	/usr/bin/python -Es /usr/sbin/tuned -l -P
1144	sshd	Tue Oct 2 21:12:27 2018	/usr/sbin/sshd -D
1148	agetty	Tue Oct 2 21:12:27 2018	/sbin/agetty --keep-baud 115200 38400 9600 hvc0 vt220
1154	docker-containe	Tue Oct 2 21:12:29 2018	docker-containerd -l unix:///var/run/docker/libcontainerd/docker-containerd.sock --shim docker-containerd-shim --start-timeout 2m --state-dir /var/run/docker/libcontainerd/containerd --runtime docker-runc --metrics-interval=0

Table 9-1 Filtering rules

Filtering Rule	Example
If the COMMAND value of a process is docker-containe, vi, vim, pause, sshd, ps, sleep, grep, tailf, tail, or systemd-udevd , and the process is not running in a container, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 1154 is not discovered by AOM because its COMMAND value is docker-containe .
If the CMD value of a process starts with [and ends with] , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 2 is not discovered by AOM because its CMD value is [kthreadd] .
If the CMD value of a process starts with (and ends with) , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 3 is not discovered by AOM because its CMD value is (ksoftirqd/0) .
If the CMD value of a process starts with /sbin/ , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 1148 is not discovered by AOM because its CMD value starts with /sbin/ .

Built-in Discovery Rules

AOM provides two built-in discovery rules: **Sys_Rule** and **Default_Rule**. These rules are executed on all hosts, including hosts added later. The priority of **Sys_Rule** is higher than that of **Default_Rule**. That is, **Sys_Rule** is executed on the host first. If **Sys_Rule** is met, **Default_Rule** is not executed. Otherwise, **Default_Rule** is executed. Rule details are as follows:

Sys_Rule (cannot be disabled)

When **Sys_Rule** is used, the component name and application name must be used together. The names are determined according to the following priorities:

- Priorities for determining the application name:
 - a. Use the value of the **Dapm_application** field in the process startup command.
 - b. If the value in **a** is empty, use the value of the **Dapm_application** field in the **JAVA_TOOL_OPTIONS** variable.
 - c. If the value in **b** is empty, use the value of the **PAAS_MONITORING_GROUP** variable.
 - d. If the value in **c** is empty, use the value of the **DAOM.APPN** field in the process startup command.
- Priorities for determining the component name:
 - a. Use the value of the **DAOM.PROCN** field in the process startup command. If the value is empty, use the value of the **Dapm_tier** field.

- b. If the value in **a** is empty, use the value of the **Dapm_tier** field in the **JAVA_TOOL_OPTIONS** variable.
- c. If the value in **b** is empty, use the value of the **PAAS_APP_NAME** variable.

In the following example, the component name is **atps-demo** and the application name is **atpd-test**.

```
PAAS_MONITORING_GROUP=atpd-test  
PAAS_APP_NAME=atps-demo  
JAVA_TOOL_OPTIONS=-javaagent:/opt/oss/servicemgr/ICAgent/pinpoint/pinpoint-bootstrap.jar -  
Dapm_application=atpd-test -Dapm_tier=atps-demo
```

Default_Rule (can be disabled)

- If the **COMMAND** value of a process is **java**, obtain the name of the JAR package in the command, the main class name in the command, and the first keyword that does not start with a hyphen (-) in the command based on the priorities in descending order as the component name, and use the default value **unknownapplicationname** as the application name.
- If the **COMMAND** value of a process is **python**, obtain the name of the first **.py/.pyc** script in the command as the component name, and use the default value **unknownapplicationname** as the application name.
- If the **COMMAND** value of a process is **node**, obtain the name of the first **.js** script in the command as the component name, and use the default value **unknownapplicationname** as the application name.

Creating a Custom Discovery Rule

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Infrastructure Monitoring > Process Monitoring**. Next, click the **Application Discovery** tab.

Step 3 On the displayed page, click **Add Custom Application Discovery Rule** and configure an application discovery rule.

Step 4 Select a host for pre-detection.

1. Customize a rule name, for example, **rule-test**.
2. Select a typical host, for example, **host-test**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in **Step 7**. Then click **Next**.

Step 5 Set an application discovery rule.

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

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

NOTE

- To precisely detect processes, you are advised to add check items about unique features of the processes.
- You must add at least one check item and can add up to five check items. If there are multiple check items, AOM only discovers the processes that meet the conditions of all check items.

2. After adding check items, click **Detect** to search for the processes that meet the conditions.

If no process is detected within 20s, modify the discovery rule and detect processes again. Only when at least one process is detected can you proceed to the next step.

Step 6 Set an application name and component name.

1. Set an application name.

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

 **NOTE**

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


2. Set a component name.

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

 **NOTE**

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

3. Preview the component name.

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

Step 7 Set a priority and detection range.

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

Step 8 Click **OK** to complete the configuration. AOM collects metrics of the process.

Step 9 After about two minutes, choose **Process Monitoring** > **Component Monitoring** in the navigation pane to view the monitored components.

----End

More Operations

After creating an application discovery rule, perform the operations listed in [Table 9-2](#) if needed.

Table 9-2 Related operations

Operation	Description
Viewing rule details	In the Name column, click the name of an application discovery rule.
Starting or stopping rules	<ul style="list-style-type: none">Click Start in the Operation column.Click Stop in the Operation column. After a rule is disabled, AOM does not collect corresponding process metrics.
Deleting rules	<ul style="list-style-type: none">To delete a discovery rule, click Delete in the Operation column.To delete one or more application discovery rules, select them and click Delete above the rule list. <p>NOTE Built-in discovery rules cannot be deleted.</p>
Modifying rules	Click Modify in the Operation column. <p>NOTE Built-in discovery rules cannot be modified.</p>

10 Settings

10.1 Cloud Service Authorization

Grant permissions to access Resource Management Service (RMS), Log Tank Service (LTS), Cloud Container Engine (CCE), Cloud Container Instance (CCI), Cloud Eye, Distributed Message Service (DMS), and Elastic Cloud Server (ECS). The permission setting takes effect for the entire AOM 2.0 service.

Prerequisites

You have been granted **AOMFullAccessPolicy**, **iam:agencies:createAgency**, and **iam:agencies:deleteAgency** permissions. For details about how to grant permissions, see [Creating a User Group and Assigning Permissions](#).

Procedure

- 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** In the upper right corner of the cloud service authorization page, click **Authorize** to grant permissions to access the preceding cloud services with one click.

Upon authorization, the **aom_admin_trust** agency will be created in IAM.

If **Cancel Authorization** is displayed in the upper right corner of the page, you have the permissions to access the preceding cloud services.

----End

10.2 Access Management

An access code is an identity credential for calling APIs. Create an access code for setting API call permissions. The permission setting takes effect for the entire AOM 2.0 service.

Precautions

You can create up to two access codes.

Creating an Access Code



- 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** In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
- Step 4** In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

----End

More Operations

After an access code is created, you can perform the operations listed in [Table 10-1](#).

Table 10-1 Related operations

Operation	Description
Viewing an access code	In the list, you can view the ID, access code, status, and creation time.
Searching for an access code	Enter the ID of the access code and click  to search.
Deleting an access code	Click Delete in the Operation column.
Refreshing an access code	Click  to obtain the latest information of the access code.

10.3 Global Settings

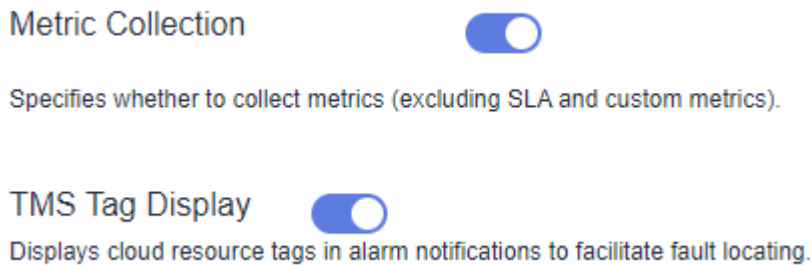
You can determine whether to enable **Metric Collection** to collect metrics (excluding SLA and custom metrics). You can also determine whether to enable **TMS Tag Display** to display cloud resource tags in alarm notifications to facilitate fault locating. The setting takes effect for entire AOM 2.0.

Procedure

- 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 On the displayed page, choose **Global Configuration**. Enable or disable functions as required.

Figure 10-1 Global configuration



NOTE

After metric collection is disabled, ICAgents will stop collecting VM metrics and related metric data will not be updated. However, custom metrics can still be reported.

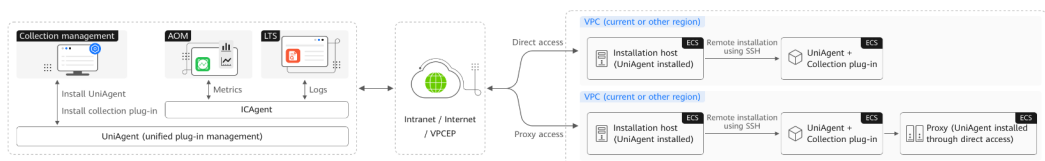
----End

10.4 Collection Settings

10.4.1 Overview

UniAgent centrally manages the life cycle of collection plug-ins and delivers instructions (such as script delivery and execution).

Figure 10-2 Getting started



UniAgent does not collect O&M data; instead, collection plug-ins do that. You can create collection tasks in the access center. For details, see [7.7.2 Exporter Access in the VM Scenario](#).

10.4.2 Connecting VMs

10.4.2.1 Installing a UniAgent

Install a UniAgent on a host manually or remotely, or by importing an Excel file.

You can select an installation mode based on site requirements.

Table 10-2 Installation modes

Mode	Application Scenario
Manual Installation	When installing a UniAgent for the first time, you must install it manually.
Remote Installation	Remote installation can be performed only when you have an installation host. NOTE An installation host is used to execute commands for remote installation.

Installation Prerequisite

Ensure that the network between the installation host and the host where the UniAgent is to be installed is normal.

UniAgent Installation Restrictions

For details about the Linux and Windows OSs supported by the UniAgent, see [Collection Management Restrictions](#).

Manual Installation

When installing a UniAgent for the first time, you must install it manually.


- 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** In the navigation pane, choose **Collection Settings > VM Access**. Then click **Install UniAgent** in the upper right corner. On the displayed page, choose **Manual**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default.)
- Step 4** On the **Install UniAgent** page, set parameters.

Figure 10-3 Manually installing a UniAgent



Table 10-3 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are two access modes: direct access and proxy access. <ul style="list-style-type: none">• Direct access: A host is directly accessed.• Proxy access: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy.	Direct access

Parameter	Description	Example
Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <p>Click  to copy the installation command.</p> <p>Linux</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 xxxxxxxxxx -s xxxxxxxxxxxx -p xxxxxx -d https://aom-uniagent- xxxxxx -m https://uniagent.master.cnxxxxxxxx,https:// xx.xx.xx.xx:xxxx -v 1.x.x -q false set -o history;</pre> <p>Windows</p> <ol style="list-style-type: none"> Download the installation package from https://aom-uniagent-<i>{region_name}</i>.obs.<i>{region_name}</i>.<i>{site domain name suffix}</i>}/+uniagentd-<i>{version}</i>-win32.zip. <i>{region_name}</i> and <i>{version}</i> can be obtained from the installation page. <ul style="list-style-type: none"> <i>region_name</i>: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions. Site domain name suffix: site domain name suffix, for example, myhuaweicloud.com. <i>version</i>: version of the installed UniAgent. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. Modify the uniagentd.conf file in C:\uniagentd\conf and enter the following configuration: <pre>ak=xxxxxxxxxxxxxxxx sk=xxxxxxxxxxxxxxxx master=https:// uniagent.master.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxx</pre> Run start.bat in the C:\uniagentd\bin directory as the administrator. <p>NOTE</p> <ul style="list-style-type: none"> If you need to verify the SHA256 value of the Windows installation package, check the file downloaded from https://aom-uniagent-<i>{region_name}</i>.obs.<i>{region_name}</i>.<i>{site domain name suffix}</i>}/uniagentd-<i>{version}</i>-win32.zip.sha256. 	Copy the Linux installation command.

Step 5 Copy the installation command and run it on the host to install the UniAgent.

Step 6 View the information on the **VM Access** page.

----End

Remote Installation

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 In the navigation pane, choose **Collection Settings > VM Access**. Then click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Remote** and set parameters. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Remote** is not available. Remote installation can be performed only when you have an installation host.)

Figure 10-4 Remotely installing a UniAgent

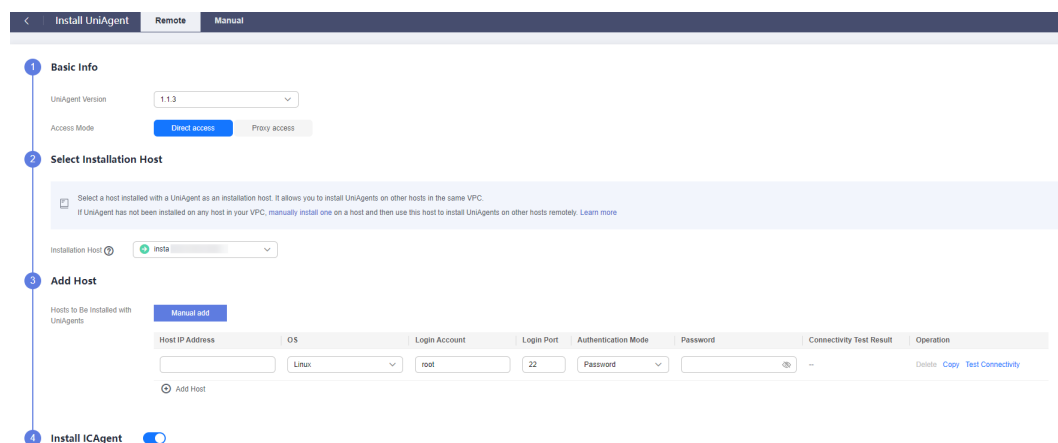
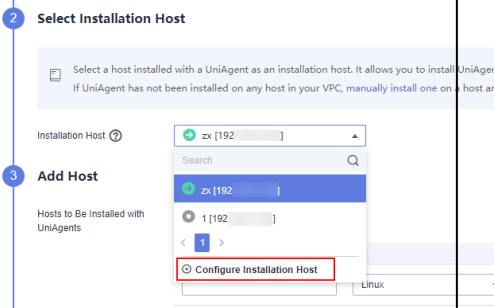


Table 10-4 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are two access modes: direct access and proxy access. <ul style="list-style-type: none"> Direct access: A host is directly accessed. Proxy access: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy. 	Direct access

Parameter	Description	Example
Proxy Area	<p>When Access Mode is set to Proxy access, you need to select a proxy area or add a proxy area.</p> <p>A proxy area is used to group and manage proxies. A proxy must be a host installed with a UniAgent.</p>	-
Installation Host	<p>An installation host is used to execute commands for remote installation. This parameter is mandatory.</p> <p>If no installation host has been configured, perform the following steps:</p> <ol style="list-style-type: none"> 1. Select Configure Installation Host from the drop-down list. <p>Figure 10-5 Configuring an installation host</p>  <ol style="list-style-type: none"> 2. In the dialog box that is displayed, select the host to be set as an installation host and specify its name. 3. Click OK. 	-

Parameter	Description	Example
Hosts to Be Installed with UniAgents	<p>Detailed information about the host where the UniAgent is to be installed. This parameter is mandatory.</p> <p>Click Add Host and enter the following information:</p> <p>Host IP Address: IP address of a host.</p> <p>OS: operating system of the host, which can be Linux or Windows.</p> <p>NOTE</p> <p>To install the UniAgent remotely, ensure that the host does not run Windows.</p> <p>Login Account: account for logging in to the host. If Linux is used, use the root account to ensure that you have sufficient read and write permissions.</p> <p>Login Port: port for accessing the host.</p> <p>Authentication Mode: Currently, only password-based authentication is supported.</p> <p>Password: password for logging in to the host.</p> <p>Connectivity Test Result: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal.</p> <p>Operation: Delete, Copy, or Test Connectivity.</p> <p>NOTE</p> <ul style="list-style-type: none">You can click Add Host to add up to 100 hosts.	-
Install ICAgent	<p>An ICAgent is a plug-in for collecting metrics and logs. The Install ICAgent option is enabled by default. It is optional. Enter an AK and SK to install an ICAgent.</p>	-

Step 5 Click **Install**. After the installation is complete, you can view the UniAgent in the UniAgent list.

----End

UniAgent Statuses

The UniAgent status can be **Running**, **Abnormal**, **Installing**, **Installation failed**, or **Not installed**.

Table 10-5 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. NOTE The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Try again.
Not installed	The UniAgent has not been installed on the host. Install the UniAgent by referring to 10.4.2.1 Installing a UniAgent .

10.4.2.2 Operating UniAgents in Batches

You can reinstall, upgrade, uninstall, or delete UniAgents on hosts in batches.

 **NOTE**

If the host where the UniAgent is to be installed runs Windows, you can only upgrade and delete the UniAgent. If you need to reinstall or uninstall the UniAgent, manually perform the operations on the host.

Reinstalling UniAgents

Reinstall UniAgents when they are in the **Abnormal**, **Installation failed**, or **Not installed** state.

- 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** In the navigation pane, choose **Collection Settings > VM Access**.
- Step 4** On the **VM Access** page, select the hosts where UniAgents are to be reinstalled and choose **UniAgent Batch Operation > Reinstall**.
- Step 5** On the page that is displayed, [install UniAgents](#).

 **NOTE**

The IP addresses of the hosts where UniAgents are to be reinstalled cannot be changed.

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version according to the following procedure:

NOTE

UniAgents will not be automatically upgraded. Manually upgrade them if needed.

- Step 1** In the navigation pane, choose **Settings > Collection Settings > VM Access**.
- Step 2** On the **VM Access** page, select the hosts where UniAgents are to be upgraded and choose **UniAgent Batch Operation > Upgrade**.
- Step 3** On the displayed page, select the target version and click **OK**.
- Step 4** Wait for about 1 minute until the upgrade is complete.

----End

Uninstalling UniAgents

Uninstall UniAgents when necessary.

- Step 1** In the navigation pane, choose **Settings > Collection Settings > VM Access**.
- Step 2** On the **VM Access** page, select the hosts where UniAgents are to be uninstalled and choose **UniAgent Batch Operation > Uninstall**.
- Step 3** In the dialog box that is displayed, click **OK** to uninstall the UniAgents.

----End

Deleting UniAgents

Delete the UniAgents that are not used or cannot be used according to the following procedure:

- Step 1** In the navigation pane, choose **Settings > Collection Settings > VM Access**.
- Step 2** On the **VM Access** page, select the hosts where UniAgents are to be deleted and choose **UniAgent Batch Operation > Delete**.
- Step 3** In the dialog box that is displayed, click **OK** to delete the UniAgents.

----End

10.4.2.3 Operating ICAgent Plug-ins in Batches

AOM will support interconnection with other types of plug-ins. You can install, upgrade, uninstall, start, stop, and restart plug-ins in batches.

Currently, ICAgents are supported. ICAgent collect metrics and logs.

Procedure

- 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** In the navigation pane, choose **Collection Settings > VM Access**.
- Step 4** On the **VM Access** page, select one or more hosts and click **Plug-in Batch Operation**.
- Step 5** In the displayed dialog box, select an operation type, set the plug-in information, and click **OK**.

Table 10-6 Plug-in operation parameters




Parameter	Description
Operation	The following batch operations are supported: install, upgrade, uninstall, start, stop, and restart.
Plug-in	ICAgent. The ICAgent of the latest version can be installed.
AK/SK	Access key ID and secret access key. For details, see How Do I Obtain an AK/SK .





----End

10.4.2.4 Other Operations

On the **UniAgent > VM Access** page, perform the following operations on the hosts where UniAgents are installed if needed:

Table 10-7 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host IP address, imported IP address, host name, installation host name, or proxy IP address.
Refreshing the host list	Click  in the upper right corner of the host list to refresh the list.
Customizing columns to display	Click  in the upper right corner of the host list to select the columns to display.
Filtering hosts	In the table heading of the host list, click  to filter hosts.

Operation	Description
Sorting hosts	In the table heading of the host list, click  next to UniAgent Heartbeat Time to sort hosts.  indicates the default order.  indicates the ascending order (that is, the host with the latest UniAgent heartbeat time is displayed at the end).  indicates the descending order (that is, the host with the latest UniAgent heartbeat time is displayed at the top).
Deleting a host	If a UniAgent is Abnormal, Not installed, or Installation failed , you can delete the corresponding host. Locate the target host and choose Delete in the Operation column. NOTE <ul style="list-style-type: none"> • Hosts with UniAgent being installed, upgraded, or uninstalled cannot be deleted. Refresh the page and wait. • Running hosts with UniAgent installed cannot be deleted. Uninstall UniAgent first. • Hosts set as installation hosts or proxies cannot be deleted. Ensure that they are not installation hosts or proxies.
Configuring an installation host	To set the name of an installation host, do as follows: Choose Configure Installation Host in the Operation column, and enter a desired name.
Canceling an installation host	To cancel an installation host, perform the following steps: Choose Cancel Installation Host in the Operation column to cancel an installation host.
Changing the name of an installation host	To change the name of a configured installation host, do as follows: Click the name of the installation host. In the dialog box that is displayed, rename it.

10.4.3 CCE Access

CCE Access displays all the CCE clusters that you have purchased. You can install, upgrade, and uninstall ICAgents on hosts in these clusters in batches.

Prerequisites

You have purchased a CCE cluster.

Viewing Clusters

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 In the navigation pane, choose **Collection Settings > CCE Access**.

Step 4 Check the connected CCE clusters. You can enter a keyword in the search box to search for your target cluster.

----End

Operating ICAgents

You can install, upgrade, and uninstall ICAgents on hosts in connected CCE clusters.

- Installing ICAgents: If no ICAgent has been installed on the hosts in a cluster, install ICAgents on them in batches.
 - a. In the **Cluster Name** area, locate the target cluster and click **Install ICAgent**.
 - b. On the page that is displayed, click **OK** to install ICAgents on all hosts in the cluster.
- Upgrading ICAgents: If the ICAgents installed on hosts in a cluster are of an earlier version, upgrade ICAgents in batches.
 - a. In the **Cluster Name** area, locate the target cluster and click **Upgrade ICAgent**.
 - b. On the page that is displayed, click **OK** to upgrade ICAgents on all hosts in the cluster.
- Uninstalling ICAgents: Uninstall ICAgents from all hosts in a cluster if needed.
 - a. In the **Cluster Name** area, locate the target cluster and click **Uninstall ICAgent**.
 - b. On the page that is displayed, click **OK** to uninstall ICAgents from all hosts in the cluster.

NOTE

Uninstalling ICAgents will cause some application O&M functions to be unavailable. Exercise caution when performing this operation.

10.4.4 Managing Host Groups

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the host group management function of [Log Tank Service \(LTS\)](#). You can perform operations on the AOM 2.0 or LTS console.

To use the host group management function on the AOM 2.0 console, [purchase LTS resources](#) first.

Table 10-8 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Host group management	Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.	<ol style="list-style-type: none"> 1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose Settings > Collection Settings > Host Groups. 	<ol style="list-style-type: none"> 1. Log in to the LTS console. 2. In the navigation pane, choose Host Management. 	Managing Host Groups

10.4.5 Proxy Area Management

To enable network communication between different clouds, purchase a Huawei Cloud ECS, set the ECS to a proxy, and bind an EIP to it. AOM then delivers deployment and control instructions to remote hosts and receives O&M data through the proxy. A proxy area contains multiple proxies for high availability.

10.4.5.1 Proxy Area

Proxy areas are used to manage proxy by category.

Adding a Proxy Area

- 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** In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.
- Step 4** Click **Add Proxy Area**. In the dialog box that is displayed, set parameters.

Table 10-9 Parameters for adding a proxy area

Parameter	Description	Example
Proxy Area Name	Enter a maximum of 50 characters.	test

Parameter	Description	Example
Network Type	Options: Private network and Public network .	Private network


Step 5 Click **OK**. The proxy area is added.

----End

Modifying a Proxy Area

After the proxy area is created, you can modify it as required. The following shows the procedure:

Step 1 In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Hover over the target proxy area and choose  > **Edit**.

Step 3 In the displayed dialog box, enter a new name and network type, and click **OK**.

----End

Deleting a Proxy Area

You can delete a proxy area that is no longer used. The procedure is as follows:

Step 1 In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.


Step 2 Hover over the target proxy area and choose  > **Delete**.

Step 3 In the dialog box that is displayed, click **Yes** to delete the proxy area.

----End

Searching for a Proxy Area

Step 1 In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Click . Then, in the search box, enter a keyword to search for your target proxy area.

----End

10.4.5.2 Proxy

A proxy is an ECS that you purchased from Huawei Cloud for network communication between different clouds.

Adding a Proxy

- 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** In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.
- Step 4** Click **Add Proxy** and set related parameters.

Table 10-10 Parameters for adding a proxy

Parameter	Description	Example
Proxy Area	Select a proxy area that you have created.	qwertyddfsdfdf
Host	Select a host where the UniAgent has been installed.	-
Proxy IP Address	Set the IP address of the proxy.	-
Port	Enter a port number, which cannot be greater than 65535.	-

- Step 5** Click **OK**. The proxy is added.
----End

Modifying a Proxy IP Address

After a proxy is created, you can change its IP address as required. The following shows the procedure:

- Step 1** In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.
- Step 2** Click **Modify Proxy IP** in the **Operation** column of the proxy. On the page that is displayed, modify the proxy IP address.
- Step 3** Click **OK**. The proxy IP address is modified.
----End

Checking a Proxy

After a proxy is created, check the proxy if needed:

- Step 1** In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.
- Step 2** Click a proxy area to view the proxy in it.
----End

Deleting a Proxy

You can delete a proxy that is no longer used. The procedure is as follows:

- Step 1** In the navigation tree on the left, choose **Collection Settings > Proxy Areas**. The **Proxy Areas** page is displayed.
 - Step 2** Click **Delete** in the **Operation** column of the target proxy.
 - Step 3** In the dialog box that is displayed, click **OK** to delete the proxy.
- End

10.4.6 Operation Logs

Operation logs record the operations (such as installation, upgrade, and uninstall) performed on UniAgents and other plug-ins.

Checking Operation Logs of UniAgent

- 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** In the navigation tree on the left, choose **Collection Settings > Operation Logs**. On the displayed page, click the **UniAgent Logs** tab.

 **NOTE**

You can search for historical tasks by date. The options are **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**.

- Step 4** Click a task ID. On the task details page that is displayed, click **View Log** to view UniAgent operation logs.
- End

Viewing Operation Logs of Plug-ins

- 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** In the navigation tree on the left, choose **Collection Settings > Operation Logs**. On the displayed page, click the **Plug-in Logs** tab.

 **NOTE**






You can search for historical tasks by date. The options are **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**.

- Step 4** Click a task ID. On the task details page that is displayed, click **View Log** to view plug-in operation logs.
- End

Other Operations

On the **Operation Logs** page, perform the operations listed in the following table if needed.

Table 10-11 Related operations

Operation	Description
Searching for historical tasks	In the search box above the task list, search for historical tasks by executor.
Filtering historical tasks by time range	In the upper part of the task list, search for historical tasks by time range. The options are Last hour , Last 6 hours , Last day , Last 3 days , and Custom .
Refreshing the task list	Click  in the upper right corner of the task list to refresh the list.
Viewing task information	Click a task ID to view the task details, including the host name, IP address, plug-in type, task type, execution status, failure cause, execution event, duration, and operation logs.
Filtering tasks	In the table heading of the task list, click  to filter tasks.
Sorting tasks	In the table heading of the task list, click  to sort task orders.  indicates the ascending order while  indicates the descending order.

10.5 Log Settings

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the log functions of [Log Tank Service \(LTS\)](#). You can perform operations on the AOM 2.0 or LTS console.

To use log functions on the AOM 2.0 console, [purchase LTS resources](#) first.

Table 10-12 Function description

Function	Description	AOM 2.0 Console	LTS Console	References
Quota configuration	When the monthly free quota (500 MB) is used up, you will be billed for any excess usage on a pay-per-use basis. To avoid extra expenses, you can stop log collection when the quota runs out.	<ol style="list-style-type: none"> 1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose Settings. The Global Configuration page is displayed. 3. In the navigation pane on the left, choose Log Settings. Click the Quota Configuration tab. 	<ol style="list-style-type: none"> 1. Log in to the LTS console. 2. In the navigation pane, choose Configuration Center. 	Quota Configuration
ICAgent collection	Configure ICAgent collection as required to reduce memory, database, and disk space usage.	<ol style="list-style-type: none"> 1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose Settings. The Global Configuration page is displayed. 3. In the navigation pane on the left, choose Log Settings. Click the ICAgent Collection tab. 	<ol style="list-style-type: none"> 1. Log in to the LTS console. 2. In the navigation pane, choose Configuration Center. 3. Click the ICAgent Collection tab. 	Log Collection

10.6 Menu Settings

You can choose to show or hide **Overview**, **Log Stream**, and **Business Monitoring** in the navigation pane of the console.

Procedure

- 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** In the navigation pane, choose **Menu Settings**. All functions are disabled by default. Enable them as required.

For example, if the **Overview** option is enabled, it will be displayed in the navigation tree on the left of the console.

----End

11 Remarks

11.1 Alarm Tags and Annotations

When creating alarm rules, you can set alarm tags and annotations. Tags are attributes that can be used to identify alarms. They are applied to alarm noise reduction scenarios. Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.

Alarm Tag Description

- Alarm tags can apply to grouping rules, suppression rules, and silence rules. The alarm management system manages alarms and notifications based on the tags.
- Each tag is in "key:value" format and can be customized. Each key and value can contain only letters, digits, and underscores (_).
- If you set a tag when creating an alarm rule, the tag is automatically added as an alarm attribute when an alarm is triggered.
- In a message template, the `$event.metadata.key1` variable specifies a tag. For details, see [Table 4-26](#).

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 Description

- Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.
- Each annotation is in "key:value" format and can be customized. You can create up to 10 custom annotations. The key and value can only contain letters, digits, and underscores (_).
- In a message template, the `$event.annotations.key2` variable specifies an annotation. For details, see [Table 4-26](#).

Managing Alarm Tags and Annotations

You can add, delete, modify, and query alarm tags or annotations on the alarm rule page.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Rules**.




Step 3 Click **Create**, or locate a desired alarm rule and click  in the **Operation** column.

Step 4 On the displayed page, click **Advanced Settings**.

Step 5 Under **Alarm Tag** or **Alarm Annotation**, click  and enter a key and value.

Step 6 Click **OK** to add an alarm tag or annotation.

NOTE

- Adding multiple alarm tags or annotations: Click  multiple times to add alarm tags or annotations (max.: 10).
- Modifying an alarm tag or annotation: Move the cursor to a desired alarm tag or annotation and click  to modify them.
- Deleting an alarm tag or annotation: Move the cursor to a desired alarm tag or annotation and click  to delete them.

----End

11.2 Prometheus Statements

AOM is interconnected with Prometheus Query Language (PromQL), which provides various built-in functions. These functions can be used to filter and aggregate metric data. You can run Prometheus statements to add metrics.

Prometheus Statement Syntax

For details about the Prometheus statement syntax, go to the [Prometheus official website](#).

Examples of Using Prometheus Statements

- **Example 1: Memory usage of a specified pod in a node (excluding the control node)**
 - Define variables:
 - Used memory of the containers in a pod (a pod may contain multiple containers or instances):
aom_container_memory_used_megabytes
 - Total memory of the node: **aom_node_memory_total_megabytes**
 - Query logic:

- For **aom_container_memory_used_megabytes**, use the aggregation function **sum** to calculate the actual used memory of a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_memory_total_megabytes**, use the aggregation function **sum** to calculate the total memory of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
 - To query the actual memory usage of the pod, use the following statement:


```
sum(aom_container_memory_used_megabytes{podID="****1461-41d8-****-bfeb-fc1213****",nodeIP="***.***.***.***"}) by (nodeIP) /
sum(aom_node_memory_total_megabytes{nodeIP="***.***.***.***"}) by (nodeIP)
```
- **Example 2: CPU usage of a specified pod in a node (excluding the control node)**
 - Define variables:
 - Used CPU cores of the containers in a pod:
aom_container_cpu_used_core
 - Actual total number of CPU cores of the node:
aom_node_cpu_limit_core
 - Query logic:
 - For **aom_container_cpu_used_core**, use the aggregation function **sum** to calculate the used CPU cores of a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_cpu_limit_core**, use the aggregation function **sum** to calculate the total CPU cores of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
 - To obtain the actual CPU usage of the pod, use the following statement:


```
sum(aom_container_cpu_used_core{nodeIP="***.***.***.***",podID="****1461-41d8-****-bfeb-****13****"}) by (nodeIP) /
sum(aom_node_cpu_limit_core{nodeIP="***.***.***.***"}) by (nodeIP)
```
- **Example 3: Requested memory of a pod/Allocable memory of the node where the pod is located**
 - Define variables:

- Memory allocated to the containers in a pod:
aom_container_memory_request_megabytes
- Total memory of the node: **aom_node_memory_total_megabytes**
- Query logic:
 - For **aom_container_memory_request_megabytes**, use the aggregation function **sum** to calculate the allocated memory of a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_memory_total_megabytes**, use the aggregation function **sum** to calculate the total memory of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
- To obtain the actual memory allocation ratio of the pod, use the following statement:

```
sum(aom_container_memory_request_megabytes{podID="****1461-41d8-4403-****-f***35****",nodeIP="***.*.*.*.*"}) by (nodeIP) /  
sum(aom_node_memory_total_megabytes{nodeIP="***.*.*.*.*"}) by (nodeIP)
```
- **Example 4: Requested CPU cores of a pod/Allocable CPU cores of the node where the pod is located**
 - Define variables:
 - CPU cores allocated to the containers in the pod:
aom_container_cpu_limit_core
 - CPU cores allocated to the node: **aom_node_cpu_limit_core**
 - Query logic:
 - For **aom_container_cpu_limit_core**, use the aggregation function **sum** to calculate the CPU cores allocated to a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_cpu_limit_core**, use the aggregation function **sum** to calculate the total CPU cores of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual CPU usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
 - To obtain the actual CPU allocation ratio of the pod, use the following statement:

```
sum(aom_container_cpu_limit_core{podID="*****461-41d8-****-bfeb-
****135*****",nodeIP="***.***.***.***"}) by (nodeIP) /
sum(aom_node_cpu_limit_core{nodeIP="***.***.***.***"}) by (nodeIP)
```

Common Prometheus Commands

Table 11-1 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 11-1 Common Prometheus commands

Metric	Tag Definition	PromQL
Host CPU usage	{nodeIP="", hostID=""}	aom_node_cpu_usage{nodeIP="192.168.57.93",hostID="ca76b63f-dbf8-4b60-9c71-7b9f13f5ad61"}
Host application request throughput	{aomApplicationID="",aomApplicationName=""}	http_requests_throughput{aomApplicationID="06dc9f3b0d8cb867453ecd273416ce2a",aomApplicationName="root"}
Success rate of host application requests	{appName="",serviceID="",clusterId=""}	http_requests_success_rate{aomApplicationID="06dc9f3b0d8cb867453ecd273416ce2a",aomApplicationName="root"}
Host component CPU usage	{appName="",serviceID="",clusterId=""}	aom_process_cpu_usage{appName="icagent",serviceID="2d29673a69cd82fabe345be5f0f7dc5f",clusterId="00000000-0000-0000-0000-00000000"}
Host process threads	{processCmd=""} {processID=""} {processName=""}	aom_process_thread_count{processCmd="cdbbc06c2c05b58d598e9430fa133aff7_b14ee84c-2b78-4f71-9ecc-2d06e053172c_ca4d29a846e9ad46a187ade88048825e",processName="icwatchdog"}
Cluster disk usage	{clusterId="",clusterName=""}	aom_cluster_disk_usage{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="servicestage-test"}
Cluster virtual memory usage	{clusterId="",clusterName=""}	aom_node_virtual_memory_usage{nodeIP="192.168.10.4",clusterId="af3cc895-bc5b-11ec-a642-0255ac101a0b",nameSpace="default"}

Metric	Tag Definition	PromQL
Available cluster virtual memory	{clusterId="",clusterName=""}	aom_cluster_virtual_memory_free_megabytes{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="servicestage-test"}
Workload file system usage	{appName="",serviceID="",clusterId="",nameSpace=""}	aom_container_filesystem_usage{appName="icagent",serviceID="cfebc2222b1ce1e29ad827628325400e",clusterId="af3cc895-bc5b-11ec-a642-0255ac101a0b",nameSpace="kube-system"}
Pod kernel usage	{podID="",podName=""}	aom_container_cpu_used_core{podID="573663db-4f09-4f30-a432-7f11bdb8fb2e",podName="icagent-bkm6q"}
Container uplink rate (BPS)	{containerID="",containerName=""}	aom_container_network_transmit_bytes{containerID="16bf66e9b62c08493ef58ff2b7056aae5d41496d5a2e4bac908c268518eb2cbc",containerName="coredns"}

11.3 What Is the Relationship Between the Time Range and Statistical Period?

In AOM, a maximum of 1440 data points can be returned for a single metric query. The relationship between the time range and statistical period is as follows:

Maximum time range = Statistical period x 1440

If you select a time range shorter than or equal to the maximum time range, all the statistical periods that meet the preceding formula can be selected. For example, if you want to query metrics in the last hour, the available statistical periods are 1 minute and 5 minutes.

For a [dashboard](#), the relationship between the time range and statistical period is shown in the following table.

Table 11-2 Relationship between the time range and statistical period

Time Range	Statistical Period
Last 30 minutes	1 minute or 5 minutes

Time Range	Statistical Period
Last hour	
Latest 6 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
Last day	
Last week	1 hour
Custom	1 minute, 5 minutes, 15 minutes, or 1 hour

12 Permissions Management

12.1 Creating a User and Granting Permissions

This section describes the fine-grained permissions management provided by IAM for your AOM. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials for accessing AOM resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or a cloud service to perform professional and efficient O&M on your AOM resources.

If your account does not need individual IAM users, then you may skip over this section.

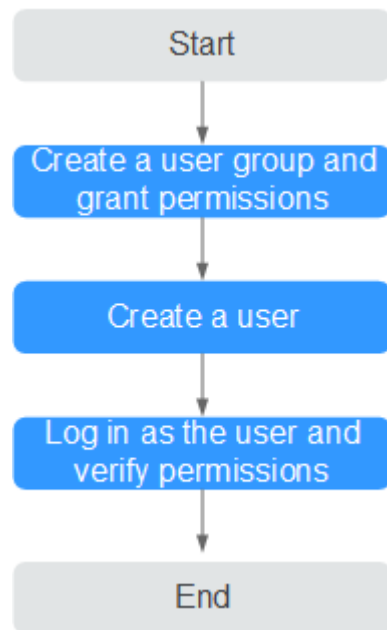
This section describes the procedure for granting permissions (see [Figure 12-1](#)).

Prerequisites

Before assigning permissions to user groups, you should learn about the AOM permissions listed in [Permissions Management](#). For the permissions of other services, see [System Permissions](#).

Process

Figure 12-1 Process for granting AOM permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the **AOM ReadOnlyAccess** policy to the group.
2. **Create a user and add the user to the user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in as an IAM user** and verify permissions.
Log in to the AOM console as the created user, and verify that it only has read permissions for AOM.

12.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of AOM. For the actions supported for custom policies, see [Permissions Policies and Supported Actions](#).

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details about how to create custom policies, see [Creating a Custom Policy](#). The following lists examples of common AOM custom policies.

Example Custom Policies

- Example 1: Allowing a user to create alarm rules

```
{  
  "Version": "1.1",
```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "aom:alarmRule:create"
    ]
  }
]
}

```

- Example 2: Forbidding a user to delete application discovery rules

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

To grant a user the **AOM FullAccess** system policy but forbid the user to delete application discovery rules, create a custom policy that denies the deletion of application discovery rules, and grant both the **AOM FullAccess** and deny policies to the user. Because the Deny action takes precedence, the user can perform all operations except deleting application discovery rules. The following is an example deny policy:

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "aom:discoveryRule:delete"
      ]
    }
  ]
}

```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain actions of multiple services that are all of the project-level type. The following is an example policy containing actions of multiple services:

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aom*:list",
        "aom*:get",
        "apm*:list",
        "apm*:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cce:cluster:get",
        "cce:cluster:list",
        "cce:node:get",
        "cce:node:list"
      ]
    }
  ]
}

```

13 Auditing

13.1 Operations Logged by CTS

AOM is a one-stop O&M platform that monitors applications and resources in real time. By analyzing dozens of metrics and correlation between alarms and logs, AOM helps O&M personnel quickly locate faults.

You can use AOM to comprehensively monitor and uniformly manage servers, storage, networks, web containers, and applications hosted in Docker and Kubernetes. This effectively prevents problems and helps O&M personnel locate faults in minutes, reducing O&M costs. Also, AOM provides unified APIs to interconnect in-house monitoring or report systems. Unlike traditional monitoring systems, AOM monitors services by application. It meets enterprises' requirements for high efficiency and fast iteration, provides effective IT support for their services, and protects and optimizes their IT assets, enabling enterprises to achieve strategic goals and maximize value. With CTS, you can record operations associated with AOM for future query, audit, and backtracking.

 **NOTE**

pe traces actually record AOM operations, but these operations are performed through CCE or ServiceStage.

Table 13-1 Operations logged by CTS

Function	Operation	Resource Type	Trace
Global Configuration	Adding an access code	icmgr	icmgrAddAccessCode
	Deleting an access code	icmgr	icmgrDelAccessCode
Resource Monitoring	Creating a dashboard	dashboard	updateDashboard
	Deleting a dashboard	dashboard	deleteDashboard

Function	Operation	Resource Type	Trace
	Updating a dashboard	dashboard	updateDashboard
	Creating a dashboard group	dashboard_folder	addDashboardFolder
	Updating a dashboard group	dashboard_folder	updateDashboardFolder
	Deleting a dashboard group	dashboard_folder	deleteDashboardFolder
	Creating or updating an alarm rule	audit_v4_alarm_rule	addOrUpdateAlarm
	Deleting an alarm rule	audit_v4_alarm_rule	delAlarmRule
	Creating a process discovery rule	appDiscoveryRule	addAppDiscoveryRule
	Updating a process discovery rule	appDiscoveryRule	updateAppDiscoveryRule
	Deleting a process discovery rule	appDiscoveryRule	delAppDiscoveryRule
	Adding an alarm template	audit_v4_alarm_rule	addAlarmRuleTemplate
	Modifying an alarm template	audit_v4_alarm_rule	modAlarmRuleTemplate
	Deleting an alarm template	audit_v4_alarm_rule	delAlarmRuleTemplate
	Adding a grouping rule	groupRule	addGroupRule
	Modifying a grouping rule	groupRule	updateGroupRule
	Deleting a grouping rule	groupRule	delGroupRule
	Adding a suppression rule	inhibitRule	addInhibitRule
	Modifying a suppression rule	inhibitRule	updateInhibitRule
	Deleting a suppression rule	inhibitRule	delInhibitRule

Function	Operation	Resource Type	Trace
	Adding a silence rule	muteRule	addMuteRule
	Modifying a silence rule	muteRule	updateMuteRule
	Deleting a silence rule	muteRule	delMuteRule
	Adding an alarm action rule	actionRule	addActionRule
	Modifying an alarm action rule	actionRule	updateActionRule
	Deleting an alarm action rule	actionRule	delActionRule
	Adding a message template	notificationTemplate	addNotificationTemplate
	Modifying a message template	notificationTemplate	updateTemplate
	Deleting a message template	notificationTemplate	delTemplate

13.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

This section describes how to query or export operation records of the last seven days on the CTS console.

- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)





Constraints

- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must

configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.

- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.




Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
 - **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.
 - **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
 - Enter any keyword in the search box and press **Enter** to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the

next line; otherwise, the text will be truncated. By default, this function is disabled.

6. For details about key fields in the trace structure, see [Trace Structure](#) and [Example Traces](#).
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
 - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
 - If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.
 - **Operator:** Select a user.
 - **Trace Status:** Select **All trace statuses, Normal, Warning, or Incident**.
 - **Time range:** Select **Last 1 hour, Last 1 day, or Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
8. Click  on the left of a trace to expand its details.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
createDockerConfig	dockerlogcmd	SWR	--	dockerlogcmd	normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace

```

request
trace_id
code
trace_name
resource_type
trace_idring
app_version
message
source_id
domain_id
trace_type
            
```

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

14 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.

Procedure



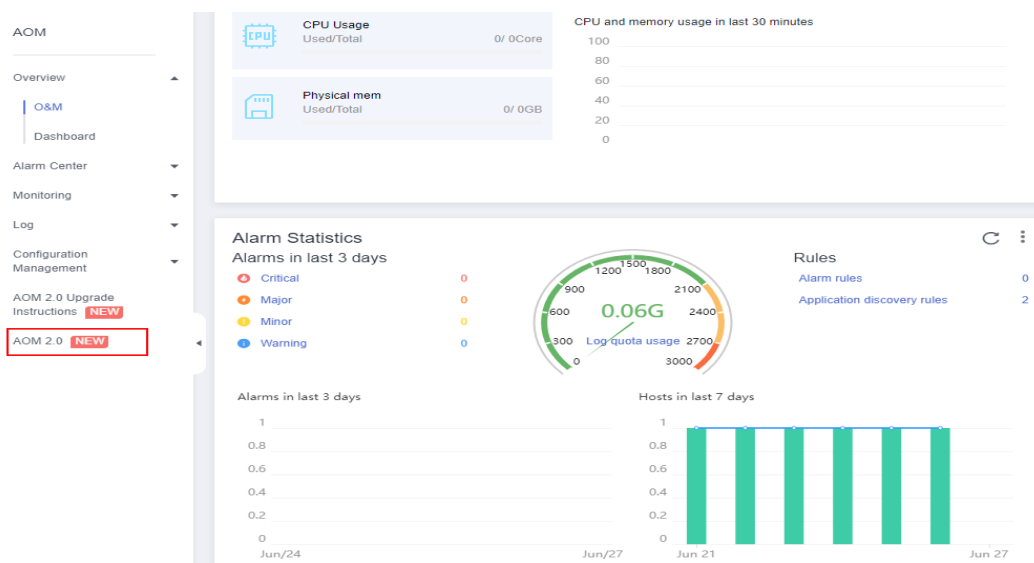
- Step 1** Log in to the Huawei Cloud management console.
- Step 2** Click  in the upper left corner and select your desired region from the drop-down list.
- Step 3** Click  on the left and choose **Management & Deployment > Application Operations Management**.
- Step 4** In the navigation pane on the left, choose **AOM 2.0**. The AOM 2.0 page is displayed.

Figure 14-1 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

15 Upgrading to AOM 2.0

15.1 Manual Upgrade

This section describes how to migrate data from AOM 1.0 to AOM 2.0. Currently, only log, collector, and alarm rule upgrades are supported.

Functions

- **Collector Upgrade**
After the upgrade, the collector can better discover processes and automatically adapt to metric browsing functions.
- **Alarm Rule Upgrade**
After alarm rules are upgraded, alarm rule data is smoothly switched from AOM 1.0 to AOM 2.0, and is automatically adapted to alarm rule functions of AOM 2.0.

Collector Upgrade

- Step 1** Log in to the AOM 1.0 console.
- Step 2** In the navigation pane, choose **Configuration Management > Agent Management**.
- Step 3** Select **Other: custom hosts** from the drop-down list on the right of the page.
- Step 4** Select a host and click **Upgrade ICAgent**.
- Step 5** Select a target AOM 2.0 version from the drop-down list and click **OK**.
- Step 6** Wait for the upgrade. This process takes about a minute. When the ICAgent status changes from **Upgrading** to **Running**, the upgrade is successful.

NOTE

If the ICAgent is abnormal after the upgrade or if the upgrade fails, log in to the host and run the installation command again. Note that there is no need for you to uninstall the original ICAgent.

----End

Alarm Rule Upgrade

- Step 1** Log in to the AOM 1.0 console.
- Step 2** In the navigation pane on the left, choose **Alarm Center > Alarm Rules**.
- Step 3** Select one or more alarm rules and click **Migrate to AOM 2.0** above the rule list.

NOTICE

- Migration cannot be undone. Exercise caution when performing this operation.
 - If the alarm rules to be migrated depend on alarm templates, these alarm templates will also be migrated.
-

- Step 4** In the displayed dialog box, click **Confirm**. The selected alarm rules will be migrated to AOM 2.0 in batches.

----End

15.2 One-click Migration

Quickly migrate dashboard and alarm rule data from AOM 1.0 to AOM 2.0.

Precautions

- AOM allows you to migrate all alarm rules in one click and query migration results.
- The backend checks data migration status:
 - Migrated: A dialog box is displayed, indicating that the migration is complete.
 - Not migrated: The one-click migration dialog box is displayed.
 - Migrating: A dialog box is displayed, indicating that the migration is in progress. (Migration will stop if you close the dialog box, but will continue if you open it again.)

Procedure

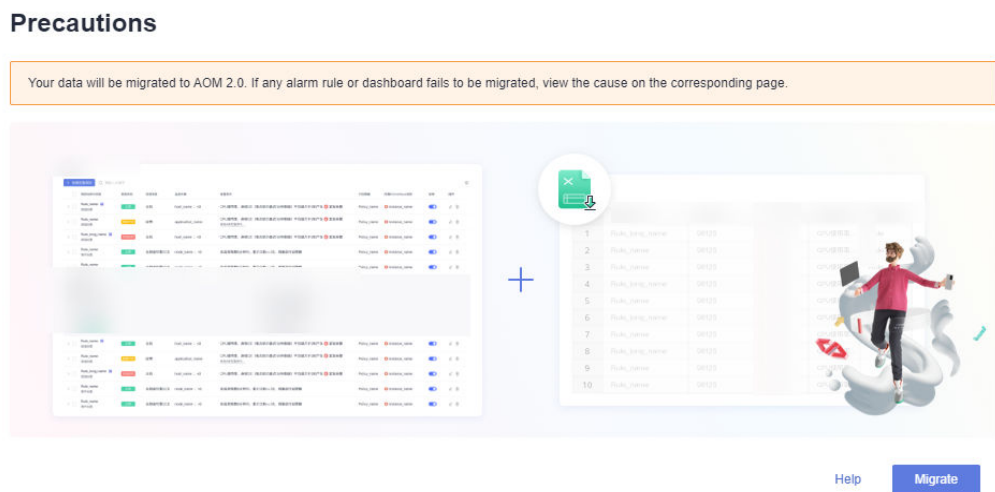
- Step 1** Log in to the AOM 1.0 console.
- Step 2** In the **AOM 2.0 New Features** dialog box, click **Migrate**.

Figure 15-1 New features dialog box



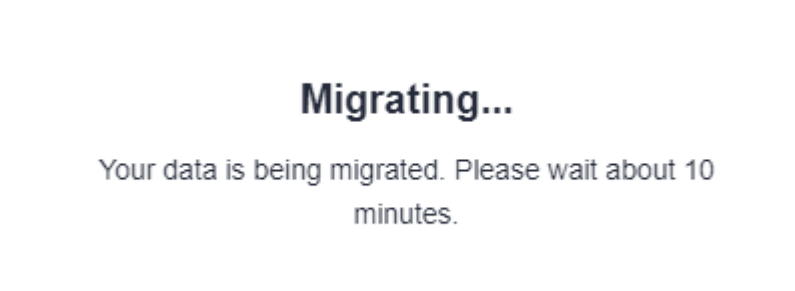
Step 3 In the **Precautions** dialog box, click **Migrate**.

Figure 15-2 Precautions dialog box



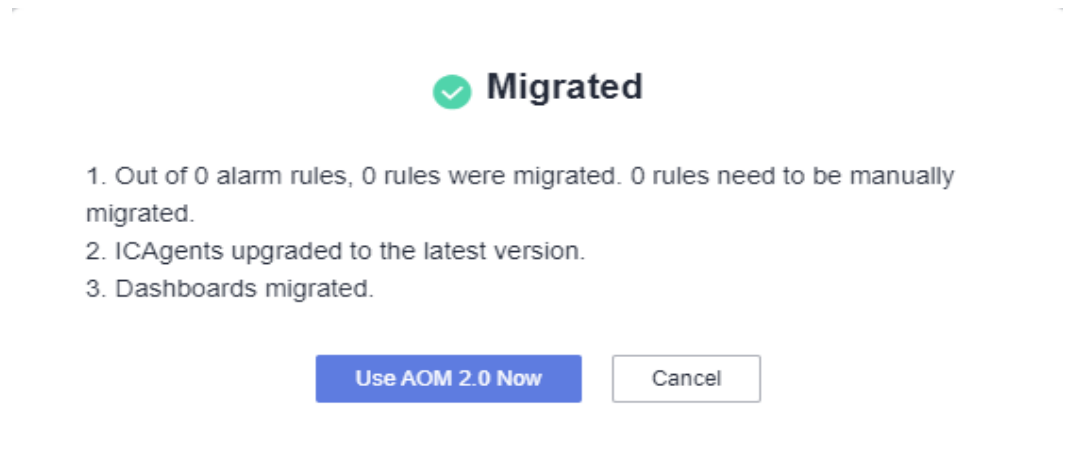
Step 4 The migration starts. A dialog box is displayed, showing "Migrating".

Figure 15-3 Migration in progress



Step 5 After the migration is complete, click **Use AOM 2.0 Now** in the dialog box to go to the AOM 2.0 console.

Figure 15-4 Migration completed



NOTE

After you click **Use AOM 2.0 Now**, you will automatically be redirected to AOM 2.0 when accessing AOM 1.0. To return to the AOM 1.0 console, choose **Back to 1.0** in the navigation pane of the AOM 2.0 console.

----End