Application Operations Management

User Guide

Issue	01
Date	2024-05-27

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 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 application or 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	Provides the alarm list, event list, alarm rules, alarm templates, and alarm notifications. • 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	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.

Category	Description
Log analysis	AOM allows you to search for logs, view log files, set log paths, dump logs, ingest logs to Log Tank Service (LTS), and use log streams. • 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. • LTS access By adding access rules, you can map logs of Cloud Container Engine (CCE), Cloud Container Instance (CCI), or custom clusters in AOM to LTS. Then you can view and analyze logs on LTS. Mapping does not generate extra fees, but duplicate mapping will. • Log streams Supports log search.
Application insights (retiring)	Provides application monitoring, CMDB, and log ingestion. • Application monitoring An application groups identical or similar components based on service requirements. AOM supports monitoring by application. • CMDB You can use CMDB to centrally manage and bind resources and applications on Huawei Cloud, and provide accurate, consistent data in time for O&M. • Log ingestion ICAgents collect logs from hosts based on your specified collection rules, and pack and send the collected log data to AOM on a log stream basis. You can view logs on the AOM console in real time.

Category	Description
Prometheus monitoring	Provides Prometheus instances and resource usage statistics. ● 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)	Enables you to create log metric rules.
Infrastructure monitoring	Monitors workloads, clusters, hosts, processes, and cloud services. ● 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. – 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. ● Cloud service monitoring Service instance statuses and metric usage are displayed in line graphs and digit graphs. You can create alarm rules for monitored items.

Category	Description
Intelligent insights (beta)	Continuously monitors your applications and resources, detects problems based on historical data and problem characteristics, and provides root cause analysis and suggestions.
Collection management	Centrally manages the lifecycle of collection plug-ins and delivers instructions (such as script delivery and execution). UniAgent does not collect data; instead, collection plug-ins do that. Such plug-ins can be installed, upgraded, or uninstalled as required. Plug-ins for Cloud Eye and Host Security Service (HSS) will be rolled out later.
Automation (Retiring)	Provides atomic operations such as batch script execution, file distribution, and cloud service change, and allows you to customize and orchestrate atomic operations and assemble them into jobs and standard O&M processes.
Settings	Provides service authorization, authentication, global settings, data subscription, and menu settings. • 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. • Data subscription Subscribe to metrics or alarms. After subscription, data can be forwarded to DMS topics or Webhook for retrieval. • Menu settings You can choose to show or hide **Overview**, **Application Insights**, **Automation**, **Cloud Service Monitoring**, **Log Stream**, and **Business Monitoring** in the navigation pane of the console.

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

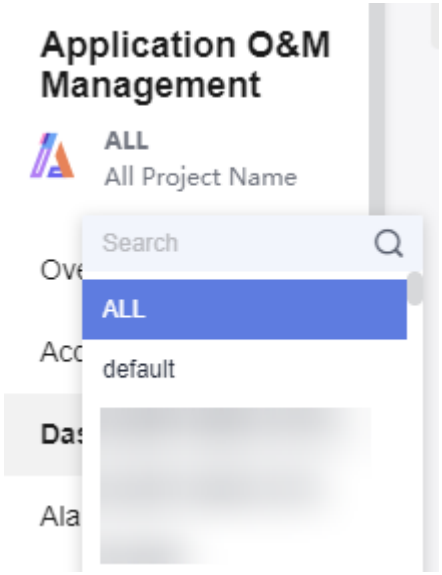
An enterprise project can contain one or more applications.

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

AOM monitors metric 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 usage of metrics and status 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 **9.1 Creating a Log Metric Rule**.
- Click the **APM Transactions** card. On the displayed page, connect APM transaction metrics.

----End

Application Access

Connect component performance graphs or API performance metrics, such as the average latency, error calls, and throughput.

Step 1 Log in to the AOM 2.0 console.

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

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

Step 4 On the displayed page, connect related application metrics.

----End

Middleware Access

Connect native or cloud middleware metrics, such as 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 **Middleware** panel, click a target card.

- Click the **MySQL** card. On the displayed page, set collection task parameters and install Exporter. After the connection, you can monitor metrics of the MySQL database. For details, see **MySQL Collection Task Parameters**.

----End

Environment Access

This function enables CCE and CCI 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 **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**.
- CCI automatically reports metrics to AOM as ready-to-use data. No manual configuration is required.

  Click the **Cloud Container Instance (CCI)** card to view the connected CCI metrics. For details about the CCI metrics that are automatically reported to AOM, see **Basic Metrics - VM Metrics**.
- Click the **ECS ICAgent (Old)** card. On the **Collection Management** page, click **Install UniAgent** to install the 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**.

----End

Connecting 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**.
- IoTDA automatically reports metrics to AOM as ready-to-use data. For details about IoTDA metrics, see **Basic Metrics - IoTDA 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 **Cloud Services** panel, click a target cloud service card.

Step 4 In the displayed dialog box, select a target cloud service and click **Confirm** to connect the cloud service metrics to the created **Prometheus instance for cloud services**.

----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 **Prometheus for Remote Write** card.

Step 4 In the displayed dialog box, **create a Prometheus instance for remote write**.

----End

API/SDK Access

Connect metric data using APIs.

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, cloud service, 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. • 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.
Bind to Application	Select an application created in CMDB to bind.
Group Type	Options: **Existing** and **New**. • **Existing**: Select an existing dashboard group from the drop-down list. • **New**: Enter a dashboard group name to create one.

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, or system data. 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 infrastructure, middleware, application, and business metrics.
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

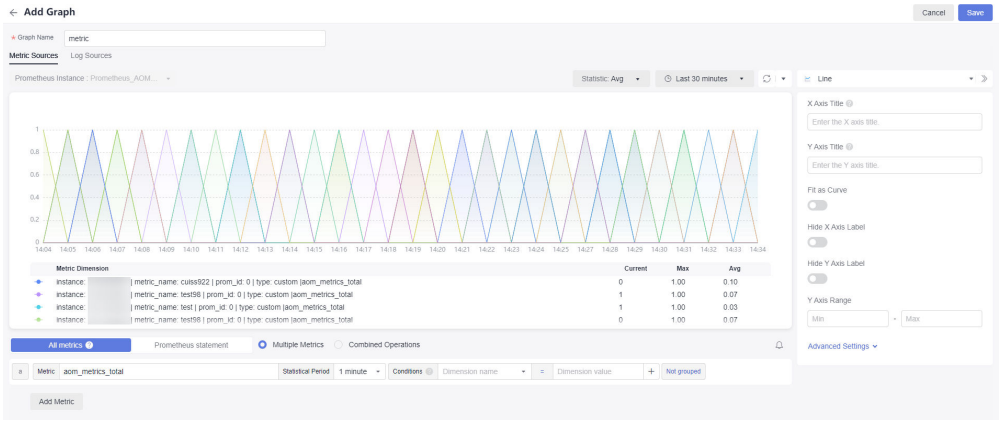


Table 3-3 Adding a metric graph

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	Add metrics as required. There are two ways to add metrics: – **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 **14.2 Prometheus Statements**. Click **Add Metric** to add up to 100 metric data records. **NOTE** – 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.
Graph Settings	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)**.
Statistic	Method used to measure metrics. Options: **Avg**, **Min**, **Max**, **Sum**, and **Samples**.
Statistical Period	Interval at which metric data is collected. 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**.
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**.

- Add a log graph. Set parameters by referring to **Table 3-4**. Then click **Save**.

Figure 3-2 Adding a log graph

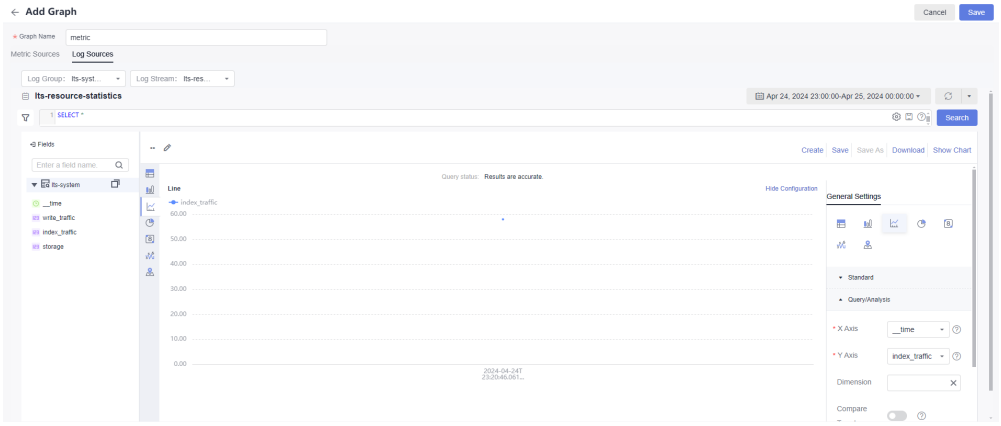


Table 3-4 Log graph parameters

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**.
Log Graph	Select a proper log graph from the drop-down list. If there is no log graph you want to select, click **Add Log Graph** to create one. For details, see **Table 3-6**.

Parameter	Description
Graph Settings	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. ▪ 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	• 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	• 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	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	You can delete a dashboard using either of the following methods: Method 1: 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**. 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.
Deleting a graph from a dashboard	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.

Operation	Description
Relocating a graph on a dashboard	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	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.
Adding alarm rules	• Adding an alarm rule when adding a graph 1. Click **Add Graph** on the page or click in the upper right corner of the page. 2. 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 1. Locate a target dashboard, move the cursor to the upper right corner of a graph, and choose > **Modify**. 2. 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**.

Operation	Description
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.
Importing a dashboard	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: Method 1: On the **Dashboard** page, click **Import Dashboard**. Method 2: In the dashboard group list, locate the group to which the dashboard is to be imported, and choose > **Import Dashboard**. Procedure: 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	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.

Table 3-6 Operations related to log graphs

Operation	Description
Creating a log group	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	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 3-3 Setting the online duration

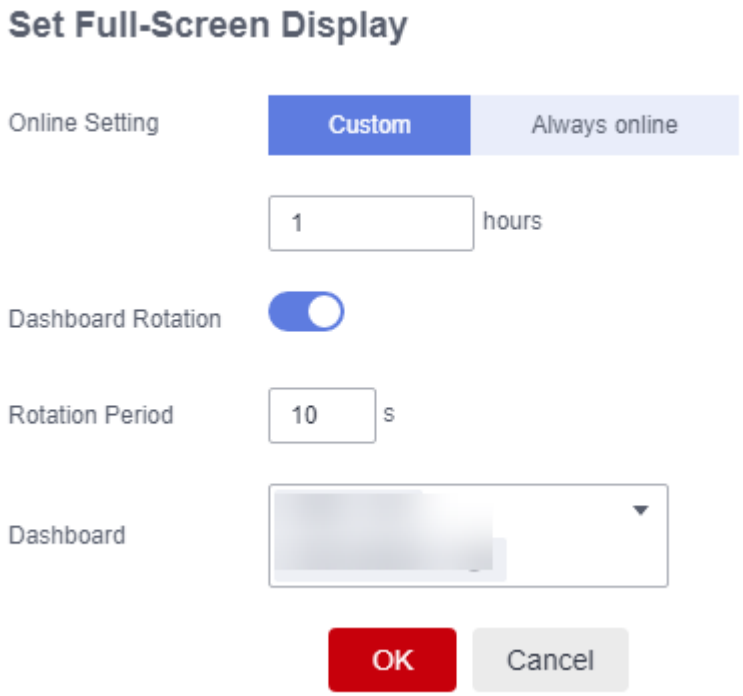


Table 3-7 Online duration parameters

Parameter	Description
Online Setting	Mode of setting the online duration. Options: • **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.

Parameter	Description
Duration	Full-screen online duration. The duration varies according to the setting mode. • **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.

Parameter	Description
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. Options: Prometheus instance for cloud services, ECS, CCE, remote write, or multi-account aggregation, or the default Prometheus instance.
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.
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.

----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

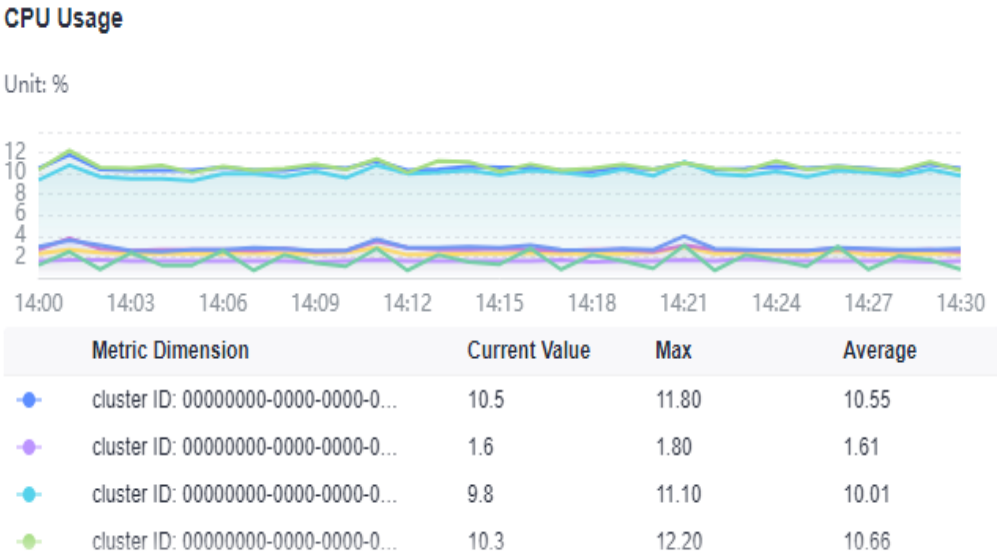


Table 3-10 Line graph parameters

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.
	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

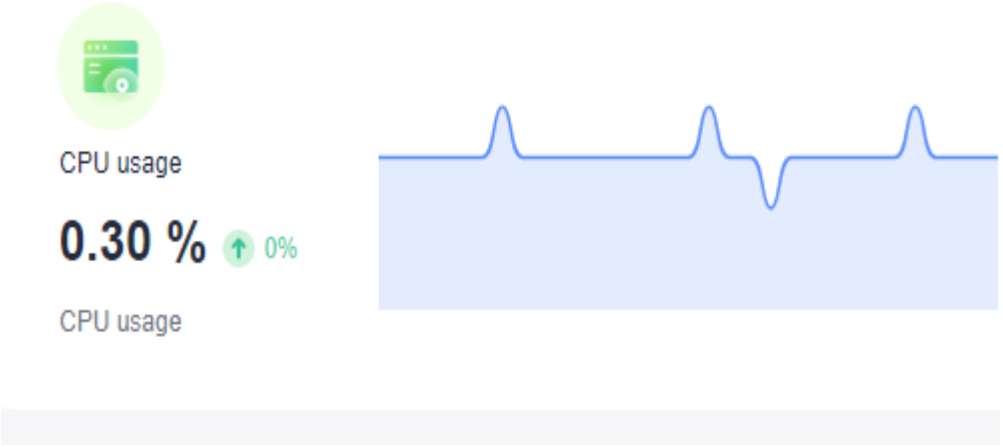


Table 3-11 Digit graph parameters

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

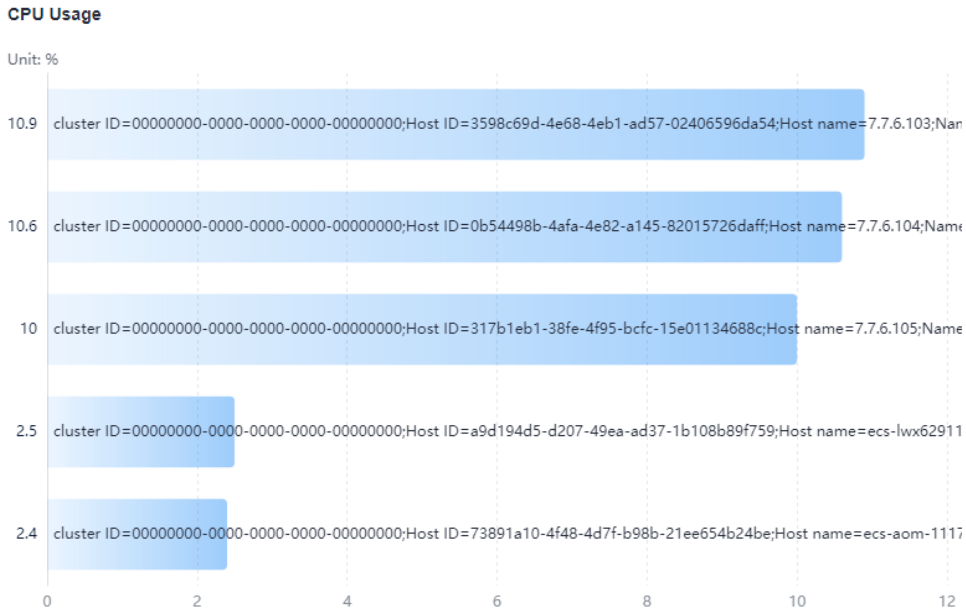


Table 3-12 Top N graph parameters

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.

Category	Parameter	Description
-	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.
-	Display Y-Axis Line	After this function is enabled, the line on the Y axis is displayed.
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.
	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

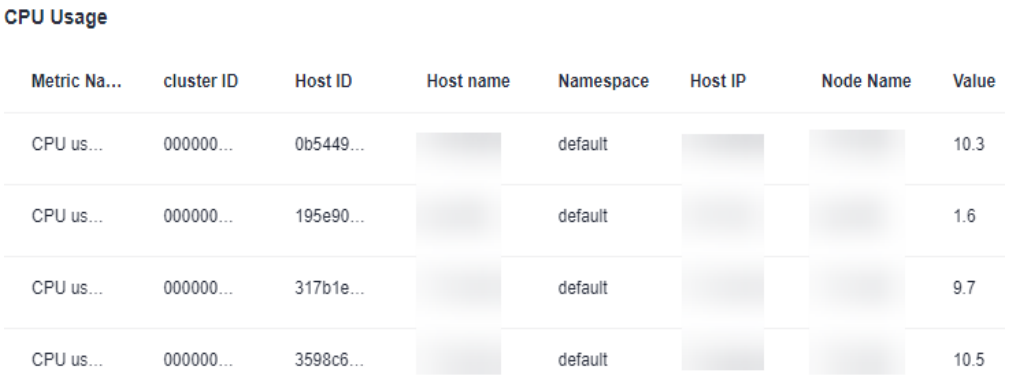


Table 3-13 Table parameters

Parameter	Description
Field Name	Name of a field.

Parameter	Description
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

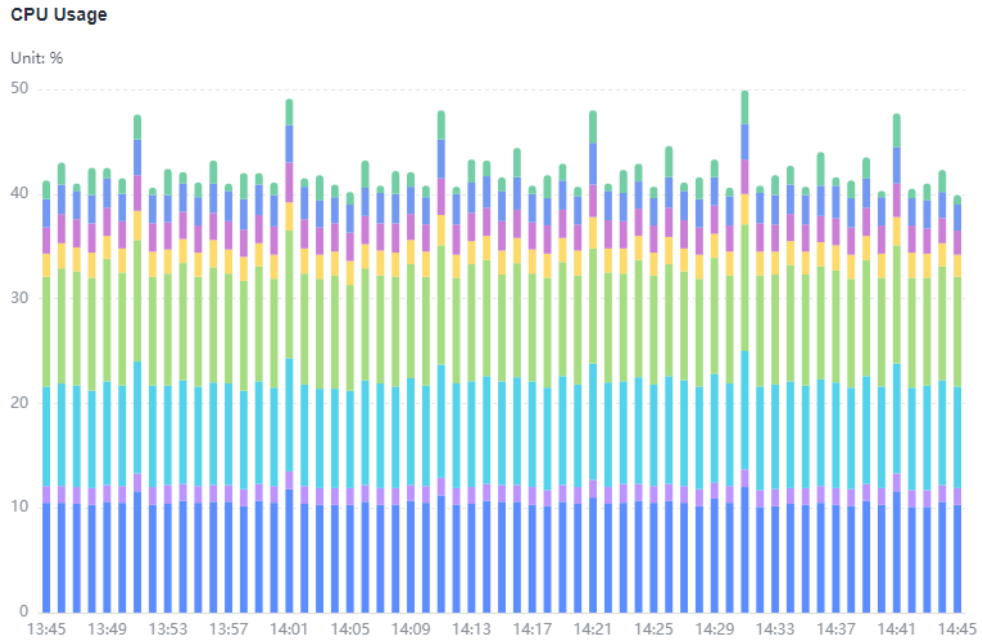


Table 3-14 Bar graph parameters

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.

Category	Parameter	Description
	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

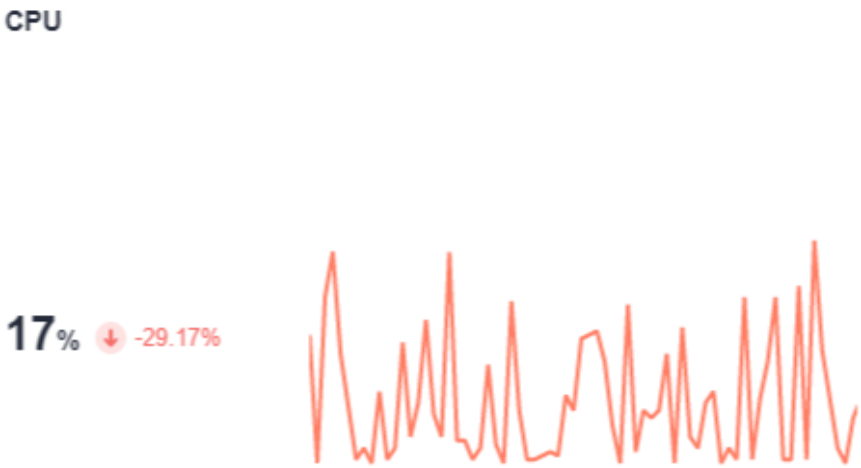


Table 3-15 Digital line graph parameters

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

  
  lts

__time	index_traffic	storage	write_traffic
2023-05-24T12:25:27.168Z	44467383	2527038132	8893476
2023-05-24T11:24:47.157Z	44358652	2489844672	8871730
2023-05-24T10:25:09.668Z	44330367	2452837903	8866073
2023-05-24T09:24:05.031Z	44296782	2415832130	8859356
2023-05-24T08:25:37.789Z	44324126	2378812284	8864825
2023-05-24T07:24:26.084Z	44619146	2341680807	8923829
2023-05-24T06:23:59.712Z	44218570	2304205483	8843714
2023-05-24T05:24:29.515Z	44394107	2267197473	8878821
2023-05-24T04:24:17.947Z	44220921	2230070342	8844184

  10 ▾ Per Page, Total 100 Records ‹ 1 2 3 ... 10 ›

  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

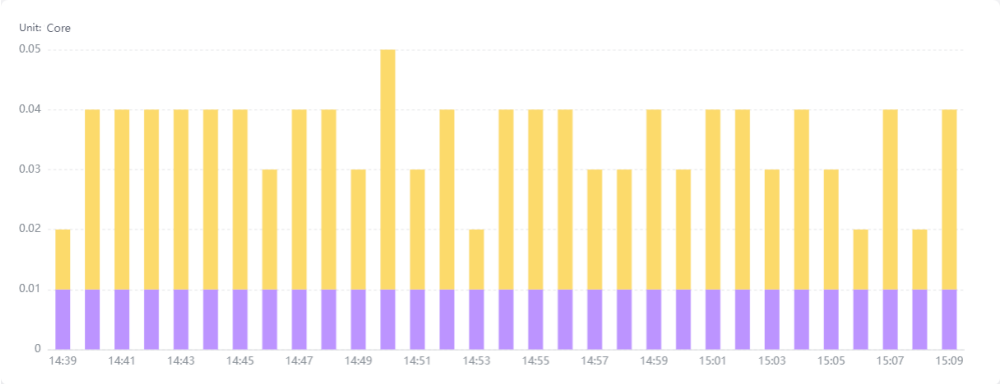


Table 3-17 Bar graph parameters

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.

Category	Parameter	Description
	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

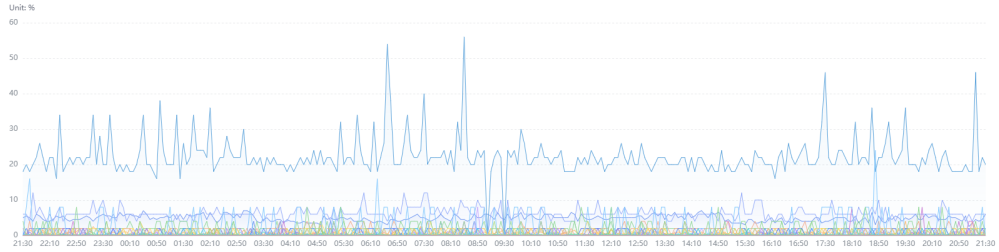
  

  Table 3-18 Line graph parameters

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.
	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.

Category	Parameter	Description
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.

- **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

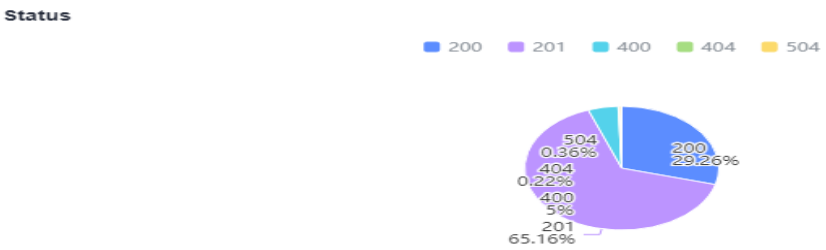
  

  Table 3-19 Pie graph parameters

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.

Category	Parameter	Description
	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.
	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

  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.

Category	Parameter	Description
	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.
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

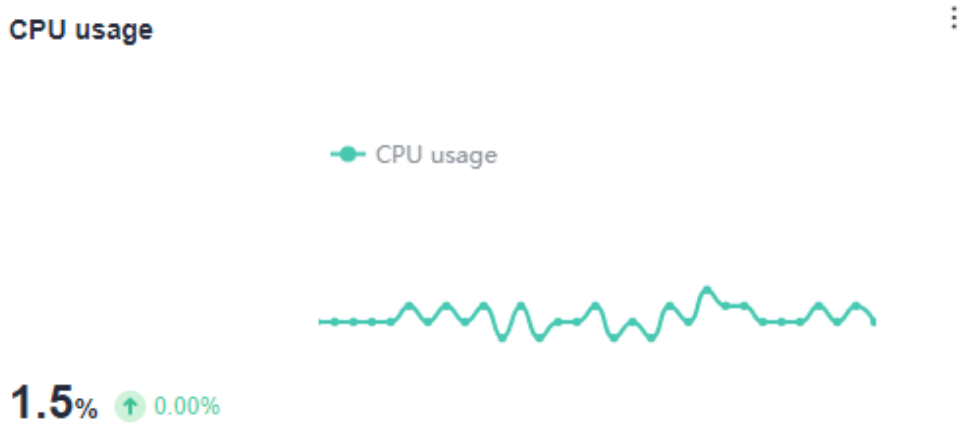


Table 3-21 Digital line graph parameters

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

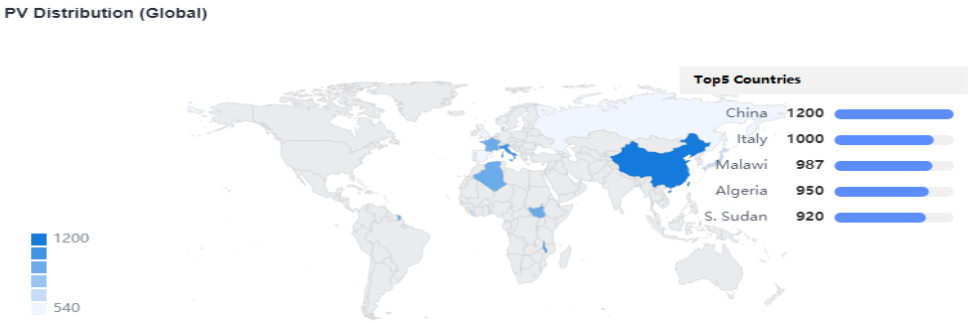


Table 3-22 Map graph parameters

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.

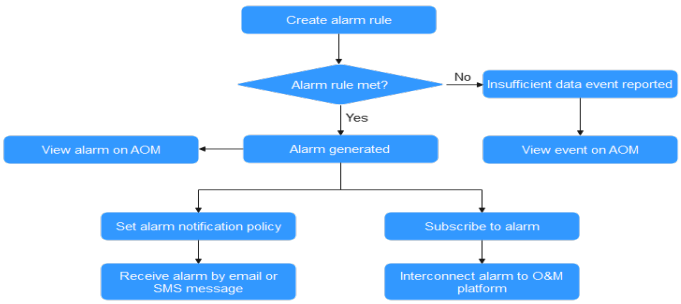
4 Alarm Management

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 **11.2.1.1 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 and log alarm rules monitor the usage of resources (such as hosts and components) in the environment in real time. 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 5.3**.
- 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

There are three configuration modes for you to create metric alarm rules: **Select from all metrics**, **PromQL**, and **Select by resource type**.

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**.

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. • 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

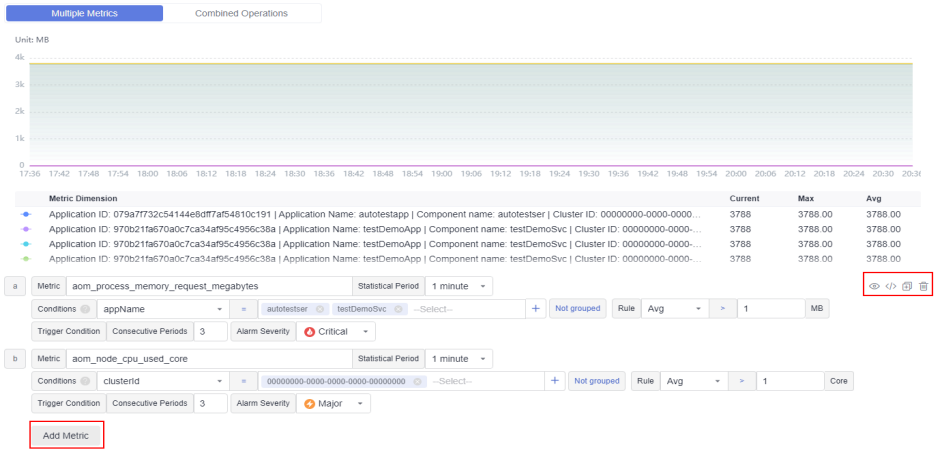


Table 4-2 Alarm rule details

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

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

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

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

Table 4-3 Advanced settings

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

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

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

Figure 4-3 Setting an alarm notification policy

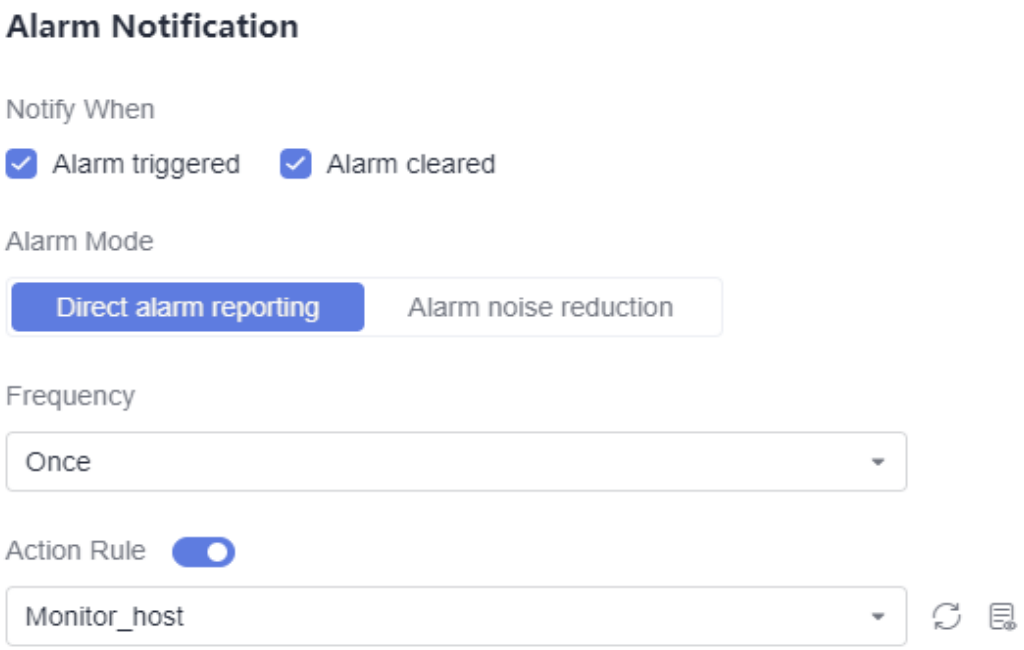


Table 4-4 Parameters for setting an alarm notification policy

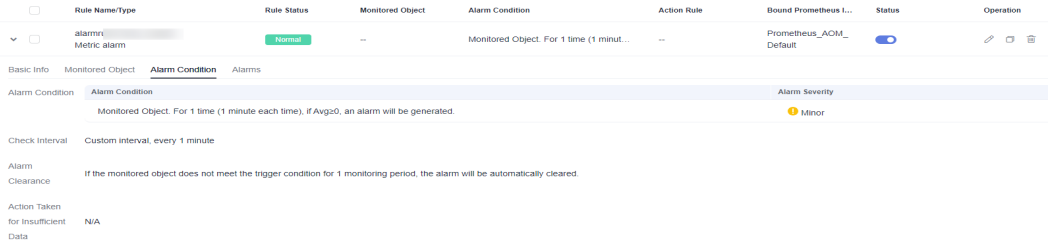
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system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

Parameter	Description
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: 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**.

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 Alarm Rule**.

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. • 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	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. – **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. You can click  to view examples. For details, see **14.2 Prometheus Statements**.
Alarm Severity	Severity of a metric alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.
Dimensions	Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.
Duration	A metric alarm will be triggered when the alarm condition is met for the specified duration. For example, if **Duration** is set to **2 minutes**, a metric alarm is triggered when the default rule condition is met for 2 minutes.

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	Interval at which metric query and analysis results are checked. • *XX* **hours**: Check the query and analysis results every XX hours. • *XX* **minutes**: Check the query and analysis results every XX minutes.

Parameter	Description
Alarm Tag	Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value". It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click + Tag. For details, see **14.1 Alarm Tags and Annotations**. **NOTE** If **tag policies** related to AOM have already been set, add alarm tags based on these policies. If a tag does not comply with the policies, tag addition may fail. Contact your organization administrator to learn more about tag policies.
Alarm Annotation	Click + Tag to add an alarm annotation. Alarm non-identification attribute. It is used in alarm notification and message template scenarios. It is in the format of "key:value". For details, see **14.1 Alarm Tags and Annotations**.

Step 7 Set an alarm notification policy. For details, see **Table 4-8**.

Figure 4-6 Setting an alarm notification policy

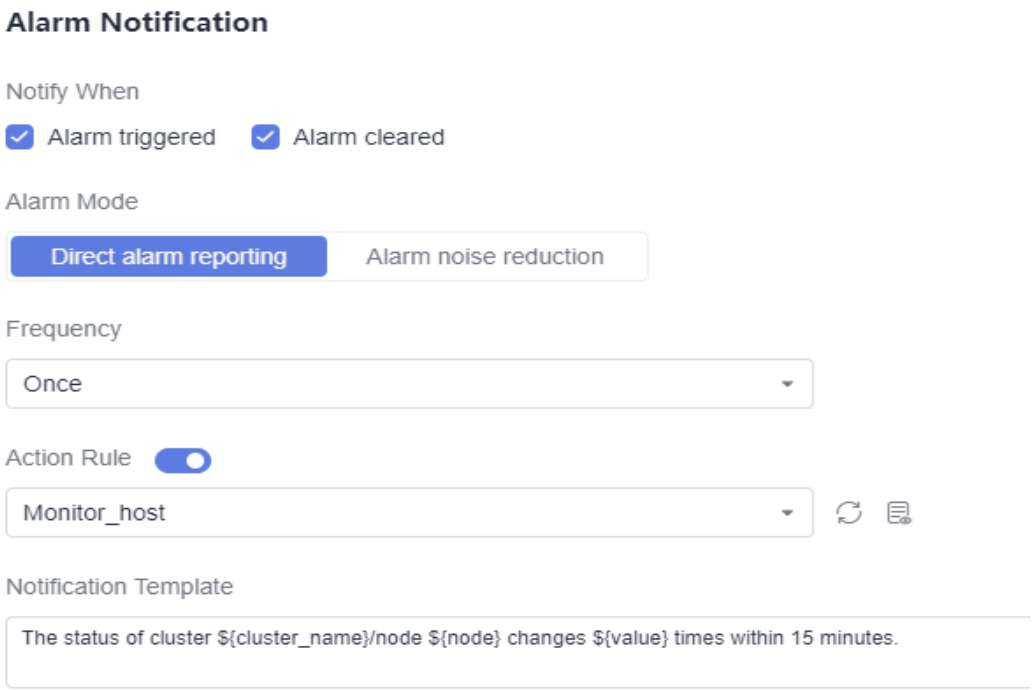


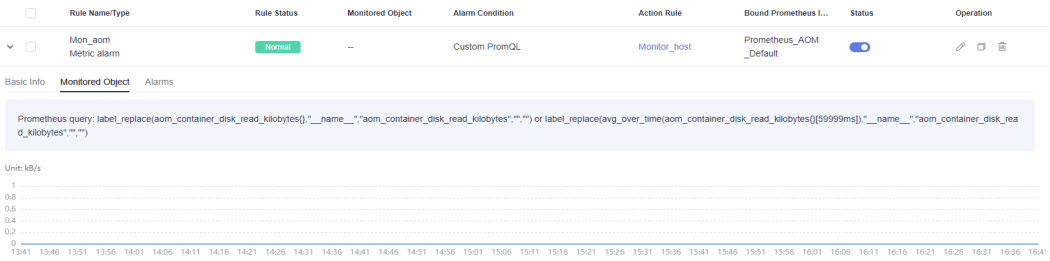
Table 4-8 Parameters for setting an alarm notification policy

Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: 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**.
Notification Template	Template for sending alarm notifications. It is automatically generated based on the Prometheus statement you set.

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

Creating Metric Alarm Rules by Resource Type (Offline Soon)

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 4-9**.

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. • 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 by resource type (Retiring)** and set **Resource Type** and **Monitored Object**. **Table 4-10** describes the parameters.

Table 4-10 Parameter description

Parameter	Description
Resource Type	Select a desired resource type from the drop-down list. – When you click the **Application Metrics** tab, you can select resources based on the following dimensions: ▪ **Host**: Select resources by host, including host, host disk, host network, host file system, and host GPU. ▪ **Application**: Select resources by application. ▪ **Component**: Select resources by component. ▪ **Process**: Select resources by process. – When you click the **Cloud Service Metrics** tab, you can select resources by cloud service. For example, if you select CCE from the cloud service list and then choose **Host** > **Host Disk**, the resource type will be **CCE/Host/Host Disk**, indicating that the disk of a CCE host is to be monitored.
Monitored Object	Click **Select Monitored Object**. All existing resources of the type you select will be displayed. Select target resources as required. If you enable **Apply to All** when selecting monitored objects, an alarm rule will be created for all resources of the type you select under an application or service. When this type of resource is added or modified, they will be automatically bound to the created alarm rule. When they are deleted, they will be automatically unbound from the alarm rule. For example, if **Resource Type** is set to **CCE/Host/Host Disk** and the **Apply to All** option is enabled when you select monitored objects, an alarm rule will be created for all CCE host disks. If a CCE host disk is added to the system, the new host disk will be automatically bound to the alarm rule.

3. Set alarm rule details. **Table 4-11** 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:

   – You can click **Add Metric** to add metrics and set the statistical period and detection rules for the metrics.

   – Click next to an alarm condition to hide the corresponding metric data record in the graph.

- Click next to an alarm condition to quickly copy the metric data and detection rule and modify them as required.
- Click next to an alarm condition to remove a metric data record from monitoring.

Figure 4-8 Setting alarm rule details

Table 4-11 Alarm rule details

Parameter	Description
Metric	Metric to be monitored. Click the **Metric** text box. In the resource tree on the right, you can also select a target metric by resource type.
Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.
Rule	Detection rule of a metric alarm, which consists of the statistical mode (**Avg**, **Min**, **Max**, **Sum**, and **Samples**), determination criterion (≥, ≤, >, and <), and threshold value. For example, if the detection rule is set to **Avg >10**, a metric alarm will be generated if the average metric value is greater than 10.
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. For example, if **Consecutive Periods** is set to **2**, a metric alarm will be triggered if the trigger condition is met for two consecutive periods.
Alarm Severity	Severity of a metric alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see **Table 4-12**.

Table 4-12 Advanced settings

Parameter	Description
Check Interval	Interval at which metric query and analysis results are checked. • **Hourly**: Query and analysis results are checked every hour. • **Daily**: Query and analysis results are checked at a fixed time every day. • **Weekly**: Query and analysis results are checked at a fixed time point on a specified day of a week. • **Custom interval**: The query and analysis results are checked at a fixed interval. • **Cron**: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: **0/5 * * * ***, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods.
Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five consecutive monitoring periods. The system supports the following actions: changing the status to **Exceeded** and sending an alarm, changing the status to **Insufficient data** and sending an event, maintaining **Previous status**, and changing the status to **Normal** and sending an alarm clearance notification.
Alarm Tag	Click + Tag to add an alarm tag. Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value". For details, see **14.1 Alarm Tags and Annotations**. **NOTE** If **tag policies** related to AOM have already been set, add alarm tags based on these policies. If a tag does not comply with the policies, tag addition may fail. Contact your organization administrator to learn more about tag policies.
Alarm Annotation	Click + Tag to add an alarm annotation. Alarm non-identification attribute. It is used in alarm notification and message template scenarios. It is in the format of "key:value". For details, see **14.1 Alarm Tags and Annotations**.

Step 7 Set an alarm notification policy. For details, see **Table 4-13**.

Figure 4-9 Setting an alarm notification policy

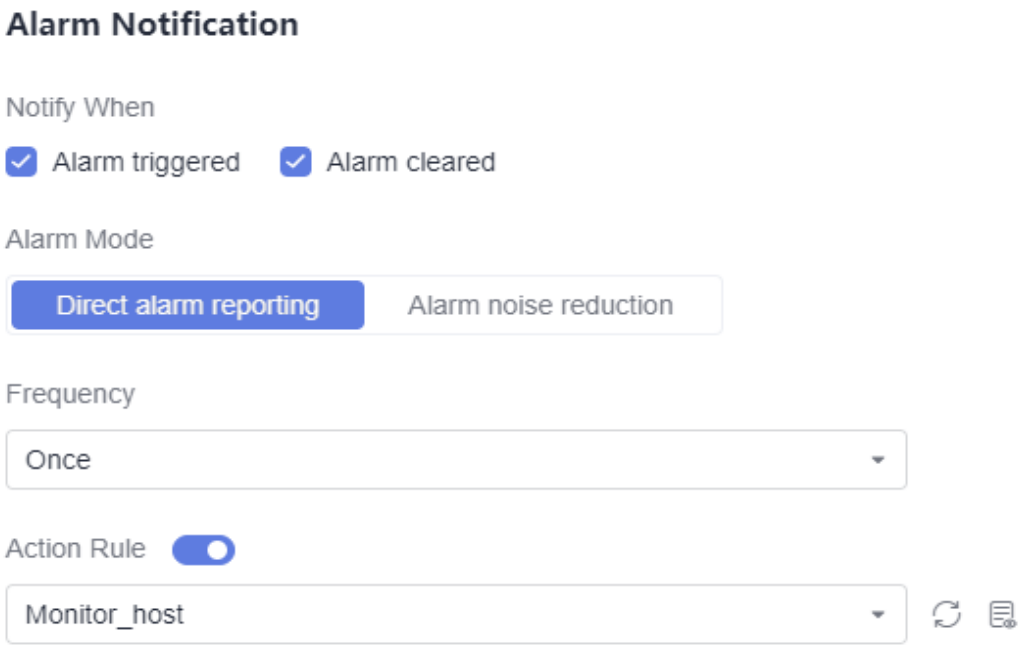


Table 4-13 Parameters for setting an alarm notification policy

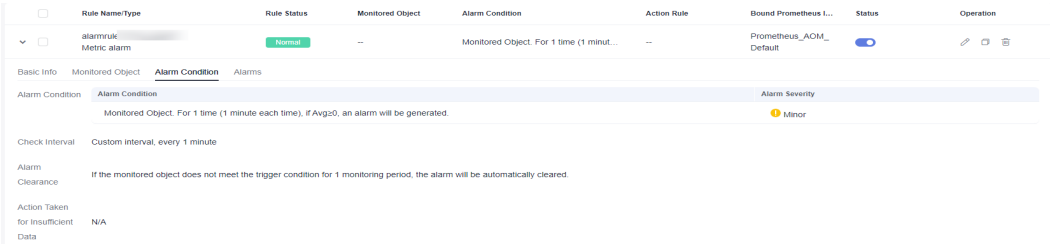
Parameter	Description
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system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

Parameter	Description
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: 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**.

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 host meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

Figure 4-10 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 Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to **Table 4-14**.

Table 4-14 Basic information

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

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **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 4-11 Setting alarm rule details

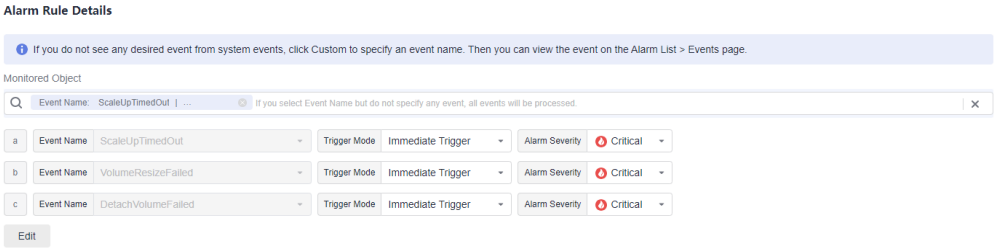


Table 4-15 Alarm rule parameters

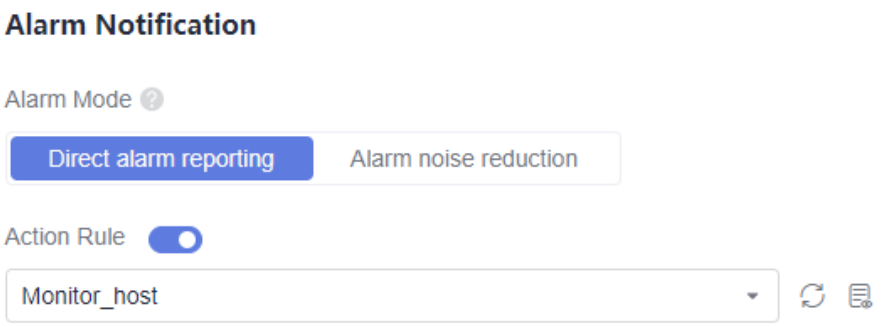
Parameter	Description
Monitored Object	Select criteria to filter service events. You can select **Notification Type**, **Event Name**, **Alarm Severity**, **Custom Attributes**, **Namespace**, or **Cluster Name** as the filter criterion. One or more criteria can be selected. **NOTE** Set **Event Name** as the filter criterion. If no event name is selected, all events are selected by default.
Alarm Condition	Condition for triggering event alarms. It contains: – **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. ▪ **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**: includes **Critical**, **Major**, **Minor**, and **Warning**. In case of multiple events, click **Batch Set** to set alarm conditions for these events in batches.

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**.

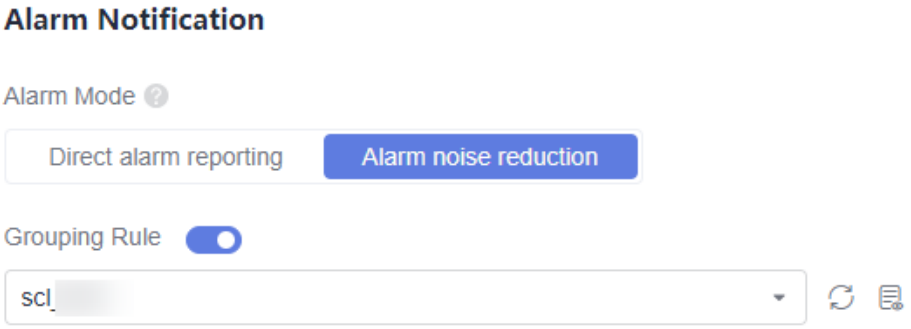
Figure 4-12 Selecting the direct alarm reporting mode



- **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**.

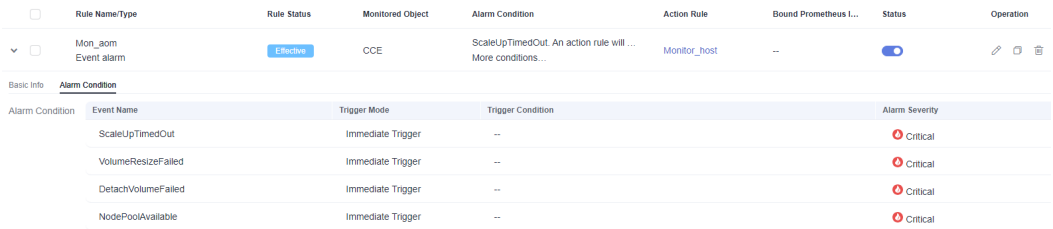
Figure 4-13 Selecting the alarm noise reduction mode



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 4-14 Created event alarm rule



----End

4.2.4 Creating a Log Alarm Rule

You can create alarm rules based on search analysis, or keyword or SQL 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**.
- You have created graphs for log streams. For details, see **Visualization**.

Precautions

- The function of creating alarm rules based on search analysis is under a closed beta test.
- The function of creating alarm rules by SQL is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, and AP-Bangkok. It is also available to whitelisted users in regions CN North-Beijing1, CN Southwest-Guiyang1, AP-Bangkok, AP-Jakarta, and CN South-Shenzhen.

Creation Mode

Create log alarm rules by referring to **Creating Log Alarm Rules Based on Search Analysis**, **Creating Log Alarm Rules by Keyword**, and **Creating Log Alarm Rules by SQL**.

Creating Log Alarm Rules Based on Search Analysis

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 4-16**.

Table 4-16 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.

Category	Parameter	Description
Statistical Analysis	Statistics	**Search Analysis**: applicable to the scenarios where alarm rules are configured based on a new SQL engine. The pipe character (|) can be used.
	Query conditions (Up to three query statements are supported.)	**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 an alarm rule based on search analysis.
		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. • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours.
		Query Statement: in the format of "Search statement | SQL analysis statement". AOM then monitors logs in the log stream based on the configured statements.

Category	Parameter	Description
	Check Rule	Enter a specific conditional expression. When the expression execution result is **true**, an alarm is generated. Basic syntax and syntax across multiple charts are supported. ● Basic syntax – Basic arithmetic operators: addition (+), subtraction (–), multiplication (*), division (/), and modulo (%). Example: **x * 10 + y > 100** – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). Example: **x >= 100**. – Logical operators: && (and) and || (or). Example: **x > 0 && y < 200** – Logical negation (!). Example: **!(x < 1 && x > 100)** – Numeric constants: processed as 64-bit floating point numbers. Example: **x > 10** – String constants. Example: **str =="string"** – Boolean constants: true and false. Example: **(x < 100)!=true** – Parentheses: used to change the order of operations. Example: **x *(y + 10) < 200** – Contains function: used to check whether a string contains a substring. For example, if you run **contains(str, "hello")** and **true** is returned, the string contains the **hello** substring. ● Syntax across multiple charts – Basic arithmetic operators: addition (+), subtraction (–), multiplication (*), division (/), and modulo (%). – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). – Logical operators: && (and) and || (or). – Logical negation (!) – Contains function – Parentheses

Category	Parameter	Description
		NOTE • Specify the number of queries and the number of times the condition (conditional expression) 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. • The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. • Number of queries: 1–10
Advanced Settings	Query Frequency	Options: • **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. **NOTE** When the query time range is larger than 1 hour, the interval must be at least 5 minutes. • **CRON**: Cron expressions use the 24-hour format and are precise down to the minute. Examples: – **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.

Category	Parameter	Description
	Restores	Configure a policy for sending an alarm clearance notification. 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. Number of last queries: 1–10
	Notify When	• **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	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. **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.
	Alarm Action Rules	Select a desired rule from the drop-down list. If no rule is available, click **Create Alarm Action Rule** on the right. For details, see **4.6.2 Creating an Alarm Action Rule**.
	Language	Specify the language (**English**) in which alarms are sent.

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

----End

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 4-17**.

Table 4-17 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.
		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. • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours.
		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.

Category	Parameter	Description
	Check Rule	Configure a condition that will trigger the alarm. **Matching Log Events**: When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered. Four comparison operators are supported: greater than (**>**), greater than or equal to (**>=**), less than (**<**), and less than or equal to (**<=**). 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. **NOTE** • The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. • Number of queries: 1–10

Category	Parameter	Description
Advanced Settings	Query Frequency	Options: • **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. **NOTE** When the query time range is larger than 1 hour, the interval must be at least 5 minutes. • **CRON**: Cron expressions use the 24-hour format and are precise down to the minute. Examples: – **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	Configure a policy for sending an alarm clearance notification. 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. Number of last queries: 1–10

Category	Parameter	Description
	Notify When	• **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	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. **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.
	Alarm Action Rules	Select a desired rule from the drop-down list. If no rule is available, click **Create Alarm Action Rule** on the right. For details, see **4.6.2 Creating an Alarm Action Rule**.
	Languages	Specify the language (**English**) in which alarms are sent.

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

----End

Creating Log Alarm Rules by SQL

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 4-18**.

Table 4-18 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 SQL**: applicable to the scenarios where alarm rules are configured based on the old SQL engine.

Category	Parameter	Description
	Charts	You can add a chart in two ways. • **Configure from Scratch**: Click **Configure from Scratch** and then select a log group and stream. Set parameters as follows: **Log Group Name**: (Required) Select a log group. **Log Stream Name**: (Required) Select a log stream. **NOTE** If no structuring rule has been configured, **configure structuring** first. **Query Time Range**: (Optional) the period specified for querying logs. It can be 1 to 60 minutes or 1 to 24 hours. **Query Statement**: Required. • **Import Configuration**: Click + Import Configuration. On the displayed **Custom** page, select a log group and stream, select a chart, and click **OK**. If there are no charts available or the charts do not fit your needs, click **Create Chart**. Configure the chart parameters, click **OK**, and click **Save and Back** in the upper right corner to return to the **Create Alarm Rule** page. You can see that the chart you just created has been selected, and the query statement has been filled in. Specify the query time range (1 to 60 minutes or 1 to 24 hours). When the query frequency is set to every 1 to 4 minutes, the query time range cannot exceed one hour. You can add more charts by clicking + Import Configuration. **NOTE** – Click to go to the visualization page of the log stream. – Click to delete an added chart. – Click **Preview** to view the data after visualized analysis. You must click **Preview**; otherwise, the alarm rule cannot be saved. – Up to three charts can be added. – The chart and the query statement cannot be left blank.

Category	Parameter	Description
	Check Rule	Enter a specific conditional expression. When the expression execution result is **true**, an alarm is generated. Basic syntax and syntax across multiple charts are supported. ● Basic syntax – Basic arithmetic operators: addition (+), subtraction (–), multiplication (*), division (/), and modulo (%). Example: **x * 10 + y > 100** – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). Example: **x >= 100**. – Logical operators: && (and) and || (or). Example: **x > 0 && y < 200** – Logical negation (!). Example: **!(x < 1 && x > 100)** – Numeric constants: processed as 64-bit floating point numbers. Example: **x > 10** – String constants. Example: **str =="string"** – Boolean constants: **true** and **false**. Example: **(x < 100)!=true** – Parentheses: used to change the order of operations. Example: **x *(y + 10) < 200** – Contains function: used to check whether a string contains a substring. For example, if you run **contains(str, "hello")** and **true** is returned, the string contains the **hello** substring. ● Syntax across multiple charts – Basic arithmetic operators: addition (+), subtraction (–), multiplication (*), division (/), and modulo (%). – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). – Logical operators: && (and) and || (or). – Logical negation (!) – Contains function – Parentheses

Category	Parameter	Description
		NOTE • Specify the number of queries and the number of times the condition (conditional expression) 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. • The alarm severity can be **Critical** (default), **Major**, **Minor**, or **Info**. • Number of queries: 1–10
Advanced Settings	Query Frequency	Options: • **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. **NOTE** When the query time range is larger than 1 hour, the interval must be at least 5 minutes. • **CRON**: Cron expressions use the 24-hour format and are precise down to the minute. Examples: – **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.

Category	Parameter	Description
	Restores	Configure a policy for sending an alarm clearance notification. 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. Number of last queries: 1–10
	Notify When	• **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	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. **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.
	Alarm Action Rules	Select a desired rule from the drop-down list. If no rule is available, click **Create Alarm Action Rule** on the right. For details, see **4.6.2 Creating an Alarm Action Rule**.
	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 4-19**.

Figure 4-15 Viewing alarm rules

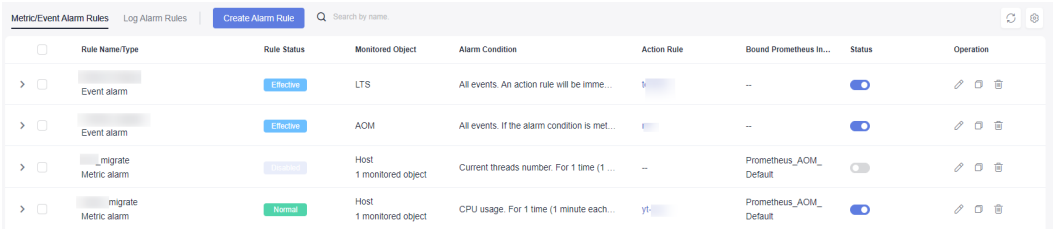


Table 4-19 Operations related to alarm rules

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	• 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	• 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)**.

Operation	Description
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.
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 Viewing 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 4-20** if needed.

Figure 4-16 Viewing alarm rules

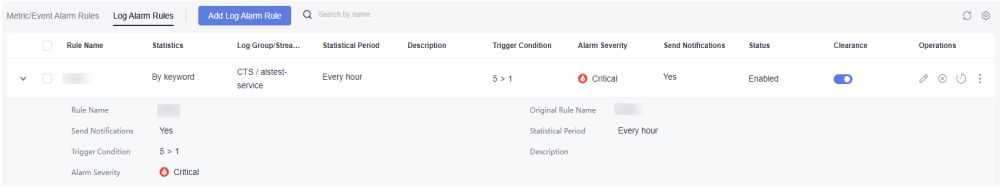


Table 4-20 Operations related to log alarm rules

Operation	Description
Searching for alarm rules	Enter an alarm rule name to search.

Operation	Description
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 **4.2.4 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	• 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	• 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	• 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	• 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	• 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**.

Operation	Description
Viewing detailed alarm information	Click > next to a rule name to view details.
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 Viewing 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 4-21** describes the parameters.

Table 4-21 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.
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Description	Description of the 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 4-22**.

Figure 4-17 Adding an alarm rule for the cloud service

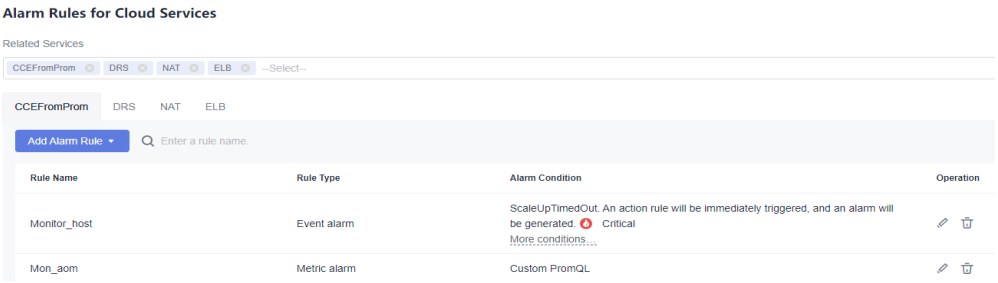


Table 4-22 Parameters for adding an alarm rule for the cloud service

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	1. Click **Add Threshold Alarm Rule**. 2. In the displayed dialog box, set the rule name, metric data, and alarm condition. For details, see **Step 5.3** and **Step 6** in **Creating Metric Alarm Rules by Resource Type (Offline Soon)**. 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 4-23**.
   - 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 4-18 Adding an event alarm rule

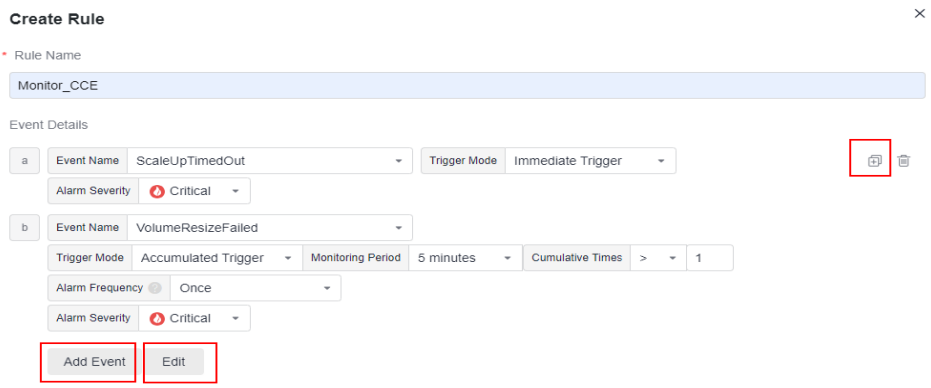


Table 4-23 Event rule parameters

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. – **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. Options: **Critical**, **Major**, **Minor**, and **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 4-24**.

Figure 4-19 Adding a PromQL alarm rule

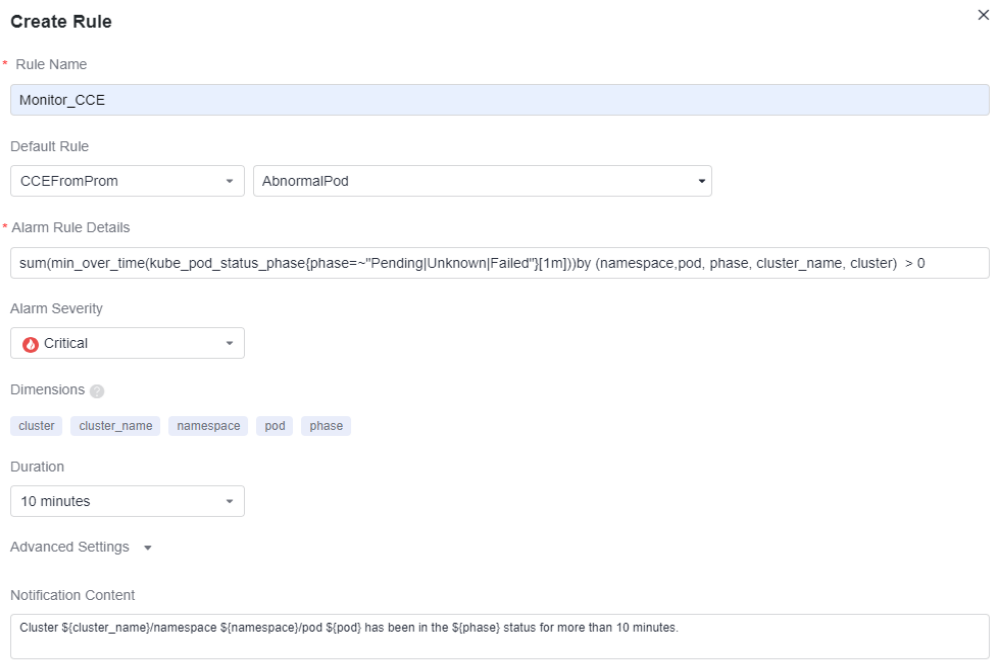


Table 4-24 PromQL alarm rule parameters

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		Detection rule generated based on Prometheus statements. The system provides two input modes: **Custom** and **CCEFromProm**. – **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. For details, see **14.2 Prometheus Statements**.
Alarm Severity		Severity of a metric alarm. Options: **Critical**, **Major**, **Minor**, and **Warning**.
Dimensions		Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.
Duration		A metric alarm will be triggered when the alarm condition is met for the specified duration. For example, if **Duration** is set to **2 minutes**, a metric alarm is triggered when the default rule condition is met for 2 minutes.
Advanced Settings	Check Interval	Interval at which metric query and analysis results are checked. – *XX* **hours**: Check the query and analysis results every *XX* hours. – *XX* **minutes**: Check the query and analysis results every *XX* minutes.
	Alarm Tag	Alarm identification attribute. It is used in alarm noise reduction scenarios. It is in the format of "key:value". It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click + Tag. For details, see **14.1 Alarm Tags and Annotations**. **NOTE** If **tag policies** related to AOM have already been set, add alarm tags based on these policies. If a tag does not comply with the policies, tag addition may fail. Contact your organization administrator to learn more about tag policies.
	Alarm Annotation	Click + Tag to add an alarm annotation. Alarm non-identification attribute. It is used in alarm notification and message template scenarios. It is in the format of "key:value". For details, see **14.1 Alarm Tags and Annotations**.

Parameter	Description
Notification Content	Alarm notification content. It is automatically generated based on the Prometheus statement you set.

3. Click **OK**.

Step 8 Click **OK** to create the alarm template.

Step 9 (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 4-25**. After the setting is complete, click **OK**.

Figure 4-20 Binding an alarm template with a Prometheus instance or cluster

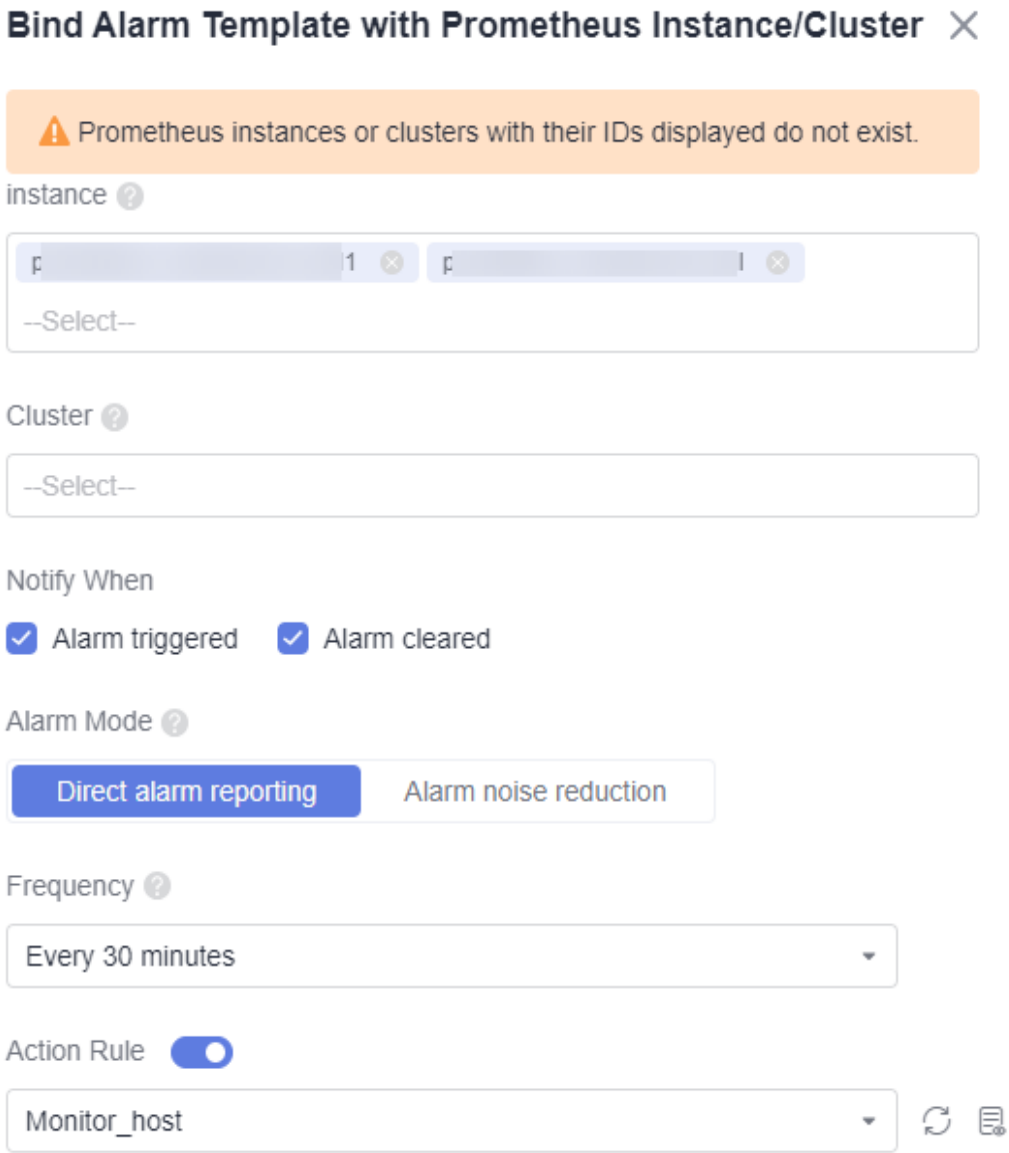


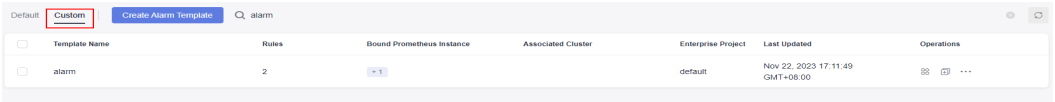
Table 4-25 Parameters for binding an alarm template

Parameter	Description
Instance	This parameter is optional. If the cloud services selected in **Step 5.1** contain services other than CCEFromProm, this parameter will be displayed. The drop-down list displays all Prometheus instances for cloud services and for multi-account aggregation under your account. Select your desired instance.
Cluster	This parameter is optional. If the cloud services selected in **Step 5.1** contain CCEFromProm, this parameter will be displayed. The drop-down list displays all CCE clusters of your account. Select your desired cluster.
Notify When	Set the scenario for sending alarm notifications. • **Alarm triggered**: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • **Alarm cleared**: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.
Alarm Mode	• **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. **Frequency**: 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**.

Step 10 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 4-21 Creating an alarm template



----End

More Operations

After the alarm template is created, you can also perform the operations listed in **Table 4-26**.

Table 4-26 Related operations

Operation	Description
Viewing an alarm template	In the template list, you can view the rule set name, number of rules, bound cluster, and enterprise project.
Binding an alarm template with a Prometheus instance or cluster	Click in the **Operation** column. For details, see **Step 9**.
Modifying an alarm template	Choose > **Edit** in the **Operation** column. For details, see **Creating an Alarm Template**.
Copying an alarm template	Click in the **Operation** column.
Deleting an alarm template	• 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.
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.

Operation	Description
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 Viewing 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 Viewing 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 deletion: Delete 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 view the alarms generated in the period.

Step 4 Perform the operations listed in **Table 4-27** as required:

Table 4-27 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	• 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. **NOTE** You can clear alarms after the problems that cause them are resolved.
Viewing alarm details	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. On the **Alarm Info** tab page, click the alarm rule, log group, or log stream in blue to drill down to view 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 view the events generated in the period.

Step 4 Perform the operations listed in **Table 4-28** as required:

Table 4-28 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. You can create an alarm action rule to associate an SMN topic with a message template. You can also customize notification content based on a message template. After an alarm action rule is created, you can choose **Alarm Management** > **Alarm Noise Reduction** > **Grouping Rules**, create a grouping rule, and associate it with the 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 4-29**.

Figure 4-22 Creating an alarm action rule

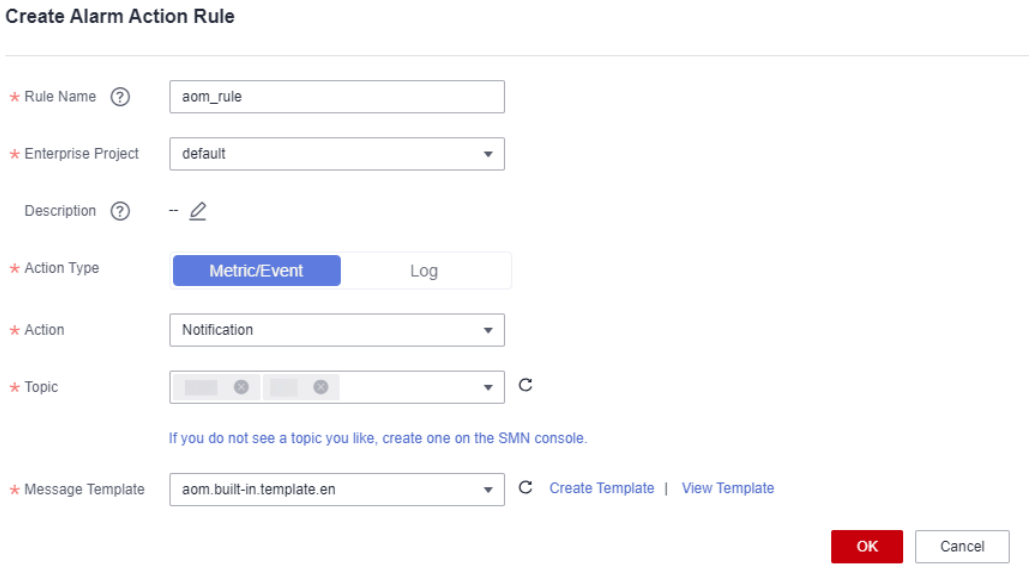


Table 4-29 Parameters of an alarm action rule

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. • 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.

Parameter	Description
Action Type	Type of the action. Select one from the drop-down list. • 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.
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 4-30**.

Table 4-30 Related operations

Operation	Description
Modifying an alarm action rule	Click **Modify** in the **Operation** column.
Deleting an alarm action rule	• 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. **NOTE** Before deleting an alarm action rule, you need to delete the alarm rule or grouping rule bound to the action rule.

Operation	Description
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, 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, HTTP, and HTTPS are supported.
- 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.

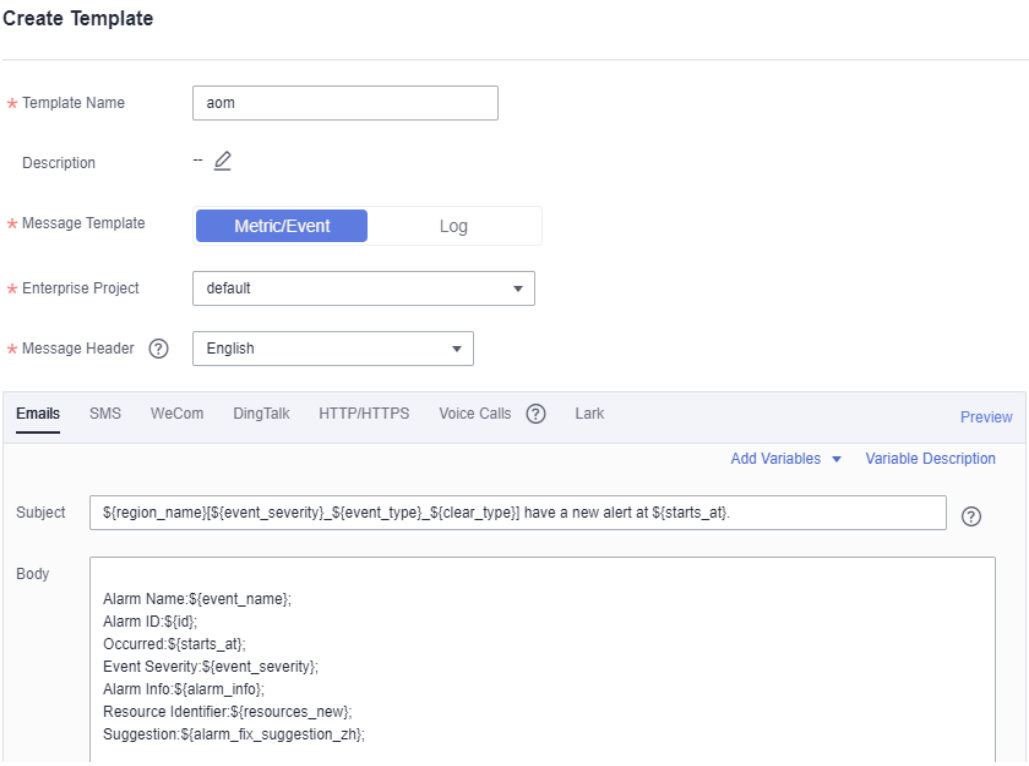
Creating a Message Template

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 4-23 Creating a message template



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

   Table 4-31 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. – 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 4-32**. For details about log templates, see **Table 4-33**.

   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 4-32 Variables in the default message template

Variable	Description	Definition
Alarm Name	Name of the alarm rule that is triggered.	${event_name}
Alarm ID	ID of the alarm rule that is triggered.	${id}
Action Rule	Name of the alarm action rule that triggers notification.	${action_rule}
Occurred	Time when the alarm or event is triggered.	${starts_at}
Event Severity	Alarm or event severity. Options: **Critical**, **Major**, **Minor**, and **Warning**.	${event_severity}
Alarm Info	Detailed alarm information.	${alarm_info}
Resource Identifier	Resource for which the alarm or event is triggered.	${resources}
Custom tag	Extended tag.	$event.metadata.key1
Suggestion	Suggestion about handing the alarm. For non-custom reporting, "NA" is displayed.	${alarm_fix_suggestion_zh}
Custom annotation	Extended annotation.	$event.annotations.key2

Table 4-33 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.	**Add variables:** – Original rule name: *${event_name}* – Alarm severity: *${event_severity}* – Occurrence time: *${starts_at}* – Occurrence region: *${region_name}* – Huawei Cloud account: *${domain_name}* – Alarm source: *$event.metadata.resource_provider* – Resource type: *$event.metadata.resource_type* – Resource ID: *${resources}* – Alarm status: *$event.annotations.alarm_status* – Expression: *$event.annotations.condition_expression* – Current value: *$event.annotations.current_value* – Statistical period: *$event.annotations.frequency* – Rule name: *$event.annotations.alarm_rule_alias* – Keyword variables 1. Query time: *$event.annotations.results[0].time* 2. Query logs: *$event.annotations.results[0].raw_results* 3. Query URL: *$event.annotations.results[0].url*	${event_name} ${event_severity} ${starts_at} ${region_name}

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

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

----End

More Operations

After creating a message template, you can perform the operations listed in **Table 4-34**.

Table 4-34 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	• 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. **NOTE** Before deleting a message template, delete the alarm action rules bound to it.
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

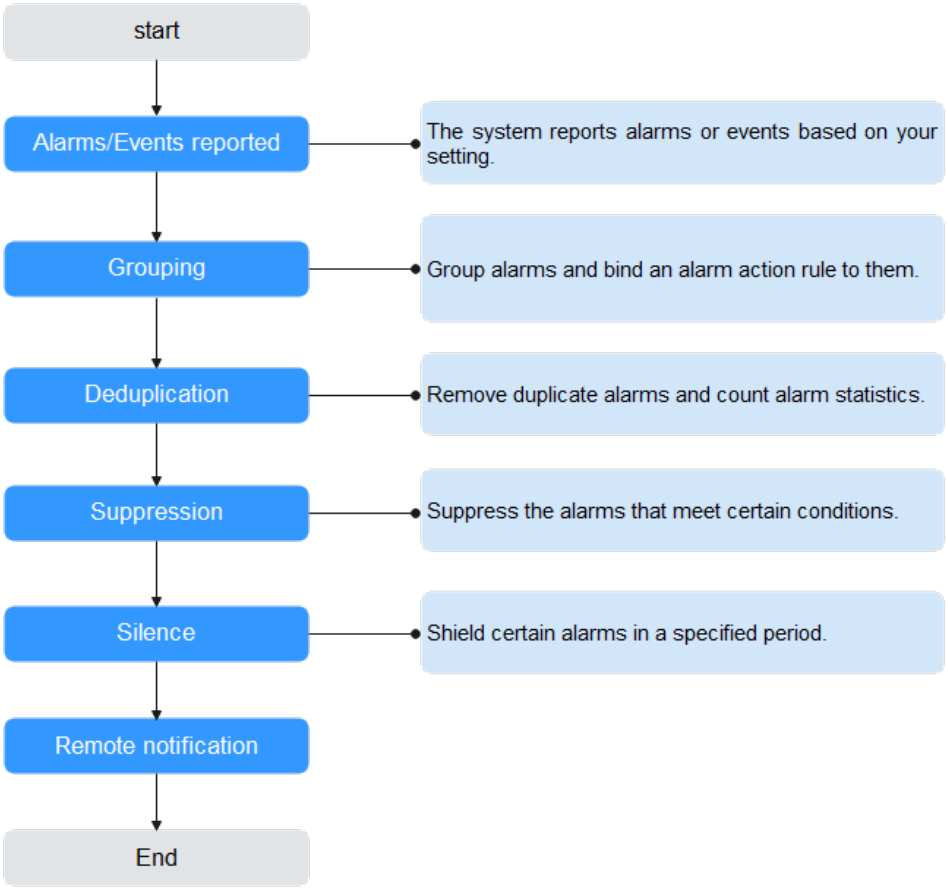
AOM supports alarm noise reduction. Alarms can be processed based on the alarm noise reduction rules to prevent notification storms.

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 4-24 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.

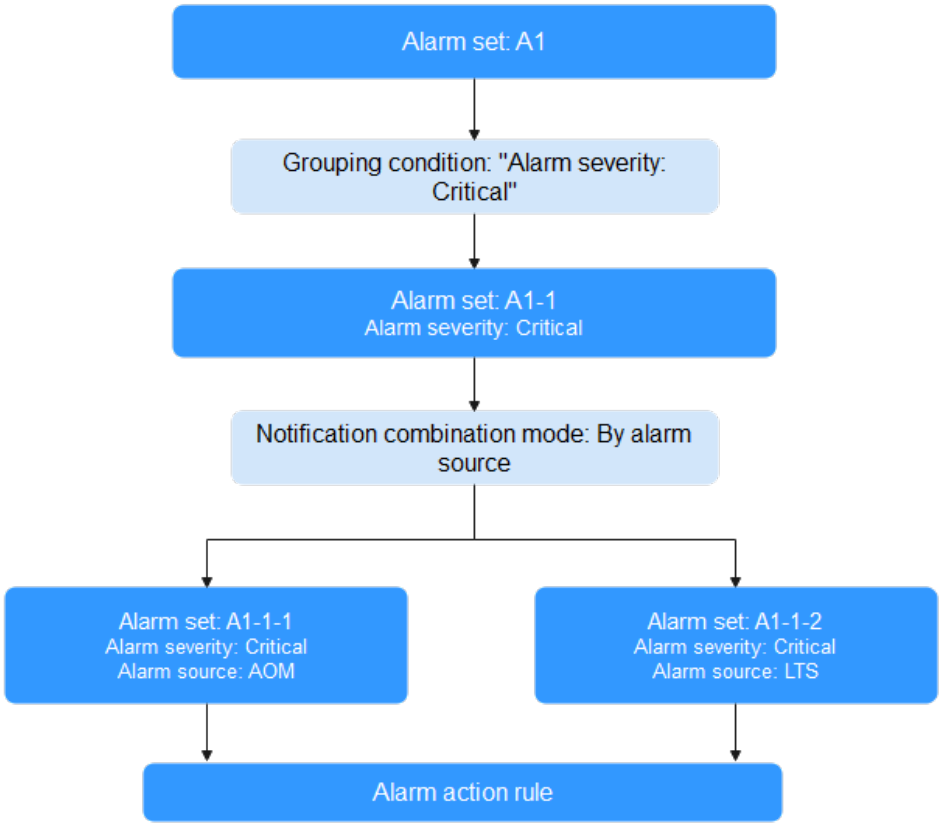
```
{
   "starts_at" : 1579420868000,
   "ends_at" : 1579420868000,
   "timeout" : 60000,
   "resource_group_id" : "5680587ab6*******755c543c1f",
   "metadata" : {
     "event_name" : "test",
     "event_severity" : "Major",
     "event_type" : "alarm",
     "resource_provider" : "ecs",
     "resource_type" : "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 4-25**, 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 4-25 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 4-35**.

Figure 4-26 Creating a grouping rule

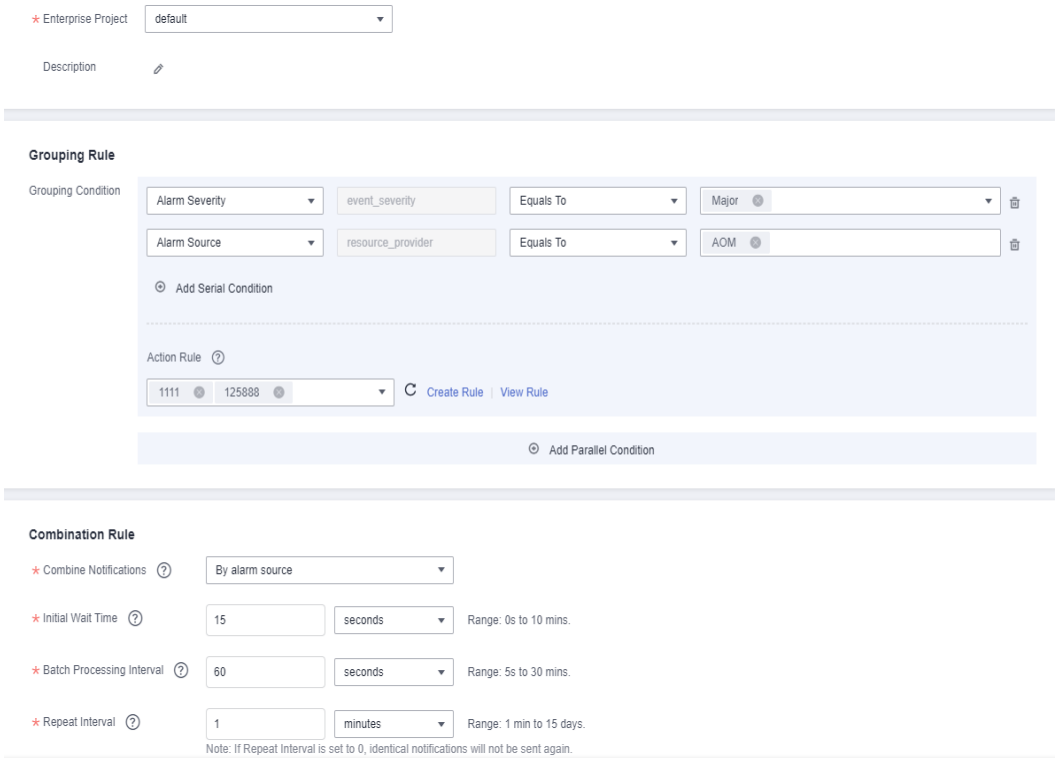


Table 4-35 Grouping rule parameters

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. • 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	Conditions set to filter alarms. After alarms are filtered out, you can set alarm action rules for them. Value range and description: • **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** • *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. Rule description: • 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. 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.

Category	Parameter	Description
Combination Rule	Combine Notifications	Combines grouped alarms based on specified fields. Alarms in the same group are aggregated for sending one notification. Notifications can be combined: • **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	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. Value range: 0s to 10 minutes. Recommended: 15s.
	Batch Processing Interval	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. The change here refers to a new alarm or an alarm status change. Value range: 5s to 30 minutes. Recommended: 60s.
	Repeat Interval	Waiting time for sending an alarm notification after the combined alarm data becomes duplicate. It is recommended that the time be set to hours. Duplication means that no new alarm is generated and no alarm status is changed while other attributes (such as titles and content) are changed. Value range: 0 minutes to 15 days. Recommended: 1 hour.

Step 4 Click **Confirm**.

----End

More Operations

After creating a grouping rule, perform the operations listed in **Table 4-36** if needed.

Table 4-36 Related operations

Operation	Description
Modifying a grouping rule	Click **Modify** in the **Operation** column.
Deleting a grouping rule	• 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 4-27 Creating a suppression rule

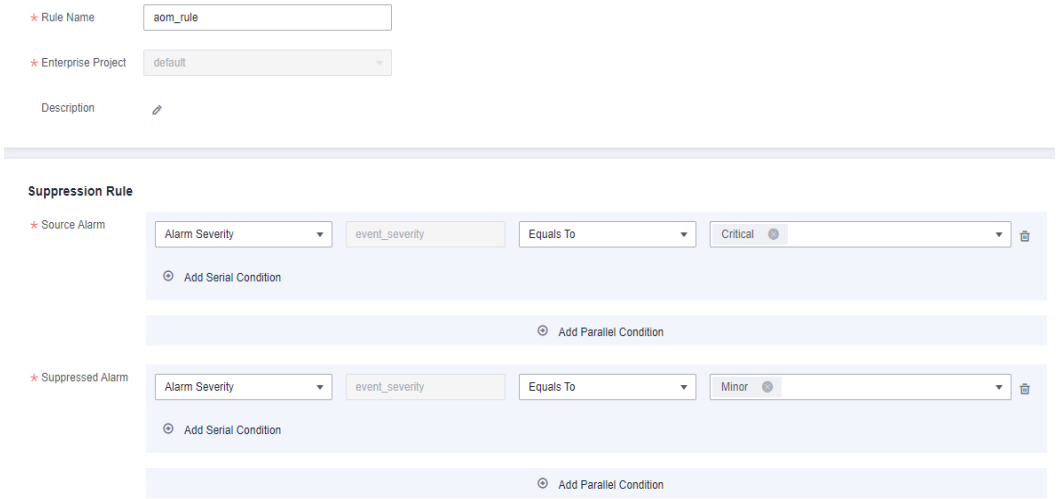


Table 4-37 Setting a suppression rule

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. • 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	Alarm that triggers suppression. Value range and description: • **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** • *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. Rule description: 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. Example: For a serial condition, if **Alarm Severity** is set to **Critical**, critical alarms are filtered out as the root alarms.
	Suppressed Alarm	Alarm that is suppressed by the root alarm. Set parameters for the suppressed alarm in the same way that you set parameters for the source alarm. 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.

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 4-38** if needed.

Table 4-38 Related operations

Operation	Description
Modifying a suppression rule	Click **Modify** in the **Operation** column.
Deleting a suppression rule	• 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 4-28 Creating a silence rule

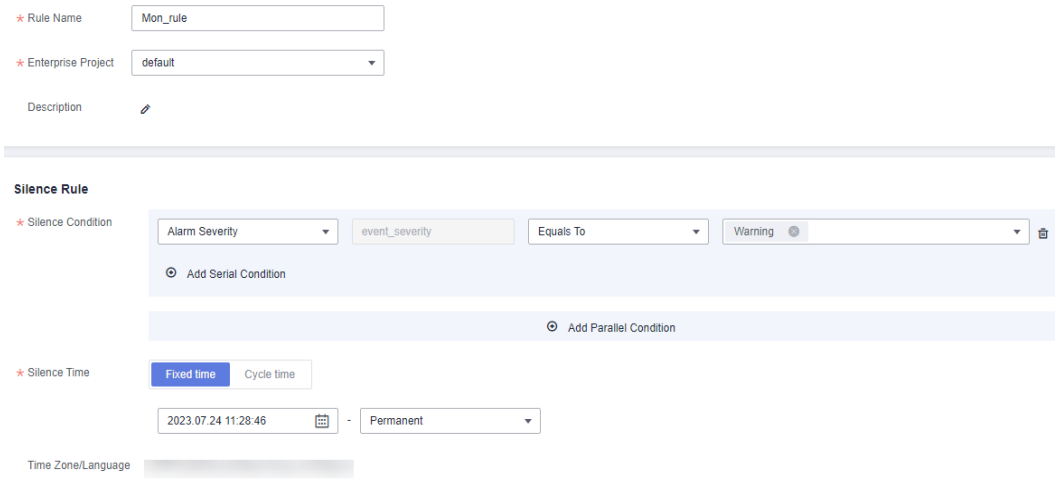


Table 4-39 Setting a silence rule

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. • 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	Any alarm notifications that meet the silence condition will be shielded. Value range and description: • **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** • *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. Rule description: 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. Example: If **Alarm Severity** is set to **Warning** in a serial condition, warnings will be shielded.
	Silence Time	Time when alarm notifications are shielded. There are two options: • **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 4-40**.

Table 4-40 Related operations

Operation	Description
Modifying a silence rule	Click **Modify** in the **Operation** column.
Deleting a silence rule	• 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.

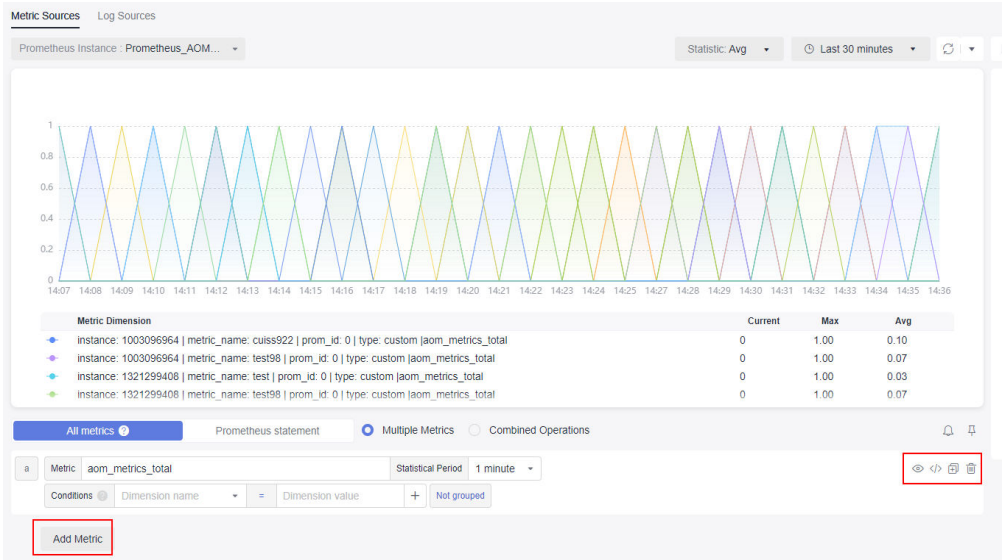
Step 2 In the navigation pane, choose **Metric Browsing**.

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. For example, different RDS DB instances have the CPU usage

metric. You need to view the CPU usage metric of a specified RDS DB instance type. The following shows the procedure:

In the **Metric** text box, select the CPU usage metric of the corresponding RDS DB instance. In the **Conditions** area, set the dimension name to **RDS for MySQL** or **RDS for PostgreSQL** and select the corresponding dimension value. The CPU usage metric of the specified RDS DB instance type will be displayed.

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 **14.2 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.

Parameter	Description
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.

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 icon 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 earliest log is displayed at the top). 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	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:14:09.089 (5397)[W] ntp_linux.go:36 update ntpStatus: &{status:1 serverStatus:1 offset:}'												
3	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:14:09.089 (5397)[W] ntp_linux.go:107 NTPConfig has no set the main NTP_Server!'												
4	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[evs-driver-fknb6] fail, podName2podInfoM: map[]'												
5	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[obs-driver-lfhjg] fail, podName2podInfoM: map[]'												
6	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[sfs-driver-f85hn] fail, podName2podInfoM: map[]'												
7	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[storage-driver-z5rv2] fail, podName2podInfoM: map[]'												
8	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-hvk57] fail, podName2podInfoM: map[]'												
9	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-mp8cm] fail, podName2podInfoM: map[]'												
10	2018-12-1	Service	a12345asd	a12345asd	172.16.0.95	default	lycluster1211	/var/ICAg	2018-12-18 16:13:58.626 (5397)[W] container_watcher.go:359 get label by pod[atps-7cc556659b-qh47x] fail, podName2podInfoM: map[]'												

Figure 6-2 Exporting logs in TXT format

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

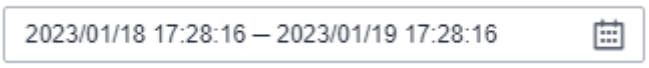
Step 1 Log in to the AOM 2.0 console.

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 6-4** 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.

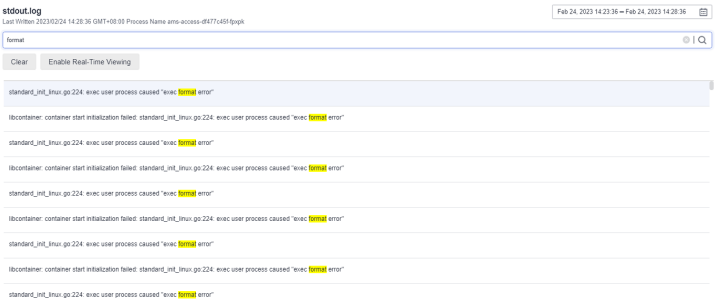
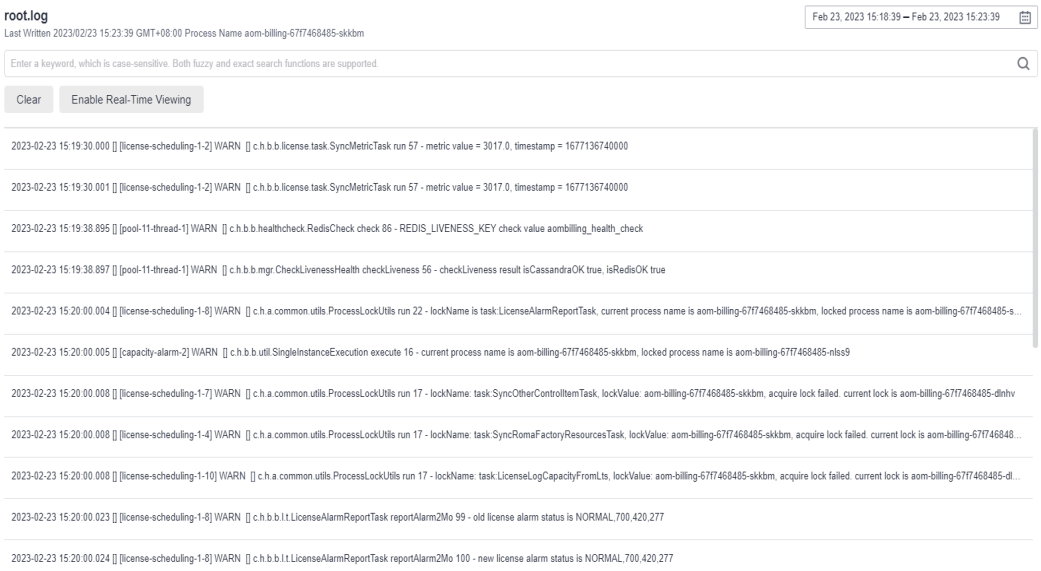
Operation	Settings	Description
	Viewing logs in real time	Real-time viewing is disabled by default. You can click **Enable Real-Time Viewing** as required. After this function is enabled, the latest written logs can be viewed. Logs can be searched only when real-time viewing is disabled. For real-time 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. Example: **Figure 6-3** Viewing logs in real time 

Figure 6-4 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.

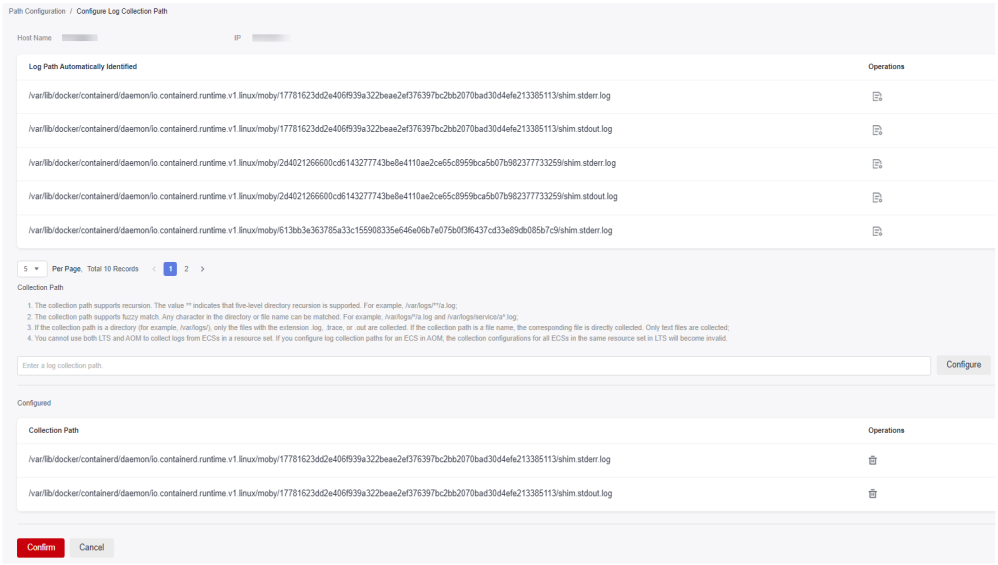
You can use the paths automatically identified by the ICAgent or manually configure paths.

- **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.

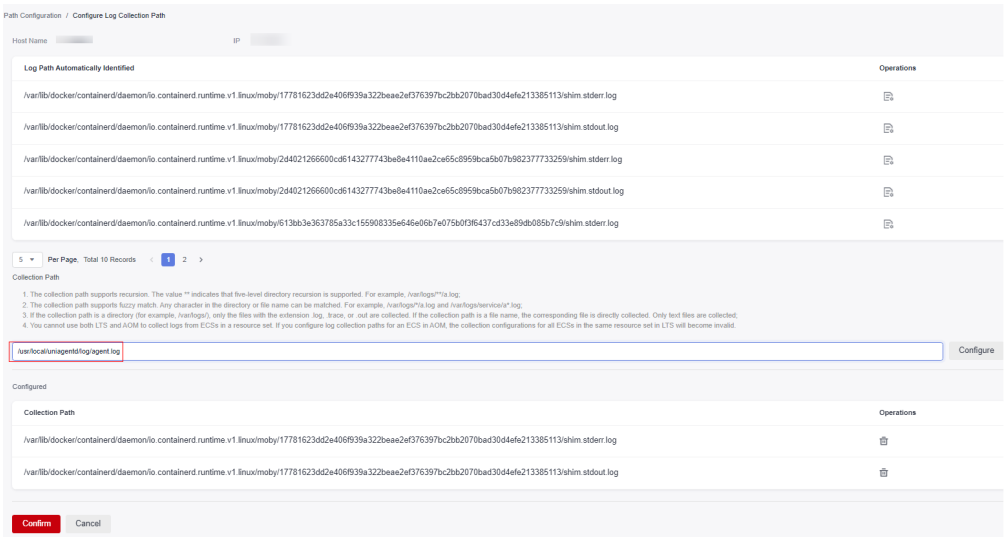
Figure 6-5 Using the paths automatically identified by the ICAgent



- **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.

Figure 6-6 Manually configuring log collection paths



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

Parameter	Description	Example
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.
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups.	log-group1
Dump Cycle	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. 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.	3 hours
Target OBS Bucket	OBS bucket for storing logs. **NOTE** You must create an OBS bucket first. Click **View OBS** to create a bucket on the OBS console.	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_erro.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
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** • 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.	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 LTS Access

6.5.1 Overview

NOTE

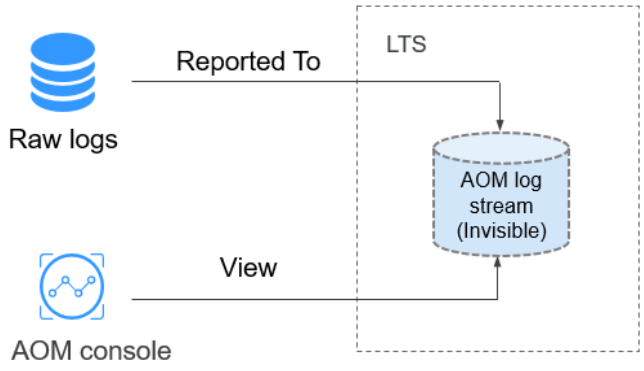
The function of connecting AOM logs to Log Tank Service (LTS) is not yet generally available. If you want to use this function, **submit a service ticket**.

LTS is a unified log management platform that allows you to search for, structure, and view logs. By adding access rules, you can map logs of CCE or custom clusters in AOM to LTS. Then you can view and analyze logs on LTS. Mapping does not generate extra fees, but duplicate mapping will.

What Is Mapping?

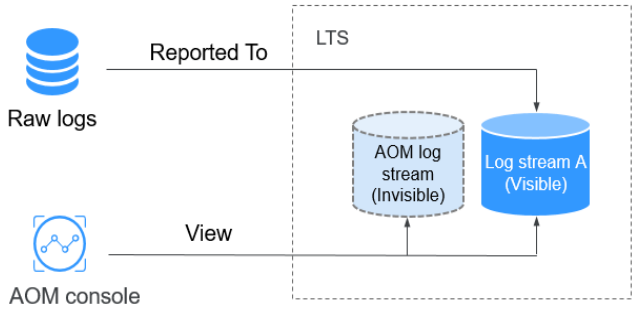
AOM logs exist in LTS in the form of a log stream, as shown in **Figure 6-7**. You can view raw logs in configured log collection paths on AOM, but cannot view the AOM log stream on LTS. You can create a mapping by adding an access rule on AOM. After the mapping is created, you can view and analyze AOM logs on LTS.

Figure 6-7 Before mapping



After you create log stream A and an access rule, the mapping from AOM to LTS is created. New AOM logs will be reported to log stream A. You can view all logs on AOM before and after the mapping. Historical logs in the AOM log stream will not be copied or migrated to log stream A, as shown in **Figure 6-8**.

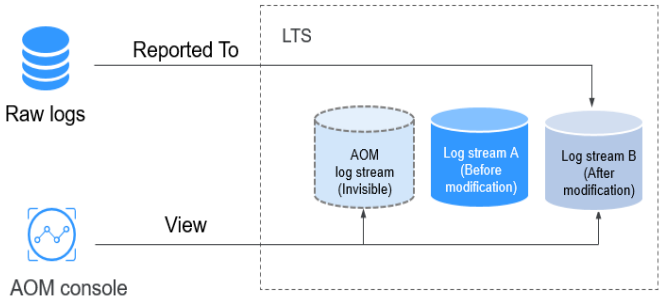
Figure 6-8 After mapping



Modifying a Mapping

If you modify a mapping, for example, change log stream A to log stream B, new logs will be reported to log stream B. You can view the content of AOM log stream and log stream B on AOM, but cannot view the content of log stream A, as shown in **Figure 6-9**.

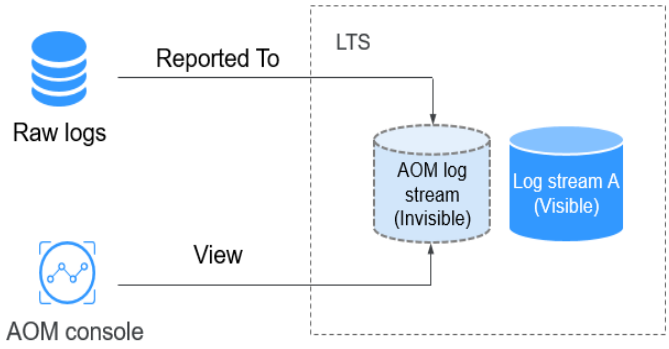
Figure 6-9 Modifying a mapping



Deleting a Mapping

When you delete an access rule or a mapped log stream, the corresponding mapping is deleted. New logs are reported only to the AOM log stream. In this case, you cannot view the content of log stream A, as shown in **Figure 6-10**. If the access rule is deleted but log stream A is not, you can still view the logs that have already been mapped on LTS.

Figure 6-10 Deleting a mapping



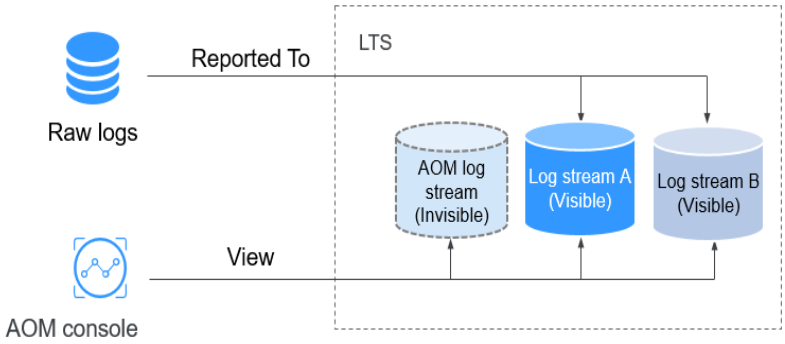
NOTE

Deleted access rules or mapped log streams cannot be recovered. Exercise caution when performing this operation.

Duplicate Mapping

If a workload or file is mapped to both log streams A and B, new logs will be reported to both of them. Duplicate logs exist on AOM and will be charged. Therefore, duplicate mapping is not recommended.

Figure 6-11 Duplicate mapping



6.5.2 Managing Access Rules

This section describes how to add, view, and delete access rules.

Prerequisites

- You have created a log group and log stream. For details, see **Creating Log Groups and Log Streams**. You can also directly create them on the **Add Access Rule** page.
- You have created a cluster, namespace, and workload. For details, see **Cloud Container Engine User Guide**.

Adding Access Rules

To map the logs of CCE or custom clusters in AOM to LTS, perform the following steps:

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click **Add Access Rule**.

Step 4 Select an access type. **Access by Namespace**, **Access by Workload**, or **Automatic Mapping** are available.

- **Access by Namespace**: All logs of the selected namespace are connected to the specified log stream.
  a. **Rule Name**: Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
  b. **Cluster**: Select a cluster from the drop-down list.
  c. **Namespace**: Select a namespace from the drop-down list.
  d. **Workload**: Retain the default value **All**.
  e. **Container Name**: Select a container from the drop-down list box.
  f. Set an access rule.
     - **Access all logs**: If you select this option, select a log group and log stream.
     - **Specify log paths**: If you select this option, specify a log path and then select a log group and log stream.

     NOTE

     If no log group or stream meets your requirements, click **Add Log Group** and **Add Log Stream** to add ones. After creating a log stream, select an enterprise project.
- **Access by Workload**: Logs of the selected workload are connected to the specified log stream.
  a. **Rule Name**: Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
  b. **Cluster**: Select a cluster from the drop-down list.
  c. **Namespace**: Select a namespace from the drop-down list.
  d. **Workload**: Select one or more workloads from the drop-down list.
  e. **Container Name**: Select a container from the drop-down list box.
  f. Set an access rule.
     - **Access all logs**: If you select this option, select a log group and log stream.
     - **Specify log paths**: If you select this option, specify a log path and then select a log group and log stream.

> NOTE
>
> If no log group or stream meets your requirements, click **Add Log Group** and **Add Log Stream** to add ones. After creating a log stream, select an enterprise project.

- **Automatic Mapping**: Workload logs are automatically connected to the generated log streams with the same names as the workloads.
  a. **Rule Name**: Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
  b. **Namespace**: Select a namespace from the drop-down list.
  c. **Workload**: Select one or more workloads from the drop-down list.
     If you select one workload, the rule name is changed to **Custom rule name_0** after the rule is created, for example, **test_0**. If you select multiple workloads, the rule names are changed to **Custom rule name_0**, **Custom rule name_1**, and so on, such as **test_0** and **test_1**.
  d. Set an access rule: Select a log group and an enterprise project, and specify a log stream prefix. A log stream will be generated based on the log stream prefix and workload name. By default, all logs of the selected workload are connected.

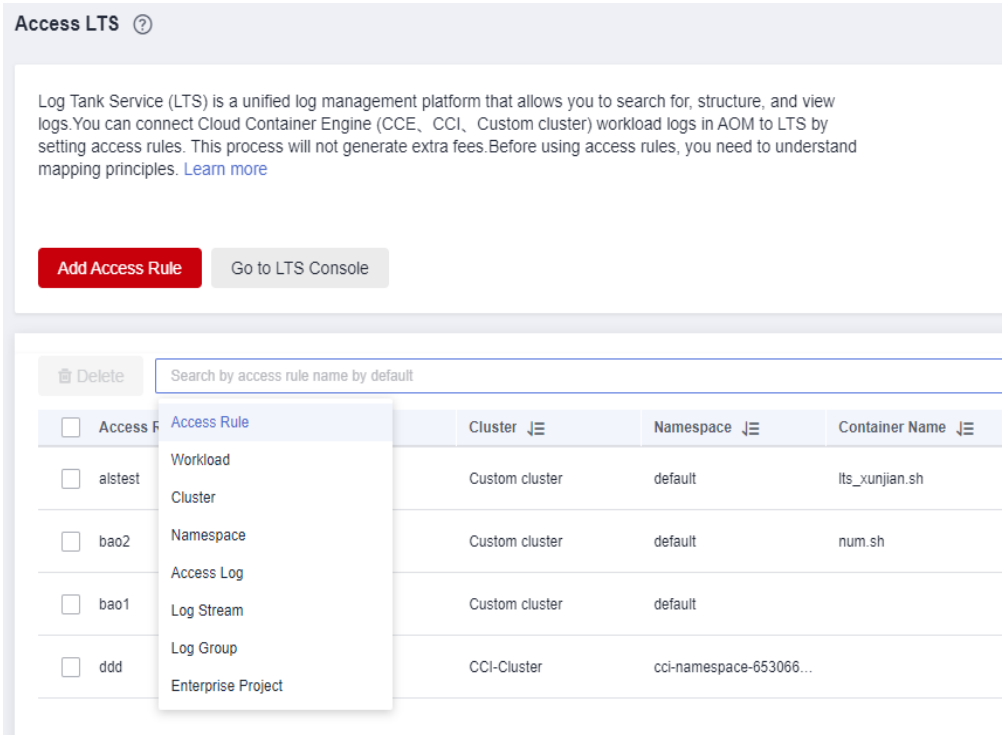
----End

Managing Access Rules

On the **LTS Access** page, you can search for, view, edit, and delete access rules.

- Search
  Click the search box, select a search dimension, for example, **Workload**, and then select options under this dimension. You can also directly enter a keyword in the search box. In this case, the system searches for information based on access rule names by default.

Figure 6-12 Selecting a filter criterion



- View

  In the rule list, view the cluster name and namespace of the created rule.

  Click  in the upper right corner of the search box to customize the display of columns. Click a log group name in the **Log Group** column to go to the log group details page on the LTS console.

- Edit

  On the **LTS Access** page, click **Edit** in the **Operation** column to edit an access rule. For details about the impact of modifying an access rule, see **Modifying a Mapping**.

- Delete

  On the **LTS Access** page, click **Delete** in the **Operation** column to delete an access rule. Select one or more access rules and click **Delete** above the rule list.

  NOTE

  Deleted access rules or mapped log streams cannot be recovered. Exercise caution when performing this operation. For details about the impact of deleting an access rule, see **Deleting a Mapping**.

6.6 Searching for and Viewing Logs

6.6.1 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 **13.5 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**.

----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.
- On the **Raw Logs** page, 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.
  - When the number of aggregation results exceeds 100,000, the aggregation results 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 icon 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.

Figure 6-13 Viewing logs in real time

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.

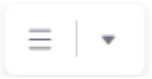
----End

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. • 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.

Operation	Description
Unfolding	Click  to unfold log content. They will be displayed in different lines. **NOTE** By default, log content is unfolded and two lines are displayed.
Downloading logs	Click . On the page that is displayed, download logs to the local host. **Direct Download**: Download log files to the local PC. Up to 5000 logs can be downloaded at a time. Select **.csv** or **.txt** from the drop-down list and click **Download** to export logs to the local PC. **NOTE** ● If you select **.csv**, logs are exported as a table. ● If you select **.txt**, logs are exported as a **.txt** file.
JSON	Move the cursor over , click **JSON**, and set JSON formatting. **NOTE** Formatting is enabled by default. The default number of expanded levels is 2. ● Formatting enabled: Set the default number of expanded levels. Maximum value: **10**. ● Formatting disabled: JSON logs will not be formatted for display.
Collapse configuration	Move the cursor over , click **Log Collapse**, and set the maximum characters to display in a log. If the number of characters in a log exceeds the maximum, the extra characters will be hidden. Click **Expand** to view all. **NOTE** Logs are collapsed by default, with a default character limit of 400.
Log time display	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. **NOTE** By default, the function of displaying milliseconds is enabled.

Syntax and Examples of Searching by Keyword

Search syntax:

Table 6-7 Search syntax

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

6.6.2 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.

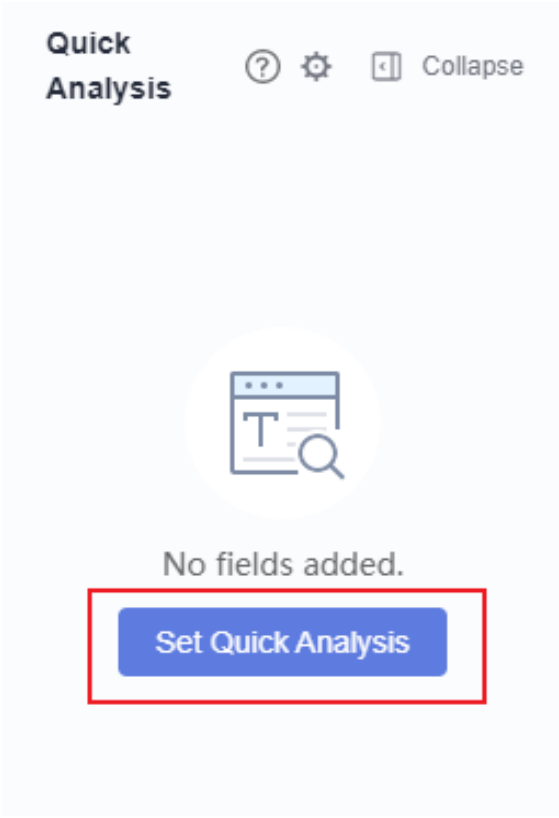
Creating a Quick Analysis Task

Step 1 Log in to the AOM 2.0 console.

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

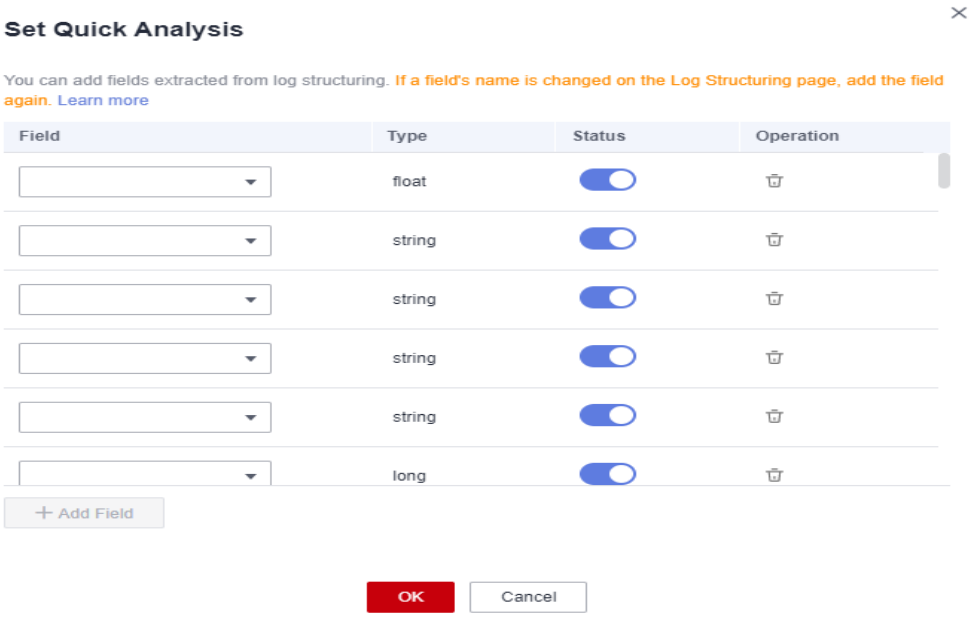
Step 3 On the **Raw Logs** page, click **Set Quick Analysis**, as shown in **Figure 6-14**.

Figure 6-14 Creating a quick analysis task



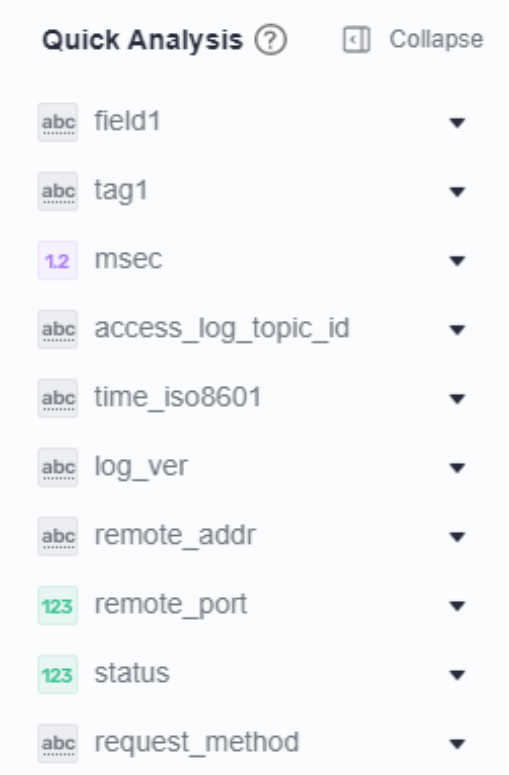
Step 4 On the displayed **Set Quick Analysis** page, select fields for quick analysis.

Figure 6-15 Adding fields



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

Figure 6-16 Viewing quick analysis results



NOTE

- abc indicates a field of the **string** type.
- 1.2 indicates a field of the **float** type.
- 123 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

6.6.3 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 6-17 Configuring quick search

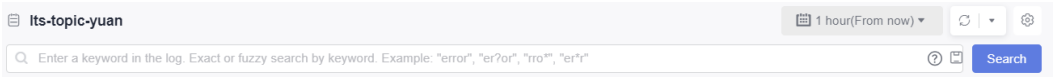


Table 6-8 Quick search parameters

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

6.6.4 Viewing the Context

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

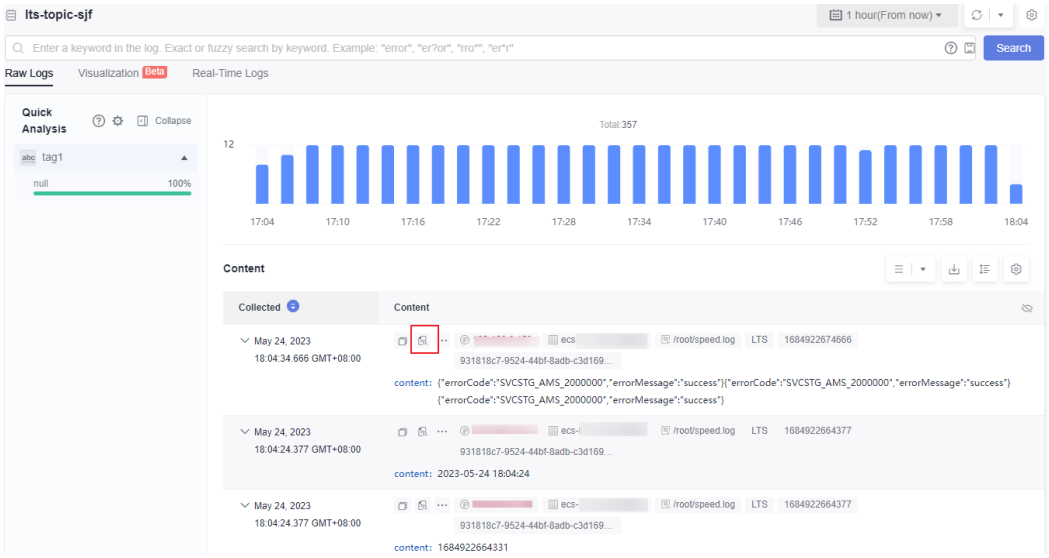
Step 1 Log in to the AOM 2.0 console.

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

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

The context of the log is displayed.

Figure 6-18 Viewing the context



----End

7 Application Insights (Retiring)

7.1 Application Monitoring

An application groups identical or similar components based on service requirements. Through application monitoring, you can learn about the resource usage, status, and alarms of applications in a timely manner to quickly respond to requests and ensure smooth system running.

Function Introduction

Based on **CMDB**, application monitoring monitors resources by layers (application, service component, and environment). The metrics monitored at each layer are different.

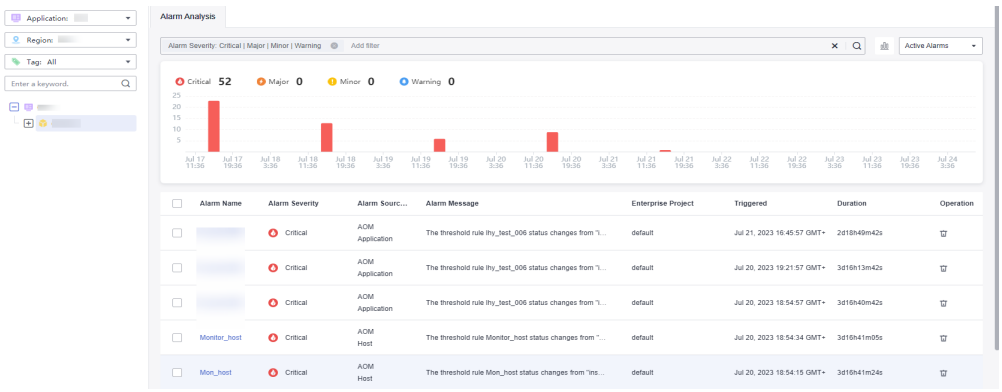
- Application monitoring

  Monitor alarm information at the business, application, middleware, and infrastructure layers, and bind the dashboards to display metric, log, and system graphs.

- Component monitoring

  Monitor alarm information of components. Query both active and historical alarms about components to quickly rectify faults.

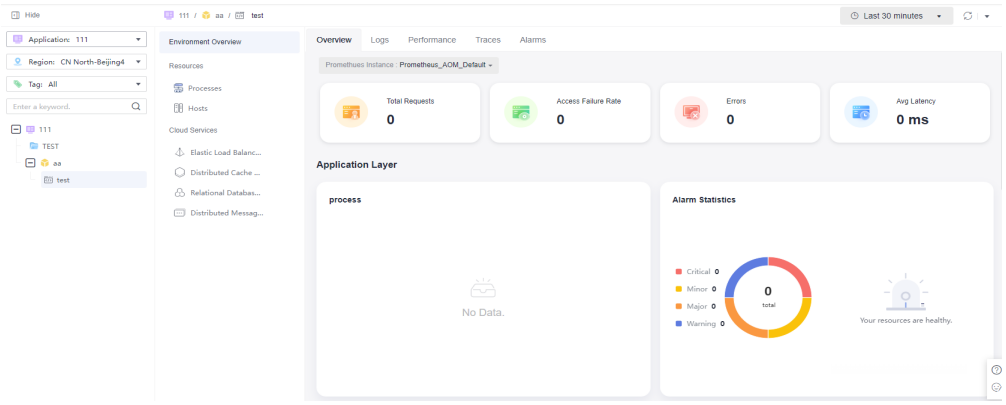
  Figure 7-1 Component monitoring



- Environment monitoring

Monitor and analyze core environment metrics from the environment overview, logs, performance, traces, and alarms. Monitor core metrics such as the process status, application performance (number of errors, number of requests, and average response time), and alarm distribution in the pre-release and production environments. You can also monitor hosts, processes, containers, performance, logs, and cloud services.

Figure 7-2 Environment monitoring



Precautions

- To use application monitoring, enable **Application Insights** in **Menu Settings**. For details, see **13.5 Menu Settings**.
- To report CCE workload metrics to AOM and mount them to the application tree on the left of the **Application Monitoring** page as components, upgrade the workloads first. The following shows the procedure:
  a. Log in to the CCE console and click a target cluster name.
  b. Choose **Workloads** in the navigation pane, and select the type of workload whose metrics are to be reported to AOM.
  c. In the **Operation** column of the workload, choose **More** > **Edit YAML**.
  d. In the displayed dialog box, locate the **spec.template.metadata.annotations** code segment.

Figure 7-3 Editing the YAML file

e. Set parameters by referring to **Table 7-1**. **Figure 7-4** shows the details.

Table 7-1 Parameters

Parameter	Description	Mandatory	Default Value
aom.application.name	Application name	Yes	-
aom.subapplication.name	Sub-application name	No	-
aom.component.name	Component name	No	Same as the workload name
aom.environment.name	Environment name	No	Same as the cluster name

Figure 7-4 Setting parameters

f. Click **Confirm** to save the modification.

g. (Optional) In the **Edit YAML** window, click **Download** to download the YAML file.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **Application Monitoring**.

Step 3 On the left of the **Application Monitoring** page, search for and select the target applications or components by application, region, tag, or keyword.

Step 4 Select an application. In the right pane, view the alarms of each layer and the dashboards bound to the application.

- Click **Business**, **Application**, **Middleware**, or **Infrastructure** to check whether resources at the corresponding layer are healthy. If resources are healthy, the resource layer is green. If an alarm is generated, the resource layer is red. When an alarm is generated, click it to view the alarm details and handling suggestions.
- For details about operations related to dashboards, see **3 Dashboard**.

Step 5 Select a component and view the alarm analysis about the component in the right pane.

- Click an alarm name to view alarm details. For details, see **4.4 Viewing Alarms**.
- Click the drop-down list box in the upper right corner and switch between **Active Alarms** or **Historical Alarms**.

Step 6 Select an environment and view the environment, process, performance, log analysis, trace, and alarm information in the right pane.

- In the **Environment Overview** area, click a resource or cloud service to view their information. Click an instance to view its metrics, logs, and alarms.
- On the **Overview** tab page, view environment metrics, and application and infrastructure information.
- On the **Logs** tab page, view the raw logs and real-time logs of the environment, and perform visualized analysis. For details, see **6.6 Searching for and Viewing Logs**.
- On the **Performance** tab page, view the performance about the environment.
- On the **Traces** tab page, view request success/failure, response time, and generation time about URLs and call methods.
- On the **Alarms** tab page, view the alarms and events in the current environment. For details, see **4.4 Viewing Alarms** and **4.5 Viewing Events**.

----End

7.2 CMDB

7.2.1 Overview

Information Technology Infrastructure Library (ITIL) implements infrastructure-oriented management, facing problems such as data isolation and information inconsistency between O&M services. CMDB centrally manages resource objects and applications, and provides accurate, consistent resource configuration data in time for AOM, LTS, and APM. It also provides data configuration interfaces for maintaining third-party systems.

Precaution

To use CMDB, enable **Application Insights** in **Menu Settings**. For details, see **13.5 Menu Settings**.

Function Description

Table 7-2 Function description

Category	Description
Homepage	On the homepage, search for resources (such as applications and hosts) by keyword or name.
Application Management	Manage the relationships between cloud service objects and applications. The "application + sub-application (optional) + component + environment" model is used.
Resource Management	Centrally manage your cloud services. You can view the association relationships between global cloud service resource objects and applications, including cloud resources that have not been bound to applications, facilitating resource analysis and management.
Environment Tags	Add tags to created application environments so that you can quickly filter environments with the same attributes.
Enterprise Project	An enterprise project can contain one or more applications.

Basic Concepts

CMDB is used to manage application structure information and related configurations. It involves the following concepts:

- **Enterprise project**: An enterprise project can contain one or more applications.
- **Application management**: Manage the relationships between resource objects and applications. CMDB uses the "application + sub-application (optional) + component + environment" model.
- **Application**: basic object of CMDB and root node of the resource management model. An application represents a logical unit, which can be a project, product, or service. After an application is created, you can view the same application topology information in all regions.
- **Sub-application** (optional): A maximum of three layers of sub-applications can be created for an application. A sub-application can be regarded as a service, which is a group of components or microservices.
- **Component**: minimum unit of an application. It can be regarded as a middleware component on which an application depends, such as Relational Database Service (RDS) and Distributed Message Service (DMS). Generally, a component is used together with environments. It can contain one or more environments. For example, an order application includes the function test environment, pressure test environment, pre-release environment, and live network environment.
- **Environment**: Components or programs with different configurations form different environments. Each environment has its own region attribute. You can filter environments by region. You can also add one or more tags when

creating an environment, and filter environments by tag. For example, environments can be classified into the formal or test environment by environment type, CN East or CN South environment by region, or Alpha, Beta, Gamma, or Product environment by DevOps pipeline phase.

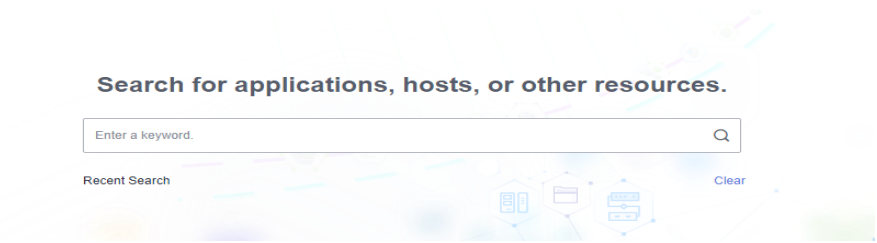
- **Environment tag**: attribute set for an environment. Multiple environments may have the same tag. You can filter required environments by tag. A tag can be added only to different environments of the same application.
- **Resource bind**: You can bind a resource object to an environment of an application. A resource object instance of an application can belong to multiple environments.
- **Resource unbind**: If the component or environment changes and the resource is not required, you can unbind the resource from the original application.
- **Resource transfer**: If the component or environment to which a resource is bound changes, transfer the resource to the target node.

7.2.2 Homepage

Resource Retrieval

On the resource retrieval page, search for resources (such as applications and hosts) by ID, keyword, or name.

Figure 7-5 Resource retrieval



NOTE

- A search criteria can contain 2 to 124 characters.
- You can enter IDs, keywords, or names for search. Separate them using commas (,). For example, to search for applications or resources whose names contain **AOM** and **LTS**, enter **aom,lts** in the search box.

Enterprise Project

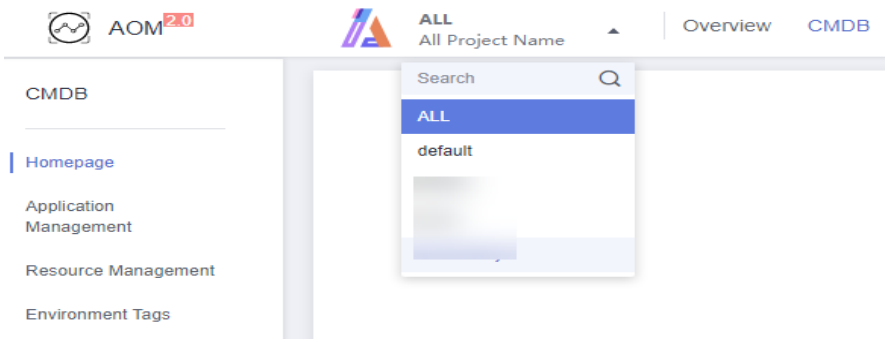
An enterprise project can contain one or more applications.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 On the menu bar, select an enterprise project from the project drop-down list.

Figure 7-6 Enterprise project



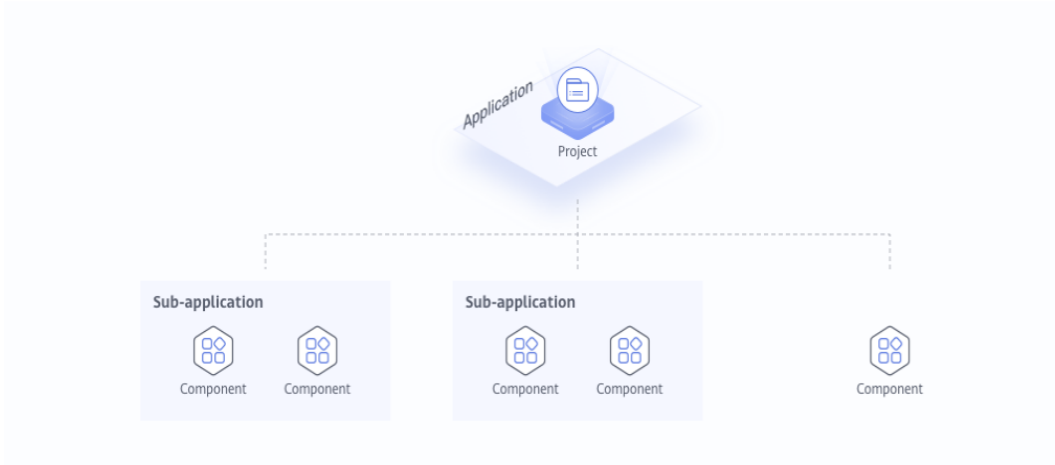
----End

7.2.3 Application Management

7.2.3.1 Usage Description

CMDB manages the relationships between cloud service resources (such as Elastic Cloud Server (ECS), Relational Database Service (RDS), and Elastic Load Balance (ELB)) and applications. It uses the model "application + sub-application (optional) + component + environment".

Figure 7-7 Application management model



7.2.3.2 Creating an Application

An application groups identical or similar components based on service requirements. After creating an application, you can add sub-applications and components to the application and monitor the service running status in real time using functions such as application monitoring.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the navigation pane, choose **Application Management**. Click **Add Application**.

Step 5 On the displayed page, set parameters to add an application.

Table 7-3 Parameters for adding an application

Parameter	Description
Unique Identifier	Unique identifier of an application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Application Name	Name of an application. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project	Enterprise project. • If no enterprise project has been selected on the global settings page, the first enterprise project in the drop-down list is displayed here by default. This option will be dimmed and cannot be changed. • 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 application. Enter up to 255 characters.

Step 6 Click **OK**.

NOTE

The created application is displayed as a tree node in the application area.

----End

More Operations

After the application is created, you can also perform the operations listed in **Table 7-4**.

Table 7-4 Related operations

Operation	Description
Adding a node	Locate the target application, click  , and add a node by referring to **7.2.3.3 Adding a Node**.

Operation	Description
Modifying an application	Locate the target application and choose > **Modify**.
Deleting an application	Locate the target application and choose > **Delete**.
Searching for application information	In the left pane of the **Application Management** page, search for an application by enterprise project, application, region, tag, or keyword.
Viewing application information	Locate an application and click the **Application Info** tab in the right pane.

7.2.3.3 Adding a Node

After an application is created, you can add nodes (such as components and sub-applications) to the application.

Adding a Node

Step 1 Log in to the AOM 2.0 console.

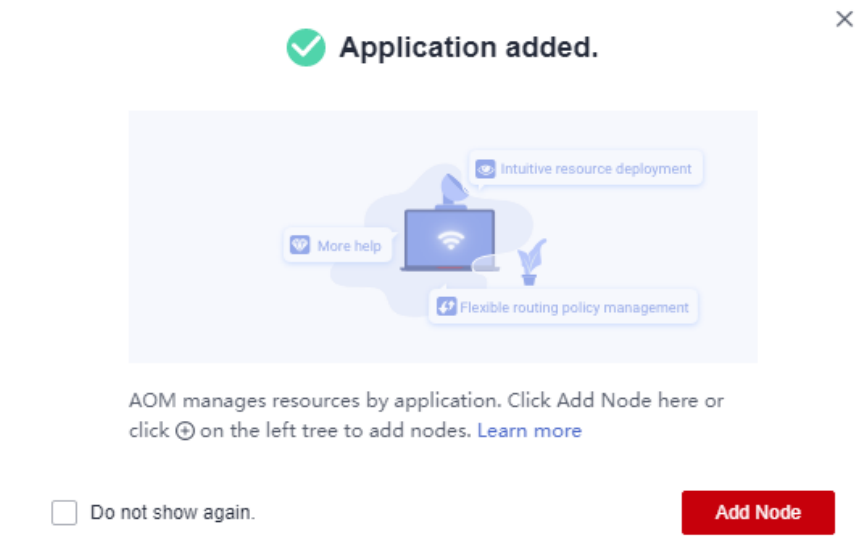
Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 Add a component or sub-application. Use either of the following methods:

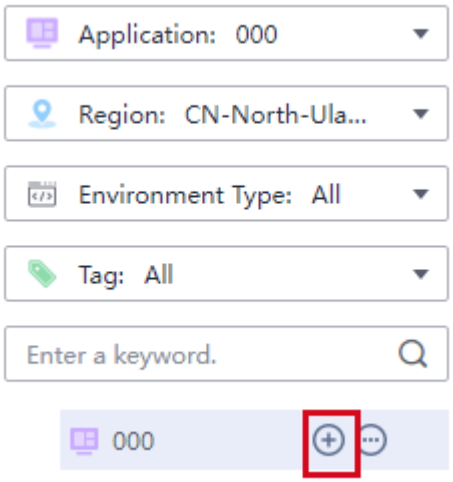
- After an application is created, click **Add Node**.

Figure 7-8 Creating a sub-application



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

Figure 7-9 Application tree



Step 5 Configure node information, including the node type and name.

Figure 7-10 Adding a node

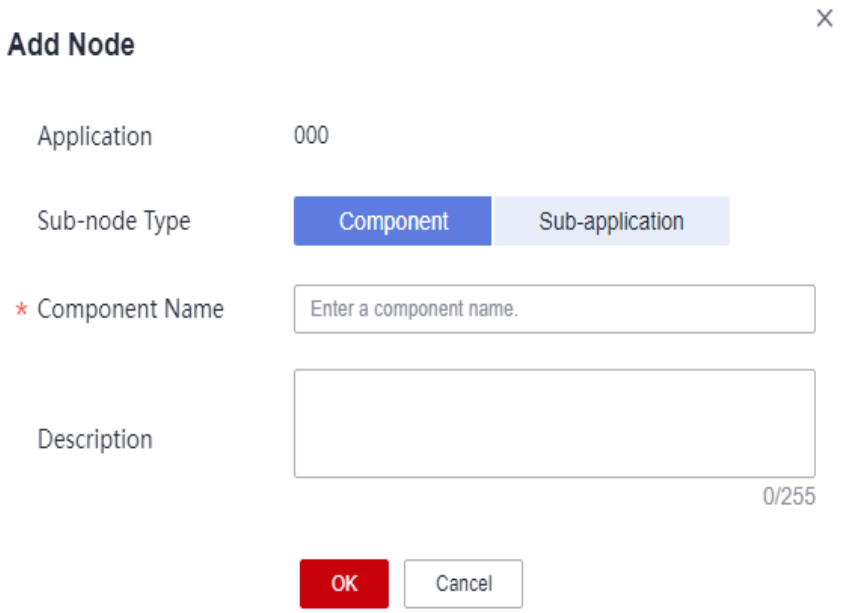


Table 7-5 Parameters for adding a node

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

NOTE

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

Step 6 Click **OK**.

----End

More Operations

After the node is created, you can also perform the operations listed in **Table 7-6**.

Table 7-6 Related operations

Operation	Description
Adding a sub-node	Locate the target node and click  to add a sub-node by referring to **Adding a Node**.
Modifying a node	Locate the target node and choose  > **Modify**.
Deleting a node	Locate the target node and choose  > **Delete**.

Operation	Description
Transferring a node	Locate the target node and choose > **Transfer**. On the page that is displayed, select the target node to transfer.
Adding an environment	Locate the target sub-node and click to add an environment by referring to **7.2.3.4 Adding an Environment**.
Viewing node information	Locate a sub-application or component and click **Sub-application Info** or **Component Info** in the right pane.

7.2.3.4 Adding an Environment

After a component is created, you can add different environments for the component based on hosts and regions for easier management.

Adding an Environment

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the tree on the left, locate the target component and click .

Step 5 On the **Add Environment** page, set information such as **Environment Type** and **OS Type**.

Table 7-7 Parameters for adding an environment

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

NOTE

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

Step 6 Click **OK**.

----End

More Operations

After the environment is created, you can also perform the operations listed in **Table 7-8**.

Table 7-8 Related operations

Operation	Description
Editing an environment	In the tree on the left, locate the target environment and click .
Deleting an environment	In the tree on the left, locate the target environment and click .
Binding a resource	In the tree on the left, locate the target environment. In the right pane, click any resource instance tab. In the lower pane, click **Bind Resource**. For details, see **7.2.3.5 Binding Resources**.
Viewing environment information	Locate an environment in the tree on the left and click **Environment Info** in the right pane.

7.2.3.5 Binding Resources

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

Viewing Resource List

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab. For details about each resource type, see **Table 7-9**.

NOTE

1. If a resource exists, it is displayed on the resource management page. If no resource exists, no resource is displayed.
2. All resources that can be bound to environments are displayed on the application management page.

Table 7-9 Resource list

Resource Type		Sub-type	Information
Elastic Cloud Server (ECS)	-	-	Name/ID, private IP address, EIP, host name, AZ, region, application environment, UniAgent status, resource status, and operation.
Cloud Container Engine (CCE)	-	Workload	Workload name, namespace, cluster, workload type, region, application environment, and last update time.
		Cluster	Cluster name, cluster ID, and region.
Databases	Relational Database Service (RDS)	-	Instance name/ID, instance type, DB engine version, resource status, private IP address, region, application environment, and operation.
	Document Database Service (DDS)	-	Name/ID, resource status, instance type, version, enterprise project, region, application environment, and operation.
	Data Replication Service (DRS)	Real-time synchronization task	Name/ID, resource status, resource type, enterprise project, region, application environment, and operation.
		Real-time migration task	
		Real-time disaster recovery task	
		Data subscription task	
		Backup migration task	
	GaussDB NoSQL	-	Name/ID, instance type, enterprise project, region, application environment, and operation.

Resource Type		Sub-type	Information
	GaussDB	-	Name/ID, resource status, type, enterprise project, region, application environment, and operation.
Networking	Elastic Load Balance (ELB)	-	Name/ID, resource status, IP address and network, listener, region, enterprise project, application environment, and operation.
Application middleware	Distributed Cache Service (DCS)	-	Name/ID, resource status, cache type, instance type, specifications (GB), IP address, region, enterprise project, application environment, and operation.
	Distributed Message Service (DMS)	Kafka	Name/ID, specifications, maximum partitions, region, application environment, and operation.
		RabbitMQ	Name/ID, specifications, region, application environment, and operation.
Storage	Object Storage Service (OBS)	-	Bucket name, region, enterprise project, region, application environment, and operation.
	Cloud Backup and Recovery (CBR)	-	Name/ID, resource status, resource type, billing mode, region, enterprise project, application environment, and operation.
Function Graph	-	Function	Name/ID, type, region, enterprise project, application environment, and operation.
Big data	Cloud Search Service (CSS)	-	Name/ID, resource status, resource type, version, region, enterprise project, application environment, and operation.

----End

Binding Resources

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab. Then, in the lower area, click **Bind Resource**.

NOTE

CCE does not support resource binding.

Step 5 Select your target resource from the resource list.

- Set filter criteria above the resource list to filter resources.
- Click  in the upper right corner to obtain the latest information about resource instances in real time.
- Click  in the upper right corner and select or deselect columns to display.

NOTE

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

Step 6 Click **Bind**.

NOTE

In case of an ECS, click **Bind Resource & Install Agent** to bind the ECS and install an Agent. For details about how to install an Agent, see **11.2.1.1 Installing a UniAgent**.

----End

Transferring Resources

If the component or environment to which a resource is bound changes, transfer the resource as required.

Perform the following steps:

Step 1 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 2 Select **an enterprise project**.

Step 3 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab.

Step 4 Perform the following operations in the resource list as required:

- To transfer one resource instance, click ⇌ in the **Operation** column of the row that contains the resource instance.
- To transfer multiple resource instances, select the check boxes of target instances and click ⇌ Transfer at the bottom.

Step 5 In the dialog box that is displayed, set resource transfer parameters by referring to **Table 7-10**.

Table 7-10 Parameters for transferring resources

Parameter	Description
Select Node	Target node to which the resource instance is to be transferred. Select a value from the drop-down list.
Transfer Mode	Resource transfer mode. Options: • **Override**: The existing environment is not retained. In this mode, the resource instance is transferred from the original environment to the target environment, and the resource instance is no longer bound with the original environment. • **Incremental update**: The existing environment is retained. In this mode, the resource instance is bound with both the original and target environments. **NOTE** – For intra-application transfer, both override and incremental update modes are supported. – For inter-application ECS transfer, the incremental update mode is not supported.

Step 6 Click **OK**.

----End

Unbinding Resources

If a component or environment changes and resources are not required, you can unbind them.

Perform the following steps:

Step 1 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 2 Select **an enterprise project**.

Step 3 In the tree on the left, locate the target environment. In the right pane, click the **Resource List** tab.

Step 4 Perform the following operations in the resource list as required:

- To unbind one resource instance, click  in the **Operation** column of the row that contains the resource instance.
- To unbind multiple resource instances, select target instances and click 

at the bottom.

NOTE

Unbinding a cloud resource from an environment will not delete the cloud service.

----End

Viewing Application Information

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the tree on the left, locate the target application. In the right pane, click **Application Info**.

----End

NOTE

To view the sub-application, component, or environment information, locate the target sub-application, component, or environment in the tree on the left and click **Sub-application Info**, **Component Info**, or **Environment Info** in the right pane.

7.2.4 Resource Management

Resource management centrally manages all your cloud services. You can view the association relationships between global cloud service resource objects and applications, including cloud resources that have not been bound to applications, facilitating resource analysis and management.

Currently, the following types of resources can be managed:

Elastic Cloud Server (ECS), Cloud Container Engine (CCE), databases (Relational Database Service (RDS), Document Database Service (DDS), Data Replication Service (DRS), GaussDB NoSQL, and GaussDB), networking (Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Elastic IP (EIP), NAT gateway, and VPN (VPN gateways and VPN connections)), application middleware (Distributed Cache Service (DCS) and Distributed Message Service (DMS) (Kafka and RabbitMQ)), storage (Object Storage Service (OBS), Elastic Volume Service (EVS), Scalable File Service (SFS), and Cloud Backup and Recovery (CBR)), FunctionGraph, and big data (Cloud Search Service (CSS))

Viewing Resource Information

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the navigation pane, choose **Resource Management**. Click a resource tab to view the names, projects, and environments of the resource's instances.

- Set filter criteria above the resource list to filter resources.
- Click  in the upper right corner to obtain the latest information about resource instances in real time.
- Click  in the upper right corner and select or deselect columns to display.
- Click the resource name/ID to go to the resource details page. On the resource details page, click **More** to go to the service console and view more information.

- After you purchase a service resource, CMDB detects and obtains the resource information in real time and displays it on the **Resource Management** page.
- For details about different types of resources, see **Table 7-11**.

Table 7-11 Resource types

Resource Type		Sub-type	Information	Operation
ECS	-	-	Name/ID, private IP address, EIP, host name, AZ, region, enterprise project, application environment, UniAgent status, resource status, image name, and VPC name.	• Click a resource name in the **Name/ID** column. The host details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
CCE	-	Workload	Workload name, namespace, cluster, workload type, region, application environment, and last update time.	• Click a workload name in the **Workload Name** column. The workload details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
		Cluster	Cluster name, cluster ID, and region.	-
Databases	RDS	-	Instance name/ID, instance type, DB engine version, resource status, private IP address, enterprise project, region, and application environment.	• Click an ID in the **Instance Name/ID** column. The RDS DB instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.

Resource Type		Sub-type	Information	Operation
	DDS	-	Name/ID, resource status, instance type, version, enterprise project, region, and application environment.	• Click an ID in the **Name/ID** column. The DDS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	DRS	Real-time synchronization task	Name/ID, resource status, instance type, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The DRS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
		Real-time migration task		
		Real-time disaster recovery task		
		Data subscription task		
		Backup migration task		

Resource Type		Sub-type	Information	Operation
	GaussDB NoSQL	-	Name/ID, instance type, enterprise project, region, and application environment.	• Click an ID in the **Name/ID** column. The GaussDB NoSQL instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	GaussDB	-	Name/ID, resource status, type, enterprise project, region, and application environment.	• Click an ID in the **Name/ID** column. The GaussDB instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
Networking	VPC	-	Name/ID, IPv4 network segment, status, region, enterprise project, and tag.	Click an ID in the **Name/ID** column. The VPC instance details page is displayed.
	ELB	-	Name/ID, resource status, IP address and network, listener, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The load balancer details page is displayed. • Click an environment in the **Listener** column. The listener details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.

Resource Type		Sub-type	Information	Operation
	EIP	-	EIP/ID, status, bandwidth, bandwidth details, bound instance, region, enterprise project, and associated application environment.	• Click an ID in the **Name/ID** column. The EIP details page is displayed. • Click an instance name in the **Bound Instance** column. The host details page is displayed, including the attributes and associated cloud services. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	NAT Gateway	-	Name/ID, status, service, resource type, region, and enterprise project.	• Click an ID in the **Name/ID** column. The NAT gateway details page is displayed.
	VPN	VPN gateway	Name/ID, resource type, public IPv4 address, status, VPN connections, region, and enterprise project.	• Click an ID in the **Name/ID** column. The VPN gateway details page is displayed.
		VPN connection	Name/ID, resource type, status, remote gateway, VPN gateway, region, and enterprise project.	• Click an ID in the **Name/ID** column. The VPN connection details page is displayed.

Resource Type		Sub-type	Information	Operation
Application middleware	DCS	-	Name/ID, resource status, cache type, instance type, specifications (GB), IP address, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The DCS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	DMS	Kafka	Name/ID, specifications, maximum partitions, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The CBR instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
		RabbitMQ	Name/ID, specifications, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The RabbitMQ instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.

Resource Type		Sub-type	Information	Operation
Storage	OBS	-	Bucket name, region, enterprise project, and application environment.	• Click a bucket name in the **Bucket Name** column. The OBS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	CBR	-	Name/ID, resource status, resource type, billing mode, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The DCS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
	EVS	-	Name/ID, status, disk specifications, disk attributes, region, and enterprise project.	• Click an ID in the **Name/ID** column. The EVS instance details page is displayed.
	SFS	-	Name/ID, status, capacity, share path, protocol type, region, and enterprise project.	• Click an ID in the **Name/ID** column. The SFS details page is displayed.

Resource Type		Sub-type	Information	Operation
FunctionGraph	-	Function	Name/ID, type, region, enterprise project, and application environment.	• Click an ID in the **Name/ID** column. The instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.
Big data	CSS	-	Name/ID, resource status, resource type, version, enterprise project, region, and application environment.	• Click an ID in the **Name/ID** column. The CSS instance details page is displayed. • Click an environment in the **Application Environment** column. The corresponding resource page under **Application Management** is displayed.

----End

7.2.5 Environment Tags

Add tags to created application environments so that you can quickly filter environments with the same attributes.

Adding a Tag

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **CMDB**.

Step 3 Select **an enterprise project**.

Step 4 In the navigation pane, choose **Environment Tags**.

Step 5 On the **Add Tag** page, set related parameters.

Figure 7-11 Adding a tag

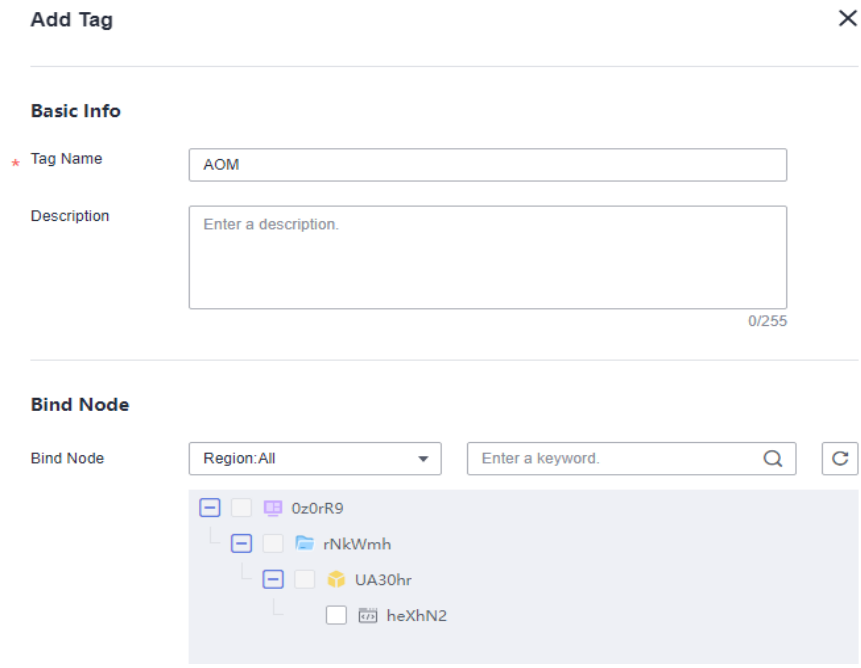


Table 7-12 Parameters for adding a tag

Parameter	Description
Tag Name	Name of a tag. Enter 2 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Description	Description of the tag. Enter up to 255 characters.
Bind Node	Node to be bound with the tag. • **Region**: region of the resource. Select a region from the drop-down list or enter a keyword to search for a region. • **Node**: node to be bound. Select a node from the application tree or enter a keyword to search for a node.

Step 6 Click **OK**.

----End

More Operations

After a tag is added, you can view the tag name, description, update time, and creation time in the tag list. You can also perform the operations listed in **Table 7-13**.

Table 7-13 Related operations

Operation	Description
Modifying a tag	Click **Modify** in the **Operation** column.
Deleting a tag	Click **Delete** in the **Operation** column.

7.3 Log Ingestion

You can set log collection paths of hosts in **CMDB**. ICAgents then collect logs from the hosts based on your specified collection rules, and pack and send the collected log data to AOM on a log stream basis. You can view logs on the AOM console in real time.

Prerequisites

- You have added a component and environment for the application. For details, see **7.2.3.3 Adding a Node** and **7.2.3.4 Adding an Environment**.
- You have created a log group and log stream. For details, see **Creating Log Groups and Log Streams**. You can also directly create them on the log ingestion page.
- You have created a cluster, namespace, and workload. For details, see **Cloud Container Engine (CCE) User Guide**.

Precautions

- To use log ingestion, enable **Application Insights** in **Menu Settings**. For details, see **13.5 Menu Settings**.
- The logs of VMs running Windows cannot be reported to AOM.

Ingesting Logs

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Application Insights (Retiring)** > **Log Ingestion**.

Step 3 Click **Access Log** in the upper right corner.

Step 4 Complete the following configurations based on your requirements:

1. **Select Log Stream**: Log files in the selected environment are to be ingested to the specified LTS log stream.
   a. **Collection Configuration Name**: Enter up to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. The name cannot start with a period or underscore, or end with a period.
   b. **Log Group**: Select a created log group from the drop-down list.
   c. **Log Stream**: Select a created log stream from the drop-down list.
2. **Host Group configuration**: Add the hosts in the selected environment to the LTS host group.

a. Click **Select Environment**.
b. Select the application and region to which the target environment belongs.
c. Search for or expand the application tree to select the required environment.
d. Click **OK**.

3. **Collection Configuration**: Set log collection rules.
   a. **Collection Path**: Add one or more host paths. LTS will collect logs from these paths.
   b. **Collect Windows Logs**: To collect logs from Windows hosts, enable this option. Filter the logs to collect by configuring **Log Type**, **First Collection Time Offset**, and **Event Severity**.
   c. **Log Format**: Specifies whether the collected log file is displayed in a single line or multiple lines.
   d. **Log Time**: When **Log Format** is set to **Single-line**, specify whether the log collection time (**System time**) or log printing time (**Time wildcard**) is displayed at the beginning of each log line.

      NOTE

      - **System time**: the time when logs are collected and sent by ICAgents to LTS.
      - **Time wildcard**: the time when logs are printed.

   e. **Time wildcard**: The log print time is used to identify a log and is displayed at the start of each log line. Logs can be filtered based on a time wildcard.
   f. **Log Segmentation**: must be specified if the **Log Format** is set to **Multi-line**. **Log time** indicates that log segmentation is implemented based on a time wildcard, whereas **By regular expression** indicates that log segmentation is implemented based on a regular expression.
   g. **Regular Expression**: used to identify a log.
   h. Click **Ingest Now**.

Step 5 View your configuration in the corresponding configuration list.

----End

Viewing and Managing Ingestion Configuration

On the **Log Ingestion** page, you can search for, view, edit, and delete ingestion configurations.

- Search

  On the **Log Ingestion** page, select the target application or component on the left and enter a keyword in the search box on the right.

- View

  You can view the created ingestion rules on the **Log Ingestion** page. Click a log group name in the **Log Group** column to go to the log group details page on the LTS console.

- Edit

  On the **Log Ingestion** page, click **Edit** in the **Operation** column in the row that contains the target configuration.

- Delete

  On the **Log Ingestion** page, click **Delete** in the **Operation** column in the row that contains the target configuration. You can also delete configurations in batches.

  NOTE

  Deleted access configurations or mapped log streams cannot be recovered. Exercise caution when performing this operation.

8 Prometheus Monitoring

8.1 Prometheus Monitoring

8.1.1 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 8-1** lists different types of instances classified based on monitored objects and application scenarios.

Table 8-1 Prometheus instance description

Prometheus Instance Type	Monitored Object	Monitoring Capability	Application Scenario
default	• Metrics reported using the API for **adding monitoring data** • Cloud service metrics reported by APIs such as IoT Device Access (IoTDA), ModelArts, Intelligent EdgeFabric (IEF), and Cloud Container Instance (CCI) APIs • Metrics reported using ICAgents	Monitors the metrics reported to AOM using APIs or ICAgents.	Common 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.
8.2.3 Prometheus Instance for CCE	CCE	• 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 Type	Monitored Object	Monitoring Capability	Application Scenario
8.2.2 Prometheus Instance for ECS	ECS	• 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.
8.2.1 Prometheus Instance for Cloud Services	Multiple cloud services	Monitors multiple cloud services, such as Relational Database Service (RDS). **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.
8.2.4 Prometheus Instance for Remote Write	Self-built Prometheus	• Provides remote storage for Prometheus time series databases. • Provides a self-developed monitoring dashboard to display data. **NOTE** Prometheus servers are maintained by you. You need to configure service discovery and data collection by yourselves.	Applicable when you have your own Prometheus servers but need to ensure data storage availability and scalability through remote write.

Prometheus Instance Type	Monitored Object	Monitoring Capability	Application Scenario
8.2.5 Prometheus Instance for Multi-Account Aggregation	CCE, ECS, and other cloud service resources of multiple accounts in the same organization	Aggregates the data of CCE, ECS, and other cloud service resources of multiple accounts in the same organization for monitoring and maintenance. **NOTE** Metrics connected through this type of Prometheus instance include: • CCE and ECS metrics. For details, see VM Metrics. • Other cloud service metrics. For details, see Cloud Service Metrics.	Applicable when you need to centrally monitor the CCE, ECS, and other cloud service resources of multiple accounts in the same organization.

8.1.2 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 8-2 Monitored object access

Function	Description
8.2 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 8-3 Monitoring metric collection

Function	Description
8.5.2 Configuring Service Discovery 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
8.5.1 Configuring Metrics	You can check, add, and discard metrics. Only the default Prometheus instance, Prometheus instances for CCE, and Prometheus instances for cloud services support this function.

Table 8-4 Data processing

Function	Description
8.7 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.
8.4 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.

8.1.3 Advantages

Table 8-5 Advantages

Out-of-the-box usability • Installs and deploys Kubernetes and cloud products in a few clicks. • Connects to various application components and alarm tools in a few clicks.	**Low cost** • 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.

Open-source compatibility • 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.	**Unlimited data** • 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.
High performance • 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.	**High availability** • 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

8.1.4 Basic Concepts

This section describes the basic concepts about Prometheus monitoring.

Table 8-6 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
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.
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.
Alarm rule	Alarm configuration for Prometheus monitoring. An alarm rule can be specified using PromQL.
Tag	A key-value pair that describes a metric.
Service discovery	Automatically discovers collection targets without static configuration. Supports multiple service discovery 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.

8.2 Creating Prometheus Instances

8.2.1 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.

Figure 8-1 Creating a Prometheus instance for cloud services

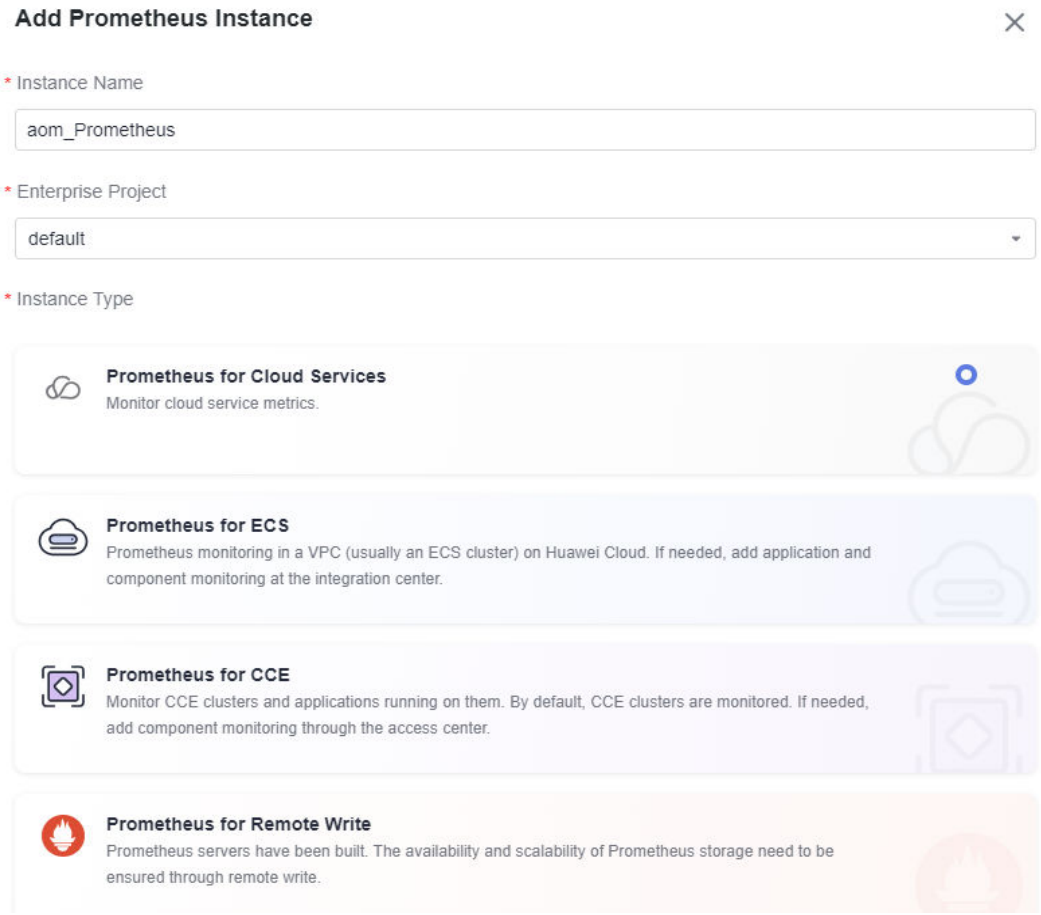


Table 8-7 Parameters for creating a Prometheus instance

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. • 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

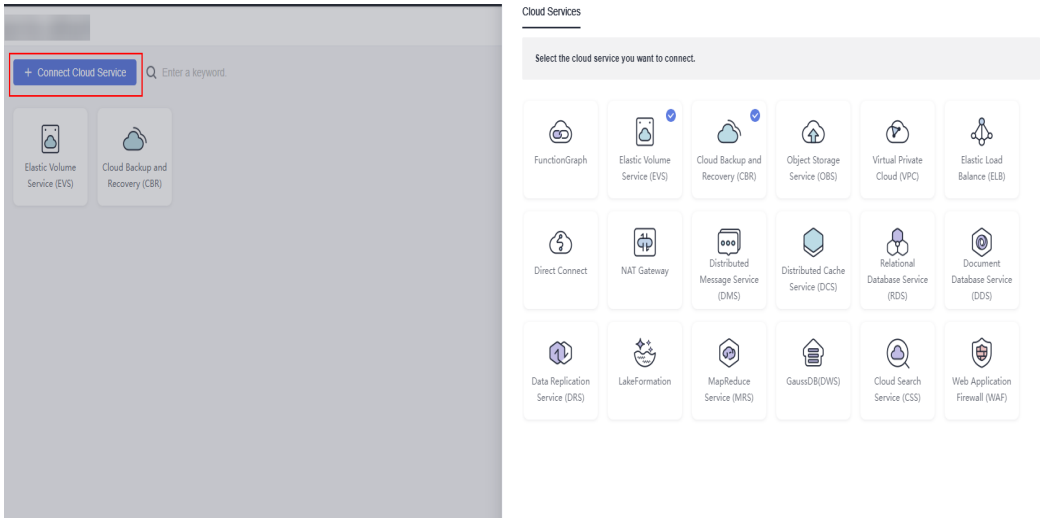
Step 1 Log in to the AOM 2.0 console.

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 Click **Connect Cloud Service** to connect desired cloud services.

Figure 8-2 Connecting cloud services



Step 5 Click **Confirm**.

----End

8.2.2 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 the instance name, enterprise project, and instance type.

Figure 8-3 Creating a Prometheus instance for ECS

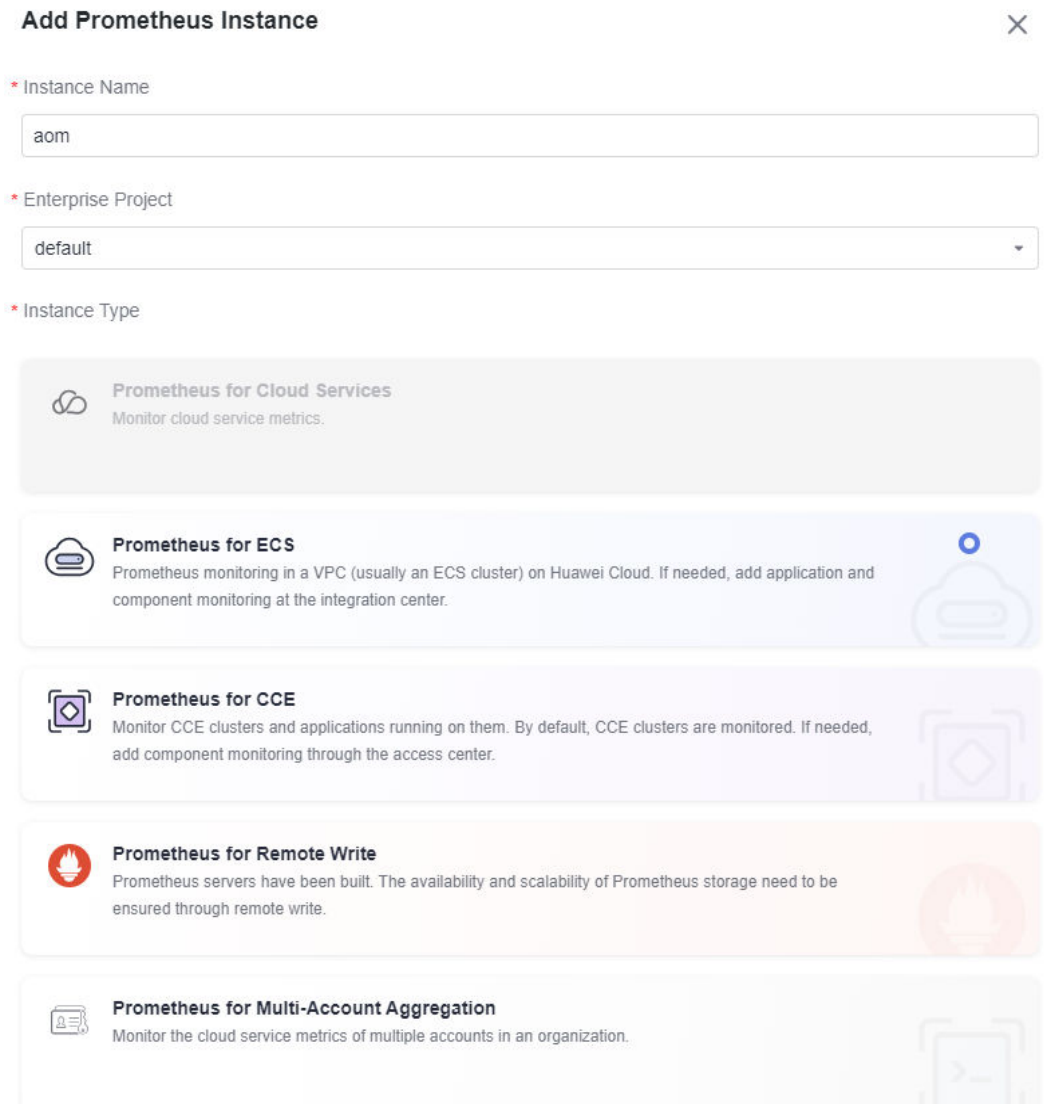


Table 8-8 Parameters for creating a Prometheus instance

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. • 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

8.2.3 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.

Figure 8-4 Creating a Prometheus instance for CCE

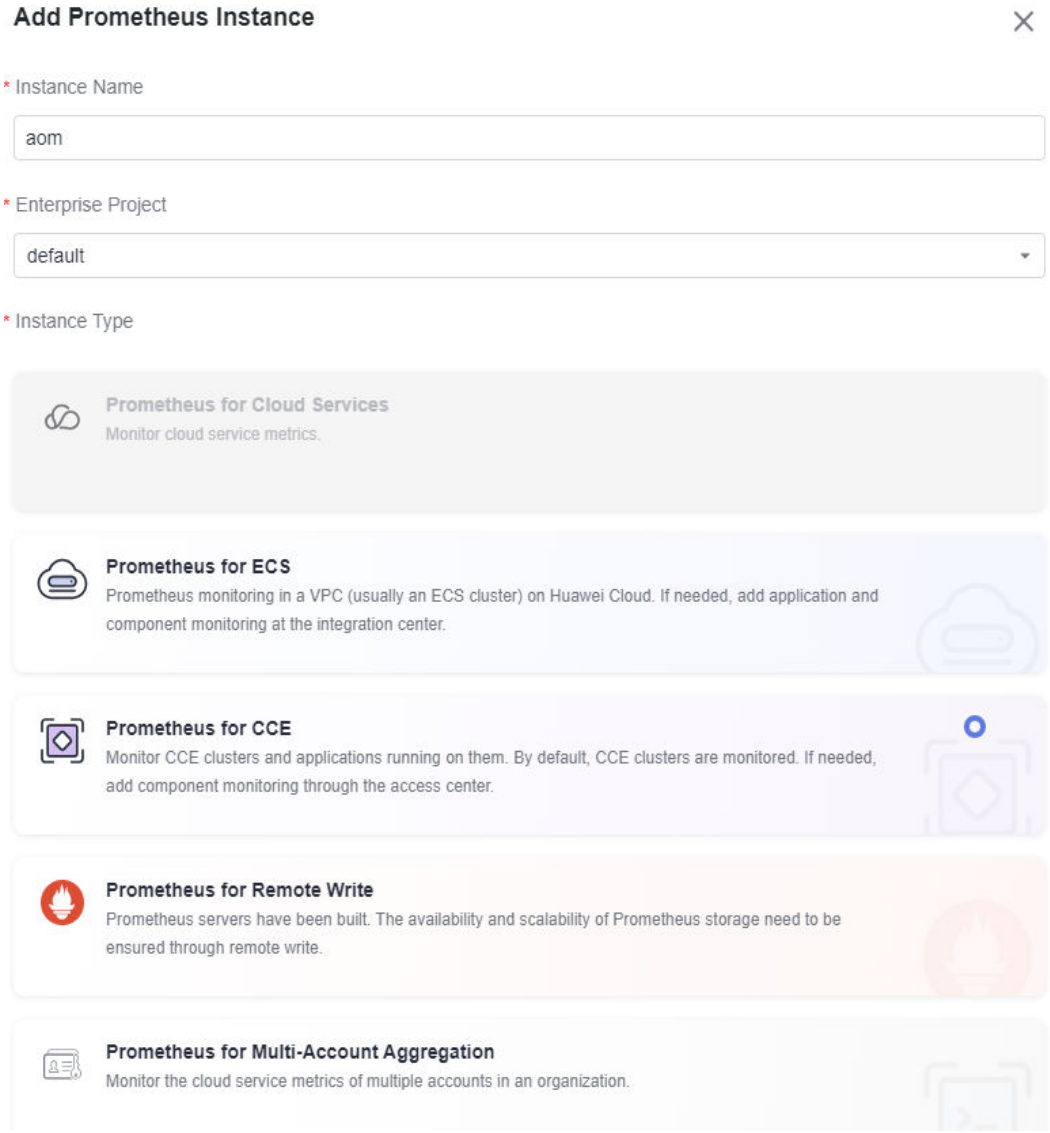


Table 8-9 Parameters for creating a Prometheus instance

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. • 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.

Parameter	Description
Instance Type	Type of the Prometheus instance. Select **Prometheus for CCE**.

Step 4 Click **OK**.

----End

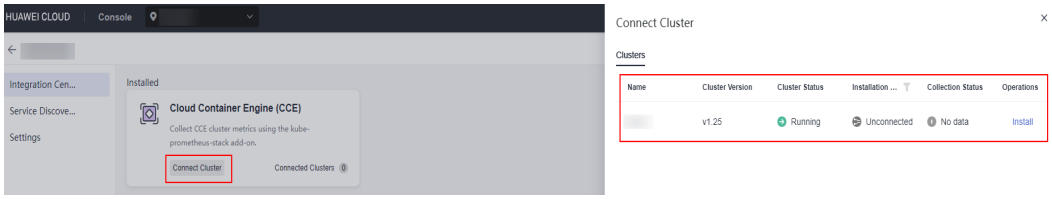
Connecting a CCE Cluster

Step 1 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

Step 2 In the instance list, click a Prometheus instance for CCE.

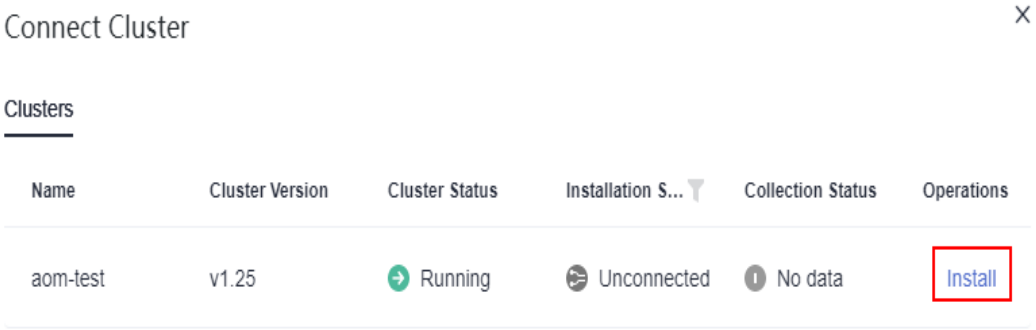
Step 3 On the **Integration Center** page, click **Connect Cluster**. In the cluster list, you can view the cluster information, installation status, and collection status.

Figure 8-5 Viewing cluster connection information



Step 4 Locate a target cluster and click **Install** in the **Operation** column to install the Prometheus add-on.

Figure 8-6 Connecting a CCE cluster



Step 5 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

8.2.4 Prometheus Instance for Remote Write

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 Prometheus Instance for Remote Write

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.

Figure 8-7 Creating a Prometheus instance for remote write

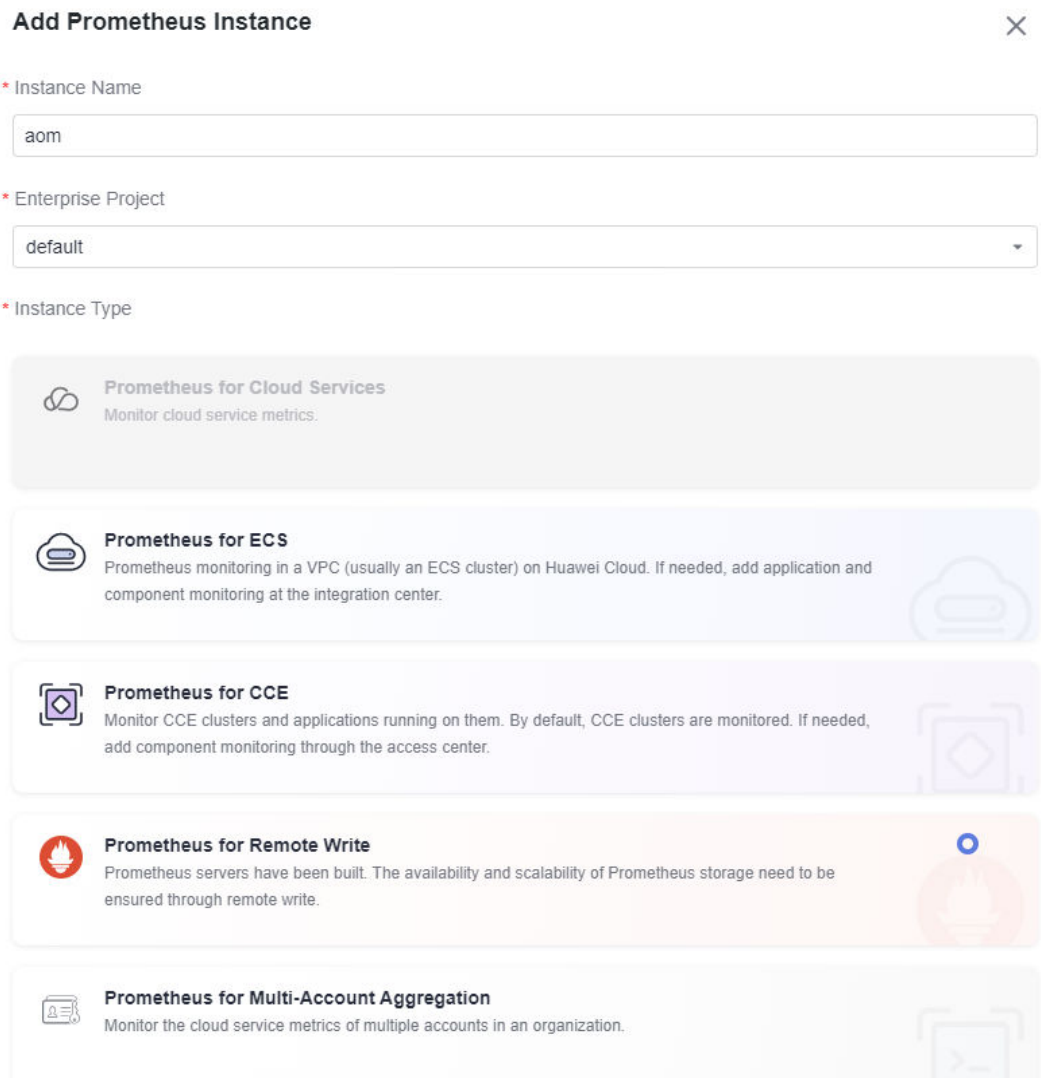


Table 8-10 Parameters for creating a Prometheus instance

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.

Parameter	Description
Enterprise Project	Enterprise project. • If you have selected All for **Enterprise Project** on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be dimmed and cannot be changed.
Instance Type	Type of the Prometheus instance. Select **Prometheus for Remote Write**.

Step 4 Click **OK**.

----End

8.2.5 Prometheus Instance for Multi-Account Aggregation

This type of instance is recommended when you need to monitor the cloud service metrics of multiple accounts in an organization.

Prerequisites

- You have enabled trusted access to AOM on the Organizations console. For details, see **Enabling or Disabling a Trusted Service**.
- Cloud service metrics have been connected for multiple accounts in an organization.

Creating a Prometheus Instance for Multi-Account Aggregation

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.

Figure 8-8 Creating a Prometheus instance for multi-account aggregation

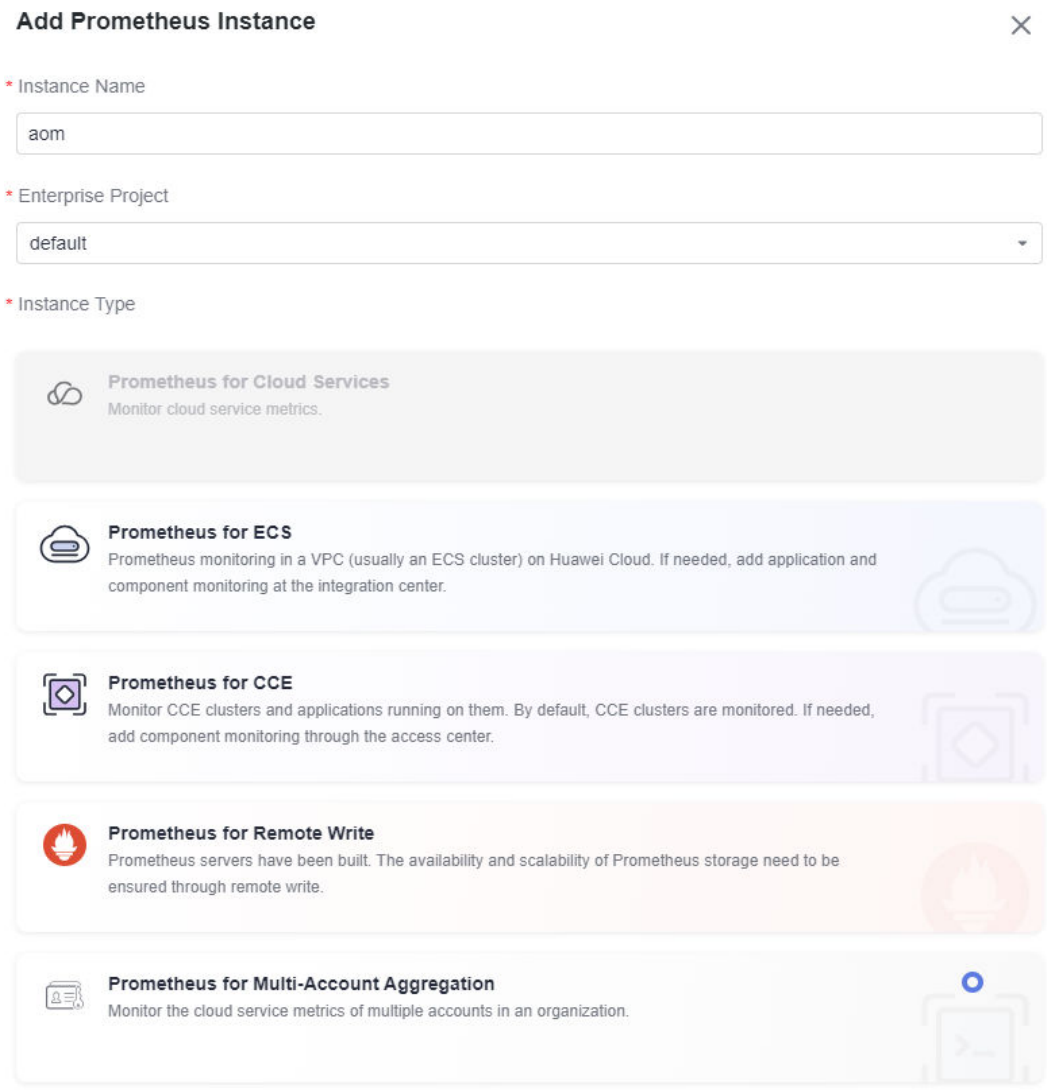


Table 8-11 Parameters for creating a Prometheus instance

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. • 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.

Parameter	Description
Instance Type	Type of the Prometheus instance. Select **Prometheus for Multi-Account Aggregation**.

Step 4 Click **OK**.

----End

Connecting Accounts

You can connect accounts only after logging in as an organization administrator or a delegated administrator. For details about how to set a delegated administrator, see **Specifying, Viewing, or Removing a Delegated Administrator**.

NOTICE

- If a delegated administrator cannot connect accounts, grant the following permissions by referring to **Assigning Permissions to an IAM User**:
  - organizations:trustedServices:list
  - organizations:organizations:get
  - organizations:delegatedAdministrators:list
  - organizations:accounts:list
  - organizations:delegatedServices:list
- AOM only supports connection to member accounts under an organizational unit (OU). When the relationship between the OU and member accounts changes, AOM will not automatically synchronize that information.

To connect accounts, do as follows:

Step 1 Log in to the AOM 2.0 console. In the navigation pane, choose **Prometheus Monitoring** > **Instances**.

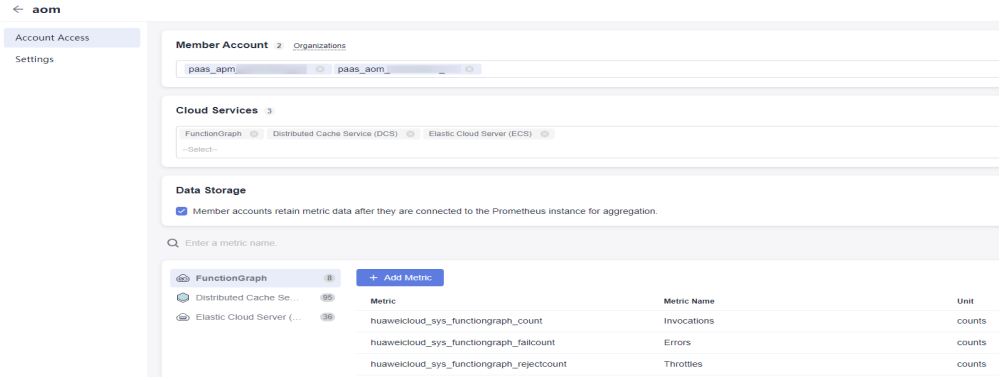
Step 2 On the Prometheus instance list page, click a Prometheus instance for multi-account aggregation.

Step 3 On the **Account Access** page, manage member accounts, connect cloud services, configure data storage, and add supported metrics.

- Managing member accounts: AOM supports account management. It allows you to incorporate cloud accounts into your organization for centralized management. There are three types of members in an organization: administrator, delegated administrator, and common user. Common users do not have the permission to monitor multi-account metrics on AOM.
  - To monitor the metrics of a member account, click the **Member Account** text box and enter an account keyword in the displayed search box. Related member accounts are automatically displayed. Then select your desired ones.
  - To stop monitoring the metrics of a member account, delete the account from the **Member Account** text box on the **Account Access** page.

- Connecting cloud services: Select one or more cloud services from the drop-down list.
- Data storage: Member accounts retain metric data after they are connected to a Prometheus instance for aggregation. By default, this function is disabled.
- Adding metrics supported by cloud services: Click **Add Metric** to add metrics for connected cloud services.

Figure 8-9 Account access page



----End

8.3 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 8-12** if needed.

Figure 8-10 Managing Prometheus instances

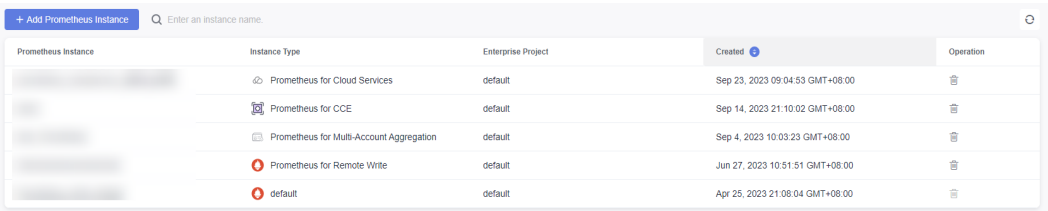


Table 8-12 Related operations

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.
Sorting Prometheus instances	Click in the **Created** column to sort Prometheus instances. indicates the default order. indicates the ascending order by time (the latest instance is displayed at the bottom). indicates the descending order by time (the latest instance is displayed at the top).

Operation	Description
Viewing a Prometheus instance	The Prometheus instance list displays information such as the instance name, instance type, enterprise project, and creation time in real time. • When you have an access code: Click an instance name. On the displayed instance details page, choose **Settings** and view the basic information and credential of the instance. – 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 **8.7 Obtaining the Service Address of a Prometheus Instance**. • When you do not have an access code: 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	• Modify a Prometheus instance name: Click in the **Operation** column that contains the target Prometheus instance. The name of each Prometheus instance in an enterprise project must be unique. • Modify Prometheus instance configurations: In the Prometheus instance list, click the name of a Prometheus instance for cloud services, CCE, or multi-account aggregation and modify the connected **cloud services**/**CCE clusters**/**accounts** if needed.
Deleting a Prometheus instance	Click in the **Operation** column that contains the target Prometheus instance.

----End

8.4 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 **8.2.3 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 8-11 Configuring a recording rule

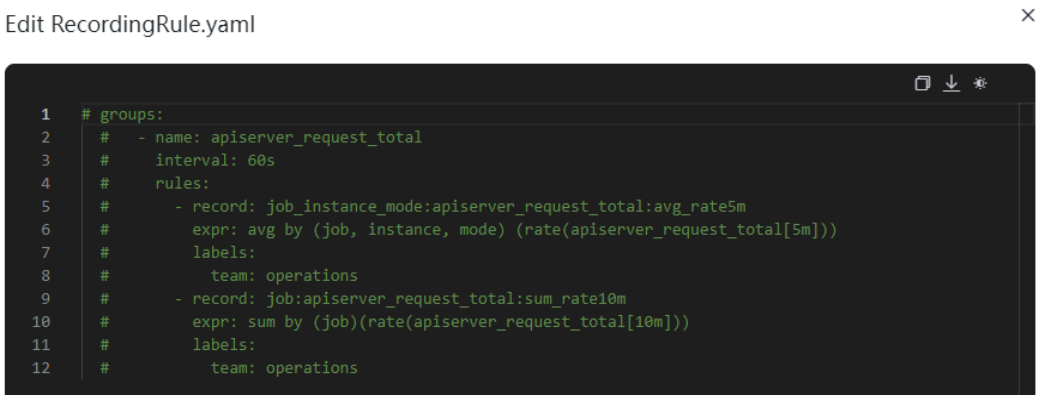


Table 8-13 Recording rule parameters

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 **8.9 Viewing Prometheus Instance Data Through Grafana**.

8.5 Configuring Service Discovery

8.5.1 Configuring Metrics

You can view the metrics of a default Prometheus instance, or a Prometheus instance for CCE or 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 **8.2.3 Prometheus Instance for CCE**.
- Both your service and cloud services have been connected to a Prometheus instance for cloud services. For details, see **8.2.1 Prometheus Instance for Cloud Services**.

Precautions

- Only the default Prometheus instance, and Prometheus instance for CCE or cloud services support the functions of viewing, 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 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.

Viewing the Metrics of a Prometheus Instance of 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 **Service Discovery**. On the **Metrics** tab page, view 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 8-14 Metric parameters

Parameter	Description
Metric Name	Name of a metric.

Parameter	Description
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

Viewing the Metrics of a Prometheus Instance of 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 **Service Discovery**. Then view 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 8-15 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. That is, the type of the connected cloud service.

----End

Viewing 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 **Service Discovery**. Then view 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 8-16 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 8-17** if needed.

Table 8-17 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	• 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.

8.5.2 Configuring Service Discovery 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 **8.2.3 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.

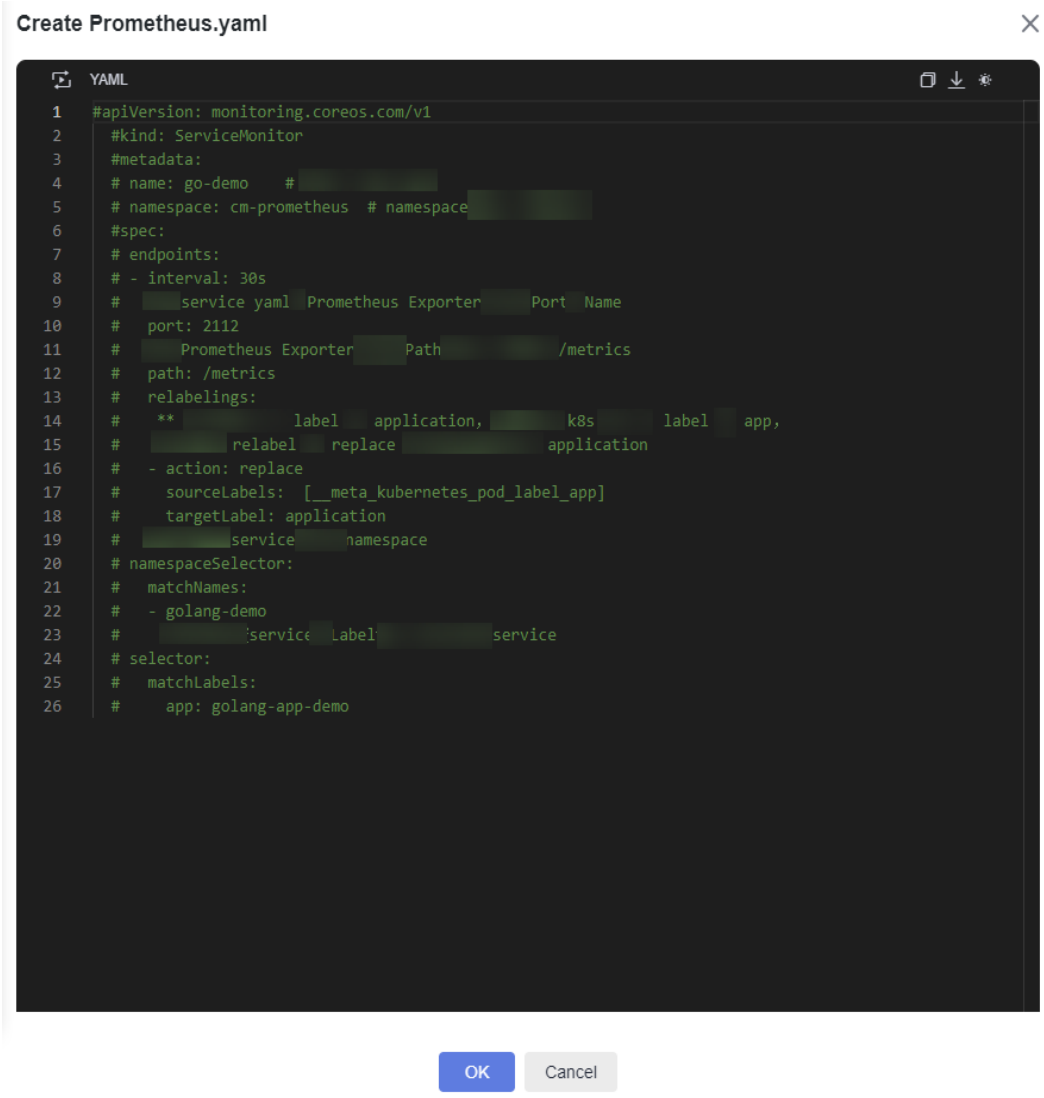
Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

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

Step 4 In the navigation pane on the left, choose **Service Discovery**. On the **Settings** tab page, click **ServiceMonitor**.

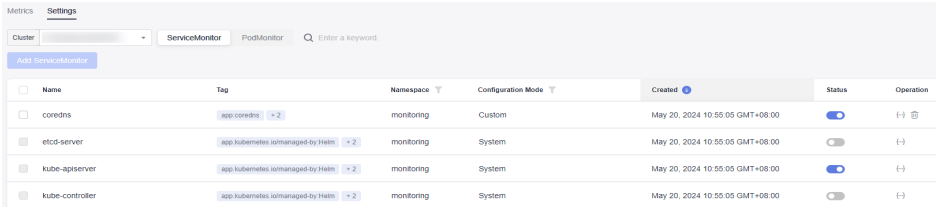
Step 5 Click **Add ServiceMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 8-12 Adding ServiceMonitor



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

Figure 8-13 Configuring a collection rule



----End

Adding PodMonitor

Step 1 Log in to the AOM 2.0 console.

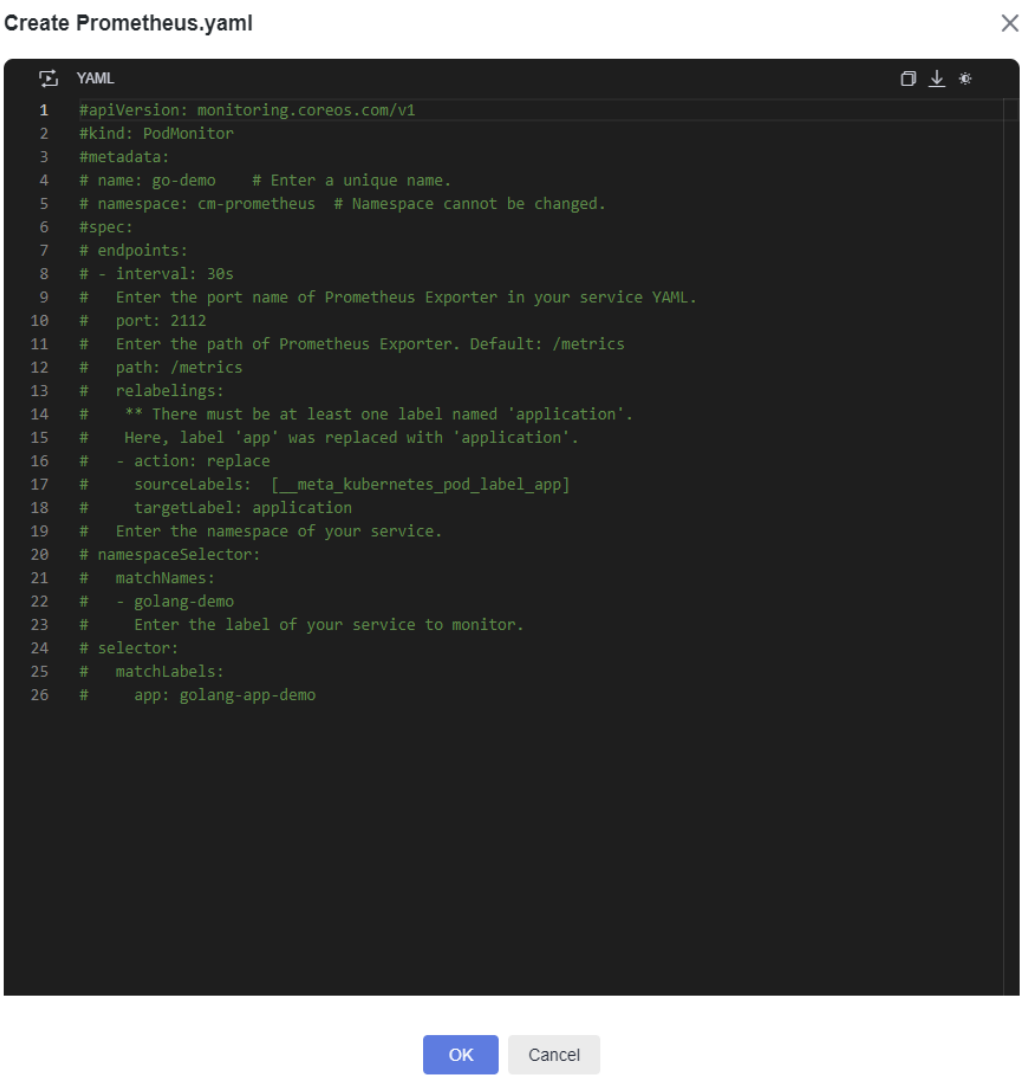
Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**.

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

Step 4 In the navigation pane on the left, choose **Service Discovery**. On the **Settings** tab page, click **PodMonitor**.

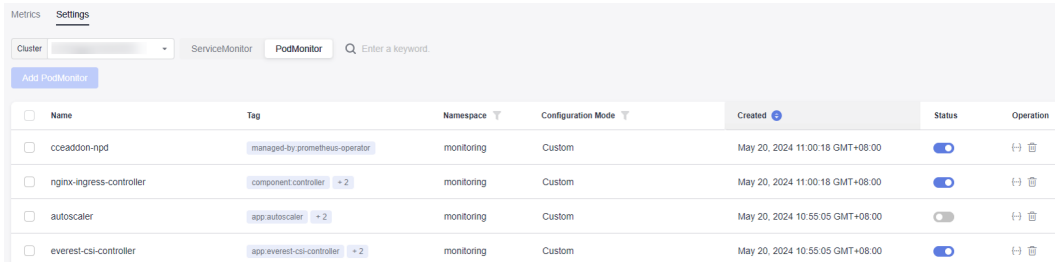
Step 5 Click **Add PodMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 8-14 Adding PodMonitor



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

Figure 8-15 Configuring a collection rule



----End

More Operations

Perform the operations listed in **Table 8-18** if needed.

Table 8-18 Related operations

Operation	Description
Viewing service discovery	• In the service discovery list, view 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	On the **Settings** tab page of the **Service Discovery** page, click in the **Status** column to enable or disable collection rules. indicates that collection rules are disabled. indicates that collection rules are enabled.
Deleting service discovery	Click in the **Operation** column.

8.6 Access Guide

8.6.1 Connecting Self-Built Middleware in the CCE Container Scenario

8.6.1.1 Connecting PostgreSQL Exporter

Application Scenario

When using PostgreSQL, you need to monitor their status and locate their faults in a timely manner. The Prometheus monitoring function monitors PostgreSQL

running using Exporter in the CCE container scenario. This section describes how to deploy PostgreSQL Exporter and implement alarm access.

Prerequisites

- A CCE cluster has been created and PostgreSQL has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **postgres_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying PostgreSQL Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Use **Secret** to manage PostgreSQL passwords.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create from YAML** to configure a YAML file. In the YAML file, use Kubernetes **Secret** to manage and encrypt passwords. When starting PostgreSQL Exporter, the secret key can be directly used but the corresponding password needs to be changed as required.

   YAML configuration example:

   ```
   apiVersion: v1
   kind: Secret
   metadata:
     name: postgres-test
   type: Opaque
   stringData:
     username: postgres
     password: you-guess # PostgreSQL password.
   ```

2. Deploy PostgreSQL Exporter.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create from YAML** to deploy Exporter.

   YAML configuration example (Change the parameters if needed):

   ```
   apiVersion: apps/v1
   kind: Deployment
   metadata:
    name: postgres-test # Change the name based on requirements. You are advised to add the
   PostgreSQL instance information.
    namespace: default # Must be the same as the namespace of the PostgreSQL service.
    labels:
      app: postgres
      app.kubernetes.io/name: postgresql
   spec:
    replicas: 1
    selector:
      matchLabels:
        app: postgres
        app.kubernetes.io/name: postgresql
    template:
      metadata:
        labels:
          app: postgres
   ```



```
      app.kubernetes.io/name: postgresql
  spec:
    containers:
    - name: postgres-exporter
      image: swr.cn-north-4.myhuaweicloud.com/aom-exporter/postgres-exporter:v0.8.0 # postgres-
exporter image uploaded to SWR.
      args:
        - "--web.listen-address=:9187" # Enabled port of Exporter.
        - "--log.level=debug" # Log level.
      env:
        - name: DATA_SOURCE_USER
          valueFrom:
            secretKeyRef:
              name: postgres-test # Secret name specified in the previous step.
              key: username  # Secret key specified in the previous step.
        - name: DATA_SOURCE_PASS
          valueFrom:
            secretKeyRef:
              name: postgres-test # Secret name specified in the previous step.
              key: password  # Secret key specified in the previous step.
        - name: DATA_SOURCE_URI
          value: "x.x.x.x:5432/postgres?sslmode=disable"  # Connection information.
      ports:
      - name: http-metrics
        containerPort: 9187
```

3. Obtain metrics.

   The running time of the Postgres instance cannot be obtained by running the **curl http://exporter:9187/metrics** command. To obtain this metric, customize a **queries.yaml** file.

   a. Create a configuration that contains **queries.yaml**.

   b. Mount the configuration as a volume to a directory of Exporter.

   c. Use the configuration through **extend.query-path**. The following shows **Secret** and **Deployment**:

```
# The following shows the queries.yaml file that contains custom metrics:
---
apiVersion: v1
kind: ConfigMap
metadata:
  name: postgres-test-configmap
  namespace: default
data:
  queries.yaml: |
    pg_postmaster:
      query: "SELECT pg_postmaster_start_time as start_time_seconds from
pg_postmaster_start_time()"
      master: true
      metrics:
        - start_time_seconds:
            usage: "GAUGE"
            description: "Time at which postmaster started"

# The following shows the mounted Secret and ConfigMap, and defines Exporter deployment
parameters (such as the image):
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres-test
  namespace: default
  labels:
    app: postgres
    app.kubernetes.io/name: postgresql
spec:
  replicas: 1
  selector:
```

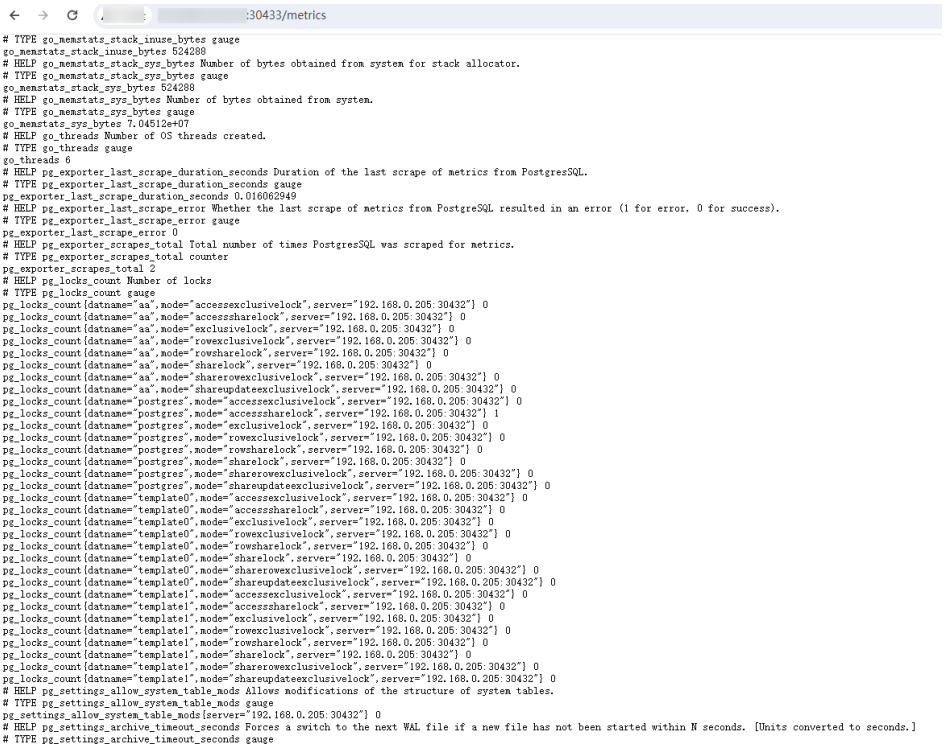


```
    matchLabels:
      app: postgres
      app.kubernetes.io/name: postgresql
  template:
    metadata:
      labels:
        app: postgres
        app.kubernetes.io/name: postgresql
    spec:
      containers:
        - name: postgres-exporter
          image: wrouesnel/postgres_exporter:latest
          args:
            - "--web.listen-address=:9187"
            - "--extend.query-path=/etc/config/queries.yaml"
            - "--log.level=debug"
          env:
            - name: DATA_SOURCE_USER
              valueFrom:
                secretKeyRef:
                  name: postgres-test-secret
                  key: username
            - name: DATA_SOURCE_PASS
              valueFrom:
                secretKeyRef:
                  name: postgres-test-secret
                  key: password
            - name: DATA_SOURCE_URI
              value: "x.x.x.x:5432/postgres?sslmode=disable"
          ports:
            - name: http-metrics
              containerPort: 9187
          volumeMounts:
            - name: config-volume
              mountPath: /etc/config
      volumes:
        - name: config-volume
          configMap:
            name: postgres-test-configmap
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  type: NodePort
  selector:
    app: postgres
    app.kubernetes.io/name: postgresql
  ports:
    - protocol: TCP
      nodePort: 30433
      port: 9187
      targetPort: 9187
```

d. Access the following address:

   http://*{Public IP address of any node in the cluster}***:30433/metrics**. You can then use the custom **queries.yaml** file to query the Postgres instance startup time.

Figure 8-16 Accessing a cluster node



----End

Adding a Collection Task

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

NOTE

In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: postgres-exporter
  namespace: default
spec:
  namespaceSelector:
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s
    path: /metrics
    port: http-metrics
  selector:
    matchLabels:
      app: postgres
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**postgres-exporter** to query metrics starting with **pg**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.2 Connecting MySQL Exporter

Application Scenario

MySQL Exporter collects MySQL database metrics. Core database metrics collected through Exporter are used for alarm reporting and dashboard display. Currently, Exporter supports MySQL 5.6 or later. If the MySQL version is earlier than 5.6, some metrics may fail to be collected.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

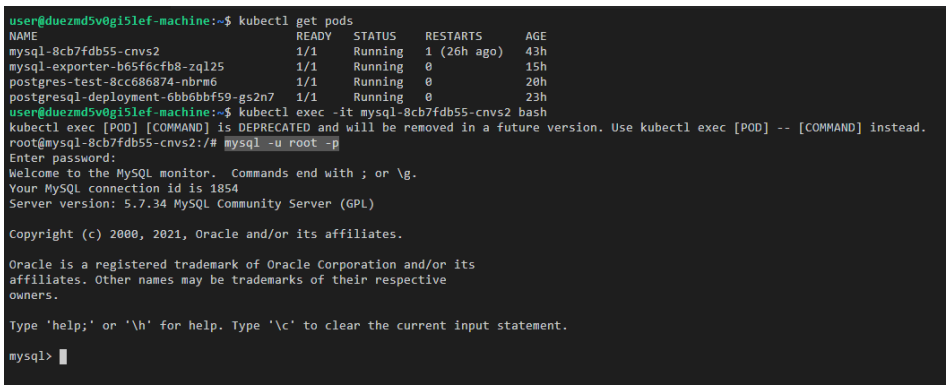
- A CCE cluster has been created and MySQL has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **mysql_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Database Authorization

Step 1 Log in to the cluster and run the following command:

```
kubectl exec -it ${mysql_podname} bash
mysql -u root -p
```

Figure 8-17 Executing the command



Step 2 Log in to the database and run the following command:

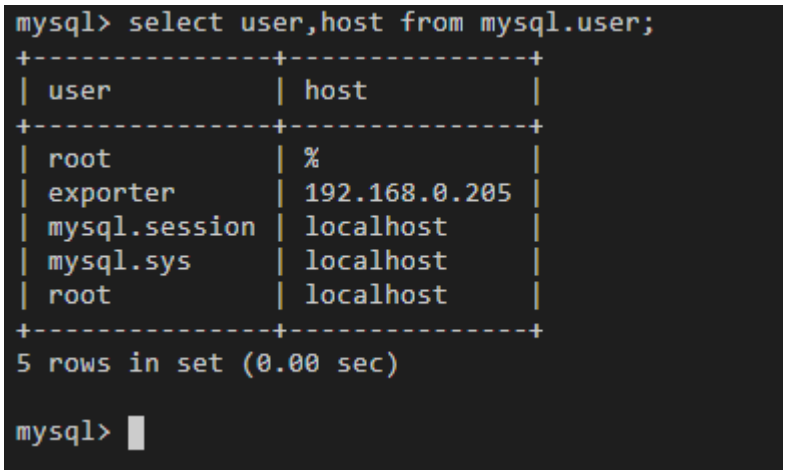
```
CREATE USER 'exporter'@'x.x.x.x(hostip)' IDENTIFIED BY 'xxxx(password)' WITH MAX_USER_CONNECTIONS 3;
GRANT PROCESS, REPLICATION CLIENT, SELECT ON *.* TO 'exporter'@'x.x.x.x(hostip)';
```

Step 3 Check whether the authorization is successful.

Enter the following SQL statement to check whether there is any Exporter data. *host* indicates the IP address of the node where the MySQL database is located.

```
select user,host from mysql.user;
```

Figure 8-18 SQL statement



----End

Deploying MySQL Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Use **Secret** to manage MySQL connection strings.

   In the navigation pane, choose **ConfigMaps and Secrets**. In the upper right corner, click **Create from YAML** and enter the following **.yml** file. The password is encrypted based on Opaque requirements.

```
apiVersion: v1
kind: Secret
metadata:
    name: mysql-secret
    namespace: default
type: Opaque
stringData:
    datasource: "user:password@tcp(ip:port)/" # MySQL connection string, which needs to be encrypted.
```

   NOTE

   For details about how to configure a secret, see **Creating a Secret**.

2. Deploy MySQL Exporter.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create Workload**. Then select the **Deployment** workload and select a desired namespace to deploy MySQL Exporter. YAML configuration example for deploying Exporter:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    k8s-app: mysql-exporter # Change the name based on service requirements. You are advised to add the MySQL instance information, for example, ckafka-2vrgx9fd-mysql-exporter.
  name: mysql-exporter # Change the name based on service requirements. You are advised to add the MySQL instance information, for example, ckafka-2vrgx9fd-mysql-exporter.
  namespace: default # Must be the same as the namespace of MySQL.
spec:
  replicas: 1
  selector:
    matchLabels:
      k8s-app: mysql-exporter # Change the name based on service requirements. You are advised to add the MySQL instance information, for example, ckafka-2vrgx9fd-mysql-exporter.
  template:
    metadata:
      labels:
        k8s-app: mysql-exporter # Change the name based on service requirements. You are advised to add the MySQL instance information, for example, ckafka-2vrgx9fd-mysql-exporter.
    spec:
      containers:
      - env:
        - name: DATA_SOURCE_NAME
          valueFrom:
            secretKeyRef:
              name: mysql-secret
              key: datasource
        image: swr.cn-north-4.myhuaweicloud.com/aom-exporter/mysqld-exporter:v0.12.1
        imagePullPolicy: IfNotPresent
        name: mysql-exporter
        ports:
        - containerPort: 9104
          name: metric-port
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      imagePullSecrets:
      - name: default-secret
      restartPolicy: Always
      schedulerName: default-scheduler
```



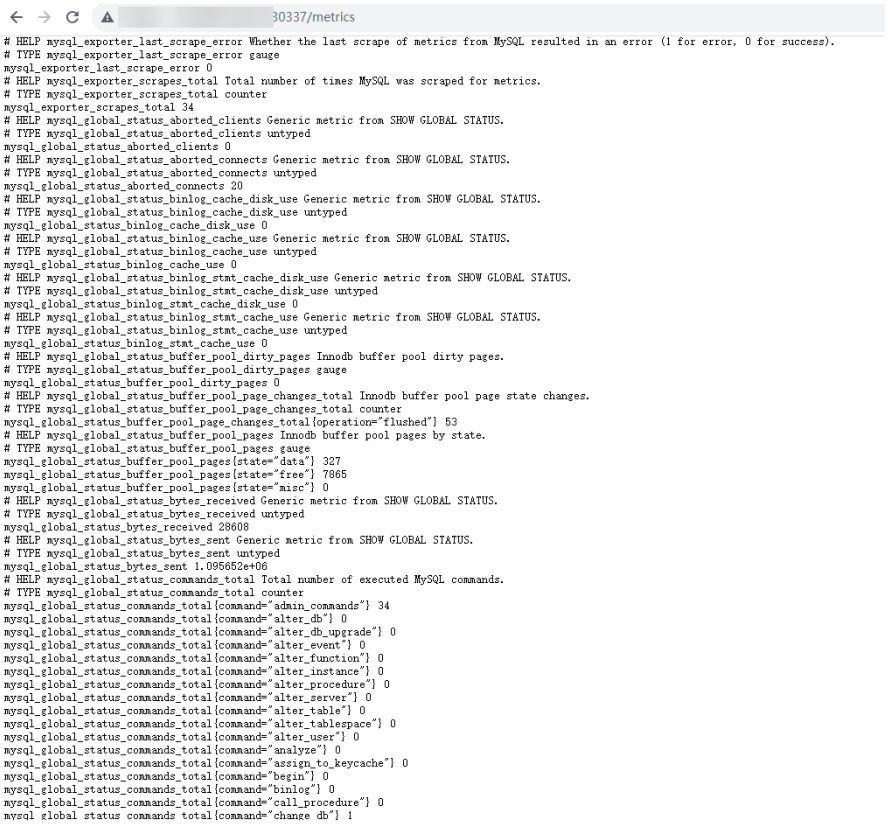
```
    securityContext: {}
    terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: mysql-exporter
spec:
  type: NodePort
  selector:
    k8s-app: mysql-exporter
  ports:
    - protocol: TCP
      nodePort: 30337
      port: 9104
      targetPort: 9104
```

NOTE

For details about Exporter parameters, see **mysql-exporter**.

3. Check whether MySQL Exporter is successfully deployed.
   a. On the **Deployments** tab page, click the Deployment created in **Step 3.2**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.
   b. Perform verification using one of the following methods:
      - Log in to a cluster node and run either of the following commands:
        curl http://*{Cluster IP address}***:9104/metrics**
        curl http://*{Private IP address of any node in the cluster}***:30337/metrics**
      - In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:
        curl http://localhost:9104/metric
      - Access **http://***{Public IP address of any node in the cluster}***:30337/metrics**.

Figure 8-19 Accessing a cluster node



----End

Collecting Service Data of the CCE Cluster

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

Configuration information:

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: mysql-exporter
  namespace: default
spec:
  namespaceSelector:
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s
    path: /metrics
    port: metric-port
  selector:
    matchLabels:
      k8s-app: mysql-exporter
```

NOTE

In this example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**mysql-exporter** to query custom metrics starting with **mysql**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.3 Connecting Kafka Exporter

Application Scenario

When using Kafka, you need to monitor their running, for example, checking the cluster status and whether messages are stacked. The Prometheus monitoring function monitors Kafka running using Exporter in the CCE container scenario. This section describes how to deploy Kafka Exporter and implement alarm access.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

- A CCE cluster has been created and Kafka has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.

- You have uploaded the **kafka_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying Kafka Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Deploy Kafka Exporter.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create Workload**. Then select the **Deployment** workload and select a desired namespace to deploy Kafka Exporter. YAML configuration example for deploying Exporter:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    k8s-app: kafka-exporter # Change the name based on service requirements. You are advised to add the Kafka instance information, for example, ckafka-2vrgx9fd-kafka-exporter.
  name: kafka-exporter # Change the name based on service requirements. You are advised to add the Kafka instance information, for example, ckafka-2vrgx9fd-kafka-exporter.
  namespace: default # Namespace of an existing cluster
spec:
  replicas: 1
  selector:
    matchLabels:
      k8s-app: kafka-exporter # Change the name based on service requirements. You are advised to add the Kafka instance information, for example, ckafka-2vrgx9fd-kafka-exporter.
  template:
    metadata:
      labels:
        k8s-app: kafka-exporter # Change the name based on service requirements. You are advised to add the Kafka instance information, for example, ckafka-2vrgx9fd-kafka-exporter.
    spec:
      containers:
      - args:
        - --kafka.server=120.46.215.4:30092 # Address of the Kafka instance
        image: swr.cn-north-4.myhuaweicloud.com/mall-swarm-demo/kafka-exporter:latest
        imagePullPolicy: IfNotPresent
        name: kafka-exporter
        ports:
        - containerPort: 9308
          name: metric-port # Required when you configure a capture task
        securityContext:
          privileged: false
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      imagePullSecrets:
      - name: default-secret
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: kafka-exporter
spec:
  type: NodePort
```



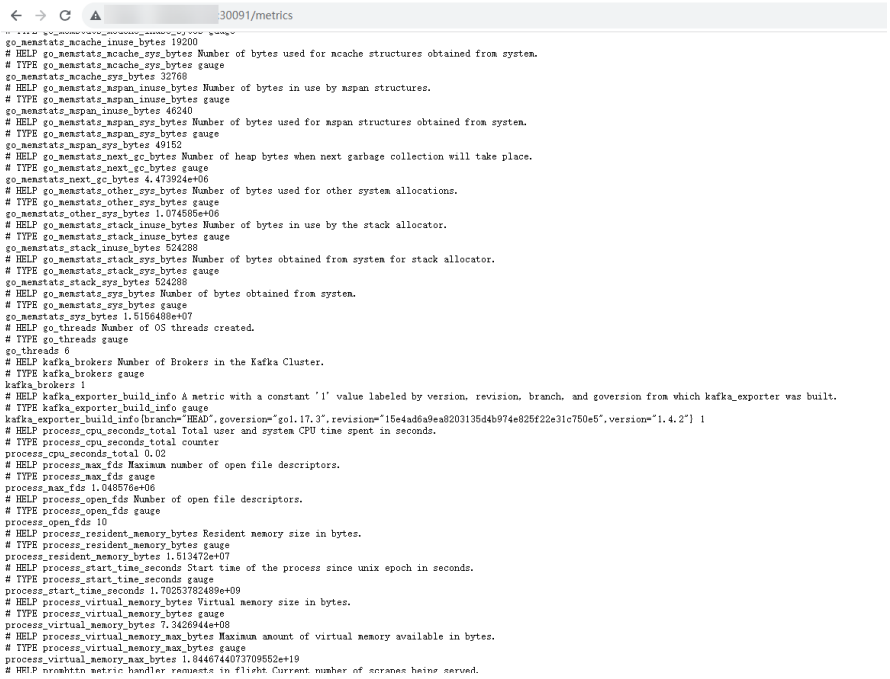
```
selector:
  k8s-app: kafka-exporter
ports:
  - protocol: TCP
    nodePort: 30091
    port: 9308
    targetPort: 9308
```

NOTE

For more details about Exporter parameters, see **kafka-exporter**.

2. Check whether Kafka Exporter is successfully deployed.
   a. On the **Deployments** tab page, click the Deployment created in **Step 3.1**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.
   b. Perform verification using one of the following methods:
      - Log in to a cluster node and run either of the following commands:
        curl http://*{Cluster IP address}***:9308/metrics**
        curl http://*{Private IP address of any node in the cluster}***:30091/metrics**
      - In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:
        curl http://localhost:9308/metric
      - Access **http://***{Public IP address of any node in the cluster}***:30091/metrics**.

        Figure 8-20 Accessing a cluster node

----End

Collecting Service Data of the CCE Cluster

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

> **NOTE**
>
> In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

Configuration information:

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: kafka-exporter
  namespace: default
spec:
  namespaceSelector:
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s
    path: /metrics
    port: metric-port
  selector:
    matchLabels:
      k8s-app: kafka-exporter
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**kafka-exporter** to query custom metrics starting with **kafka**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.4 Connecting Memcached Exporter

Application Scenario

When using Memcached, you need to monitor their running and locate their faults in a timely manner. The Prometheus monitoring function monitors Memcached running using Exporter in the CCE container scenario. This section describes how to monitor Memcached.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

- A CCE cluster has been created and Memcached has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **memcached_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying Memcached Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Configure a secret.

   In the navigation pane, choose **ConfigMaps and Secrets**. Then click **Create from YAML** in the upper right corner of the page. YAML configuration example:

   ```
   apiVersion: v1
   kind: Secret
   metadata:
     name: memcached-exporter-secret
     namespace: default
   type: Opaque
   stringData:
     memcachedURI: 120.46.215.4:11211  # Memcached address
   ```

   NOTE

   - Format of the Memcached connection string: **http://***{ip}*:*{port}*.
   - For details about how to configure a secret, see **Creating a Secret**.

2. Deploy Memcached Exporter.

   In the navigation pane, choose **Workloads**. On the **Deployments** tab page, click **Create from YAML** in the upper right corner and then configure a YAML file to deploy Exporter.

   YAML configuration example:

   ```
   apiVersion: apps/v1
   kind: Deployment
   metadata:
    labels:
   ```



```
    k8s-app: memcached-exporter # Change the value based on service requirements.
  name: memcached-exporter # Change the value based on service requirements.
  namespace: default
spec:
  replicas: 1
  selector:
    matchLabels:
      k8s-app: memcached-exporter # Change the value based on service requirements.
  template:
    metadata:
      labels:
        k8s-app: memcached-exporter # Change the value based on service requirements.
    spec:
      containers:
      - env:
          - name: Memcached_Url
            valueFrom:
              secretKeyRef:
                name: memcached-exporter-secret # Secret name specified in the previous step.
                key: memcachedURI # Secret key specified in the previous step.
          - name: Memcached_ALL
            value: "true"
        image: swr.cn-east-3.myhuaweicloud.com/aom-org/bitnami/memcached-exporter:0.13.0 #
Image uploaded to SWR, as described in "Prerequisites".
        imagePullPolicy: IfNotPresent
        name: memcached-exporter
        ports:
        - containerPort: 9150
          name: metric-port
        securityContext:
          privileged: false
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
    dnsPolicy: ClusterFirst
    imagePullSecrets:
    - name: default-secret
    restartPolicy: Always
    schedulerName: default-scheduler
    securityContext: {}
    terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: memcached-exporter
spec:
  type: NodePort
  selector:
    k8s-app: memcached-exporter
  ports:
    - protocol: TCP
      nodePort: 30122
      port: 9150
      targetPort: 9150
```

NOTE

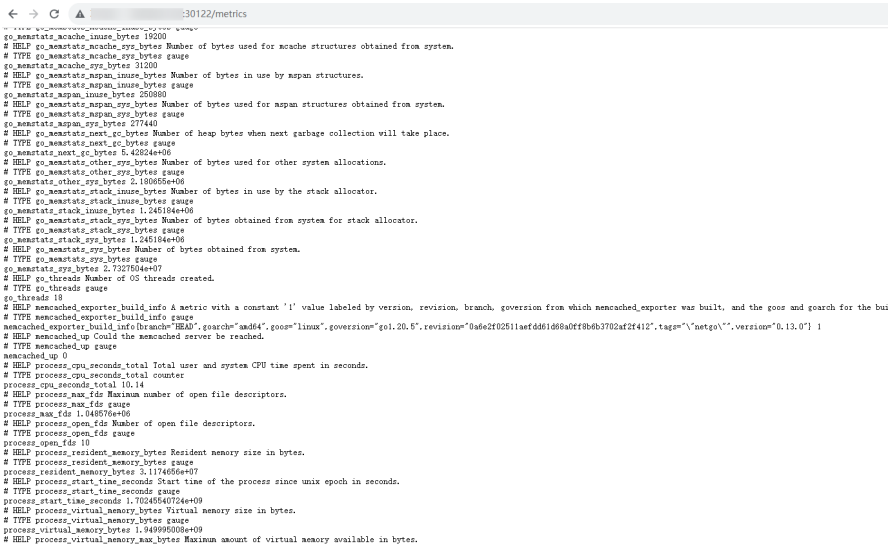
For more details about Exporter parameters, see **memcached_exporter**.

3. Check whether Memcached Exporter is successfully deployed.
   a. On the **Deployments** tab page, click the Deployment created in **Step 3.2**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.
   b. Perform verification using one of the following methods:
      - Log in to a cluster node and run either of the following commands:
        curl http://*{Cluster IP address}***:9150/metrics**


```
curl http://{Private IP address of any node in the cluster}:30122/metrics
```

- Access **http://*{Public IP address of any node in the cluster}*:30122/metrics**.

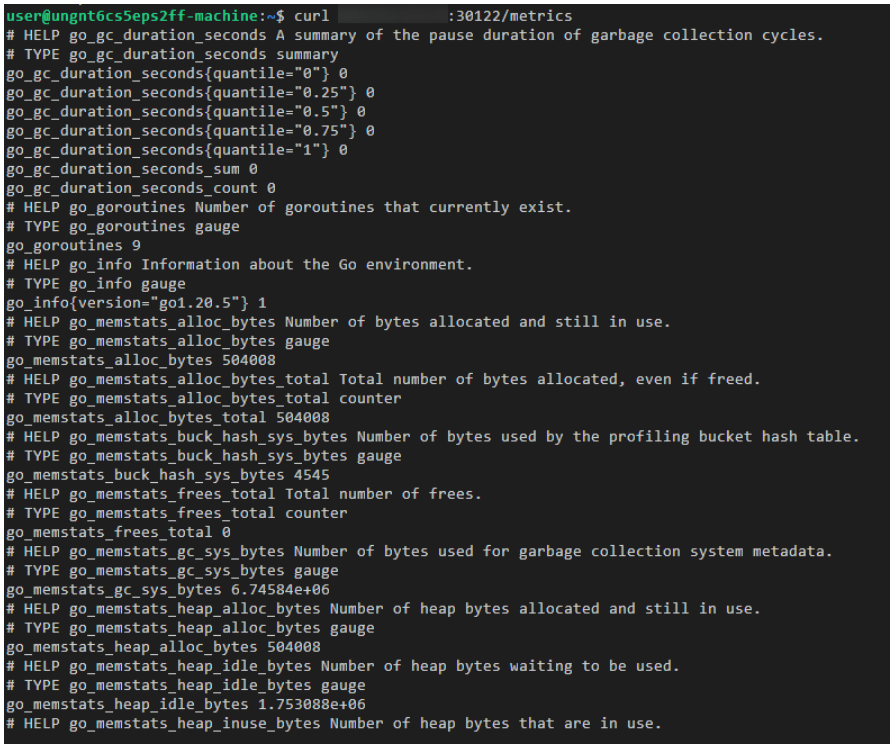
Figure 8-21 Accessing a cluster node



- In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:

```
curl http://localhost:9150/metric
```

Figure 8-22 Executing the command



----End

Adding a Collection Task

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

NOTE

In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: memcached-exporter
  namespace: default
spec:
  namespaceSelector:
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s
    path: /metrics
    port: metric-port
  selector:
    matchLabels:
      k8s-app: memcached-exporter
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**memcached-exporter** to query metrics starting with **go_memstats**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.

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

c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.5 Connecting MongoDB Exporter

Application Scenario

When using MongoDB, you need to monitor MongoDB running and locate their faults in a timely manner. The Prometheus monitoring function monitors MongoDB running using Exporter in the CCE container scenario. This section describes how to deploy MongoDB Exporter and implement alarm access.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

- A CCE cluster has been created and MongoDB has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **mongodb_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying MongoDB Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Configure a secret.

   In the navigation pane, choose **ConfigMaps and Secrets**. Then click **Create from YAML** in the upper right corner of the page. YAML configuration example:

   ```
   apiVersion: v1
   kind: Secret
   metadata:
     name: mongodb-secret-test
     namespace: default
   type: Opaque
   stringData:
     datasource: "mongodb://{user}:{passwd}@{host1}:{port1},{host2}:{port2},{host3}:{port3}/admin"  # Corresponding URI.
   ```

   NOTE

   - The password has been encrypted based on Opaque requirements.
   - For details about how to configure a secret, see **Creating a Secret**.

2. Deploy MongoDB Exporter.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create Workload**. Then select the **Deployment** workload and select a desired

namespace to deploy MongoDB Exporter. YAML configuration example for deploying Exporter:

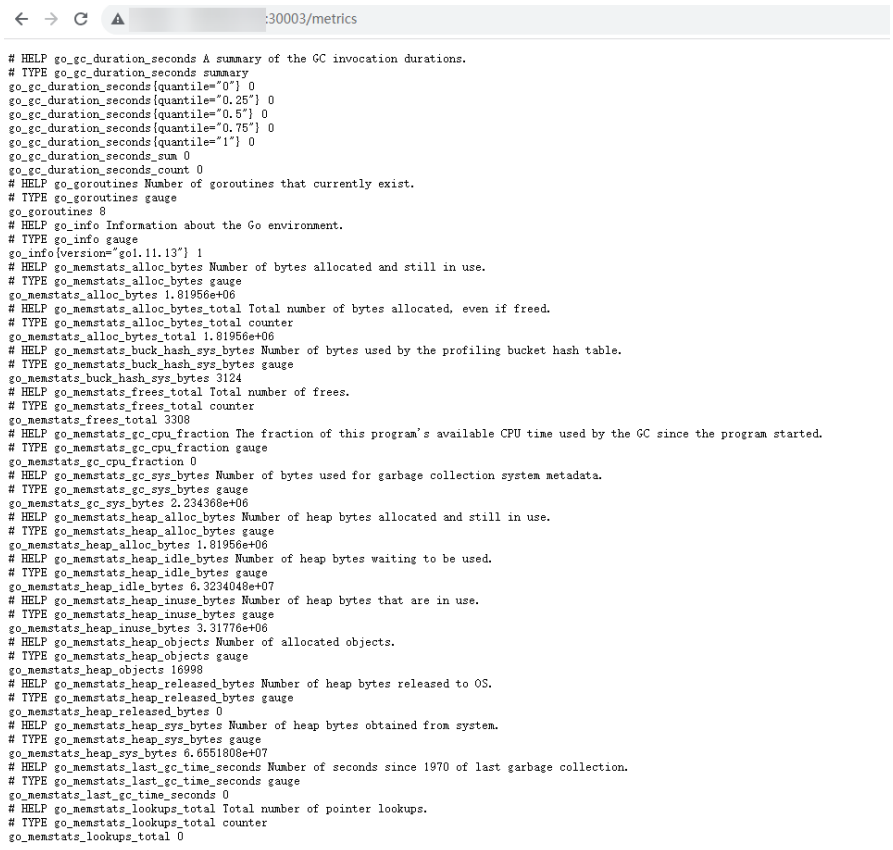
```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    k8s-app: mongodb-exporter # Change the value based on service requirements. You are advised to add the MongoDB instance information.
  name: mongodb-exporter # Change the value based on service requirements. You are advised to add the MongoDB instance information.
  namespace: default #Must be the same as the namespace of MongoDB.
spec:
  replicas: 1
  selector:
    matchLabels:
      k8s-app: mongodb-exporter # Change the value based on service requirements. You are advised to add the MongoDB instance information.
  template:
    metadata:
      labels:
        k8s-app: mongodb-exporter # Change the value based on service requirements. You are advised to add the MongoDB instance information.
    spec:
      containers:
        - args:
            - --collect.database       # Enable collection of database metrics.
            - --collect.collection     # Enable collection of metric sets.
            - --collect.topmetrics     # Enable collection of database header metrics.
            - --collect.indexusage     # Enable collection of index usage statistics.
            - --collect.connpoolstats  # Enable collection of MongoDB connection pool statistics.
          env:
            - name: MONGODB_URI
              valueFrom:
                secretKeyRef:
                  name: mongodb-secret-test
                  key: datasource
          image: swr.cn-north-4.myhuaweicloud.com/mall-swarm-demo/mongodb-exporter:0.10.0
          imagePullPolicy: IfNotPresent
          name: mongodb-exporter
          ports:
            - containerPort: 9216
              name: metric-port  # Required when you configure a capture task.
          securityContext:
            privileged: false
          terminationMessagePath: /dev/termination-log
          terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      imagePullSecrets:
        - name: default-secret
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: { }
      terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: mongodb-exporter
spec:
  type: NodePort
  selector:
    k8s-app: mongodb-exporter
  ports:
    - protocol: TCP
      nodePort: 30003
      port: 9216
      targetPort: 9216
```


NOTE

For more details about Exporter parameters, see **mongodb_exporter**.

3. Check whether MongoDB Exporter is successfully deployed.
   a. On the **Deployments** tab page, click the Deployment created in **Step 3.2**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.
   b. Perform verification using one of the following methods:
      - Log in to a cluster node and run either of the following commands:
        curl http://*{Cluster IP address}***:9216/metrics**
        curl http://*{Private IP address of any node in the cluster}***:30003/metrics**
      - Access **http://***{Public IP address of any node in the cluster}***:30003/metrics**.

        Figure 8-23 Accessing a cluster node

      - In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:
        curl http://localhost:9216/metric

----End

Collecting Service Data of the CCE Cluster

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

> **NOTE**
>
> In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: mongodb-exporter
  namespace: default
spec:
  namespaceSelector:
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s
    path: /metrics
    port: metric-port
  selector:
    matchLabels:
      k8s-app: mongodb-exporter
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**MongoDB-exporter** to query custom metrics starting with **mongodb**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.6 Connecting Elasticsearch Exporter

Application Scenario

When using Elasticsearch, you need to monitor Elasticsearch running, such as the cluster and index status. The Prometheus monitoring function monitors Elasticsearch running using Exporter in the CCE container scenario. This section describes how to deploy Elasticsearch Exporter and implement alarm access.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

- A CCE cluster has been created and Elasticsearch has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **elasticsearch_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying Elasticsearch Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. Configure a secret.

   In the navigation pane, choose **ConfigMaps and Secrets**. Then click **Create from YAML** in the upper right corner of the page. The following shows a YAML configuration example:

   ```
   apiVersion: v1
   kind: Secret
   metadata:
     name: es-secret-test
     namespace: default
   type: Opaque
   stringData:
     esURI: http://124.70.14.51:30920 # URI of Elasticsearch. Use the IP address of the cluster or any node in the cluster.
   ```

   NOTE

   - Format of the Elasticsearch connection string: *<proto>*://*<user>*:*<password>*@*<host>*:*<port>*, for example, **http://admin:pass@localhost:9200**. You can also leave the password blank, for example, **http://10.247.43.50:9200**.
   - The password has been encrypted based on Opaque requirements.
   - For details about how to configure a secret, see **Creating a Secret**.

2. Deploy Elasticsearch Exporter.

   In the navigation pane, choose **Workloads**. In the upper right corner, click **Create Workload**. Then select the **Deployment** workload and a desired

namespace to deploy Elasticsearch Exporter. YAML configuration example for deploying Exporter:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    k8s-app: es-exporter # Change the value based on service requirements.
  name: es-exporter # Change the value based on service requirements.
  namespace: default #Select a proper namespace to deploy Exporter. If no namespace is available,
create one.
spec:
  replicas: 1
  selector:
    matchLabels:
      k8s-app: es-exporter # Change the value based on service requirements.
  template:
    metadata:
      labels:
        k8s-app: es-exporter # Change the value based on service requirements.
    spec:
      containers:
      - env:
          - name: ES_URI
            valueFrom:
              secretKeyRef:
                name: es-secret-test # Secret name specified in the previous step.
                key: esURI # Secret key specified in the previous step.
          - name: ES_ALL
            value: "true"
        image: swr.cn-north-4.myhuaweicloud.com/mall-swarm-demo/es-exporter:1.1.0
        imagePullPolicy: IfNotPresent
        name: es-exporter
        ports:
        - containerPort: 9114
          name: metric-port
        securityContext:
          privileged: false
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      imagePullSecrets:
      - name: default-secret
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: es-exporter
  name-space: default # Must be the same as the namespace where Exporter is deployed.
spec:
  type: NodePort
  selector:
    k8s-app: es-exporter
  ports:
    - protocol: TCP
      nodePort: 30921
      port: 9114
      targetPort: 9114
```

NOTE

In the preceding example, **ES_ALL** is used to collect all Elasticsearch monitoring items. You can change parameters if needed. For more details about Exporter parameters, see **elasticsearch_exporter**.

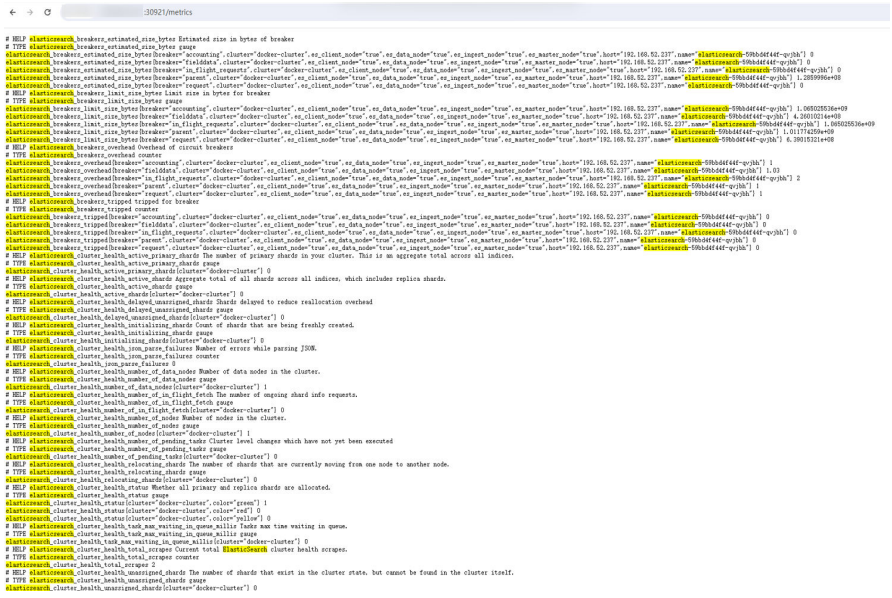
3. Check whether Elasticsearch Exporter is successfully deployed.

a. On the **Deployments** tab page, click the Deployment created in **Step 3.2**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.

b. Perform verification using one of the following methods:

- Log in to a cluster node and run either of the following commands:
  curl http://*{Cluster IP address}***:9114/metrics**
  curl http://*{Private IP address of any node in the cluster}***:30921/metrics**
- Access **http://***{Public IP address of any node in the cluster}***:30921/metrics**.

  Figure 8-24 Accessing a cluster node

- In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:
  curl http://localhost:9114/metric

----End

Collecting Service Data of the CCE Cluster

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

NOTE

In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: elasticSearch-exporter
  namespace: default
spec:
  namespaceSelector: # Select the namespace where Exporter is deployed.
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
```



```
  - interval: 30s # Set the metric collection period.
    path: /metrics # Enter the path corresponding to Prometheus Exporter. Default: /metrics.
port: metric-port #Enter the name of "ports" in the YAML file corresponding to Prometheus Exporter.
  selector: # Enter the label of the target Exporter pod.
    matchLabels:
      k8s-app: elasticSearch-exporter
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Select job *{namespace}*/**elasticsearch-exporter** to query custom metrics starting with **elasticsearch**.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.7 Connecting Redis Exporter

Application Scenario

When using Redis, you need to monitor Redis running and locate their faults in a timely manner. The Prometheus monitoring function monitors Redis running using Exporter in the CCE container scenario. This section describes how to monitor Redis.

NOTE

You are advised to use CCE for unified Exporter management.

Prerequisites

- A CCE cluster has been created and Redis has been installed.
- Your service has been connected for Prometheus monitoring and a CCE cluster has also been connected. For details, see **Prometheus Instance for CCE**.
- You have uploaded the **redis_exporter** image to SoftWare Repository for Container (SWR). For details, see **Uploading an Image Through a Container Engine Client**.

Deploying Redis Exporter

Step 1 Log in to the CCE console.

Step 2 Click the connected cluster. The cluster management page is displayed.

Step 3 Perform the following operations to deploy Exporter:

1. In the navigation pane, choose **ConfigMaps and Secrets**. Switch to the **Secrets** tab. Then click **Create from YAML** in the upper right corner of the page. The following shows a YAML configuration example:

```
apiVersion: v1
kind: Secret
metadata:
  name: redis-secret-test
  namespace: default # Must be the same as the namespace where Exporter is deployed.
type: Opaque
stringData:
  password: redis123  # Redis password.
```

NOTE

   - The password has been encrypted based on Opaque requirements.
   - For details about how to configure a secret, see **Creating a Secret**.

2. Deploy Redis Exporter.

   In the navigation pane, choose **Workloads**. On the displayed page, click the **Deployments** tab, click **Create from YAML** in the upper right corner, and select a namespace. You can deploy Exporter through the console or using a YAML file. The following shows a YAML configuration example:

```
apiVersion: apps/v1
kind: Deployment
metadata:
 labels:
  k8s-app: redis-exporter # Change the value based on service requirements. You are advised to add the Redis instance information, for example, crs-66e112fp-redis-exporter.
 name: redis-exporter # Change the value based on service requirements. You are advised to add the Redis instance information, for example, crs-66e112fp-redis-exporter.
 namespace: default #Select a proper namespace to deploy Exporter. If no namespace is available, create one.
spec:
 replicas: 1
 selector:
  matchLabels:
   k8s-app: redis-exporter # Change the name based on service requirements. You are advised to add the Redis instance information, for example, crs-66e112fp-redis-exporter.
 template:
  metadata:
   labels:
    k8s-app: redis-exporter # Change the name based on service requirements. You are advised to add the Redis instance information, for example, crs-66e112fp-redis-exporter.
  spec:
   containers:
```



```
      - env:
        - name: REDIS_ADDR
          value: 120.46.215.4:30379 # IP address:port number of Redis
        - name: REDIS_PASSWORD
          valueFrom:
            secretKeyRef:
              name: redis-secret-test # Secret name specified in the previous step.
              key: password  # Secret key specified in the previous step.
        image: swr.cn-north-4.myhuaweicloud.com/mall-swarm-demo/redis-exporter:v1.32.0  # Replace
the value with the address of the image you uploaded to SWR.
        imagePullPolicy: IfNotPresent
        name: redis-exporter
        ports:
        - containerPort: 9121
          name: metric-port # Required when you configure a collection task.
        securityContext:
          privileged: false
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      imagePullSecrets:
      - name: default-secret
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      terminationGracePeriodSeconds: 30
---
apiVersion: v1
kind: Service
metadata:
  name: redis-exporter
  name-space: default # Must be the same as the namespace where Exporter is deployed.
spec:
  type: NodePort
  selector:
    k8s-app: redis-exporter
  ports:
    - protocol: TCP
      nodePort: 30378
      port: 9121
      targetPort: 9121
```

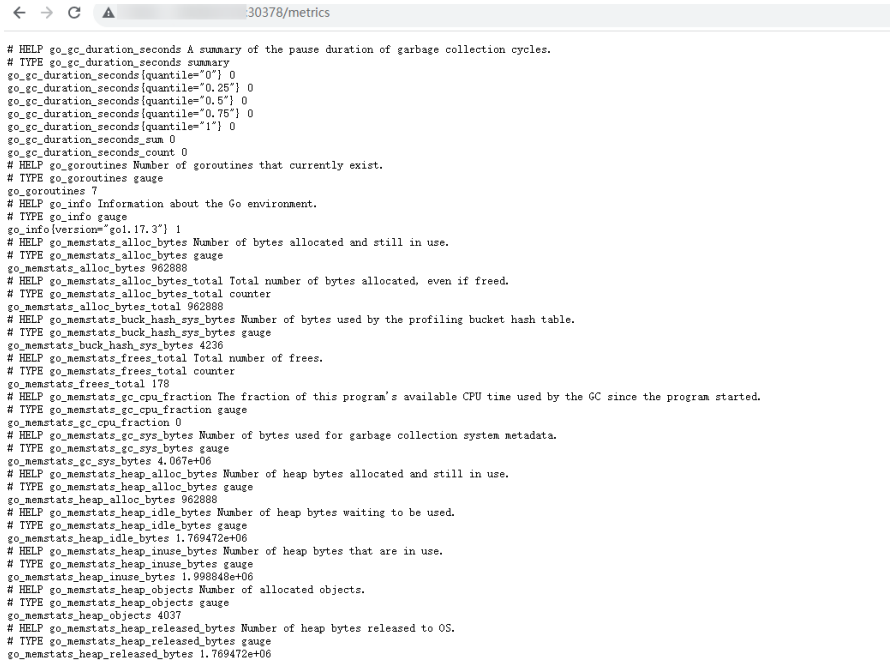
NOTE

For more details about Exporter parameters, see **redis_exporter**.

3. Check whether Redis Exporter is successfully deployed.
   a. On the **Deployments** tab page, click the Deployment created in **Step 3.2**. In the pod list, choose **More** > **View Logs** in the **Operation** column. The Exporter is successfully started and its access address is exposed.
   b. Perform verification using one of the following methods:
      - Log in to a cluster node and run either of the following commands:
        curl http://*{Cluster IP address}***:9121/metrics**
        curl http://*{Private IP address of any node in the cluster}***:30378/metrics**
      - Access **http://***{Public IP address of any node in the cluster}***:30378/metrics**.

        If no data is obtained, check whether the values of "REDIS_ADDR" and "REDIS_PASSWORD" in the YAML file set during **Redis Exporter deployment** are correct. The following shows an example:

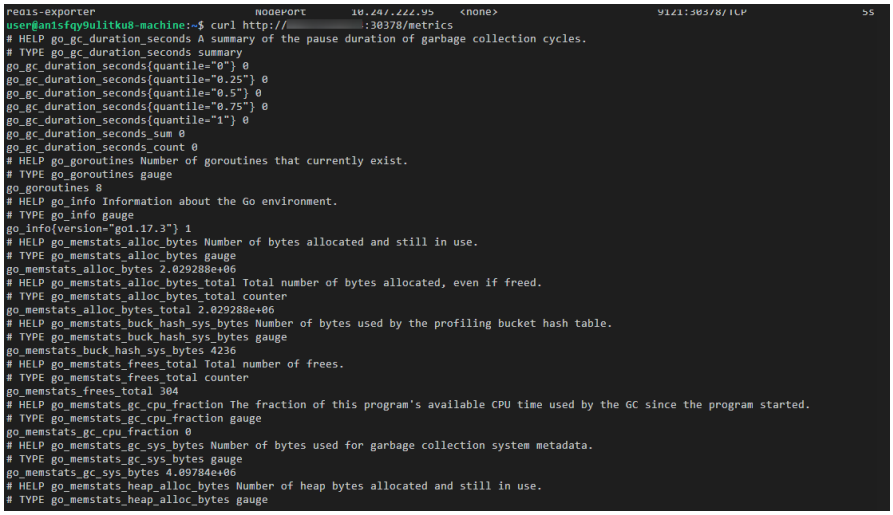
Figure 8-25 Accessing a cluster node



- In the instance list, choose **More** > **Remote Login** in the **Operation** column and run the following command:

```
curl http://localhost:9121/metrics
```

Figure 8-26 Executing the command



----End

Adding a Collection Task

Add PodMonitor to configure a collection rule for monitoring the service data of applications deployed in the CCE cluster.

NOTE

In the following example, metrics are collected every 30s. Therefore, you can check the reported metrics on the AOM page about 30s later.

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: redis-exporter
  namespace: default
spec:
  namespaceSelector: # Select the namespace where the target Exporter pod is located.
    matchNames:
      - default # Namespace where Exporter is located.
  podMetricsEndpoints:
  - interval: 30s # Set the metric collection period.
    path: /metrics # Enter the path corresponding to Prometheus Exporter. Default: metrics.
    port: metric-port# Enter the name of "ports" in the YAML file corresponding to Prometheus Exporter.
  selector: # Enter the label of the target Exporter pod.
    matchLabels:
      k8s-app: redis-exporter
```

Verifying that Metrics Can Be Reported to AOM

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 Click the Prometheus instance connected to the CCE cluster. The instance details page is displayed.

Step 4 On the **Metrics** tab page of the **Service Discovery** page, select your target cluster.

Step 5 Enter **redis** in the search box to search. If metrics starting with **redis** are displayed, the metrics are successfully connected to AOM.

----End

Setting a Dashboard and Alarm Rule on AOM

By setting a dashboard, you can monitor CCE cluster data on the same screen. By setting an alarm rule, you can detect cluster faults and implement warning in a timely manner.

- Setting a dashboard
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Dashboard**. On the displayed page, click **Add Dashboard** to add a dashboard. For details, see **Creating a Dashboard**.
  c. On the **Dashboard** page, select a Prometheus instance for CCE and click **Add Graph**. For details, see **Adding a Graph to a Dashboard**.
- Setting an alarm rule
  a. Log in to the AOM 2.0 console.
  b. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
  c. Click **Create Alarm Rule** to set an alarm rule. For details, see **Creating a Metric Alarm Rule**.

8.6.1.8 Connecting Other Exporters

Application Scenario

Guidance has been provided for connecting common Exporters. AOM is compatible with the native Prometheus, so you can also connect other Exporters in the community.

Methods

Customize dashboards or use either of the following methods to integrate basic components for monitoring:

1. **Integrating Exporters in the open-source community**
2. Instructions in **connecting common self-built middleware in the container scenario**

8.7 Obtaining the Service Address of a Prometheus Instance

In the **Service Addresses** area on the **Settings** tab page of the default Prometheus instance or of the Prometheus instance for ECS, CCE, and remote write, 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 or multi-account aggregation, 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**
- **Prometheus Instance for Remote Write**
- **Prometheus Instance for Multi-Account Aggregation**

Procedure

Step 1 Log in to the AOM 2.0 console.

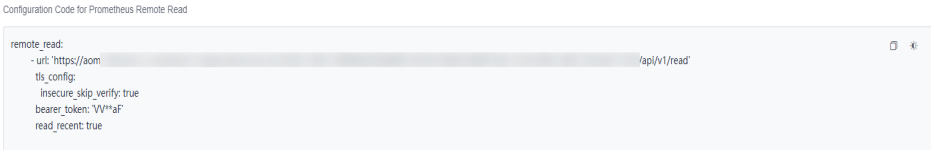
Step 2 In the navigation pane on the left, choose **Prometheus Monitoring** > **Instances**. In the instance list, click the created Prometheus instance.

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 8-27 Configuration code for Prometheus remote 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 8-28 Configuration code for Prometheus remote write

  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

8.8 Regions that Support Public Network Addresses for Remote Write

Huawei Cloud users must use public network addresses for Prometheus remote read or write. Intranet addresses are only used for service invocation within Huawei Cloud.

Only regions listed in **Table 8-19** support public network addresses for remote write.

Table 8-19 Regions that support public network addresses for remote write

Region Name	Region	Public Access Address
CN East-Shanghai1	cn-east-3	aom-access.cn-east-3.myhuaweicloud.com
CN East-Shanghai2	cn-east-2	aom-access.cn-east-2.myhuaweicloud.com
CN North-Beijing4	cn-north-4	aom-access.cn-north-4.myhuaweicloud.com
CN South-Guangzhou	cn-south-1	aom-access.cn-south-1.myhuaweicloud.com

8.9 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 **purchased** an ECS. For details, see **Elastic Cloud Server (ECS) Getting Started**.
- You have **purchased** an EIP and bound it to the purchased ECS. For details, see **Elastic IP (EIP) Getting Started**.
- Your service has been connected for Prometheus monitoring. For more details, see:
  - **8.2.1 Prometheus Instance for Cloud Services**
  - **Prometheus Instance for ECS**
  - **Prometheus Instance for CCE**
  - **Prometheus Instance for Remote Write**
  - **Prometheus Instance for Multi-Account Aggregation**

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.

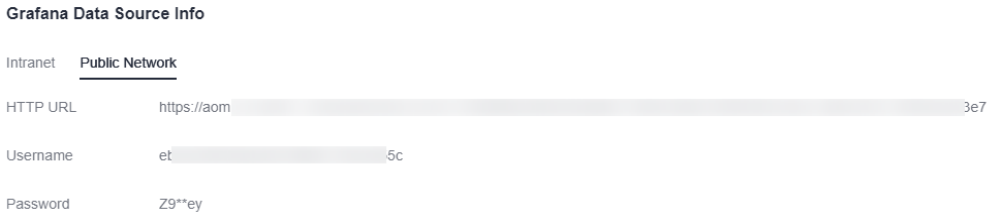
NOTE

- 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.

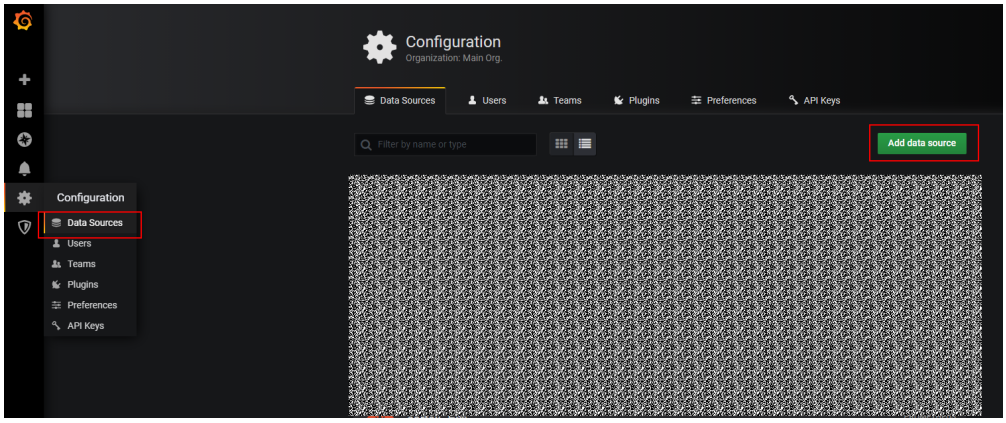
Figure 8-29 Grafana data source information



Step 4 Configure Grafana.

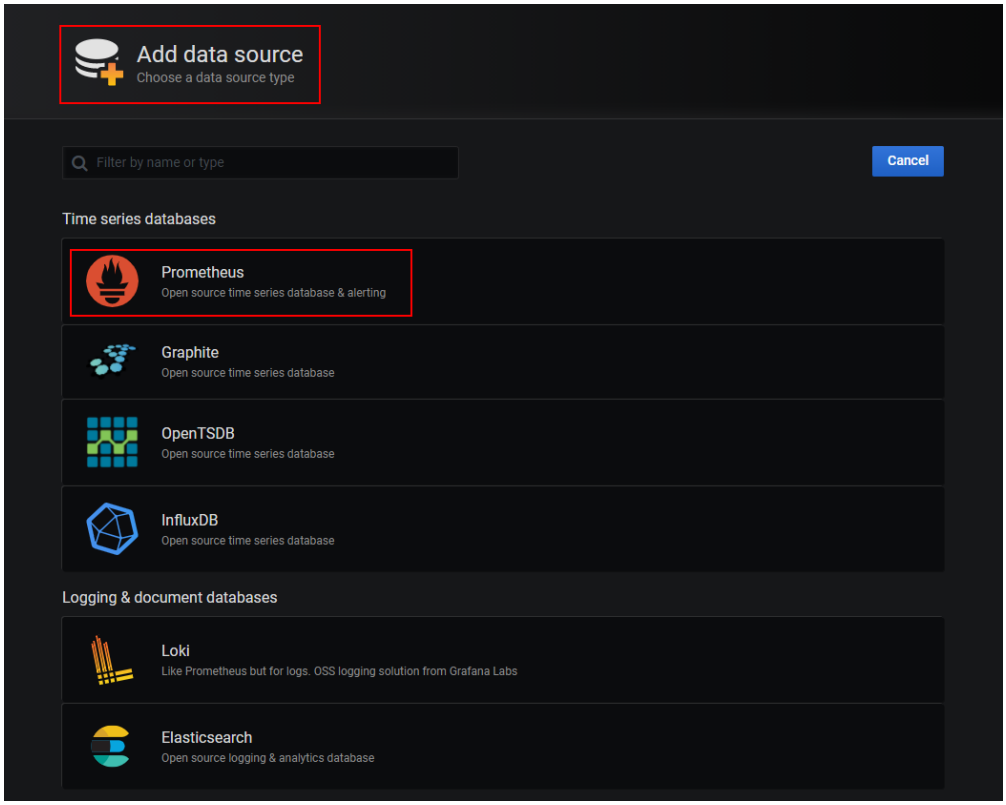
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration** > **Data Sources**. Then click **Add data source**.

Figure 8-30 Configuring Grafana



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

Figure 8-31 Prometheus configuration page

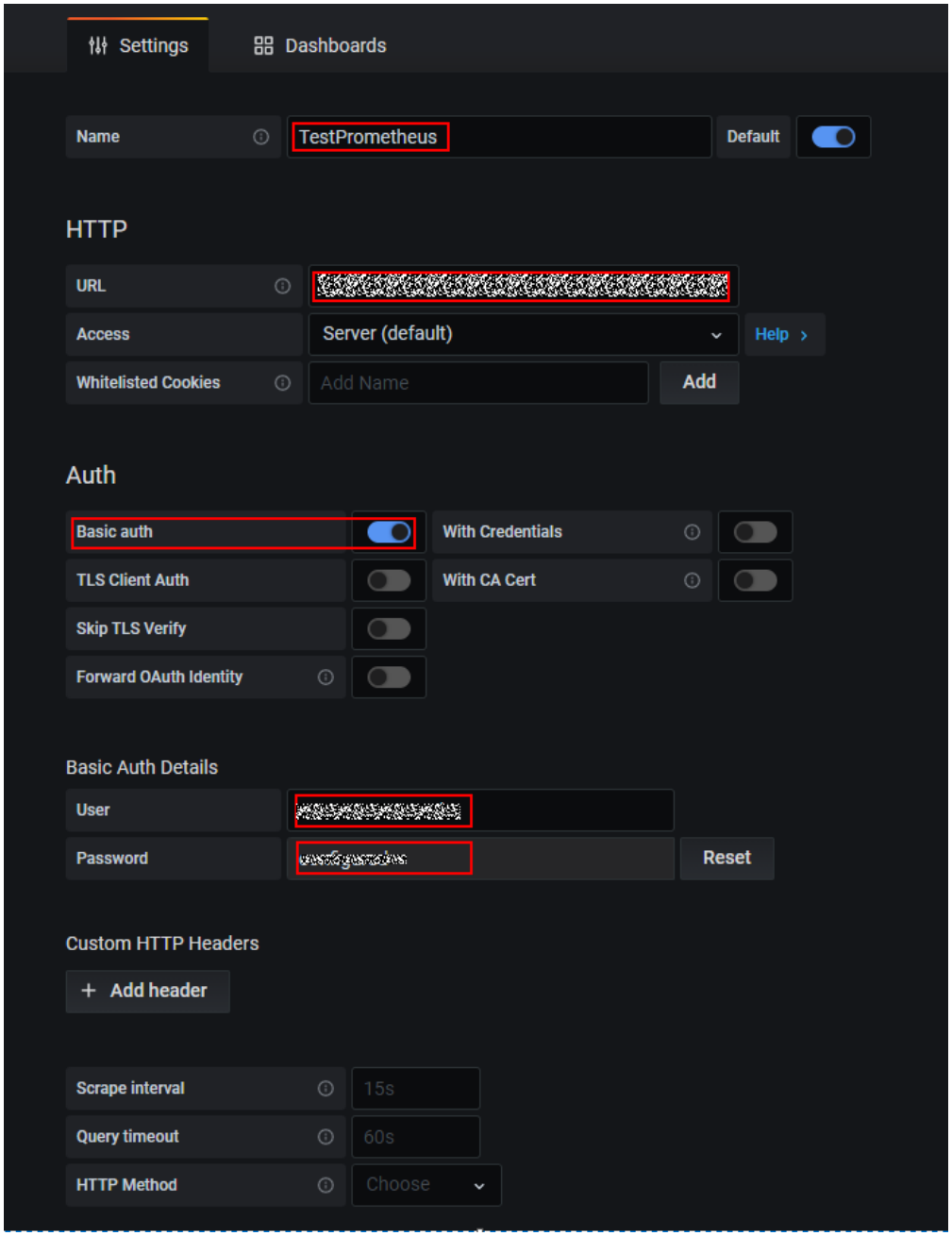


4. Set Grafana data source parameters.
   - **URL**: HTTP URL obtained in **Step 3**.
   - **User**: username obtained in **Step 3**.
   - **Password**: password obtained in **Step 3**.

   NOTE

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

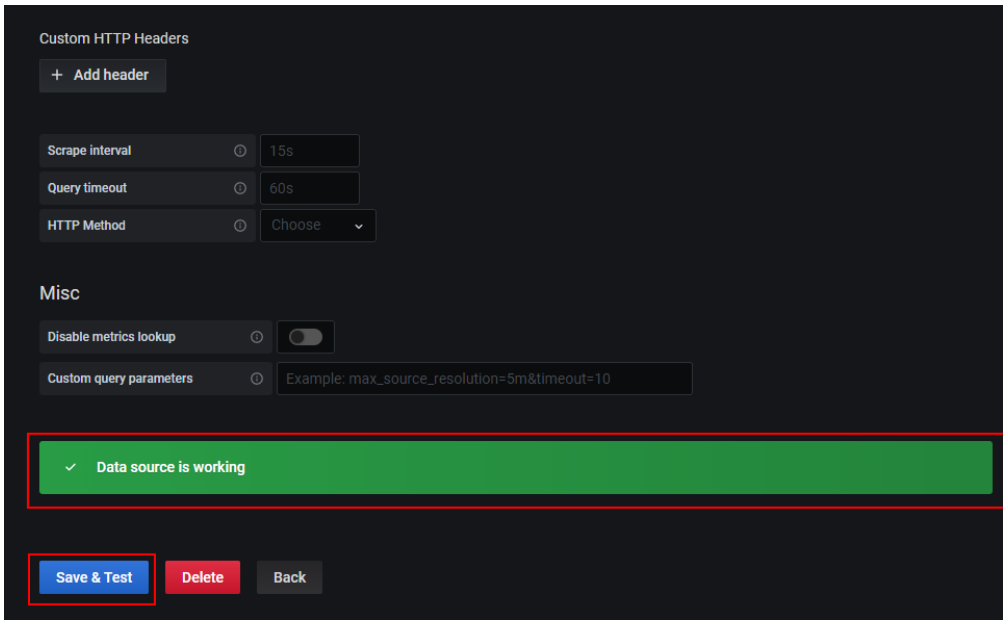
Figure 8-32 Setting parameters



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 8-33 Checking whether the configuration is successful



----End

8.10 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 oen 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:
  - **8.2.1 Prometheus Instance for Cloud Services**
  - **8.2.2 Prometheus Instance for ECS**
  - **8.2.3 Prometheus Instance for CCE**
  - **8.2.4 Prometheus Instance for Remote Write**
  - **8.2.5 Prometheus Instance for Multi-Account Aggregation**

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 ]
```

8.11 Reporting Self-Built Prometheus Instance Data to AOM

On the **Settings** tab page of the default Prometheus instance or of the Prometheus instance for ECS, CCE, or remote write, 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 **purchased** 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**
  - **Prometheus Instance for Remote Write**

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 8-34 Configuration code for Prometheus remote write

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

8.12 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**
  - **Prometheus Instance for Remote Write**

Precautions

- The **Resource Usage** page does not display the number of basic and custom metric samples reported by Prometheus instances for cloud services or for multi-account aggregation.
- 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.

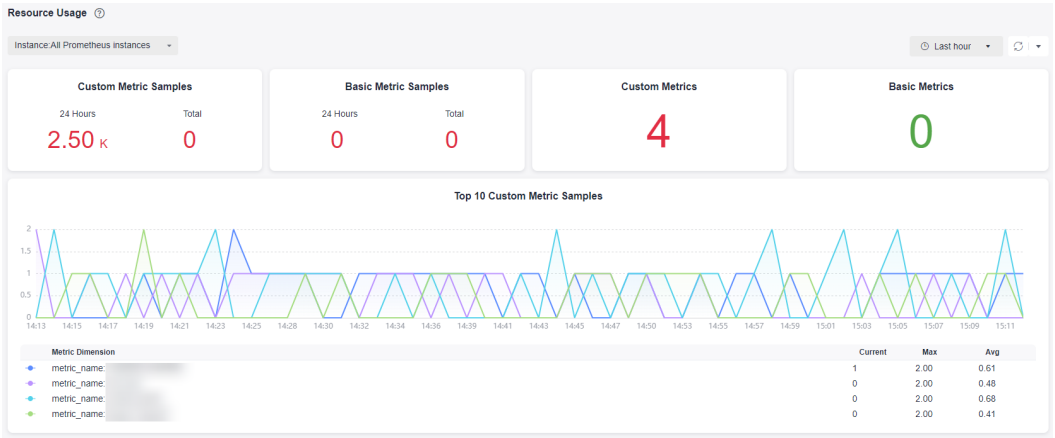
   Method 2: Specify the start time and end time (max. 30 days).

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 8-35 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

9 Business Monitoring (Beta)

9.1 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 **13.5 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)** > **Log Metric Rules**.

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 9-1**.

Figure 9-1 Ingesting logs

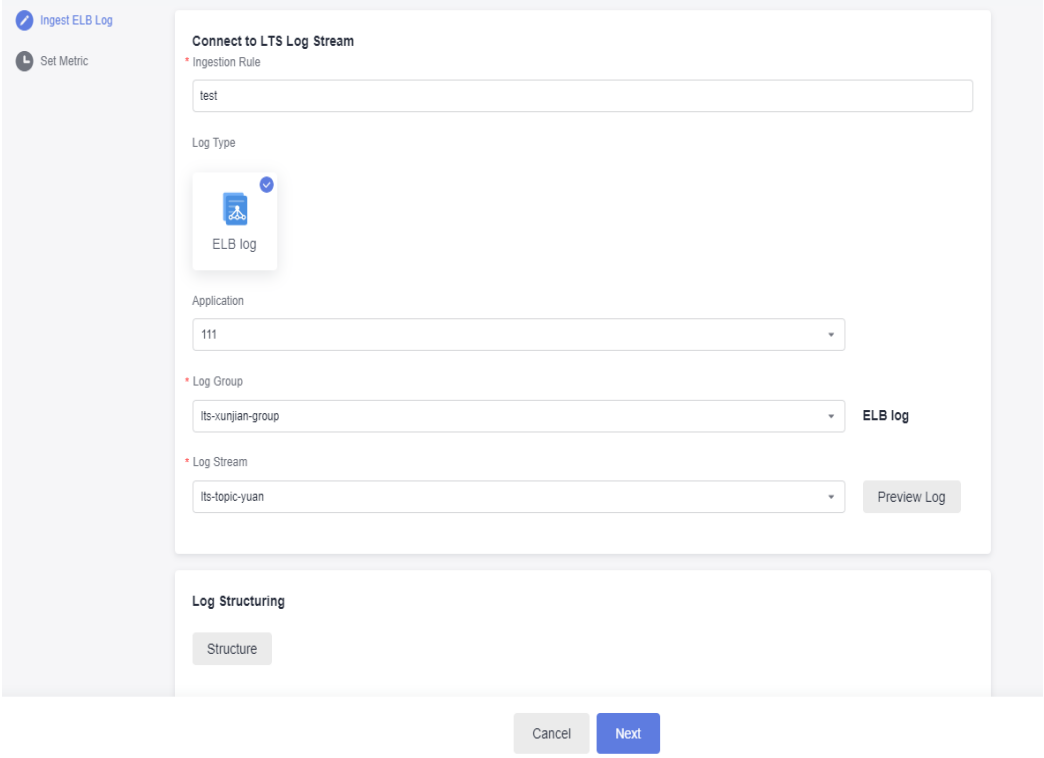


Table 9-1 Log ingestion parameters

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 9-2**.

Figure 9-2 Adding a metric

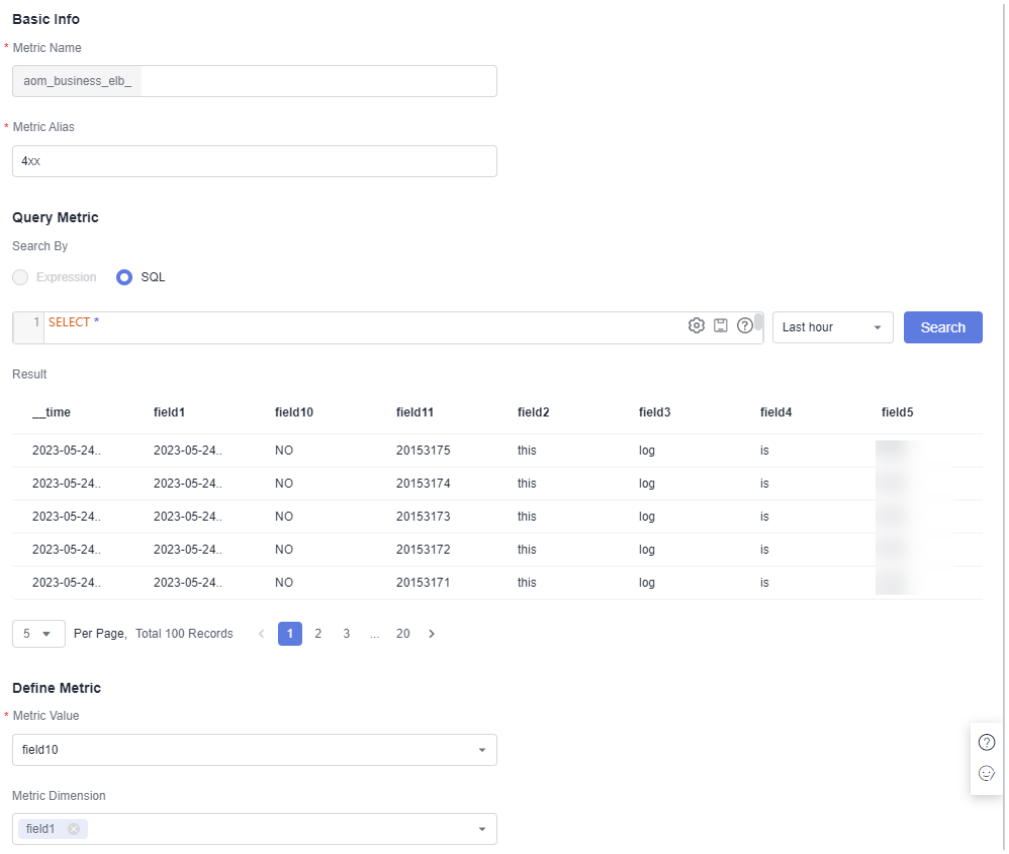


Table 9-2 Metric configuration parameters

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. Options: **Last minute**, **Last 10 minutes**, **Last 15 minutes**, **Last hour**, **Last 6 hours**, **Last day**, and **Last week**.
Define Metric	Metric Value	Select a value from the drop-down list. Only numeric fields can be selected.

Category	Parameter	Description
	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 9-3** if needed.

Table 9-3 Related operations

Operation	Description
Querying a log metric rule	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	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	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	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	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	1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select an access metric card and click . For details, see **Step 6**.
Deleting a metric	1. In the log metric rule list on the left, click a rule name. 2. In the right pane, select an access metric card and click .
Searching for a metric	1. In the log metric rule list on the left, click a rule name. 2. On the right of the page, enter a rule name keyword in the search box next to **Add Metric** and click .

10 Infrastructure Monitoring

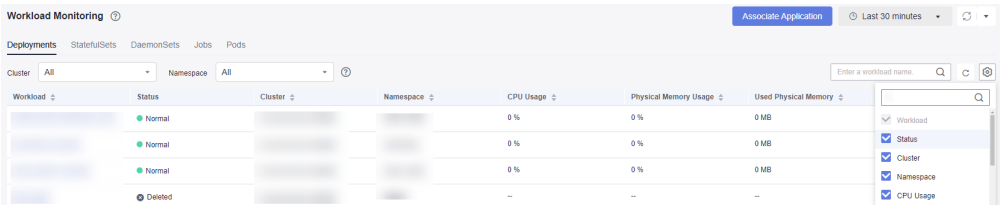
10.1 Workload Monitoring

Workload monitoring is for CCE and CCI 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

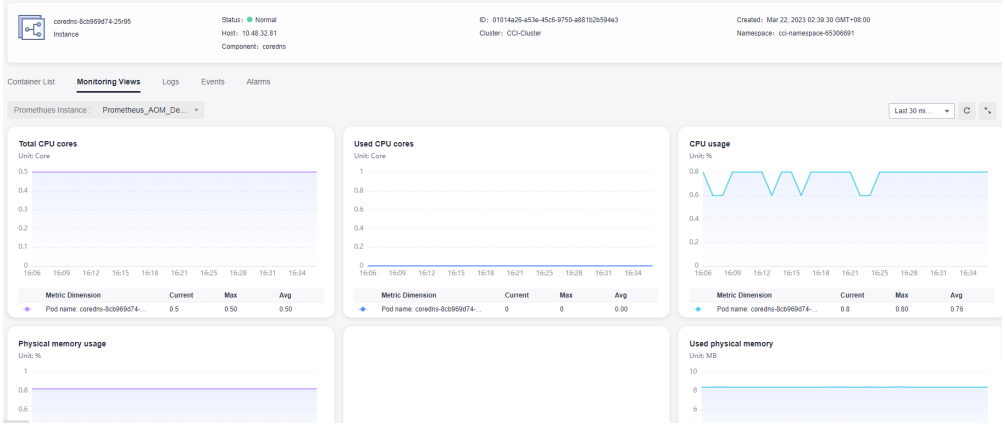
- The workload monitoring solution is ready-to-use. After AOM is enabled, the workload status, CPU usage, and physical memory usage of CCE and CCI are displayed on the workload monitoring page by default.

  Figure 10-1 Workload monitoring

- 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, logs, and alarms are monitored at each layer.

Figure 10-2 Workload details



- In the upper right corner of the workload monitoring page, click **Associate Application** and perform operations as prompted. Then CCE workloads can be reported to AOM. They can also be displayed as components in the application tree on the **Application Monitoring** page.

  NOTE

  To use the function of associating applications, enable **Application Insights** in **Menu Settings**. For details, see **13.5 Menu Settings**.

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, pod, or namespace name.

  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 **Logs** tab page, view the raw and real-time logs of the workload and analyze them as required. For details, see **6.6 Searching for and Viewing Logs**.
  - On the **Alarms** tab page, view the alarm details of the workload. For details, see **4.4 Viewing Alarms**.
  - On the **Events** tab page, view the event details of the workload. For details, see **4.5 Viewing Events**.

----End

10.2 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.

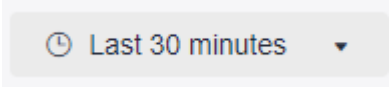
Step 5 Click a cluster to go to its details page. In the navigation pane on the left, monitor cluster running conditions by cluster, dashboard, or alarm.

- 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 **8.2.3 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.

        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. View nodes, workloads, and container groups by name.
- View the cluster running status from the alarm management perspective.
  - In the navigation pane on the left, choose **Alarm Management** > **Alarm List** to view alarm details of the cluster. For details, see **4.4 Viewing 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 **8.2.3 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

10.3 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 as required:

- **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 **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 Viewing Alarms**.
- 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 **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

10.4 Process Monitoring

10.4.1 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.

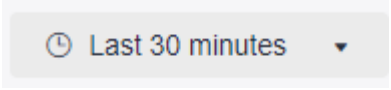
After application discovery rules are set, AOM automatically discovers applications that meet the rules and monitors related metrics. For details, see **10.4.3 Application Discovery**.

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 Viewing Alarms**.

----End

10.4.2 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

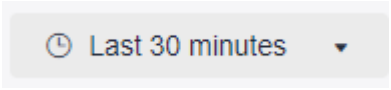
to a process. By viewing the status of each layer, you can implement dimensional monitoring for components.

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 as required:

- **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 Viewing Alarms**.
- On the **Events** tab page, view the event details of the component. For details, see **4.5 Viewing Events**.

----End

10.4.3 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 10-1**. 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 10-1 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-vswitchd unix:** and environment variables contain **SUDO_USER=paas**.

   NOTE

   - To precisely detect processes, you are advised to add check items about unique features of the processes.
   - You must add at least one check item and can add up to five check items. If there are multiple check items, AOM only discovers the processes that meet the conditions of all check items.

2. After adding check items, click **Detect** to search for the processes that meet the conditions.

   If no process is detected within 20s, modify the discovery rule and detect processes again. Only when at least one process is detected can you proceed to the next step.

Step 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 10-2** if needed.

Table 10-2 Related operations

Operation	Description
Viewing rule details	In the **Name** column, click the name of an application discovery rule.
Starting or stopping rules	• 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	• 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. **NOTE** Built-in discovery rules cannot be deleted.
Modifying rules	Click **Modify** in the **Operation** column. **NOTE** Built-in discovery rules cannot be modified.

10.5 Cloud Service Monitoring

Cloud service monitoring displays service instance statuses and metric usage in graphs such as line graphs and digit graphs.

Precaution

To use cloud service monitoring, enable this function in **Menu Settings**. For details, see **13.5 Menu Settings**.

Function Introduction

The following table lists the cloud services that can be monitored.

Table 10-3 Cloud service monitoring

Category	Cloud Service
Compute	FunctionGraph
Storage	Object Storage Service (OBS)
Network	EIP and bandwidth, Elastic Load Balance (ELB), and NAT gateway
Databases	Relational Database Service (RDS)
Application middleware	Distributed Message Service (DMS) and Distributed Cache Service (DCS)

Procedure

Step 1 Log in to the AOM 2.0 console.

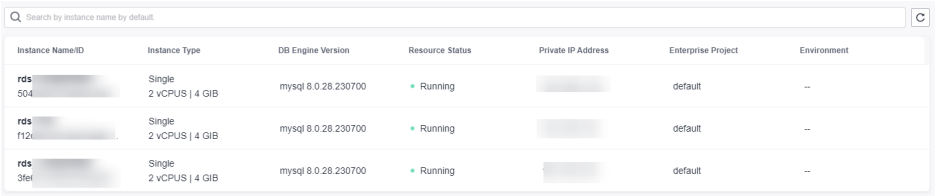
Step 2 In the navigation pane, choose **Infrastructure Monitoring** > **Cloud Service Monitoring**.

Step 3 Select a cloud service from the cloud service list. In the right pane, view all instances, related enterprise projects, and environments of the cloud service.

NOTE

- If **Connect Now** is displayed on the right, the cloud service has not been connected to AOM. Click **Connect Now** or click **Connect Cloud Service** in the upper right corner of the page. After a cloud service is connected, you can monitor it.
- Before connecting a cloud service, select an enterprise project. If you have selected an enterprise project on the global settings page, skip this step. If no enterprise project has been selected on the global settings page, select one from the drop-down list here.

Figure 10-3 Viewing cloud service information



- In the upper right corner of the cloud service instance list, set filter criteria or search for cloud service instances by instance name or ID.
- Click in the upper right corner to obtain the latest information about all instances of the cloud service in real time.

Step 4 Click an instance name. On the displayed page, monitor its metric graphs.

- In the upper right corner of the page, set different statistical periods to view data.
  a. Set a time range to view the metrics that are 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 (max. 30 days).

  b. 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**.
- Enter a metric name in the search box so that you can quickly view required information.
- In the upper right corner of a metric card, choose > **Full Screen**. The card is displayed in full screen.
- In the upper right corner of a metric card, choose > **Refresh**. If you are in full screen mode, choose > **Refresh**.
- In the upper right corner of the page, click **View Resource Details** to go to the corresponding console and view more information.

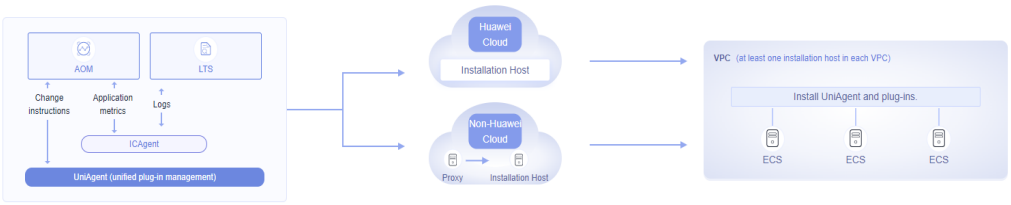
----End

11 Collection Management

11.1 Overview

The UniAgent centrally manages the life cycle of collection plug-ins and delivers instructions (such as script delivery and execution). It does not collect data; instead, collection plug-ins do that. Such plug-ins can be installed, upgraded, or uninstalled as required. Plug-ins for Cloud Eye and Host Security Service (HSS) will be rolled out later.

Figure 11-1 Getting started



11.2 UniAgent Management

11.2.1 VM Access

11.2.1.1 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 11-1 Installation modes

Mode	Application Scenario
Manual Installation	When installing a UniAgent for the first time, you must install it manually.

Mode	Application Scenario
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 by Importing an Excel File	Ensure that an installation host and an Excel file with data are available. **NOTE** The Excel import function is opened restrictedly. If you need this function, **submit a service ticket**.

Installation Prerequisite

Ensure that the network between the installation host and the host where the UniAgent is to be installed is normal.

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 **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **VM Access**. On the displayed page, click **Install UniAgent** in the upper right corner. Then, 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 11-2 Manually installing a UniAgent

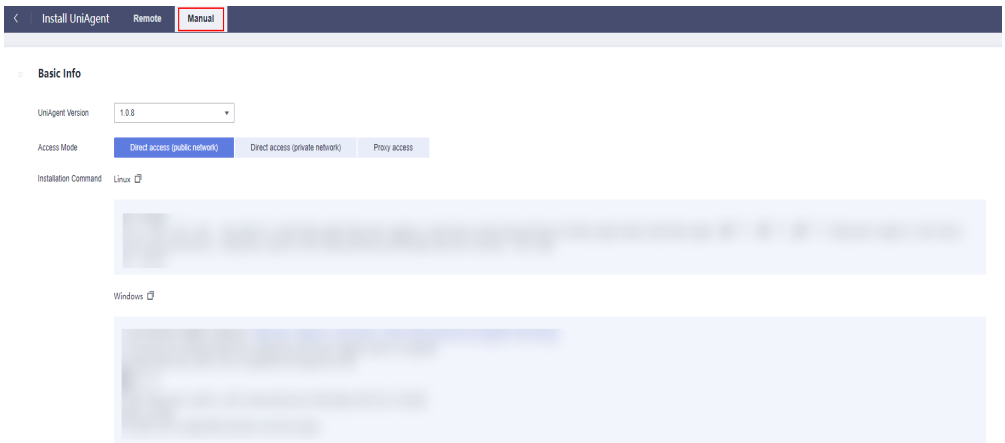


Table 11-2 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are three access modes: **Direct access (private network)**, **Direct access (public network)**, and **Proxy access**. • **Direct access (private network)**: intended for Huawei Cloud hosts. • **Direct access (public network)**: intended for non-Huawei Cloud hosts. • **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 (private network)

Parameter	Description	Example
Installation Command	Command for installing the UniAgent. Commands for Linux and Windows are different. Click  to copy the installation command. **Linux** 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 xxxxxxxxxx -p xxxxxx -d https://aom-uniagent-xxxxxx -m https://uniagent.master.cnxxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x set -o history; **Windows** 1. Download the installation package from **https://aom-uniagent-*{region_name}*.obs.*{region_name}*.*{site domain name suffix}*/ +uniagentd-*{version}*-win32.zip**. *{region_name}* and *{version}* can be obtained from the installation page. – *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**. – *version*: version of the installed UniAgent. 2. Decompress the package, click **uniagentd.msi**, and specify path **C:\uniagentd** for installation. 3. Modify the **uniagentd.conf** file in **C:\uniagentd\conf** and enter the following configuration: **ak=***xxxxxxxxxxxxx* **sk=***xxxxxxxxxxxx* **master=https://uniagent.master.***xxxxxxxxxx*,**https://***xx.xx.xx.xx:xxxxx* 4. Run **start.bat** in the **C:\uniagentd\bin** directory as the administrator. **NOTE** • If you need to verify the SHA256 value of the Windows installation package, check the file downloaded from **https://aom-uniagent-*{region_name}*.obs.*{region_name}*.*{site domain name suffix}*/uniagentd-*{version}*-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 **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **VM Access**. On the displayed page, 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 11-3 Remotely installing a UniAgent

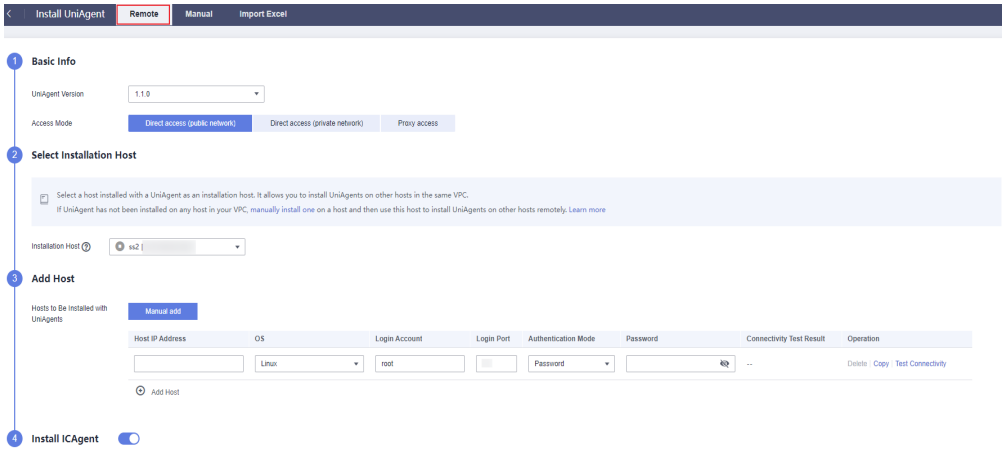
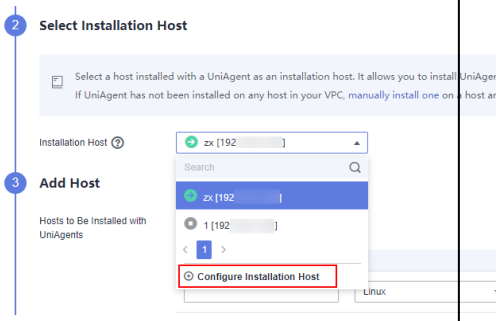


Table 11-3 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8

Parameter	Description	Example
Access Mode	There are three access modes: **Direct access (private network)**, **Direct access (public network)**, and **Proxy access**. • **Direct access (private network)**: intended for Huawei Cloud hosts. • **Direct access (public network)**: intended for non-Huawei Cloud hosts. • **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 (private network)
Proxy Area	When **Access Mode** is set to **Proxy access**, you need to select a proxy area or **add a proxy area**. A proxy area is used to group and manage proxies. **A proxy** is a Huawei Cloud ECS used for network communication across clouds.	-
Installation Host	An installation host is used to execute commands for remote installation. This parameter is mandatory. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 11-4** Configuring an installation host  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	Detailed information about the host where the UniAgent is to be installed. This parameter is mandatory. Click **Add Host** and enter the following information: **Host IP Address**: IP address of a host. **OS**: operating system of the host, which can be **Linux** or **Windows**. **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. **Login Port**: port for accessing the host. **Authentication Mode**: Currently, only password-based authentication is supported. **Password**: password for logging in to the host. **Connectivity Test Result**: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal. **Operation**: **Delete**, **Copy**, or **Test Connectivity**. **NOTE** • You can click **Add Host** to add up to 100 hosts. • The hosts that run Windows do not support connectivity tests.	-
Install ICAgent	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.	-

Step 5 Click **Install**. After the installation is complete, you can view the UniAgent in the UniAgent list.

----End

Installation by Importing an Excel File

NOTE

The Excel import function is opened restrictedly. If you need this function, **submit a service ticket**.

Step 1 On the menu bar, choose **Collection Management**.

Step 2 Click **Install UniAgent** in the upper right corner and select **Import Excel**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Import Excel** is not available.)

Step 3 On the **Install UniAgent** page, set parameters.

Figure 11-5 Installation by importing an Excel file

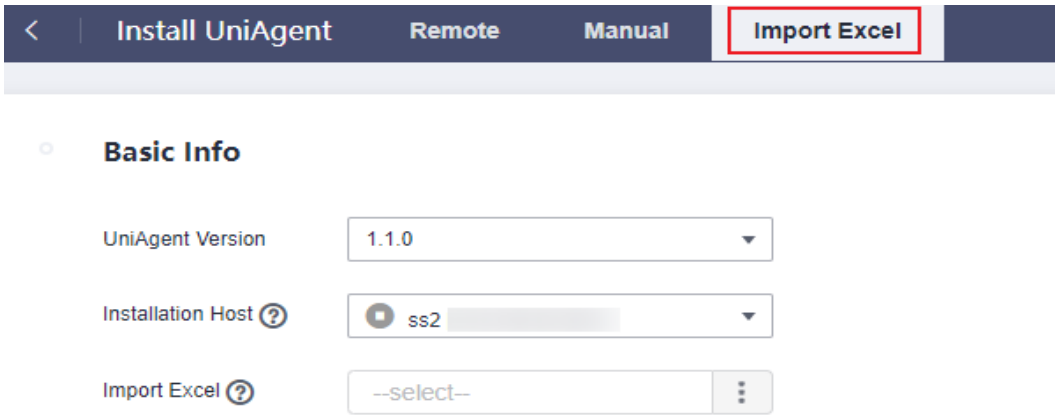
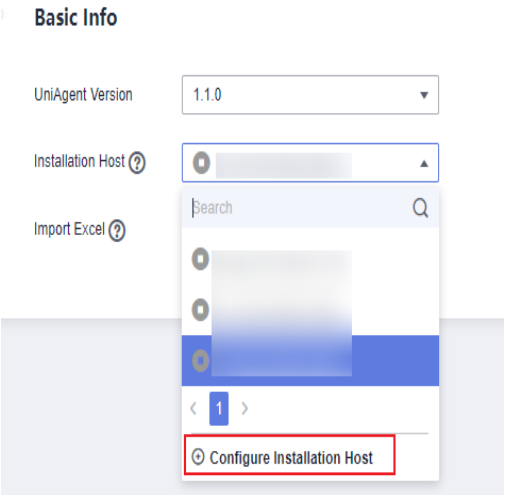


Table 11-4 Parameters for installation by importing an Excel file

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.1.0

Parameter	Description	Example
Installation Host	An installation host is used to execute commands for Excel-based installation. This parameter is mandatory. If no installation host has been configured, perform the following steps: 1. Select **Configure Installation Host** from the drop-down list. **Figure 11-6** Configuring an installation host  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**.	-
Import Excel	Only an **.xls** or **.xlsx** file with up to 5000 records can be uploaded.	-

Step 4 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 11-5 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 **11.2.1.1 Installing a UniAgent**.

Troubleshooting

If you encounter any problem when installing the UniAgent, see **Collection Management FAQs**.

11.2.1.2 Operating UniAgents in Batches

You can reinstall, upgrade, uninstall, or delete UniAgents on hosts in batches.

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 **Collection Management**.

Step 3 In the navigation pane, choose **UniAgent** > **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 tree on the left, choose **UniAgent** > **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

Step 1 In the navigation pane, choose **UniAgent** > **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 tree on the left, choose **UniAgent** > **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

11.2.1.3 Operating Other Plug-ins in Batches

Collection Management will support interconnection with other types of plug-ins. You can install, upgrade, and uninstall plug-ins in batches.

The following plug-ins have been interconnected:

- ICAgent: collects metrics and logs.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **UniAgent** > **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 11-6 Plug-in operation parameters

Parameter	Description
Operation	Options: **Install**, **Upgrade**, and **Uninstall**.
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

11.2.1.4 Other Operations

On the **UniAgent** > **VM Access** page, perform the following operations on the hosts where UniAgents are installed if needed:

Table 11-7 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.
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).

Operation	Description
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** • 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.

11.2.2 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 **Collection Management**.

Step 3 In the navigation pane, choose **UniAgent** > **CCE Access** to view 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.

11.2.3 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.

11.2.3.1 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 **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click **Add Proxy Area**. In the dialog box that is displayed, set parameters.

Table 11-8 Parameters for adding a proxy area

Parameter	Description	Example
Proxy Area Name	Enter a maximum of 64 characters.	test
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 procedure is as follows:

Step 1 In the navigation tree on the left, choose **UniAgent** > **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 **UniAgent** > **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 **UniAgent** > **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

11.2.3.2 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 **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click **Add Proxy** and set related parameters.

Table 11-9 Parameters for adding a proxy

Parameter	Description	Example
Proxy Area	Select a **proxy area** that you have created.	qwsertyddfsdfdf
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 procedure is as follows:

Step 1 In the navigation tree on the left, choose **UniAgent** > **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

Viewing a Proxy

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 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 **UniAgent** > **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

11.2.4 Operation Logs

Operation logs record the operations (such as installation, upgrade, and uninstall) performed on UniAgents and other plug-ins.

Viewing Operation Logs of UniAgent

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **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 **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent** > **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 **Collection Management** > **Operation Logs** page, perform the operations listed in the following table if needed.

Table 11-10 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.

11.3 Plug-in Market

11.3.1 Overview

The plug-in market is a collection of O&M data collection plug-ins, including middleware, and custom plug-ins.

- **Middleware plug-ins**: built-in; cannot be modified, deleted, or viewed. The following types of middleware plug-ins are supported:
  - **MYSQL**: MySQL collector.
  - **REDIS**: Redis collector.
  - **MONGODB**: MongoDB collector.
  - **NGINX**: Nginx collector.
  - **NODE**: node collector.
  - **HAPROXY**: HAProxy collector.
  - **COMP_EXPORTER**: exporter collector that can be installed.
  - **COMP_REDIS_EXPORTER**: Redis Exporter collector (unavailable soon).
  - **COMP_MYSQL_EXPORTER**: MySQL Exporter collector (unavailable soon).
- **Custom plug-ins**: user-defined.

11.3.2 Creating a Plug-in

You can customize a script to create a plug-in and use it to collect metric data.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **Plug-in Market** and click **Create Plug-in**.

Step 4 On the displayed page, set related parameters.

- Plug-in information

  Table 11-11 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.

- Plug-in configuration

  Table 11-12 Plug-in configuration parameters

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

Plug-in Script	Custom plug-in script. Options: **Linux** and **Windows**.
	Linux: Shell or Python script.
	Example:
	`#!/bin/bash`
	`#Examples`
	`echo "metric_name{label_name=\"label_value\"} 100"`
	Windows: BAT script
	Example:
	`::Examples`
	`@echo off`
	`echo metric_name{label_name="label_value"} 100`

Parameter	Description
Default Script Parameter	Custom script parameter template. Only letters, digits, and underscores (_) are allowed. The rules are as follows: – **Letter**: For example, **-a**. – **Character combination**: For example, **http://127.0.0.1:80**. The following special characters are not allowed: &|><;`!()$- – **${*Parameter*}**: Enter a maximum of 64 characters starting with a letter. Only letters, digits, and underscores (_) are allowed. For example, *${a_b}*. You can combine parameters as required and separate them with spaces. The total length of these parameters cannot exceed 250 characters.
Script Parameter	Parameters in the default script parameters. After you enter the default script parameters, the system automatically identifies script parameters based on your settings. Script parameter description: – **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**.

----End

11.3.3 Other Operations

On the **Collection Management** > **Plug-in Market** page, create versions for plug-ins, and search for, edit, and delete plug-ins.

Searching for a Plug-in

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **Plug-in Market**.

Step 4 Enter a plug-in name in the search box.

----End

Modifying a Plug-in

Step 1 In the navigation pane, choose **Plug-in Market**. Then click **Custom**.

Step 2 Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Modify**.

Step 3 On the displayed page, modify the **plug-in information**.

Step 4 Click **Save**.

----End

Creating a Version

Step 1 In the navigation pane, choose **Plug-in Market**. Then click **Custom**.

Step 2 Click the target plug-in. The plug-in details page is displayed.

Step 3 Click **Create Version**. On the displayed page, **set the plug-in**.

NOTE

- 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.

Step 4 Set **the parameters** and click **Save**.

----End

Deleting a Plug-in

NOTE

System plug-ins and middleware plug-ins cannot be deleted.

Step 1 In the navigation pane, choose **Plug-in Market**. Then click **Custom**.

Step 2 Locate the target plug-in, hover the mouse pointer over the plug-in, and choose > **Delete**.

Step 3 On the displayed page, click **OK** to delete the plug-in.

NOTE

If a collection task has been configured for a plug-in, deleting the plug-in will also delete the collection task.

----End

11.3.4 Plug-in Statuses

The following table lists the plug-in statuses.

Table 11-13 Plug-in statuses

Status	Description
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.

11.4 Collection Tasks

11.4.1 Overview

Prometheus monitoring integrates common infrastructure, middleware, and custom components. 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, so you can 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: Collect metrics using **middleware plug-ins**, such as MySQL, Redis, MongoDB, Nginx, Node, and HAProxy.
- Custom collection tasks: Collect metrics using **custom plug-ins**.

11.4.2 Middleware Collection Tasks

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

You can create collection tasks using the following built-in middleware plug-ins:

- **MYSQL**: monitors MySQL metrics.
- **REDIS**: monitors Redis metrics.
- **MONGODB**: monitors MongoDB metrics.
- **NGINX**: monitors Nginx metrics.
- **NODE**: monitors node metrics.
- **HAPROXY**: monitors HAProxy metrics.
- **COMP_EXPORTER**: monitors custom metrics.
- **COMP_REDIS_EXPORTER**: monitors Redis metrics. (Unavailable soon)
- **COMP_MYSQL_EXPORTER**: monitors MySQL Exporter metrics. (Unavailable soon)

11.4.2.1 MySQL Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the collection task configuration page, set parameters by referring to the following table.

Table 11-14 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** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **MYSQL**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
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. ● 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. ● **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 5 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.

Parameter	Description
MySQL Username	Username of MySQL.
MySQL Password	Password of MySQL.
MySQL Address	IP address and port number of MySQL, for example, **127.0.0.1:3306**.

Step 6 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 view the configuration of the collection task.

----End

11.4.2.2 Redis Component Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the displayed page, set parameters by referring to the following table and click **Next**.

Table 11-15 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** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **Redis**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.
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. • 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.

Operation	Parameter	Description
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. • **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 5 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.

Parameter	Description
Redis Address	Address of Redis.
Redis Password	Password for logging in to Redis.

Step 6 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 view the configuration of the collection task.

----End

11.4.2.3 MongoDB Component Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the displayed page, set parameters by referring to the following table and click **Next**.

Table 11-16 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 MongoDB plug-in, select **Linux**. **NOTE** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **MongoDB**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
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. ● 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. ● **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 5 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.

Parameter	Description
MongoDB Address	IP address of MongoDB, for example, **127.0.0.1**.
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 6 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 view the configuration of the collection task.

----End

11.4.2.4 Nginx Component Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the displayed page, set parameters by referring to the following table and click **Next**.

Table 11-17 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** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **Nginx**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.
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. • 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.

Operation	Parameter	Description
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. • **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 5 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.

Parameter	Description
Nginx URL	Nginx connection address.

Step 6 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 view the configuration of the collection task.

----End

11.4.2.5 Node Component Access

Scenario

Create collection tasks using the built-in Node plug-in. After installing this plug-in, you can monitor Node 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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the displayed page, set parameters by referring to the following table and click **Next**.

Table 11-18 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 Node plug-in, select **Linux**. **NOTE** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **Node**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.
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.

Operation	Parameter	Description
	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. • 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. • **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 5 Click **Install** to install Exporter. 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.

Step 6 Click **Create** to connect the Node 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 view the configuration of the collection task.

----End

11.4.2.6 HAProxy Component Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then click **Create Collection Task**.

Step 4 On the displayed page, set parameters by referring to the following table and click **Next**.

Table 11-19 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** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **HAProxy**.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.
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. • 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 middleware plug-in, only one host can be selected.
	Metrics	Metrics to be collected, for example, **metric1,metric2**.
	Metric Dimension	When **Collection Plug-in** is set to a middleware plug-in, the default metrics of the plug-in are displayed. Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.

Operation	Parameter	Description
	Advanced Settings	Set **Collection Period (s)** and **Timeout Period (s)**. • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period cannot exceed the collection period. • **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 5 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.

Parameter	Description
HAProxy URL	HAProxy connection address.

Step 6 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 view the configuration of the collection task.

----End

11.4.2.7 Custom Exporter Access

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, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then, click **Create Collection Task**.

Step 4 On the collection task configuration page, set parameters by referring to the following table.

Table 11-20 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 COMP_EXPORTER plug-in, select **Linux**. **NOTE** • 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	Click **Add Plug-in**. On the displayed page, choose **Middleware** > **COMP_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. • 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 middleware plug-in, only one host can be selected.

Operation	Parameter	Description
	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, **127.0.0.1:9100**. • **Component Address**: host where Exporter starts instance monitoring. Generally, set this parameter to the IP address of the host. • **Metrics**: The default value is single quotation marks (''), indicating that all metrics are exported. If you need to filter metrics, set this parameter in the following format, for example, **'metric1,metric2'**.
	Indicator Dimension	Click **+ Tag** and then set a custom dimension name and value. Enter up to 20 characters. 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.
	Advanced Settings	Includes **Collection Period (s)** and **Timeout Period (s)**. • **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). • **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period must be shorter than or equal to the collection period. • **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 5 Click **Create**.

Step 6 On the displayed collection task page, click the target collection task to view its details.

----End

11.4.3 Custom Collection Tasks

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.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**. Then, click **Create Collection Task**.

Step 4 On the collection task configuration page, set parameters by referring to the following table.

Table 11-21 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** • 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	Click **Add Plug-in**. On the displayed page, choose **Custom** and then select a custom plug-in.
	Plug-in Version	Select a plug-in version. **NOTE** Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
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. ● 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)**. ● **Collection Period (s)**: O&M data collection period, in seconds. Options: **10s**, **30s**, and **60s** (default). ● **Timeout Period (s)**: the maximum time for executing a collection task, in seconds. Options: **10s**, **30s**, and **60s** (default). **NOTE** The timeout period must be shorter than or equal to the collection period. ● **Executor**: user who executes the collection task, that is, the user of the selected host. Default: **nobody**. Enter the name of the user who executes the collection task. Recommended: **nobody**.

Step 5 Click **Create**.

Step 6 On the displayed collection task page, click the target collection task to view its details.

----End

11.4.4 Other Operations

Viewing a Collection Task

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **Collection Tasks**.

Step 4 Click a collection task name to view the task details.

----End

Starting or Stopping a Collection Task

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 On the collection task page, click  in the **Start/Stop** column of a collection task to start or stop it.

NOTE

Only middleware and custom collection tasks can be started or stopped.

----End

Searching for a Collection Task

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 On the collection task page, enter a keyword of a collection task or plug-in, and click **Confirm** to search.

----End

Changing a Target Host

NOTE

Target hosts of middleware collection tasks cannot be changed.

To change the target host after a collection task is created, perform the following operations:

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 Locate the target collection task and click  in the **Operation** column.

Step 3 On the displayed **Add Host** page, change the target host.

Step 4 Click **OK**.

----End

Copying a Collection Task

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 Locate the target collection task and click  in the **Operation** column.

Step 3 On the displayed page, modify parameters as required.

NOTE

If you do not need to modify the parameters, skip this step.

Step 4 Click **Create**.

----End

Modifying a Collection Task

NOTE

Middleware collection tasks cannot be modified.

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 Locate the target collection task and choose ··· > **Modify** in the **Operation** column.

Step 3 On the displayed page, modify the parameters of the collection task as required.

Step 4 Click **Save**.

----End

Deleting a Collection Task

Step 1 In the navigation pane, choose **Collection Tasks**.

Step 2 Locate the target collection task and choose ··· > **Delete** in the **Operation** column.

Step 3 On the displayed page, click **OK** to delete the collection task.

----End

12 O&M Management

12.1 Overview

Automation depends on Huawei Cloud UniAgent capabilities. It supports atomic operations such as batch script execution, file distribution, and cloud service change. It allows you to orchestrate atomic operations, and assemble them into jobs and form standard O&M processes. Automation accumulates routine O&M operations and releases them as services for standardized, automatic, and non-differentiated O&M. It frees O&M personnel from repeated and complex application change operations, improves O&M quality and efficiency, and helps enterprises transform O&M to improve value.

Precaution

To use Automation, enable this function in **Menu Settings**. For details, see **13.5 Menu Settings**.

Function description

Table 12-1 Function description

Category	Description
Scenarios	Different types of tasks are provided, and cards of different atomic service scenarios can be managed.
Scheduled O&M	AOM provides functions such as creating scheduled tasks, and displays execution records of scheduled tasks.
Tasks	AOM provides functions such as task execution, and displays the execution records of all tasks.
Parameters	AOM provides functions such as creating parameters, and displays all existing parameter information.
Jobs	AOM provides functions such as job creation and management.
Scripts	AOM provides functions such as creating scripts and managing script versions.

Category	Description
Packages	AOM provides functions such as creating packages and managing package versions.
Settings	AOM manages accounts, access credentials, and scenarios by category.
Tool market	AOM provides different atomic service scenarios, and allows you to bring service scenario cards online or offline.

12.2 Enabling the Automation Service

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

NOTE

When you use Automation for the first time, add the **Security Administrator** role first. When you use Automation later, there is no need to add this role again.

Automation is available in CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, AP-Singapore, AP-Bangkok, CN-Hong Kong, and ME-Riyadh.

Step 1 Subscribe to AOM 2.0 by referring to **17 Subscribing to AOM 2.0**.

Skip this step if AOM 2.0 has been enabled.

Step 2 Log in to the AOM 2.0 console.

Step 3 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 4 On the service authorization page that is displayed, click **Agree and Enable**.

----End

12.3 Permissions Management

12.3.1 Creating a User and Granting Permissions

This section describes the fine-grained permissions management provided by IAM for your Automation. 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 Automation 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 Automation resources.

If your account does not need individual IAM users, then you may skip over this section.

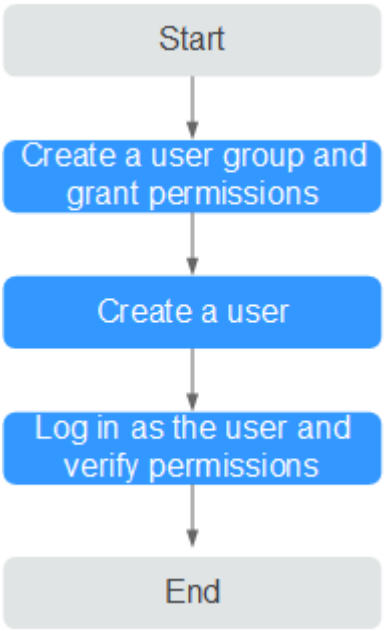
This section describes the procedure for granting permissions (see **Figure 12-1**).

Prerequisites

Before assigning permissions to user groups, you should learn about Automation policies and select the policies based on service requirements. For the system permissions of other services, see **System Permissions**.

Process

Figure 12-1 Process for granting Automation permissions



1. Creating a User Group and Assigning Permissions

   Create a user group on the IAM console, and assign the **CMS ReadOnlyAccess** policy to the group.

2. Creating a User and Adding the User to a User Group

   Create a user on the IAM console and add the user to the group created in **1**.

3. Logging In as a User and Verifying Permissions

   Log in to the console as the created user, and verify that it only has read permissions for Automation.

12.3.2 Custom Policies for Automation

Custom policies can be created as a supplement to the system policies of Automation. 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, see **Creating a Custom Policy**. The following contains examples of common Automation custom policies.

Example Custom Policies of Automation

Example: Prohibiting a user to release or remove a service card

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.

The following method can be used if you need to assign permissions of the **CMS FullAccess** policy to a user but you want to prevent the user from releasing and removing cards. Create a custom policy for denying card release and removal, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on Automation except card release and removal. The following is an example deny policy:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "cms:toolmarket:update"
         ],
      }
   ]
}
```

12.4 Scenarios

12.4.1 Scenario Overview

Released tool cards are displayed based on scenarios described in **12.11.3 Scenarios**. You can use the cards to quickly create tasks, add the cards to favorites, or remove them from the tool market. To prevent a card from being removed, follow the instructions provided in **12.3.2 Custom Policies for Automation**. For details, see **Table 12-2**.

Table 12-2 Related operations

Operation	Description
Adding a card to favorites	Click ☆ to add a card to favorites.

Operation	Description
Removing a card	Click in the upper right corner of a card and choose **Remove**. **NOTE** • Before removing a service, check whether it has been referenced by a scheduled O&M scenario. If yes, delete the scenario first. For details, see **Reference Details**. • After a card is removed, it will not be displayed on the **Scenarios** page. In addition, the card will also be removed from the tool market, and the status of the execution plan corresponding to the card will be changed to **Not published**. • After a card is removed, the tasks associated with the card cannot be executed. The execution can be resumed only after the card is published again. • **File Management** and **Script Management** are default functions and cannot be removed.

Common

By default, the **File Management** and **Script Management** cards are displayed under the **Common** tab. Add cards as required. You can use a card to quickly create a task, add a card to favorites, or remove a card. For details, see **12.9 Scripts** and **12.10 Packages**.

Cloud Services

Cloud Services lists the tool cards that have been released for starting and stopping ECSs, restarting RDS DB instances, changing ECS non-administrator passwords, and restarting CCE workloads. You can use a card to quickly create a task, add a card to favorites, or remove a card. For details, see **12.4.2 Starting an ECS**, **12.4.3 Stopping an ECS**, **12.4.4 Restarting an RDS DB Instance**, **12.4.5 Changing an ECS Non-Administrator Password**, and **12.4.6 Restarting a CCE Workload**.

Software Deployment

By default, there is no card under the **Software Deployment** tab. Add cards as required. You can use a card to quickly create a task, add a card to favorites, or remove a card.

Troubleshooting

By default, the **Clearing Disk Space** is displayed under the **Troubleshooting** tab. Add cards as required. You can use a card to quickly create a task, add a card to favorites, or remove a card. For details, see **12.4.7 Clearing Disk Space**.

Routine Inspection

By default, there is no card under the **Routine Inspection** tab. Add cards as required. You can use a card to quickly create a task, add a card to favorites, or remove a card.

12.4.2 Starting an ECS

You can use the **Starting an ECS Instance** card to create a task to start one or more ECSs.

Creating a Task for Starting an ECS

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Starting an ECS Instance** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-3**.

Figure 12-2 Starting an ECS

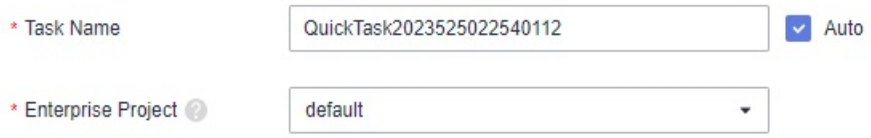


Table 12-3 Parameters for starting an ECS

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. A maximum of 100 instances can be selected for a single task.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-4**.

Figure 12-3 Selecting an instance

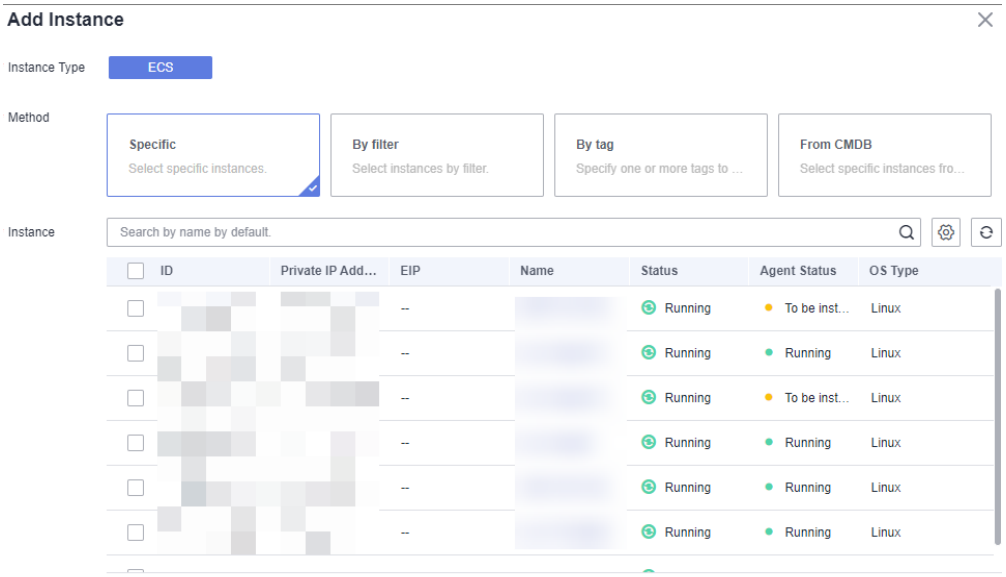


Table 12-4 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-5**.

Table 12-5 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.4.3 Stopping an ECS

You can use the **Stopping an ECS Instance** card to create a task to stop one or more ECSs.

Creating a Task for Stopping an ECS

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Stopping an ECS Instance** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-6**.

Figure 12-4 Stopping an ECS

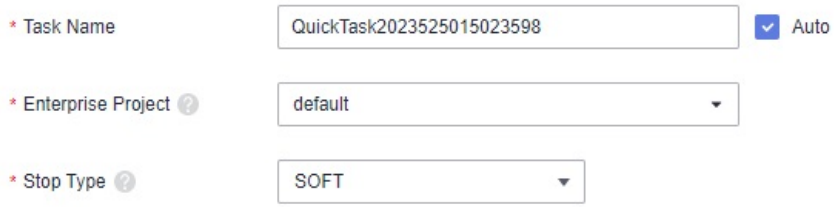


Table 12-6 Parameters for stopping an ECS

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.
Stop Type	ECS shutdown type. The default value is **SOFT**. • **SOFT**: normal shutdown • **HARD**: forcible shutdown

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. A maximum of 100 instances can be selected for a single task.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-7**.

Figure 12-5 Selecting an instance

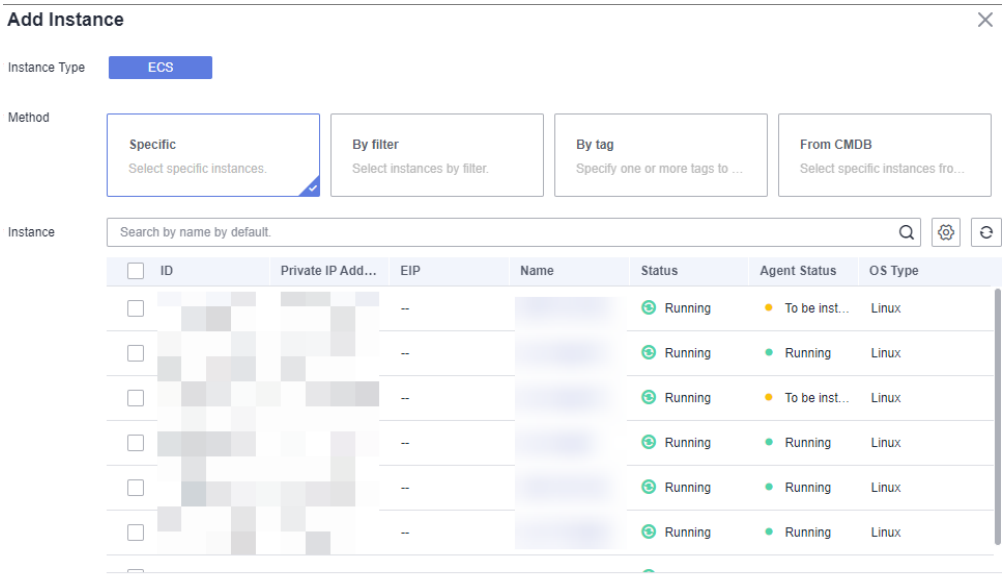


Table 12-7 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-8**.

Table 12-8 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.

Category	Parameter	Description
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.4.4 Restarting an RDS DB Instance

You can use the **Restart the RDS DB Instance** card to create a task to restart one or more RDS DB instances.

Creating a Task for Restarting an RDS DB Instance

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Restart the RDS DB Instance** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-9**.

Figure 12-6 Restarting an RDS DB instance

Table 12-9 Parameters for restarting an RDS DB instance

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. Up to 20 instances can be restarted in a single task.
2. The default instance type is **RDS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-10**.

Figure 12-7 Selecting an instance

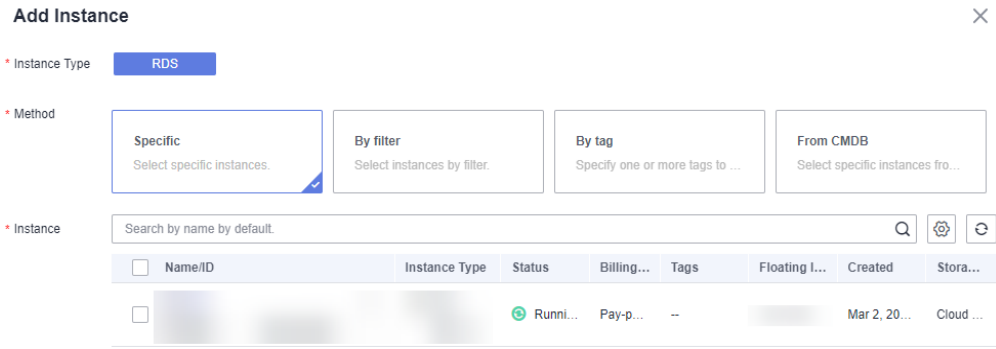


Table 12-10 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an RDS DB instance under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain RDS DB instances under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-11**.

Table 12-11 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.4.5 Changing an ECS Non-Administrator Password

You can use the **Change ECS Non-Administrator Password** card to change the password of a non-administrator user.

Prerequisites

UniAgents have been installed for all ECSs, and are in the running state.

Creating a Task for Changing the ECS Non-administrator Password

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Change ECS Non-Administrator Password** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-12**.

Figure 12-8 Changing the ECS non-administrator password

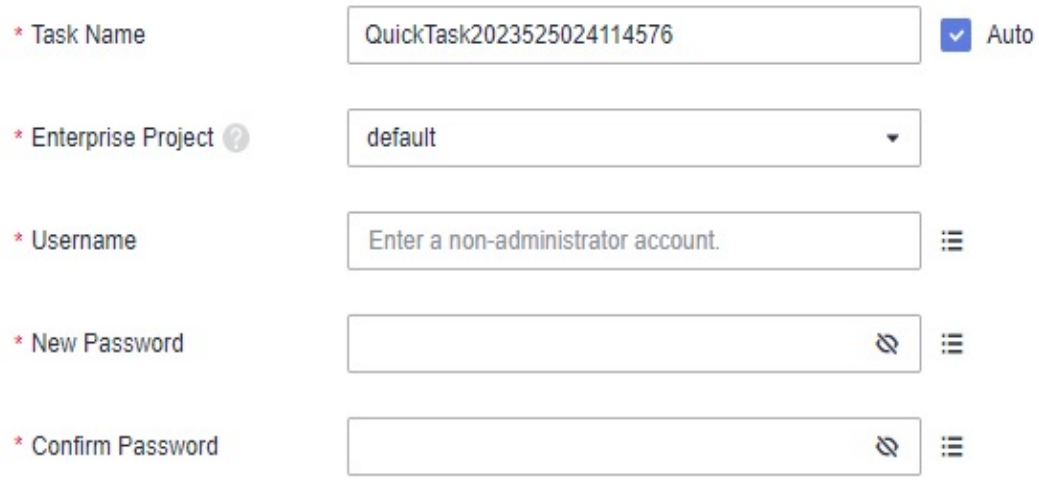


Table 12-12 Parameters for changing the ECS non-administrator password

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.
Username	Non-administrator user name. • Enter up to 64 characters. Only letters, digits, and underscores (_) are allowed. • You can also click and select a parameter from the parameter library.
New Password	New password of a non-administrator user. • Enter 8 to 26 characters. • The password can contain only letters, digits, and special characters, and must contain at least three of the four types. • Cannot contain the username or the username spelled backwards. • You can also click and select a parameter from the parameter library.

Parameter	Description
Confirm Password	New password of a non-administrator user. • The value must be the same as the new password. • Enter 8 to 26 characters. • The password can contain only letters, digits, and special characters, and must contain at least three of the four types. • Cannot contain the username or the username spelled backwards. • You can also click and select a parameter from the parameter library.

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. A maximum of 100 instances can be selected for a single task.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-13**.

Figure 12-9 Selecting an instance

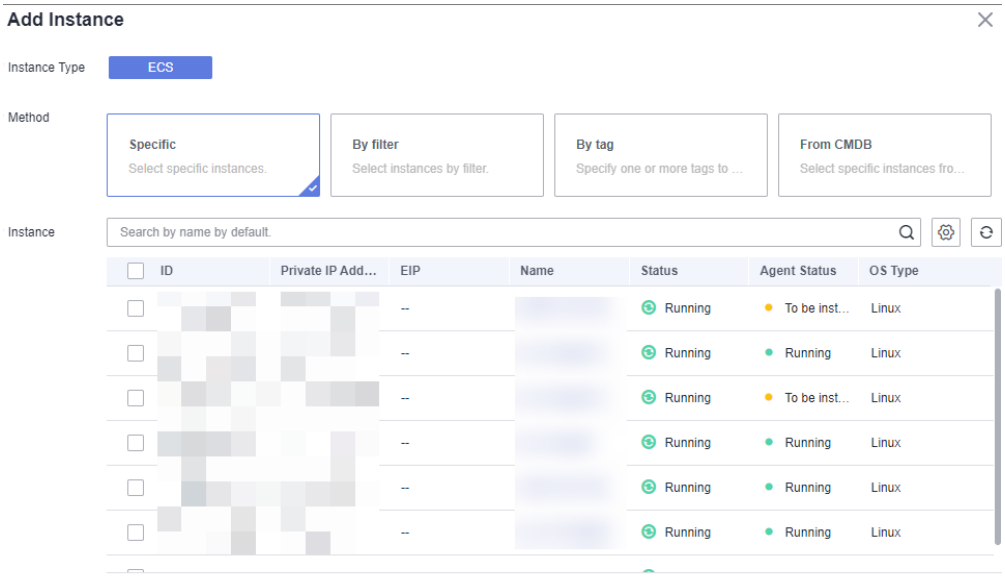


Table 12-13 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.

Selection Method	Description
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-14**.

Table 12-14 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.4.6 Restarting a CCE Workload

You can use the **Restart CCE Workload** card to create a task to restart one or more CCE workloads.

NOTE

Only StatefulSets and Deployments can be restarted.

Creating a Task for Restarting a CCE Workload

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Restart CCE Workload** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-15**.

Figure 12-10 Restarting a CCE workload

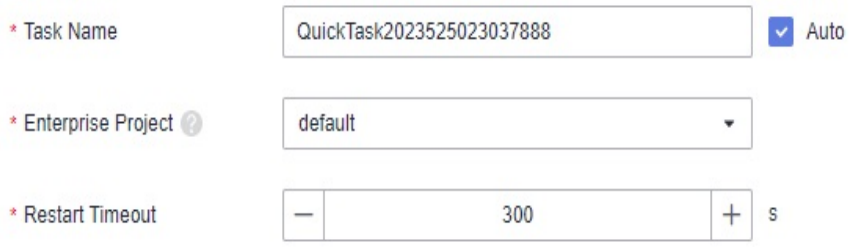


Table 12-15 Parameters for restarting a CCE workload

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.
Restart Timeout	Timeout duration for restarting a CCE workload. Enter an integer from 10 to 600.

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. Up to 10 workload instances can be restarted in a single task.
2. The default instance type is **CCE**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-16**.

Figure 12-11 Creating a task for restarting a CCE workload

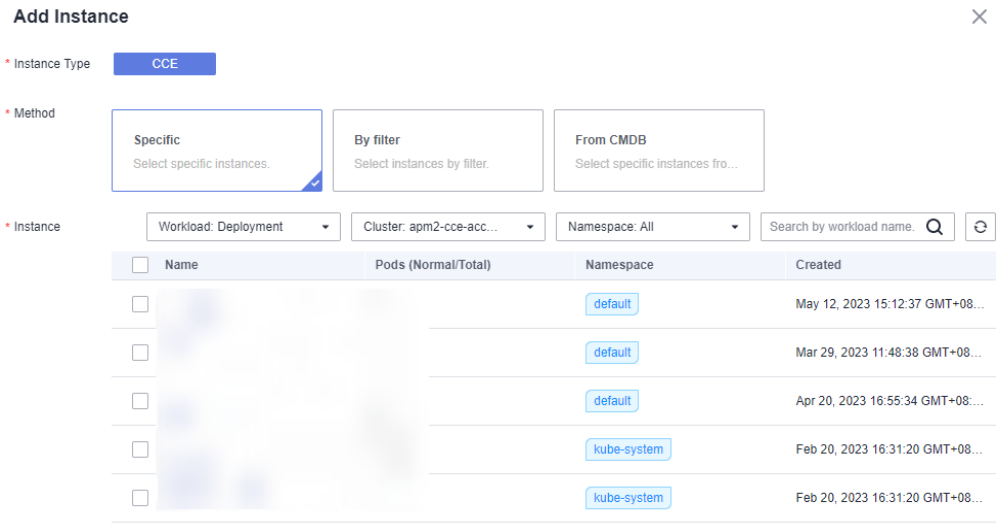


Table 12-16 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	Select an instance by workload type, cluster name, and namespace. This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select a CCE instance under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain CCE instances under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-17**.

Table 12-17 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.4.7 Clearing Disk Space

You can use the **Clearing Disk Space** card to create a task for clearing the disk space of a specified directory on an ECS.

Prerequisites

UniAgents have been installed for all ECSs, and are in the running state.

Creating a Task for Clearing Disk Space

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scenarios**. On the displayed page, click the **Clearing Disk Space** card, or choose > **Create Task** in the upper right corner of the card.

Step 4 Set parameters by referring to **Table 12-18**.

Figure 12-12 Clearing disk space

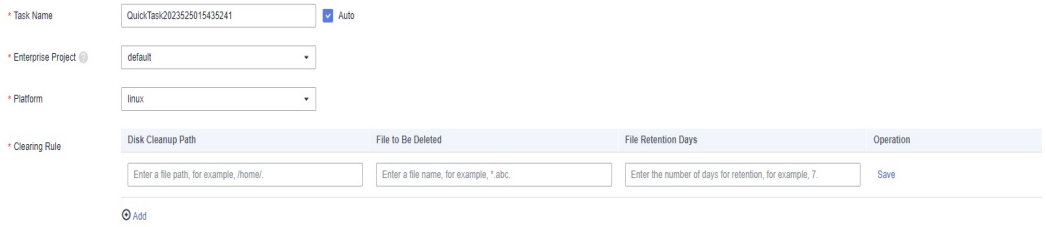


Table 12-18 Parameters for clearing disk space

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.
Enterprise Project	Select the enterprise project to which the task belongs.
Platform	Select a platform that the task runs on. Currently, only Linux is supported.
Clearing Rule	Enter a disk cleanup path, name of the file to be deleted, and file retention days, and click **Save** in the **Operation** column. You can also click **Add** to add more rules. **NOTE** • Files in the **/**, **/bin**, **/sbin**, **/etc**, **/usr**, **/usr/bin**, **/usr/sbin**, **/boot**, and **/lib** directories cannot be deleted. • You can enter an absolute path. • Paths for fuzzy match (for example, **/var/logs/*/a.log**) are not supported. • Recursive paths (for example, **/var/logs/**/a.log**) are not supported. • Files generated 1 to 1000 days ago can be deleted from 00:00 on the current day.

Step 5 Select an instance.

1. Click **Add**. The instance selection page is displayed. A maximum of 100 instances can be selected for a single task.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-19**.

Figure 12-13 Selecting an instance

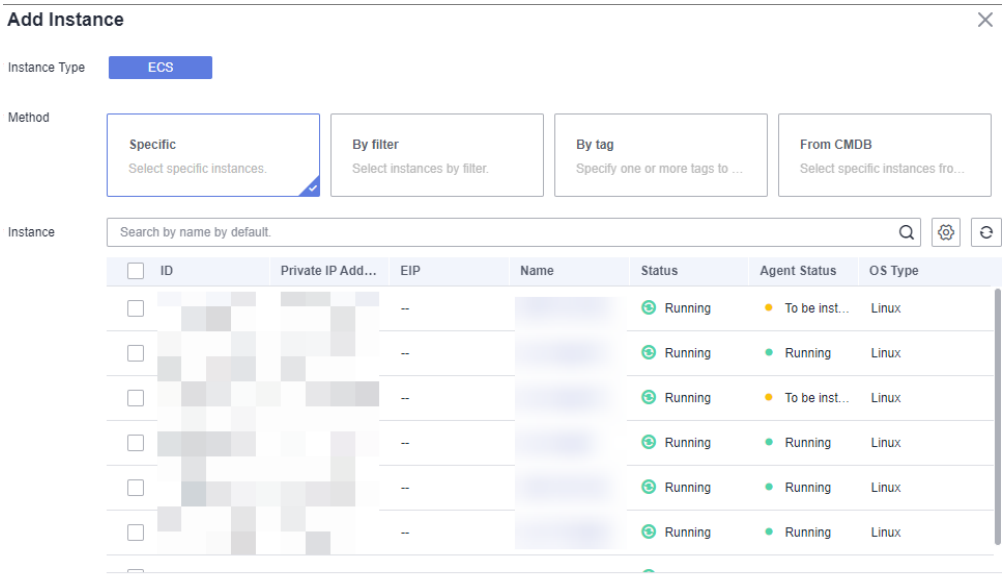


Table 12-19 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

Step 6 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-20**.

Table 12-20 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 7 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

12.5 Scheduled O&M

The **Scheduled O&M** page displays the execution records of all scheduled tasks. You can create and manage scheduled tasks on this page. After scheduled tasks are created, operations (such as script execution and file/scenario/job management) are performed at a specified time or periodically. You can create up to 100 scheduled tasks.

Creating a Task

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scheduled O&M** and click **Create Scheduled Task** in the upper right corner to create a task.

Step 4 Set parameters by referring to **Table 12-21**.

Figure 12-14 Basic information for creating a scheduled task

Table 12-21 Parameters for creating a task

Parameter	Description
Task Name	User-defined task name. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. By default, **Auto** is selected, which means that the system automatically generates a task name.

Step 5 Set parameters by referring to **Table 12-22**.

Figure 12-15 Creating a scheduled task

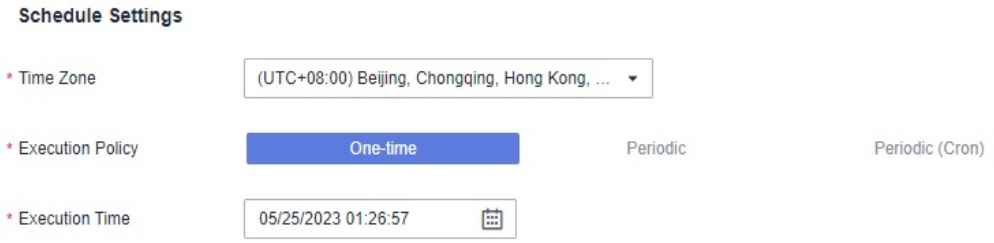


Table 12-22 Parameters for creating a scheduled task

Parameter	Description
Time Zone	Time zone of the scheduled task. You can select a desired time zone from the drop-down list.
Execution Policy	Execution policy of a scheduled task. Options: • **One-time**: The task is performed once at a specified time. • **Periodic**: The task is executed regularly based on the preset period. • **Periodic (Cron)**: The task is performed based on the configured cron expression.
Execution Time	Time when a scheduled task is executed.
Execution Interval	This parameter is mandatory only when **Execution Policy** is set to **Periodic**. • **Daily**: every day in the period. • **Weekly**: Select one or more days from a week. By default, all days in a week are selected.

Parameter	Description
Execution Rule	This parameter is mandatory only when **Execution Policy** is set to **Periodic (Cron)**. The task is performed based on the configured cron expression. Currently, the execution time can only start from minute 0 (ascending order) and the minimum interval is 30 minutes. For details about the rules and configuration methods, click **View Details** on the console.

Step 6 Set notifications by referring to **Table 12-23**.

Figure 12-16 Notification settings

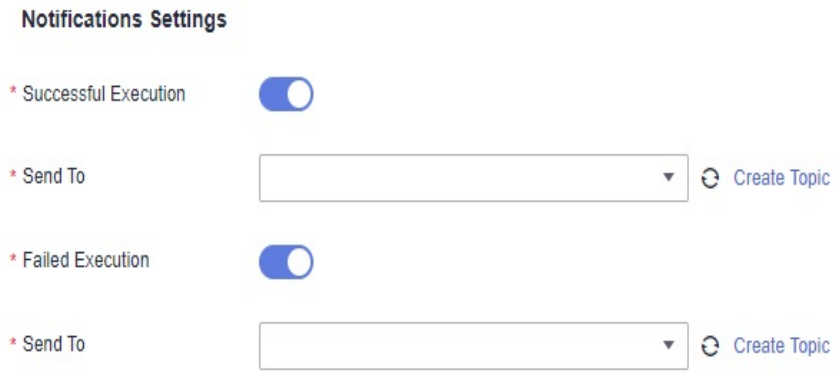


Table 12-23 Notification parameters

Parameter	Description
Successful Execution	When a task is successfully executed, a notification is sent to related personnel. By default, this function is disabled. • **Send To**: Select one or more recipients from the drop-down list. • You can also click **Create Topic** for notification. Specifically, **create a topic** and add subscriptions to the topic for notification.
Failed Execution	When a task fails to be executed, a notification is sent to related personnel. By default, this function is disabled. • **Send To**: Select one or more recipients from the drop-down list. • You can also click **Create Topic** for notification. Specifically, **create a topic** and add subscriptions to the topic for notification.

NOTE

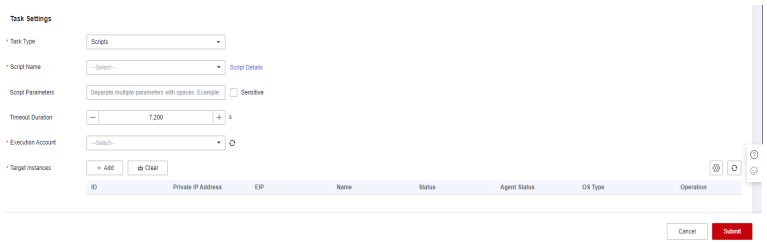
Notifications can be sent by email or SMS.

Step 7 Set a task. The task type can be **Scripts**, **Packages**, **Scenarios**, and **Jobs**.

- Set a script execution task.
  a. Set **Task Type** to **Scripts**.
  b. Enter the script name, script parameters, timeout duration, and execution account. The **Script Name** drop-down list displays only released scripts. Script version, which is automatically obtained based on the selected script name.

     If **Sensitive** next to **Script Parameters** is selected, the content you enter will not be explicitly displayed in the **Script Parameters** text box.

     Figure 12-17 Setting a script execution task

  c. Select target instances. Specifically, click **Add**. The instance selection page is displayed. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-24**.

     Table 12-24 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	■ Enter filter attributes and values to search for instances. ■ If there are multiple filter criteria, the search is performed based on the AND relationship. ■ This method also takes effect for instances added later.
By tag	■ Set tag keys and values, and specify one or more tags to select instances. ■ If there are multiple tags, the search is performed based on the AND relationship. ■ This method also takes effect for instances added later.

Selection Method	Description
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: ■ **Static**: Select an ECS under a specified CMDB application. ■ **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

- Set a package management task.
  a. Set **Task Type** to **Packages**.
  b. Enter the package name, version, type, timeout duration, storage path, and execution account. Only released packages are displayed in the drop-down list. Versions are automatically displayed based on the packages you select.

  Figure 12-18 Setting a package management task

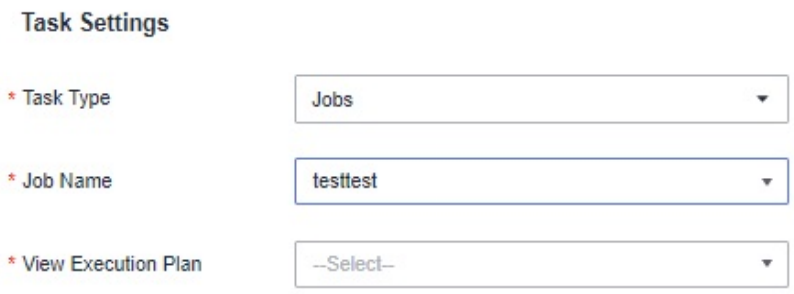
  c. Select target instances. Specifically, click **Add**. The instance selection page is displayed. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-24**.
- Set a scenario task.
  a. Set **Task Type** to **Scenarios**.
  b. Select a scenario from the drop-down list. For details about operations in different scenarios, see **12.4 Scenarios**.

  Figure 12-19 Setting a scenario task

- Set a job management task.
  a. Set **Task Type** to **Jobs**.
  b. Select a job name and an execution plan from the drop-down lists.

Figure 12-20 Setting a job management task



Step 8 If needed, expand **More** to set the review configuration and execution policy by referring to **Table 12-25**.

Table 12-25 More settings

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, the setting cannot be changed. To change the review settings for default scenarios, go to the **Tool Market** to set atomic cards; for job execution plans, go to the **Jobs** page; for packages, go to the **Packages** page; for scripts, go to the **Scripts** page.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Step 9 Click **Submit** to create a scheduled task.

----End

More Operations

After a task is created or executed, you can view **Task Name**, **Task Type**, **Execution Policy**, **Latest Execution**, **Updated By**, **Updated**, **Start/Stop Task**, and **Operation** on the task list page. You can also perform the operations listed in **Table 12-26**.

Table 12-26 Related operations

Operation	Description
Starting or stopping a task	Click the button in the **Start/Stop Task** column to start or stop a task.
Modifying a task	Click **Modify** in the **Operation** column to modify a task. You can modify a task only when the task is closed.
Viewing execution records	Click **Execution Records** in the **Operation** column to view the task execution details (such as task name/ID/ status, execution time, and reviewer).
Deleting a task	Click **Delete** in the **Operation** column to delete a task. You can delete a task only when the task is closed.
Searching for a task	You can search for tasks by task name, creator, modifier, latest execution result, task type, and enterprise project. Enter a keyword in the search box in the upper right corner and click  .
Hiding/Showing columns in the task list	Click  and select or deselect columns to display.
Refreshing the task list	Click  to refresh the task list.

12.6 Tasks

The **Tasks** page displays the execution records of all tasks. You can execute a created task on this page.

Supported Operations

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scheduled O&M** and click **Create Scheduled Task** in the upper right corner to create a task.

Step 4 View the task name, type, status, and duration on the task list page. You can also perform the operations listed in **Table 12-27**.

Table 12-27 Supported operations

Operation	Description
Viewing the task execution status	Click the name of an executed task to view the details, including the execution log, executor, and task content. • By default, execution records of the last seven days are displayed. You can select **Last 1 day**, **Last 1 week**, **Last 30 days**, or **Custom** from the time drop-down list in the upper right corner. **NOTE** By default, the update time is not displayed in the list. You can click  in the upper right corner of the list and select **Updated** from the drop-down list to view the update time. • The system stores execution records for up to one year. • The custom time range can be 30 days at most.
Executing a task	• Click **Execute** in the **Operation** column of a task that has never been executed. • Click **Re-execute** in the **Operation** column of a task that has ever been executed.
Deleting a task	Click **Delete** in the **Operation** column to delete a task. **Delete** is displayed in the **Operation** column only when tasks have never been executed.
Searching for a task	You can search for a task by enterprise project, task name, executor, task type, or task status. Enter a keyword in the search box in the upper right corner and click  .
Hiding/Showing columns in the task list	Click  and select or deselect columns to display.
Refreshing the task list	Click  to refresh the task list.

----End

12.7 Parameters

The **Parameters** page displays all existing parameters. You can create, modify, or delete parameters on this page. When changing an ECS non-administrator password and creating a job, you can use created parameters to quickly set user password and global parameters. You can create up to 25 parameters.

Creating a Parameter

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Parameters** and click **Create Parameter** in the upper right corner.

Step 4 Set parameters by referring to **Table 12-28**.

Figure 12-21 Setting parameters

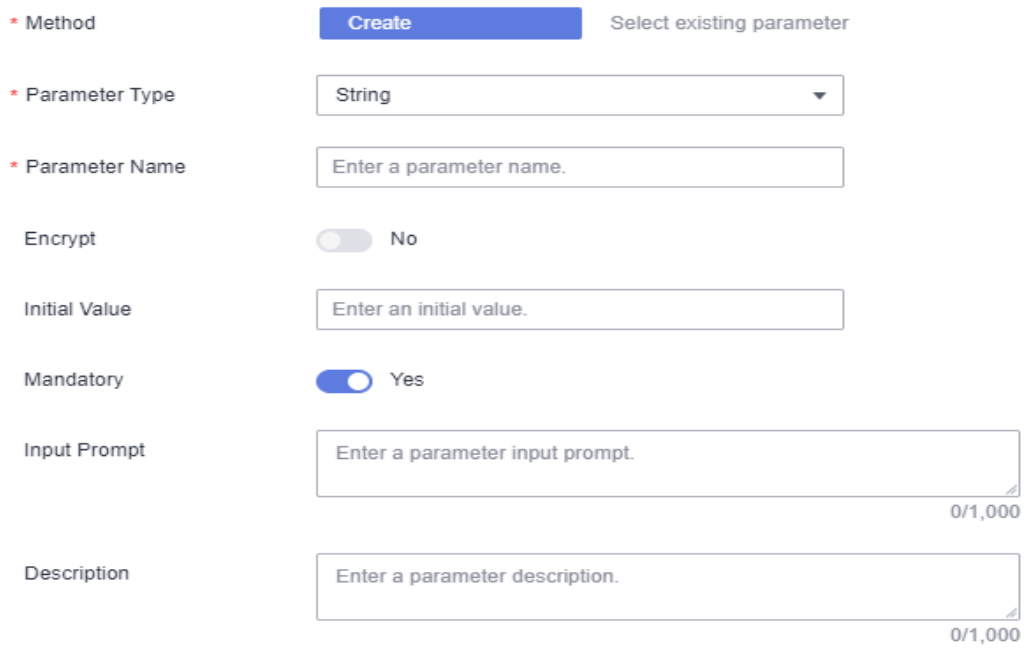


Table 12-28 Parameters

Parameter	Description
Parameter Type	Type of a parameter, which can only be **String**.
Parameter Name	Name of a parameter. Enter up to 64 characters. Only letters are allowed.
Encrypt	By default, this option is disabled. Encryption is not supported at present.
Initial Value	Initial parameter value. Enter up to 1000 characters.
Mandatory	Specifies whether the parameter is mandatory when it is referenced. By default, this option is enabled.
Input Prompt	Message displayed when the parameter is referenced. Enter up to 1000 characters.
Description	Parameter description. Enter up to 1000 characters.

Step 5 Click **Save**.

----End

More Operations

After a parameter is created, you can view the name, type, and creator of the parameter on the parameter list page. You can also perform the operations listed in **Table 12-29**.

Table 12-29 Related operations

Operation	Description
Modifying a parameter	Click **Modify** in the **Operation** column.
Deleting a parameter	Click **Delete** in the **Operation** column.

12.8 Jobs

The **Jobs** page displays all job information. You can create a job, create or delete an execution plan, and release the execution plan as a service. You can view the released service in **12.4 Scenarios**.

Precautions

- You can create up to 1000 jobs.
- Up to 20 global parameters, 20 steps, and 50 execution plans can be created for each job.

Creating a Job

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Jobs**. On the displayed page, click **Create Job**.

Step 4 Set parameters by referring to **Table 12-30**.

Figure 12-22 Creating a job

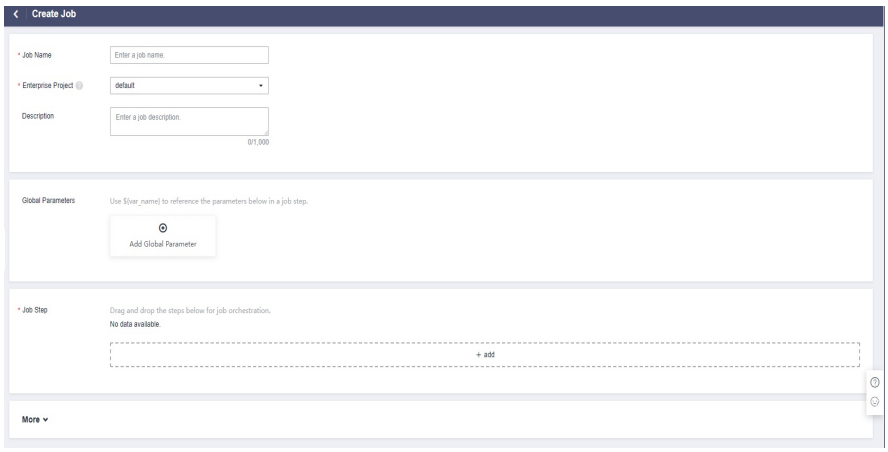


Table 12-30 Parameters for creating a job

Parameter	Description
Job Name	Name of a job. Enter up to 64 characters. Only letters, digits, and underscores (_) are allowed.
Enterprise Project	Select the enterprise project to which the job belongs.
Description	Description of a job. Enter up to 1000 characters.

Step 5 Add global parameters.

1. On the **Create Job** page, click **Add Global Parameter** in the **Global Parameters** area.
2. Set global parameters by referring to **Table 12-31**.

Figure 12-23 Adding global parameters

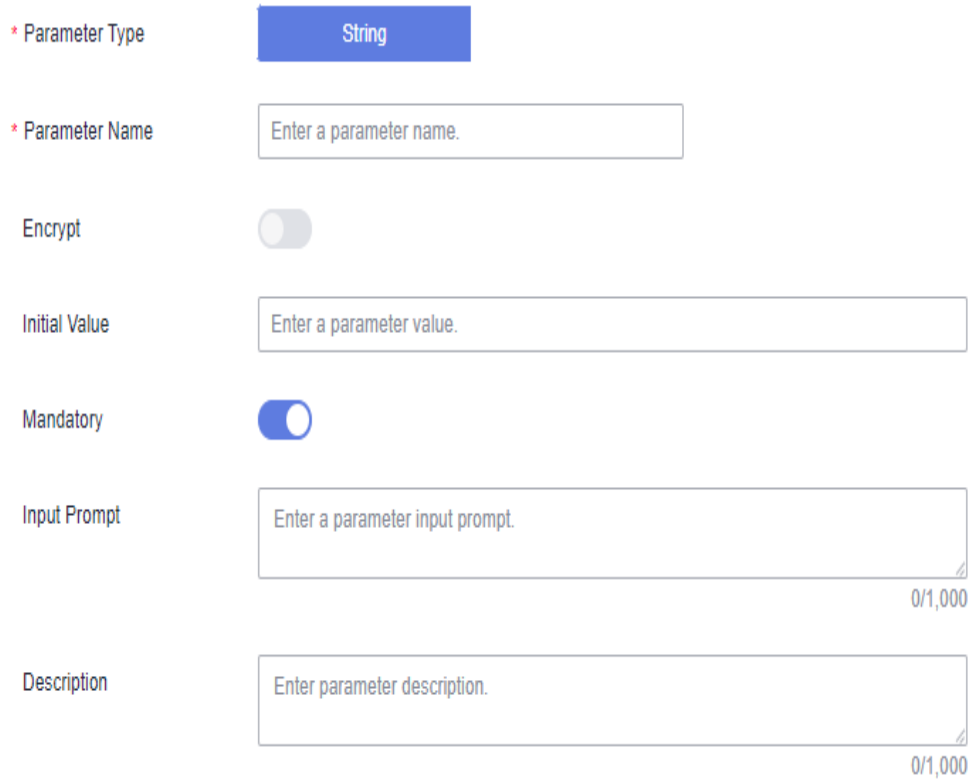


Table 12-31 Global parameters

Parameter	Description
Method	Mode for adding parameters. Options: **Create** and **Select existing parameter**.
Parameter Type	– **Create**: The parameter type can be **String** (default) or **Host**. – **Select existing parameter**: The parameter type can only be **String**.
Parameter Name	– **Create**: The parameter name can contain up to 64 letters. – **Select existing parameter**: Select a parameter from the parameter library. After a parameter is selected from the parameter library, the parameter is saved in the job and is no longer associated with the parameter in the parameter library.
Encrypt	By default, this option is disabled. Encryption is not supported at present.
Initial Value	– For parameter type **String**, the initial value can contain up to 1000 characters. – For parameter type **Host**, click **Add** to add up to 100 instances.

Parameter	Description
Mandatory	Specifies whether the parameter is mandatory. The default value is **Yes**.
Input Prompt	Parameter input prompt. Enter up to 1000 characters.
Description	Parameter description. Enter up to 1000 characters.

3. Click **Save**. You can also click **Submit and Save to Parameter Library** to add the parameter and create a parameter with the same name in the parameter library.

Step 6 Add a job step.

1. On the **Create Job** page, click **Add** in the **Job Step** area.
2. Set job step parameters by referring to **Table 12-32**.

Figure 12-24 Adding a job step (script)

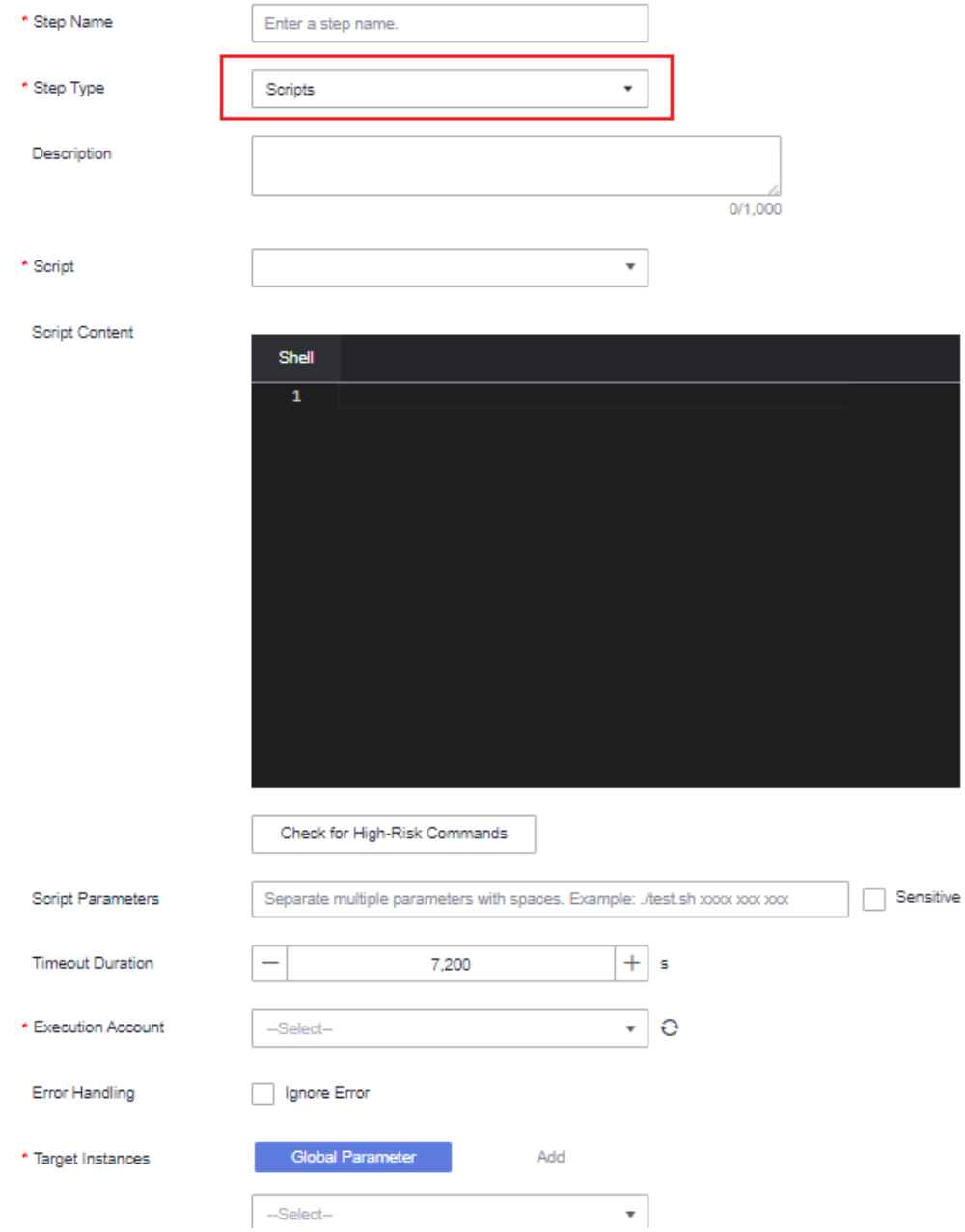


Figure 12-25 Adding a job step (package)

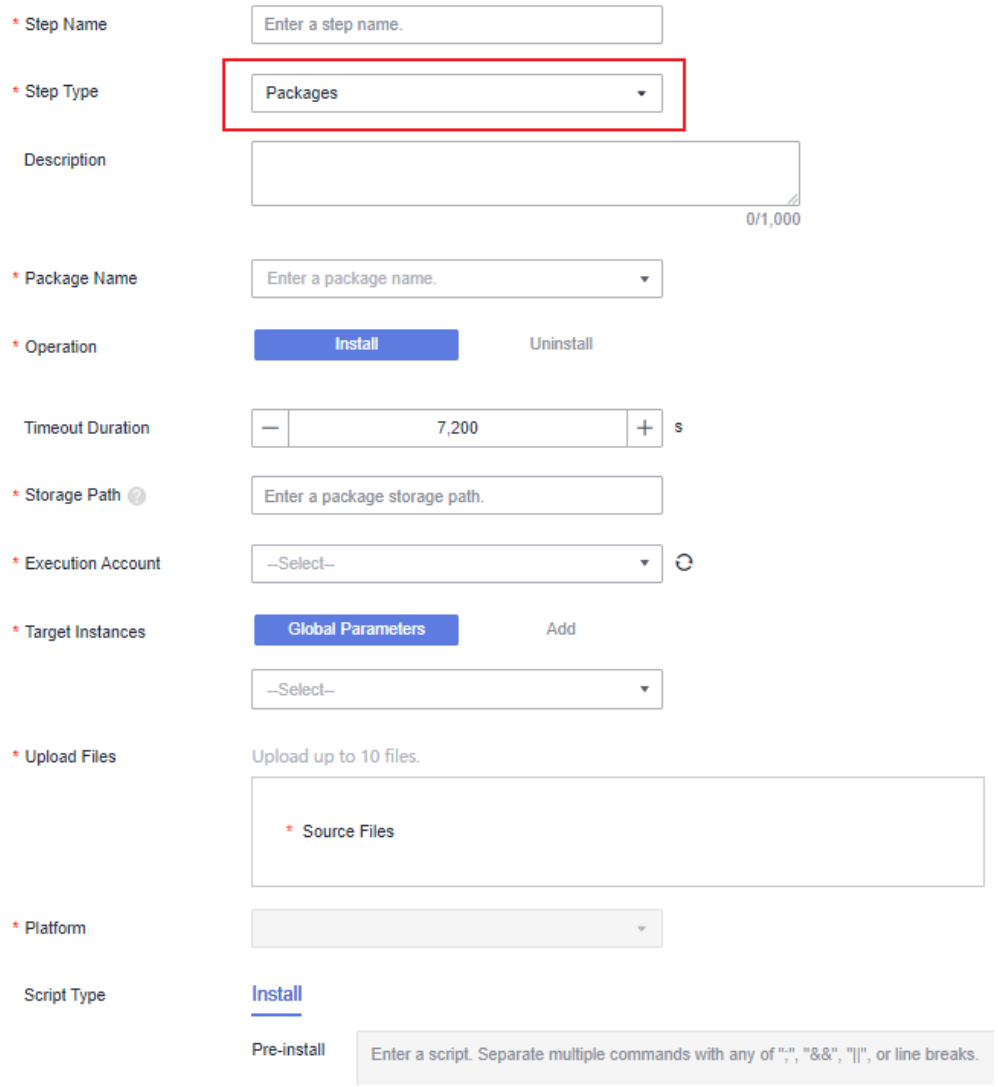


Table 12-32 Parameters for adding a step

Category	Parameter	Description
-	Step Name	Name of a step. Enter up to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Step Type	Type of a step. Options: **Scripts**, **Packages**, and **Pause**.
	Description	Step description. Enter up to 1000 characters.
	Timeout Duration	Timeout duration of a script installation or uninstallation task. The value must range from 1 to 43,200.

Category	Parameter	Description
	Execution Account	Name of the OS account that executes the script.
	Target Instances	– **Global Parameter**: Select a host parameter from the drop-down list. – **Add**: Manually add ECSs or select them from CMDB.
Scripts	Script	Select a script from the script list. The drop-down list displays only released scripts.
	Script Content	– Script version and script content. – After setting the parameters, click **Check for High-Risk Commands**. High-risk commands undergo regular expression verification. If the verification fails, risks may occur. For details about high-risk commands, see **Table 12-48**.
	Script Parameters	Separate multiple parameters with spaces. Global variables in the string format can be referenced using *${var_name}*.
	Sensitive	If you select **Sensitive**, the content you enter will not be displayed in the script parameter box. By default, **Sensitive** is not selected.
	Error Handling	– If you select **Ignore Error**, the system continues to execute the next step after the current job step fails. – If you do not select **Ignore Error**, the job will be paused after a job step fails. In that case, click **Retry** or skip this step.
Packages	Package Name	Name of a package. Select a package name from the drop-down list. Only released packages are displayed in the drop-down list.
	Version	Software version, which is automatically obtained based on the selected package name.
	Operation	Operation type, which can be **Install** or **Uninstall**.
	Storage Path	Global variables in the string format can be referenced using *${var_name}*.
	Source Files	Enter the source of the selected package version. For details, see **Table 12-40**.

Category	Parameter	Description
	Platform	Platform on which the package runs. Currently, only Linux is supported.
	Script Type	– If **Operation** is **Install**, **Script Type** is **Install**. The **Pre-install** dialog box displays the pre-installation script. The **Install** dialog box displays the installation script. Up to 1000 characters can be displayed. – If **Operation** is **Uninstall**, **Script Type** is **Uninstall**. The **Uninstall** dialog box displays the uninstallation script. Up to 1000 characters can be displayed.
Pause	Description	Step description. Enter up to 1000 characters.

Step 7 Perform the operations listed in **Table 12-33** if needed.

Table 12-33 Related operations

Parameter	Description
Execution Policy	• **Batch Release**: specifies whether to enable batch release. By default, this function is disabled. • **Instances for Each Batch**: number of instances on which tasks can be executed at the same time. • **Interval**: interval for executing each batch of tasks.
Review	• Manual review. If there is any risky operation, a review is recommended. By default, this function is disabled.

Step 8 Click **Save**.

----End

NOTE

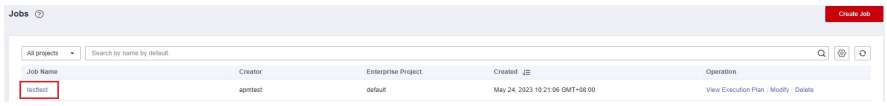
- If the information for adding a job step is incomplete, "Insufficient information" will be displayed after you save the settings.
- To adjust step sequence, drag at the beginning of the row where the job step is located.
- To delete a step, click in the row that contains the target step.

Creating an Execution Plan

After a job is created, create an execution plan for the job:

Step 1 In the navigation pane, choose **Jobs**. Then, click the desired job.

Figure 12-26 Clicking a job



Step 2 Click **Select Plan** in the upper right corner.

Step 3 On the plan list page, click **Create Execution Plan** in the upper right corner.

Step 4 Set parameters by referring to **Table 12-34**.

Figure 12-27 Creating an execution plan

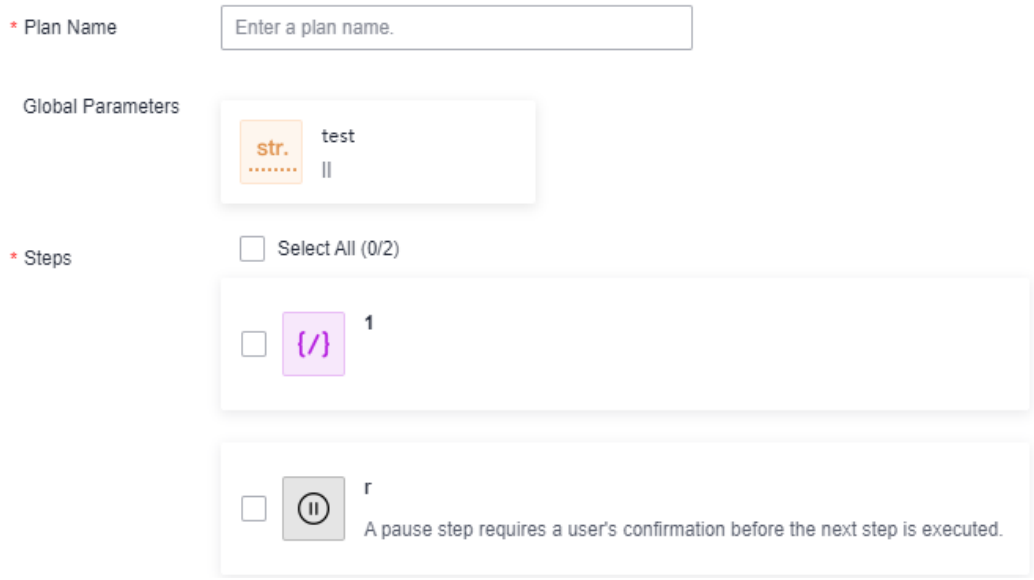


Table 12-34 Parameters for creating an execution plan

Parameter	Description
Plan Name	Name of a plan. Enter up to 64 characters. Only letters, digits, and underscores (_) are allowed.
Global Parameters	Global parameters that have been added. You can view their details and change their initial values.
Steps	Steps to be performed. You can select one or more steps. Click a step to view its details.

Step 5 Click **Submit**.

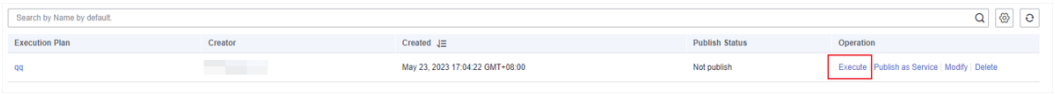
----End

Executing a Plan

After an execution plan is created, execute it:

Step 1 In the navigation pane, choose **Jobs**. Then, locate the desired job, and click **View Execution Plan** in the **Operation** column. On the displayed page, locate the desired plan and click **Execute** in the **Operation** column.

Figure 12-28 Executing a plan



Step 2 On the task creation page, click **Execute**.

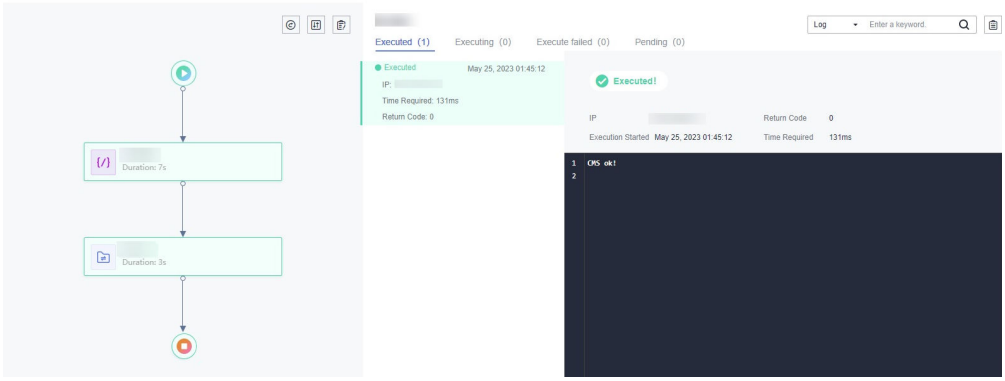
NOTE

If you set **Parameter Type** to **Host** during global parameter adding and click **Execute**, the message "Are you sure you want to perform the operation on the following instance?" will be displayed. Click **Yes**.

Step 3 On the task execution page, view the task execution status.

-  : The task fails to be executed.
- : The task has been executed successfully.
-  : The task is being executed or has been paused.
- : The task has not been executed yet.

Figure 12-29 Plan execution details



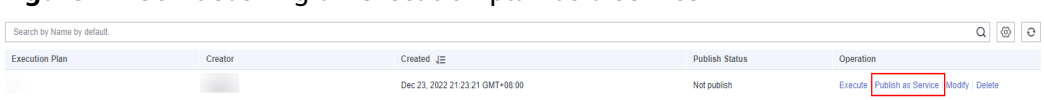
----End

Publishing an Execution Plan as a Service

The execution plan of a job can be published as a service card. After it is published, you can view it on the **Scenarios** page. To publish an execution plan as a service, you must have the **cms:publish:update** or **cms:toolmarket:update** permission. For details about operations related to service cards, see 12.4 Scenarios.

Step 1 In the navigation pane, choose **Jobs**. Then, locate the desired job, and click **View Execution Plan** in the **Operation** column. On the displayed page, locate the desired plan and click **Publish as Service** in the **Operation** column.

Figure 12-30 Publishing an execution plan as a service



Step 2 Enter basic information and click **OK**. For details, see **Table 12-35**.

Figure 12-31 Publishing a plan as a service

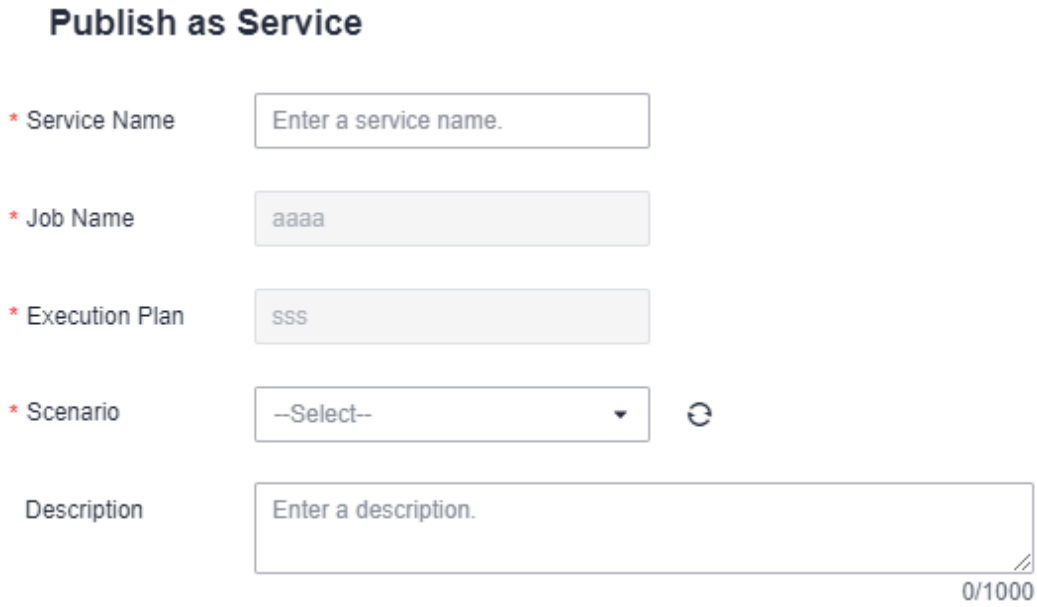


Table 12-35 Parameters for publishing a plan as a service

Parameter	Description
Service Name	Name of a service. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Scenario	Scenario where the service is used. Options: **Common**, **Software Deployment**, **Troubleshooting**, and **Routine Inspection**.
Description	Description of the service to be released. Enter up to 1000 characters.

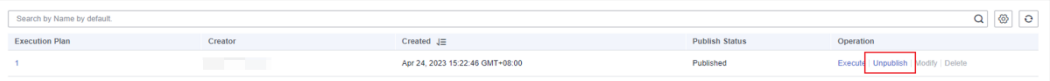
----End

Canceling a Published Plan

You can cancel an execution plan that has been published as a service. After the published plan is canceled, it will be removed from the **Scenarios** page. Before canceling an execution plan, check whether it has been referenced by a scheduled O&M scenario. If yes, delete the referenced scenario first.

Step 1 In the navigation pane, choose **Jobs**. Then, locate the desired job, and click **View Execution Plan** in the **Operation** column. On the displayed page, locate the desired plan and click **Unpublish** in the **Operation** column.

Figure 12-32 Canceling a published plan



Step 2 In the displayed dialog box, click **Yes** to cancel a published plan.

----End

More Operations

After a job is created, you can click the job name to go to its details page and view the basic information, global parameters, and steps of the job. You can also perform the operations listed in **Table 12-36**.

Table 12-36 Related operations

Operation	Description
Modifying a job	Click **Modify** in the upper right corner to modify a job. **NOTE** To use the modified job, you need to create an execution plan.
Selecting a plan	Click **Select Plan** in the upper right corner.
Deleting a job	Click **Delete** in the upper right corner.
Modifying a plan	Locate the target execution plan and click **Modify**. Before modifying a plan, check whether the plan has been referenced by a scheduled O&M scenario. If yes, delete the referenced scenario first.
Deleting a plan	Locate the target execution plan and click **Delete**. Before deleting a plan, check whether the plan has been referenced by a scheduled O&M scenario. If yes, delete the referenced scenario first.

12.9 Scripts

The **Scripts** page displays information about all existing scripts. You can create, modify, or copy a script. After a script is created, you can create an execution task for the script. Alternatively, you can create a task and execute and view it on the **Tasks** page. Each script supports up to 20 versions. Each user can create up to 1000 script versions.

Creating a Script

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Scripts** and click **Create Script** in the upper right corner.

Step 4 Set parameters by referring to **Table 12-37**.

Figure 12-33 Creating a script

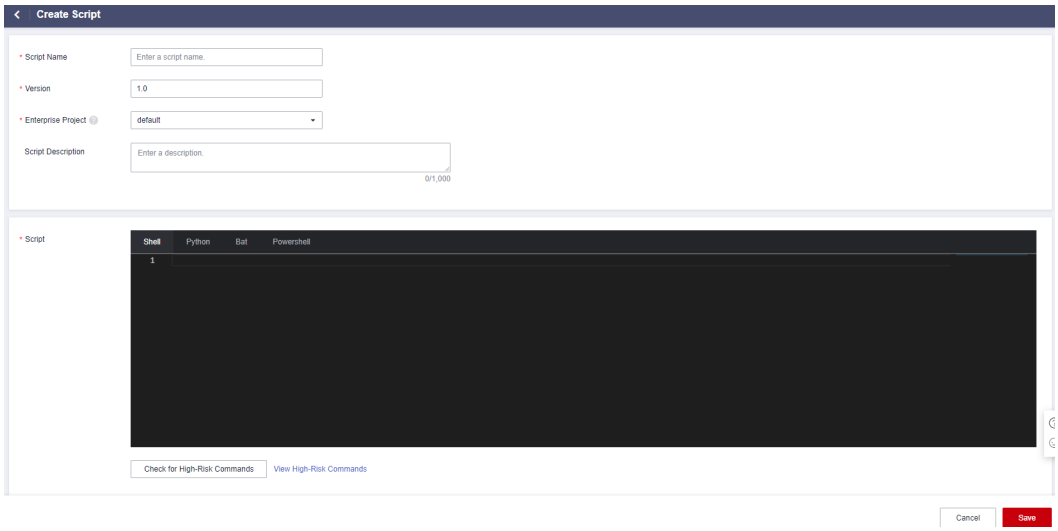


Table 12-37 Script information description

Category	Parameter	Description
-	Script Name	Name of a script. Enter up to 64 characters. Only letters, digits, and underscores (_) are allowed.
	Version	Version of the script. Enter the actual value.
	Enterprise Project	Select the enterprise project to which the script belongs.
	Script Description	Description of the script. Enter up to 1000 characters.

Category	Parameter	Description
	Script	• Manually enter commands. Currently, Shell, BAT, PowerShell, and Python scripts can be executed. A script can contain up to 30,000 bytes. **NOTE** – Shell and Python scripts can be executed only on Linux hosts. – BAT and PowerShell scripts can be executed only on Windows hosts. • The UniAgent reads the standard output of the script and writes it into logs. The **print()** output of Python has a cache and may not be updated to the standard output in real time. As a result, the execution logs of the Python script cannot be updated in real time. To output Python logs in real time, use any of the following methods: – Use **sys.stdout.flush()** to print the output. – Use **sys.stderr.write()** to print the output. – Use **print(message.flush=True)** to print the output. • After setting the parameters, click **Check for High-Risk Commands**. High-risk commands undergo regular expression verification. If the verification fails, risks may occur. For details about high-risk commands, see **Table 12-48**.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.

Step 5 Click **Save**.

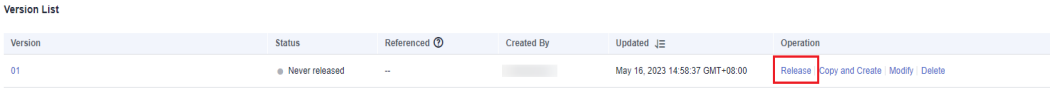
----End

Releasing a Script

After a script is created, it is in the **Unreleased** state. The script task can be executed only after the script is released.

Step 1 In the navigation pane, choose **Scripts**. On the version management page, locate the row that contains the target version and click **Release** in the **Operation** column.

Figure 12-34 Releasing a script



Step 2 On the release confirmation dialog box that is displayed, click **Yes**.

----End

Executing a Script

After a script is released, you can execute the script task on the script list page. Script execution depends on the UniAgent capability. You need to ensure that the UniAgent has been installed and is running on the ECS where the script is to be executed.

Step 1 In the navigation pane, choose **Scripts**. On the script management page, locate the target script and click **Execute** in the **Operation** column.

Step 2 Specify **Script Parameters**, **Timeout Duration**, and **Execution Account**. You can also select **Sensitive** for script parameters. If **Sensitive** is selected, the entered content will not be explicitly displayed in the script parameter box.

Figure 12-35 Script parameters

Step 3 Select target instances.

1. Click **Add**. The instance selection page is displayed.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-38**.

Figure 12-36 Adding instances

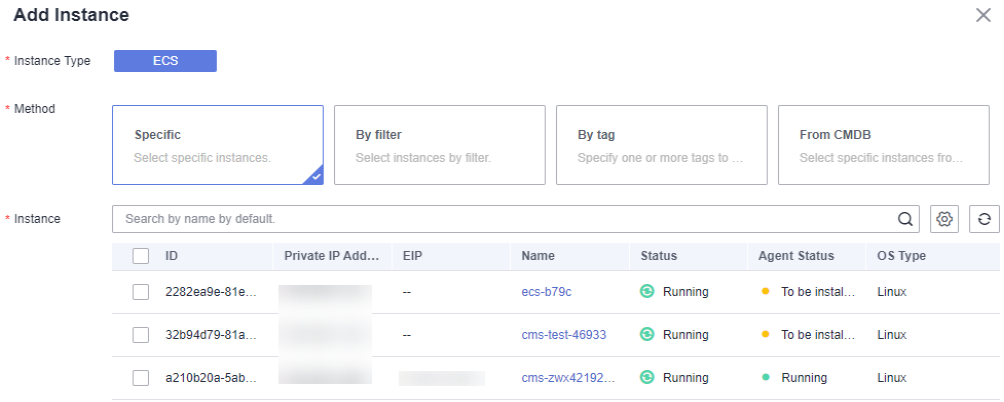


Table 12-38 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

3. Click **OK**.

Step 4 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

More Operations

After the script is created, you can view the script name, version, and creation time on the script list page. You can also perform the operations listed in **Table 12-39**.

Table 12-39 Related operations

Operation	Description
Managing a script version	Click **Manage Version** in the **Operation** column. On the version management page that is displayed, view and modify the script version information and execute the script as required.
Copying and creating a script	On the version management page, click **Copy and Create** in the **Operation** column of a released or unreleased script and copy the original script content to create a script.
Managing an unreleased script	On the version management page, click **Release**, **Modify**, or **Delete** in the **Operation** column of a script that has never been released. A script can only have one released version. Tasks associated with an unreleased version cannot be executed. After the version is released again, the tasks can be executed.

12.10 Packages

The **Packages** page displays all existing packages. You can create packages, and create and execute package installation and uninstallation tasks. For details about created tasks, see **12.6 Tasks**. Each package supports up to 20 versions. Each user can create up to 1000 package versions.

Creating a Package

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Packages**. On the displayed page, click **Create Package**.

Step 4 Set parameters by referring to **Table 12-40**.

Figure 12-37 Creating a package

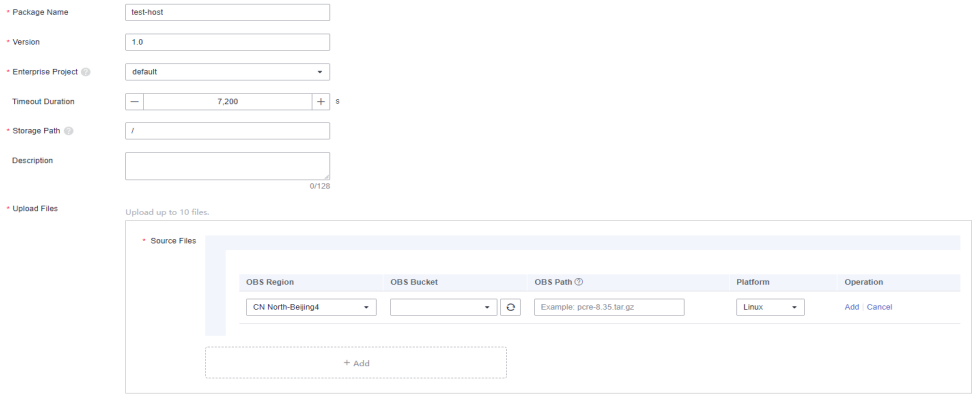


Table 12-40 Parameters for creating a package

Category	Parameter	Description
-	Package Name	Name of a package. Enter up to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
-	Version	Version of the software. Enter the actual value.
-	Enterprise Project	Select the enterprise project to which the package belongs.
-	Timeout Duration	Timeout duration of a package installation or uninstallation task.
-	Storage Path	Enter the path for storing the package distributed to the ECS.
-	Description	Description of the package. Enter up to 128 characters.
Source Files	OBS Region	Region where the OBS bucket resides. Select a region from the drop-down list.
	OBS Bucket	OBS bucket where the package is located. Select a bucket from the drop-down list.

Category	Parameter	Description
	OBS Path	Enter the path of an OBS object. Before obtaining an OBS object, choose **Settings** > **Access Credentials** to set an access credential. To copy an OBS object path, perform the following steps: 1. Click **Go to OBS** and go to the **Objects** page. 2. Select a desired object from the object list on the right and click **Copy Path** in the **Operation** column. – If **Copy Path** is not directly displayed, choose **More** > **Copy Path** in the **Operation** column. – If a folder is displayed in the **Name** column, click the folder to expand the object list, select an object, and copy the path.
	Platform	Platform on which the package runs. Currently, only Linux is supported.
	Operation	After the source file information is added, click **Add**. You can also edit or delete an added source file.
-	Platform	Platform on which the software runs. Currently, only Linux is supported.
Script Type	Install	Script for installing the software. Enter up to 1000 characters. Separate commands by ";", "&&", or "||". After the input, click **Check for High-Risk Commands** to check the script content. High-risk commands undergo regular expression verification. If the verification fails, risks may occur. For details about high-risk commands, see **Table 12-48**.
	Uninstall	Script for uninstalling software. Enter up to 1000 characters. Separate commands by ";", "&&", or "||". After the input, click **Check for High-Risk Commands** to check the script content. High-risk commands undergo regular expression verification. If the verification fails, risks may occur. For details about high-risk commands, see **Table 12-48**.
Execution Policy	Batch Release	Specifies whether to enable batch release. By default, this function is disabled.
	Instances for Each Batch	Number of instances on which tasks can be executed at the same time.
	Interval	Interval for executing each batch of tasks.

Category	Parameter	Description
Review	Review	Specifies whether to enable manual review. By default, this function is disabled. You can only modify the review configuration by modifying the atomic service card in the tool market.
	Reviewer	After manual review is enabled, you need to select a reviewer. Alternatively, create a topic and add a subscription on the SMN console to notify a reviewer.

Step 5 Click **Save**.

----End

Executing an Installation or Uninstallation Task

After a package is created, install or uninstall it as required. Script execution depends on the UniAgent capability. You need to ensure that the UniAgent has been installed and is running on the ECS where the script is to be executed.

Step 1 In the navigation pane, choose **Packages**. On the **Packages** page, locate the target package and click **Install** or **Uninstall** in the **Operation** column.

Step 2 On the package installation or uninstallation page, select an OS account from the **Execution Account** drop-down list.

Step 3 Select target instances.

1. Click **Add**. The instance selection page is displayed.
2. For **Instance Type**, the default value is **ECS**. For **Method**, the default value is **Specific**. For details about the methods, see **Table 12-41**.

Figure 12-38 Adding instances

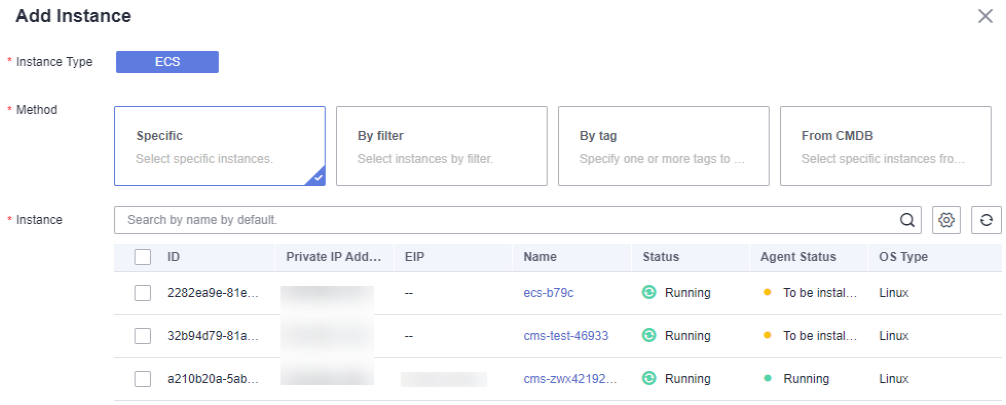


Table 12-41 Selection method description

Selection Method	Description
Specific	Enter search criteria and select instances from the instance list. By default, instances are searched by name.
By filter	– Enter filter attributes and values to search for instances. – If there are multiple filter criteria, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
By tag	– Set tag keys and values, and specify one or more tags to select instances. – If there are multiple tags, the search is performed based on the AND relationship. – This method also takes effect for instances added later.
From CMDB	Enter search criteria or keywords and select instances from CMDB. There are two types of nodes: – **Static**: Select an ECS under a specified CMDB application. – **Dynamic**: Select a node in the CMDB application to dynamically obtain ECSs under the node. This method also takes effect for instances added later.

3. Click **OK**.

Step 4 Click **Execute**. On the task execution page that is displayed, view the task execution status.

You can also click **Save**. The created task is displayed on the task management page for subsequent task execution or other operations.

----End

More Operations

After a package is created, you can go to its details page and view the basic information, status, number of tasks referenced by scheduled O&M, number of tasks referenced by standard O&M, and version list of the file package. You can also perform the operations listed in **Table 12-42**.

Table 12-42 Related operations

Operation	Description
Creating a version	Click **Create Version** in the upper right corner.

Operation	Description
Modifying the package information	Click **Modify** in the upper right corner to modify parameters.
Installing or uninstalling a package	Locate the target version and click **Install Package** or **Uninstall Package** in the **Operation** column.
Copying and creating a package version	Locate the target version and click **Copy and Create** in the **Operation** column to copy the content of one version for creating another version.
Releasing a version	Locate the target version and click **Release** in the **Operation** column.
Modifying a version	Locate the target version, click **Modify** in the **Operation** column, and modify information such as the version, file source, and platform.
Deleting a version	Locate the target version and click **Delete** in the **Operation** column.

12.11 Settings

12.11.1 OS Accounts

You can manage different types of system accounts for script execution and package management. Each user can create up to 100 accounts.

Creating an Account

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Settings** > **OS Accounts**.

Step 4 Click **Create Account** in the upper right corner.

Step 5 Set parameters by referring to **Table 12-43**.

Figure 12-39 Creating an account

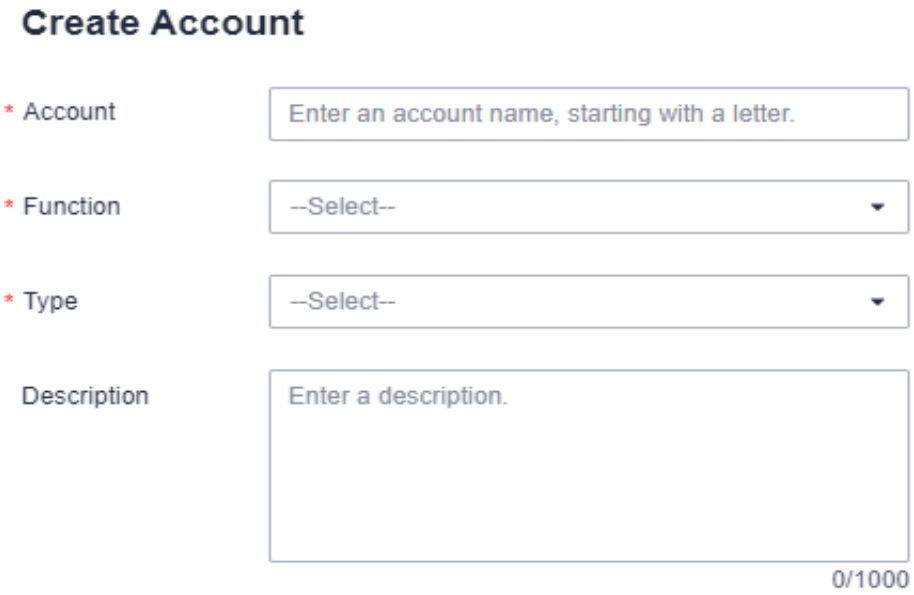


Table 12-43 Parameters for creating an account

Parameter	Description
Account	Name of an account. Enter up to 64 characters starting with a letter. Only digits, letters, and underscores (_) are allowed.
Function	Function of the account. Select your desired function from the drop-down list.
Type	Type of the account. Select your desired type from the drop-down list.
Description	Description of the account.

Step 6 Click **Yes**.

----End

More Operations

After creating an account, you can view the account information on the account list page and perform operations listed in **Table 12-44**.

Table 12-44 Related operations

Operation	Description
Modifying an account	Click **Modify** in the **Operation** column.

Operation	Description
Deleting an account	Click **Delete** in the **Operation** column.
Searching for an account	By default, the search is based on the account name. Enter a keyword in the search box above the list and click  .
Hiding/Showing columns in the account list	Click  and select or deselect columns to display.
Refreshing the account list	Click  to refresh the account list.

12.11.2 Access Credentials

To obtain packages from OBS, obtain an access credential first. Each user can create only one credential.

Creating a Credential

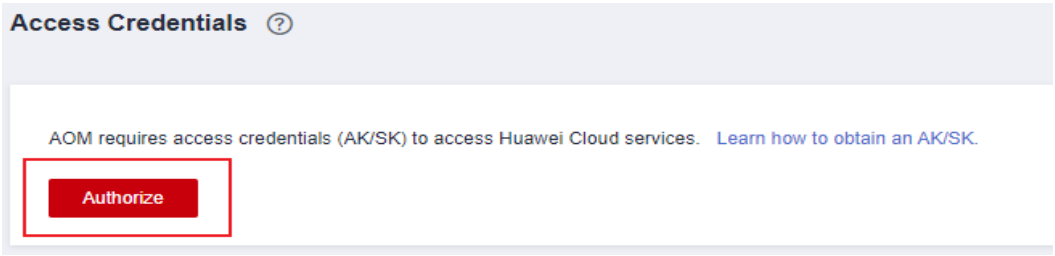
Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose Automation (Retiring). The Automation page is displayed.

Step 3 In the navigation pane, choose **Settings** > **Access Credentials**.

Step 4 Click **Authorize**.

Figure 12-40 Access credential



Step 5 On the **Create Credential** page that is displayed, set the parameters listed in the following table.

Table 12-45 Creating a credential

Parameter	Description
Account	Account name corresponding to the credential. Enter up to 64 characters.
AK	Access key ID.

Parameter	Description
SK	Secret access key.
Description	Description of the credential.

Step 6 Click **OK**.

----End

More Operations

After creating a credential, you can view the credential information on the credential list page and perform operations listed in **Table 12-46**.

Table 12-46 Related operations

Operation	Description
Modifying a credential	Click **Modify** in the **Operation** column.
Deleting a credential	Click **Delete** in the **Operation** column. After the credential is deleted, it will not be displayed. You can create another credential instead. For details, see **Creating a Credential**.

12.11.3 Scenarios

Automation can be used in the following scenarios:

- Troubleshooting
- Routine Inspection
- Software Deployment
- Cloud Services
- Common

12.12 Tool Market

The tool market classifies tool cards based on **12.11.3 Scenarios**. Currently, the following tool cards are supported:

- Common: **12.9 Scripts** and **12.10 Packages**
- Cloud services: **12.4.2 Starting an ECS**, **12.4.3 Stopping an ECS**, **12.4.4 Restarting an RDS DB Instance**, **12.4.5 Changing an ECS Non-Administrator Password**, and **12.4.6 Restarting a CCE Workload**
- Software deployment: None
- Routine inspection: None
- Troubleshooting: **12.4.7 Clearing Disk Space**

Card Management

On the **Tool Market** page, you can directly create a task based on a card. You can also remove, publish, or set a non-common scenario card by referring to **Table 12-47**.

NOTE

If you do not need to remove, publish, or set a card, prohibit card modifications by referring to **12.3.2 Custom Policies for Automation**.

Table 12-47 Related operations

Operation	Description
Creating a task	Click a card or click ⋮ in the upper right corner of the card and choose **Create Task**.
Removing a card	• Click ⋮ in the upper right corner of a card and choose **Remove**. After the card is removed, it will no longer be displayed on the service scenario page. In addition, atomic tasks associated with the atomic service scenario cannot be executed. They can be executed only when the atomic service scenario card is published again. • Before removing a service, check whether it has been referenced by a scheduled O&M scenario. If yes, delete the scenario first. For details, see **Reference Details**.
Publishing a card	Click ⋮ in the upper right corner of the card and choose **Publish**. After being published, the card can be used.
Setting a card	Click ⋮ in the upper right corner of the card and choose **Settings** to set the review and execution policy. • Review – Specifies whether to enable manual review. By default, this function is disabled. – After manual review is enabled, you need to select a reviewer. – Currently, review notifications can be sent by email or SMS. • Execution Policy – Specifies whether to enable batch release. By default, this function is disabled. – **Instances for Each Batch**: number of instances on which tasks can be executed at the same time. – **Interval**: interval for executing each batch of tasks.

12.13 High-Risk Commands

High-risk commands affect the normal running of the system or services, or cause special system files to be maliciously deleted or modified. For high-risk commands related to Automation, see **Table 12-48**.

Table 12-48 Description of high-risk commands

High-Risk Command Name	Verification Rule	Example	Risk
vi /etc/xxx.xx command	\\s*(vi|vim)\\s+/(boot|etc|lib|sys|selinux|bin|sbin|root|usr|var|proc|opt|srv)+\\s*	vi /etc/vconsole.conf	Modifying system files may affect the normal running of the system and services or make your system unrecoverable.
service xxx restart/stop command	\\s*service\\s+.*\\s+(restart|stop)\\s*	service network stop	If a command contains **service xxx restart/stop**, services may be restarted or stopped, affecting the normal running of the system or services.
mkfs.ext3 /dev/sdxxx command	\\s*mkfs\\.ext3\\s+/dev/[a-z]d[a-z]+\\s*	mkfs.ext3 /dev/sda	If a command contains **mkfs.ext3 /dev/xdxxx**, the block device will be formatted, making your system unrecoverable.
umount command	\\s*umount\\s+.*	umount -v /dev/sda1	The normal running of the system or services may be affected.
poweroff command	\\s*poweroff\\s*	poweroff	If a command contains **poweroff**, hosts may be powered off, affecting the system or service running.
kill command	\\s*kill\\s+.*	kill 12345	If a command contains **kill**, the running programs or tasks may be deleted, affecting the normal running of the system or services.

High-Risk Command Name	Verification Rule	Example	Risk
mv xxx /dev/null command	\\s*mv\\s+.*\\s+/dev/null\\s*	mv test /dev/null	If a command contains **mv xxx /dev/null**, **xxx** files may be deleted.
xxx > /dev/sdx command	\\s*.*\\s+>\\s+/dev/sd[a-z]+\\s*	cat test.txt > /dev/sda	If a command contains **> /dev/xdx**, all data in the path may be lost.
init 0 command	\\s*init\\s+0\\s*	init 0	If a command contains **init 0**, hosts may be shut down, affecting the normal running of the system or services.
reboot command	\\s*reboot\\s*	reboot	If a command contains **reboot**, a device may be restarted, affecting the normal running of the system or services.
halt command	\\s*halt\\s*	halt	If a command contains **halt**, a device may be powered off, affecting the normal running of the system or services.
Fork Bomb	\\s*:\\(\\)\\{:\\|:&\\};:\\s*	:(){:|:&};:	Command injection attacks may occur, causing system breakdown.
rm command	\\s*rm\\s+.*	rm test.txt	If a command contains **rm**, special system files may be maliciously deleted or modified.
> file command	\\s*>\\s+.*	> file	If a command contains **>**, the file content may be cleared.
dd if=/dev/random of=/dev/sdxxx command	\\s*dd\\s+if=/dev/random\\s+of=/dev/sd[a-z]+\\s*	dd if=/dev/random of=/dev/sda	Random junk files are written to block device sdxxx to erase data. As a result, the system may become disordered and cannot be recovered.

High-Risk Command Name	Verification Rule	Example	Risk
shutdown command	\\s*shutdown\\s+.*	shutdown -h now	If a command contains **shutdown**, hosts may be shut down, affecting the system or service running.

13 Settings

13.1 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

13.2 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 13-1**.

Table 13-1 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.

13.3 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.

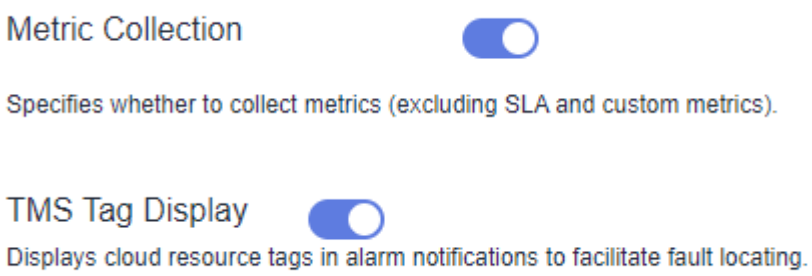
Procedure

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 Settings**. Enable or disable functions as required.

Figure 13-1 Global settings



NOTE

After metric collection is disabled, ICAgents will stop collecting metric data and related metric data will not be updated. However, custom metrics can still be reported.

----End

13.4 Data Subscription

AOM allows you to subscribe to metrics or alarms. After the subscription, data can be forwarded to DMS or Webhook topics for you to retrieve.

A maximum of 10 data subscription rules can be created.

NOTE

Webhook subscription is not yet generally available. If you want to use this function, **submit a service ticket**.

Creating a Subscription Rule

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 **Data Subscription**. Click **Create Subscription Rule**. On the displayed page, set **Subscription Content** to **Distributed Message Service (DMS)** or **Webhook** as required.

- When **Subscription Content** is set to **DMS**:
  a. Set parameters by referring to **Table 13-2** and click **OK**.

Table 13-2 Subscription rule parameters

Parameter	Description
Rule Name	Name of a subscription rule. Only letters, digits, hyphens (-), and underscores (_) are allowed. Enter up to 64 characters starting with a letter.
Subscription Content	Select **Distributed Message Service (DMS)**.
Data Type	Options: **Metric** and **Alarm**.
Instance	Select a DMS instance from the drop-down list. If the existing DMS instances do not meet your requirements, click **Create DMS Instance** to create one.

b. Verify the DMS instance connectivity.

   To subscribe data to DMS, ensure that you have created the **apm_admin_trust** agency on IAM.

c. Enter the DMS username and password.

d. Click **Verify and Save DMS Configuration**.

e. Select a topic for transmitting data and click **OK**.

- Set **Subscription Content** to **Webhook**.

  Set parameters by referring to **Table 13-3** and click **OK**.

Table 13-3 Subscription rule parameters

Parameter	Description
Rule Name	Name of a subscription rule. Only letters, digits, hyphens (-), and underscores (_) are allowed. Enter up to 64 characters starting with a letter.
Subscription Content	Select **Webhook**.
Address	Enter the remote write address of the Prometheus instance on the user side as the destination to which metrics are sent. Select a protocol used to send requests from the drop-down list box. HTTPS is recommended.
Data Type	Default: **Metric**
Prometheus Instance	Select the Prometheus instance whose metrics need to be forwarded. All Prometheus instances for remote write under your account are displayed in the drop-down list.

Parameter	Description
Authentication Mode	Mode for authenticating access to the Prometheus instance on the user side. – **Token**: A token is required for authentication. – **None**: No authentication is required.

After the rule is created, you can view it in the rule list.

----End

Data Subscription Format

- Metric data example (in JSON format)

```
package metric

type MetricDatas struct {
  Metrics   []Metrics `json:"metrics"`
  ProjectId string    `json:"project_id"`
}

type Metrics struct {
  Metric      Metric  `json:"metric"`
  Values      []Value `json:"values"`
  CollectTime int64   `json:"collect_time"`
}

type Metric struct {
  Namespace  string      `json:"namespace"`
  Dimensions []Dimension `json:"dimensions"`
}

type Value struct {
  Value           interface{} `json:"value"`
  Type            string      `json:"type"`
  Unit            string      `json:"unit"`
  StatisticValues string      `json:"statisticvalues"`
  MetricName      string      `json:"metric_name"`
}

type Dimension struct {
  Name  string `json:"name"`
  Value string `json:"value"`
}
```

- Kafka message example

```
key:,
value:{"metrics":[{"metric":{"namespace":"PAAS.NODE","dimensions":
[{"name":"nodeName","value":"test-aom-4-vss-cop-master-1"},{"name":"nodeIP","value":"1.1.1.1"},
{"name":"hostID","value":"75d97111-4734-4c6c-ae9e-f6111111111"},
{"name":"nameSpace","value":"default"},
{"name":"clusterId","value":"46a7bc0d-1d8b-11ea-9b04-333333333333333"},
{"name":"clusterName","value":"test-aom-4-vss-111"},{"name":"diskDevice","value":"vda"},
{"name":"master","value":"true"}]},"values":[{"value":0,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskReadRate"},{"value":30.267,"type":"","unit":"Kilobytes/
Second","statisticvalues":"","metric_name":"diskWriteRate"}],"collect_time":1597821030037}],"project_i
d":"11111111111111111111"}
```

- Alarm data format

Example:


```
{
   "events": [{
      "id": "4346299651651991683",
      "starts_at": 1597822250194,
      "ends_at": 0,
      "arrives_at": 1597822250194,
      "timeout": 300000,
      "resource_group_id": "31231312311222222222232131312131",
      "metadata": {
         "kind": "Pod",
         "event_severity": "Major",
         "resource_type": "service",
         "clusterId": "6add4ef5-1358-11ea-a5bf-111111111",
         "event_type": "alarm",
         "clusterName": "cce-ief-4516140c-96ca-4a5f-8d85-1111111",
         "namespace": "PAAS.NODE",
         "name": "test15769793809553052-f5557bd7f-qnfkm",
         "event_name": "FailedScheduling",
         "resource_id": "clusterName=cce-
ief-4516140c-96ca-4a5f-8d85-111111;clusterID=6add4ef5-1358-11ea-
a5bf-11111111111;kind=Pod;namespace=30d5758f166947c6b164af604a654b09;name=test157697938
09553052-f5557bd7f-qnfkm;uid=589fc746-245d-11ea-a465-fa163e5fc15d",
         "nameSpace": "30d5758f166947c6b164af604a654b09",
         "resource_provider": "CCE",
         "nodeID": "589fc746-245d-11ea-a465-fa163e5fc15d"
      },
      "annotations": {
         "alarm_probableCause_zh_cn": "FailedScheduling",
         "alarm_probableCause_en_us": "FailedScheduling",
         "message": "0/110 nodes are available: 1 node(s) had taints that the pod didn't tolerate, 109
node(s) didn't match node selector."
      },
      "attach_rule": {

      }
   }],
   "project_id": "31231312311222222222232131312131"
}
```


Parameter description:

Table 13-4 Alarm parameters

Parameter	Type	Description
events	Array of objects. For details, see **Table 13-5**.	Event or alarm details.
project_id	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 13-5 Event model

Parameter	Type	Description
id	String	Event or alarm ID, which is automatically generated by the system.

Parameter	Type	Description
starts_at	Long	Time when an event or alarm is generated. The value is a China Standard Time (CST) timestamp precise down to the millisecond.
ends_at	Long	Time when an event or alarm is cleared. The value is a CST timestamp precise down to the millisecond. If the value is **0**, the event or alarm is not deleted.
arrives_at	Long	Time when an event or alarm reaches AOM. The value is a CST timestamp precise down to the millisecond.
timeout	Long	Duration at which an alarm is automatically cleared. Unit: ms. For example, if the duration is 1 minute, set this parameter to **60000**. The default duration is three days.
resource_group_id	String	Reserved field for a resource group. The default value is the same as the value of **projectid**.
metadata	Object	Details of an event or alarm. The value is a key-value pair. The following fields are mandatory: ● **event_name**: event or alarm name, which is a string. ● **event_severity**: event severity, which is an enumerated value. It is a string. Options: **Critical**, **Major**, **Minor**, and **Info**. ● **event_type**: Event type, which is an enumerated value. Options: **event** and **alarm**. ● **resource_provider**: Name of a cloud service corresponding to an event, which is a string. It is a string. ● **resource_type**: Resource type corresponding to an event. It is a string. ● **resource_id**: ID of the resource corresponding to the event. It is a string.
annotations	Object	Additional field for an event or alarm, which can be left blank.
attach_rule	Object	Reserved field for an event or alarm, which can be left blank.

Follow-up Operations

After the data subscription rule is created, AOM will send data to your DMS or Webhook topic so that you can retrieve the subscribed metrics or alarms.

13.5 Menu Settings

You can choose to show or hide **Overview**, **Application Insights**, **Automation**, **Cloud Service Monitoring**, **Log Stream**, and **Business Monitoring** in the navigation pane of the console.

Procedure

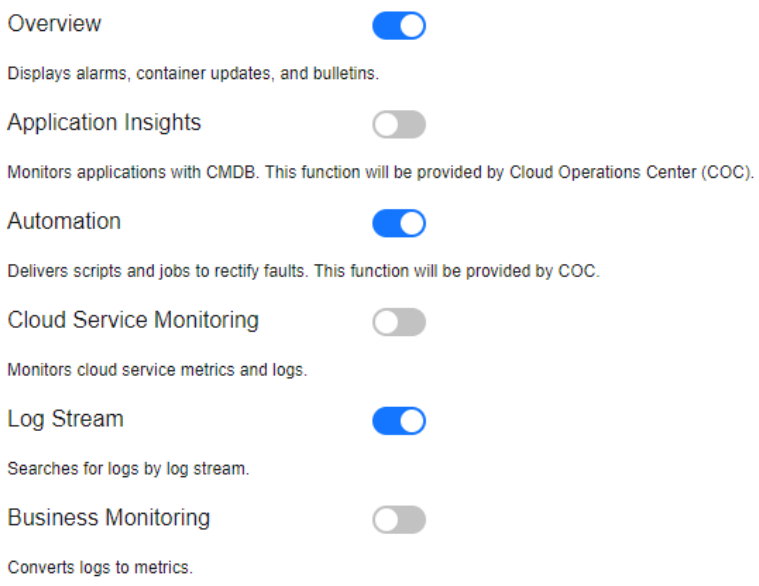
Step 1 Log in to the AOM 2.0 console.

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.

Figure 13-2 Menu settings



----End

14 Remarks

14.1 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. You can create up to 10 custom tags. The key and value can only contain 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 4-32**.

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 4-32**.

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 Alarm Rule**, 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 + Tag 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 + Tag 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

14.2 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 14-1 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 14-1 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="cdbc06c2c05b58d598e9430fa133aff7_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"}

14.3 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 14-2 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

15 Permissions Management

15.1 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.

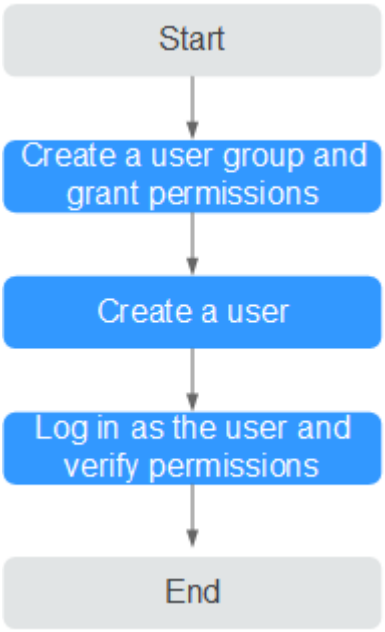
This section describes the procedure for granting permissions (see **Figure 15-1**).

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-defined Permissions**.

Process

Figure 15-1 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.

15.2 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"
            ]
        }
    ]
}
```


16 Auditing

16.1 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 16-1 Operations logged by CTS

Function	Operation	Resource Type	Trace
Global Configuration	Adding an access code	icmgr	icmgrAddAccessCode
	Deleting an access code	icmgr	icmgrDelAccessCode
CMDB	Creating an application	application	createApp
	Updating an application	application	updateApp

Function	Operation	Resource Type	Trace
	Deleting an application	application	deleteApp
	Creating an application (for other services to invoke)	application	createAomApp
	Modifying the EPS ID of an application (for EPS to invoke)	application	updateAppEpsId
	Adding a sub-application	sub_application	createSubApp
	Deleting a sub-application	sub_application	deleteSubApp
	Updating a sub-application	sub_application	updateSubApp
	Creating a sub-application (for other services to invoke)	sub_application	createAomSubApp
	Transferring a sub-application	sub_application	transferSubApp
	Adding a component	component	createComponent
	Transferring a component	component	transferComponent
	Updating a component	component	updateComponent
	Deleting a component	component	deleteComponent
	Creating a component (for other services to invoke)	component	createAomComponent
	Creating an environment	environment	createEnvironment
	Modifying an environment	environment	updateEnvironment

Function	Operation	Resource Type	Trace
	Deleting an environment	environment	deleteEnvironment
	Creating an environment (for other services to invoke)	environment	createAomEnv
	Creating an environment tag	tag	createTag
	Updating a tag	tag	updateTag
	Deleting an environment tag	tag	deleteTag
	Updating an environment tag	tag	updateEnvTag
	Adding a multi-cloud account	cloud_account	addCloudAccount
	Modifying a multi-cloud account	cloud_account	updateCloudAccount
	Deleting a multi-cloud account	cloud_account	deleteCloudAccount
	Creating a workload	workload	createWorkload
	Deleting a workload	workload	deleteWorkload
	Updating a workload	workload	updateWorkload
	Reporting ECS information	ecs	aomImportECS
Resource Monitoring	Creating a dashboard	dashboard	updateDashboard
	Deleting a dashboard	dashboard	deleteDashboard
	Updating a dashboard	dashboard	updateDashboard
	Creating a dashboard group	dashboard_folder	addDashboardFolder
	Updating a dashboard group	dashboard_folder	updateDashboardFolder

Function	Operation	Resource Type	Trace
	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
	Creating a data subscription rule	apminventory	createSubscribeRule
	Verifying DMS connectivity	apminventory	verifyConnect
	Deleting a data subscription rule	apminventory	deleteSubscribeRule
	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
Automation	Enabling the Automation service	function	functionRegister
	Updating user information	function	functionRegister
	Updating a task timer trigger	workflow	operateCronTriggerFlow
	Creating a task	workflow	createWorkflow
	Modifying a task	workflow	updateWorkflow
	Executing a task	execution	execute
	Stopping a task	execution	terminateWorkflow
	Deleting a task	workflow	deleteWorkflow
	Creating a job execution plan	template	createTemplate
	Release a job execution plan	template	publishTemplate
	Deleting a job execution plan	template	deleteTemplate

Function	Operation	Resource Type	Trace
	Creating an account	account	createAccount
	Updating an account	account	updateAccount
	Deleting an account	account	deleteAccount
	Creating global parameters	param	createParams
	Deleting global parameters	param	deleteParams
	Creating a package	package	createPack
	Updating a package	package	updateBasicPack
	Deleting a package	package	deletePack
	Creating a job	job	createJob
	Updating a job	job	updateJob
	Deleting a job	job	deleteJobByJobId
	Applying for a review	approve	createApprove
	Saving the review setting	approve	saveApprove
	Creating a script version	script	createScriptAndVersion
	Updating a script version	script	updateVersionByVersionId
	Deleting a script version	script	deleteVersionByVersionId
	Publishing a service	serviceScenario	onboardToolMarketTenantInfo
	Adding a service to favorites	serviceScenario	serviceScenarioFavorites
	Updating a script	script	updateScript
	Executing a script	ecs	runScript

16.2 Querying Real-Time Traces

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 OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and 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

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

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.

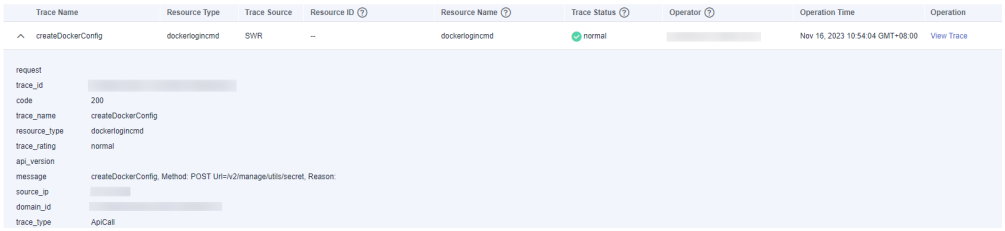
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and press Enter to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 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

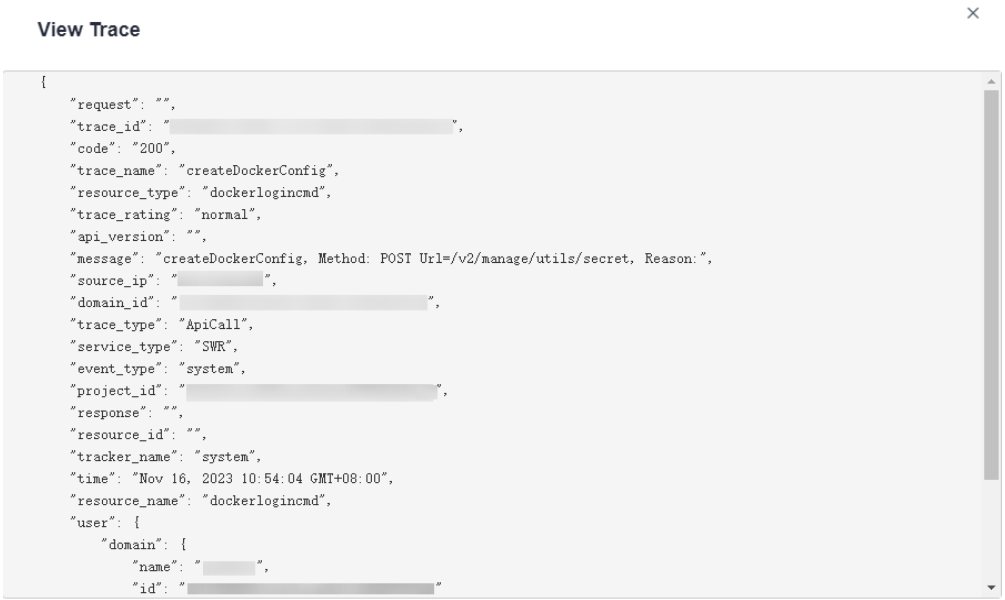
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed 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: You can query traces generated during any time range in the last seven days.
- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

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 5000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

17 Subscribing to AOM 2.0

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

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

NOTE

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

Procedure

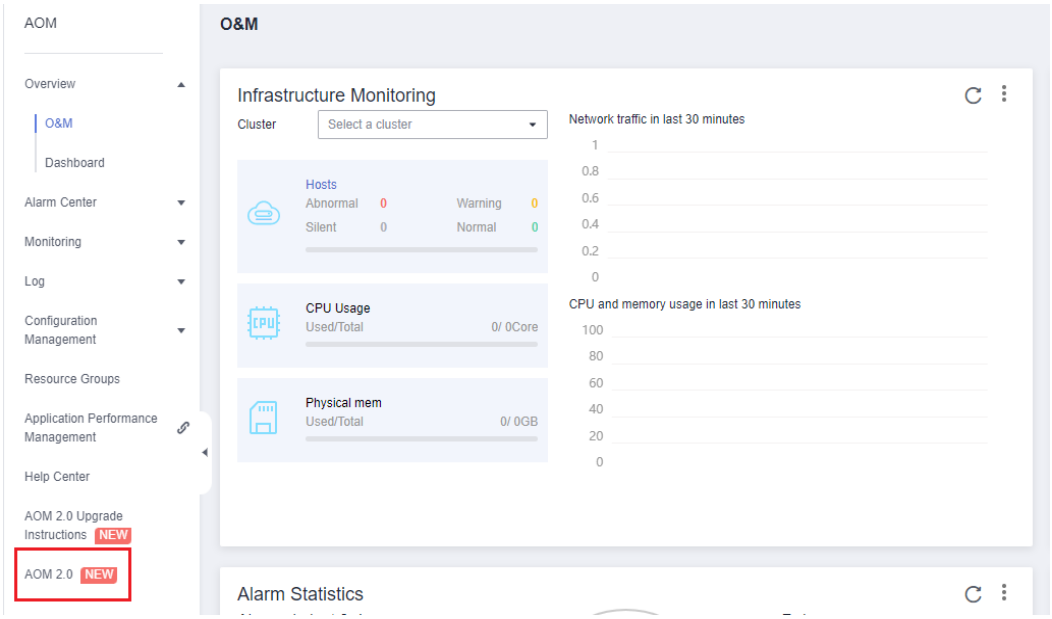
Step 1 Log in to the Huawei Cloud management console.

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

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

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

Figure 17-1 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

18 Upgrading to AOM 2.0

18.1 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

- **Log Upgrade**

  After the log upgrade, container logs and VM logs are connected to AOM 2.0. You can log in to AOM 1.0 to view historical VM logs.
- **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.

Log Upgrade

Step 1 Log in to the AOM 2.0 console.

Step 2 Ingest container and VM logs:

- Ingestion of container logs: Choose **LTS Access** and ingest container logs as prompted. For details, see **Adding Access Rules**.
- Ingestion of VM logs: Choose **Log Ingestion** and ingest VM logs as prompted. For details, see **Ingesting Logs**.

----End

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

18.2 One-click Migration

Quickly migrate dashboard and alarm rule data from AOM 1.0 to AOM 2.0.

Precautions

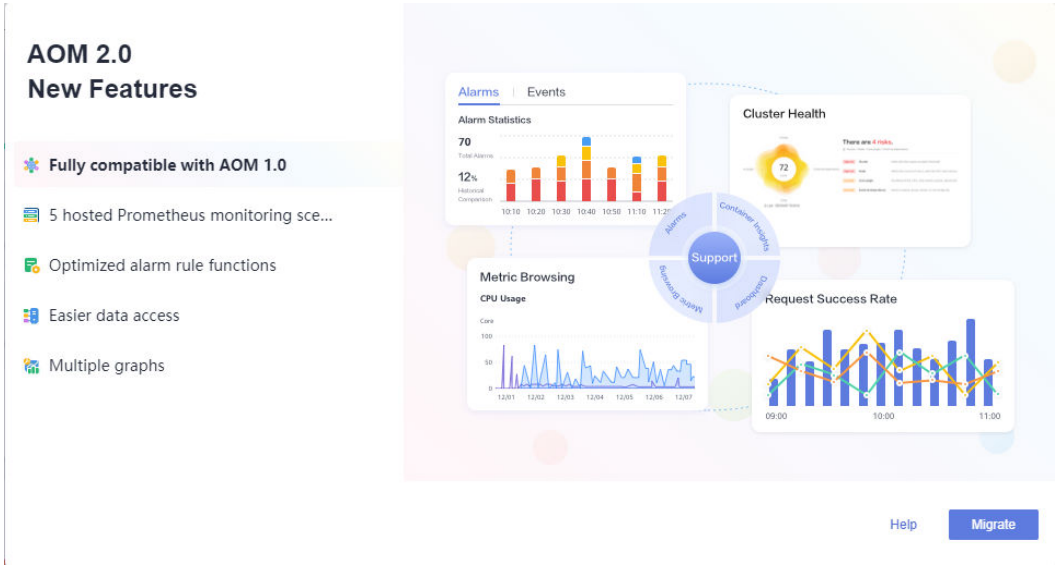
- AOM allows you to migrate all alarm rules in one click and query migration results.
- The backend checks data migration status:
  - Migrated: A dialog box is displayed, indicating that the migration is complete.
  - Not migrated: The one-click migration dialog box is displayed.
  - Migrating: A dialog 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.

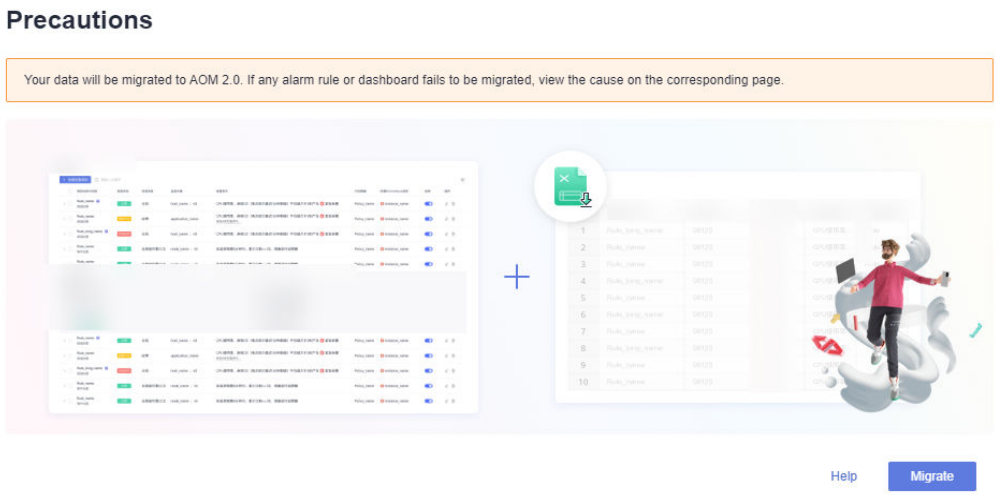
Step 2 In the **AOM 2.0 New Features** dialog box, click **Migrate**.

Figure 18-1 New features dialog box



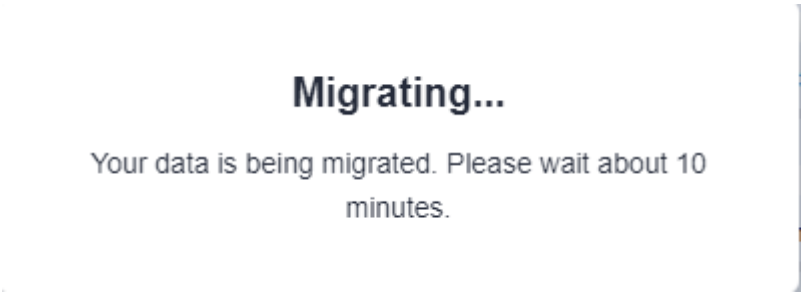
Step 3 In the **Precautions** dialog box, click **Migrate**.

Figure 18-2 Precautions dialog box



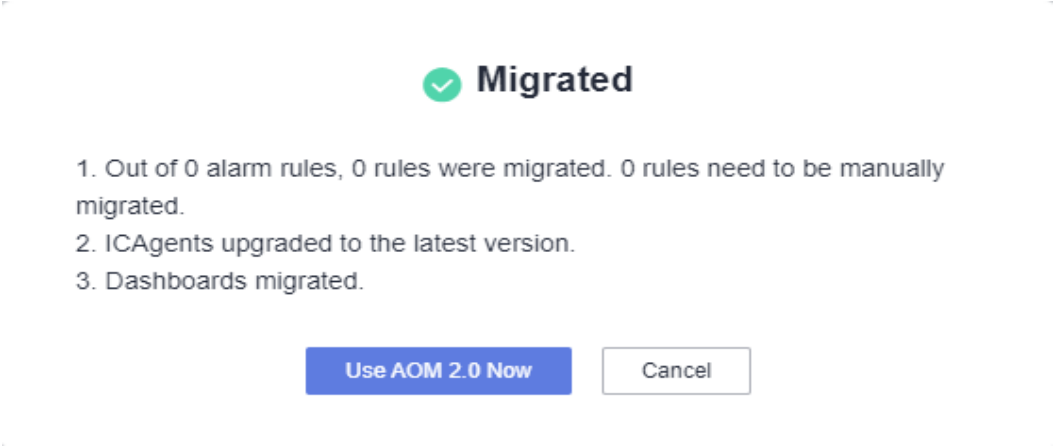
Step 4 The migration starts. A dialog box is displayed, showing "Migrating".

Figure 18-3 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 18-4 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

